Guía del administrador de PAN-OS®

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 10, 2020

Table of Contents

Primeros pasos 19
Integración del firewall en la red de gestión 21
Determinación de la estrategia de gestión 21
Realización de la configuración inicial 22
Establecimiento de acceso a la red para servicios externos 27
Registro del cortafuegos 34
Cree una nueva cuenta de soporte y registre un cortafuegos 34
Registre un cortafuegos 36
(Opcional) Configuración inicial 38
Segmentar su red con interfaces y zonas 41
Segmentación de la red para una superficie de ataque reducida 41
Configuración de interfaces y zonas 41
Configuración de una política de seguridad básica 45
Evaluación del tráfico de red 49
Habilitación del reenvío gratuito de WildFire 51
Prácticas recomendadas para completar la implementación del cortafuegos 53
Prácticas recomendadas para proteger el acceso administrativo 54
Aislamiento de la red de gestión 54
Uso de rutas de servicio para acceder a servicios externos 55
Restricción de acceso a la interfaz de gestión 56
Gestión del acceso de administrador 58
Creación de contraseñas de administrador seguras 59
Búsqueda de todo el tráfico destinado a la interfaz de gestión 59
Sustitución del certificado para el tráfico de gestión entrante 61
Mantenimiento de las actualizaciones de contenido y software 61

Suscripciones 63
Suscripciones disponibles para los cortafuegos 65
Activación de licencias de suscripción 68
¿Qué ocurre cuando la licencia caduca? 70
Logs mejorados de aplicaciones para servicios en la nube de Palo Alto Networks 72

Actualizaciones de software y contenido 75
Actualizaciones del software PAN-OS 77
Actualizaciones dinámicas de contenido 78
Instalación de actualizaciones de contenido 80
Actualización de contenido de aplicaciones y amenazas 83
Implementación de actualizaciones de contenido de aplicaciones y amenazas 84
Sugerencias para las actualizaciones de contenido 85
Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas 87
Prácticas recomendadas para las actualizaciones de contenido: nivel crítico 87
Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad 91
Infraestructura de red de entrega de contenido 94

Administración del cortafuegos 95

Interfaces de gestión....97
Uso de la interfaz web....98
Inicio de la interfaz web....98
Configuración de banners, mensaje del día y logotipos....99
Uso de los indicadores de actividad de inicio de sesión de administrador para detectar el uso indebido de la cuenta....100
Gestión y supervisión de tareas administrativas....103
Confirmación, validación y previsualización de los cambios de configuración del cortafuegos....103
Exportación de los datos de la tabla de configuración....106
Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama....107
Gestión de bloqueos para restringir cambios de configuración....109
Gestión de las copias de seguridad de la configuración....111
Guardado y exportación de configuraciones de cortafuegos....111
Reversión de los cambios de configuración del cortafuegos....113
Gestión de los administradores de cortafuegos....116
Tipos de funciones administrativas....116
Configuración de un perfil de función de administrador....117
Autenticación administrativa....118
Configurar cuentas y autenticación administrativa....119
Referencia: acceso de administrador a la interfaz web....126
Privilegios de acceso a la interfaz web....126
Privilegios de Acceso a la interfaz web de Panorama....193
Referencia: Uso de número de puerto....198
Puertos usados para funciones de gestión....198
Puertos usados para HA....199
Puertos usados para Panorama....200
Puertos usados para GlobalProtect....201
Puertos usados para User-ID....202
Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica....205
Arranque del cortafuegos....206
Soporte de la unidad Flash USB....206
Archivos init-cfg.txt de muestra....206
Preparación de una unidad Fash USB para el arranque de un cortafuegos....208
Arranque de un cortafuegos usando una unidad Flash USB....211

Telemetría de dispositivos....213
Descripción general de telemetría de dispositivos....215
Recopilación de telemetría de dispositivos e intervalos de transmisión....216
Gestión de telemetría de dispositivos....217
Habilitación de telemetría de dispositivos....217
Deshabilitación de telemetría de dispositivos....217
Gestión de datos que recopila la telemetría de dispositivos....218
Gestión de telemetría de dispositivos histórica....218
Supervisión de telemetría de dispositivos....220
Muestra de los datos que recopila la telemetría de dispositivos....221

Autenticación....223
Tipos de autenticación....225
Servicios de autenticación externos....225
Autenticación de múltiples factores....225
SAML....226

Kerberos ... 227
TACACS+ ... 228
RADIUS ... 229
LDAP: ... 230
Autenticación local ... 231
Planificación de su implementación de autenticación ... 232
Configuración de la autenticación multifactor ... 233
Configuración de la MFA entre SecurID de RSA y el cortafuegos ... 236
Configuración de la MFA entre Okta y el cortafuegos ... 243
Configuración de la MFA entre Duo y el cortafuegos ... 252
Configuración de la autenticación SAML ... 262
Configuración de un inicio de sesión único de Kerberos ... 267
Configuración de la autenticación del servidor Kerberos ... 269
Configuración de la autenticación TACACS+ ... 270
Configuración de la autenticación RADIUS ... 273
Configuración de la autenticación LDAP ... 277
Tiempos de espera de conexión de los servidores de autenticación ... 279
Directrices de configuración de tiempo de espera de autenticación ... 279
Modificación del tiempo de espera de servidor web de PAN-OS ... 280
Modificación del tiempo de espera de sesión del portal de autenticación ... 280
Configuración de la autenticación de la base de datos local ... 282
Configuración de una secuencia y perfil de autenticación ... 283
Comprobación de la conectividad del servidor de autenticación ... 287
Política de autenticación ... 289
Marcas de tiempo de la autenticación ... 289
Configuración de la información de autenticación ... 290
Solución de problemas de autenticación ... 293

Gestión de certificados ... 295
Claves y certificados ... 297
Entidades de certificación (CA) de confianza predeterminadas ... 300
Revocación de certificados ... 301
Lista de revocación de certificados (CRL) ... 301
Protocolo de estado de certificado en línea (OCSP) ... 302
Implementación de certificados ... 303
Configuración de la verificación del estado de revocación de certificados ... 304
Configuración de un OCSP responder ... 304
Configuración de la verificación del estado de revocación de los certificados ... 305
Configuración de la verificación del estado de revocación de certificados utilizados para el descifrado SSL/TLS ... 305
Configuración de la clave maestra ... 307
Cifrado de la clave maestra ... 310
Configuración del nivel de cifrado de la clave maestra ... 310
Cifrado de la clave maestra en un par de HA de cortafuegos ... 312
Logs de cifrado de la clave maestra ... 312
Cifrados de la clave maestra únicos para AES-256-GCM ... 312
Obtención de certificados ... 314
Creación de un certificado de CA raíz autofirmado ... 314
Generar un certificado ... 315
Importación de un certificado y una clave privada ... 316
Obtención de un certificado desde una CA externa ... 317
Instalación de un certificado del dispositivo ... 319
Implementación de certificados utilizando SCEP ... 319
Exportación de un certificado y una clave privada ... 323

Configuración de un perfil de certificado....324
Configuración de un perfil de servicio SSL/TLS....326
Configuración de un perfil de servicio SSH....328
Creación de un perfil de administración SSH....328
Creación de un perfil de HA SSH....330
Sustitución del certificado para el tráfico de gestión entrante....333
Configuración del tamaño de clave para los certificados de servidor proxy SSL de reenvío....334
Revocación y renovación de certificados....335
Revocación de un certificado....335
Renovación de un certificado....335
Claves seguras con módulos de seguridad de hardware....336
Configuración de la conectividad con un HSM....336
Cifrado de una clave maestra utilizando un HSM....342
Almacenamiento de claves privadas en un HSM....343
Gestión de la implementación del HSM....344

High Availability....345
Descripción general de la alta disponibilidad....347
Conceptos de HA....348
Modos de HA....348
Enlaces de HA y enlaces de backup....349
Prioridad y preferencia de dispositivos....354
Conmutación por error....354
Negociación previa de LACP y LLDP para HA activa/pasiva....356
Dirección IP flotante y dirección MAC virtual....356
Distribución de carga de ARP....358
Redundancia basada en la ruta....360
Temporizadores de HA....361
Propietario de sesión....364
Configuración de sesión....364
NAT en modo HA activa/activa....366
ECMP en modo HA activa/activa....367
Configuración de la HA activo/pasivo....368
Requisitos para la HA activa/pasiva....368
Directrices de configuración para la HA activo/pasivo....368
Configuración de la HA activa/pasiva....371
Definición de las condiciones de conmutación por error de HA....376
Verificación de conmutación por error....378
Configuración de HA activa/activa....379
Requisitos previos para la HA activa/activa....379
Configuración de la HA activa/activa....380
Determinación del caso de uso activo/activo....385
Descripción general de agrupación en clústeres de HA....401
Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA....404
Configuración de la agrupación en clústeres de HA....406
Actualización de las claves de SSH de HA1 y configuración de sus opciones....409
Estados del cortafuegos HA....415
Referencia: Sincronización HA....417
¿Qué ajustes no se sincronizan en HA Activo/pasivo?....417
¿Qué ajustes no se sincronizan en HA Activo/activo?....420
Sincronización de información de tiempos de ejecución del sistema....424

Monitorización....427
Uso del panel....429
Uso del Centro de control de aplicaciones....431
ACC: primer vistazo....431
Pestañas de ACC....433
Widgets de ACC....435
Descripciones de widget....436
Filtros de ACC....442
Interacción con el ACC....443
Caso de uso: ACC: Ruta de descubrimiento de información....447
Uso de los informes de App Scope....454
Informe de resumen....454
Informe del supervisor de cambios....455
Informe del supervisor de amenazas....456
Informe del mapa de amenazas....457
Informe del supervisor de red....458
Informe del mapa de tráfico....459
Use el motor de correlación automatizada....461
Conceptos del motor de correlación automatizada....461
Visualización de los objetos de correlación....462
Interpretación de eventos correlacionados....463
Uso del widget de los hosts en riesgo en el ACC....465
Realización de capturas de paquetes....466
Tipos de captura de paquetes....466
Deshabilitación de descarga de hardware....467
Captura de paquetes personalizada....468
Captura de paquetes de amenazas....471
Tome una captura de paquetes de aplicaciones....473
Captura de paquetes en la interfaz de gestión....477
Supervisión de aplicaciones y amenazas....479
Visualización y gestión de logs....480
Tipos de logs y niveles de gravedad....480
Visualización de logs....487
Filtrar logs....488
Exportación de logs....489
Configuración de cuotas de almacenamiento y periodos de vencimiento de logs....489
Programación de exportaciones de logs a un servidor SCP o FTP....490
Supervisión de la lista de bloqueo....492
Visualización y gestión de informes....493
Tipos de informes....493
Visualización de informes....494
Configuración del período de vencimiento y de ejecución para los informes....495
Deshabilitación de informes predefinidos....495
Informes personalizados....495
Generación de informes personalizados....498
Generación de informes de Botnet....501
Generación de informes de uso de la aplicación SaaS....503
Gestión de informes de resumen en PDF....506
Generación de informes de actividad del usuario/grupo....507
Gestión de grupos de informes....508
Programación de informes para entrega de correos electrónicos....509
Gestión de la capacidad de almacenamiento de informes....510
Visualización de la utilización de las reglas de la política....512

Uso de servicios externos para la monitorización....516
Configuración de reenvío de logs....517
Configuración de alertas de correo electrónico....520
Uso de syslog para la monitorización....522
Configuración de la monitorización de syslog....522
Descripciones de los campos de syslog....524
Monitorización de SNMP y capturas....593
Compatibilidad de SNMP....593
Active el gestor SNMP para explorar MIB y objetos....594
Habilitación de servicios SNMP para elementos de red asegurados por el cortafuegos....597
Monitorización de estadísticas mediante SNMP....598
Reenvío de capturas a un administrador SNMP....599
MIB admitidas....601
Reenvío de logs a un destino de HTTP/S....609
Monitorización de NetFlow....612
Configuración de exportaciones de NetFlow....612
Plantillas de NetFlow....613
Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow....619
Supervisión de transceptores....622

User-ID....623
Descripción general de User-ID....625
Conceptos de User-ID....627
Asignación de grupos....627
Asignación de usuario....627
Habilitación de User-ID....632
Asignación de usuarios a grupos....636
Asignación de direcciones IP a usuarios....642
Creación de una cuenta de servicio exclusiva para el agente de User-ID....643
Configuración de la asignación de usuarios mediante el agente de User-ID de Windows....660
Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS....671
Configuración de la supervisión de servidores con WinRM....675
Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios....681
Asignación de direcciones IP a nombres de usuario mediante un portal de autenticación....690
Configuración de la asignación de usuarios para usuarios del servidor de terminal....695
Envío de asignaciones de usuarios a User-ID mediante la API XML....705
Habilitación de política basada en usuarios y grupos....706
Habilitación de política para usuarios con múltiples cuentas....707
Verificación de la configuración de User-ID....709
Implementación de User-ID en una red a gran escala....711
Implementación de User-ID para numerosas fuentes de información de asignación....711
Inserción de nombre de usuario en encabezados HTTP....716
Redistribución de las marcas de tiempo de autenticación y datos....717
Asignaciones de User-ID compartidas entre sistemas virtuales....723

App-ID 725
Descripción general de App-ID 727
Reglas de políticas de App-ID mejoradas 728
Creación de un filtro de aplicaciones mediante etiquetas 728
Creación de un filtro de aplicaciones basado en etiquetas personalizadas 729
Inspección de App-ID y HTTP/2 731
Gestión de aplicaciones personalizadas o desconocidas 733
Gestión de App-ID nuevas y modificadas 734
Flujo de trabajo para incorporar mejor las App-ID nuevas y modificadas 734
Visualización de las ID de aplicación nuevas y modificadas en una versión de contenido 735
Cómo las App-ID nuevas y modificadas afectan su política de seguridad 736
Garantizar que se permitan nuevas App-ID críticas 737
Supervisión de nuevos App-ID 739
Deshabilitación y habilitación de App-ID 740
Uso de objetos de aplicación en la política 742
Creación de un grupo de aplicaciones 742
Creación de un filtro de aplicaciones 743
Creación de una aplicación personalizada 744
Resolución de dependencias de aplicaciones 748
Habilitación segura de aplicaciones en los puertos predeterminados 750
Aplicaciones con compatibilidad implícita 752
Optimización de las reglas de la política de seguridad 756
Conceptos de Policy Optimizer 757
Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID 762
Caso de uso de migración mediante la clonación de reglas: navegación web y tráfico SSL 770
Adición de aplicaciones a reglas existentes 773
Identificación de reglas de la política de seguridad con aplicaciones no utilizadas 776
Alta disponibilidad para las estadísticas sobre el uso de las aplicaciones 780
Habilitación o deshabilitación de Policy Optimizer 780
Gateways de nivel de aplicación 782
Deshabilitación de la gateway de nivel de aplicación (ALG) SIP 784
Uso de encabezados de HTTP para la gestión del acceso a aplicaciones de SaaS 786
Comprensión de los encabezados personalizados de SaaS 786
Dominios utilizados por los tipos de aplicación SaaS predefinidos 788
Creación de entradas de inserción de encabezados HTTP utilizando tipos predefinidos 789
Creación de entradas de inserción de encabezado HTTP personalizadas 790
Mantenimiento de los tiempos de espera personalizados para aplicaciones de centros de datos 792

ID de dispositivo 795
Descripción general de Device-ID 797
Preparación para la implementación de Device-ID 800
Configuración de Device-ID 803
Gestión de Device-ID 806
Comandos de la CLI para Device-ID 808

Threat Prevention 811

Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7 813
Configuración de antivirus, antispyware y protección frente a vulnerabilidades 822
DNS Security 825
Información sobre DNS Security 825
Medidas de protección y firmas de DNS ofrecidas en la nube 826
Análisis de seguridad DNS 827
Habilitación de DNS Security 829
Uso de consultas de DNS para identificar hosts infectados en la red 835
Funcionamiento del sinkholing de DNS 835
Configuración del sinkholing de DNS 836
Configuración del sinkholing de DNS para una lista de dominios personalizados 837
Configuración de la dirección IP del sinkhole en un servidor local de la red 839
Consulta de hosts infectados que intentan conectar a dominios malintencionados 842
Data Filtering 845
Creación de perfiles de filtrado de datos 845
Patrones predefinidos de filtrado de datos 848
WildFire Inline ML 852
Configuración de WildFire Inline ML (Aprendizaje automático en línea de WildFire) 852
Configuración de bloqueo de archivos 856
Prevención de ataques de fuerza bruta 859
Personalización de la acción y las condiciones de activación para una firma de fuerza bruta 860
Habilitación de las firmas de evasión 863
Supervisión de direcciones IP bloqueadas 864
Categorías de firma de amenazas 867
Creación de excepciones de amenazas 875
Firmas personalizadas 878
Supervisión y obtención de informes sobre amenazas 879
Supervisión de actividad y creación de informes personalizados en función de las categorías de amenazas 879
Más información sobre las firmas de amenazas 881
Inteligencia contra amenazas de AutoFocus para el tráfico de red 884
Uso compartido de inteligencia de amenazas con Palo Alto Networks 891
Recursos de prevención de amenazas 892

descifrado 893
Descripción general del descifrado 895
Conceptos de descifrado 897
Políticas de claves y certificados para el descifrado 897
Proxy SSL de reenvío 899
Perfil de descifrado del proxy SSL de reenvío 901
Inspección de entrada SSL 904
Perfil de descifrado de inspección de entrada SSL 905
Perfil de descifrado de la configuración de protocolo SSL 906
Proxy SSH 908
Perfil de descifrado del proxy SSH 909
Perfil para configuración sin cifrado 910
Descifrado SSL para certificados de criptografía de curva elíptica (ECC) 912
Compatibilidad del secreto perfecto y permanente (PFS) para el descifrado SSL 912
Descifrado SSL y nombres alternativos del asunto (SAN) 913
Descifrado TLSv1.3 913
Asistencia de alta disponibilidad para sesiones descifradas 916

Reflejo de descifrado ... 916
Preparación para implementar el descifrado ... 918
Trabajo con las partes interesadas para desarrollar una estrategia de implementación de descifrado ... 918
Desarrollo de un plan de implementación de PKI ... 920
Medición de la implementación de descifrado de cortafuegos ... 921
Planificación de una implementación en etapas con prioridad ... 923
Definición del tráfico para descifrar ... 925
Creación de un perfil de descifrado ... 926
Creación de una regla de política de descifrado ... 928
Configuración del proxy SSL de reenvío ... 931
Configuración de la inspección de entrada SSL ... 936
Configuración del Proxy SSH ... 938
Configuración de una verificación del certificado de servidor para el tráfico sin descifrar ... 939
Exclusiones de descifrado ... 940
Exclusiones predefinidas de descifrado de Palo Alto Networks ... 941
Exclusión de un servidor del descifrado por motivos técnicos ... 942
Caché de exclusión de descifrado local ... 943
Creación de una exclusión al descifrado basada en la política ... 945
Bloqueo de exportación de claves privadas ... 949
Generación de una clave privada y su bloqueo ... 949
Importación de una clave privada y su bloqueo ... 950
Importación de una clave privada para la puerta de enlace de IKE y su bloqueo ... 952
Verificación del bloqueo de la clave privada ... 953
Permisos para que los usuarios excluyan el descifrado SSL ... 955
Deshabilitación temporal del descifrado SSL ... 957
Configuración del reflejo del puerto de descifrado ... 958
Verificación de descifrado ... 961
Solución de problemas y supervisión del descifrado ... 965
Widgets del Centro de control de aplicaciones de descifrado ... 966
Log de descifrado ... 970
Plantillas de informes personalizados de descifrado ... 984
Parámetros no compatibles mediante tipo de proxy y versión de TLS ... 986
Ejemplos de flujo de trabajo de solución de problemas de descifrado ... 987
Agente de descifrado ... 1007
Cómo funciona el agente de descifrado ... 1007
Conceptos del agente de descifrado ... 1008
Pautas de la cadena de seguridad de capa 3 ... 1014
Configuración de un agente de descifrado con una o más cadenas de seguridad de capa 3 ... 1015
Pautas de la cadena de seguridad de puente transparente ... 1017
Configuración del agente de descifrado con una cadena de seguridad de puente transparente ... 1018
Configuración del agente de descifrado con varias cadenas de seguridad de puente transparente ... 1020
Activación de las licencias gratuitas para usar las funciones de descifrado ... 1022

Filtrado de URLs ... 1025
Información sobre URL Filtering ... 1027
Funcionamiento del filtrado de URLs ... 1028
ML en línea de filtrado de URL ... 1030
Casos de uso de filtrado de URL ... 1031
Categorías de URL ... 1034

Categorías de URL centradas en la seguridad....1034
Categorías de URL maliciosas....1035
Categorías de URL verificadas....1037
Acciones que puede realizar según las categorías de URL....1037
Planificar la implementación de filtrado de URL....1040
Prácticas recomendadas de filtrado de URL....1043
Habilitación de PAN-DB....1045
Configuración de filtrado de URL....1047
Configuración de aprendizaje automático en línea de filtrado de URL....1051
Supervisión de la actividad web....1054
Supervisión de la actividad web de los usuarios de red....1054
Visualización del informe de actividad del usuario....1056
Configuración de informes de filtrado de URL personalizados....1058
Registro solo de las páginas que visita un usuario....1062
Creación de una categoría de URL personalizada....1063
Excepciones de la categoría de URL....1065
Pautas básicas para las listas de excepción de categoría de URL....1065
Pautas de comodines para las listas de excepción de categoría de URL....1065
Lista de excepción de categoría de URL: ejemplos de comodines....1066
Uso de una lista dinámica externa en un perfil de filtro de URL....1068
Habilitación del acceso a determinados sitios mediante contraseña....1070
Prevención de phishing de credenciales....1073
Métodos para comprobar los envíos de credenciales corporativas....1073
Configuración de la detección de credenciales con el agente de User-ID de Windows....1075
Configuración de la prevención de suplantación de identidad de credenciales....1077
Forzaje de búsquedas seguras....1082
Configuración de búsqueda segura para proveedores de búsqueda....1082
Bloqueo de los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada....1084
Habilitación transparente de la búsqueda segura para los usuarios....1087
Páginas de respuesta de filtrado de URL....1092
Personalización de las páginas de respuesta de filtrado de URL....1096
Creación de logs del encabezado HTTP....1098
Solicitud para cambiar la categoría de una URL....1099
Realización de una solicitud de cambio en línea....1099
Realización de una solicitud de cambio masivo....1100
Realización de una solicitud de cambio desde el cortafuegos....1101
Solución de problemas del filtrado de URL....1103
Problemas en la activación de PAN-DB....1103
Problemas de conectividad con la nube de PAN-DB....1103
URL clasificadas como no resueltas....1104
Categorización incorrecta....1105
Nube privada de PAN-DB....1107
Dispositivo M-600 para la nube privada de PAN-DB....1107
Configuración de la nube privada de PAN-DB....1109

Calidad de servicio....1117
Descripción general del QoS....1119
Conceptos de QoS....1121
QoS para aplicaciones y usuarios....1121
Política de QoS....1121
Perfil de QoS....1121
Clases de QoS....1122

Establecimiento de colas de prioridad de QoS 1122
Gestión del ancho de banda de QoS 1123
Interfaz de salida de QoS 1123
QoS para texto no cifrado y tráfico de túnel 1124
Configuración de QoS 1125
Configuración de QoS para un sistema virtual 1130
Aplicación forzada de QoS basada en la clasificación DSCP 1135
Casos de uso de QoS 1138
Caso de uso: QoS para un único usuario 1138
Caso de uso: QoS para aplicaciones de voz y vídeo 1140

VPN 1145
Implementaciones de VPN 1147
Descripción general de VPN de sitio a sitio 1148
Conceptos de VPN de sitio a sitio 1149
Puerta de enlace de IKE 1149
Interfaz túnel 1149
Monitorización de túnel 1150
Intercambio de claves por red (IKE) para VPN 1150
IKEv2 1153
Configuración de VPN de sitio a sitio 1156
Configuración de una puerta de enlace de IKE 1156
Definición de perfiles criptográficos 1162
Configuración de un túnel de IPSec 1165
Configuración de la supervisión de túnel 1168
Habilitación/deshabilitación, actualización o reinicio de un gateway IKE o túnel IPSec 1169
Prueba de conectividad VPN 1170
Interpretación de mensajes de error de VPN 1171
Configuraciones rápidas de VPN de sitio a sitio 1173
VPN de sitio a sitio con rutas estáticas 1173
VPN de sitio a sitio con OSPF 1176
VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico 1180

VPN a gran escala (LSVPN) 1187
Descripción general de LSVPN 1189
Creación de interfaces y zonas para la LSVPN 1190
Habilitación de SSL entre componentes de LSVPN de GlobalProtect 1192
Acerca de la implementación de certificados 1192
Implementación de certificados de servidor en los componentes de LSVPN de GlobalProtect 1192
Implementación de certificados cliente en los satélites de GlobalProtect usando SCEP 1195
Configuración del portal para autenticar satélites 1198
Configuración de puertas de enlace de GlobalProtect para LSVPN 1200
Configuración del portal de GlobalProtect para LSVPN 1204
Tareas previas del portal de GlobalProtect para LSVPN 1204
Configuración del portal 1204
Definición de las configuraciones de satélites 1205
Preparación del satélite para unirse a la LSVPN 1209
Verificación de la configuración de LSVPN 1212
Configuraciones rápidas de LSVPN 1213
Configuración básica de LSVPN con rutas estáticas 1213

Configuración avanzada de LSVPN con enrutamiento dinámico....1215
Configuración avanzada de LSVPN con iBGP....1217

Networking....1223
Configuración de interfaces....1225
Interfaces de modo tap....1225
Interfaces de cable virtual....1226
Interfaces de capa 2....1234
Interfaces de capa 3....1240
Configuración de los grupos de interfaces de agregación....1250
Reflector de Bonjour para la segmentación de red....1252
Uso de los perfiles de gestión de interfaz para restringir el acceso....1255
Enrutadores virtuales....1257
Rutas de servicio....1259
Rutas estáticas....1261
Descripción general de la ruta estática....1261
Eliminación de ruta estática basada en el control de ruta....1262
Configuración de una ruta estática....1264
Configuración del control de ruta para una ruta estática....1265
RIP....1268
OSPF....1270
Conceptos de OSPF....1270
Configuración de OSPF....1272
Configuración de OSPFv3....1274
Configuración del reinicio correcto de OSPF....1277
Confirmación del funcionamiento de OSPF....1278
BGP....1279
Descripción general del BGP....1279
MP-BGP....1279
Configuración de BGP....1281
Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6....1286
Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4..1288
Confederaciones BGP....1290
IP de multidifusión....1295
IGMP....1295
PIM....1296
Configuración de IP de multidifusión....1301
Visualización de información de IP de multidifusión....1307
Redistribución de ruta....1310
Túneles GRE....1313
Descripción general de los túneles de GRE....1313
Creación de túneles de GRE....1314
DHCP....1318
Descripción general de DHCP....1318
Cortafuegos como servidor y cliente DHCP....1319
Mensajes DHCP....1319
Direccionamiento DHCP....1320
Opciones de DHCP....1321
Configure una interfaz como servidor DHCP....1324
Configure una interfaz como cliente DHCP....1327
Configuración de la interfaz de gestión como cliente DHCP....1329
Configure una interfaz como agente de relé DHCP....1331
Supervisión y resolución de problemas de DHCP....1332
DNS:....1334

Descripción general del DNS ... 1334
Objeto proxy DNS ... 1335
Perfil de servidor DNS ... 1336
Implementaciones de DNS multiusuario ... 1337
Configuración de un objeto proxy DNS ... 1338
Configuración de un perfil de servidor DNS ... 1339
Caso de uso 1: el cortafuegos exige la resolución de DNS ... 1340
Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual ... 1342
Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor ... 1344
Regla de proxy DNS y coincidencia FQDN ... 1345
Descripción general del DNS dinámico ... 1350
Configuración del DNS dinámico en las interfaces de cortafuegos ... 1352
NAT ... 1354
Reglas de políticas NAT ... 1354
NAT de origen y destino ... 1356
Capacidades de regla NAT ... 1363
Sobresuscripción de NAT de IP dinámica y puerto ... 1363
Estadísticas de memoria NAT de plano de datos ... 1365
Configuración de NAT ... 1365
Ejemplos de configuración de NAT ... 1374
NPTv6 ... 1381
Resumen de NPTv6 ... 1381
Funcionamiento de NPTv6 ... 1382
Proxy NDP ... 1384
Ejemplo de NPTv6 y Proxy NDP ... 1385
Creación de una política NPTv6 ... 1386
NAT64 ... 1389
Descripción general de NAT64 ... 1389
Dirección IPv6 integrada en la dirección IPv4 ... 1390
Servidor DNS64 ... 1390
Detección de MTU de ruta ... 1390
Comunicación de Pv6 iniciada ... 1391
Configuración de NAT64 para la comunicación iniciada por IPv6 ... 1392
Configuración de NAT64 para la comunicación iniciada por IPv4 ... 1394
Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto ... 1397
ECMP ... 1400
Algoritmos de equilibrio de carga de ECMP ... 1400
Compatibilidad con modelo de ECMP, interfaz y enrutamiento de IP ... 1401
Configuración de ECMP en un enrutador virtual ... 1402
Habilitación de ECMP para varios sistemas BGP autónomos ... 1404
Verificación de ECMP ... 1405
LLDP ... 1406
Descripción general de LLDP ... 1406
TLV compatibles con LLDP ... 1407
Mensajes de Syslog LLDP y capturas de SNMP ... 1408
Configuración de LLDP ... 1409
Visualización de estados y configuración de LLDP ... 1410
Borrado de estadísticas de LLDP ... 1411
BFD ... 1412
Descripción general de BFD ... 1412
Configuración de BFD ... 1414
Referencia: Detalles de BFD ... 1419
Configuración de sesión y tiempos de espera de sesión ... 1424

Sesiones de capa de transporte....1424
TCP....1424
UDP....1429
ICMP....1429
Control de tipos y códigos específicos de ICMP o ICMPv6....1431
Configuración de los tiempos de espera de sesión....1432
Configuración de los ajustes de sesión....1434
Política de distribución de sesiones....1437
Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP....1441
Inspección del contenido del túnel....1442
Descripción general de la inspección del contenido del túnel....1442
Configuración de la inspección del contenido del túnel....1446
Visualización de actividad de túneles inspeccionados....1452
Visualización de información del túnel en logs....1453
Creación de un informe personalizado basado en el tráfico de túnel etiquetado....1454
Deshabilitación de aceleración de túneles....1454

Política....1457
Tipos de políticas....1459
Política de seguridad....1460
Componentes de una regla de política de seguridad....1460
Acciones de la política de seguridad....1463
Creación de una regla de política de seguridad....1464
Objetos de políticas....1468
Perfiles de seguridad....1470
Creación de un grupo de perfiles de seguridad....1477
Configuración o cancelación de un grupo de perfiles de seguridad predeterminado....1478
Seguimiento de las reglas de las bases de reglas....1480
Números de regla....1480
UUID de las reglas....1481
Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas....1486
Duplicación o traslado de una regla de políticas u objeto a un sistema virtual diferente....1489
Uso de objetos de dirección para representar direcciones IP....1491
Objetos de dirección....1491
Creación de objetos de dirección....1492
Uso de etiquetas para agrupar objetos y distinguirlos visualmente....1494
Creación y aplicación de etiquetas....1494
Modificación de etiquetas....1495
Consulta de las reglas por grupos de etiquetas....1495
Uso de una lista dinámica externa en políticas....1498
Lista dinámica externa....1498
Directrices de formato para listas dinámicas externas....1501
Listas dinámicas externas integradas....1503
Configuración del cortafuegos para acceder a una lista dinámica externa....1504
Recuperación de una lista dinámica externa del servidor web....1507
Visualización de entradas de lista dinámica externa....1507
Exclusión de entradas de una lista dinámica externa....1508
Aplicación de la política en una lista dinámica externa....1508
Búsqueda de listas dinámicas externas con autenticación fallida....1511
Deshabilitación de autenticación para una lista dinámica externa....1512
Registro de direcciones IP y etiquetas dinámicamente....1514

Uso de grupos de usuarios dinámicos en políticas....1516
Uso de etiquetado automático para automatizar acciones de seguridad....1519
Supervisión de cambios en el entorno virtual....1523
Habilitación de supervisión de VM para el registro de cambios en la red virtual....1523
Atributos supervisados en máquinas virtuales en plataformas en la nube....1525
Uso de grupos de direcciones dinámicas en políticas....1529
Comandos de la CLI para etiquetas y direcciones IP....1533
Cumplimiento de la política en endpoints y usuarios detrás de un dispositivo de subida...1536
Uso de valores XFF para políticas basadas en usuarios de origen....1536
Uso de valores de la dirección IP de XFF en la política de seguridad y logs....1537
Uso de la dirección IP en el encabezado de XFF para eventos de solución de problemas....1540
Reenvío basado en políticas....1542
PBF....1542
Creación de una regla de reenvío basada en políticas....1544
Caso de uso: PBF para acceso saliente con ISP duales....1546
Comprobación de las reglas de las políticas....1554

Virtual Systems....1555
Descripción general de los sistemas virtuales....1557
Componentes y segmentación de los sistemas virtuales....1557
Ventajas de los sistemas virtuales....1558
Casos de uso de sistemas virtuales....1558
Compatibilidad con plataformas y licencias de sistemas virtuales....1559
Funciones de administrador para sistemas virtuales....1559
Objetos compartidos para sistemas virtuales....1560
Comunicación entre sistemas virtuales....1561
Tráfico entre VSYS que debe abandonar el cortafuegos....1561
Tráfico entre VSYS que permanece en el cortafuegos....1561
La comunicación entre VSYS usa dos sesiones....1563
Puerta de enlace compartida....1565
Zonas externas y puerta de enlace compartida....1565
Consideraciones de red para una puerta de enlace compartida....1566
Configuración de sistemas virtuales....1567
Configuración de la comunicación entre sistemas virtuales dentro del cortafuegos....1572
Configuración de un gateway compartido....1573
Personalización de rutas de servicio para un sistema virtual....1574
Personalización de rutas de servicio a servicios para un sistema virtual....1574
Configure un cortafuegos PA-7000 Series para logging por sistema virtual....1576
Configuración de acceso administrativo por sistema virtual o cortafuegos....1578
Funcionalidad de sistema virtual con otras funciones....1580

Protección de zona y protección contra DoS....1581
Segmentación de la red con zonas....1583
¿Cómo las zonas protegen la red?....1584
Defensa de zona....1585
Herramientas de defensa de zona....1585
¿Cómo funcionan las herramientas de defensa de zona?....1587
Selección de ubicación del cortafuegos para la protección DoS....1588
Medidas de CPS de referencia para establecer umbrales de inundación....1588
Perfiles de protección de zonas....1590
Protección de búfer de paquetes....1594
Perfiles de protección y reglas de la política del DoS....1597

Configuración de la protección de la zona para aumentar la seguridad de la red....1603
Configuración de la protección de reconocimiento....1603
Configuración de la protección de ataques basada en paquetes....1604
Configuración de la protección de protocolos....1605
Configuración de la protección de búfer de paquetes....1609
Configuración de la protección de búfer de paquetes basada en la latencia....1610
Configuración de la protección de SGT Ethernet....1611
Protección DoS contra inundaciones de nuevas sesiones....1613
Ataque DoS multisesión....1613
Ataque DoS de una sesión....1617
Configuración de protección DoS contra inundaciones de nuevas sesiones....1617
Finalización de un ataque DoS de una sesión....1620
Identificación de sesiones que utilizan un porcentaje excesivo del búfer de paquete....1621
Eliminación de una sesión sin confirmación....1623

Certificaciones....1625
Habilitación de FIPS y compatibilidad con criterios comunes....1627
Acceda a la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT)....1627
Cambio del modo operativo a modo FIPS-CC....1629
Funciones de seguridad de FIPS-CC....1630
Limpieza de memoria de intercambio en un cortafuegos o aplicaciones que se ejecutan en modo FIPS-CC....1631

Primeros pasos

Los siguientes temas proporcionan pasos detallados para ayudarle a implementar un nuevo cortafuegos de nueva generación de Palo Alto Networks. En ellos se detallan los procedimientos para integrar en la red un cortafuegos nuevo y para configurar una política de seguridad básica. Si desea obtener instrucciones para implementar a continuación las funciones de la plataforma de seguridad según sus requisitos de protección de la red, consulte Prácticas recomendadas para completar la implementación del cortafuegos.

- Integración del firewall en la red de gestión
- Registro del cortafuegos
- Segmentar su red con interfaces y zonas
- Configuración de una política de seguridad básica
- Evaluación del tráfico de red
- Habilitación del reenvío gratuito de WildFire
- Prácticas recomendadas para completar la implementación del cortafuegos
- Prácticas recomendadas para proteger el acceso administrativo

© 2020 Palo Alto Networks, Inc.

Integración del firewall en la red de gestión

Todos los cortafuegos de Palo Alto Networks incluyen un puerto de gestión (MGT) fuera de banda que puede usar para llevar a cabo las funciones de administración del cortafuegos. Al usar el puerto MGT, está separando las funciones de gestión del cortafuegos de las funciones de procesamiento de datos, de modo que protege el acceso al cortafuegos y mejora el rendimiento. Al usar la interfaz web, debe realizar todas las tareas de configuración inicial desde el puerto MGT, incluso aunque pretenda usar un puerto dentro de banda para gestionar su cortafuegos más adelante.

Algunas tareas de gestión, como la recuperación de licencias y la actualización de amenazas y firmas de aplicaciones en el cortafuegos requieren acceso a Internet. Si no desea habilitar el acceso externo a su puerto MGT, deberá establecer un puerto de datos en banda para permitir el acceso a los servicios externos requeridos (usando rutas de servicio) o planificar la carga manual de actualizaciones de forma periódica.



No permite el acceso a la interfaz de gestión desde internet o desde otras zonas no fiables dentro de sus límites de seguridad empresariales. Esto se aplica si utiliza el puerto de gestión dedicado (dedicated management port, MGT) o si configura un puerto de datos como su interfaz de gestión. Cuando integra el cortafuegos en su red de gestión, respete las Prácticas recomendadas para proteger el acceso administrativo *para garantizar la seguridad del acceso administrativo a sus cortafuegos y otros dispositivos de seguridad, de modo que evite ataques eficaces.*

Los siguientes temas describen cómo realizar los pasos de la configuración inicial necesarios para integrar un nuevo cortafuegos en la red de gestión e implementarlo con una configuración de seguridad básica.

- Determinación de la estrategia de gestión
- Realización de la configuración inicial
- Establecimiento de acceso a la red para servicios externos



Los siguientes temas describen cómo integrar un único cortafuegos de nueva generación de Palo Alto Networks en su red. Sin embargo, para obtener redundancia, debería implementar dos cortafuegos en una configuración de alta disponibilidad*.*

Determinación de la estrategia de gestión

El cortafuegos Palo Alto Networks se puede configurar y administrar localmente o de forma central usando Panorama, el sistema de administración de seguridad centralizado de Palo Alto Networks. Si tiene seis o más cortafuegos implementados en su red, use Panorama para obtener las siguientes ventajas:

- Reducir la complejidad y la carga administrativa en la gestión de configuración, políticas, software y actualizaciones de contenido dinámico. Usando las plantillas y grupos de dispositivos de Panorama puede gestionar eficazmente la configuración específica de los cortafuegos de manera local en un cortafuegos y aplicar políticas compartidas en todos los cortafuegos o grupos de cortafuegos.
- Agregue datos de todos los cortafuegos gestionados y obtenga visibilidad en todo el tráfico de su red. El Centro de control de aplicaciones (ACC) de Panorama ofrece un panel de pantalla única para la gestión unificada de informes de todos los cortafuegos, lo que le permite realizar análisis, investigaciones e informes de forma central sobre el tráfico de red, los incidentes de seguridad y las modificaciones administrativas.

Los procedimientos siguientes describen cómo gestionar el cortafuegos usando la interfaz web local. Si desea utilizar Panorama para la gestión centralizada, proceda primero con la Realización de la configuración inicial y compruebe que el cortafuegos puede establecer una conexión con Panorama. A partir de aquí, puede usar Panorama para configurar su cortafuegos de forma centralizada.

© 2020 Palo Alto Networks, Inc.

Realización de la configuración inicial

Por defecto, la dirección IP del cortafuegos es 192.168.1.1 y el nombre de usuario/contraseña es admin/admin. Por motivos de seguridad, debe cambiar estos ajustes antes de continuar con otras tareas de configuración del cortafuegos. Debe realizar estas tareas de configuración inicial desde la interfaz MGT, incluso aunque no pretenda usar esta interfaz para la gestión de su cortafuegos, o usar una conexión en serie directa al puerto de la consola del cortafuegos.

STEP 1 | Instale el cortafuegos y conéctelo a la fuente de alimentación.

Si el modelo del cortafuegos tiene dos fuentes de alimentación, conecte la segunda para la redundancia. Consulte la guía de referencia de hardware de su modelo para obtener más información.

STEP 2 | Obtenga la información necesaria de su administrador de red.

- Dirección IP para el puerto MGT
- Máscara de red
- Puerta de enlace predeterminada
- Dirección de servidor DNS

STEP 3 | conectar su ordenador al cortafuegos.

Puede conectarse al cortafuegos de uno de estos modos:

- Conecte un cable en serie desde su ordenador hasta el puerto de la consola y conéctese al cortafuegos usando el software de emulación de terminal (9600-8-N-1). Espere unos minutos hasta que se complete la secuencia de arranque; cuando el cortafuegos esté listo, el mensaje cambiará al nombre del cortafuegos, por ejemplo `PA-220 login (inicio de sesión de PA-220).`
- Conecte un cable Ethernet RJ-45 de su ordenador al puerto MGT del cortafuegos. Desde un navegador, visite **`https://192.168.1.1`**.

Es posible que deba cambiar la dirección IP de su ordenador por una dirección de la red 192.168.1.0/24, como 192.168.1.2, para acceder a esta URL.

STEP 4 | Cuando se le indique, inicie sesión en el cortafuegos.

Debe iniciar sesión usando el nombre de usuario y contraseña predeterminados (admin/admin). El cortafuegos comenzará a inicializarse.

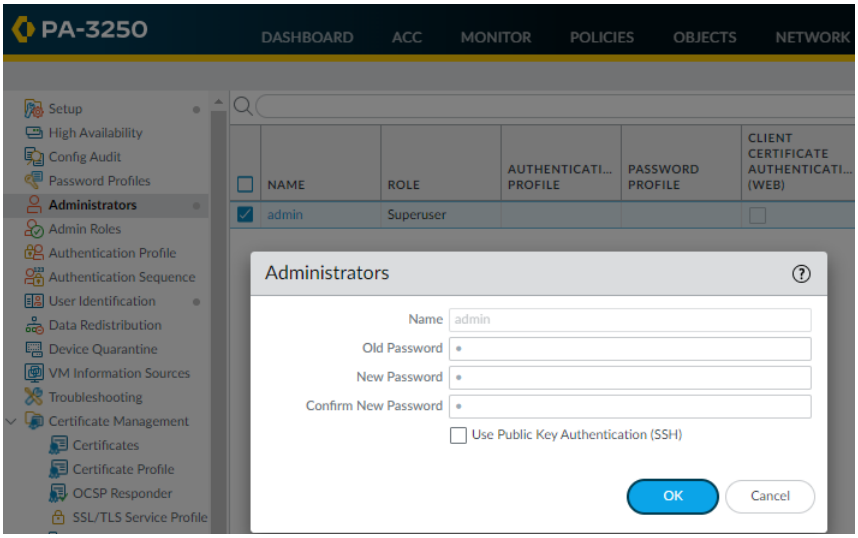
STEP 5 | Establezca una contraseña segura para la cuenta de administrador.

A partir de PAN-OS 9.0.4, la contraseña de administrador predefinida y predeterminada (admin/admin) debe cambiarse la primera vez que inicie sesión en el dispositivo. La nueva contraseña debe tener un mínimo de ocho caracteres e incluir un mínimo de un carácter en minúsculas y otro en mayúsculas, así como un número y un carácter especial.

Asegúrese de seguir las prácticas recomendadas sobre seguridad de la contraseña para garantizar que la contraseña sea segura y revise la configuración de complejidad de la contraseña.

1. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)**.
2. Seleccione la función **admin**.
3. Introduzca la contraseña predeterminada actual y la nueva contraseña.

© 2020 Palo Alto Networks, Inc.



4. Haga clic en Aceptar para guardar la configuración.

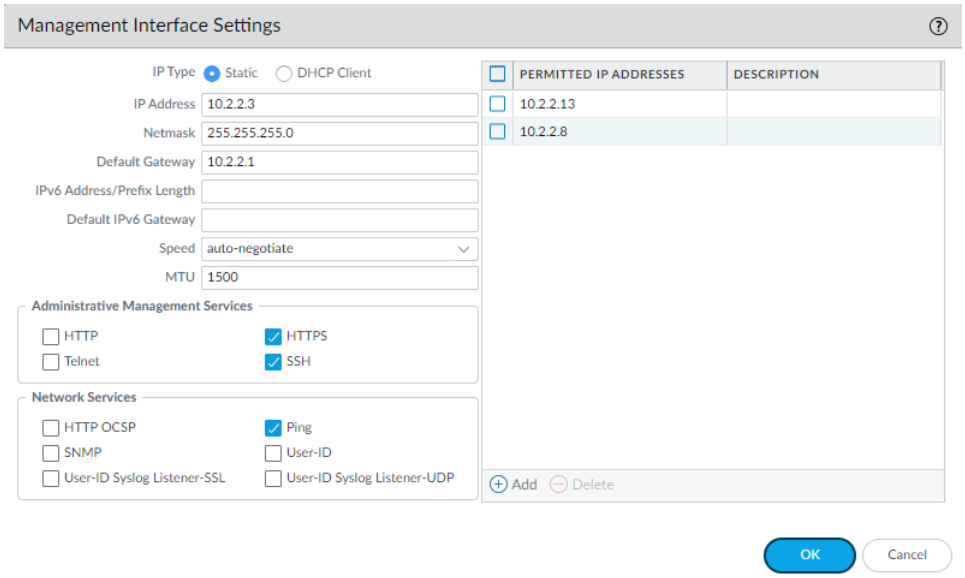
STEP 6 | Configure la interfaz MGT.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Interfaces** y edite la interfaz **Management (Gestión)**.
2. Configure los ajustes de dirección para la interfaz MGT usando uno de los siguientes métodos:
   - Para configurar los ajustes de la dirección IP para la interfaz MGT, configure el **IP Type (Tipo de IP)** en **Static (Estática)** e introduzca la **IP Address (Dirección IP)**, **Netmask (Máscara de red)** y **Default Gateway (Puerta de enlace por defecto)**.
   - Para configurar de forma dinámica los ajustes de la dirección de interfaz MGT, configure el **IP Type (Tipo de IP)** en **DHCP Client (Cliente DHCP)**. Para usar este método, debe configurar la interfaz de gestión como un cliente DHCP.

   Para evitar el acceso no autorizado a la interfaz de gestión, se recomienda que añada las direcciones IP permitidas desde las que un administrador puede acceder a la interfaz MGT.
3. Fije la **Speed (Velocidad)** en **auto-negotiate (negociación automática)**.
4. Seleccione los servicios de gestión que permitirá en la interfaz.

   Asegúrese de que ni Telnet ni HTTP estén seleccionados, ya que estos servicios usan texto sin formato y no son tan seguros como otros servicios, y podrían comprometer las credenciales de administrador.

© 2020 Palo Alto Networks, Inc.



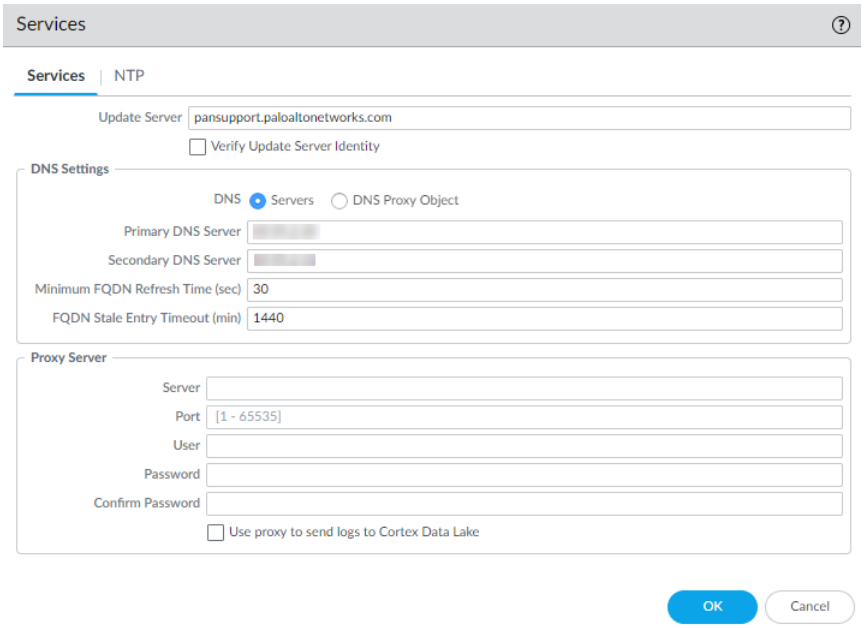
5. Haga clic en **OK (Aceptar)**.

STEP 7 | Configure los ajustes de DNS, servidor de actualización y servidor proxy.

Debe configurar manualmente al menos un servidor DNS en el cortafuegos o no podrá resolver los nombres de host; no usará configuraciones del servidor DNS de otra fuente, como un ISP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
   - En plataformas de múltiples sistemas virtuales, seleccione **Global** y edite la sección Services.
   - En plataformas de un único sistema virtual, edite la sección Servicios.
2. En la pestaña **Services (Servicios)**, para **DNS**, seleccione una de las siguientes opciones:
   - **Servers (Servidores)**: ingrese la dirección del **Primary DNS Server (Servidor DNS principal)** y la del **Secondary DNS Server (Servidor DNS secundario)**.
   - **DNS Proxy Object (Objeto proxy DNS)**: en el menú desplegable, seleccione el **DNS Proxy** que desea usar para configurar servicios DNS globales, o haga clic en **DNS Proxy** para configurar un nuevo objeto proxy DNS.

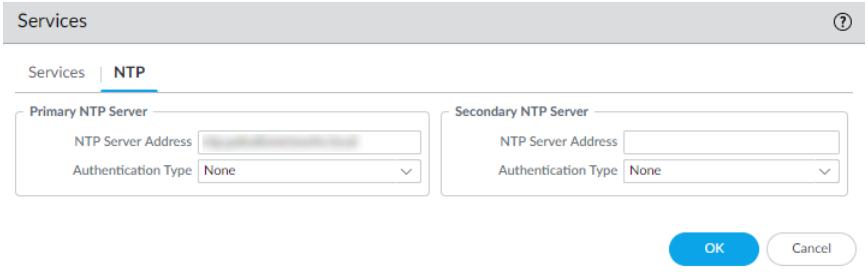
© 2020 Palo Alto Networks, Inc.



3. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure los ajustes de fecha y hora (NTP).

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
   - En plataformas de múltiples sistemas virtuales, seleccione **Global** y edite la sección Services.
   - En plataformas de un único sistema virtual, edite la sección Servicios.
2. En la pestaña **NTP**, para usar el clúster virtual de los servidores de tiempo en Internet, introduzca el nombre de host `pool.ntp.org` como el **Primary NTP Server** o introduzca la dirección IP de su servidor NTP principal.



3. (Opcional) Introduzca una dirección **Secondary NTP Server**.
4. (Opcional) Para autenticar actualizaciones de tiempo de los servidores NTP, en **Authentication Type** (Tipo de autenticación), seleccione uno de los siguientes en cada servidor:
   - **None (Ninguna)**: (opción por defecto) deshabilita la autenticación NTP.
   - **Symmetric Key (Clave simétrica)**: el cortafuegos usa intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de tiempo.
     - **Key ID (ID de clave)**: introduzca el ID de clave (1-65534).
     - **Algorithm**: seleccione el algoritmo que se debe utilizar en la autenticación del NTP (**MD5** o **SHA1**).
   - **Autokey (Clave automática)**: el cortafuegos usa la clave automática (criptografía de clave pública) para autenticar las actualizaciones de tiempo.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 9 | (Opcional) Configure los ajustes generales del cortafuegos según fuera necesario.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite {0>General Settings (Configuración general)<0}.
2. Introduzca un **Hostname** para el cortafuegos y el nombre de **Domain** de su red. El nombre de dominio tan solo es una etiqueta, no se usará para unirse al dominio.
3. Introduzca el texto del **Login Banner** que informa a los usuarios que están intentando iniciar sesión de que deben tener autorización para acceder a las funciones de gestión del cortafuegos.

   Se recomienda no utilizar mensaje de bienvenida. Además, debe pedir a su departamento de asuntos legales que revise el mensaje del banner para garantizar que advierta adecuadamente que se prohíbe el acceso no autorizado.
4. Introduzca la **Latitude (Latitud)** y **Longitude (Longitud)** para permitir la colocación precisa del cortafuegos en el mapamundi.
5. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.



Al guardar los cambios de configuración, perderá la conectividad con la interfaz web, ya que la dirección IP habrá cambiado.

Haga clic en **Commit (Confirmar)** en la parte superior derecha de la interfaz web. El cortafuegos puede tardar hasta 90 segundos en guardar sus cambios.

STEP 11 | Conecte el cortafuegos a su red.

1. Desconecte el cortafuegos de su ordenador.
2. Conecte el puerto de gestión a un puerto de conmutador en su red de gestión usando un cable Ethernet RJ-45. Asegúrese de que el puerto de conmutación que conecta al cortafuegos mediante un cable esté configurado para negociación automática.

STEP 12 | Abra una sesión de gestión SSH en el cortafuegos.

Mediante un software de emulación de terminal, tal como PuTTY, inicie una sesión SSH en el cortafuegos usando la nueva dirección IP que le ha asignado.

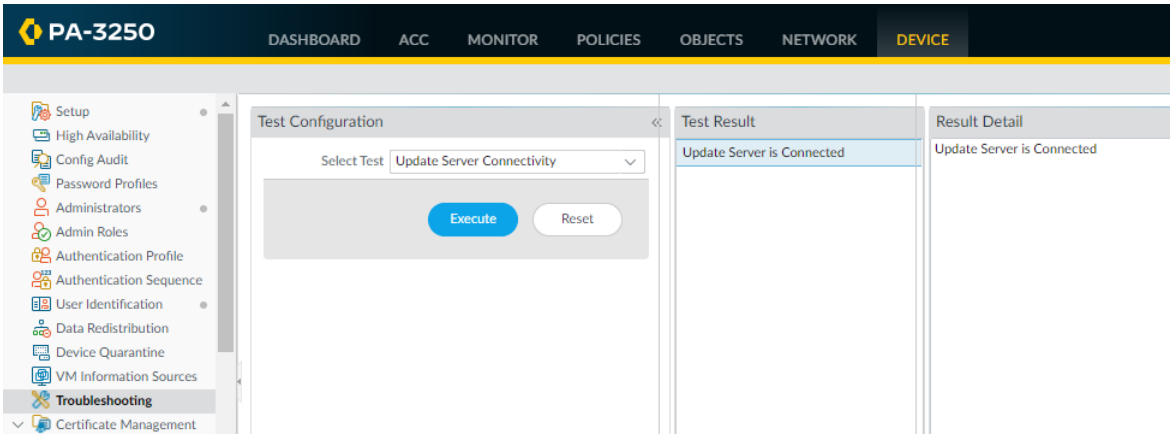
STEP 13 | Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks:

Puede hacerlo de uno de estos modos:

- Si no desea permitir que una red externa acceda a la interfaz MGT, tendrá que configurar un puerto de datos para recuperar las actualizaciones de servicio requeridas. Proceda con la Configuración de acceso a la red para servicios externos.
- Si planea permitir el acceso de la red externa a la interfaz MGT, compruebe que haya conectividad y continúe por Registro del cortafuegos y por Activación de licencias de suscripción.

1. Para verificar la conectividad de red al servidor de actualizaciones de Palo Alto Networks, realice la prueba que se muestra en el siguiente ejemplo.
   1. Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y, luego, seleccione **Update Server Connectivity (Conectividad al servidor de actualizaciones)** en el menú desplegable Select Test (Seleccionar prueba).
   2. Haga clic en **Execute (Ejecutar)** para comprobar la conectividad al servidor de actualizaciones.

© 2020 Palo Alto Networks, Inc.



2. Use el siguiente comando de la CLI para recuperar información sobre el derecho a la asistencia técnica para el cortafuegos desde el servidor de actualizaciones de Palo Alto Networks:

```
request support
check
```

Si tiene conectividad, el servidor de actualizaciones responde con el estado de asistencia para el cortafuegos. Si su cortafuegos todavía no está registrado, el servidor de actualizaciones devuelve el siguiente mensaje:

```
Contact Us

https://www.paloaltonetworks.com/company/contact-us.html

Support Home

https://www.paloaltonetworks.com/support/tabs/overview.html

Device not found on this update server
```

Establecimiento de acceso a la red para servicios externos

Por defecto, el cortafuegos usa la interfaz MGT para acceder a servicios remotos, como servidores DNS, actualizaciones de contenido y recuperación de licencias. Si no desea habilitar el acceso de red externa a su red de gestión, debe configurar un puerto de datos en banda para brindar acceso a los servicios externos necesarios y configurar rutas de servicio para indicar al cortafuegos qué puerto debe usar para acceder a los servicios externos.

No permite el acceso administrativo desde internet o desde otras zonas no fiables dentro de sus límites de seguridad empresariales. Respete las Prácticas recomendadas para proteger el acceso administrativo para garantizar que protege adecuadamente el cortafuegos.

Para esta tarea debe estar familiarizado con zonas, políticas e interfaces de cortafuegos. Para obtener más información sobre estos temas, consulte Configuración de interfaces y zonas y Configuración de una política de seguridad básica.

STEP 1 | Decida la interfaz que desea usar para acceder a servicios externos y conéctelo al puerto del conmutador o al puerto del enrutador.

© 2020 Palo Alto Networks, Inc.

La interfaz que use deberá tener una dirección IP estática.

STEP 2 | Inicie sesión en la interfaz web.

Si usa una conexión segura (https) desde su navegador web, inicie sesión usando la nueva dirección IP y contraseña que asignó durante la configuración inicial (https://<dirección IP>). Verá una advertencia de certificación; es normal. Vaya a la página web.

STEP 3 | (Opcional) El firewall viene preconfigurado con una interfaz de cable virtual predeterminada entre los puertos Ethernet 1/1 y Ethernet 1/2 (y sus correspondientes zonas y políticas de seguridad predeterminadas). Si no pretende usar esta configuración de Virtual Wire, debe eliminar manualmente la configuración para evitar que interfiera con otras configuraciones de interfaz que defina.

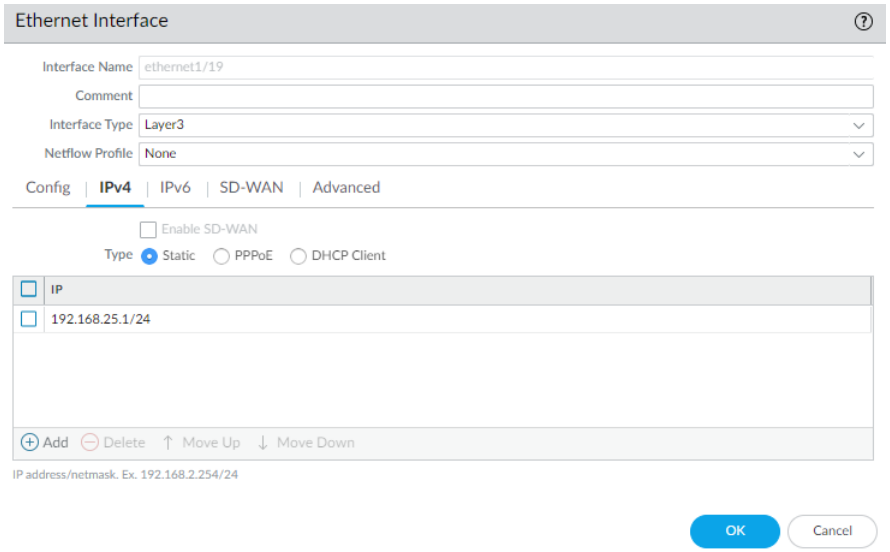
Debe eliminar la configuración en el siguiente orden:

1. Para eliminar la política de seguridad predeterminada, seleccione **Policies (Políticas)** > **Security (Seguridad)**, seleccione la regla y haga clic en **Delete (Eliminar)**.
2. Para eliminar el cable virtual predeterminado, seleccione **Network (Red)** > **Virtual Wires (Cables virtuales)**, seleccione el cable virtual y haga clic en **Delete (Eliminar)**.
3. Para eliminar las zonas fiables y no fiables predeterminadas, seleccione **Network (Red)** > **Zones (Zonas)**, seleccione cada zona y haga clic en **Delete (Eliminar)**.
4. Para eliminar las configuraciones de interfaz, seleccione **Network (Red)** > **Interfaces** y, a continuación, seleccione cada interfaz (ethernet1/1 y ethernet1/2), y haga clic en **Delete (Eliminar)**.
5. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 4 | Configure la interfaz que planea utilizar para el acceso externo a los servicios de gestión.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz que corresponde a la interfaz en la que conectó el cable en el paso 1.
2. Seleccione **Interface Type (Tipo de interfaz)**. Aunque su decisión aquí depende de la topología de su red, este ejemplo muestra los pasos para **Layer3**.
3. En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**.
4. En el cuadro de diálogo Zone (Zona), defina un nombre en **Name** para una nueva zona, por ejemplo Gestión y, a continuación, haga clic en **OK (Aceptar)**.
5. Seleccione la pestaña **IPv4**, seleccione el botón de opción **Estático**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.1.254/24. Debe usar una dirección IP estática en esta interfaz.

© 2020 Palo Alto Networks, Inc.

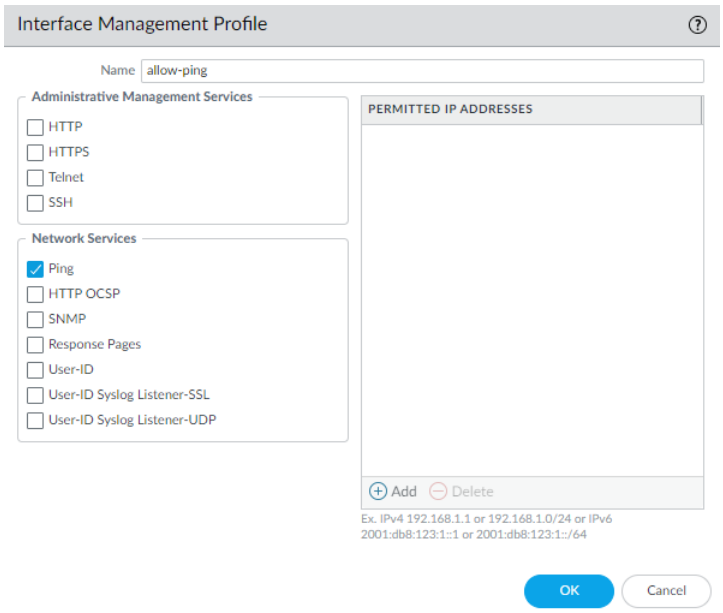


6. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**, amplíe el menú desplegable **Management Profile (Perfil de gestión)** y seleccione **New Management Profile (Nuevo perfil de gestión)**.
7. Introduzca un **Nombre** para el perfil, como permitir_ping, y seleccione a continuación los servicios que desea permitir en la interfaz. Para permitir el acceso a los servicios externos, probablemente solo tenga que habilitar **Ping** y después hacer clic en **OK (Aceptar)**.



Estos servicios ofrecen acceso de gestión al cortafuegos, así que seleccione solo los servicios que correspondan a actividades de gestión que desee permitir en esta interfaz. Por ejemplo, no habilite HTTP ni Telnet porque esos protocolos realizan transmisiones de texto sin cifrar y, por lo tanto, no son seguros. Si planea utilizar la interfaz MGT para las tareas de configuración del cortafuegos por medio de la interfaz web o la CLI, tampoco debe habilitar HTTP, HTTPS, SSH ni Telnet a fin de evitar el acceso no autorizado a través de esta interfaz (si tiene que permitir HTTPS o SSH en este caso, limite el acceso a un conjunto concreto de direcciones IP permitidas). Para obtener detalles, consulte Uso de los perfiles de gestión de interfaz para restringir el acceso.

© 2020 Palo Alto Networks, Inc.



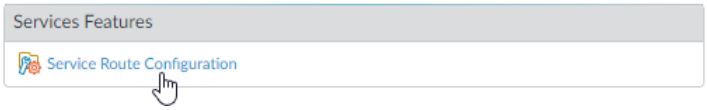
8. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 5 | Configure las Service Routes (Rutas de servicio).

Por defecto, el cortafuegos utiliza la interfaz MGT para acceder a los servicios externos que necesita. Para cambiar la interfaz que usa el cortafuegos para enviar solicitudes a servicios externos, debe editar las rutas de servicio.

Este ejemplo muestra cómo configurar rutas de servicio globales. Para obtener información sobre la configuración de acceso de red a servicios externos basada en sistemas virtuales en vez de global, consulte Personalización de las rutas de servicio en servicios para sistemas virtuales.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global** y haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.



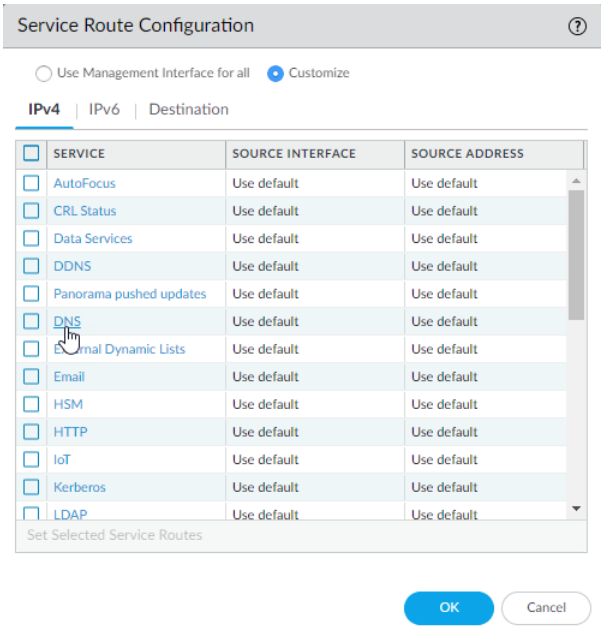
Para activar sus licencias y obtener el contenido y las actualizaciones de software más recientes, debe cambiar la ruta de servicios de DNS, Palo Alto Networks Services (Servicios de Palo Alto Networks), URL Updates (Actualizaciones de URL) y AutoFocus.

2. Haga clic en el botón de opción **Customize (Personalizar)** y seleccione una de las siguientes opciones:
   - Para un servicio predefinido, seleccione **IPv4** o **IPv6** y haga clic en el enlace del servicio. Para limitar la lista desplegable de direcciones de origen, seleccione **Source Interface (Interfaz de origen)** y seleccione la interfaz que configuró recientemente. Después, seleccione una dirección de origen (de la interfaz) como la ruta de servicio.

     Si se configura más de una dirección IP para la interfaz seleccionada, el menú desplegable **Source Address (Dirección de origen)** le permite seleccionar una dirección IP.
   - Para crear una ruta de servicio para un destino personalizado, seleccione **Destination (Destino)** y haga clic en **Add (Añadir)**. Introduzca una dirección IP de **Destination (Destino)**. Un paquete entrante con una dirección de destino que coincide con esta dirección utilizará la dirección de

© 2020 Palo Alto Networks, Inc.

origen que especificó para esta ruta de servicio como su origen. Para limitar la lista desplegable de Source Address (Dirección de origen), seleccione una **Source Interface (Interfaz de origen)**. Si se configura más de una dirección IP para la interfaz seleccionada, el menú desplegable **Source Address (Dirección de origen)** le permite seleccionar una dirección IP.



3. Haga clic en **OK (Aceptar)** para guardar los ajustes.
4. Repita los pasos del 5.2 al 5.3 indicados anteriormente con cada ruta de servicio que desee modificar.
5. **Commit (Confirmar)** los cambios.

STEP 6 | Configure una interfaz externa y una zona asociada y, a continuación, cree una regla de política de seguridad para permitir que el cortafuegos envíe solicitudes de servicio desde la zona interna hacia la externa.

1. Seleccione **Network (Red)** > **Interfaces** y, a continuación, seleccione su interfaz de orientación externa. Seleccione **Layer3** en **Interface Type (Tipo de interfaz)**, luego seleccione **Add (Añadir)** para añadir la dirección **IP** (en la pestaña **IPv4** o **IPv6**) y cree la **Security Zone (Zona de seguridad)** asociada (en la pestaña **Config**), tal como Internet. Esta interfaz debe tener una dirección IP estática; no es necesario que configure servicios de gestión en esta interfaz.
2. Para configurar una regla de seguridad que permita el tráfico desde su red interna hasta el servidor de actualización de Palo Alto Networks, seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.

Se recomienda que al crear reglas de política de seguridad use reglas basadas en aplicaciones en lugar de reglas basadas en políticas para garantizar que esté identificando de manera precisa la aplicación subyacente, independientemente del puerto, del protocolo, de las tácticas de evasión o del cifrado en uso. Siempre deje la opción Service configurada en application-default. En este caso, cree una regla de política de seguridad que permita el acceso al servidor de actualización (y a otros servicios de Palo Alto Networks).

© 2020 Palo Alto Networks, Inc.

	NAME	Source ZONE	Destination ZONE	APPLICATION	SERVICE	ACTION
1	Palo Alto Networks Services	Management	Internet	paloalto-dns-security paloalto-logging-service paloalto-updates paloalto-wildfire-cloud	application-...	Allow

STEP 7 | Cree una regla de política NAT.

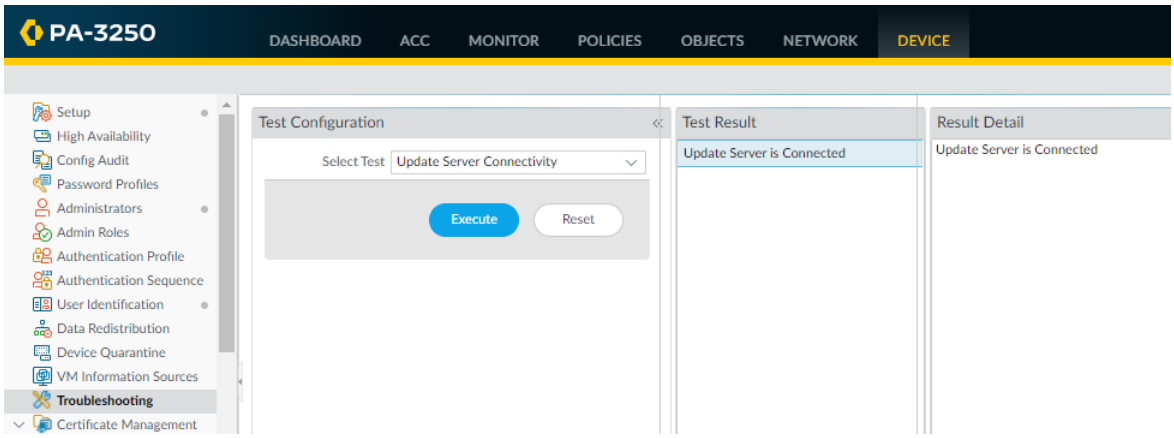
1. Si usa una dirección IP privada en la interfaz de orientación interna, deberá crear una regla NAT de origen para traducir la dirección a una dirección enrutable públicamente. Seleccione **Policies (Políticas)** > **NAT** y, a continuación, haga clic en **Add (Añadir)**. Como mínimo deberá definir un nombre para la regla (pestaña **General**), especificar una zona de origen y destino, Management a Internet en este caso (pestaña **Original Packet**), y definir la configuración de traducción de dirección de origen (pestaña **Translated Packet**) y luego hacer clic en **OK**.
2. **Commit (Confirmar)** los cambios.

	NAME	Original Packet SOURCE ZONE	DESTINATION ZONE	SERVICE	Translated Packet SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source NAT	Management	Internet	any	dynamic-ip-and-port	none

STEP 8 | Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y compruebe si hay conectividad entre el puerto de datos y los servicios externos (incluida la puerta de enlace predeterminada) con la prueba **Ping**, por un lado, y el servidor de actualizaciones de Palo Alto Networks con la prueba **Update Server Connectivity (Conectividad al servidor de actualizaciones)**, por otro. En este ejemplo, se comprueba la conectividad del cortafuegos al servidor de actualizaciones de Palo Alto Networks.

Después de verificar que existe la conectividad de red necesaria, continúe por Registro del cortafuegos y por Activación de licencias de suscripción.

1. Seleccione **Update Server Connectivity (Conectividad al servidor de actualizaciones)** en el menú desplegable Select Test (Seleccionar prueba).
2. Haga clic en **Execute (Ejecutar)** para comprobar la conectividad al servidor de actualizaciones de Palo Alto Networks.



3. Acceda a la CLI del cortafuegos y use el siguiente comando para recuperar información sobre su derecho a asistencia técnica desde el servidor de actualizaciones de Palo Alto Networks:

```
request support
```


© 2020 Palo Alto Networks, Inc.

check

Si tiene conectividad, el servidor de actualizaciones responde con el estado de asistencia para el cortafuegos. Debido a que su cortafuegos no está registrado, el servidor de actualizaciones devuelve el siguiente mensaje:

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```


© 2020 Palo Alto Networks, Inc.

Registro del cortafuegos

Para poder activar el soporte y otras licencias y suscripciones, primero debe registrar el cortafuegos. Sin embargo, antes de poder registrar un cortafuegos, primero debe tener una cuenta de soporte activa. Realice una de las siguientes tareas dependiendo de si tiene una cuenta de soporte activa:

- Si no tiene una cuenta de soporte activa, Cree una nueva cuenta de soporte y registre un cortafuegos.
- Si ya tiene una cuenta de soporte activa, entonces está listo para Registre un cortafuegos.
- (Opcional) Configuración inicial en un cortafuegos registrado.

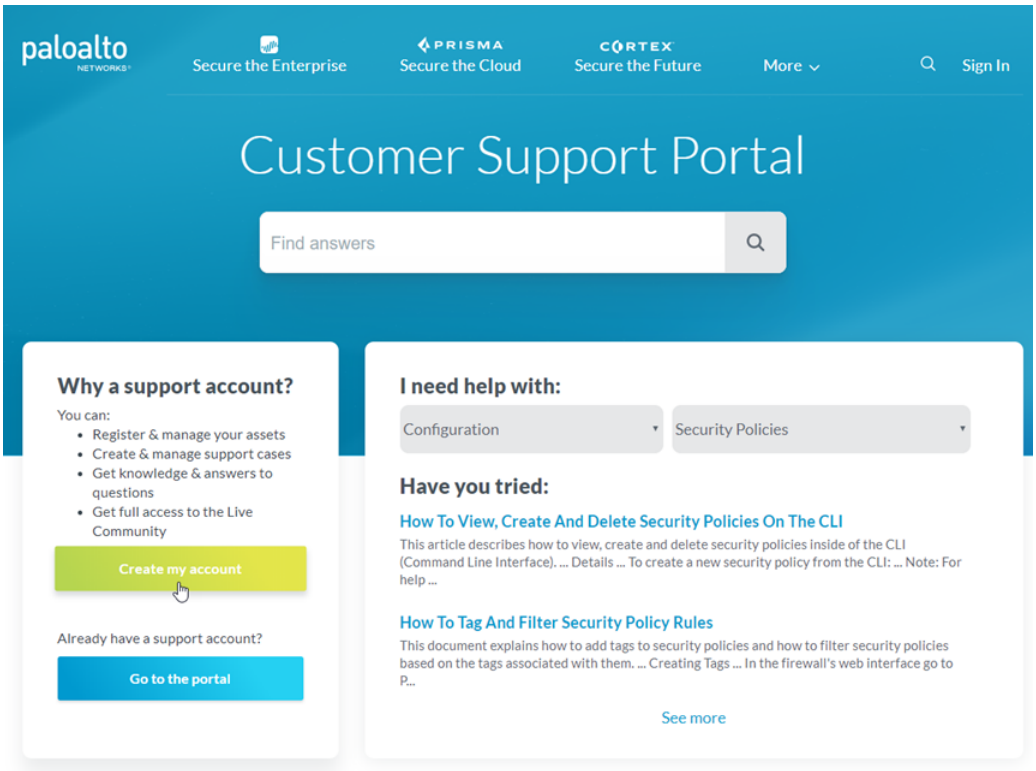
Si está registrando un cortafuegos VM-Series, consulte la Guía de implementación de VM-Series para obtener instrucciones.

Cree una nueva cuenta de soporte y registre un cortafuegos

Si todavía no tiene una cuenta de soporte activa de Palo Alto Networks, debe registrar su cortafuegos cuando cree una nueva.

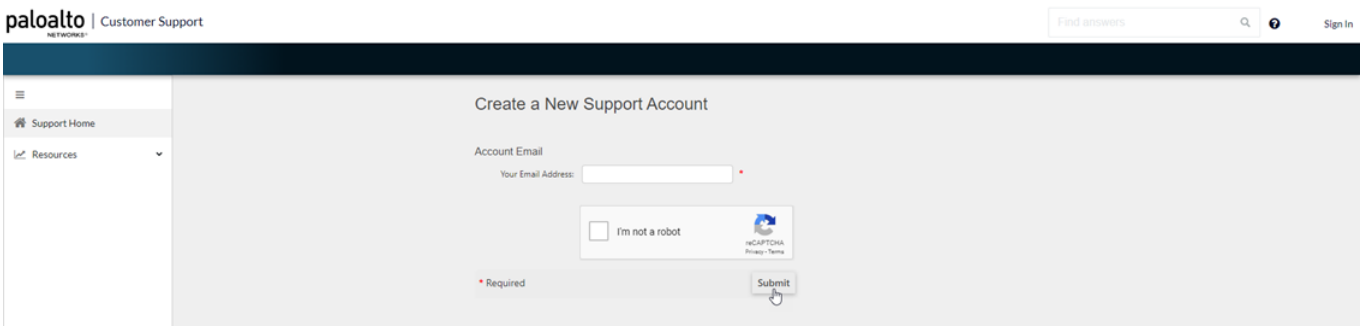
STEP 1 | Visite el portal de atención al cliente de Palo Alto Networks.

STEP 2 | Haga clic en **Create my account (Crear mi cuenta)**.

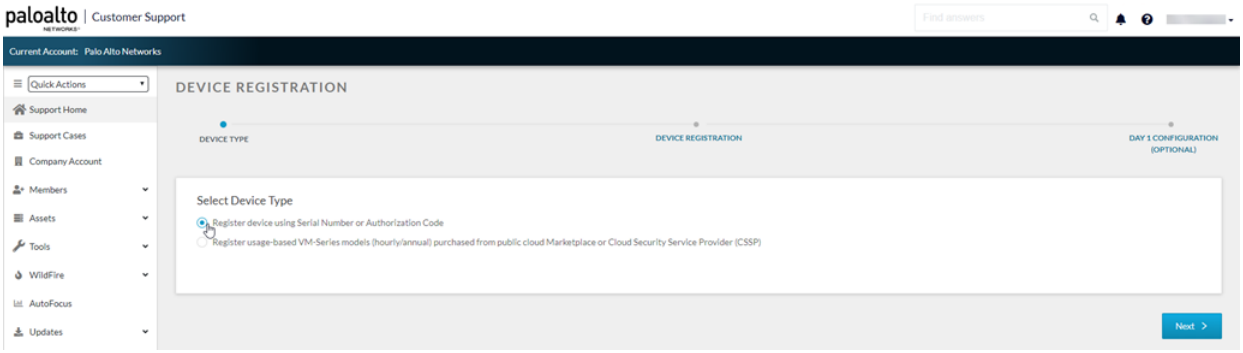


STEP 3 | Introduzca su dirección en **Your Email Address (Dirección de correo electrónico)**, marque la casilla **I'm not a robot (No soy un robot)** y haga clic en **Submit (Enviar)**.

© 2020 Palo Alto Networks, Inc.



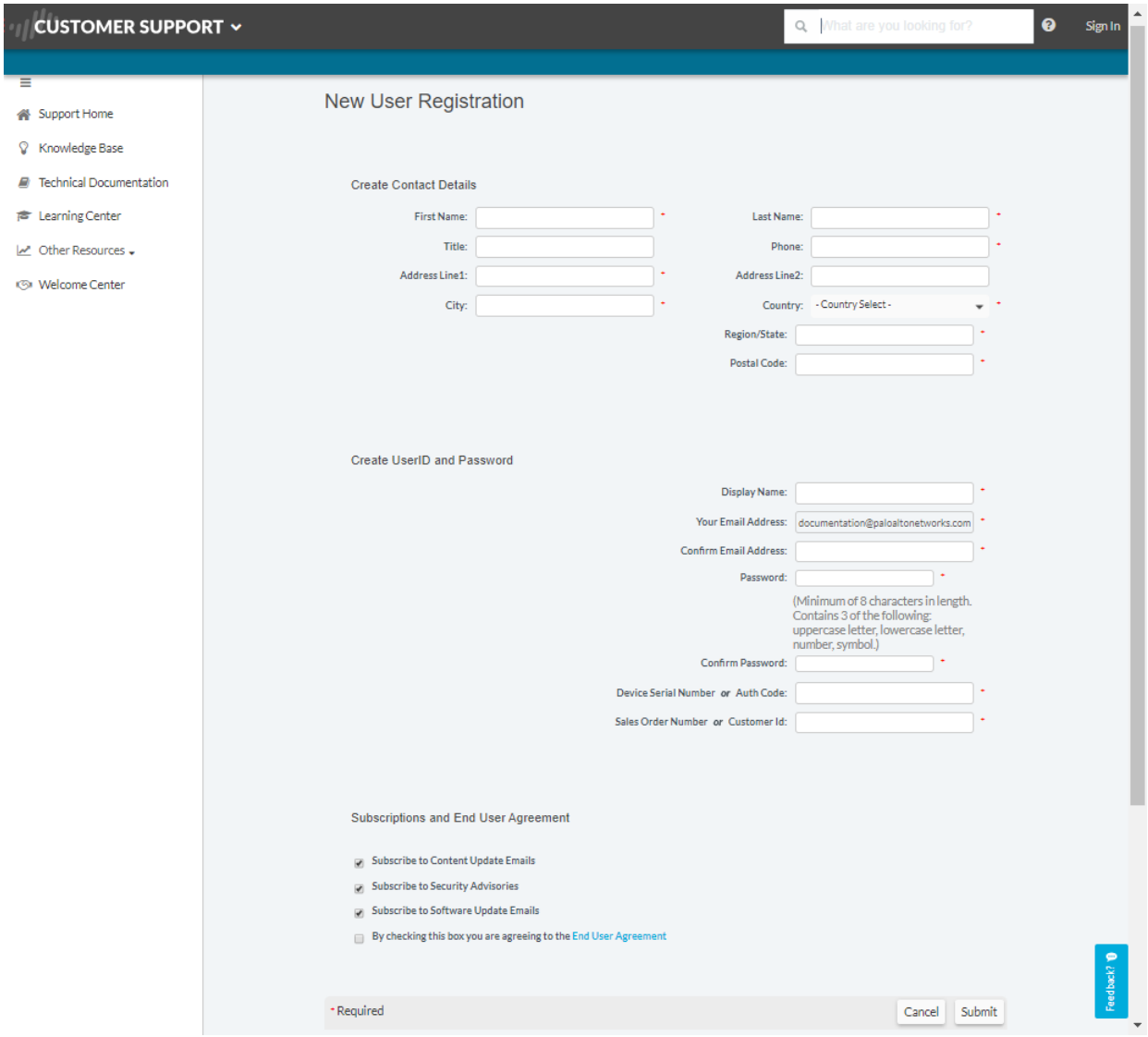
STEP 4 | Seleccione **Register device using Serial Number or Authorization Code (Registrar el dispositivo mediante un número de serie o código de autorización)** y haga clic en **Next (Siguiente)**.



STEP 5 | Complete el formulario de registro.

1. Introduzca la información de contacto de la persona en su organización que será propietaria de esta cuenta. Los campos obligatorios se indican con asteriscos rojos.
2. Cree una ID de usuario y contraseña para la cuenta. Los campos obligatorios se indican con asteriscos rojos.
3. Introduzca el **número de serie del dispositivo** o el **código de autenticación**.
4. Introduzca su **Sales Order Number (Número de pedido de venta)** o **Customer ID (ID de cliente)**.
5. Para garantizar que reciba siempre alertas sobre las actualizaciones y las recomendaciones de seguridad más recientes, marque **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**, **Subscribe to Security Advisories (Suscribirse para recibir recomendaciones de seguridad)** y **Subscribe to Software Update Emails (Suscribirse para recibir actualizaciones de software por correo electrónico)**.
6. Seleccione la casilla de verificación para aceptar el Acuerdo de usuario final y haga clic en **Submit (Enviar)**.

© 2020 Palo Alto Networks, Inc.



Registre un cortafuegos

Si ya tiene una cuenta activa de atención al cliente de Palo Alto Networks, lleve a cabo la siguiente tarea para registrar su cortafuegos.

STEP 1 | Inicie sesión en la interfaz web del cortafuegos.

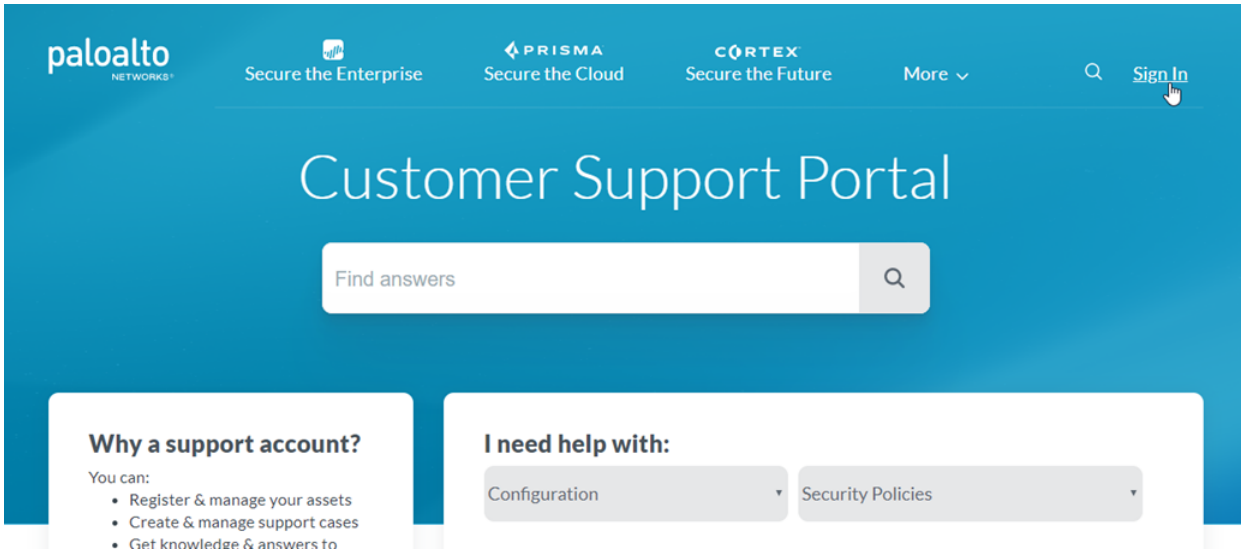
Si usa una conexión segura (HTTPS) desde su navegador web, inicie sesión usando la nueva dirección IP y contraseña que asignó durante la configuración inicial (https://<dirección IP>).

STEP 2 | Busque el número de serie y cópielo en el portapapeles.

En el **Panel**, busque su **número de serie** en la sección Información general de la pantalla.

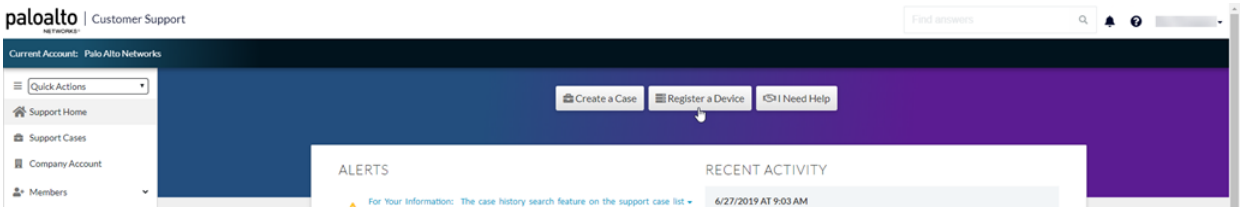
STEP 3 | Visite el portal de atención al cliente de Palo Alto Networks y, si todavía no ha iniciado sesión, haga clic en **Sign In (Iniciar sesión)** para hacerlo ahora.

© 2020 Palo Alto Networks, Inc.

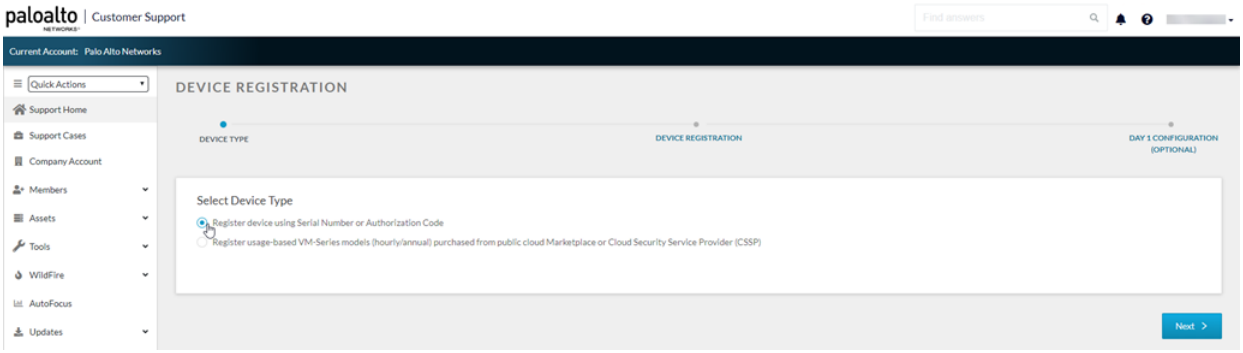


STEP 4 | Registre el cortafuegos.

1. En la página Support Home (Página de inicio del servicio de asistencia), haga clic en **Register a Device (Registrar dispositivo)**.

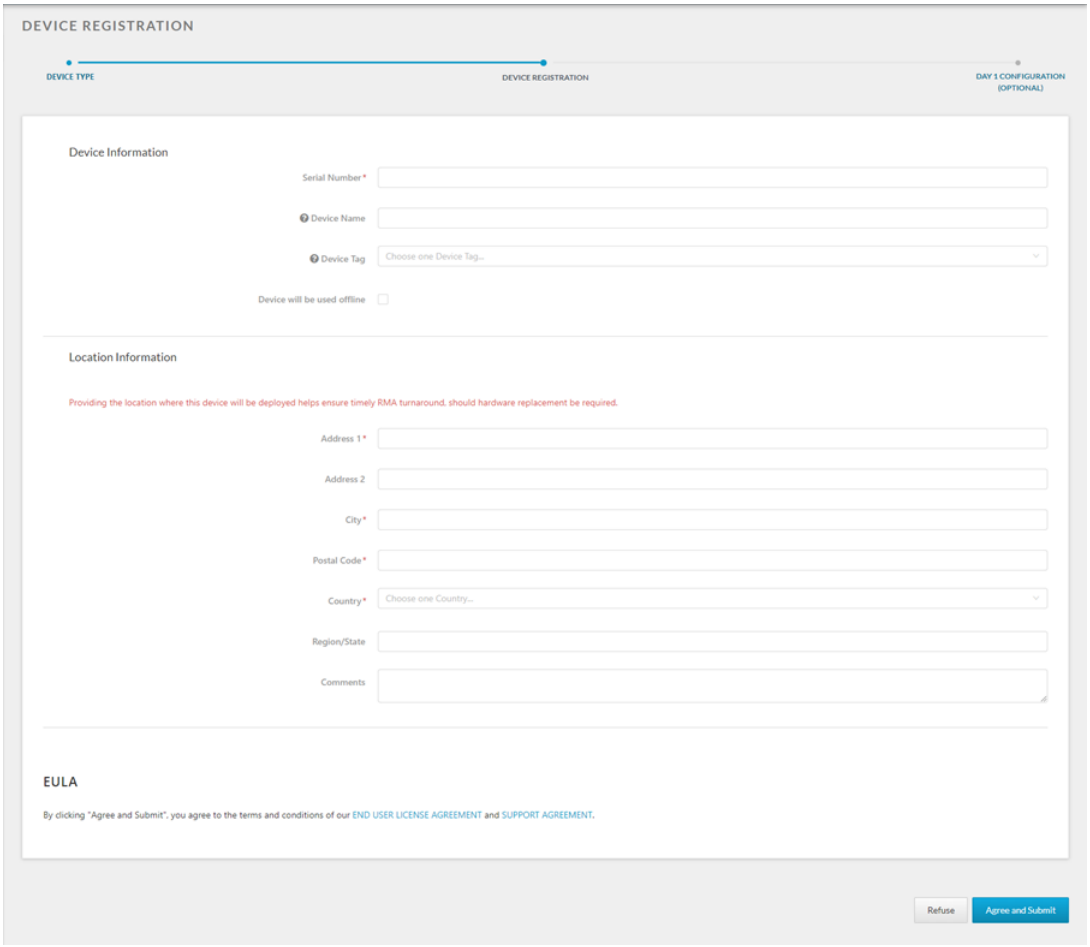


2. Seleccione **Register device using Serial Number or Authorization Code (Registrar el dispositivo mediante un número de serie o código de autorización)** y haga clic en **Next (Siguiente)**.



3. Introduzca el **número de serie** del cortafuegos (puede copiarlo y pegarlo desde el panel del cortafuegos).
4. ({0>Opcional<0}) Introduzca el **Device Name (Nombre del dispositivo)** y **Device Tag (Etiqueta de dispositivo)**.
5. (Opcional) Si el dispositivo no va a disponer de conexión a Internet, seleccione la casilla de verificación **Device will be used Offline (El dispositivo se usará sin conexión)** y, luego, seleccione la **OS Release (Versión de SO)** que planea utilizar.
6. Proporcione información sobre dónde planea implementar el cortafuegos, esto incluye la **dirección**, **ciudad**, **código postal** y **país**.
7. Lea el Acuerdo de licencia de usuario final (end-user license agreement, EULA) y el Acuerdo de soporte técnico y, luego, haga clic en **Agree and Submit (Aceptar y enviar)**.

© 2020 Palo Alto Networks, Inc.



Puede ver la entrada para el cortafuegos que acaba de registrar en **Devices (Dispositivos)**.

(Opcional) Configuración inicial

Después de registrar el cortafuegos, tiene la opción de ejecutar la configuración inicial. La herramienta Day 1 Configuration (Configuración inicial) proporciona plantillas de configuración según las prácticas recomendadas de Palo Alto Networks, que puede usar como punto de partida para crear el resto de su configuración.

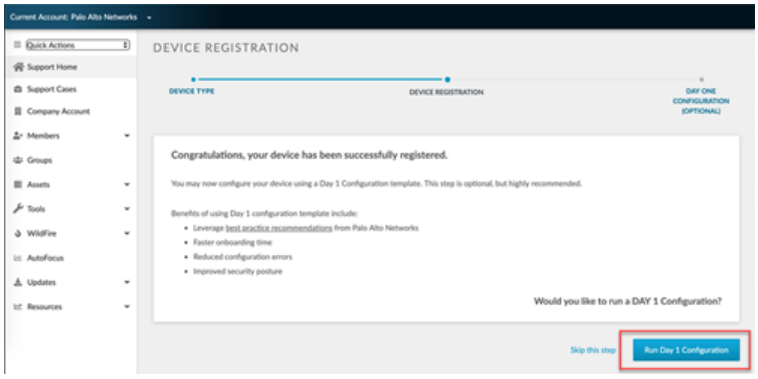
Estas son algunas de las ventajas de dichas plantillas:

- Implementación en menos tiempo
- Reducción de los errores de configuración
- Mejora de la estrategia de seguridad

Para ejecutar la configuración inicial, realice los pasos siguientes:

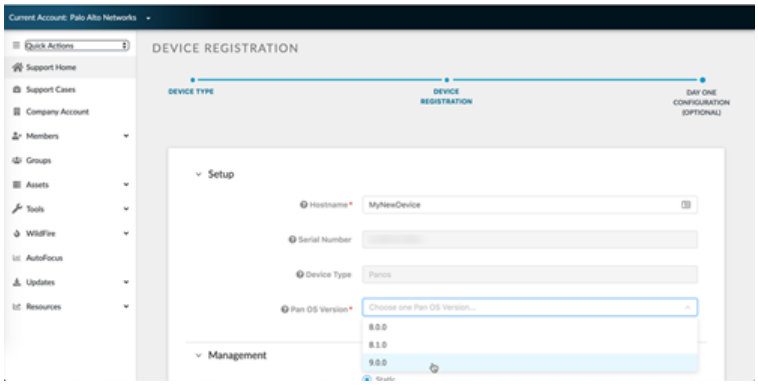
STEP 1 | Después de registrar el cortafuegos, se muestra una página que solo aparece una vez. En ella, haga clic en **Run Day 1 Configuration (Ejecutar configuración inicial)**.

© 2020 Palo Alto Networks, Inc.



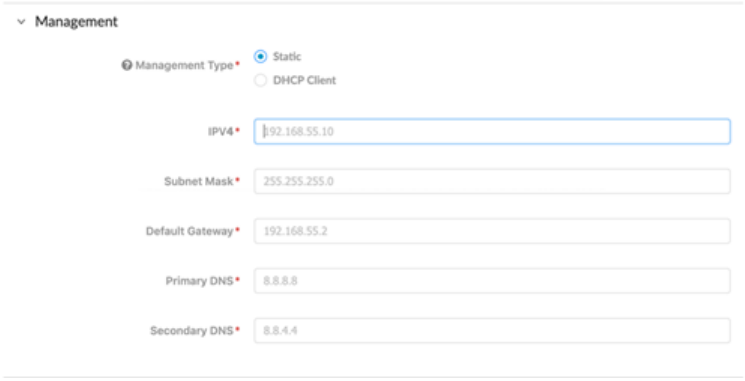
Si ya ha registrado el cortafuegos, pero no ha ejecutado Day 1 Configuration (Configuración inicial), también puede hacerlo desde la página de inicio del Portal de atención al cliente en Tools (Herramientas) > Run Day 1 Configuration (Ejecutar configuración inicial).

STEP 2 | Introduzca en **Hostname (Nombre de host)** y en **Pan OS Version (Versión de Pan-OS)** los valores que correspondan al nuevo dispositivo. También puede especificar los valores opcionales **Serial Number (Número de serie)** y **Device Type (Tipo de dispositivo)**.



STEP 3 | En la sección **Management (Gestión)**, seleccione **Static (Estático)** o **DHCP Client (Cliente DHCP)** en **Management Type (Tipo de gestión)**.

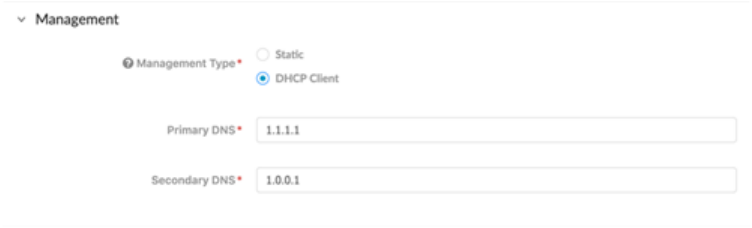
Si selecciona **Static (Estático)**, debe rellenar los campos **IPV4 (Ipv4),, Subnet Mask (Máscara de subred)** y **Default Gateway (Puerta de enlace predeterminada)**.



Si selecciona **DHCP Client (Cliente DHCP)**, solo tiene que rellenar los campos **Primary DNS (DNS primario)** y **Secondary DNS (DNS secundario)**. Si el dispositivo está configurado en el modo de

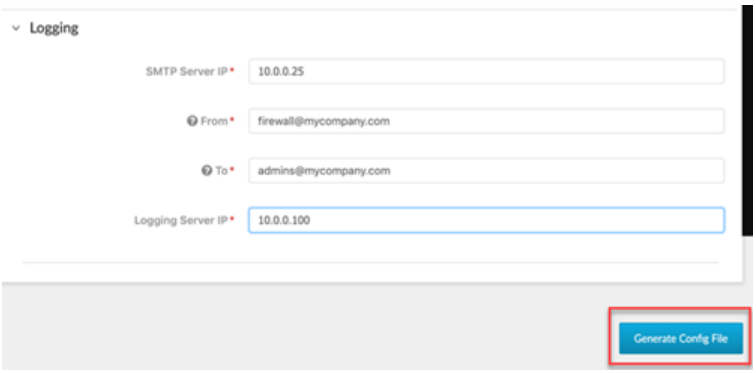
© 2020 Palo Alto Networks, Inc.

cliente DHCP, se asegura de que la interfaz de gestión reciba un dirección IP del servidor DHCP local o, si conoce los parámetros, los rellena.



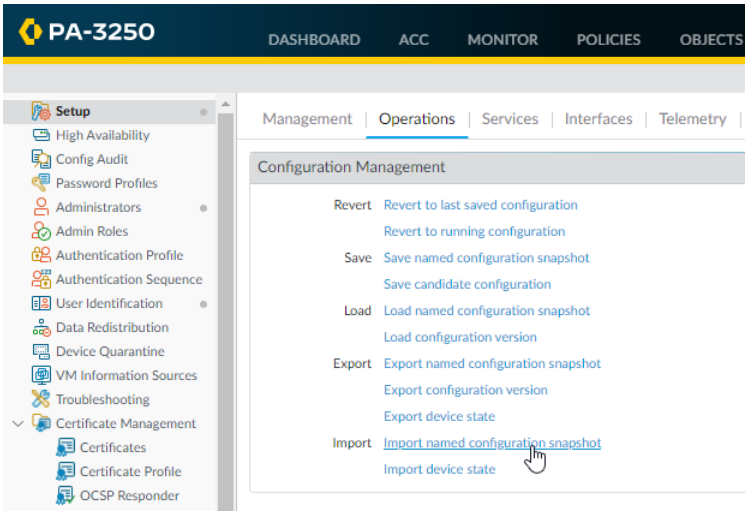
STEP 4 | Rellene todos los campos de la sección **Logging (Creación de logs)**.

STEP 5 | Haga clic en **Generate Config File (Generar archivo de configuración)**.



STEP 6 | Para importar el archivo de configuración inicial que acaba de descargar y cargarlo en el cortafuegos:

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
3. Haga clic en **Import named configuration snapshot (Importar instantánea de configuración con nombre)**.
4. Seleccione el archivo.



© 2020 Palo Alto Networks, Inc.

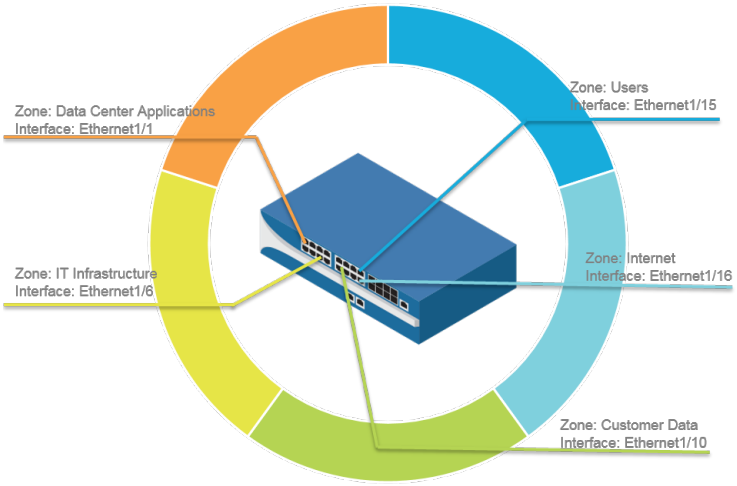
Segmentar su red con interfaces y zonas

El tráfico debe pasar por el cortafuegos para que este pueda gestionarlo y controlarlo. Físicamente, el tráfico entra en el cortafuegos y sale de este a través de las *interfaces*. El cortafuegos determina el modo en que se actúa en un paquete dependiendo de si el paquete coincide con una *regla de política de seguridad*. En el nivel más básico, cada regla de la política de seguridad debe identificar de dónde viene el tráfico y a dónde va. En un cortafuegos de nueva generación Palo Alto Networks, las reglas de la política de seguridad se aplican entre zonas. Una *zona* es un grupo de interfaces (físicas o virtuales) que representa un segmento de su red que está conectado con, y controlado por, el cortafuegos. Debido a que el tráfico solo puede fluir entre zonas si existe una regla de política de seguridad que lo permita, esta es su primera línea de defensa. Mientras más pormenorizadas sean las zonas que cree, mayor control tendrá sobre el acceso a aplicaciones y datos delicados, y mayor protección tendrá contra el malware que se mueve de manera lateral por la red. Por ejemplo, podría segmentar el acceso a los servidores de base de datos que almacenan los datos de sus clientes en una zona denominada Datos de clientes. Luego puede definir políticas de seguridad que solo permitan a ciertos usuarios o grupos de usuarios acceder a la zona de Datos de clientes, con lo cual evita el acceso no autorizado interno o externo a los datos almacenados en ese segmento.

- Segmentación de la red para una superficie de ataque reducida
- Configuración de interfaces y zonas

Segmentación de la red para una superficie de ataque reducida

El siguiente diagrama muestra un ejemplo básico de la Segmentación de la red con zonas. Mientras más pormenorizadas sean las zonas (y las correspondientes reglas de política de seguridad que permiten el tráfico entre las zonas), más reducida será la superficie de ataque de la red. Esto se debe a que el tráfico puede fluir libremente dentro de una zona (tráfico intrazona), pero el tráfico no puede fluir entre zonas (tráfico interzona) hasta que usted defina una regla de política de seguridad que lo permita. Además, una interfaz no puede procesar el tráfico hasta que lo haya asignado a una zona. Por lo tanto, al segmentar su red en zonas pormenorizadas, tiene mayor control sobre el acceso a aplicaciones o datos delicados, y puede prevenir que el tráfico malintencionado establezca un canal de comunicación dentro de su red, con lo cual reduce la probabilidad de un ataque consumado en la red.



Configuración de interfaces y zonas

Una vez que identifique cómo desea segmentar la red y las zonas que deberá crear para lograr la segmentación (además de las interfaces para asignar a cada zona), puede comenzar por configurar las

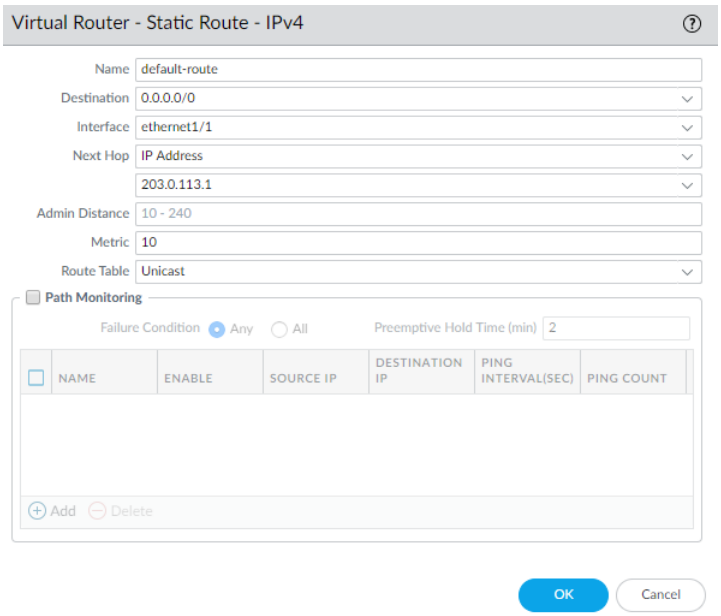
© 2020 Palo Alto Networks, Inc.

interfaces y zonas en el cortafuegos. Configure interfaces en el cortafuegos para admitir la topología de cada parte de la red con la que está conectándose. El siguiente flujo de trabajo muestra cómo configurar las interfaces de capa 3 y cómo asignarlas a zonas. Para obtener detalles sobre la integración del cortafuegos usando un tipo diferente de implementaciones de interfaz (por ejemplo, como interfaces de cable virtual o como interfaces de capa 2), consulte Redes.

El cortafuegos viene preconfigurado con una interfaz de Virtual Wire por defecto entre los puertos Ethernet 1/1 y Ethernet 1/2 (y una política de seguridad y un enrutador virtual predeterminados correspondientes). Si no tiene previsto usar el cable virtual predeterminado, debe eliminar manualmente la configuración y confirmar el cambio antes de continuar para evitar que interfiera con otras configuraciones que defina. Para obtener instrucciones sobre cómo eliminar el cable virtual predeterminado y sus zonas y política de seguridad asociadas, consulte el Paso 3 en Configuración de acceso para servicios externos.

STEP 1 | Configure una ruta predeterminada hacia su enrutador de Internet.

1. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y luego seleccione el enlace **default (predeterminado)** para que se abra el cuadro de diálogo Virtual Router (Enrutador virtual).
2. Seleccione la pestaña **Static Routes (Rutas estáticas)** y haga clic en **Add (Añadir)**. Introduzca un **Nombre** para la ruta e introduzca la ruta en el campo **Destino** (por ejemplo, 0.0.0.0/0).
3. Seleccione el botón de opción **Dirección IP** en el campo **Siguiente salto** y, a continuación, introduzca la dirección IP y la máscara de red para su puerta de enlace de Internet (por ejemplo, 203.0.113.1).



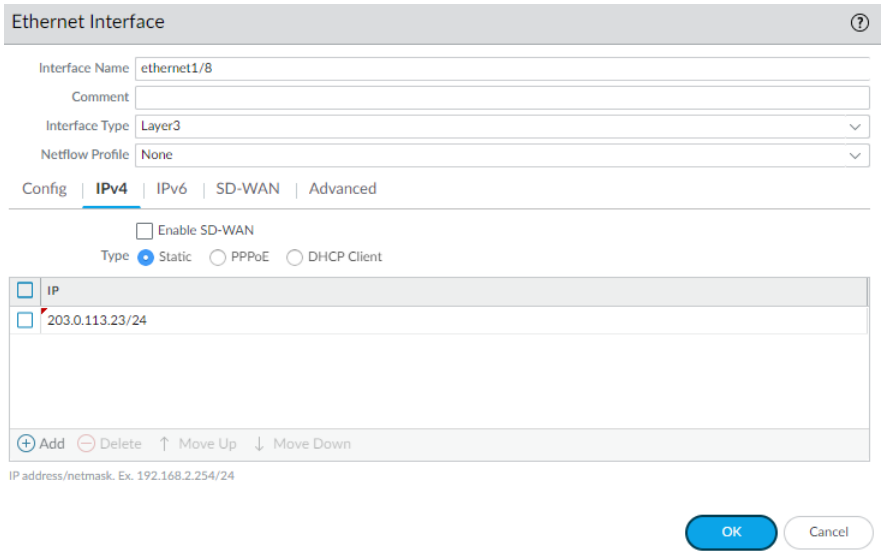
4. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración de enrutador virtual.

STEP 2 | Configure la interfaz externa (la interfaz que se conecta a Internet).

1. Seleccione **Network (Red)** > **Interfaces** y luego seleccione la interfaz que desea configurar. En este ejemplo, estamos configurando Ethernet1/8 como la interfaz externa.
2. Seleccione **Interface Type (Tipo de interfaz)**. Aunque su decisión aquí depende de la topología de su red, este ejemplo muestra los pasos para **Layer3**.
3. En la pestaña **Config (Configuración)**, seleccione **New Zone (Nueva zona)** en el menú desplegable **Security Zone (Zona de seguridad)**. En el cuadro de diálogo Zone, defina un **nombre** para la nueva zona, por ejemplo, Internet, y a continuación haga clic en **OK**.
4. En el menú desplegable **Virtual Router (Enrutador virtual)**, seleccione **default (predeterminado)**.

© 2020 Palo Alto Networks, Inc.

5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 203.0.113.23/24.



6. Para que pueda hacer ping en la interfaz, seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**, expanda la lista desplegable **Management Profile (Perfil de gestión)** y seleccione **New Management Profile (Nuevo perfil de gestión)**. Introduzca un **Nombre** para el perfil, seleccione **Ping** y, a continuación, haga clic en **Aceptar**.
7. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 3 | Configure la interfaz que se conecta a su red interna.

En este ejemplo, la interfaz se conecta a un segmento de red que utiliza direcciones IP privadas. Dado que las direcciones IP privadas no se pueden enrutar externamente, debe configurar NAT.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz que desea configurar. En este ejemplo, estamos configurando Ethernet1/15 como la interfaz interna a la que se conectan nuestros usuarios.
2. Seleccione **Layer3** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. En el cuadro de diálogo Zone, defina un **Name (Nombre)** para la nueva zona; por ejemplo, Usuarios, y a continuación haga clic en **OK (Aceptar)**.
4. Seleccione el mismo enrutador virtual que utilizó anteriormente; en este ejemplo, el predeterminado.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.1.4/24.
6. Para poder hacer ping a la interfaz, seleccione el perfil de gestión que acaba de crear.
7. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 4 | Configure la interfaz que se conecta a sus aplicaciones del centro de datos.

Asegúrese de definir zonas granulares para evitar el acceso no autorizado a aplicaciones o datos confidenciales y eliminar la posibilidad de que el malware se mueva lateralmente dentro de su centro de datos.

1. Seleccione la interfaz que desee configurar.

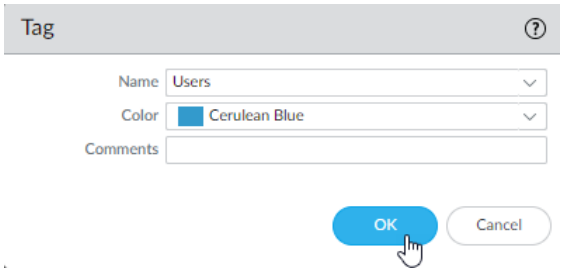
© 2020 Palo Alto Networks, Inc.

2. Seleccione **Layer3** en el menú desplegable **Interface Type**. En este ejemplo, estamos configurando Ethernet1/1 como la interfaz que le proporciona acceso a sus aplicaciones del centro de datos.
3. En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**. En el cuadro de diálogo Zone, defina un **nombre** para la nueva zona; por ejemplo Aplicaciones del centro de datos y, a continuación, haga clic en **OK**.
4. Seleccione el mismo enrutador virtual que utilizó anteriormente; en este ejemplo, el predeterminado.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 10.1.1.1/24.
6. Para poder hacer ping a la interfaz, seleccione el perfil de gestión que acaba de crear.
7. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 5 | (Opcional) Cree etiquetas para cada zona.

Las etiquetas le permitirán explorar visualmente las reglas de política.

1. Seleccione **Objects (Objetos)** > **Tags (Etiquetas)** y **Add (Añadir)**.
2. Seleccione un nombre para la zona en **Nombre**.
3. Seleccione un **Color** para la etiqueta y haga clic en **OK**.



STEP 6 | Guarde la configuración de la interfaz.

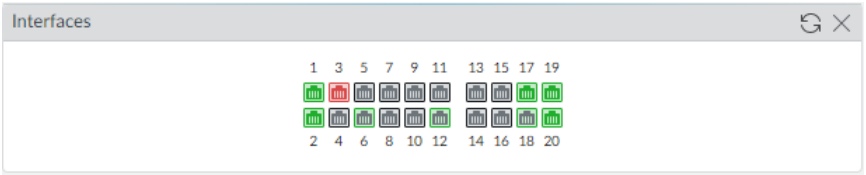
Haga clic en **Commit (Confirmar)**.

STEP 7 | Conecte los cables del cortafuegos.

Conecte cables directos desde las interfaces que ha configurado al conmutador o enrutador de cada segmento de red.

STEP 8 | Verifique que las interfaces estén activas.

Seleccione **Dashboard (Panel)** y verifique que las interfaces que configuró aparezcan en verde en el widget de las interfaces.



© 2020 Palo Alto Networks, Inc.

Configuración de una política de seguridad básica

Ahora que ha definido algunas zonas y las ha vinculado a interfaces, ya puede empezar a crear su política de seguridad. El cortafuegos impedirá el flujo de tráfico de una zona a otra, a menos que exista una regla de política de seguridad que lo permita. Cuando un paquete ingresa en la interfaz de un cortafuegos, el cortafuegos compara los atributos del paquete con las reglas de políticas de seguridad para determinar si una sesión se bloqueará o se permitirá basándose en atributos tales como la zona de seguridad de origen y destino, la dirección IP de origen y destino, la aplicación, el usuario y el servicio. El cortafuegos evalúa, de izquierda a derecha y de arriba abajo, el tráfico entrante en función de la base de reglas de la política de seguridad y, luego, toma la medida que se especifica en la primera regla de seguridad coincidente (por ejemplo, si se debe permitir, denegar o descartar el paquete). Esto significa que, para garantizar que el cortafuegos aplique la política como se espera, debe ordenar las reglas de la base de reglas de la política de seguridad de modo que las más específicas estén al principio de dicha base y las más generales, al final.

Aunque una regla de política de seguridad permita un paquete, eso no significa que el tráfico está libre de amenazas. Para permitir que el cortafuegos analice el tráfico que permite según una regla de la política de seguridad, también debe vincular perfiles de seguridad (filtrado de URL, antivirus, antispyware, bloqueo de archivos y análisis de WildFire incluidos) a cada regla (los perfiles que puede usar dependen de las Suscripciones que compre). Al crear su política de seguridad básica, utilice los perfiles de seguridad predefinidos para garantizar que se analice el tráfico permitido en la red en busca de amenazas. Puede personalizar estos perfiles más tarde según fuera necesario para su entorno.

Use el siguiente flujo de trabajo para configurar una política de seguridad muy básica que permita el acceso a la infraestructura de red, a las aplicaciones del centro de datos y a internet. Esto le permite poner en funcionamiento el cortafuegos para verificar si se ha configurado correctamente. No obstante, esta política inicial no es lo suficientemente integral para proteger su red. Después de verificar que haya configurado el cortafuegos y lo haya integrado en su red correctamente, continúe con la práctica recomendada de política de seguridad de puerta de enlace de internet, que franquea el acceso seguro a las aplicaciones y, a la vez, protege su red contra ataques.

STEP 1 | (Opcional) Elimine la regla de política de seguridad predeterminada.

De forma predeterminada, el cortafuegos incluye una regla de política de seguridad, denominada *rule1 (regla1)*, que permite todo el tráfico de la zona fiable a la zona no fiable. Puede eliminar la regla o modificarla para reflejar su convención de denominación de zonas.

STEP 2 | Permita el acceso a sus recursos de infraestructura de red.

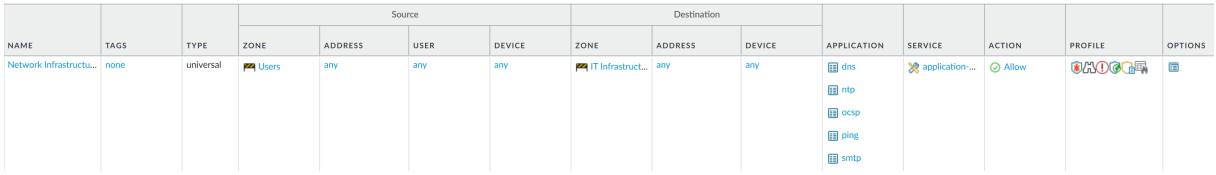
1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name** para la regla.
3. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en **Users (Usuarios)**.
4. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** en **IT Infrastructure (Infraestructura de TI)**.



Se recomienda usar objetos de dirección en el campo Destination Address (Dirección de destino) para habilitar el acceso únicamente a servidores o grupos de servidores concretos, en particular para servicios como DNS y SMTP, que suelen tener vulnerabilidades. Si restringe a los usuarios a direcciones del servidor de destino concretas, previene que se filtren datos y, además, que el tráfico de comando y control establezca la comunicación mediante técnicas como la tunelización de DNS.

© 2020 Palo Alto Networks, Inc.

5. En la pestaña **Applications**, seleccione **Add** para añadir las aplicaciones que corresponden a los servicios de red que desea habilitar de manera segura. Por ejemplo, seleccione **dns**, **ntp**, **ocsp**, **ping** y **smtp**.
6. En la pestaña **Service/URL Category (Categoría de servicio/URL)**, mantenga **Service (Servicio)** establecido como **application-default (aplicación-predeterminado)**.
7. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
8. Configure **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione los siguientes perfiles de seguridad para adjuntarlos a la regla de política:
   - En **Antivirus**, seleccione **default (predeterminado)**.
   - En **Vulnerability Protection (Protección contra vulnerabilidades)**, seleccione **strict (estricta)**.
   - En **Anti-Spyware (Antispyware)**, seleccione **strict (estricto)**.
   - En **URL Filtering (Filtrado de URL)**, seleccione **default (predeterminado)**.
   - En **File Blocking (Bloqueo de archivos)**, seleccione **basic file blocking (bloqueo de archivos básico)**.
   - En **WildFire Analysis (Análisis de WildFire)**, seleccione **default (predeterminado)**.
9. Verifique que **Log at Session End** esté habilitado. Solo se registra el tráfico que coincida con alguna regla de la política de seguridad.
10. Haga clic en **OK (Aceptar)**.



STEP 3 | Habilite el acceso a las aplicaciones generales de internet.

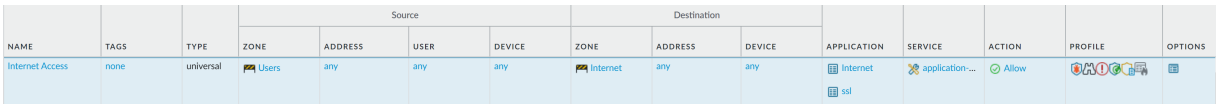
> *Esta es una regla temporal que le permite recopilar información sobre el tráfico de su red. En cuanto obtiene más información sobre las aplicaciones a las que deben acceder los usuarios, puede tomar decisiones fundamentadas sobre qué aplicaciones permitir y crear reglas más pormenorizadas y basadas en aplicaciones para cada grupo de usuarios.*

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego haga clic en **Add (Añadir)** para añadir una regla.
2. En la pestaña **General**, introduzca un **Name** para la regla.
3. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en **Users (Usuarios)**.
4. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** en **Internet**.
5. En la pestaña **Applications (Aplicaciones)**, haga clic en **Add (Añadir)** para añadir un filtro de aplicaciones en **Application Filter (Filtro de aplicación)** e introduzca un nombre en **Name (Nombre)**. Para habilitar de manera segura el acceso a aplicaciones web legítimas, configure la opción **Category (Categoría)** del filtro de aplicaciones en **general-internet (internet general)** y, luego, haga clic en **OK (Aceptar)**. Para habilitar el acceso a sitios cifrados, seleccione **Add (Añadir)** para añadir la aplicación **ssl**.
6. En la pestaña **Service/URL Category (Categoría de servicio/URL)**, mantenga **Service (Servicio)** establecido como **application-default (aplicación-predeterminado)**.
7. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
8. Configure **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione los siguientes perfiles de seguridad para adjuntarlos a la regla de política:
   - En **Antivirus**, seleccione **default (predeterminado)**.
   - En **Vulnerability Protection (Protección contra vulnerabilidades)**, seleccione **strict (estricta)**.

© 2020 Palo Alto Networks, Inc.

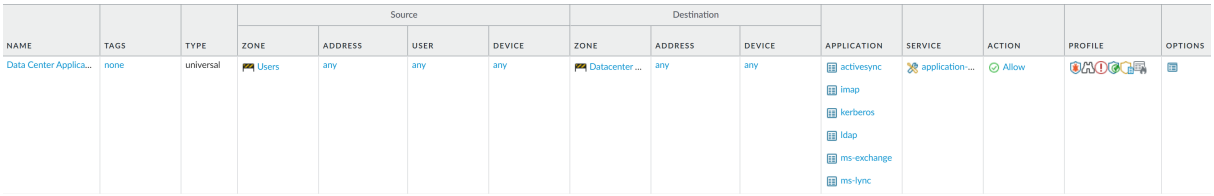
- En **Anti-Spyware (Antispyware)**, seleccione **strict (estricto)**.
- En **URL Filtering (Filtrado de URL)**, seleccione **default (predeterminado)**.
- En **File Blocking (Bloqueo de archivos)**, seleccione **strict file blocking (bloqueo de archivos estricto)**.
- En **WildFire Analysis (Análisis de WildFire)**, seleccione **default (predeterminado)**.

9. Verifique que **Log at Session End** esté habilitado. Únicamente se registrará el tráfico que coincida con una regla de seguridad.
10. Haga clic en **OK (Aceptar)**.



STEP 4 | Habilite el acceso a las aplicaciones del centro de datos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y, luego haga clic en **Add (Añadir)** para añadir una regla.
2. En la pestaña **General**, introduzca un nombre descriptivo para la regla en **Name (Nombre)**.
3. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en **Users (Usuarios)**.
4. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** en **Data Center Applications (Aplicaciones de centros de datos)**.
5. En la pestaña **Applications**, seleccione **Add** para añadir las aplicaciones que corresponden a los servicios de red que desea habilitar de manera segura. Por ejemplo, seleccione **activesync**, **imap**, **kerberos**, **ldap**, **ms-exchange** y **ms-lync**.
6. En la pestaña **Service/URL Category (Categoría de servicio/URL)**, mantenga **Service (Servicio)** establecido como **application-default (aplicación-predeterminado)**.
7. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
8. Configure **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione los siguientes perfiles de seguridad para adjuntarlos a la regla de política:
   - En **Antivirus**, seleccione **default (predeterminado)**.
   - Para **Vulnerability Protection (Protección de vulnerabilidades)**, seleccione **strict (estricta)**.
   - Para **Anti-Spyware**, seleccione **strict (estricto)**.
   - Para **URL Filtering (Filtrado de URL)**, seleccione **default (predeterminado)**.
   - Para **File Blocking (Bloqueo de archivos)**, seleccione **basic file blocking (bloqueo de archivos básico)**.
   - Para **WildFire Analysis (Análisis de WildFire)**, seleccione **default (predeterminado)**.
9. Verifique que **Log at Session End** esté habilitado. Únicamente se registrará el tráfico que coincida con una regla de seguridad.
10. Haga clic en **OK (Aceptar)**.



STEP 5 | Guarde las reglas de política en la configuración que se esté ejecutando en el cortafuegos.

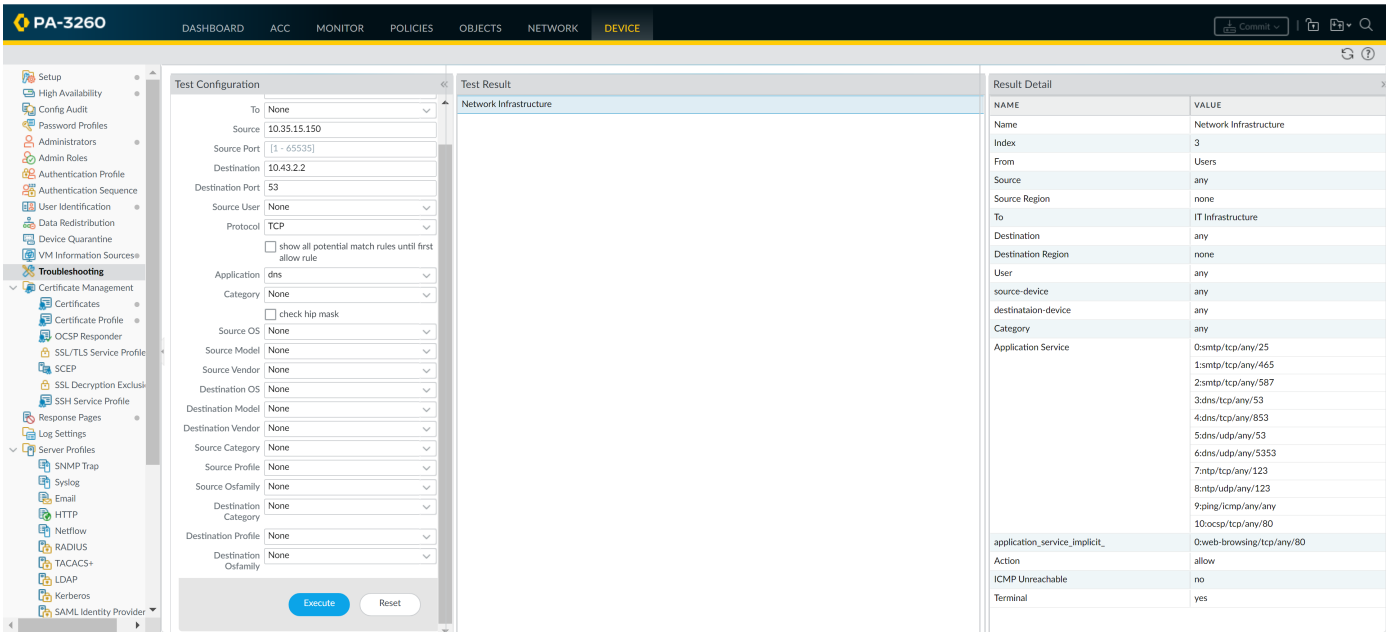
Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Para verificar que ha configurado las políticas de seguridad básicas de manera eficaz, compruebe si se están evaluando sus reglas y determine cuál de ellas se aplica a cada flujo de tráfico.

Por ejemplo, para verificar la regla de política que se aplicará a un cliente en la zona de usuario con la dirección IP 10.35.14.150 cuando envía una consulta DNS al servidor DNS en el centro de datos:

1. Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y, luego, seleccione **Security Policy Match (Coincidencia con política de seguridad)** en **Select Test (Seleccionar prueba)**.
2. Introduzca las direcciones IP correspondientes en **Source (Origen)** y en **Destination (Destino)**.
3. Introduzca el **protocolo**.
4. Seleccione **dns** en **Application (Aplicación)**.
5. Haga clic en **Execute (Ejecutar)** para comprobar la coincidencia con la política de seguridad.



© 2020 Palo Alto Networks, Inc.

Evaluación del tráfico de red

Ahora que tiene una política de seguridad básica, podrá revisar las estadísticas y los datos en el Centro de control de aplicaciones (Application Command Center, ACC), además de los logs de tráfico y logs de amenazas para observar tendencias en su red. Use esta información para identificar dónde necesita para crear reglas de política de seguridad más detalladas.

- Utilice el centro de control de aplicaciones y Utilice el motor de correlación automatizada.

  En el ACC, revise las aplicaciones más utilizadas y las aplicaciones de alto riesgo en su red. El ACC resume gráficamente la información de logs para resaltar las aplicaciones que cruzan la red, quién las está utilizando (con el ID de usuario habilitado) y el posible impacto en la seguridad del contenido para ayudarle a identificar qué sucede en la red en tiempo real. A continuación, podrá utilizar esta información para crear reglas de políticas de seguridad adecuadas que bloqueen las aplicaciones no deseadas y que permitan y habiliten aplicaciones de manera segura.

  El widget Hosts en riesgo en **ACC** > **Threat Activity (Actividad de amenazas)** muestra los hosts potencialmente en riesgo en su red y los logs, y asocia pruebas que corroboran los eventos.

- Determine qué actualizaciones/modificaciones son necesarias para sus reglas de políticas de seguridad de red e implemente los cambios.

  Por ejemplo:

  - Evalúe si desea permitir contenido web según la programación, los usuarios o los grupos.
  - Permita o controle determinadas aplicaciones o funciones dentro de una aplicación.
  - Descifre e inspeccione contenido.
  - Permita con exploración en busca de amenazas y explotaciones.

  Para obtener información sobre cómo refinar sus políticas de seguridad y adjuntar perfiles de seguridad personalizados, consulte cómo Crear una regla de política de seguridad y Perfiles de seguridad.

- Visualización de logs.

  De manera específica, visualice los logs de tráfico y amenaza (**Monitor [Supervisar]** > **Logs [Logs]**).

  Los logs de tráfico dependen del modo en que sus políticas de seguridad están definidas y configuradas para registrar el tráfico. Sin embargo, el widget Application Usage en ACC registra aplicaciones y estadísticas independientemente de la configuración de las políticas; muestra todo el tráfico que se permite en su red, por lo que incluye el tráfico interzona, que permite la política y el tráfico de la misma zona que se permite implícitamente.

- Configuración de cuotas de almacenamiento y periodos de vencimiento de logs.

  Revise el resumen de inteligencia de AutoFocus para los artefactos de sus logs. Un *artefacto* es un elemento, propiedad, actividad o comportamiento asociado con eventos de logs en el cortafuegos. El resumen de inteligencia revela la cantidad de sesiones y muestras en las que WildFire detectó el artefacto. Use la información de veredicto de WildFire (benigna, grayware, malware) y las etiquetas coincidentes de AutoFocus para buscar posibles riesgos en la red.

  Las etiquetas de AutoFocus creadas por Unit 42, el equipo de inteligencia de amenazas de Palo Alto Networks, llaman la atención sobre campañas y amenazas avanzadas y específicas de su red.

© 2020 Palo Alto Networks, Inc.

A partir del resumen de inteligencia de AutoFocus, usted puede iniciar una búsqueda de AutoFocus para detectar artefactos y evaluar su expansión en el contexto global, industrial y de red.

- Supervisión de la actividad web de los usuarios de red.

  Revise los logs de filtrado de URL para examinar alertas, URL y categorías denegadas. Los logs de URL se generan cuando un tráfico coincide con una regla de seguridad que tenga un perfil de filtrado de URL adjunto con una acción de alertar, continuar, sobrescribir o bloquear.

© 2020 Palo Alto Networks, Inc.

Habilitación del reenvío gratuito de WildFire

WildFire es un entorno virtual basado en la nube que analiza y ejecuta muestras desconocidas (archivos y enlaces de correo electrónico), y determina si las muestras son malintencionadas, phishing, grayware o benignas. Con WildFire habilitado, un cortafuegos de Palo Alto Networks puede reenviar muestras desconocidas a WildFire para su análisis. Para el malware recién descubierto, WildFire genera una firma para detectar el malware, que está disponible para su recuperación en tiempo real para todos los cortafuegos con una suscripción activa de WildFire. Esto habilita a los cortafuegos de nueva generación de Palo Alto en todo el mundo a detectar y prevenir el malware detectado por un único cortafuegos. Las firmas de malware a menudo coinciden con múltiples variantes de la misma familia de malware y, como tales, bloquean nuevas variantes de malware que el cortafuegos nunca había visto antes. El equipo de investigación de amenazas de Palo Alto Networks utiliza la inteligencia contra amenazas recopilada de las variantes de malware para bloquear direcciones IP, dominios y URL malintencionadas.

El servicio básico de WildFire se incluye como parte del cortafuegos de nueva generación de Palo Alto Networks y no requiere una suscripción a WildFire. Con el servicio básico de WildFire, usted puede habilitar el cortafuegos para reenviar archivos portables ejecutables (portable executable, PE). Además, si no tiene una suscripción a WildFire, pero sí tiene una suscripción de prevención de amenazas, puede recibir firmas para el malware que WildFire identifica cada 24 o 48 horas (como parte de las actualizaciones del antivirus).

Más allá del servicio básico de WildFire, se necesita una suscripción a WildFire para que el cortafuegos realice lo siguiente:

- Obtenga las últimas firmas de WildFire en tiempo real.
- Evite que los archivos ejecutables portátiles maliciosos y los scripts de PowerShell accedan a su red en tiempo real mediante WildFire Inline ML.
- Reenvíe tipos de archivos avanzados y enlaces de correo electrónico para su análisis.
- Uso de la API de WildFire.
- Utilice un dispositivo WildFire para alojar una nube privada de WildFire o una nube híbrida de WildFire.

Si tiene una suscripción a WildFire, siga adelante y comience a usar WildFire para aprovechar al máximo su suscripción. De lo contrario, realice los siguientes pasos para habilitar el reenvío básico de WildFire:

STEP 1 | Confirme que su cortafuegos está registrado y que tiene una cuenta válida de asistencia técnica, así como las suscripciones que usted requiera.

1. Inicie sesión en el Portal de atención al cliente (Customer Support Portal, CSP) de Palo Alto Networks y en el panel de navegación de la izquierda, seleccione **Assets (Activos)** > **Devices (Dispositivos)**.
2. Verifique que el cortafuegos está incluido en la lista. Si no está en la lista, seleccione **Register New Device (Registrar dispositivo nuevo)** y continúe con el registro del cortafuegos.
3. (Opcional) Si tiene una suscripción a Threat Prevention, realice el procedimiento Activación de licencias de suscripción.

STEP 2 | Inicie sesión en el cortafuegos y configure los ajustes de reenvío de WildFire.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** y modifique la configuración general.
2. Configure el campo **WildFire Public Cloud (Nube pública de WildFire)** para que reenvíe los archivos a la nube pública de WildFire en: **`wildfire.paloaltonetworks.com`**.



También puede reenviar archivos a una nube regional o una nube privada según su ubicación y sus requisitos organizativos.

© 2020 Palo Alto Networks, Inc.

3. Revise los **File Size Limits (Límites de tamaño de archivo)** para los PE que el cortafuegos reenvía para el análisis de WildFire. Configure el **Size Limit (Límite de tamaño)** para los PE que el cortafuegos puede reenviar en el límite máximo disponible de 10 MB.

   Como práctica recomendada de WildFire, configure el Size Limit (Límite de tamaño) para los PE en el límite máximo disponible de 10 MB.

4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 3 | Habilite el cortafuegos para que reenvíe PE para su análisis.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **WildFire Analysis (Análisis de WildFire)** y luego **Add (Añadir)** para añadir una nueva regla de perfil.
2. Indique un nombre para la nueva regla de perfil en **Name**.
3. Seleccione **Add (Añadir)** para añadir una regla de reenvío e introduzca un nombre en **Name** para dicha regla.
4. En la columna **File Types (Tipos de archivo)**, añada archivos **pe** a la regla de reenvío.
5. En la columna **Analysis**, seleccione **public-cloud** para reenviar PE a la nube pública de WildFire.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Aplique el nuevo perfil de análisis de WildFire al tráfico que permite el cortafuegos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una política existente o cree una nueva política según se describe en Configuración de una política de seguridad básica.
2. Seleccione **Actions (Acciones)** y en la sección Profile Settings, configure el **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)**.
3. Seleccione el perfil **WildFire Analysis (Análisis de WildFire)** que acaba de crear para aplicar esa regla de perfil a todo el tráfico que la política permite.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Habilite el cortafuegos para que reenvíe tráfico SSL descifrado para el análisis de WildFire.

STEP 6 | Revise e implemente las prácticas recomendadas de WildFire para asegurarse de aprovechar al máximo las prestaciones de detección y prevención de WildFire.

STEP 7 | Seleccione **Commit (Confirmar)** para confirmar sus cambios de configuración.

STEP 8 | Verifique que el cortafuegos esté reenviando archivos PE a la nube pública de WildFire.

Seleccione **Monitor (Supervisar)** > **Logs** > **WildFire Submissions (Envíos de WildFire)** para visualizar las entradas del log para los PE que el cortafuegos envió correctamente para el análisis de WildFire. La columna Verdict (Veredicto) muestra si WildFire detectó que el PE es malintencionado, grayware o benigno. (WildFire solo asigna el veredicto de phishing a enlaces de correo electrónico). La columna Action (Acción) indica si el cortafuegos permitió o bloqueó la muestra. La columna de gravedad indica la gravedad de amenaza que representa una muestra para una organización con los siguientes valores: crítica, alta, intermedia, baja, información.

STEP 9 | (Suscripción de prevención de amenazas únicamente) Si tiene una suscripción de prevención de amenazas, pero no tiene una suscripción a WildFire, puede recibir actualizaciones de firmas de WildFire cada 24 o 48 horas.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Compruebe que el cortafuegos esté configurado para descargar e instalar actualizaciones de antivirus.

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas para completar la implementación del cortafuegos

Ahora que ha integrado el cortafuegos en su red y ha habilitado las funciones de seguridad básicas, puede empezar a configurar funciones más avanzadas. Estos son algunos aspectos que debería considerar a continuación:

- Respete las prácticas recomendadas para proteger el acceso administrativo con el fin de garantizar la adecuada protección de las interfaces de gestión.
- Configure una base de regla de política de seguridad recomendada para habilitar de manera segura las aplicaciones y proteger su red contra ataques. Vaya a la página Prácticas recomendadas y seleccione la práctica recomendada de la política de seguridad para la implementación de cortafuegos.
- Configuración de la alta disponibilidad: la alta disponibilidad (high availability, HA) es una configuración en la que dos cortafuegos se colocan en un grupo y su configuración y tablas de sesión se sincronizan para prevenir el fallo de un único punto en su red. La conexión de heartbeat entre los peers del cortafuegos garantiza una conmutación por error sin problemas en el caso de que falle un peer. La configuración en un clúster de dos cortafuegos proporciona redundancia y le permite garantizar la continuidad de la actividad comercial.
- Habilitación de la identificación de usuarios (User-ID): User-ID es una función de los cortafuegos de nueva generación de Palo Alto Networks que le permite crear políticas y realizar informes basándose en usuarios y grupos en lugar de direcciones IP individuales.
- Habilitación del descifrado: los cortafuegos de Palo Alto Networks ofrecen la capacidad de descifrar e inspeccionar el tráfico para lograr visibilidad, control y seguridad detallada. Utilice el descifrado en un cortafuegos para evitar que entre en su red contenido malicioso o que salga de ella contenido confidencial, escondido como tráfico cifrado o de túnel.
- Realice las Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7.
- Uso compartido de la inteligencia de amenazas con Palo Alto Networks: permita que el cortafuegos recoja y envíe periódicamente información sobre las aplicaciones, las amenazas y la condición del dispositivo a Palo Alto Networks. La telemetría incluye opciones que permiten la supervisión de DNS pasivo y permiten que se ejecuten firmas de prueba experimentales en segundo plano, que no afectan sus reglas de políticas de seguridad, logs del cortafuegos o rendimiento del cortafuegos. Todos los clientes de Palo Alto Networks se benefician de la inteligencia que se recoge con la telemetría, que Palo Alto Networks utiliza para mejorar las capacidades de prevención de amenazas del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas para proteger el acceso administrativo

La protección de su red contra los ataques cibernéticos comienza con la implementación de un cortafuegos seguro. Si la red que utiliza para gestionar sus dispositivos IT críticos (que incluye cortafuegos de nueva generación de Palo Alto Networks y Panorama) no se protege adecuadamente, no podrá detectar ni defenderse de los exploits de vulnerabilidad que podrían conducir a una infiltración o una pérdida de datos confidenciales. El objetivo principal de la protección del acceso al cortafuegos es garantizar que, incluso aunque un atacante logra acceder a credenciales privilegiadas, usted pueda frustrar su capacidad de acceder y provocar daños. Respete estas pautas recomendadas para garantizar que protege el acceso administrativo a sus cortafuegos y otros dispositivos de seguridad de un modo que evite ataques eficaces.

- Aislamiento de la red de gestión
- Uso de rutas de servicio para acceder a servicios externos
- Restricción del acceso a la interfaz de gestión
- Gestión del acceso de administrador
- Creación de contraseñas de administrador seguras
- Búsqueda de todo el tráfico destinado a la interfaz de gestión
- Sustitución del certificado para el tráfico de gestión entrante
- Mantenimiento de las actualizaciones de contenido y software

Aislamiento de la red de gestión

Todos los cortafuegos de Palo Alto Networks incluyen un puerto de gestión (MGT) fuera de banda que puede usar para llevar a cabo las funciones de administración del cortafuegos. De manera alternativa, puede utilizar el puerto de MGT para la configuración inicial y configurar un puerto de datos para el acceso de gestión al cortafuegos. De cualquier manera, debido a que la interfaz de gestión proporciona acceso a su configuración de seguridad, debe respetar las siguientes precauciones para proteger el acceso a esta interfaz:



No permite el acceso a la interfaz de gestión desde internet o desde otras zonas no fiables dentro de sus límites de seguridad empresariales. Hágalo tanto si utiliza el puerto de gestión dedicado (dedicated management port, MGT) como si configura un puerto de datos como interfaz de gestión.

- ❑ Aísle la interfaz de gestión en una VLAn de gestión dedicada.
- ❑ Limite las direcciones IP de origen que se permiten en la red gestión a las de los dispositivos de gestión, como un servidor de salto o una pasarela de aplicaciones.
- ❑ Utilice un servidor de salto o una pasarela de aplicaciones (con grabación de pantalla) para brindar acceso seguro desde su red corporativa a su red de gestión dedicada, y solicite que los usuarios se autentiquen y cuenten con autorización para acceder a su red de gestión.
- ❑ Si no hay pasarela de aplicaciones, aplique una política de autenticación multifactor (multi-factor authentication, MFA) para exigir que los administradores se autentiquen antes de franquearles el acceso a la página de inicio de sesión de la interfaz web del cortafuegos o al mensaje para iniciar sesión de la CLI. Esto evita el acceso a la interfaz de gestión por medio de credenciales robadas o exploits de vulnerabilidad.

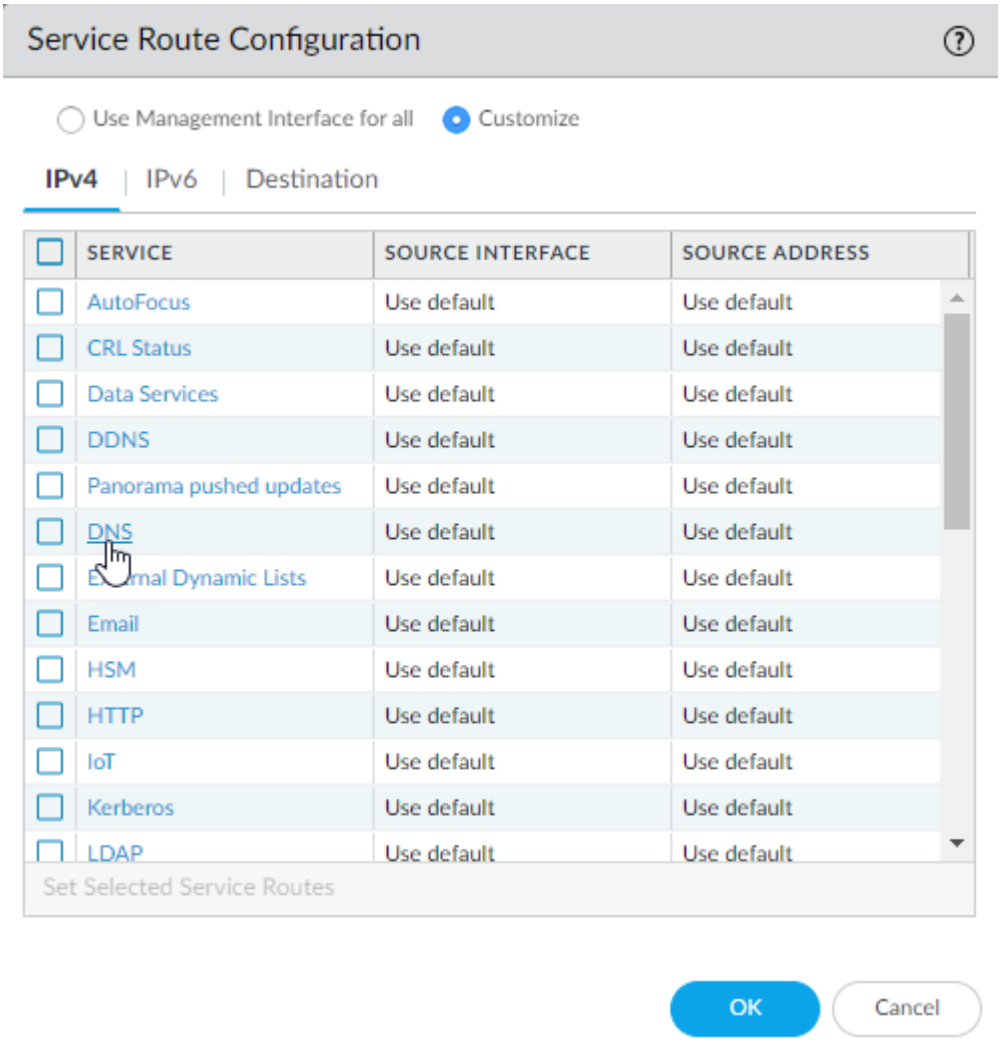
© 2020 Palo Alto Networks, Inc.

- Limite el acceso a los usuarios en los grupos de administración de seguridad, administración de red o usuarios de TI, según corresponda en su organización.
- Si debe permitir el acceso remoto a la red de gestión, requiera acceso por medio de un túnel de VPN utilizando GlobalProtect. Después de que los administradores establezcan un túnel de VPN a su zona de VPN correctamente, continuarán autenticándose en la red de gestión a través de su pasarela de aplicaciones.
- No utilice un perfil de gestión de interfaz que permita HTTP, HTTPS, Telnet o SSH en la interfaz donde ha configurado un portal o puerta de enlace de GlobalProtect porque esto permite el acceso a su interfaz de gestión desde internet. No emplee HTTP ni Telnet de forma interna porque esos protocolos realizan transmisiones de texto sin cifrar.
- Si utiliza una plantilla para implementar un cortafuegos serie VM que incluye un campo de restricción de acceso de gestión a direcciones IP específicas, asegúrese de brindar un bloque CIDR que corresponda a su red o sus direcciones IP de gestión dedicadas. Si es necesario, modifique el grupo de seguridad correspondiente para añadir hosts o redes adicionales tras el inicio de la plantilla. No haga que la red permitida sea más grande de lo necesario y nunca configure la fuente permitida como 0.0.0.0/0.

Uso de rutas de servicio para acceder a servicios externos

De manera predeterminada, el cortafuegos utiliza el puerto de gestión (Management, MGT) que está fuera de la red de gestión en redes potencialmente no fiables para acceder a los servicios, como servidores DNS, servidores NTP y servidores de autenticación, incluso los servicios que requieren acceso a internet, como los servicios de Palo Alto Networks y AutoFocus. Debido a que su interfaz de gestión (ya sea que se encuentre en un puerto de MGT o un puerto de datos) debe aislarse en la red de gestión, debe utilizar las rutas de servicio (**Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de ruta de servicio)**) para permitir el acceso a estos servicios. Cuando configura una ruta de servicio, el cortafuegos utiliza la interfaz y la dirección de origen especificadas para acceder a los servicios que necesita. Especifique la dirección IP/interfaz de origen de la ruta de servicio en una interfaz cuyo acceso de gestión (HTTPS o SSH) no esté habilitado.

© 2020 Palo Alto Networks, Inc.



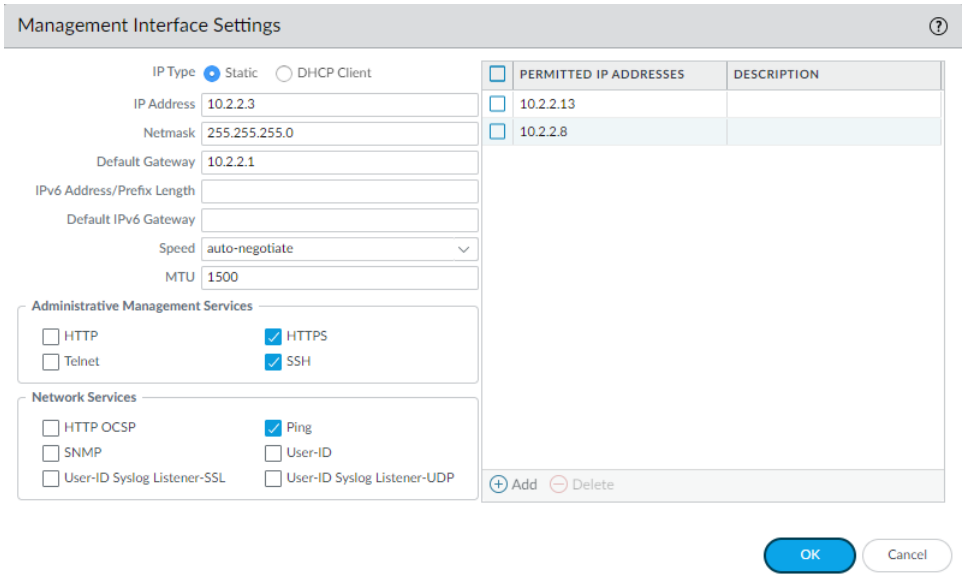
Restricción de acceso a la interfaz de gestión

- Restrinja las direcciones IP que pueden acceder a la interfaz de gestión.

  Incluso si su cortafuegos se encuentra en una red de gestión dedicada que únicamente se puede acceder por medio de un dispositivo en la misma VLAN, una pasarela de aplicaciones o un túnel de VPN, puede proteger el cortafuegos restringiendo las direcciones IP de origen que pueden acceder a la interfaz de gestión a las dirección IP de origen de los administradores. Limitar el acceso a la interfaz de gestión reduce la superficie de ataque ayudando a evitar el acceso de direcciones IP o subredes inesperadas, y evita el acceso con credenciales robadas.
- Restrinja los servicios disponibles en la interfaz de gestión.
  - No permita el acceso a través de Telnet y HTTP ya que estos servicios usan texto sin formato y no son tan seguros como otros servicios, y podrían comprometer las credenciales de administrador. En cambio, solicite a los administradores que accedan a las interfaces del cortafuegos a través de SSH o HTTPS.
  - Habilite ping si desea probar la conectividad a la interfaz, pero no habilite otros servicios en la interfaz de gestión.

© 2020 Palo Alto Networks, Inc.

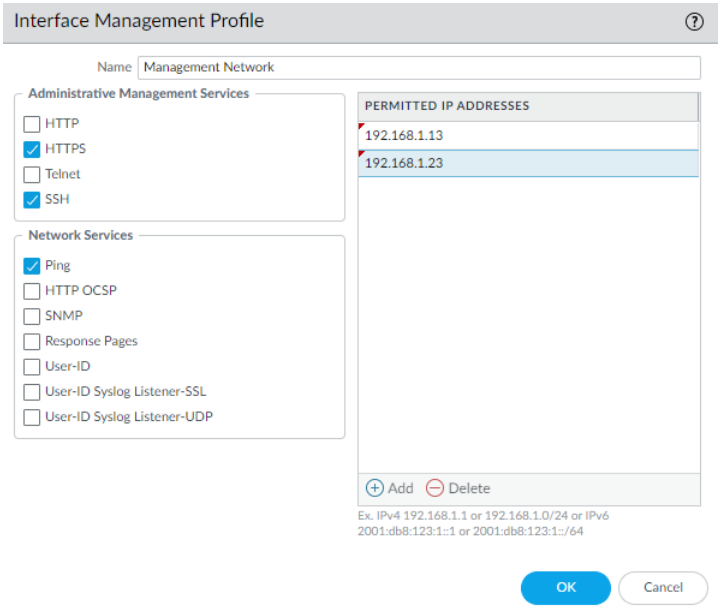
- La manera en la que configura estos ajustes depende de si utiliza el puerto de MGT o un puerto de datos para acceder a las interfaces de gestión del cortafuegos:
  - Si utiliza un puerto de MGT como su interfaz de gestión, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Interfaces (Interfaces)** y seleccione la interfaz de **Management (Gestión)** para configurar los ajustes que restringen el acceso a la interfaz de gestión y los servicios que permite la interfaz.



  - Si utiliza un puerto de datos como interfaz de gestión, tras configurar la interfaz, seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaces)** y haga clic en **Add (Añadir)** para añadir un perfil de gestión de interfaces que restrinja el acceso a dicha interfaz y a los servicios que permite.

    No adjunte un perfil de gestión de interfaz que permita Telnet, SSH, HTTP o HTTPS a una interfaz en la que haya configurado un portal o puerta de enlace de GlobalProtect debido a que esto expondrá la interfaz de gestión a internet. No emplee HTTP ni Telnet para ningún perfil de gestión de interfaces porque esos protocolos realizan transmisiones de texto sin cifrar.

© 2020 Palo Alto Networks, Inc.



Gestión del acceso de administrador

- El viene preconfigurado con una cuenta administrativa predeterminada (admin), que proporciona un acceso completo de lectura-escritura (también conocido como acceso de superusuario) al cortafuegos. Debe cambiar la contraseña de la cuenta de administrador predeterminada (**Device (Dispositivo)** > **Administrators (Administradores)** > **admin (administración)**) de inmediato tras la configuración inicial.

  Si los requisitos de cumplimiento, auditoría o seguridad exigen eliminar la cuenta administrativa predeterminada de los dispositivos, hágalo después de crear al menos otra cuenta administrativa de superusuario; no se puede eliminar hasta que configure otra cuenta de ese tipo en el dispositivo.
- Realice la Configuración de una cuenta administrativa de cortafuegos para cada persona que necesite acceder a las funciones de administración o creación de informes del cortafuegos. Esto le permite proteger mejor el cortafuegos contra la configuración (o modificación) no autorizadas y habilitar la creación de logs de las acciones de cada uno de los administradores.
- Asigne cada cuenta de administrador a un perfil de función de administrador que limite los privilegios de gestión únicamente a las funciones que necesita el administrador individual.
- En el caso de los administradores con privilegios de modificación, exija la MFA mediante autenticación y autorización externas con RADIUS o SAML. Consulte Configuración de la autenticación local o externa para los administradores del cortafuegos para obtener información detallada sobre la configuración de la autenticación externa con MFA.

  Si posee una infraestructura de autenticación sólida que utiliza tarjetas inteligentes, implemente la Configuración de una autenticación de administrador basada en certificados en la interfaz web y la Configuración de la autenticación de administrador basada en claves de SSH para el CLI.

  Si están disponibles, utilice soluciones de gestión de cuenta con privilegios (privileged account management, PAM) o gestión de identidad con privilegios (privileged identity management, PIM) para proteger las credenciales de administrador de manera externa.
- Supervise los logs de sistema para identificar la actividad anormal de la cuenta en cualquiera de las cuentas de administrador. Por ejemplo, si los logs muestran demasiados intentos de inicio de sesión

© 2020 Palo Alto Networks, Inc.

o inicios de sesión repetidos en determinados momentos del día, es posible que esto indique que una cuenta administrativa se ha visto comprometida. Además, proporcione información a todos los administradores sobre cómo implementar el Uso de los indicadores de actividad de inicio de sesión de administrador para detectar el uso indebido de la cuenta.

Creación de contraseñas de administrador seguras

Configure una política de contraseña estricta, que incluya el requisito de cambiar con frecuencia la contraseña (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Minimum Password Complexity (Complejidad mínima de contraseña)**).

Usted es el responsable de evaluar los requisitos de contraseña apropiados para su empresa; sin embargo, las características que se muestran a continuación son las recomendables para crear contraseñas seguras. Las contraseñas deben tener las siguientes características:

- Tener un mínimo de ocho caracteres.
- No estar basadas en una única palabra del diccionario.
- No incluir palabras específicas de un contexto (por ejemplo, el nombre de un sitio web).
- No incluir un nombre de usuario o derivados de él (por ejemplo, @dmin, Johnny).
- No tener caracteres secuenciales o repetitivos (por ejemplo, aaaaaa, 1234abcd).
- Deben incluir caracteres en mayúsculas y minúsculas, números y caracteres especiales (incluidos los espacios).

Una forma de crear una contraseña segura es crear una frase de contraseña larga en lugar de una contraseña compleja. Los estándares del sector recomiendan crear frases de contraseña largas y únicas que recuerde fácilmente (con los caracteres que desee, incluidas las palabras del diccionario) en lugar de crear contraseñas complicadas y complejas que sean fáciles de olvidar. Se cree que las contraseñas más largas con un mínimo de 15 caracteres compensan el uso de palabras del diccionario. Intente crear una frase de contraseña basada en frases largas y familiares que solo usted conozca o junte al menos cuatro palabras.

Para obtener más información sobre cómo determinar los requisitos de contraseña apropiados para su empresa, recomendamos los siguientes recursos:

- NIST SP 800-63B, Digital Identity Guidelines (NIST SP 800-63B, Directrices de identidad digital)
- NIST, Easy Ways to Build a Better P@$5w0rd (NIST, Formas sencillas de crear una mejor C@Nt2SeÑa)

Búsqueda de todo el tráfico destinado a la interfaz de gestión



Debido a que la política de seguridad y la política de descifrado no evalúan el tráfico del plano de gestión, no puede buscar amenazas directamente en el puerto de MGT. Si utiliza un puerto de MGT como su interfaz de gestión, considere permitir el enrutamiento del tráfico destinado al puerto de MGT a través de un puerto de datos o a través de otro cortafuegos, de modo que pueda aplicar estas comprobaciones de seguridad importantes en su tráfico de gestión.

- Cree reglas en la política de seguridad que permitan el acceso a las interfaces de gestión del cortafuegos y Panorama (interfaz web o CLI). La manera en la que define la política depende de si utiliza o no una pasarela de aplicaciones para permitir el acceso a la red de gestión.
  - Si no utiliza una pasarela de aplicaciones para aislar su red de gestión, cree una regla en la política de seguridad para permitir el acceso desde la zona de usuarios a la zona de infraestructura de TI. Esta regla de la política de seguridad debe ser muy detallada y debe especificar la zona de origen la dirección IP de origen (si está disponible) y el grupo de usuarios de origen del usuario que

© 2020 Palo Alto Networks, Inc.

intenta acceder a la interfaz de gestión, además de la zona de destino, la dirección IP del dispositivo (cortafuegos o Panorama) y la App-ID para especificar la aplicación de gestión específica (interfaz web o CLI) que se ejecuta en el puerto predeterminado de la aplicación. Por ejemplo, usaría la App-ID panos-web-interface para permitir el acceso a la interfaz web y la App-ID ssh para permitir el acceso a la CLI. Además, debe adjuntar un perfil de protección frente a vulnerabilidades a la regla, como se describe en la siguiente sección.

El siguiente ejemplo de regla permite acceso desde la zona de usuarios directamente a la zona de infraestructura de TI y restringe el acceso a usuarios en el grupo de administradores de TI que intenten acceder a la dirección IP de la interfaz de gestión para acceder a la aplicación panos-web-interface únicamente en el puerto application-default (Valor predeterminado de aplicación):

	Source		Destination				
NAME	ZONE	USER	ZONE	APPLICATION	SERVICE	ACTION	PROFILE
FW-mgt	Users	IT-admins	IT-infrastruc...	panos-web-interface ssh	application-default	Allow	

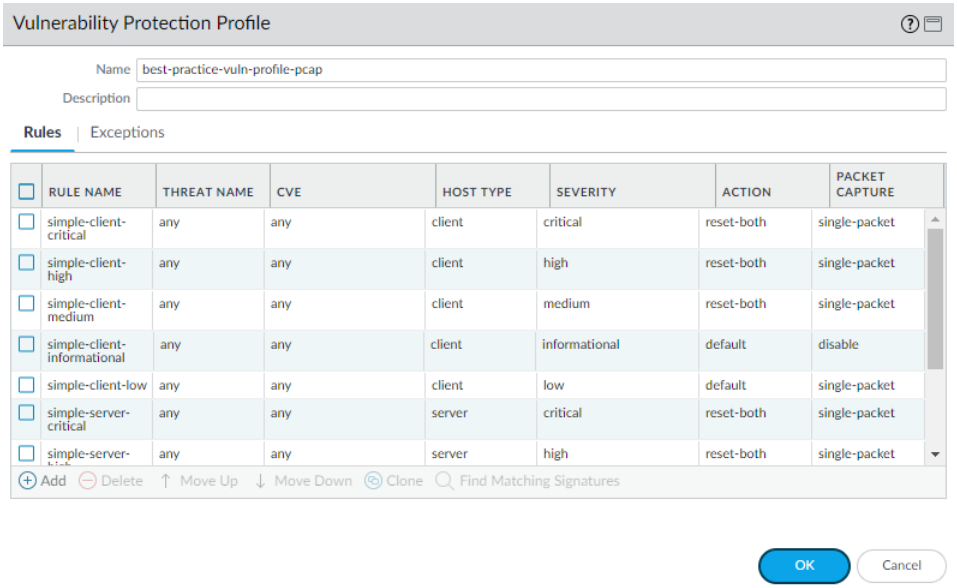
- Si utiliza una pasarela de aplicaciones para permitir el acceso a su red de gestión, necesita dos reglas de la política de seguridad: una regla que permita el acceso desde la zona de usuarios a la zona de la pasarela de aplicaciones, y una segunda regla que permita el acceso desde la zona de la pasarela de aplicaciones a la zona de infraestructura de TI. Nuevamente, ambas reglas de la política de seguridad deben ser lo más detalladas posible e incluir la zona de origen, la dirección (si está disponible), el usuario y la zona de destino y la dirección, y la App-ID. Tenga en cuenta que si utiliza una pasarela de aplicaciones, por lo general, la dirección IP del usuario es la dirección IP de la pasarela de aplicaciones, de modo que no puede identificar el ID de usuario del administrador a menos que utilice el agente de servidor de terminal en la pasarela de aplicaciones para identificar a los usuarios individuales. En este caso, también debe adjuntar un perfil de protección frente a vulnerabilidades a ambas reglas, como se describe en la siguiente sección.

  En los ejemplos de reglas a continuación, la primera regla permite el acceso desde la zona de usuarios a la zona de la pasarela de aplicaciones a los usuarios en el grupo de administradores de TI que intentan acceder a la dirección IP del servidor de la pasarela de aplicaciones con SSH o RDP. La segunda regla permite el acceso a los usuarios desde la zona de la pasarela de aplicaciones a la zona de infraestructura de TI que intentan acceder a la aplicación panos-web-interface en el puerto predeterminado del cortafuegos con la dirección de destino especificada.

	Source		Destination				
NAME	ZONE	USER	ZONE	APPLICATION	SERVICE	ACTION	PROFILE
Bastion-host-access	Users	IT-admins	Bastion-host	ms-rdp ssh	application-default	Allow	
FW-mgt	Bastion-host	IT-admins	IT-infrastruc...	panos-web-interface ssh	application-default	Allow	

- Vincule un perfil recomendado de protección frente a vulnerabilidades a las reglas de la política de seguridad que permiten el acceso a la red de gestión a fin de protegerla contra los desbordamientos de búfer, la ejecución de código ilegal y otros intentos de aprovechar vulnerabilidades de los clientes y de los servidores. Para crear un perfil con el objetivo de proteger su interfaz de gestión, clone el perfil estricto y habilite la captura de paquetes extendida que le permitirá realizar un seguimiento del origen de los posibles ataques.

© 2020 Palo Alto Networks, Inc.



- Configure la inspección de entrada SSL o el proxy SSL de reenvío para el tráfico con destino u origen en la interfaz de gestión; eso garantiza que se descifre y se busquen amenazas en él. Vincule un perfil recomendado de descifrado a la regla de la política de descifrado para garantizar que se bloqueen las versiones de SSL o TLS vulnerables, como TLS 1.0 y SSL v. 3, y que se rechacen las sesiones que utilicen algoritmos poco seguros de cifrado (como RC4 y 3DES) y de autenticación (como MD5 y SHA1).

Sustitución del certificado para el tráfico de gestión entrante

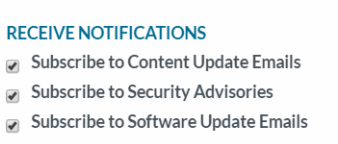
Por defecto, el cortafuegos se envía con un certificado por defecto que habilita el acceso HTTPS a la interfaz web en la interfaz de gestión (MGT) o en cualquier otra interfaz que admita el tráfico de gestión HTTPS. Para mejorar la seguridad del tráfico de gestión entrante, reemplace el certificado por defecto por un nuevo certificado emitido específicamente para su organización. Utilice certificados firmados por la CA de su empresa, de modo que los usuarios no ignoren las advertencias del certificado. Asimismo, en el perfil de SSL o TLS, configure **Min version (Versión mínima)** en **TLSv1.2 (TLS v. 1.2)** para utilizar el protocolo más seguro y configure **Max version (Versión máxima)** en **Max (Máxima)** para seguir usando el protocolo más seguro a medida que aparezcan versiones reforzadas.

Mantenimiento de las actualizaciones de contenido y software

Mantener al día las actualizaciones de contenido y software permite garantizar que siempre esté protegido con los parches de seguridad y las actualizaciones de prevención de amenazas más recientes.

- Para garantizar que siempre reciba alertas sobre las actualizaciones y las recomendaciones de seguridad más recientes, vaya al portal de asistencia técnica de Palo Alto Networks, seleccione **Edit Profile (Editar perfil)**, y seleccione **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**, **Subscribe to Security Advisories (Suscribirse para recibir recomendaciones de seguridad)** y **Subscribe to Software Update Emails (Suscribirse para recibir actualizaciones de software por correo electrónico)**. Asegúrese de hacer clic en **Save Edits (Guardar editados)**.

© 2020 Palo Alto Networks, Inc.



- Siga el procedimiento Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas para actualizar a la última versión de contenido.
- Antes de realizar una actualización de PAN-OS, lea las notas de la versión más recientes.

Suscripciones

Obtenga información sobre todas las suscripciones y todos los servicios que funcionan con el cortafuegos. Para empezar, active las licencias de suscripción:

- Suscripciones disponibles para los cortafuegos
- Activación de licencias de suscripción
- ¿Qué ocurre cuando la licencia caduca?
- Logs mejorados de aplicaciones para servicios en la nube de Palo Alto Networks



Algunos de los servicios en la nube, como Cortex XDR™, no se integran directamente con el cortafuegos, sino que dependen de los datos almacenados en Cortex Data Lake para tener visibilidad sobre la actividad de la red. La creación de logs de aplicaciones mejorada es una función que incorpora una suscripción a Cortex Data Lake: permite que el cortafuegos recopile datos específicamente para que Cortex XDR los use para detectar actividades anómalas en la red. Se recomienda activar la creación de logs de aplicaciones mejorada en Cortex XDR.

© 2020 Palo Alto Networks, Inc.

Suscripciones disponibles para los cortafuegos

Palo Alto Networks ofrece suscripciones para desbloquear algunas funciones del cortafuegos o para habilitar este con el fin de aprovechar el servicio prestado en la nube de Palo Alto Networks (o ambos). A continuación se indican los servicios o las funciones que exigen la suscripción para funcionar con el cortafuegos. Para habilitar una suscripción, primero debe realizar el procedimiento Activación de licencias de suscripción. Cuando los servicios de suscripción están activos, la mayoría puede recurrir a las Actualizaciones dinámicas de contenido para que el cortafuegos disponga siempre de las funciones nuevas y actualizadas.

Suscripciones disponibles para los cortafuegos	
IoT Security (Seguridad de IoT)	La solución de seguridad de IoT funciona con cortafuegos de nueva generación para detectar y mantener de forma dinámica un inventario en tiempo real de los dispositivos de IoT en su red. A través de la inteligencia artificial y los algoritmos de aprendizaje automático, la solución de seguridad de IoT logra un alto nivel de precisión, incluso mediante la clasificación de los tipos de dispositivos de IoT encontrados por primera vez. Además, puesto que es dinámico, su inventario de dispositivos de IoT siempre está actualizado. La seguridad de IoT también proporciona la generación automática de recomendaciones de políticas para controlar el tráfico de dispositivos de IoT, así como la creación automática de atributos de dispositivos de IoT para su uso en políticas de cortafuegos. • Aspectos básicos de la seguridad de IoT
SD-WAN	Proporciona una selección de rutas inteligentes y dinámicas sobre la plataforma de seguridad líder en el sector que el software PAN-OS ya ofrece. Con la gestión de Panorama, la implementación de SD-WAN incluye lo siguiente: • Gestión centralizada de la configuración • Creación automática de la topología de VPN • Distribución de tráfico • Supervisión y solución de problemas • Introducción a SD-WAN
Threat Prevention	Threat Prevention ofrece lo siguiente: • Protección contra virus, spyware (comando y control) y frente a vulnerabilidades. • Listas dinámicas externas integradas para proteger la red de hosts malintencionados. • Capacidad para identificar los hosts infectados que intentan conectarse a dominios malintencionados. • Aspectos básicos de Threat Prevention
DNS Security	La consulta en DNS Security aporta funciones mejoradas de sinkholing de DNS. Este servicio extensible en la nube puede generar firmas de DNS basándose en el análisis predictivo avanzado y el aprendizaje automático. Además, franquea el pleno acceso a la

© 2020 Palo Alto Networks, Inc.

Suscripciones disponibles para los cortafuegos	
	inteligencia contra amenazas basada en DNS que genera y amplía de forma constante Palo Alto Networks. Para configurar DNS Security, primero debe adquirir e instalar la licencia de Threat Prevention. • Aspectos básicos de DNS Security
Filtrado de URLs	No solo permite controlar el acceso web, sino también la interacción de los usuarios con el contenido en línea en función de categorías de URL dinámicas. También puede evitar el robo de credenciales controlando los sitios a los que los usuarios pueden enviar credenciales corporativas. Para configurar el filtrado de URL, se debe adquirir e instalar una suscripción a un base de datos de filtrado de URL compatible, PAN-DB. Con PAN-DB, puede configurar el acceso a la nube pública de PAN-DB o a la nube privada de PAN-DB. • Aspectos básicos de URL Filtering
WildFire	Aunque la licencia de Threat Prevention incluye compatibilidad básica con WildFire®, el servicio de suscripción a WildFire ofrece servicios mejorados a las organizaciones que requieren cobertura inmediata contra amenazas, actualizaciones frecuentes de firmas de WildFire y reenvío avanzado de tipos de archivos (APK, PDF, Microsoft Office y Java Applet), además de capacidad para cargar archivos usando la API de WildFire. También se requiere una suscripción a WildFire si sus cortafuegos van a reenviar archivos a un dispositivo WF-500 en las instalaciones. • Comenzar con WildFire
AutoFocus	Proporciona un análisis gráfico de los logs de tráfico del cortafuegos e identifica posibles riesgos para la red usando inteligencia contra amenazas del portal de AutoFocus. Con una licencia activa, también puede abrir una búsqueda en AutoFocus en función de los logs registrados en el cortafuegos. • Aspectos básicos de AutoFocus
Cortex Data Lake	Ofrece agregación y almacenamiento centralizados y basados en la nube de los logs. Cortex Data Lake es necesario o muy recomendable para admitir otros servicios proporcionados en la nube, incluidos Cortex XDR, IoT Security y Prisma Access, y el servicio de administración de Traps. • Introducción a Cortex Data Lake
GlobalProtect	Ofrece soluciones de movilidad o funciones de VPN a gran escala. De forma predeterminada, puede implementar portales y gateways de GlobalProtect (sin comprobaciones de HIP) sin licencia. Si desea usar características de GlobalProtect avanzadas (comprobaciones HIP y actualizaciones de contenido relacionadas, la aplicación móvil de GlobalProtect, conexiones IPv6 o VPN sin cliente de GlobalProtect), necesitará una licencia (suscripción) GlobalProtect para cada puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Suscripciones disponibles para los cortafuegos	
	• Aspectos básicos de GlobalProtect
Virtual Systems	Esta licencia perpetua es necesaria para permitir el uso de varios sistemas virtuales en los cortafuegos PA-3200 Series. También debe adquirir la licencia de Virtual Systems si desea utilizar más sistemas virtuales de los permitidos de manera predeterminada con los cortafuegos PA-5200 Series y PA-7000 Series (el número básico varía según la plataforma). Los cortafuegos PA-800 Series, PA-220 y VM-Series no admiten sistemas virtuales. • Aspectos básicos de Virtual Systems
Enterprise Data Loss Prevention (DLP, Prevención de pérdida de datos empresariales)	Proporciona protección basada en la nube contra el acceso no autorizado, el uso incorrecto, la extracción y el intercambio de información confidencial. Enterprise DLP proporciona un motor único para la detección precisa y la aplicación de políticas coherentes para datos confidenciales en reposo y en movimiento mediante la clasificación de datos basada en aprendizaje automático, cientos de patrones de datos que utilizan expresiones regulares o palabras clave y perfiles de datos que utilizan lógica booleana para buscar tipos colectivos de datos. • Introducción a la prevención de pérdida de datos empresariales

© 2020 Palo Alto Networks, Inc.

Activación de licencias de suscripción

Siga estos pasos para activar una licencia nueva en el cortafuegos.

Para que funcionen algunas características de descifrado, como el reflejo de descifrado y el agente de descifrado, es preciso que active la licencia gratuita correspondiente. Para ello, siga los pasos del procedimiento Activación de las licencias gratuitas para usar las funciones de descifrado.

STEP 1 | Encuentre los códigos de activación de las licencias que ha adquirido.

Al comprar las suscripciones debió recibir un mensaje de correo electrónico del servicio de atención al cliente de Palo Alto Networks con los códigos de activación asociados a cada suscripción. Si no encuentra este mensaje de correo electrónico, póngase en contacto con el Servicio de atención al cliente para obtener sus códigos de activación antes de continuar.

STEP 2 | Active su licencia de asistencia técnica.

No podrá actualizar su software PAN-OS si no tiene una licencia de asistencia técnica válida.

1. Inicie sesión en la interfaz web y luego seleccione **Device (Dispositivo)** > **Support (Asistencia técnica)**.
2. Haga clic en **Activate support using authorization code**.
3. Introduzca el **Authorization Code (Código de autorización)** y, a continuación, haga clic en **OK (Aceptar)**.

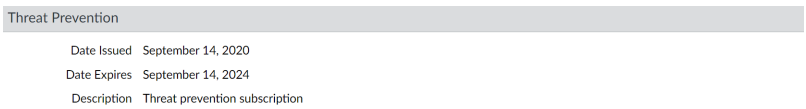
STEP 3 | Active todas las licencias que ha adquirido.

Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y luego active sus licencias y suscripciones de alguna de las siguientes maneras:

- **Retrieve license keys from license server (Recuperar de claves de licencia del servidor de licencias)**: use esta opción si ha activado su licencia en el portal del Servicio de atención al cliente.
- **Activación de la función usando un código de autorización**: Use esta opción para habilitar las suscripciones adquiridas con un código de autorización para licencias que no han sido previamente activadas en el portal de asistencia técnica. Cuando se le indique, introduzca el **Authorization Code (Código de autorización)** y haga clic en **OK (Aceptar)**.
- **Manually upload license key (Cargar manualmente la clave de licencia)**: use esta opción si su cortafuegos no tiene conectividad con el portal de asistencia técnica de Palo Alto Networks. En este caso, debe descargar una clave de licencia del sitio de asistencia técnica a través de un ordenador conectado a Internet y después cargarla en el cortafuegos.

STEP 4 | Compruebe que la licencia esté activada correctamente.

En la página **Device (Dispositivo)** > **Licenses (Licencias)** compruebe que la licencia esté activada correctamente. Por ejemplo, tras activar la licencia de WildFire, debería ver que la licencia es válida:



STEP 5 | (Solo suscripciones a WildFire) Realice una confirmación para completar la activación de la suscripción a WildFire.

Tras activar una suscripción a WildFire, se necesita una confirmación para que el cortafuegos empiece a reenviar tipos de archivos avanzados. Debe elegir una de las siguientes opciones:

- Compile cualquier cambio pendiente.

© 2020 Palo Alto Networks, Inc.

- Compruebe si las Reglas de perfil de análisis de WildFire incluyen los tipos de archivo avanzados que son compatibles ahora con la suscripción a WildFire. Si no es necesario ningún cambio en las reglas, modifique mínimamente una descripción de reglas y realice la compilación.

© 2020 Palo Alto Networks, Inc.

¿Qué ocurre cuando la licencia caduca?

Las subscripciones de Palo Alto Networks proporcionan al cortafuegos una funcionalidad adicional o acceso a un servicio proporcionado en la nube de Palo Alto Networks. Cuando la licencia caduca, algunas suscripciones siguen funcionando con una capacidad limitada y otras dejan de funcionar por completo. Aquí puede conocer qué sucede cuando caduca cada suscripción.

Suscripción	Comportamiento de caducidad
Threat Prevention	Aparecen alertas en el log del sistema que indican que la licencia ha caducado. **Puede seguir realizando las siguientes acciones:** • Utilice firmas que se instalaron en el momento en que caducó la licencia, a no ser que instale una nueva actualización de contenido solo para aplicaciones, ya sea manualmente o como parte de una programación automática. Si lo hace, la actualización eliminará sus firmas de amenazas existentes y ya no recibirá protección contra ellas. • Utilizar y modificar App-ID™ personalizado y firmas de amenazas. **Ya no puede realizar las siguientes acciones:** • Instalar nuevas firmas. • Revertir las firmas a versiones anteriores.
DNS Security	**Puede seguir realizando las siguientes acciones:** • Usar firmas DNS locales si tiene una licencia de Threat Prevention activa. **Ya no puede realizar las siguientes acciones:** • Obtener nuevas firmas DNS.
Filtrado de URLs	**Puede seguir realizando las siguientes acciones:** • Aplicar la política con categorías de URL personalizadas. • Aplicar la política con categorías de PAN-DB que estaban en su caché local cuando caducó la licencia. **Ya no puede realizar las siguientes acciones:** • Obtener actualizaciones en las categorías de PAN-DB almacenadas en caché. • Obtener categorías de PAN-DB de URL no almacenadas en caché.
WildFire	**Puede seguir realizando las siguientes acciones:** • Reenviar PE para el análisis. • Obtener actualizaciones de firmas cada 24-48 horas si dispone de una suscripción a Threat Prevention activa. **Ya no puede realizar las siguientes acciones:**

© 2020 Palo Alto Networks, Inc.

Suscripción	Comportamiento de caducidad
	• Proporcionar actualizaciones de cinco minutos a través de las nubes pública y privada de WildFire. • Reenviar tipos de archivos avanzados como APK, archivos Flash, PDF, archivos de Microsoft Office, applets Java, archivos Java (.jar y .class) y enlaces de correo electrónico HTTP/HTTPS contenidos en mensajes de correo electrónico SMTP y POP3. • Usar la API de WildFire. • Utilice un dispositivo WildFire para alojar una nube privada de WildFire o una nube híbrida de WildFire.
AutoFocus	**Puede seguir realizando las siguientes acciones:** • Usar la lista dinámica externa con datos de AutoFocus para un periodo de gracia de tres meses. **Ya no puede realizar las siguientes acciones:** • Acceder al portal de AutoFocus. • Ver el resumen de inteligencia de AutoFocus para el log de supervisión o los artefactos de ACC.
Cortex Data Lake	**Puede seguir realizando las siguientes acciones:** • Almacenar datos de logs durante un periodo de gracia de 30 días. Después de ese periodo, se eliminarán. • Reenviar logs a Cortex Data Lake hasta que acabe el periodo de gracia de 30 días.
GlobalProtect	**Puede seguir realizando las siguientes acciones:** • Utilice la aplicación los endpoints que ejecutan Windows o macOS • Configurar una o varias puertas de enlace internas o externas. **Ya no puede realizar las siguientes acciones:** • Acceder a la aplicación Linux OS ni a la aplicación móvil para iOS, Android, Chrome OS y Windows 10 UWP. • Usar las puertas de enlace externas de IPv6. • Ejecutar comprobaciones HIP. • Usar VPN sin cliente. • Habilitar la división de túnel.
VM-SERIES	**Puede seguir realizando las siguientes acciones:** • Configurar y usar los cortafuegos que implementó cuando caducó la licencia.
Soporte	**Ya no puede realizar las siguientes acciones:** • Recibir actualizaciones de software. • Descargar imágenes de VM. • Beneficiarse del soporte técnico.

© 2020 Palo Alto Networks, Inc.

Logs mejorados de aplicaciones para servicios en la nube de Palo Alto Networks

El cortafuegos puede recopilar datos que aumenten la visibilidad sobre la actividad en la red de las aplicaciones y servicios de Palo Alto Networks, como Cortex XDR. Los logs mejorados de aplicaciones se diseñan estrictamente para que los usen y procesen las aplicaciones y servicios de Palo Alto Networks; no se pueden ver en el cortafuegos ni en Panorama. Solo los cortafuegos que envíen logs a Cortex Data Lake podrán generar logs de aplicaciones mejorados.

Algunos ejemplos de los tipos de datos que recopilan los logs mejorados de aplicaciones son registros de consultas DNS, el campo User Agent (Agente de usuario) del encabezado HTTP que especifica la herramienta o el navegador web empleados para acceder a una URL, e información sobre la asignación DHCP automática de direcciones IP. A partir de la información de DHCP, por ejemplo, Cortex XDR™ puede emitir alertas sobre actividad inusual según el nombre de host en lugar de la dirección IP. Eso permite a los analistas de seguridad que usan Cortex XDR evaluar de manera eficaz si la actividad del usuario se corresponde con las atribuciones de su función o no para tomar medidas con mayor rapidez a fin de detener la actividad.

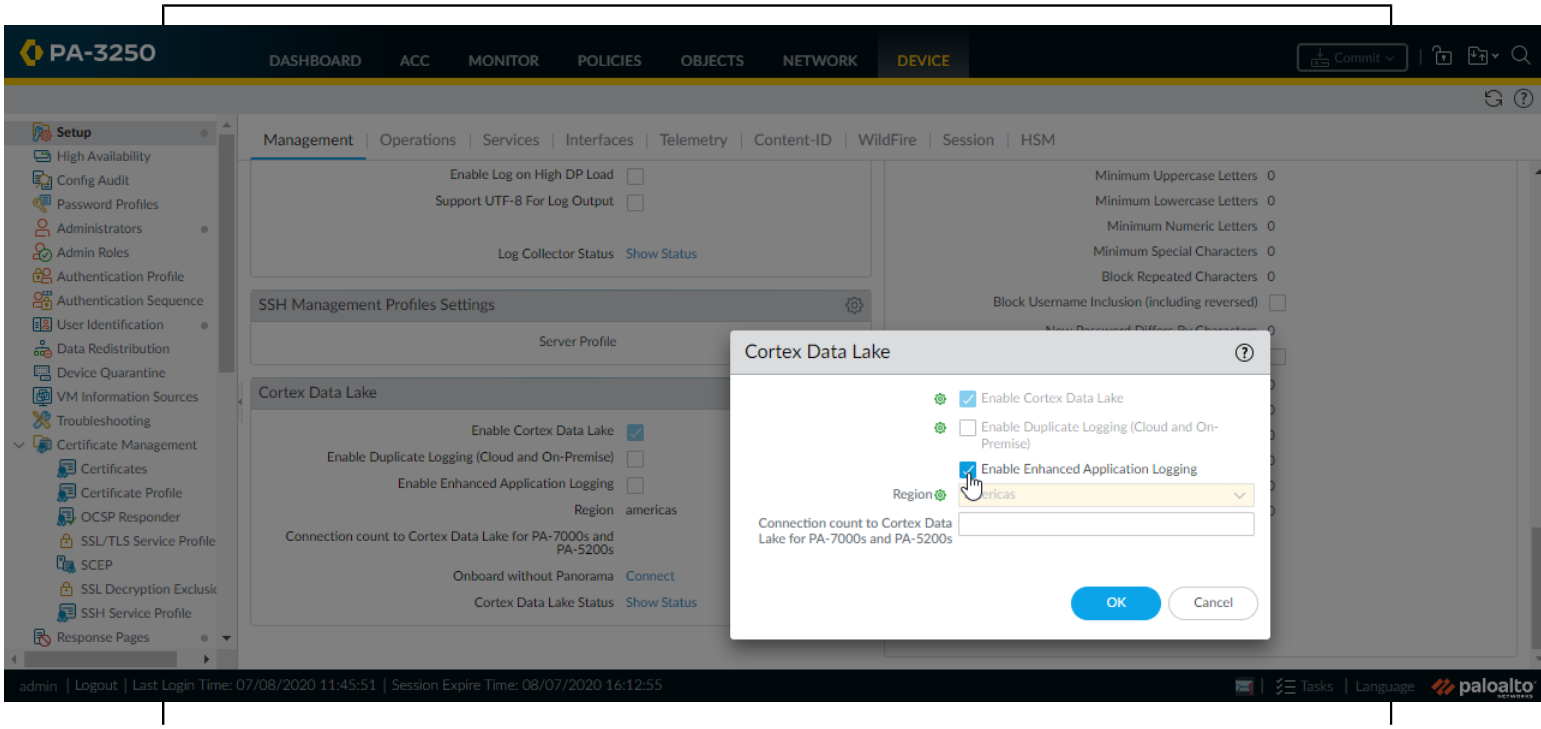
Para aprovechar el conjunto más completo de logs mejorados de aplicaciones, debe habilitar User-ID. Las implementaciones del agente de User-ID basado en Windows y el agente de User-ID integrado de PAN-OS recopilan datos que no se reflejan en los logs de User-ID del cortafuegos, pero resultan útiles para asociar la actividad en la red a usuarios concretos.

Para comenzar el reenvío de logs mejorados de aplicaciones a Cortex Data Lake, active la creación de logs mejorados de aplicación globalmente y habilítela en una función de una regla de seguridad (utilizando un perfil de reenvío de logs). Esta configuración global es necesaria y captura datos de tráfico que no se basa en las sesiones (solicitudes ARP por ejemplo). La configuración por la regla de la política se recomienda encarecidamente; la mayoría de los logs mejorados de aplicaciones se recopilan en el tráfico basado en las sesiones que aplican las reglas de su política de seguridad.

STEP 1 | La creación de logs de aplicaciones mejorada requiere una suscripción a Cortex Data Lake y también se recomienda User-ID. Estos son los pasos necesarios para comenzar con Cortex Data Lake y habilitar User-ID.

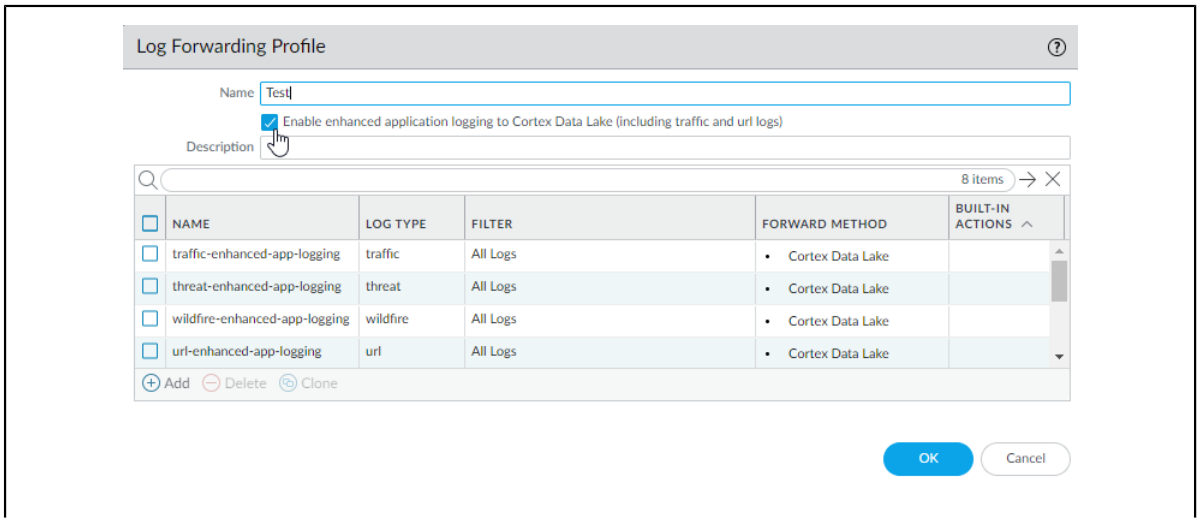
STEP 2 | Para **Enable Enhanced Application Logging (Habilitar creación mejorada de logs de aplicación)** en el cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Cortex Data Lake** y edite los ajustes de Cortex Data Lake.

© 2020 Palo Alto Networks, Inc.



STEP 3 | Habilite la creación de logs mejorados de aplicaciones para las reglas de la política de seguridad que controlan el tráfico para el que desea visibilidad extendida.

1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**, haga clic en **Add (Añadir)** para añadir un perfil de reenvío de logs o modifique uno existente.
2. Actualice el perfil para **habilitar el log mejorado de aplicaciones en Cortex Data Lake (incluidos el tráfico y los logs de URL)**.



Tenga en cuenta que cuando habilita la creación de logs mejorados de aplicaciones en un perfil de reenvío de logs, las listas de coincidencia que especifican los tipos de logs necesarios para la creación de logs mejorados de aplicaciones se añaden automáticamente al perfil.

3. Haga clic en **OK (Aceptar)** para guardar el perfil y actualizar los perfiles necesarios.
4. Asegúrese de que el perfil de reenvío de logs que actualizó esté adjunto a una regla de la política de seguridad para activar la generación y el reenvío de logs del tráfico que coincide con la regla.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** para ver los perfiles adjuntos a cada regla de la política de seguridad.
2. Para actualizar el perfil de reenvío de logs adjunto a una regla, haga clic en **Add (Añadir)** para añadir una regla o edite una existente, y seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Actions (Acciones)** > **Log Forwarding (Reenvío de logs)**

Actualizaciones de software y contenido

PAN-OS es el software que ejecuta todos los cortafuegos de nueva generación de Palo Alto Networks. Además, Palo Alto Networks publica a menudo actualizaciones para dotar los cortafuegos de las últimas funciones de seguridad. Los cortafuegos pueden aplicar políticas basadas en las firmas de aplicaciones, amenazas, etc. que aportan las actualizaciones de contenido, sin que el usuario deba actualizar su configuración.

Después de descargar e instalar correctamente una actualización de software PAN-OS en el cortafuegos físico, la actualización de software se valida después de que el cortafuegos físico se reinicie como parte del proceso de instalación del software para garantizar la integridad del software PAN-OS. Esto garantiza que la nueva actualización de software en ejecución sea buena y que el cortafuegos no se vea comprometido debido a la explotación remota o física.

- Actualizaciones del software PAN-OS
- Actualizaciones dinámicas de contenido
- Instalación de actualizaciones de contenido
- Actualización de contenido de aplicaciones y amenazas
- Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas
- Infraestructura de red de entrega de contenido

© 2020 Palo Alto Networks, Inc.

Actualizaciones del software PAN-OS

PAN-OS es el software que ejecuta todos los cortafuegos de nueva generación de Palo Alto Networks. La versión del software PAN-OS que ejecuta el cortafuegos se muestra en su pantalla **Dashboard (Panel)**.

Puede buscar las nuevas versiones de PAN-OS directamente en el cortafuegos o bien en el portal de atención al cliente de Palo Alto Networks. Para actualizar el cortafuegos a la última versión de PAN-OS:

STEP 1 | Compruebe las novedades disponibles en las notas de la versión de PAN-OS más recientes. Lea también el documento de consideraciones sobre el cambio a versiones anteriores o posteriores de PAN-OS para conocer todas las modificaciones que pueden aparecer con la versión.

STEP 2 | Compruebe si hay versiones de PAN-OS nuevas:

- **En el cortafuegos**, seleccione **Device (Dispositivo)** > **Software** y haga clic en **Check Now (Buscar ahora)** para que busque versiones nuevas de PAN-OS en el servidor de actualizaciones de Palo Alto Networks.
- **En el portal de atención al cliente** (support.paloaltonetworks.com), seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** en la barra de menús de la izquierda. Descargue y guarde la versión que desee usar para actualizar el cortafuegos.

STEP 3 | En cuanto haya decidido qué versión le interesa, siga el flujo de trabajo completo para actualizar el cortafuegos a la nueva versión de PAN-OS. Los pasos dependen de la versión que ejecute, de si tiene una implementación de alta disponibilidad (high availability, HA) y de si utiliza Panorama para gestionar los cortafuegos.

© 2020 Palo Alto Networks, Inc.

Actualizaciones dinámicas de contenido

Palo Alto Networks publica a menudo actualizaciones que el cortafuegos utiliza para aplicar políticas de seguridad sin que sea preciso actualizar el software PAN-OS ni modificar la configuración del cortafuegos. Estas actualizaciones permiten dotar los cortafuegos de la inteligencia contra amenazas y las funciones de seguridad más recientes.

Aparte de las actualizaciones de aplicaciones y algunas actualizaciones de antivirus, que reciben todos los cortafuegos, las actualizaciones dinámicas de contenido que tiene a su disposición dependen de sus Suscripciones. En **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, puede configurar una programación para cada una de las actualizaciones dinámicas de contenido si quiere definir la frecuencia con la que el cortafuegos busca, descarga o instala actualizaciones nuevas.

Actualización dinámica de contenido	Contenido del paquete
Antivirus	Las actualizaciones de antivirus se publican cada 24 horas e incluyen lo siguiente: • Firmas de WildFire para el malware recién detectado. Para obtener estas actualizaciones cada cinco minutos en lugar de una vez al día, debe tener una suscripción a WildFire. • (Threat Prevention obligatorio) Firmas de comando y control (command-and-control, C2) generadas automáticamente para detectar ciertos patrones en el tráfico de C2. Estas firmas permiten que el cortafuegos detecte la actividad de C2 incluso cuando el host de C2 es desconocido o cambia con rapidez. • (Threat Prevention obligatorio) Entradas nuevas y actualizadas de las listas dinámicas externas integradas. Estas listas incluyen direcciones IP malintencionadas, blindadas y de alto riesgo proporcionadas por hosts malintencionados, contra los que ofrecen protección. • (Threat Prevention obligatorio) Actualizaciones del conjunto local de firmas de DNS que usa el cortafuegos para identificar los dominios malintencionados conocidos. Si configura el sinkholing de DNS, el cortafuegos puede identificar los hosts de su red que intentan conectarse a esos dominios. Si desea que el cortafuegos coteje los dominios con toda la base de datos de firmas de DNS, configure DNS Security.
applications	Las actualizaciones de aplicaciones proporcionan firmas de aplicaciones o App-ID nuevos y modificados. Esta actualización no requiere suscripciones adicionales, pero sí un contrato de asistencia/mantenimiento en vigor. Las actualizaciones de aplicaciones nuevas solo se publican el tercer martes de cada mes. Así dispone de tiempo para preparar con antelación las actualizaciones necesarias en las políticas. Las modificaciones de App-ID se publican con más frecuencia. Los App-ID nuevos y modificados permiten al cortafuegos aplicar la política de seguridad con una precisión cada vez mayor, lo que provoca cambios en la aplicación de dicha política que pueden afectar a la disponibilidad de las aplicaciones. Para sacar el máximo partido de las actualizaciones de aplicaciones, siga los consejos que se ofrecen en Gestión de App-ID nuevas y modificadas.
Aplicaciones y amenazas	Incluye firmas de aplicaciones y contra amenazas nuevas y actualizadas. Esta actualización está disponible si cuenta con una suscripción a Threat Prevention (en este caso, sustituye la actualización de aplicaciones). Las actualizaciones de amenazas nuevas se publican a menudo (en ocasiones, varias veces a la semana),

© 2020 Palo Alto Networks, Inc.

Actualización dinámica de contenido	Contenido del paquete
	junto con los App-ID actualizados. Los App-ID nuevos solo se publican el tercer martes de cada mes. El cortafuegos puede obtener las últimas actualizaciones de aplicaciones y amenazas en menos de 30 minutos desde que están disponibles. Si desea saber cómo habilitar las actualizaciones de aplicaciones y amenazas del modo óptimo para garantizar la disponibilidad de las aplicaciones y su protección frente a las últimas amenazas, consulte Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.
GlobalProtect Data File (Archivo de datos de GlobalProtect)	Contiene información específica del proveedor para definir y evaluar los datos de perfiles de información de hosts (host information profile, HIP) que proporcionan las aplicaciones de GlobalProtect. Para recibir estas actualizaciones, debe tener una suscripción a las puertas de enlace de GlobalProtect. Además, para que GlobalProtect funcione, también debe crear una programación para estas actualizaciones.
VPN sin cliente de GlobalProtect	Contiene firmas de aplicaciones nuevas y actualizadas para franquear el acceso a aplicaciones web comunes desde el portal de GlobalProtect por VPN sin cliente. Para recibir estas actualizaciones, debe tener una suscripción a GlobalProtect. Además, para que GlobalProtect Clientless VPN funcione, también debe crear una programación para estas actualizaciones. Como práctica recomendada, se recomienda instalar siempre las últimas actualizaciones de contenido para la VPN sin cliente de GlobalProtect.
WildFire	Proporciona acceso a firmas de malware y antivirus generadas por la nube pública de WildFire en tiempo real. Opcionalmente, puede configurar PAN-OS para recuperar los paquetes de actualización de firmas de WildFire. Puede configurar el cortafuegos de modo que busque actualizaciones nuevas incluso cada minuto para asegurarse de que obtiene las últimas firmas de WildFire en menos de un minuto desde que están disponibles. Si carece de la suscripción a WildFire, debe esperar al menos 24 horas para recibir las firmas con la actualización de antivirus.
WF-Private (Archivo específico de WildFire)	Proporciona, casi en tiempo real, las firmas contra malware y antivirus creadas como resultado del análisis realizado por un dispositivo de WildFire. Para recibir actualizaciones de contenido de un dispositivo de WildFire, tanto este como el cortafuegos deben ejecutar PAN-OS 6.1 o una versión posterior. Además, el cortafuegos debe estar configurado para reenviar archivos y enlaces de correo electrónico a la nube privada de WildFire.

© 2020 Palo Alto Networks, Inc.

Instalación de actualizaciones de contenido

Para garantizar una protección constante contra las amenazas más recientes (incluidas aquellas que aún no se han descubierto), debe asegurarse de mantener actualizados sus cortafuegos con las actualizaciones y el contenido más reciente de Palo Alto Networks. Las Actualizaciones dinámicas de contenido que tiene a su disposición dependen de sus Suscripciones.

Siga estos pasos para instalar las actualizaciones de contenido. También puede configurar una programación si quiere definir la frecuencia con la que el cortafuegos obtiene e instala actualizaciones de contenido.

Las actualizaciones de contenido de aplicaciones y amenazas no funcionan exactamente igual que los demás tipos de actualizaciones. Para sacar el máximo partido de la prevención de amenazas y los conocimientos sobre aplicaciones más recientes, siga las directrices de Implementación de actualizaciones de contenido de aplicaciones y amenazas en lugar de estos pasos.

STEP 1 | Asegúrese de que el cortafuegos tenga acceso al servidor de actualización.

1. De manera predeterminada, el cortafuegos accede a **Update Server (Servidor de actualizaciones)** en **`updates.paloaltonetworks.com`** para que el cortafuegos reciba actualizaciones de contenido del servidor más cercano en la Infraestructura de red de entrega de contenido para actualizaciones dinámicas. Si el cortafuegos ha restringido el acceso a Internet, establezca la dirección del servidor de actualizaciones para usar el nombre de host **`staticupdates.paloaltonetworks.com`** en lugar de seleccionar de forma dinámica un servidor de la infraestructura CDN.
2. (Opcional) Haga clic en **Verify Update Server Identity** para obtener un nivel adicional de validación para habilitar el cortafuegos y comprobar que el certificado SSL del servidor esté firmado por una autoridad fiable. Esta opción está habilitada de manera predeterminada.
3. (Opcional) Si el cortafuegos necesita utilizar un servidor proxy para acceder a los servicios de actualización de Palo Alto Networks, en la ventana **Proxy Server (Servidor proxy)**, introduzca:
   - **Server**: dirección IP o nombre de host del servidor proxy.
   - **Port**: puerto para el servidor proxy. Intervalo: 1-65535.
   - **User**: nombre de usuario para acceder al servidor.
   - **Password (Contraseña)**: contraseña para que el usuario acceda al servidor proxy. Vuelva a introducir la contraseña en **Confirm Password**.
4. (Opcional) Configure hasta tres intentos de reconexión si se produce un fallo en la conexión. Utilice **`debug set-content-download-retry attempts`** para establecer el número de intentos de conexión. El valor predeterminado es 0.

STEP 2 | Compruebe las actualizaciones de contenido más recientes.

Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** (ubicado en la esquina inferior izquierda de la ventana) para comprobar las últimas actualizaciones. El enlace de la columna **Action (Acción)** indica si una actualización está disponible:

- **Download (Descargar)**: indica que hay disponible un nuevo archivo de actualización. Haga clic en el enlace para iniciar la descarga directamente en el cortafuegos. Tras descargarlo correctamente, el enlace en la columna **Action (Acción)** cambia de **Download (Descargar)** a **Install (Instalar)**.



No puede descargar la actualización de antivirus hasta que haya instalado la actualización de aplicaciones y amenazas.

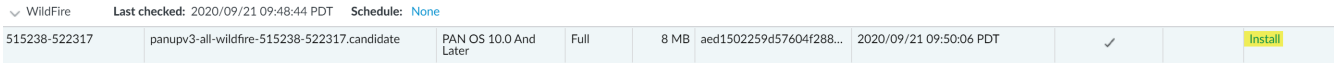
© 2020 Palo Alto Networks, Inc.

- **Revert (Revertir)**: indica que hay disponible una versión previa la versión de software o contenido. Puede decidir revertir a la versión instalada anteriormente.

STEP 3 | Instale las actualizaciones de contenido.

La instalación puede tardar hasta 10 minutos en los cortafuegos PA-220 y hasta 2 minutos en los cortafuegos PA-5200 Series, PA-7000 Series o VM-Series.

Haga clic en el enlace **Instalar** de la columna **Acción**. Cuando se complete la instalación, aparecerá una marca de verificación en la columna **Currently Installed (Instalado actualmente)**.



STEP 4 | Programe cada actualización de contenido.

Repita este paso en cada actualización que desee programar.

Escalone las programaciones de actualizaciones, ya que el cortafuegos no puede descargar más de una actualización a la vez. Si ha programado la descarga de varias actualizaciones al mismo tiempo, solo la primera se realizará correctamente.

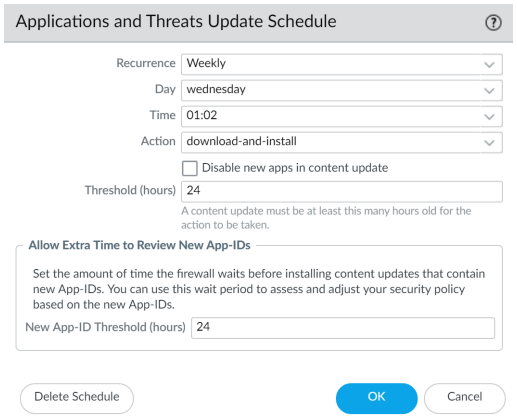
1. Establezca la programación de cada tipo de actualización haciendo clic en el enlace **Ninguna**.



2. Especifique la frecuencia de las actualizaciones seleccionando un valor en el menú desplegable **Recurrence (Periodicidad)**. Los valores disponibles varían según el tipo de contenido (las actualizaciones de WildFire están disponibles en **Real-time** [Tiempo real], **Every Minute [Cada minuto]**, **Every 15 Minutes [Cada 15 minutos]**, **Every 30 minutes [Cada 30 minutos]** o **Every Hour [Cada hora]**, mientras que las actualizaciones de aplicaciones y amenazas pueden programarse **Weekly [Semanalmente]**, **Daily [Diariamente]**, **Hourly [Por hora]** o **Every 30 Minutes [Cada 30 minutos]**, y las actualizaciones de antivirus pueden programarse **Hourly [Cada hora]**, **Daily [Diariamente]** o **Weekly [Semanalmente]**).
3. Especifique la **hora** (o los minutos que pasan de una hora en el caso de WildFire) y, si está disponible en función de la **Periodicidad** seleccionada, el **día** de la semana para realizar la actualización.
4. Especifique si desea que el sistema use la opción **Download Only (Únicamente descargar)** o, como opción recomendada, **Download And Install (Descargar e instalar)** la actualización.
5. Introduzca cuánto tiempo una publicación debe esperar antes de realizar una actualización de contenido en el campo **Threshold (Hours)**. En raras ocasiones puede haber errores en las actualizaciones de contenido. Por este motivo, tal vez desee retrasar la instalación de nuevas actualizaciones hasta que lleven varias horas publicadas.

   Si tiene aplicaciones vitales que deben estar totalmente disponibles, configure el umbral de las actualizaciones de aplicaciones o las actualizaciones de aplicaciones y amenazas en un mínimo de 24 horas y siga el procedimiento Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas. Además, después de configurar la programación de las actualizaciones de contenido, tarea que solo se realiza una vez o con poca frecuencia, debe seguir gestionando los App-ID nuevos y modificados que se incluyen en las versiones de contenido, ya que pueden cambiar la manera de aplicar la política de seguridad.
6. (Opcional) Especifique los **nuevos umbrales de ID de aplicación** en horas para establecer la cantidad de tiempo que el cortafuegos debe esperar antes de instalar actualizaciones de contenido que contengan nuevos App-ID.

© 2020 Palo Alto Networks, Inc.



7. Haga clic en **OK (Aceptar)** para guardar estos ajustes de programación.
8. Haga clic en **Commit (Confirmar)** para guardar estos ajustes en la configuración actual.

STEP 5 | Actualización de PAN-OS.

Siempre actualice el contenido antes de actualizar PAN-OS. Cada versión de PAN-OS tiene una versión de publicación de contenido compatible mínima*.*

1. Revise las notas de versión.
2. Actualice el software de PAN-OS.

© 2020 Palo Alto Networks, Inc.

Actualización de contenido de aplicaciones y amenazas

Las actualizaciones de contenido de aplicaciones y amenazas proporcionan las firmas de aplicaciones y prevención de amenazas más recientes al cortafuegos. La sección de aplicaciones del paquete incluye ID de aplicación nuevas y modificadas y no requiere una licencia. El paquete completo de contenido de aplicaciones y prevención de amenazas, que también incluye firmas de prevención de amenazas nuevas y modificadas, requiere una licencia de prevención de amenazas. Dado que el cortafuegos recupera e instala automáticamente las firmas de aplicaciones y prevención de amenazas más recientes (en función de los ajustes personalizados), puede comenzar a aplicar una política de seguridad en función de las ID de aplicación y la protección frente a amenazas más reciente sin una configuración adicional.

Las firmas de prevención de amenazas nuevas y modificadas y las ID de aplicación modificadas se publican, al menos, una vez a la semana y generalmente con mayor frecuencia. Los App-ID nuevos se publican el tercer martes de cada mes. Dado que las ID de aplicación nuevas pueden cambiar cómo la política de seguridad aplica el tráfico, esta liberación más limitada de ID de aplicación nuevas tiene como objetivo proporcionarle una ventana predecible para preparar y actualizar su política de seguridad. Además, las actualizaciones de contenido se acumulan; esto significa que la actualización de contenido más reciente siempre incluye las firmas de aplicaciones y de prevención de amenazas publicadas en las versiones anteriores.

Debido a que las firmas de aplicaciones y amenazas se entregan en un solo paquete (los mismos decodificadores que permiten que las firmas de aplicaciones identifiquen las aplicaciones también permiten que las firmas de prevención de amenazas inspeccionen el tráfico), debe considerar si desea implementar las firmas en conjunto o por separado. Cómo la elección de la implementación de las actualizaciones de contenido depende de los requisitos de seguridad de red y de disponibilidad de la aplicación de la organización. En primer lugar, identifique a su organización con una de las siguientes posturas (o quizás ambas según la ubicación del cortafuegos):

- Una organización que pone *la seguridad en primer lugar* prioriza la protección con las firmas contra amenazas más actualizadas por encima de la disponibilidad de la aplicación. Básicamente está utilizando el cortafuegos para las prestaciones de prevención de amenazas. Los cambios en la ID de aplicación que afectan cómo la política de seguridad aplica el tráfico de la aplicación son secundarios.
- Una red *crítica* prioriza la disponibilidad de la aplicación por encima de la protección con las firmas contra amenazas más actualizadas. Su red tiene una tolerancia cero de los periodos de inactividad. El cortafuegos se implementa en línea para aplicar la política de seguridad y, si está utilizando una ID de aplicación en la política de seguridad, todo cambio que introduja una versión de contenido que afecte la ID de aplicación podría causar un periodo de inactividad.

Usted puede adoptar un enfoque de red crítica o de seguridad en primer lugar para implementar las actualizaciones de contenido, o puede aplicar una combinación de ambos enfoques para satisfacer las necesidades de la empresa. Lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas y tenga en cuenta las recomendaciones a la hora de decidir cómo implementa las actualizaciones de aplicaciones y amenazas. A continuación:

- ❑ Siga el procedimiento Implementación de actualizaciones de contenido de aplicaciones y amenazas.
- ❑ Siga los consejos de Sugerencias para las actualizaciones de contenido.



Mientras que la programación de las actualizaciones de contenido es una tarea única o poco frecuente, después de establecer una programación, deberá continuar con la Gestión de App-ID nuevas y modificadas *en las versiones de contenido, dado que estas App-ID pueden cambiar cómo se aplica la política de seguridad.*

© 2020 Palo Alto Networks, Inc.

Implementación de actualizaciones de contenido de aplicaciones y amenazas

Antes de seguir los pasos para configurar las actualizaciones de contenido de aplicaciones y amenazas, aprenda cómo funcionan y lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas para decidir cómo desea implementarlas.

Además, Panorama le permite implementar actualizaciones de contenido en los cortafuegos con facilidad y rapidez. Si utiliza Panorama para gestionar los cortafuegos, siga estos pasos para implementar las actualizaciones de contenido, en lugar de seguir los pasos a continuación.

STEP 1 | Para desbloquear el paquete completo de contenido de aplicaciones y prevención de amenazas, obtenga una licencia de prevención de amenazas y active la licencia en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Cargue manualmente la clave de la licencia o recupérela del servidor de licencias de Palo Alto Networks.
3. Verifique que la licencia de prevención contra amenazas esté activa.

STEP 2 | Establezca una programación para que el cortafuegos recupere e instale actualizaciones de contenido.

Cuando complete los siguientes pasos, reviste especial importancia tener en cuenta si la organización se centra en los objetivos o en la seguridad (o en una combinación de ambos) y leer Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Seleccione la **Schedule (Programación)** de las actualizaciones de contenido de aplicaciones y prevención de amenazas.
3. Establezca la frecuencia (**Recurrence [Periodicidad]**) con la que el cortafuegos comprueba el servidor de actualización de Palo Alto Networks para buscar nuevas versiones de contenido de aplicaciones y prevención de amenazas, y el **Day (Día)** y la **Time (Hora)**.
4. Establezca la **Action (Acción)** que realizará el cortafuegos cuando descubra y recupere una nueva versión de contenido.
5. Establezca el **Threshold (Umbral)** de instalación para las versiones de contenido. Las versiones de contenido deben estar disponibles en el servidor de actualización de Palo Alto Networks al menos durante este período de tiempo antes de que el cortafuegos recupere la licencia y realice la acción que configuró en el último paso.
6. Si su red es crítica, con tolerancia cero a los periodos de inactividad de la aplicación (la disponibilidad de la aplicación es casi tan importante como la prevención de amenazas más reciente), puede establecer un **New App-ID Threshold (Umbral de App-ID nueva)**. El cortafuegos únicamente recupera actualizaciones de contenido que contienen App-ID nuevas luego de que haya estado disponible durante este período de tiempo.
7. Haga clic en **OK (Aceptar)** para guardar la programación de actualizaciones de contenido de aplicaciones y prevención de amenazas, y haga clic en **Commit (Confirmar)**.

STEP 3 | Realice la Configuración del reenvío de logs para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event (Evento): (subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message).

© 2020 Palo Alto Networks, Inc.

STEP 4 | Mientras que la programación de las actualizaciones de contenido es una tarea única o poco frecuente, después de establecer una programación, deberá continuar con la Gestión de App-ID nuevas y modificadas en las versiones de contenido, dado que estas App-ID pueden cambiar cómo se aplica la política de seguridad.

Sugerencias para las actualizaciones de contenido

Las versiones de contenido de aplicaciones y prevención de amenazas de Palo Alto Networks experimentan evaluaciones estrictas de rendimiento y calidad. Sin embargo, debido a que existen demasiadas variables posibles en el entorno de un cliente, rara vez una versión de contenido afecta una red de manera inesperada. Siga estas sugerencias para mitigar o solucionar un problema relacionado con una versión de contenido, de modo que su red se vea afectada lo menos posible.

- **Siga las prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas.**

  Lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas y aplique las recomendaciones. Cómo la elección de la implementación de las actualizaciones de contenido depende de sus requisitos de seguridad de red y de disponibilidad de la aplicación.
- **Compruebe si está ejecutando el contenido más reciente.**

  Obtenga la actualización de contenido más reciente si no configuró el cortafuegos para descargarla e instalarla automáticamente.

  El cortafuegos valida que Palo Alto Networks aún recomiende las actualizaciones de contenido descargadas en el momento de la instalación. Esta comprobación, que el cortafuegos realiza de manera predeterminada, es útil cuando las actualizaciones de contenido se descargan del servidor de actualización de Palo Alto Networks (manualmente o de manera programada) antes de la instalación. Debido a que en contadas ocasiones Palo Alto Networks elimina una actualización de contenido, esta opción evita que el cortafuegos instale una actualización de contenido que Palo Alto Networks eliminó, incluso si el cortafuegos ya la descargó. Si observa un mensaje de error que indica que la actualización de contenido que intenta instalar ya no es válida, haga clic en **Check Now (Comprobar ahora)** para obtener la actualización de contenido más reciente e instale esa versión (**Device [Dispositivo]** > **Dynamic Updates [Actualizaciones dinámicas]**).
- **Active la telemetría de inteligencia contra amenazas.**

  Active la telemetría de inteligencia contra amenazas que el cortafuegos envía a Palo Alto Networks. Utilizamos datos de telemetría para identificar y solucionar problemas de las actualizaciones de contenido.

  Los datos de telemetría nos ayudan a reconocer con rapidez una actualización de contenido que afecta el rendimiento del cortafuegos o la aplicación de una política de seguridad de manera inesperada en la base de clientes de Palo Alto Networks. Cuanto más rápido identificamos un problema, con mayor rapidez podemos ayudarte a evitar el problema o mitigar el impacto en su red.

  Para permitir que el cortafuegos recopile y comparta datos de telemetría con Palo Alto Networks:

  1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**.
  2. Edite los ajustes de **Telemetry (Telemetría)** y haga clic en **Select All (Seleccionar todos)**.
  3. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para guardar los cambios.
- **Reenvíe las alertas de actualizaciones de contenido de Palo Alto Networks a las personas indicadas.**

  Habilite el reenvío de logs para las alertas de contenido crítico de Palo Alto Networks, de modo que los mensajes importantes sobre los problemas en la versión de contenido se dirijan directamente al personal adecuado.

© 2020 Palo Alto Networks, Inc.

Ahora, Palo Alto Networks puede emitir alertas sobre problemas de actualización de contenido directamente en la interfaz web del cortafuegos o (si habilitó el reenvío de logs) en el servicio externo que utiliza para la supervisión. Las alertas de contenido crítico describen el problema, de modo que pueda comprender cómo lo afectan e incluyen medidas a tomar de ser necesario.

En la interfaz web del cortafuegos, las alertas críticas sobre problemas de contenido se muestran de manera similar al mensaje del día. Cuando Palo Alto Networks emite una alerta crítica sobre una actualización de contenido, la alerta se muestra de manera predeterminada cuando inicia sesión en la interfaz web del cortafuegos. Si ya inicio sesión en la interfaz web del cortafuegos, observará que aparece un signo de exclamación sobre el icono de mensaje en la barra de menú ubicada en la parte inferior de la interfaz web; haga clic en el icono de mensaje para ver la alerta.

Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) **dynamic-updates** y Event (Evento) **palo-alto-networks-message**. Utilice el siguiente filtro para ver esas entradas del log: (subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message).

- **Use Panorama para revertir la versión del contenido a una anterior si es necesario.**

  Tras recibir la notificación de un problema en una actualización de contenido, puede utilizar Panorama para restablecer rápidamente los cortafuegos gestionados a la última versión de actualización de contenido, en lugar de restablecer manualmente la versión de contenido en los cortafuegos individuales: Restablezca actualizaciones de contenido en cortafuegos gestionados.

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas

Las prácticas recomendadas para implementar actualizaciones de contenido ayudan a garantizar una aplicación correcta de la política a medida que se introducen aplicaciones y firmas contra amenazas nuevas y modificadas en el cortafuegos. A pesar de que las firmas de aplicaciones y amenazas se entregan en un solo paquete de actualizaciones de contenido (obtenga más información sobre las actualizaciones de contenido de aplicaciones y amenazas), cuenta con la flexibilidad para implementarlas de manera diferente en función de los requisitos de seguridad y disponibilidad de su red:

- Una organización que pone *la seguridad en primer lugar* prioriza la protección con las firmas contra amenazas más actualizadas por encima de la disponibilidad de la aplicación. Básicamente está utilizando el cortafuegos para las prestaciones de prevención de amenazas.
- Una red *crítica* prioriza la disponibilidad de la aplicación por encima de la protección con las firmas contra amenazas más actualizadas. Su red tiene una tolerancia cero de los periodos de inactividad. El cortafuegos se implementa en línea para aplicar la política de seguridad y, si está usando una ID de aplicación en la política de seguridad, todo cambio del contenido que afecte la ID de aplicación podría causar un periodo de inactividad.

Usted puede adoptar un enfoque de red crítica o de seguridad en primer lugar para implementar las actualizaciones de contenido, o puede aplicar una combinación de ambos enfoques para satisfacer las necesidades de la empresa. Considere su enfoque mientras aplica las siguientes prácticas recomendadas para aprovechar mejor las firmas de aplicaciones y contra amenazas nuevas y modificadas:

- Prácticas recomendadas para las actualizaciones de contenido: nivel crítico
- Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad

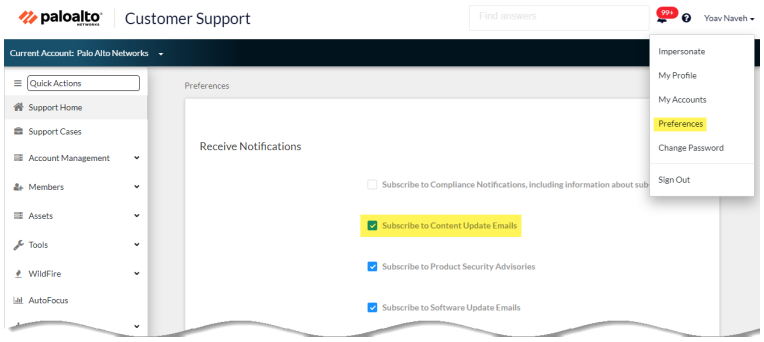
Prácticas recomendadas para las actualizaciones de contenido: nivel crítico

Las Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas permiten garantizar la correcta aplicación de las políticas a medida que se publican firmas nuevas de aplicaciones y contra amenazas. Respete estas prácticas recomendadas para implementar las actualizaciones de contenido en una *red crítica*, donde tiene una tolerancia cero a los periodos de inactividad de la aplicación.

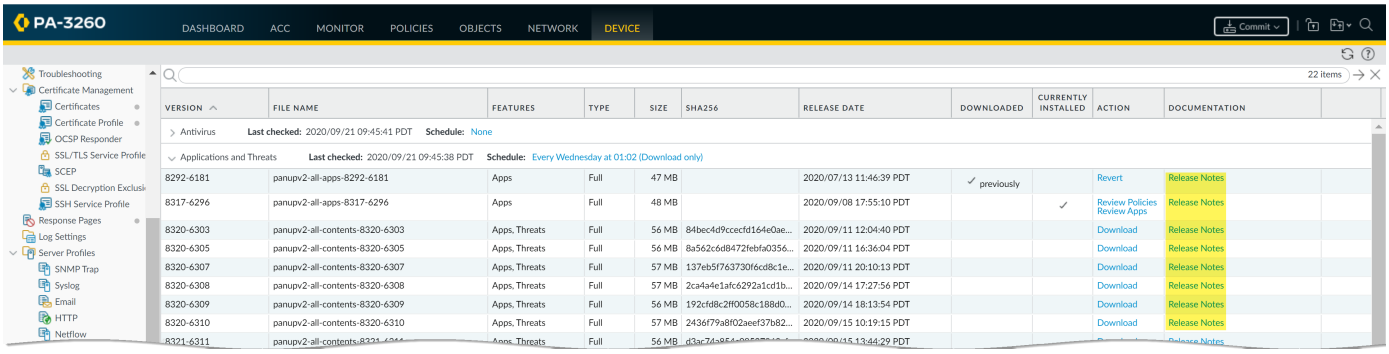
- ❑ Siempre revise las notas de la versión de contenido para conocer la lista de las aplicaciones identificadas y modificadas recientemente, y las firmas de amenazas que introduce la versión de contenido. Las notas de la versión de contenido también describen de qué manera la actualización puede afectar la aplicación de la política de seguridad existente y ofrece recomendaciones sobre cómo puede modificar su política de seguridad para aprovechar mejor lo nuevo.

  Para suscribirse y recibir notificaciones de las nuevas actualizaciones de contenido, visite el portal de asistencia al cliente, edite **Preferences (Preferencias)** y seleccione **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**.

© 2020 Palo Alto Networks, Inc.



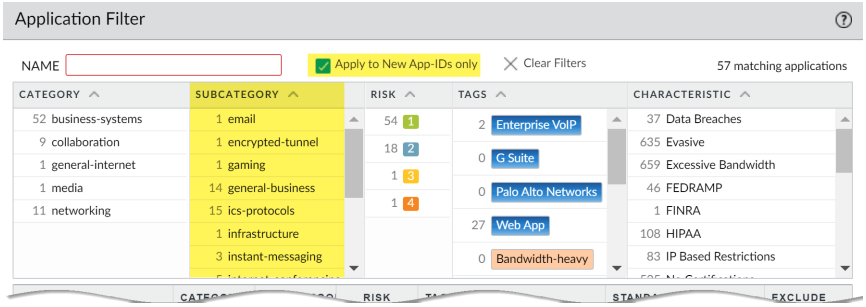
También puede revisar las notas de la versión de contenido para aplicaciones y prevención de amenazas en el portal de asistencia técnica de Palo Alto Networks o directamente en la interfaz web del cortafuegos: seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y abra la **Release Note (Nota de la versión)** de una versión de contenido específica.



La sección Notes (Notas) de las notas de versión de contenido resalta las futuras actualizaciones que Palo Alto Networks ha identificado como posibles impactos considerables para la cobertura; por ejemplo, nuevas ID de aplicación o decodificadores. Verifique estas futuras actualizaciones, de manera que pueda prever con antelación cualquier impacto de la versión en la política.

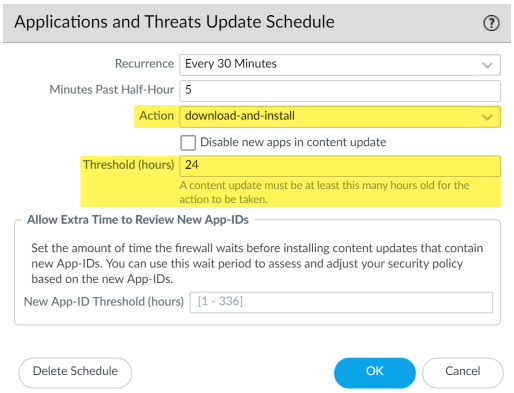
- Cree una regla en la política de seguridad para siempre permitir ciertas categorías de App-ID nuevos, como aplicaciones de autenticación o desarrollo de software en las que confían las funciones empresariales críticas. Esto significa que cuando una versión de contenido introduce o cambia la cobertura de una aplicación empresarial importante, el cortafuegos continúa permitiendo sin inconvenientes la aplicación sin requerir una actualización en la política de seguridad. Esto elimina el posible impacto en la disponibilidad de los App-ID de categorías críticas y ofrece treinta días (los App-ID nuevos se liberan una vez al mes) para ajustar su política de seguridad de modo que permita los App-ID críticos.

  Para hacerlo, cree un filtro de aplicación para App-ID nuevas en categorías críticas application (**Objects [Objetos] > Application Filters [Filtros de aplicación]**),

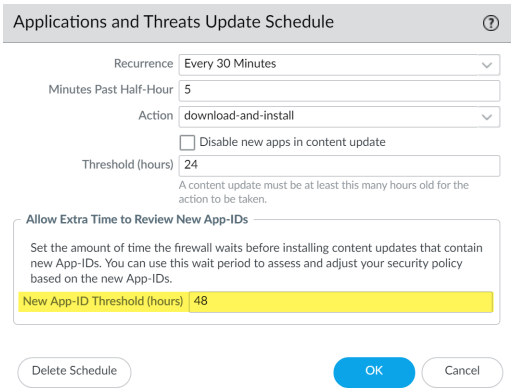


© 2020 Palo Alto Networks, Inc.

- Para mitigar el impacto en la aplicación de la política de seguridad asociada con la habilitación de nuevas firmas de aplicaciones y amenazas, puede alternar la implementación del contenido nuevo. Proporcione el nuevo contenido a las ubicaciones con menos riesgo comercial (menor usuarios en sucursales) antes de implementarlo en las ubicaciones con mayor riesgo comercial (tal como las ubicaciones con aplicaciones críticas). El confinamiento de las actualizaciones de contenido más recientes a ciertos cortafuegos antes de implementarlas en toda la red también facilita la detección de problemas e inconvenientes que puedan surgir. Puede utilizar Panorama para enviar programaciones escalonadas y umbrales de instalación para los cortafuegos y los grupos de dispositivos en función de la organización o ubicación (Utilización de Panorama para implementar actualizaciones en los cortafuegos).
- Programe las actualizaciones de contenido, de modo que se puedan **download-and-install (descargar e instalar)** automáticamente. Luego, establezca un **Threshold (Umbral)** que determine la cantidad de tiempo que espera el cortafuegos antes de instalar el contenido más reciente. En una red crítica, programe un umbral de hasta 48 horas.

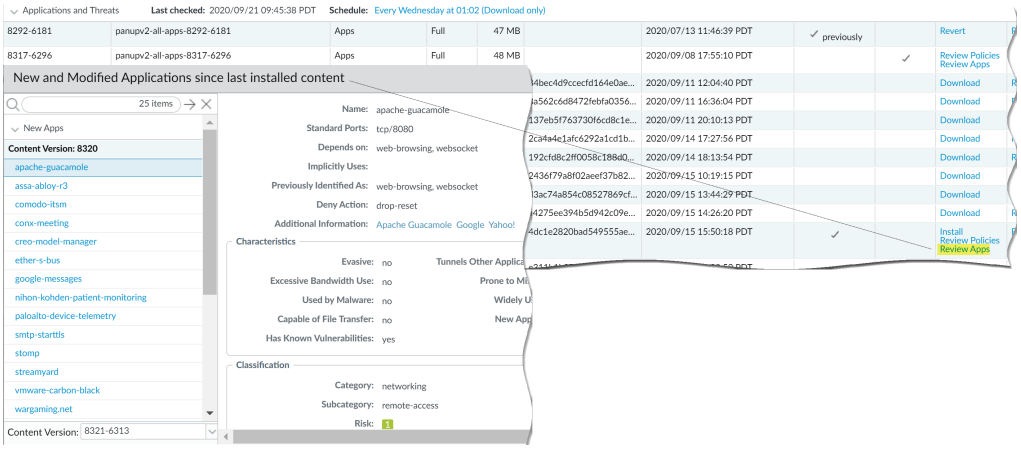


  La demora en la instalación garantiza que el cortafuegos únicamente instale contenido que ha estado disponible y que funciona en los entornos del cliente durante ese período de tiempo específico. Para programar actualizaciones de contenido, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** > **Schedule (Programar)**.
- Proporcione tiempo adicional para ajustar su política de seguridad en función de las App-ID antes de instalarlas. Para hacerlo, establezca un umbral de instalación que se aplique únicamente a las actualizaciones de contenido que contienen nuevas App-ID. Las actualizaciones de contenido con nuevas App-ID se liberan únicamente una vez al mes y el umbral de instalación se activa únicamente en ese momento. Programe actualizaciones de contenido para configurar un **New App-ID Threshold (Umbral de nueva App-ID)** (**Device [Dispositivo]** > **Dynamic Updates [Actualizaciones dinámicas]** > **Schedule [Programar]**).

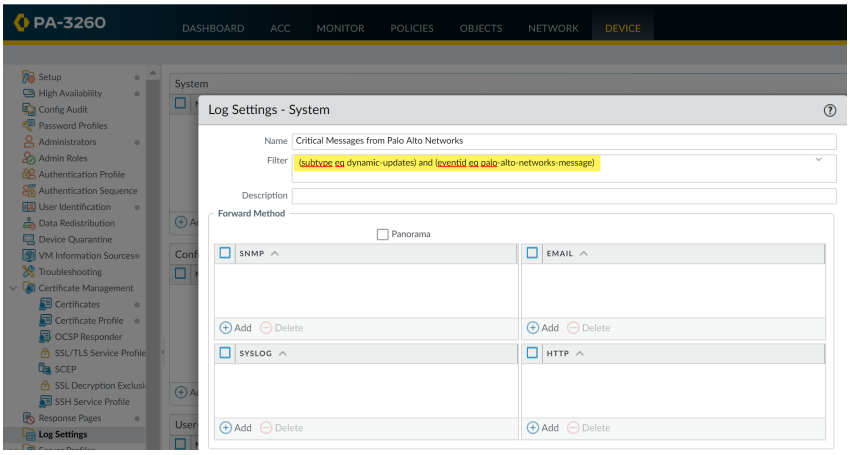


- Siempre revise las App-ID nuevas y modificadas que introduce una versión de contenido para evaluar cómo estos cambios afectan su política de seguridad. El siguiente tema describe las opciones que puede utilizar para actualizar su política de seguridad antes y después de instalar nuevas App-ID: Realice la Gestión de ID de aplicación nuevas y modificadas.

© 2020 Palo Alto Networks, Inc.



- Realice la Configuración del reenvío de logs para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event (Evento): **`(subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message)`**.





PAN-OS 8.1.2 modificó el tipo de log para las alertas de contenido críticas de ***`general`*** *a* ***`dynamic-updates`****. Si utiliza PAN-OS 8.1.0 o PAN-OS 8.1.1, el contenido crítico se registra como entradas de log del sistema con el siguiente Type (Tipo) y Event (Evento), y debe configurar el reenvío para estas alertas con el siguiente filtro:* ***`(subtype eq general) y (eventid eq palo-alto-networks-message)`***.

- Pruebe las actualizaciones nuevas de contenido de aplicaciones y amenazas en un entorno de prueba dedicado antes de habilitarlas en su entorno de producción. La manera más fácil de comprobar las nuevas aplicaciones y contenido contra amenazas es usar un cortafuegos de prueba para acceder al tráfico de producción. Instale el contenido más reciente en el cortafuegos de prueba y contrólelo a medida que procesa el tráfico copiado de su entorno de producción. También puede usar clientes de prueba y un cortafuegos de prueba, o capturas de paquetes (packet captures, PCAP) para simular el tráfico de producción. El uso de PCAP funciona bien para simular el tráfico de distintas implementaciones en las que la política de seguridad del cortafuegos varía según la ubicación.

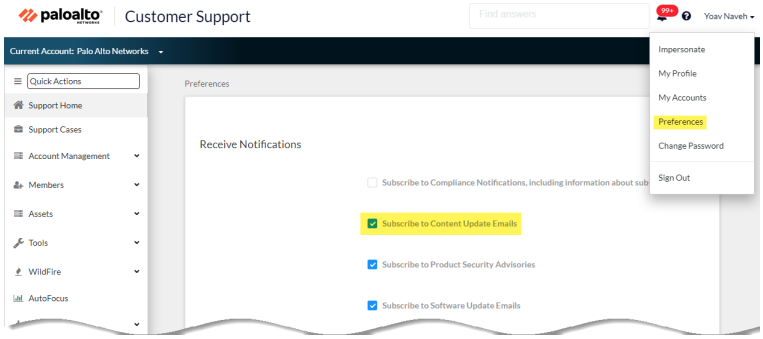
© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas para las actualizaciones de contenido: prioridad de seguridad

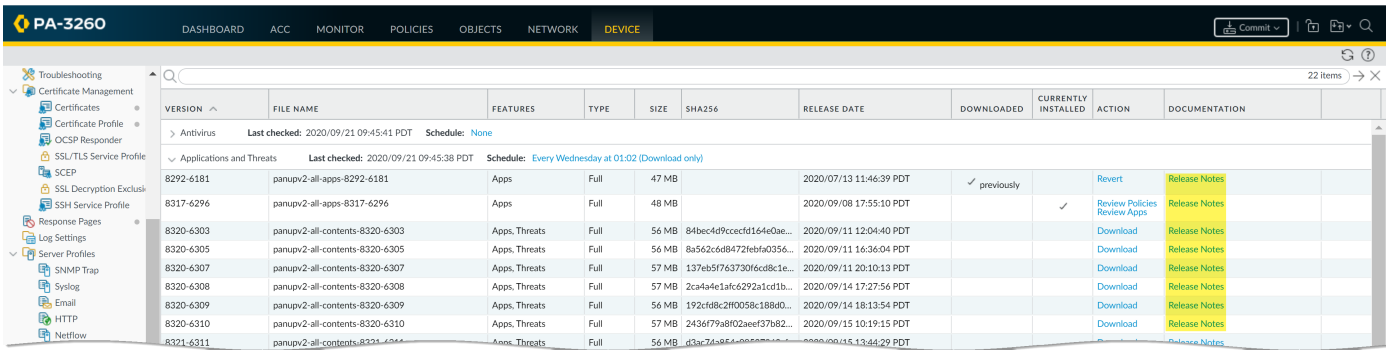
Las Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas permiten garantizar la correcta aplicación de las políticas a medida que se publican firmas nuevas de aplicaciones y contra amenazas. Respete estas prácticas recomendadas para implementar las actualizaciones de contenido en una *red con prioridad de seguridad*, donde utiliza principalmente el cortafuegos para las capacidades de prevención de amenazas y su primera prioridad es la defensa frente al ataque.

- Siempre revise las notas de la versión de contenido para conocer la lista de las aplicaciones identificadas y modificadas recientemente, y las firmas de amenazas que introduce la versión de contenido. Las notas de la versión de contenido también describen de qué manera la actualización puede afectar la aplicación de la política de seguridad existente y ofrece recomendaciones sobre cómo puede modificar su política de seguridad para aprovechar mejor lo nuevo.

  Para suscribirse y recibir notificaciones de las nuevas actualizaciones de contenido, visite el portal de asistencia al cliente, edite **Preferences (Preferencias)** y seleccione **Subscribe to Content Update Emails (Suscribirse para recibir actualizaciones de contenido por correo electrónico)**.



  También puede revisar las notas de la versión de contenido para aplicaciones y prevención de amenazas en el portal de asistencia técnica de Palo Alto Networks o directamente en la interfaz web del cortafuegos: seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y abra la **Release Note (Nota de la versión)** de una versión de contenido específica.



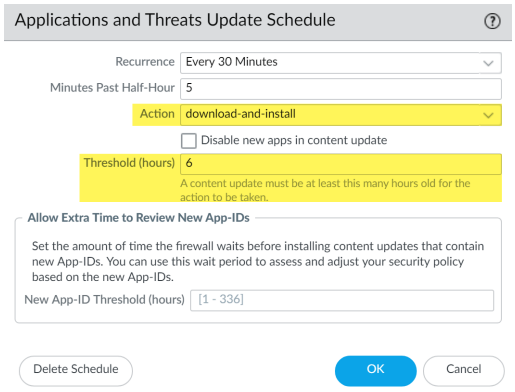
  La sección Notes (Notas) de las notas de versión de contenido resalta las futuras actualizaciones que Palo Alto Networks ha identificado como posibles impactos considerables para la cobertura; por ejemplo, nuevas ID de aplicación o decodificadores. Verifique estas futuras actualizaciones, de manera que pueda prever con antelación cualquier impacto de la versión en la política.

- Para mitigar el impacto en la aplicación de la política de seguridad asociada con la habilitación de nuevas firmas de aplicaciones y amenazas, puede alternar la implementación del contenido nuevo. Proporcione el nuevo contenido a las ubicaciones con menos riesgo comercial (menor usuarios en sucursales)

© 2020 Palo Alto Networks, Inc.

antes de implementarlo en las ubicaciones con mayor riesgo comercial (tal como las ubicaciones con aplicaciones críticas). El confinamiento de las actualizaciones de contenido más recientes a ciertos cortafuegos antes de implementarlas en toda la red también facilita la detección de problemas e inconvenientes que puedan surgir. Puede utilizar Panorama para enviar programaciones escalonadas y umbrales de instalación para los cortafuegos y los grupos de dispositivos en función de la organización o ubicación (Utilización de Panorama para implementar actualizaciones en los cortafuegos).

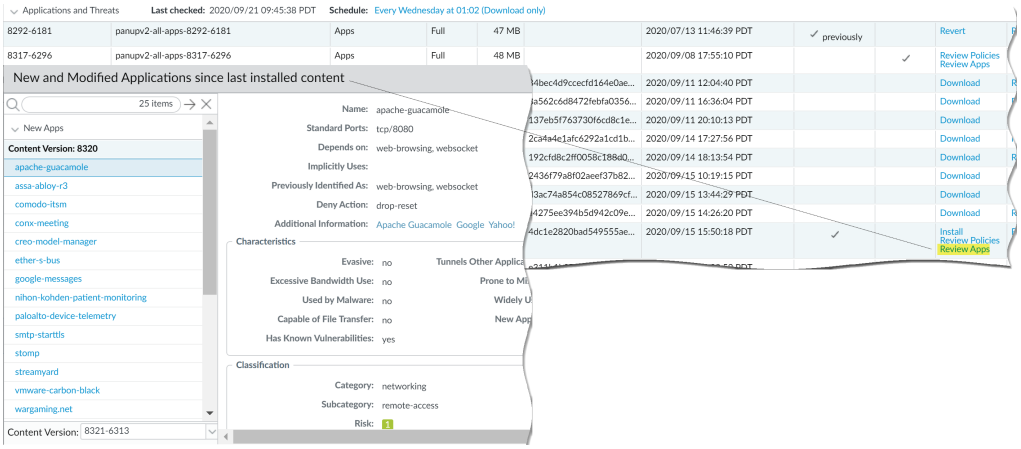
- Programe las actualizaciones de contenido, de modo que se puedan **download-and-install (descargar e instalar)** automáticamente. Luego, establezca un **Threshold (Umbral)** que determine la cantidad de tiempo que espera el cortafuegos antes de instalar el contenido más reciente. En una red con prioridad de seguridad, programe un umbral de seis a doce horas.



La demora en la instalación garantiza que el cortafuegos únicamente instale contenido que ha estado disponible y que funciona en los entornos del cliente durante ese período de tiempo específico. Para programar actualizaciones de contenido, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** > **Schedule (Programar)**.

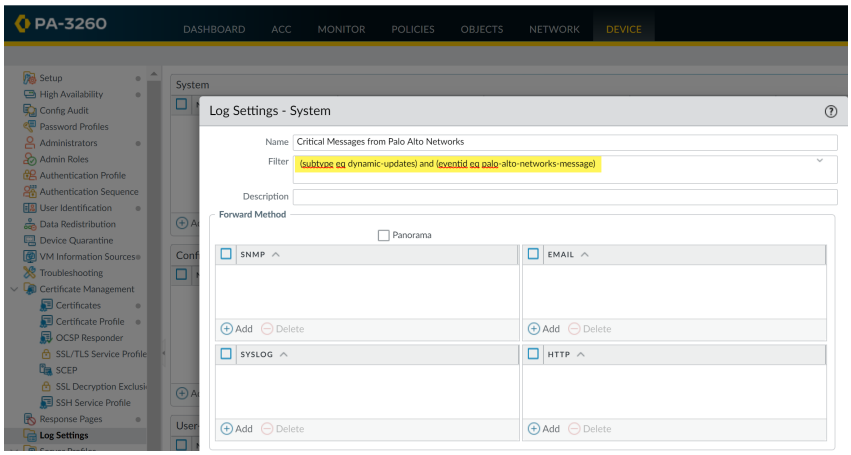
No programe un New App-ID Threshold (Umbral de nueva App-ID). Este umbral brinda a las organizaciones críticas tiempo adicinal para ajustar la aplicación de la política de seguridad en función de las nuevas App-ID. Sin embargo, debido a que este umbral también demora la entrega de las actualizaciones de contenido de prevención de amenazas más recientes, no se recomienda a las organizaciones que ponen la seguridad en primer lugar.

- Revise las App-ID nuevas y modificadas que introduce una versión de contenido para evaluar cómo estos cambios afectan su política de seguridad. El siguiente tema describe las opciones que puede utilizar para actualizar su política de seguridad antes y después de instalar nuevas App-ID: Realice la Gestión de ID de aplicación nuevas y modificadas.



© 2020 Palo Alto Networks, Inc.

- Realice la Configuración del reenvío de logs para enviar alertas de contenido crítico de Palo Alto Networks a servicios externos que utiliza para supervisar la actividad de la red y el cortafuegos. Esto le permite garantizar que el personal adecuado reciba la notificación sobre problemas de contenido críticos, de modo que se puedan tomar las medidas necesarias. Las alertas críticas de actualización de contenido también se guardan como entradas en el log del sistema con Type (Tipo) y Event (Evento): `(subtype eq dynamic-updates) y (eventid eq palo-alto-networks-message)`.



PAN-OS 8.1.2 modificó el tipo de log para las alertas de contenido críticas de ***`general`*** *a* ***`dynamic-updates`****. Si utiliza PAN-OS 8.1.0 o PAN-OS 8.1.1, el contenido crítico se registra como entradas de log del sistema con el siguiente Type (Tipo) y Event (Evento), y debe configurar el reenvío para estas alertas con el siguiente filtro:* ***`(subtype eq general) y (eventid eq palo-alto-networks-message)`****.*

© 2020 Palo Alto Networks, Inc.

Infraestructura de red de entrega de contenido

Palo Alto Networks mantiene una infraestructura de red de entrega de contenidos (Content Delivery Network, CDN) para entregar actualizaciones de contenido a los cortafuegos de Palo Alto Networks. Estos cortafuegos acceden a los recursos web en la CDN para realizar diferentes funciones de identificación de contenido y aplicaciones.

La siguiente tabla enumera los recursos de Internet a los que accede el cortafuegos para una función o aplicación:

Recurso	URL	Direcciones estáticas (si se requiere un servidor estático)
Base de datos de aplicaciones	• updates.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443	staticupdates.paloaltonetworks.com
Base de datos amenazas/ antivirus	• updates.paloaltonetworks.com:443 • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 Como práctica recomendada, establezca el servidor de actualizaciones para que acceda a updates.paloaltonetworks.com. De esta forma, el cortafuegos de Palo Alto Network podrá recibir actualizaciones de contenido desde el servidor que esté más cercano en la infraestructura de CDN.	staticupdates.paloaltonetworks.com
PAN-DB URL Filtering	*.urlcloud.paloaltonetworks.com Se resuelve como la dirección URL principal s0000.urlcloud.paloaltonetworks.com y, a continuación, se redirige al servidor regional más próximo: • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com • s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	Las direcciones IP estáticas no están disponibles. No obstante, puede resolver manualmente una dirección URL como una dirección IP y permitir el acceso a la dirección IP del servidor regional.

Administración del cortafuegos

Los administradores pueden configurar, gestionar y supervisar los cortafuegos de Palo Alto Networks a través de la interfaz web, el CLI y la interfaz de gestión de la API. Usted puede personalizar el acceso administrativo a las interfaces de gestión basado en las funciones para delegar tareas o permisos específicos a ciertos administradores.

- Interfaces de gestión
- Uso de la interfaz web
- Gestión de las copias de seguridad de la configuración
- Gestión de los administradores de cortafuegos
- Referencia: acceso de administrador a la interfaz web
- Referencia: uso de número de puerto
- Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica
- Arranque del cortafuegos

© 2020 Palo Alto Networks, Inc.

Interfaces de gestión

Puede utilizar las siguientes interfaces de usuario para gestionar el cortafuegos de Palo Alto Networks:



No permite el acceso administrativo desde internet o desde otras zonas no fiables dentro de sus límites de seguridad empresariales. Respete las Prácticas recomendadas para proteger el acceso administrativo *para garantizar que protege adecuadamente el cortafuegos.*

- Garantice el Uso de la interfaz web para realizar la configuración y supervisar tareas con relativa facilidad. Esta interfaz gráfica le permite acceder al cortafuegos con HTTPS (recomendado) o HTTP, y es la mejor forma de realizar tareas administrativas.
- Garantice el Uso de la interfaz de línea de comandos (CLI) para realizar una serie de tareas introduciendo rápidamente comandos en secuencia en SSH (recomendado), Telnet o el puerto de la consola. El CLI es una interfaz sencilla que admite dos modos de comandos, operativo y de configuración, cada uno con su propia jerarquía de comandos e instrucciones. Cuando conoce la estructura de anidamiento y la sintaxis de los comandos, el CLI permite tiempos de respuesta rápidos y ofrece eficacia administrativa.
- Use la API XML para dinamizar las operaciones e integrarse con las aplicaciones y repositorios existentes desarrollados internamente. La API XML es un servicio web implementado usando solicitudes y respuestas de HTTP/HTTPS.
- Garantice el Uso de Panorama para llevar a cabo una gestión basada en la web, la creación de informes y la recopilación de logs para varios cortafuegos. La interfaz web de Panorama se parece a la interfaz web del cortafuegos, pero contiene funciones adicionales para la gestión centralizada.

© 2020 Palo Alto Networks, Inc.

Uso de la interfaz web

Los siguientes temas describen cómo usar la interfaz web del cortafuegos. Si desea información detallada sobre las pestañas y los campos específicos de la interfaz web, consulte la Guía de referencia de la interfaz web.

- Inicio de la interfaz web
- Configuración de banners, mensaje del día y logotipos
- Uso de los indicadores de actividad de inicio de sesión de administrador para detectar el uso indebido de la cuenta
- Gestión y supervisión de tareas administrativas
- Confirmación, validación y previsualización de los cambios de configuración del cortafuegos
- Exportación de los datos de la tabla de configuración
- Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama
- Gestión de bloqueos para restringir cambios de configuración

Inicio de la interfaz web

Los siguientes exploradores web son compatibles para acceder a la interfaz web:

- Internet Explorer 11 y posteriores
- Firefox 3.6 y posteriores
- Safari 5 y posteriores
- Chrome 11 y posteriores

Realice las siguientes tareas para ejecutar la interfaz web.

STEP 1 | Abra una ventana del explorador e introduzca la dirección IP del cortafuegos en el campo de la URL (https://<dirección IP>).



Por defecto, la interfaz de gestión (MGT) permite solo el acceso de HTTPS a la interfaz web. Para habilitar otros protocolos, seleccione Device (Dispositivo) > Setup (Configuración) > Interfaces y edite la interfaz Management (Gestión).

STEP 2 | Inicie sesión en el cortafuegos según el tipo de autenticación que utilice su cuenta. Si inicia sesión en el cortafuegos por primera vez, utilice el valor predeterminado **admin (administrador)** para su nombre de usuario y contraseña.

- **SAML:** haga clic en **Use Single Sign-On (SSO) (Utilizar el inicio de sesión único)**. Si el cortafuegos realiza la autenticación (asignación de funciones) para los administradores, introduzca un nombre de usuario en **Username (Nombre de usuario)** y haga clic en **Continue (Continuar)**. Si el proveedor de identidad (IdP) SAML realiza la autorización, haga clic en **Continue (Continuar)** sin introducir un nombre de usuario en **Username (Nombre de usuario)**. En ambos casos, el cortafuegos lo redirige al IdP, que le pide que introduzca un nombre de usuario y una contraseña. Luego de la autenticación en el IdP, se muestra la interfaz web del cortafuegos.
- **Cualquier otro tipo de autenticación:** introduzca el nombre de su usuario en **Name (Nombre)** y la contraseña en **Password (Contraseña)**. Lea el banner de inicio de sesión y seleccione **I Accept and Acknowledge the Statement Below (Acepto el siguiente enunciado)** si la página de inicio de sesión tiene el banner y la casilla de verificación. Luego, haga clic en **Login (Iniciar sesión)**.

STEP 3 | Lea y **cierre** los mensajes del día.

© 2020 Palo Alto Networks, Inc.

Configuración de banners, mensaje del día y logotipos

Un *banner de inicio de sesión* es texto opcional que puede agregar en la página de inicio de sesión para que los administradores vean información que deben conocer antes de iniciar sesión. Por ejemplo, puede agregar un mensaje para notificar a los usuarios sobre restricciones de uso no autorizado del cortafuegos.

Puede añadir bandas de color que resalten el texto superpuesto en la parte superior (*banner de encabezado*) y en la parte inferior (*banner al pie*) de la interfaz web para garantizar que los administradores vean información crítica, tal como el nivel de clasificación para la administración del cortafuegos.

Se muestra un cuadro de diálogo con un *mensaje del día* automáticamente después de que inicia sesión. El cuadro de diálogo muestra mensajes que Palo Alto Networks inserta en información importante destacada que está asociada a una versión de contenido o software. También puede añadir mensajes personalizados para garantizar que los administradores vean información, tal como un reinicio de sistema inminente, que podría afectar sus tareas.

Puede reemplazar los logotipos por defecto que aparecen en la página de inicio de sesión y en el encabezado de la interfaz web por los logotipos de su organización.

STEP 1 | Configure el banner de inicio de sesión.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite General Settings (Configuración general).
2. Introduzca el **banner de inicio de sesión** (hasta 3200 caracteres).
3. (Opcional) Seleccione **Force Admins to Acknowledge Login Banner** para obligar a los administradores a seleccionar la casilla de verificación **I Accept and Acknowledge the Statement Below** arriba del texto del banner para activar el botón **Login**.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Seleccione el mensaje del día.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de banners y mensajes.
2. Habilite la opción **Message of the Day (Mensaje del día)**.
3. Introduzca el **mensaje del día** (hasta 3200 caracteres).

   Después de introducir el mensaje y hacer clic en OK (Aceptar), los administradores que posteriormente inician sesión y los administradores activos que actualizan sus navegadores verán el mensaje nuevo o actualizado de inmediato sin necesidad de confirmación. Esto le permite advertir a otros administradores sobre una confirmación inminente que podría afectar sus cambios de configuración. Según el tiempo de confirmación que su mensaje especifique, los administradores pueden decidir completar, guardar o deshacer los cambios.
4. (Opcional) Seleccione **Allow Do Not Display Again** (por defecto está deshabilitada) para brindar a los administradores la opción de suprimir un mensaje del día después de la primera sesión iniciada. Cada administrador puede suprimir mensajes solo para sus propias sesiones iniciadas. En el cuadro de diálogo de mensaje del día, cada mensaje tendrá su propia opción de supresión.
5. (Opcional) En **Title (Título)**, introduzca el encabezado del cuadro de diálogo de mensaje del día; el valor predeterminado es `Message of the Day (Mensaje del día)`.

STEP 3 | Configure los banners de encabezado y al pie.

Un fondo de color brillante y el texto en color contrastante pueden aumentar las probabilidades de que los administradores adviertan y lean el banner. También puede usar colores que correspondan a los niveles de clasificación de su organización.

© 2020 Palo Alto Networks, Inc.

1. Introduzca el **banner de encabezado** (hasta 3200 caracteres).
2. (Opcional) Desmarque **Same Banner Header and Footer (Mismo encabezado de banner y al pie)** (habilitado por defecto) para usar banners de encabezado y al pie diferentes.
3. Introduzca el **banner al pie** (hasta 3200 caracteres) si los banners de encabezado y al pie son diferentes.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Reemplace los logotipos de la página de inicio de sesión y en el encabezado.

El tamaño máximo para cualquier imagen de logotipo es de 128 KB. Los tipos de archivos admitidos son png, gif y jpg. El cortafuegos no admite archivos de imágenes que estén entrelazados o que contengan canales alfa.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Custom Logos (Personalizar logotipos)** en la sección Miscellaneous (Varios).
2. Siga los pasos a continuación para el logotipo de **Login Screen** y el logotipo de **Main UI** (encabezado).
   1. Haga clic en cargar .
   2. Seleccione la imagen del logotipo y haga clic en **Open (Abrir)**.

      Puede obtener la vista previa de la imagen para ver de qué manera PAN-OS la recortará para ajustarla, a través del icono de la lupa.
   3. Haga clic en **Close (Cerrar)**.
3. **Commit (Confirmar)** los cambios.

STEP 5 | Verifique que los banners, el mensaje del día y los logotipos se muestren según lo previsto.

1. Cierre sesión para regresar a la página de inicio de sesión, que muestra los nuevos logotipos que seleccionó.
2. Introduzca sus credenciales de inicio de sesión, revise el banner, seleccione **I Accept and Acknowledge the Statement Below (Acepto y confirmo la declaración a continuación)** para habilitar el botón **Login (Iniciar sesión)** y luego **inicie sesión**.

   Un cuadro de diálogo muestra el mensaje del día. Los mensajes incorporados por Palo Alto Networks se muestran en páginas separadas en el mismo cuadro de diálogo. Para navegar por las páginas, haga clic en las flechas derecha o izquierda junto a los laterales del cuadro de diálogo, o haga clic en un selector de página al final del cuadro de diálogo.
3. (Opcional) Puede seleccionar **Do not show again** para los mensajes que configuró y para cualquier mensaje que Palo Alto Network haya integrado.
4. **Cierre** el cuadro de diálogo de mensaje del día para acceder a la interfaz web.

   Los banners de encabezado y al pie aparecen en cada página de interfaz web con el texto y los colores que usted configuró. El nuevo logotipo que usted seleccionó para la interfaz web aparece debajo del banner del encabezado.

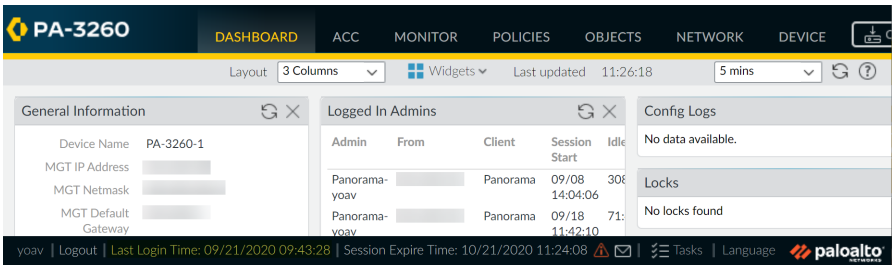
Uso de los indicadores de actividad de inicio de sesión de administrador para detectar el uso indebido de la cuenta

Los indicadores de hora del último inicio de sesión e intentos de inicio de sesión erróneos brindan una manera visual de detectar el uso indebido de su cuenta de administrador en un cortafuegos o servidor de gestión de Panorama de Palo Alto Network. Use la información del último inicio de sesión para determinar si alguien más inició sesión usando sus credenciales y use el indicador de intentos de inicio de sesión erróneos para determinar si su cuenta es blanco de un ataque de fuerza bruta.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Visualice los indicadores de actividad de inicio de sesión para controlar la actividad reciente de su cuenta.

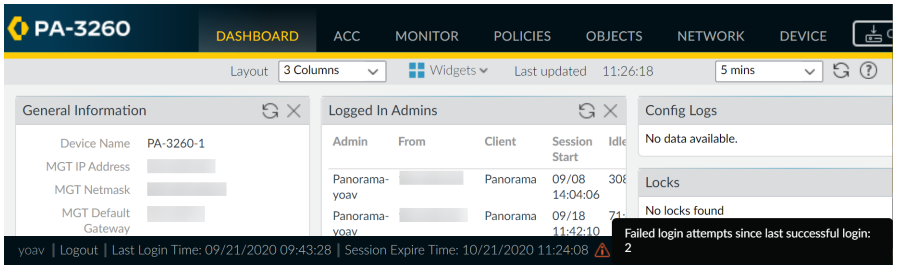
1. Inicie sesión en la interfaz web de su cortafuegos o servidor de gestión de Panorama.
2. Visualice los detalles del último inicio de sesión ubicados en el extremo inferior izquierdo de la ventana y verifique que la marca de tiempo corresponda a su último inicio de sesión.



3. Busca un símbolo de precaución a la derecha de la información de hora del último inicio de sesión para conocer los intentos erróneos de inicio de sesión.

   El indicador de inicio de sesión erróneo aparece si se produjeron uno o más intentos erróneos de inicio de sesión usando su cuenta desde el último inicio de sesión correcto.

   1. Si ve el símbolo de precaución, mueva el puntero sobre él para que aparezca la cantidad de intentos de inicio de sesión erróneos.



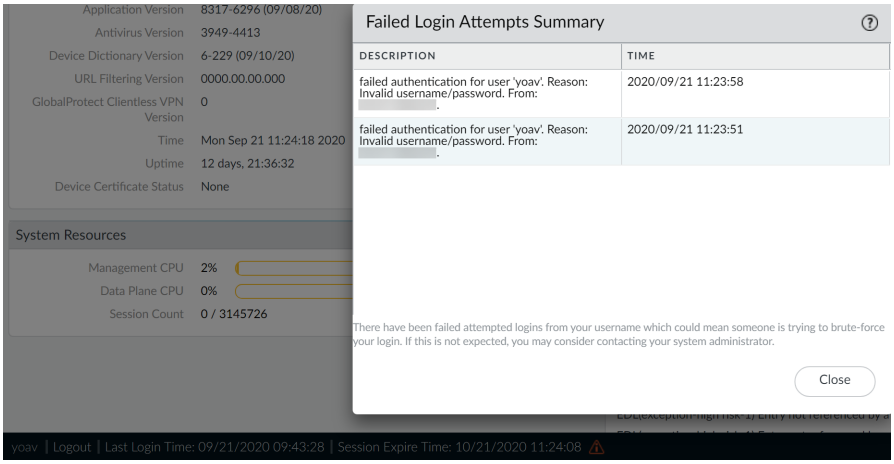
   2. Haga clic en el símbolo de precaución para ver el resumen de intentos de inicio de sesión erróneos. Los detalles incluyen el nombre de la cuenta admin, el motivo del error al iniciar sesión, la dirección IP de origen y la fecha y hora.

> *Después de iniciar sesión correctamente y luego cerrar sesión, el contador de inicio de sesión erróneo vuelve a cero por lo que verá los nuevos datos de inicio de sesión erróneo, si hubiera, la próxima vez que inicie sesión.*

STEP 2 | Busque los hosts que intentan constantemente iniciar sesión en su cortafuegos o servidor de gestión de Panorama.

1. Haga clic en el símbolo de precaución por inicio de sesión erróneo para ver el resumen de intentos de inicio de sesión erróneos.
2. Encuentre y registre la dirección IP de origen del host que intentó iniciar sesión. Por ejemplo, la siguiente figura muestra varios intentos fallidos de inicio de sesión.

© 2020 Palo Alto Networks, Inc.



3. Trabaje con su administrador de red para encontrar el usuario y host que están usando la dirección IP que identificó.

   Si no puede encontrar el sistema que está perpetrando el ataque de fuerza bruta, considere cambiar el nombre de la cuenta para evitar futuros ataques.

STEP 3 | Tome las siguientes medidas si detecta un peligro para la cuenta.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **Configuration (Configuración)** y vea el historial de cambios y confirmaciones de la configuración para determinar si su cuenta se utilizó para realizar cambios sin su conocimiento.
2. Seleccione **Device (Dispositivo)** > **Config Audit (Auditoría de configuraciones)** para comparar la configuración actual y la configuración que se ejecutaba antes de la configuración que sospecha que se modificó utilizando sus credenciales. También puede hacer esto usando Panorama.

   Si su cuenta de administrador se usó para crear una nueva cuenta, la realización de una auditoría de configuración lo ayudará también a detectar cambios que estén asociados con una cuenta no autorizada.
3. Revierta la configuración a una configuración conocida fiable si observa que los logs se borraron o si tiene dificultades para determinar si se realizaron cambios inadecuados con su cuenta.

   Antes de confirmar el restablecimiento de una configuración anterior, revísela para asegurarse de que contenga los ajustes correctos. Por ejemplo, es posible que la configuración a la que regrese no contenga cambios recientes, por lo que debe aplicar esos cambios después de confirmar la configuración de respaldo.

   Aplique las siguientes prácticas recomendadas para prevenir ataques de fuerza bruta en cuentas con privilegios.

   - *Limite la cantidad de intentos erróneos permitidos antes de que el cortafuegos bloquee una cuenta con privilegios configurando la cantidad de intentos fallidos y el tiempo de bloqueo (min) en el perfil de autenticación o en la configuración de autenticación para la interfaz de gestión (Device [Dispositivo] > Setup [Configuración] > Management [Gestión] > Authentication Settings [Configuración de autenticación]).*
   - Uso de los perfiles de gestión de interfaz para restringir el acceso.
   - *Aplique* contraseñas complejas *para las cuentas con privilegios.*

© 2020 Palo Alto Networks, Inc.

Gestión y supervisión de tareas administrativas

El gestor de tareas muestra detalles sobre todas las operaciones que usted y otros administradores iniciaron (tal como confirmaciones manuales) o que el cortafuegos inició (tal como la generación de informes programados) desde el último inicio del cortafuegos. Puede usar el gestor de tareas para solucionar problemas de operaciones erróneas, investigar advertencias asociadas a confirmaciones realizadas, visualizar detalles sobre confirmaciones en cola o cancelar confirmaciones pendientes.



También puede visualizar los logs del sistema para controlar los eventos del sistema en el cortafuegos o visualizar los logs de configuración para controlar los cambios de configuración del cortafuegos.

STEP 1 | Haga clic en **Tasks** en la parte inferior de la interfaz web.

STEP 2 | Seleccione **Show** para mostrar solo tareas **Running** (en curso) o seleccione **All** para mostrar todas las tareas (opción por defecto). O bien, filtre las tareas según el tipo:

- **Jobs**: confirmaciones iniciadas por el administrador, confirmaciones iniciadas por el cortafuegos y descargas e instalaciones de software o contenido.
- **Reports**: informes programados.
- **Log Requests (Solicitudes de log)**: las consultas de logs que activa al acceder a **Dashboard (Panel)** o a una página de **Monitor (Supervisor)**.

STEP 3 | Tome una de las siguientes medidas:

- **Display or hide task details**: por defecto, el gestor de tareas muestra el tipo, estado, hora de inicio y los mensajes para cada tarea. Para ver la hora de finalización y la ID de trabajo para una tarea, debe configurar manualmente la visualización para exponer esas columnas. Para mostrar u ocultar una columna, abra el menú desplegable en cualquier encabezado de columna, seleccione **Columns** y seleccione o elimine la selección de los nombres de columna según fuera necesario.
- **Investigate warnings or failures**: lea las entradas en la columna de mensajes para ver detalles de las tareas. Si la columna dice `Too many messages (Demasiados mensajes)`, haga clic en la entrada correspondiente del tipo de columna para ver más información.
- **Mostrar una descripción de confirmación**: si un administrador introdujo una descripción al configurar una confirmación, puede hacer clic en **Commit Description (Descripción de confirmación)** en la columna de mensajes para mostrar la descripción.
- **Check the position of a commit in the queue**: la columna de mensajes indica la posición en cola de las confirmaciones que están en curso.
- **Cancel pending commits**: haga clic en **Clear Commit Queue** para cancelar todas las confirmaciones pendientes (disponible únicamente para las funciones administrativas predefinidas). Para cancelar una confirmación individual, haga clic en la **x** de la columna Action para esa confirmación (la confirmación permanece en la cola hasta que el cortafuegos la quita de la cola). No puede cancelar confirmaciones que están en curso.

Confirmación, validación y previsualización de los cambios de configuración del cortafuegos

La confirmación es el proceso de activar los cambios pendientes en la configuración del cortafuegos. Puede filtrar los cambios pendientes mediante el administrador o la *ubicación* y luego previsualizar, validar o confirmar solo esos cambios. Las ubicaciones pueden ser sistemas virtuales específicos, políticas y objetos compartidos, o configuraciones de red y dispositivo compartidas.

© 2020 Palo Alto Networks, Inc.

El cortafuegos pone en cola las solicitudes de confirmación de modo que pueda iniciar una nueva confirmación mientras una confirmación previa está en progreso. El cortafuegos lleva a cabo la confirmación en el orden en que se iniciaron, pero prioriza las confirmaciones que el cortafuegos inicia automáticamente (como las actualizaciones de FQDN). No obstante, si la cola ya tiene el número máximo de confirmaciones iniciadas por el administrador, debe esperar que el cortafuegos finalice de procesar una confirmación pendiente antes de iniciar una nueva confirmación. Para cancelar las confirmaciones pendientes o visualizar los detalles sobre confirmaciones de estado, consulte Gestionar y supervisar tareas administrativas.

Cuando inicia una confirmación, el cortafuegos comprueba la validez de los cambios antes de activarlos. El resultado de la validación exhibe condiciones que bloquean la confirmación (errores) o que son importantes de conocer (advertencias). Por ejemplo, la validación podría indicar un destino de ruta no válido que debe fijar para que la confirmación se realice correctamente. La validación le permite encontrar y corregir errores antes de compilar (no realiza cambios en la configuración en ejecución). Esto es útil si tiene una fecha límite de compilación y quiere asegurarse de que la compilación funcionará sin errores.

Cuando están habilitados y administrados por un servidor de gestión Panorama ™, los cortafuegos gestionados prueban de forma local la configuración confirmada localmente o se envían desde Panorama para comprobar que los nuevos cambios no interrumpan la conexión entre Panorama y el cortafuegos gestionado. Si la configuración confirmada interrumpe la conexión entre Panorama y un cortafuegos gestionado, el cortafuegos rechaza automáticamente la confirmación y la configuración se revierte a la configuración anterior en ejecución. Además, los cortafuegos gestionados por un servidor de gestión Panorama prueban la conexión a Panorama cada 60 minutos y si esos cortafuegos detectan que ya no puede conectarse correctamente a Panorama, revertirán su configuración a la configuración anterior en ejecución.



Las operaciones de confirmar, validar, previsualizar, guardar y revertir se aplican solo a los cambios realizados después de la última confirmación. Para restaurar las configuraciones al estado en que estaban antes de la última confirmación, debe cargar una configuración con copia de respaldo previa.

Para evitar que varios administradores realicen cambios de configuración durante sesiones concurrentes, consulte Gestión de bloqueos para restringir cambios de configuración.

STEP 1 | Configure el alcance de los cambios de configuración que confirmará, validará o previsualizará.

1. Haga clic en **Commit (Compilar)** en la parte superior de la interfaz web.
2. Seleccione una de las siguientes opciones:
   - **Commit All Changes (Confirmar todos los cambios)** (predeterminada): se aplica a todos los cambios para los cuales usted posee privilegios administrativos. Usted no puede filtrar manualmente el alcance de la confirmación cuando selecciona esta opción. En lugar de eso, la función de administrador asignada a la cuenta que utilizó para iniciar sesión determina el alcance de la confirmación.
   - **Commit Changes Made By (Confirmar los cambios realizados por)**: le permite filtrar el alcance de la confirmación según el administrador o ubicación. La función administrativa asignada a la cuenta que usted utilizó para iniciar sesión determina qué cambios puede filtrar.

   Para confirmar los cambios de otros administradores, la cuenta que utilizó para iniciar sesión debe estar asignada a la función de superusuario o un perfil de rol de administrador *con el privilegio Commit For Other Admins (Confirmar para otros administradores) habilitado.*
3. (Opcional) Para filtrar el alcance de la confirmación mediante el administrador, seleccione **Commit Changes Made By (Confirmar cambios realizados por)**, haga clic en el enlace adyacente, seleccione los administradores y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

4. (Opcional) Para filtrar por ubicación, seleccione **Commit Changes Made By (Confirmar cambios realizados por)** y borre los cambios que desee excluir del alcance de la confirmación.



Si las dependencias entre los cambios de configuración que incluyó y excluyó producen un error de validación, realice la confirmación con todos los cambios incluidos. Por ejemplo, cuando confirma cambios en un sistema virtual, debe incluir los cambios de todos los administradores que añadieron, eliminaron o reposicionaron reglas para la misma base de reglas en ese sistema virtual.

STEP 2 | Previsualice los cambios que la confirmación activará.

Esto puede ser útil si, por ejemplo, usted no recuerda todos los cambios y no está seguro de que desee activar todos.

Permite comparar las configuraciones seleccionadas en Commit Scope (Ámbito de compilación) con la configuración en ejecución. La ventana de previsualización muestra las configuraciones en paralelo y utiliza codificación por color para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo).

Seleccione **Preview Changes (Previsualizar los cambios)** y seleccione las **Lines of Context (Líneas de contexto)**, que es la cantidad de líneas de los archivos de configuración comparados que se mostrarán antes y después de cada diferencia resaltada. Estas líneas adicionales pueden ayudarlo a correlacionar los resultados de previsualización con las configuraciones de la interfaz web. Cierre la ventana de previsualización cuando termine de revisar los cambios.



Debido a que la vista previa se muestra en una nueva ventana del navegador, este debe permitir ventanas emergentes. Si la ventana de vista previa no se abre, consulte la documentación de su navegador para ver los pasos para permitir ventanas emergentes.

STEP 3 | Previsualice los ajustes individuales en los que está confirmando cambios.

Esto puede ser útil si desea conocer detalles sobre los cambios, tales como los tipos de configuraciones y quiénes las cambiaron.

1. Haga clic en **Change Summary (Cambiar el resumen)**.
2. (Opcional) **Group By (Agrupar por)** un nombre de columna (tal como el **Type [Tipo]** de configuración).
3. Seleccione **Close (Cerrar)** el cuadro de diálogo Change Summary (Cambiar resumen) para terminar de revisar los cambios.

STEP 4 | Valide los cambios antes de confirmarlos para asegurarse de que la confirmación se realizará correctamente.

1. Seleccione **Validate Changes (Validar los cambios)**.

   Los resultados mostrarán todos los errores y advertencias que mostraría una confirmación real.
2. Resuelva todos los errores que los resultados de la validación identifiquen

STEP 5 | Confirme sus cambios de configuración.

Seleccione **Commit (Confirmar)** para confirmar los cambios a fin de validarlos y activarlos.



Para ver los detalles sobre las confirmaciones pendientes (que aún puede cancelar), en curso, completadas o fallidas, consulte Gestionar y supervisar las tareas administrativas*.*

© 2020 Palo Alto Networks, Inc.

Exportación de los datos de la tabla de configuración

Exporte reglas de la política, objetos de configuración y firmas de IPS desde Panorama™ y los cortafuegos para demostrar el cumplimiento de las normativas a auditores externos, para realizar revisiones periódicas de la configuración del cortafuegos y para generar informes de las políticas de cortafuegos. Esto evita que deba brindarles a los auditores acceso directo a sus cortafuegos y dispositivos para realizar capturas de pantalla o acceder a la API XML a fin de generar informes de configuración. En la interfaz web, puede exportar los datos de la tabla de configuración para la configuración de políticas, objetos, redes, cortafuegos y Panorama, además de las excepciones de las firmas en los perfiles de seguridad de antivirus, antispyware y protección frente a vulnerabilidades en un archivo PFD o CSV.

La exportación de la tabla de configuración funciona como una impresión; no puede importar archivos generados nuevamente a Panorama o el cortafuegos. Cuando exporta los datos como un archivo PDF y los datos de la tabla superan las 50 000 filas, los datos se dividen en varios archivos PDF (por ejemplo, <report-name>_part1.pdf y <report-name>_part2.pdf). Cuando exporta datos como un archivo CSV, los datos se exportan en un solo archivo. Estos formatos de exportación le permiten aplicar filtros que coinciden con sus criterios de informe y buscar en los informes en PDF para encontrar datos específicos con rapidez. Además, cuando exporta los datos de la tabla de configuración, se genera un log de sistema para registrar el evento.

STEP 1 | Inicie la interfaz web e identifique los datos de configuración que debe exportar.

STEP 2 | Aplique los filtros necesarios para producir los datos de configuración que debe exportar y haga clic en **PDF/CSV**.



STEP 3 | Configure el informe de exportación de la tabla de configuración:

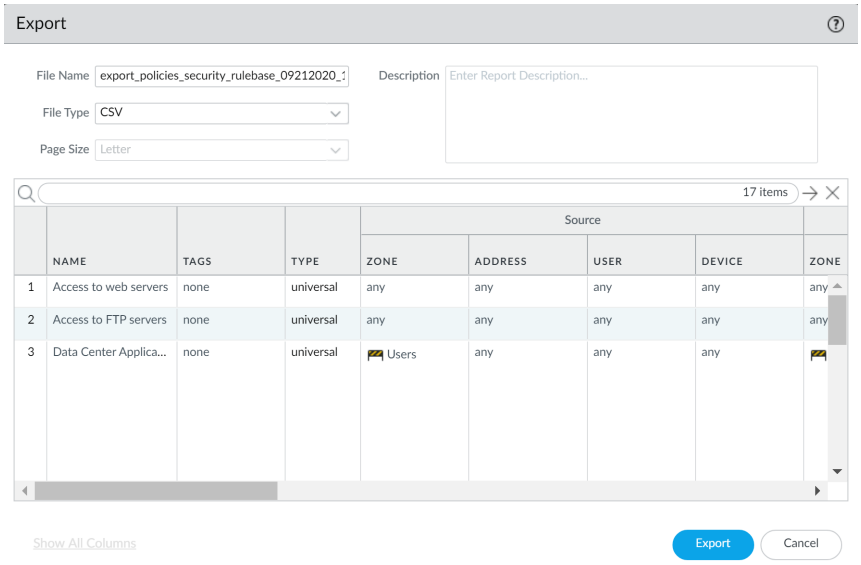
1. Introduzca el **File Name (Nombre de archivo)**.
2. Seleccione el **File Type (Tipo de archivo)**.
3. (Opcional) Introduzca una Description (Descripción) para el informe.
4. Confirme que los datos de la tabla de configuración coincidan con los filtros aplicados.

Seleccione Show All Columns (Mostrar todas las columnas) para mostrar todos los filtros aplicados.

STEP 4 | Haga clic en **Export (Exportar)** para exportar los datos de la tabla de configuración.

La exportación de la tabla de configuración funciona como una impresión; no puede importar archivos generados nuevamente a Panorama o el cortafuegos.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Seleccione una ubicación para guardar el archivo exportado.

Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama

Global Find (Búsqueda global) permite buscar en la configuración candidata de un cortafuegos o de Panorama una cadena concreta, como una dirección IP; el nombre de un objeto, de una regla de política o de una aplicación; una ID de amenaza o un identificador único universal (universal unique identifier, UUID). Además de buscar objetos de configuración y configuraciones, puede buscar por ID de trabajo o tipo de trabajo en el caso de las confirmaciones manuales que realizan los administradores o las confirmaciones automáticas que realiza el cortafuegos o Panorama. Los resultados de búsqueda se agrupan por categoría y proporcionan enlaces a la ubicación de la configuración en la interfaz web, de modo que pueda encontrar fácilmente todos los lugares donde se hace referencia a la cadena. Los resultados de la búsqueda también le ayudan a identificar otros objetos que dependen de o hacen referencia al término o la cadena de búsqueda. Por ejemplo, cuando deje de usar un perfil de seguridad, escriba el nombre del perfil en la búsqueda global para encontrar todas las instancias del perfil y haga clic en cada instancia para navegar hacia la página de configuración y realizar el cambio necesario. Cuando haya eliminado todas las referencias, podrá eliminar el perfil. Puede hacer esto con cualquier elemento de configuración que tenga dependencias.

Ver el vídeo.

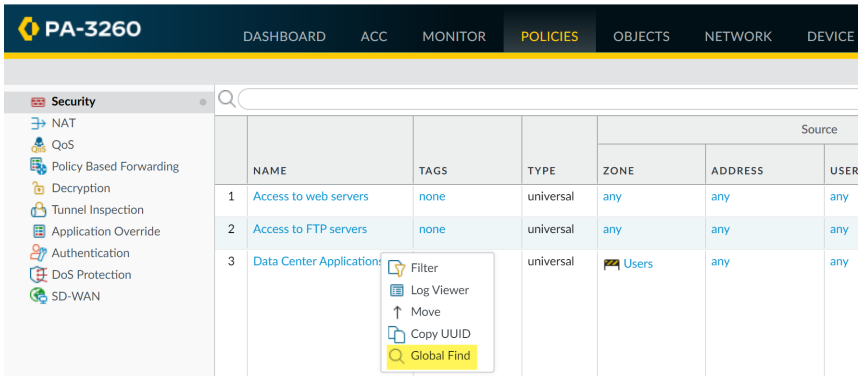
La búsqueda global no buscará contenido dinámico (como logs, intervalos de direcciones o direcciones DHPC asignadas). En el caso de DHCP, puede buscar un atributo de servidor DHCP, como la entrada DNS, pero no puede buscar direcciones individuales asignadas a usuarios. La búsqueda global tampoco busca nombre de usuarios individuales o grupos identificados por User-ID a menos que el usuario/grupo se defina en una política. Por lo general, solamente puede buscar contenido que el cortafuegos escriba en la configuración.

- Inicie la búsqueda global haciendo clic en el icono **Search (Buscar)** que se encuentra en la esquina superior derecha de la interfaz web.

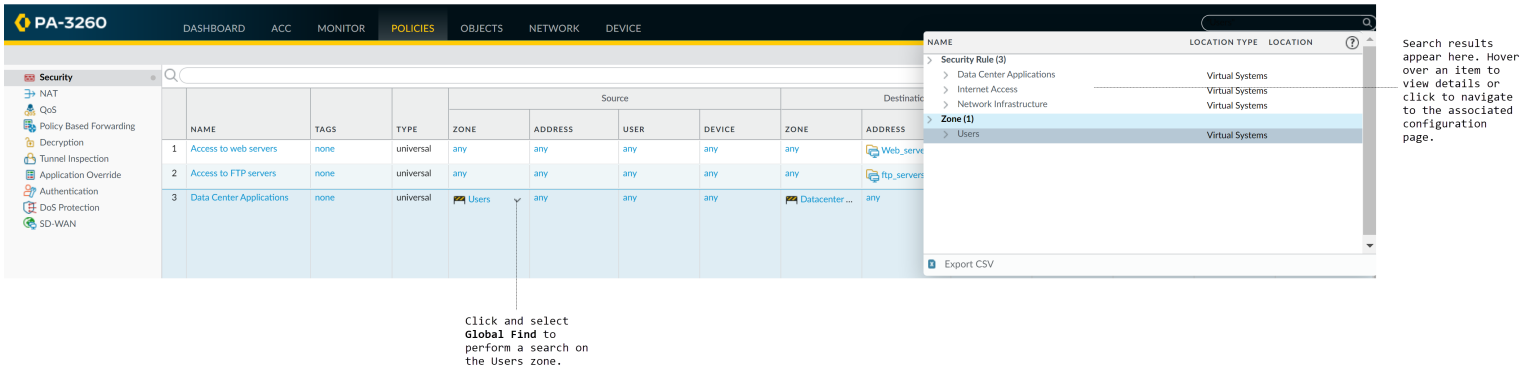
© 2020 Palo Alto Networks, Inc.



- Para acceder a la función de búsqueda global desde el interior de un área de configuración, haga clic en la lista desplegable situada junto a un elemento y seleccione **Global Find (Búsqueda global)**:



Por ejemplo, haga clic en **Global Find (Búsqueda global)** en una zona denominada **Users (Usuarios)** para buscar la configuración candidata para cada ubicación donde se haga referencia a la zona. La captura de pantalla siguiente muestra los resultados de búsqueda de la zona Users (Usuarios):



Sugerencias de búsqueda:

- Si inicia una búsqueda en un cortafuegos con varios sistemas virtuales habilitados o si los Tipos de funciones administrativas personalizados están definidos, la búsqueda global solamente devolverá resultados de las áreas del cortafuegos para las que el administrador tenga permisos. Lo mismo ocurre con los grupos de dispositivos de Panorama.
- Los espacios de los términos de búsqueda se tratan como operaciones AND. Por ejemplo, si busca **`política corporativa`**, los resultados de la búsqueda incluirán casos en los que tanto la palabra política como la palabra corporativa existen en la configuración.
- Para encontrar una frase exacta, indíquela entre comillas.
- Para volver a ejecutar una búsqueda anterior, haga clic en el icono de búsqueda (situado en la parte superior derecha de la interfaz web) y aparecerá una lista con las últimas 20 búsquedas. Haga clic en un elemento de la lista para volver a ejecutar dicha búsqueda. El historial de búsqueda es exclusivo de cada cuenta de administrador.
- Para buscar un UUID, debe copiarlo y pegarlo.

© 2020 Palo Alto Networks, Inc.

Gestión de bloqueos para restringir cambios de configuración

Puede utilizar bloqueos de configuración para evitar que otros administradores cambien la configuración del candidato o confirmen cambios en la configuración hasta que elimine manualmente el bloqueo o el cortafuegos lo elimine automáticamente (tras una confirmación). Los bloqueos garantizan que los administradores no realicen cambios conflictivos para los mismos ajustes o para ajustes interdependientes durante sesiones iniciadas simultáneas.

El cortafuegos coloca en cola las solicitudes de confirmación y las lleva a cabo en el orden en que los administradores las hayan iniciado. Para obtener información detallada, consulte Confirmación, validación y previsualización de los cambios de configuración del cortafuegos. *Para ver el estado de las confirmaciones en cola, consulte* Gestión y supervisión de tareas administrativas.

- Visualice detalles sobre los bloqueos actuales.

  Por ejemplo, puede comprobar si otros administradores configuraron bloqueos y leer los comentarios que introdujeron para explicar los bloqueos.

  Haga clic en el icono de bloqueo en la parte superior de la interfaz web. Un número adyacente indica la cantidad de bloqueos actuales.

- Bloquee una configuración.
  1. Haga clic en el icono de bloqueo en la parte superior de la interfaz web.

     La imagen del bloqueo varía en función de si existen bloqueos existentes configurados o no configurados.
  2. Seleccione **Take a Lock** para seleccionar un bloqueo y luego seleccione el tipo de bloqueo en **Type**:
     - **Config**: bloquea los cambios en la configuración candidata por parte de otros administradores.
     - **Commit (Confirmación)**: impide que otros administradores confirmen cambios en la configuración candidata.
  3. (Cortafuegos con varios sistemas virtuales únicamente) Seleccione una ubicación en **Location** para bloquear la configuración para un sistema virtual específico o **Shared** para seleccionar la ubicación compartida.
  4. (Opcional) Como práctica recomendada, introduzca un comentario en **Comment** para que otros administradores comprendan el motivo del bloqueo.
  5. Haga clic en **OK (Aceptar)** y **Close (Cerrar)**.

- Desbloquee una configuración.

  Solo un superusuario o el administrador que bloqueó la configuración pueden desbloquearla manualmente. Sin embargo, el cortafuegos elimina automáticamente un bloqueo después de completar la operación de confirmación.

  1. Haga clic en el icono de bloqueo en la parte superior de la interfaz web.
  2. Seleccione la entrada de bloqueo de la lista.
  3. Haga clic en **Remove Lock (Eliminar bloqueo)**, **OK (Aceptar)** y **Close (Cerrar)**.

- Configure el cortafuegos para aplicar automáticamente un bloqueo de confirmación cuando cambie la configuración candidata. Este ajuste se aplica a todos los administradores.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite {0>General Settings (Configuración general)<0}.
2. Seleccione **Automatically Acquire Commit Lock (Obtener bloqueo de compilación automáticamente)** y luego haga clic en **OK (Aceptar)** y **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Gestión de las copias de seguridad de la configuración

La configuración en ejecución en el cortafuegos abarca todos los ajustes que ha confirmado y que, por lo tanto, están activos, tales como las reglas de la política que actualmente bloquean o permiten diferentes tipos de tráfico en la red. La configuración candidata es una copia de la configuración que se está ejecutando más las modificaciones inactivas que ha realizado después de la última confirmación. Si realiza una copia de seguridad de las versiones de la configuración candidata o en ejecución, permite que luego se puedan restaurar esas versiones. Por ejemplo, si una validación de confirmación muestra que la configuración candidata actual tiene más errores que los que desea reparar, puede restaurarla a una configuración candidata anterior. También puede volver a la configuración en ejecución actual sin guardar una copia de seguridad antes. Si debe exportar partes específicas de la configuración para una revisión o auditoría interna, puede realizar la Exportación de los datos de la tabla de configuración.

Consulte Confirmación, validación y previsualización de los cambios de configuración del cortafuegos *para obtener información detallada sobre las operaciones de confirmación.*

- Guardado y exportación de configuraciones de cortafuegos
- Reversión de los cambios de configuración del cortafuegos

Guardado y exportación de configuraciones de cortafuegos

El guardar una copia de seguridad de la configuración candidata en almacenamiento permanente en el cortafuegos le permite revertir los ajustes más tarde a esa copia de seguridad (consulte Reversión de los cambios de configuración del cortafuegos). Esto resulta útil para preservar los cambios que, de lo contrario, se perderían si un evento del sistema o una acción del administrador hacen que el cortafuegos se reinicie. Después del reinicio, PAN-OS automáticamente regresa a la versión actual de la configuración en ejecución, que el cortafuegos almacena en un archivo denominado running-config.xml. El guardar copias de seguridad también resulta útil si desea revertir los ajustes a una configuración del cortafuegos que es anterior a la configuración actual en ejecución. El cortafuegos no guarda automáticamente la configuración candidata en el almacenamiento permanente. Debe guardar la configuración candidata manualmente como un archivo de instantánea predeterminado (.snapshot.xml) o como un archivo de instantánea con un nombre personalizado. El cortafuegos almacena el archivo de instantánea a nivel local, pero usted puede exportarlo a un host externo.

No es necesario que guarde una copia de seguridad de la configuración para revertir los cambios realizados desde la última confirmación o reinicio; simplemente seleccione Config (Configuración) > Revert Changes (Revertir cambios) (consulte Reversión de los cambios de configuración del cortafuegos*).*

Cuando edita un ajuste y hace clic en OK, el cortafuegos actualiza la configuración candidata, pero no guarda la instantánea de la copia de seguridad.

Además, el guardar los cambios no los activa. Para activar los cambios, realice una confirmación (consulte Confirmación, validación y previsualización de los cambios de configuración del cortafuegos*).*

Palo Alto Networks le recomienda crear la copia de seguridad de cualquier configuración importante en un host externo al cortafuegos.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Guarde la instantánea de la copia de seguridad de la configuración candidata si contiene cambios que desea preservar en caso de que el cortafuegos se reinicie.

Estos son cambios que no está listo para confirmar; por ejemplo, cambios que no puede finalizar en la sesión iniciada actual.

Para sobrescribir el archivo de instantánea predeterminado (.snapshot.xml), realice alguno de los siguientes pasos:

- Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Save candidate configuration (Guardar configuración candidata)**.
- Inicie sesión en el cortafuegos con una cuenta administrativa asignada a la función de superusuario o un perfil de rol de administrador con el privilegio **Save For Other Admins (Guardar para otros administradores)** habilitado. Luego seleccione **Config (Configuración)Save Changes (Guardar cambios)** en la parte superior de la interfaz web, seleccione **Save All Changes (Guardar todos los cambios)** y **Save (Guardar)**.

Para crear una instantánea que incluya todos los cambios que los administradores realizaron, pero sin sobrescribir el archivo de instantánea predeterminado:

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Save named configuration snapshot (Guardar instantánea de configuración con nombre)**.
2. En **Name (Nombre)**, especifique el nombre de un archivo de configuración nuevo o existente.
3. Haga clic en **OK (Aceptar)** y **Close (Cerrar)**.

Para guardar solo los cambios específicos de la configuración candidata sin sobrescribir ninguna parte del archivo de instantánea predeterminado:

1. Inicie sesión en el cortafuegos con una cuenta administrativa que tenga los privilegios de rol necesarios para guardar los cambios deseados.
2. Seleccione **Config (Configuración)** > **Save Changes (Guardar cambios)** en la parte superior de la interfaz web.
3. Seleccione **Save Changes Made By (Guardar cambios realizados por)**.
4. Para filtrar el alcance del guardado por administrador, haga clic en **<administrator-name>**, selecciónelo y haga clic en **OK (Aceptar)**.
5. Para filtrar el alcance del guardado por ubicación, borre las ubicaciones que desee excluir. Las ubicaciones pueden ser sistemas virtuales específicos, políticas y objetos compartidos, o configuraciones de red y dispositivo compartidas.
6. Haga clic en **Save (Guardar)**, especifique el **Name (Nombre)** de un archivo de configuración nuevo o existente, y haga clic en **OK (Aceptar)**.

STEP 2 | Exporte una configuración candidata, una configuración en ejecución o la información de estado del cortafuegos a un host externo al él.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en la opción de exportación:

- **Export named configuration snapshot (Exportar instantánea de configuración con nombre)**: exporte la configuración en ejecución actual, una instantánea de la configuración candidata con nombre o una configuración importada anteriormente (candidata o en ejecución). El cortafuegos exporta la configuración como un archivo XML con el **nombre** especificado.
- **Export configuration version**: seleccione una **versión** de la configuración en ejecución para exportar como archivo XML. El cortafuegos crea una versión siempre que confirme los cambios de configuración.
- **Export device state (Exportar estado de dispositivo)**: exporta la información de estado del cortafuegos como un lote. Además de la configuración en ejecución, la información de estado incluye la configuración de plantillas y grupos de dispositivos enviados desde Panorama. Si el cortafuegos es un portal de GlobalProtect, la información también incluye información del certificado, una lista de

© 2020 Palo Alto Networks, Inc.

satélites y la información de autenticación del satélite. Si reemplaza un cortafuegos o portal, puede restaurar la información exportada en el reemplazo importante el lote de estado.

Reversión de los cambios de configuración del cortafuegos

Las operaciones de reversión reemplazan los ajustes de la configuración candidata actual por los ajustes de otra configuración. La reversión de cambios es útil cuando desea deshacer los cambios de varios ajustes como una misma operación, en lugar de reconfigurar manualmente cada ajuste.

Puede revertir los cambios pendientes que se realizaron a la configuración del cortafuegos desde la última vez que se guardaron los cambios. El cortafuegos ofrece la opción de filtrar los cambios pendientes por administrador o por *ubicación*. Las ubicaciones pueden ser sistemas virtuales específicos, políticas y objetos compartidos, o configuraciones de red y dispositivo compartidas. Si usted guardó un archivo de instantánea para una configuración candidata que sea anterior a la configuración actual en ejecución (consulte Guardado y exportación de configuraciones de cortafuegos), también puede revertir los ajustes a esa instantánea. Al revertir a una instantánea usted puede restaurar una configuración candidata que existía antes de la última vez que se guardaron los cambios. El cortafuegos automáticamente guarda una nueva versión de la configuración en ejecución siempre que usted confirma los cambios y puede restaurar cualquiera de estas versiones.

- Revierta a la configuración actual en ejecución (archivo de nombre running-config.xml).

  Esta operación deshace todos los cambios que realizó a la configuración desde la última confirmación.

  Para revertir todos los cambios que realizaron los administradores, realice alguno de los siguientes pasos:

  - Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones), Revert to running configuration (Revertir a la configuración en ejecución)** y haga clic en **Yes (Sí)** para confirmar la operación.
  - Inicie sesión en el cortafuegos con una cuenta administrativa asignada a la función de superusuario o un perfil de rol de administrador con el privilegio **Commit For Other Admins (Confirmar para otros administradores)** habilitado. Luego seleccione **Config (Configuración)Revert Changes (Revertir cambios)** en la parte superior de la interfaz web, seleccione **Revert All Changes (Revertir todos los cambios)** y **Revert (Revertir)**.

  Para revertir solo cambios específicos a la configuración candidata:

  1. Inicie sesión en el cortafuegos con una cuenta administrativa que tenga los privilegios de rol necesarios para revertir los cambios deseados.

     Los privilegios que controlan las operaciones de confirmación también controlan las operaciones de reversión.
  2. Seleccione **Config (Configuración)** > **Revert Changes (Revertir cambios)** en la parte superior de la interfaz web.
  3. Seleccione **Revert Changes Made By (Revertir cambios realizados por)**.
  4. Para filtrar el alcance de la reversión por administrador, haga clic en **<administrator-name>**, selecciónelo y haga clic en **OK (Aceptar)**.
  5. Para filtrar el alcance de la reversión por ubicación, borre las ubicaciones que desee excluir.
  6. Seleccione **Revert (Revertir)** para revertir los cambios.

- Revierta los ajustes a la instantánea predeterminada de la configuración candidata.

  Esta es la instantánea que crea o sobrescribe cuando hace clic en **Config** > **Save Changes (Guardar cambios)** en la parte superior de la interfaz web.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Revert to last saved configuration (Revertir a la última configuración guardada)**.
2. Haga clic en **Yes (Sí)** para confirmar la operación.
3. (Opcional) Haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con la instantánea.

- Restaure una versión previa de la configuración en ejecución que se almacena en el cortafuegos.

  El cortafuegos crea una versión siempre que confirme los cambios de configuración.

  1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Load configuration version (Cargar versión de la configuración)**.
  2. Seleccione una versión de la configuración en **Version** y haga clic en **OK**.
  3. (Opcional) Haga clic en **Commit** para sobrescribir la configuración en ejecución con la versión que acaba de restaurar.

- Puede revertir a una de las siguientes opciones:
  - La versión con nombre personalizado de la configuración en ejecución que importó previamente.
  - Instantánea de la configuración candidata con nombre personalizado (en lugar de la instantánea por defecto).

  1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y haga clic en **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**.
  2. Seleccione el **nombre** de la instantánea y haga clic en **OK**.
  3. (Opcional) Haga clic en **Commit (Confirmar)** para sobrescribir la configuración en ejecución con la instantánea.

- Puede revertir los ajustes a una configuración en ejecución o candidata que haya exportado previamente a un host externo.
  1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import named configuration snapshot (Importar instantánea de configuración con nombre)** y en **Browse (Examinar)** para buscar el archivo de configuración en el host externo y, por último, haga clic en **OK (Aceptar)**.
  2. Haga clic en **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**, seleccione el **Name (Nombre)** del archivo de configuración que acaba de importar, y haga clic en **OK (Aceptar)**.
  3. (Opcional) Haga clic en **Commit** para sobrescribir la configuración en ejecución con la instantánea que acaba de importar.

- Restaure la información de estado que exportó de un cortafuegos.

  Además de la configuración en ejecución, la información de estado incluye la configuración de plantillas y grupos de dispositivos enviados desde Panorama. Si el cortafuegos es un portal de GlobalProtect, la información también incluye información del certificado, una lista de satélites y la información de autenticación del satélite. Si reemplaza un cortafuegos o portal, puede restaurar la información en el reemplazo importante el lote de estado.

  Importe la información de estado:

  1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**, haga clic en **Import device state (Importar estado de dispositivo)**, seleccione **Browse (Examinar)** para buscar el lote de estado y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

2. (Opcional) Haga clic en **Commit (Confirmar)** para aplicar la información de estado importada a la configuración en ejecución.

© 2020 Palo Alto Networks, Inc.

Gestión de los administradores de cortafuegos

Las cuentas administrativas especifican funciones y métodos de autenticación para los administradores de cortafuegos de Palo Alto Networks. Todos los cortafuegos de Palo Alto Networks vienen preconfigurados con una cuenta administrativa predeterminada (admin) que proporciona acceso completo de lectura-escritura (también conocido como acceso de superusuario) al cortafuegos.



Es recomendable que cree una cuenta administrativa diferente para cada persona que necesite acceder a las funciones de administración o creación de informes del cortafuegos. Esto le permite proteger mejor el cortafuegos de una configuración no autorizada y realizar el logging de las acciones de cada uno de los administradores individuales. Asegúrese de respetar las recomendaciones de las Prácticas recomendadas para proteger el acceso administrativo *para garantizar la seguridad del acceso administrativo a sus cortafuegos y otros dispositivos de seguridad, de modo que evite ataques eficaces.*

- Tipos de funciones administrativas
- Configuración de un perfil de función de administrador
- Autenticación administrativa
- Configurar cuentas y autenticación administrativa

Tipos de funciones administrativas

Una *función* define el tipo de acceso al sistema que tiene el administrador asociado. Estos son los tipos de administrador:

- **Basado en funciones**: funciones personalizadas que puede configurar para ofrecer un control de acceso más pormenorizado sobre las áreas funcionales de la interfaz web, la CLI y la API XML. Por ejemplo, puede crear un perfil de función de administrador para su personal de operaciones que proporcione acceso a las áreas de configuración de red y dispositivo de la interfaz web y un perfil separado para los administradores de seguridad que proporcione acceso a la definición de política de seguridad, logs e informes. En un cortafuegos con múltiples sistemas virtuales, puede seleccionar si la función define el acceso a todos los sistemas virtuales o a sistemas virtuales específicos. Cuando se añaden nuevas funciones al producto, usted debe actualizar las funciones con los correspondientes privilegios de acceso: el cortafuegos no añade automáticamente nuevas funciones a las definiciones de función personalizadas. Si desea información detallada sobre los privilegios que puede configurar para las funciones de administrador personalizado, consulte Referencia: Acceso de administrador a la interfaz web.
- **Dinámico**: funciones integradas que franquean el acceso al cortafuegos. Al añadir nuevas funciones, el cortafuegos actualiza automáticamente las definiciones de funciones dinámicas; usted no necesitará actualizarlas manualmente en ningún momento. En la siguiente tabla se enumeran los privilegios de acceso asociados con las funciones dinámicas.

Función dinámica	Privilegios
Superusuario	Tiene acceso completo al cortafuegos y puede definir nuevas cuentas de administrador y sistemas virtuales. Debe tener privilegios de superusuario para crear un usuario administrativo con esos mismos privilegios.
Superusuario (solo lectura)	Acceso de solo lectura al cortafuegos.

© 2020 Palo Alto Networks, Inc.

Función dinámica	Privilegios
Administrador de dispositivo	Acceso completo a todas las configuraciones del cortafuegos, excepto para definir nuevas cuentas o sistemas virtuales.
Administrador de dispositivo (solo lectura)	Acceso de solo lectura a todos los ajustes del cortafuegos, excepto a los perfiles de contraseña (sin acceso) y a las cuentas del administrador (solo está visible la cuenta con sesión iniciada).
Administrador del sistema virtual	Acceso a determinados sistemas virtuales del cortafuegos para crear y gestionar aspectos concretos de dichos sistemas. Los administradores de sistemas virtuales no tienen acceso a las interfaces de red, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de IPSec, los túneles de GRE, los perfiles de red, el proxy DNS, DHCP, QoS ni LLDP.
Administrador del sistema virtual (solo lectura)	Acceso de solo lectura a determinados sistemas virtuales del cortafuegos y a aspectos concretos de dichos sistemas. Los administradores de sistemas virtuales con acceso de solo lectura no tienen acceso a las interfaces de red, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de IPSec, los túneles de GRE, los perfiles de red, el proxy DNS, DHCP, QoS ni LLDP.

Configuración de un perfil de función de administrador

Los perfiles de función de administrador le permiten definir privilegios de acceso administrativo granulares que garantizan la protección de información confidencial de su compañía y la privacidad de los usuarios finales.



Se recomienda crear perfiles de función de administrador que permitan a los administradores acceder únicamente a las áreas de las interfaces de gestión que necesitan para realizar su trabajo.

STEP 1 | Seleccione **Device (Dispositivo)** > **Admin Roles (Funciones de administración)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca en **Name** un nombre para identificar la función.

STEP 3 | Para el entorno de la función en **Role (Función)**, seleccione **Device (Dispositivo)** o **Virtual System (Sistema virtual)**.

STEP 4 | En las pestañas **Web UI (Interfaz web)** y **REST API (API de REST)**, haga clic en el icono de cada área funcional para alternar al ajuste deseado: Enable (Habilitar), Read Only (Solo lectura) o Disable. (Deshabilitar). Para la pestaña **XML API (API de XML)**, seleccione Enable (Habilitar) o Disable (Deshabilitar). Si desea información detallada de las opciones de **Web UI (Interfaz web)**, consulte los Privilegios de acceso a la interfaz web.

STEP 5 | Seleccione la pestaña **Command Line (Línea de comando)** y seleccione una opción de acceso al CLI. El ámbito de **Role** controla las opciones disponibles:

- Función **Device (Dispositivo)**: **superuser**, **superreader**, **deviceadmin**, **devicereader** o **None**.
- Función **Virtual System**: **vsysadmin**, **vsysreader** o **None**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 7 | Asigne la función a un administrador. Consulte la Configuración de una cuenta administrativa de cortafuegos.

Autenticación administrativa

Puede configurar los siguientes tipos de autenticación y autorización (asignación de dominio de función y acceso) para los administradores del cortafuegos:

Authentication Method	Método de autorización	Description (Descripción)
Local	Local	Las credenciales de la cuenta de administrador y los mecanismos de autenticación se encuentran en el cortafuegos. Puede definir las cuentas con o sin un base de datos de usuarios en el cortafuegos. Consulte Autenticación local para obtener información sobre las ventajas y las desventadas de utilizar una base de datos local. Puede utilizar el cortafuegos para gestionar las asignaciones de las funciones, pero los dominios de acceso no son compatibles. Para obtener los detalles, consulte Configuración de la autenticación local o externa para los administradores del cortafuegos.
Claves SSH	Local	Las cuentas administrativas se encuentran en el cortafuegos, pero la autenticación de la CLI se realiza en función de las claves SSH. Puede utilizar el cortafuegos para gestionar las asignaciones de las funciones, pero los dominios de acceso no son compatibles. Para obtener los detalles, consulte Configuración de la autenticación de administrador basada en claves de SSH para el CLI.
certificates	Local	Las cuentas administrativas se encuentran en el cortafuegos, pero la autenticación de la interfaz web se realiza en función de los certificados de los clientes. Puede utilizar el cortafuegos para gestionar las asignaciones de las funciones, pero los dominios de acceso no son compatibles. Para obtener los detalles, consulte Configuración de la autenticación de administrador basada en certificados para la interfaz web.
Servicio externo	Local	Las cuentas administrativas que define localmente en el cortafuegos funcionan como referencias de las cuentas definidas en un servidor de autenticación multifactor, SAML, Kerberos, TACACS+, RADIUS o LDAP externo. El servidor externo realiza la autenticación. Puede utilizar el cortafuegos para gestionar las asignaciones de las funciones, pero los dominios de acceso no son compatibles. Para obtener los detalles, consulte Configuración de la autenticación local o externa para los administradores del cortafuegos.
Servicio externo	Servicio externo	Las cuentas administrativas se definen en un servidor SAML, TACACS+ o RADIUS externo. El servidor realiza la autenticación y la autorización. En el caso de la autorización, puede definir los Vendor-Specific Attributes (Atributos específicos del proveedor, VSA) en el servidor TACACS+ o RADIUS, o los atributos SAML en el servidor SAML. PAN-OS asigna los atributos a las funciones del administrador, los dominios

© 2020 Palo Alto Networks, Inc.

Authentication Method	Método de autorización	Description (Descripción)
		de acceso, los grupos de usuario y los sistemas virtuales que define en el cortafuegos. Para obtener los detalles, consulte: • Configuración de la autenticación SAML • Configuración de la autenticación TACACS+ • Configuración de la autenticación RADIUS

Configurar cuentas y autenticación administrativa

Si ya configuró un perfil de autenticación (consulte la Configuración de una secuencia y perfil de autenticación) o si no necesita uno para autenticar a los administradores, se encuentra listo para realizar la Configuración de una cuenta administrativa del cortafuegos. De lo contrario, realice uno de los siguientes procedimientos que se enumeran a continuación para configurar cuentas administrativas para tipos específicos de autenticación.

- Configuración de una cuenta administrativa del cortafuegos.
- Configuración de la autenticación local o externa para los administradores del cortafuegos.
- Configuración de una autenticación de administrador basada en certificados en la interfaz web
- Configuración de la autenticación de administrador basada en claves de SSH para el CLI
- Configuración de la vigencia de las claves de las API

Configuración de una cuenta administrativa del cortafuegos.

Las cuentas administrativas especifican funciones y métodos de autenticación para los administradores de cortafuegos. El servicio que utiliza para asignar funciones y realizar la autenticación determina si añade las cuentas al cortafuegos, a un servidor externo o a ambos (consulte Autenticación administrativa). Si el método de autenticación depende de una base de datos de cortafuegos local o de un servicio externo, debe configurar un perfil de autenticación antes de añadir una cuenta administrativa (consulte la Configuración de cuentas administrativas y autenticación). Si ya configuró el perfil de autenticación o si va a utilizar la autenticación local sin una base de datos de cortafuegos, realice los siguientes pasos para añadir una cuenta administrativa al cortafuegos.



Cree una cuenta administrativa diferente para cada usuario que deba acceder a las funciones de administración o creación de informes del cortafuegos. Esto le permite proteger mejor el cortafuegos de una configuración no autorizada y realizar el logging de las acciones de cada uno de los administradores individuales.

Asegúrese de respetar las recomendaciones de las Prácticas recomendadas para proteger el acceso administrativo para garantizar la seguridad del acceso administrativo a sus cortafuegos y otros dispositivos de seguridad, de modo que evite ataques eficaces.

STEP 1 | Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y **Add (Añadir)** para añadir una cuenta.

STEP 2 | Introduzca un nombre de usuario en **Name**.

Si el cortafuegos utiliza una base de datos de usuario local para autenticar la cuenta, introduzca el nombre que especificó para la cuenta en la base de datos (consulte la Adición de un grupo de usuarios a la base de datos local.)

© 2020 Palo Alto Networks, Inc.

STEP 3 | Seleccione un **Authentication Profile (Perfil de autenticación)** o una secuencia si ha configurado alguno de ellos para el administrador.

Si el cortafuegos utiliza la autenticación local sin una base de datos de usuario local para la cuenta, seleccione **None (Ninguno)** (predeterminado) e introduzca una **Password (Contraseña)**.

STEP 4 | Seleccione el **Administrator Type**.

Si ha configurado una función personalizada para el usuario, seleccione **Role Based (Basado en la función)** y seleccione el **Profile (Perfil)** de la función de administrador. De lo contrario, seleccione **Dynamic (Dinámico)** (el valor por defecto) y seleccione una función dinámica. Si la función dinámica es **virtual system administrator**, añada uno o más sistemas virtuales que el administrador del sistema virtual puede gestionar.

STEP 5 | (Opcional) Seleccione un **Password Profile (Perfil de contraseña)** para administradores que el cortafuegos autentica localmente sin una base de datos de usuario local. Si desea información detallada, consulte Definición de perfiles de contraseña.

STEP 6 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de la autenticación local o externa para los administradores del cortafuegos.

Puede utilizar los servicios de autenticación local o autenticación externa para autenticar a los administradores que acceden al cortafuegos. Estos métodos de autenticación les piden a los administradores que respondan a uno o más desafíos de autenticación, como una página de inicio de sesión en la que introduce un nombre de usuario y una contraseña.

Si utiliza un servicio externo para gestionar la autenticación y la autorización (asignaciones de funciones y dominios de acceso), consulte las siguientes secciones:

- Configuración de la autenticación SAML
- Configuración de la autenticación TACACS+
- Configuración de la autenticación RADIUS

Para autenticar a los administradores sin un mecanismo de respuesta a desafíos, puede realizar la Configuración de una autenticación de administrador basada en certificados en la interfaz web *y la* Configuración de la autenticación de administrador basada en claves de SSH para el CLI.

STEP 1 | (Solo autenticación externa) Permita que el cortafuegos se conecte a un servidor externo para autenticar a los administradores.

Configure un perfil de servidor:

- Añada un perfil de servidor RADIUS.

  Si el cortafuegos se integra con un servicio de autenticación multifactor (MFA) mediante RADIUS, debe añadir un perfil de servidor de RADIUS. En este caso, el servicio de MFA proporciona todos los factores de autenticación (desafíos). Si el cortafuegos se integra con un servicio MFA a través de una API de proveedor, se puede seguir usando un perfil de servidor RADIUS para el primer factor, pero se necesitan los perfiles de servidor MFA para los factores adicionales.
- Añada un perfil de servidor MFA.
- Añada un perfil de servidor TACACS+.

© 2020 Palo Alto Networks, Inc.

- Añada un perfil de servidor SAML IdP. No puede combinar el inicio de sesión único (SSO) de Kerberos con SSO SAML; puede utilizar solo un tipo de servicio de SSO.
- Añada un perfil de servidor Kerberos.
- Añada un perfil de servidor LDAP.

STEP 2 | (Autenticación de base de datos local únicamente) Configure una base de datos de usuario que sea local para el cortafuegos.

1. Añada la cuenta de usuario a la base de datos local.
2. (Opcional) Añada el grupo de usuarios a la base de datos local.

STEP 3 | (Solo autenticación local) Defina la complejidad de la contraseña y la configuración del vencimiento.

Esta configuración puede ayudar a proteger el cortafuegos contra el acceso no autorizado al hacer más difícil que los atacantes adivinen las contraseñas.

1. Define la complejidad de la contraseña global y los ajustes de vencimiento para todos los administradores locales. La configuración no se aplica a las cuentas de base de datos locales para las que especificó un hash de contraseña en lugar de una contraseña (consulte Autenticación local).
    1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de complejidad de contraseña mínima.
    2. Seleccione **Enabled (Habilitado)**.
    3. Defina los ajustes de la contraseña y haga clic en **OK (Aceptar)**.
2. Defina un perfil de contraseña.

    Asigna el perfil a las cuentas administrativas en las que desea anular la configuración de vencimiento de contraseña global. Los perfiles están disponibles solo en las cuentas que no están asociadas a una base de datos local (consulte Autenticación local).

    1. Seleccione **Device (Dispositivo)** > **Password Profiles (Perfiles de contraseña)** y luego **Add (Añadir)** para añadir un perfil.
    2. Introduzca un **Name (Nombre)** para identificar el perfil.
    3. Defina los ajustes de vencimiento de la contraseña y haga clic en **OK (Aceptar)**.

STEP 4 | (Solo SSO de Kerberos) Cree una keytab de Kerberos.

Un keytab es un archivo que contiene información de cuenta de Kerberos para el cortafuegos. Para respaldar el SSO de Kerberos, su red debe contar con una infraestructura Kerberos.

STEP 5 | Configure un perfil de autenticación.

Si sus cuentas administrativas están en múltiples tipos de servidores, puede crear un perfil de autenticación para cada tipo y añadir todos los perfiles a una secuencia de autenticación.

Realice la Configuración de una secuencia y perfil de autenticación. En el perfil de autenticación, especifique el **Type (Tipo)** de servicio de autenticación y la configuración relacionada:

- **Servicio externo:** seleccione el **Type (Tipo)** de servicio externo y seleccione el **Server Profile (Perfil de servidor)** que creó para él.
- **Autenticación de base de datos local**: configure el **Type (Tipo)** en **Local Database (Base de datos local)**.
- **Autenticación local sin una base de datos:** configure el **Type (Tipo)** como **None (Ninguno)**.
- **SSO de Kerberos**: especifique el **Kerberos Realm (Dominio Kerberos)** y seleccione **Import (Importar)** para importar el **Kerberos Keytab**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Asigne el perfil o secuencia de autenticación a una cuenta administrativa.

1. Configuración de una cuenta administrativa del cortafuegos.
   - Asigne el **Authentication Profile (Perfil de autenticación)** o la secuencia que configuró.
   - (Solo autenticación de base de datos local) Especifique el **Name (Nombre)** de la cuenta de usuario que añadió a la base de datos local.
2. **Commit (Confirmar)** los cambios.
3. (Opcional) Realice la Comprobación de la conectividad del servidor de autenticación para comprobar que el cortafuegos puede utilizar el perfil de autenticación para autenticar a los administradores.

Configuración de una autenticación de administrador basada en certificados en la interfaz web

Como una alternativa más segura a la autenticación basada en contraseña para la interfaz web del cortafuegos, puede configurar una autenticación basada en certificado para las cuentas administrativas que sean locales en el cortafuegos. La autenticación basada en certificados implica el intercambio y verificación de una firma digital en lugar de una contraseña.

La configuración de una autenticación basada en certificados para cualquier administrador deshabilita los inicios de sesión de nombre de usuario/contraseña para todos los administradores del cortafuegos; por ello, los administradores necesitarán el certificado para iniciar sesión.

STEP 1 | Genere un certificado de autoridad de certificación (certificate authority, CA) en el cortafuegos.

Puede usar este certificado de CA para firmar el certificado de cliente de cada administrador.

Cree un certificado de CA raíz autofirmado.

De manera alternativa, realice la Importación de un certificado y una clave privada *para su CA empresarial o CA externo.*

STEP 2 | Configure un perfil de certificado para proteger el acceso a la interfaz web.

Configuración de un perfil de certificado.

- Defina el **Username Field (Campo de nombre de usuario)** en **Subject (Asunto)**.
- En la sección de certificados de CA, seleccione **Add** para añadir el **certificado de CA** que acaba de crear o importar.

STEP 3 | Configure el cortafuegos para usar el perfil de certificados para autenticar a los administradores.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite los ajustes de Authentication Settings (Configuración de autenticación).
2. Seleccione el **Certificate Profile** que creó para autenticar a los administradores y haga clic en **OK**.

STEP 4 | Configure las cuentas de administrador para usar la autenticación de certificado cliente.

Para cada administrador que accederá a la interfaz web del cortafuegos, realice la Configuración de una cuenta administrativa de cortafuegos y seleccione **Use only client certificate authentication (Utilizar solo autenticación con certificado de cliente)**.

Si ya ha implementado certificados de cliente que ha generado su CA empresarial, continúe con el paso 8. De lo contrario, diríjase al paso 5.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Genere un certificado de cliente para cada administrador.

Generar un certificado. En la lista desplegable **Signed By**, seleccione un certificado de CA raíz autofirmado.

STEP 6 | Exporte el certificado de cliente.

1. Exporte un certificado y una clave privada.
2. **Commit (Confirmar)** los cambios. El cortafuegos se reinicia y finaliza su sesión. Así, los administradores pueden acceder a la interfaz web únicamente desde sistemas cliente que tengan el certificado de cliente que ha generado.

STEP 7 | Importe el certificado de cliente en el sistema cliente de cada administrador que vaya a acceder a la interfaz web.

Consulte la documentación de su navegador web.

STEP 8 | Verifique que los administradores pueden acceder a la interfaz web.

1. Abra la dirección IP del cortafuegos en un navegador en el ordenador que tenga el certificado de cliente.
2. Cuando se le indique, seleccione el certificado que ha importado y haga clic en **OK**. El explorador muestra una advertencia de certificado.
3. Añada el certificado a la lista de excepciones del explorador.
4. Haga clic en **Login (Inicio de sesión)**. La interfaz web debería aparecer sin pedirle un nombre de usuario o contraseña.

Configuración de la autenticación de administrador basada en claves de SSH para el CLI

Para los administradores que usan el shell seguro (SSH) para acceder al CLI de un cortafuegos de Palo Alto Networks, las claves SSH ofrecen un método de autenticación más seguro que las contraseñas. Las claves SSH prácticamente eliminan el riesgo de ataques de fuerza bruta, ofrecen la posibilidad de una autenticación de dos factores (clave y frase de contraseña) y no envían contraseñas por la red. Las claves SSH también permiten que las secuencias de comandos automatizadas accedan al CLI.

STEP 1 | Use una herramienta de generación de claves SSH para crear un par de claves asimétrico en el sistema cliente del administrador.

Los formatos de clave admitidos son IETF SECSH y Open SSH. Los algoritmos admitidos son DSA (1024 bits) y RSA (768-4096 bits).

Para que los comandos generen un par de claves, consulte la documentación de cliente SSH.

La clave pública y la privada son archivos distintos. Guarde ambos en una ubicación a la que pueda acceder el cortafuegos. Para una mayor seguridad, introduzca una frase de contraseña para cifrar la clave privada. El cortafuegos solicita al administrador la frase de contraseña durante el inicio de sesión.

STEP 2 | Configure la cuenta del administrador para usar la autenticación de clave pública.

1. Configuración de una cuenta administrativa del cortafuegos.
   - Configure el método de autenticación que deberá utilizarse si falla la autenticación de clave SSH. Si ha configurado un **perfil de autenticación** para el administrador, selecciónelo en la lista desplegable. Si selecciona **None**, deberá introducir una contraseña en **Password** y después repetirla en **Confirm Password**.
   - Seleccione **Use Public Key Authentication (Utilizar autenticación de clave pública) (SSH)**, luego, **Import Key (Importar clave)**, **Browse (Explorar)** para buscar la clave pública que acaba de generar, y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

2. **Commit (Confirmar)** los cambios.

STEP 3 | Configure el cliente SSH para usar la clave privada para autenticarse en el cortafuegos.

Realice esta tarea en el sistema cliente del administrador. Para conocer los pasos, consulte la documentación de su cliente SSH.

STEP 4 | Compruebe que el administrador puede acceder al CLI del cortafuegos usando la autenticación de clave SSH.

1. Use un navegador en el sistema cliente del administrador para ir a la dirección IP del cortafuegos.
2. Inicie sesión en el CLI del cortafuegos como administrador. Después de escribir un nombre de usuario, verá la siguiente salida (el valor de clave es un ejemplo):

```
Authenticating with public key "dsa-key-20130415"
```

3. Si se le solicita, introduzca la frase de contraseña definida al crear las claves.

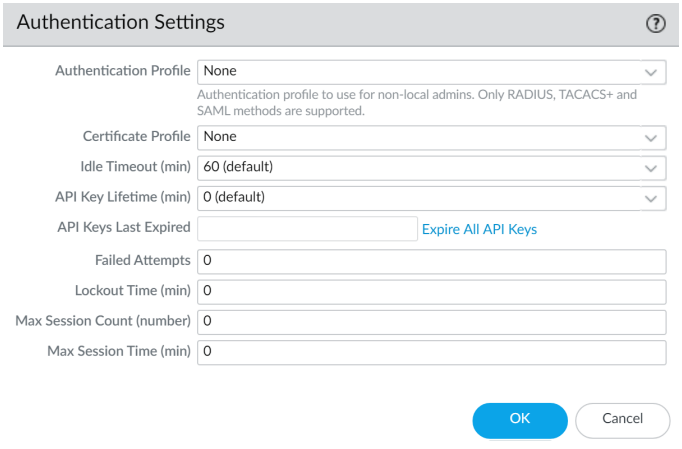
Configuración de la vigencia de las claves de las API

Las claves de las API del cortafuegos y de Panorama permiten autenticar las llamadas a la API XML y a la API REST. Como estas claves conceden acceso al cortafuegos y a Panorama y, por lo tanto, son elementos fundamentales de la estrategia de seguridad, es recomendable especificar una vigencia máxima para garantizar su rotación periódica. Tras especificar la vigencia, se genera una clave de la API única en cada ocasión.

Además de configurar la vigencia que solicita la generación periódica de claves nuevas, también puede revocar todas las claves de las API válidas si alguna está en riesgo. La revocación de claves es un método para hacer que venzan todas las claves válidas en el momento.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.

STEP 2 | En Authentication Settings (Configuración de autenticación), edite **API Key Lifetime (min) (Duración de claves de API [min])** para especificar la vigencia.



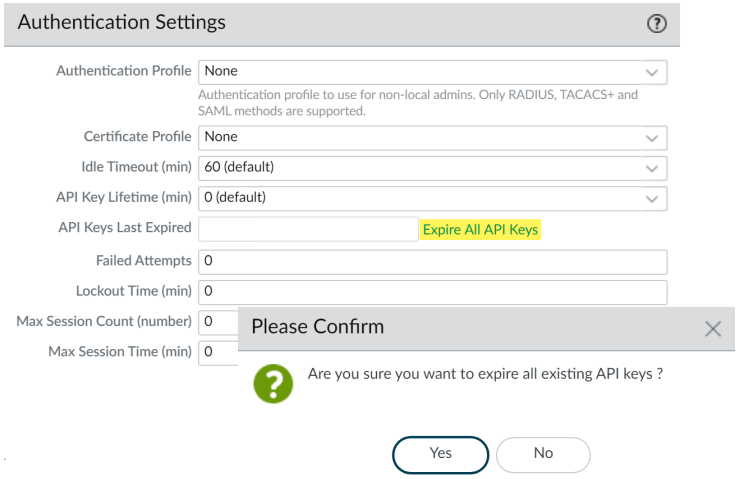
Configure una vigencia que ofrezca protección frente a las situaciones de riesgo y reduzca los efectos de exposiciones accidentales. La duración está configurada en cero (0) de manera predeterminada, lo cual significa que las claves no vencen nunca. Para garantizar que las claves se rotan a menudo y se crean otras únicas en cada ocasión, especifique un período de validez de entre 1 minuto y 525 600. Consulte las políticas de auditoría y cumplimiento de su empresa a fin de determinar la vigencia adecuada para las claves de las API.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 4 | (Para revocar todas las claves de las API) Marque **Expire all API Keys (Hacer que venzan todas las claves de API)** para renovarlas todas.

Si acaba de configurar la vigencia y desea renovar todas las claves para que cumplan el plazo indicado, puede hacer que venzan.



Una vez confirmada la acción, las claves se revocan; consulte la marca de tiempo correspondiente en **API Keys Last Expired (Último vencimiento de claves de API)**.

© 2020 Palo Alto Networks, Inc.

Referencia: acceso de administrador a la interfaz web

Puede configurar privilegios para un cortafuegos completo o para uno o más sistemas virtuales (en plataformas que admitan varios sistemas virtuales). En esa designación de **Device** o **Virtual System**, puede configurar privilegios para funciones de administrador personalizadas, que son más pormenorizadas que los privilegios fijos asociados con una función de administrador dinámica.

La configuración de privilegios a nivel granular garantiza que los administradores de nivel inferior no puedan a acceder a cierta información. Puede crear funciones personalizadas para administradores de cortafuegos (consulte Configuración de una cuenta administrativa de cortafuegos), administradores de Panorama o administradores de grupo de dispositivos y plantilla (consulte la Guía del administrador de Panorama). Usted aplica la función de administrador a una cuenta de administrador basada en la función en la que puede asignar uno o más sistemas virtuales. Los siguientes temas describen los privilegios que puede configurar para las funciones de administrador personalizadas.

- Privilegios de acceso a la interfaz web
- Privilegios de Acceso a la interfaz web de Panorama

Privilegios de acceso a la interfaz web

Si desea impedir que un administrador basado en roles acceda a pestañas específicas de la interfaz web, puede deshabilitar la pestaña y el administrador ni siquiera la verá cuando inicie sesión con la cuenta administrativa basada en funciones asociada. Por ejemplo, podría crear un perfil de función de administrador para su personal de operaciones que únicamente proporcione acceso a las pestañas **Device (Dispositivo)** y **Network (Red)** y un perfil separado para los administradores de seguridad que proporcione acceso a las pestañas **Object (Objetos)**, **Policy (Política)** y **Monitor (Supervisar)**.

Una función de administrador puede aplicarse en el nivel del **dispositivo** o el **sistema virtual** como lo define el botón de opción **Device (Dispositivo)** o **Virtual System (Sistema virtual)**. Si selecciona **Virtual System (Sistema virtual)**, el administrador asignado por este perfil se restringe al sistema virtual al que está asignado. Además, solo la pestaña **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Virtual Systems (Sistemas virtuales)** está disponible para ese administrador, no la pestaña **Global (Global)**.

Los siguientes temas describen cómo establecer los privilegios de la función de administrador en las diferentes partes de la interfaz web:

- Definición del acceso a las pestañas de la interfaz web
- Acceso detallado a la pestaña Supervisar
- Acceso detallado a la pestaña Política
- Acceso detallado a la pestaña Objetos
- Acceso detallado a la pestaña Red
- Acceso detallado a la pestaña Dispositivo
- Definición de ajustes de privacidad de usuario en el perfil de función de administrador
- Restricción del acceso de administrador a funciones de confirmación y validación
- Acceso detallado a ajustes globales
- Concesión de acceso granular a la pestaña Panorama

Definición del acceso a las pestañas de la interfaz web

La siguiente tabla describe los privilegios de acceso a nivel superior que puede asignar a un perfil de función de administrador (**Device [Dispositivo]** > **Admin Roles [Funciones de administrador]**). Puede habilitar,

© 2020 Palo Alto Networks, Inc.

deshabilitar o definir privilegios de acceso de solo lectura en las pestañas de nivel superior en la interfaz web.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Dashboard (Panel)	Controla el acceso a la pestaña **Panel**. Si deshabilita este privilegio, el administrador no verá la pestaña ni tendrá acceso a ninguno de los widgets del panel.	yes (sí)	No	yes (sí)
ACC	Controla el acceso al Centro de control de aplicaciones (Application Command Center, ACC). Si deshabilita este privilegio, la pestaña **ACC** no aparecerá en la interfaz web. Recuerde que si desea proteger la privacidad de sus usuarios y a la vez seguir proporcionando acceso al ACC, puede deshabilitar la opción {0>**Privacy (Privacidad)Show Full IP Addresses (Mostrar direcciones IP completas)**<0} y/o la opción **Show User Names In Logs And Reports (Mostrar nombres de usuario en logs e informes)**.	yes (sí)	No	yes (sí)
Monitor (Supervisar)	Controla el acceso a la pestaña **Monitor (Supervisar)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Monitor (Supervisar)** ni tendrá acceso a ninguno de los logs, capturas de paquetes, información de sesión, informes o Appscope. Para obtener un control más detallado sobre qué información de supervisión puede ver el administrador, deje la opción Monitor (Supervisar) habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Monitor (Supervisar).	yes (sí)	No	yes (sí)
Políticas	Controla el acceso a la pestaña **Políticas**. Si deshabilita este privilegio, el administrador no verá la pestaña **Políticas** ni tendrá acceso a ninguna información de política. Para obtener un control más detallado sobre qué información de políticas puede ver el administrador; por ejemplo, para habilitar el acceso a un tipo de política específico o para habilitar el acceso de solo lectura a información de políticas, deje la opción **Policies (Políticas)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Policy (Política).	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Objetos	Controla el acceso a la pestaña **Objects (Objetos)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Objects (Objetos)** ni tendrá acceso a ninguno de los objetos, perfiles de seguridad, perfiles de reenvío de logs, perfiles de descifrado o programaciones. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Objects (Objetos)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Objects (Objetos).	yes (sí)	No	yes (sí)
network	Controla el acceso a la pestaña **Network (Red)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Network (Red)** ni tendrá acceso a ninguna información de configuración de interfaz, zona, VLAN, Virtual Wire, enrutador virtual, túnel de IPSec, DHCP, proxy DNS, GlobalProtect o QoS o a los perfiles de red. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Networks (Red)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Network (Red).	yes (sí)	No	yes (sí)
Dispositivo	Controla el acceso a la pestaña **Device (Dispositivo)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Device** ni tendrá acceso a ninguna información de configuración de todo el cortafuegos, como información de configuración de User-ID, alta disponibilidad, perfil de servidor o certificado. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Objects (Objetos)** habilitada y, a continuación, habilite o deshabilite los nodos específicos en la pestaña como se describe en Concesión de acceso detallado a la pestaña Device (Dispositivo). *No puede habilitar el acceso a los nodos Funciones de administrador o Administradores para un administrador basado en funciones aunque habilite un*	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	acceso completo a la pestaña Dispositivo.			

Acceso detallado a la pestaña Supervisar

En algunos casos, puede que desee habilitar al administrador para que vea algunas pero no todas las áreas de la pestaña **Monitor**. Por ejemplo, puede querer restringir los administradores de operaciones a los logs Config y Sistema únicamente, ya que no contienen datos privados de usuarios. Aunque esta sección de la definición de función de administrador especifica qué áreas de la pestaña **Monitor** puede ver el administrador, también puede emparejar los privilegios de esta sección con privilegios de privacidad, como deshabilitar la capacidad de ver nombres de usuarios en logs e informes. Sin embargo, una cosa que hay que tener en cuenta es que los informes generados por el sistema seguirán mostrando nombres de usuario y direcciones IP incluso si deshabilita esa funcionalidad en la función. Por este motivo, si no desea que el administrador vea ninguna de la información de usuario privada, debería deshabilitar el acceso a informes específicos como se indica en la tabla siguiente.

La siguiente tabla muestra los niveles de acceso de la pestaña **Monitor** y las funciones de administrador para las que están disponibles.

Las funciones de grupo de dispositivos y plantilla pueden ver los datos de logs únicamente para los grupos de dispositivos que están en dominios de acceso asignados a esas funciones.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Monitor (Supervisar)	Habilita o deshabilita el acceso a la pestaña **Supervisar**. Si está deshabilitado, el administrador no verá esta pestaña ni ninguno de los logs o informes asociados.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Logs	Habilita o deshabilita el acceso a todos los archivos de log. También puede dejar este privilegio habilitado y, a continuación, deshabilitar logs específicos que no desea que vea el administrador. Tenga en cuenta que si desea proteger la privacidad de sus usuarios mientras sigue ofreciendo acceso a uno o más logs, puede deshabilitar la opción **Privacy (Privacidad)** > **Show Full IP Addresses (Mostrar direcciones IP completas)** y la opción **Show User Names In Logs And Reports (Mostrar nombres de usuario en logs e informes)**.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Tráfico	Especifica si el administrador puede ver los logs de tráfico.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
threat	Especifica si el administrador puede ver los logs de amenaza.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Filtrado de URLs	Especifica si el administrador puede ver los logs de filtrado de URL.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Envíos a WildFire	Especifica si el administrador puede ver los logs de WildFire. Estos logs solamente están disponibles si tiene una suscripción a WildFire.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Data Filtering	Especifica si el administrador puede ver los logs de filtrado de datos.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Coincidencia HIP	Especifica si el administrador puede ver los logs de coincidencias HIP. Los logs de coincidencias HIP solo están disponibles si tiene una licencia de GlobalProtect (esto es, una suscripción).	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
GlobalProtect	Especifica si el administrador puede ver los logs de GlobalProtect. Estos logs solo están disponibles si tiene una licencia de GlobalProtect (esto es, una suscripción).	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
User-ID	Especifica si el administrador puede ver los logs de User-ID.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
GTP	Especifica si el operador de la red móvil puede ver los logs GTP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Inspección de túnel	Especifica si el administrador puede ver los logs de inspección de túnel.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
SCTP	Especifica si el operador de la red móvil puede ver los logs del Protocolo de transmisión de control de secuencias (Stream Control Transmission Protocol, SCTP). *Debe habilitar SCTP en Panorama (Device [Dispositivo] > Setup [Configuración] > Management [Gestión]) antes de controlar el acceso de administrador a los logs de SCTP, los informes personalizados o los informes predefinidos para Panorama y el grupo/plantilla de dispositivos.*	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Configuración	Especifica si el administrador puede ver los logs de configuración.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Sistema	Especifica si el administrador puede ver los logs de sistema.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Alarmas	Especifica si el administrador puede ver las alarmas generadas por el sistema.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Autenticación	Especifica si el administrador puede ver los logs de autenticación.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Motor de correlación automatizada	Habilita o deshabilita el acceso a los objetos de correlación y los logs de eventos correlacionados en el cortafuegos.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Objetos de correlación	Especifica si el administrador puede ver y habilitar o deshabilitar los objetos de correlación.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Eventos correlacionados	Especifica si el administrador	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Captura de paquetes	Especifica si el administrador puede ver capturas de paquetes (packet captures, pcaps) en la pestaña **Monitor**. Recuerde que las capturas de paquetes son datos de flujo sin procesar y, por lo tanto, pueden contener direcciones IP de usuarios. Si deshabilita los privilegios **Mostrar direcciones IP completas**, no ocultará la dirección IP en la pcap y, por ello, debería deshabilitar el privilegio Captura de paquetes si le preocupa la privacidad del usuario.	Cortafuegos: yes (sí) Panorama: No Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Appscope	Especifica si el administrador puede ver las herramientas de análisis y visibilidad de App Scope. Al habilitar Appscope, permite el acceso a todos los gráficos de **App Scope**.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Explorador de sesión	Especifica si el administrador puede examinar y filtrar las sesiones que se están ejecutando actualmente en el cortafuegos. Recuerde que el explorador de sesión muestra datos de flujo sin procesar y, por lo tanto, puede contener direcciones IP de usuarios. Si deshabilita los privilegios **Mostrar direcciones IP completas**, no ocultará la dirección IP en el explorador de sesión y, por ello, debería deshabilitar el privilegio **Explorador de sesión** si le preocupa la privacidad del usuario.	Cortafuegos: yes (sí) Panorama: No Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Lista de IP bloqueadas	Especifica si el administrador puede ver la lista de bloqueo (habilitada o solo lectura) y eliminar las entradas de la lista (habilitada). Si deshabilita el ajuste, el administrador no podrá ver ni eliminar las entradas de la lista de bloqueo.	Cortafuegos: yes (sí) Panorama: en Context Switch UI: yes (sí) Plantilla: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Botnet	Especifica si el administrador puede generar y ver informes de análisis de Botnet o ver informes de Botnet en modo de solo lectura. Si deshabilita los privilegios **Mostrar direcciones IP completas**, no ocultará la dirección IP en informes de Botnet programados y, por ello, debería deshabilitar el privilegio **Botnet** si le preocupa la privacidad del usuario.	Cortafuegos: yes (sí) Panorama: No Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Informes en PDF	Habilita o deshabilita el acceso a todos los informes en PDF. También puede dejar este privilegio habilitado y, a continuación, deshabilitar informes en PDF específicos que no quiera que vea el administrador. Tenga en cuenta que si desea proteger la privacidad de sus usuarios mientras sigue ofreciendo acceso a uno o más informes, puede deshabilitar la opción **Privacy (Privacidad)** > **Show Full IP Addresses (Mostrar direcciones IP completas)** y la opción **Show User Names In Logs**	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
	And Reports (Mostrar nombres de usuario en logs e informes).				
Gestionar resumen de PDF	Especifica si el administrador puede ver, añadir o eliminar definiciones de informes de resumen en PDF. Con el acceso de solo lectura, el administrador puede ver definiciones de informes de resumen en PDF, pero no puede añadirlas ni eliminarlas. Si deshabilita esta opción, el administrador no puede ver las definiciones de los informes ni añadirlas/eliminarlas.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Informes de resumen en PDF	Especifica si el administrador puede ver los informes de resumen en PDF generados en **Monitor (Supervisar)** > **Reports (Informes)**. Si deshabilita esta opción, la categoría **Informes de resumen en PDF** no se mostrará en el nodo **Informes**.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Informe de actividad del usuario	Especifica si el administrador puede ver, añadir o eliminar definiciones de informes de actividad del usuario y descargar los informes. Con el acceso de solo lectura, el administrador puede ver definiciones de informes de actividad del usuario, pero no puede añadirlas, eliminarlas ni descargarlas. Si deshabilita esta opción, el administrador no podrá ver esta categoría de informe en PDF.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Informe de uso de aplicación SaaS	Especifica si el administrador puede ver, añadir o eliminar un informe de uso de aplicación SaaS. Con el acceso de solo lectura, el administrador puede ver definiciones de informes de uso de aplicación SaaS, pero no puede añadirlas ni eliminarlas. Si deshabilita esta opción, el administrador no puede ver las definiciones de los informes ni añadirlas/eliminarlas.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Grupos de informes	Especifica si el administrador puede ver, añadir o eliminar definiciones de grupos de informes. Con el acceso de solo lectura, el administrador puede ver definiciones de grupos de informes, pero no puede añadirlas ni eliminarlas. Si deshabilita esta opción, el administrador no podrá ver esta categoría de informe en PDF.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Programador de correo electrónico	Especifica si el administrador puede programar grupos de informes para correo electrónico. Como los informes generados que se envían por correo electrónico pueden contener datos de usuario confidenciales que no se eliminan al deshabilitar la opción **Privacy (Privacidad)** > **Show Full IP Addresses (Mostrar direcciones IP completas)** o la opción **Show User Names In Logs And Reports (Mostrar nombres de usuario en logs e informes)**, y debido a que pueden mostrar datos de logs a los que el administrador no tiene acceso, deberá deshabilitar la opción **Email Scheduler (Programador de correo electrónico)** si tiene requisitos de privacidad del usuario.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Gestionar informes personalizados	Habilita o deshabilita el acceso a toda la funcionalidad de informe personalizado. También puede dejar este privilegio habilitado y, a continuación, deshabilitar categorías específicas de informes personalizados a los que no desee que el administrador pueda acceder. Tenga en cuenta que si desea proteger la privacidad de sus usuarios mientras sigue ofreciendo acceso a uno o más informes, puede deshabilitar la opción **Privacy (Privacidad)** > **Show Full IP Addresses (Mostrar direcciones IP completas)** y la opción **Show User Names In Logs**	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
	And Reports (Mostrar nombres de usuario en logs e informes).  *Los informes programados para ejecutarse en lugar de ejecutarse a petición mostrarán la dirección IP e información de usuario. En este caso, asegúrese de restringir el acceso a las áreas de informe correspondientes. Además, la función de informe personalizado no restringe la capacidad de generar informes que contengan datos de log incluidos en logs que estén excluidos de la función de administrador.*				
Estadísticas de aplicación	Especifica si el administrador puede crear un informe personalizado que incluya datos de la base de datos de estadísticas de aplicación.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Log de filtrado de datos	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de filtrado de datos.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
log amenaza	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de amenaza.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Resumen de amenaza	Especifica si el administrador puede crear un informe personalizado que incluya datos de la base de datos de resumen de amenaza.	Cortafuegos: yes (sí) Panorama: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
		Plantilla/grupo de dispositivos: yes (sí)			
log de tráfico	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de tráfico.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Resumen de tráfico	Especifica si el administrador puede crear un informe personalizado que incluya datos de la base de datos de resumen de amenaza.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Log de URL	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de filtrado de URL.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Coincidencia HIP	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de coincidencias HIP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
GlobalProtect	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de GlobalProtect.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Log de WildFire	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de WildFire.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Log de GTP	Especifica si el operador de la red móvil puede crear un informe personalizado que incluya datos de los logs de GTP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Resumen de GTP	Especifica si el operador de la red móvil puede crear un informe personalizado que incluya datos de los logs de GTP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
Log de túnel	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de inspección de túnel.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Resumen de túnel	Especifica si el administrador puede crear un informe personalizado que incluya datos de la base de datos de resumen de túnel.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Logs de SCTP	Especifica si el operador de la red móvil puede crear un informe personalizado que incluya datos de los logs de SCTP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Resumen de SCTP	Especifica si el operador de la red móvil puede crear un informe personalizado que incluya datos de la base de datos del resumen de SCTP.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
ID de usuario	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de User-ID.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Aut	Especifica si el administrador puede crear un informe personalizado que incluya datos de los logs de autenticación.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes personalizados programados	Especifica si el administrador puede ver un informe personalizado que se haya programado para su generación.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes de aplicación predefinidos	Especifica si el administrador puede ver informes de aplicación. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los informes	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
	si tiene requisitos de privacidad de usuario.				
Ver informes de amenazas predefinidos	Especifica si el administrador puede ver informes de amenazas. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los informes si tiene requisitos de privacidad de usuario.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes de filtrado de URL predefinidos	Especifica si el administrador puede ver informes de filtrado de URL. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los informes si tiene requisitos de privacidad de usuario.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes de tráfico predefinidos	Especifica si el administrador puede ver informes de tráfico. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los informes si tiene requisitos de privacidad de usuario.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes GTP predefinidos	Especifica si el operador de la red móvil puede ver los informes de GTP. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los informes si tiene requisitos de privacidad de usuario.	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)
Ver informes de SCTP predefinidos	Especifica si el operador de la red móvil puede ver los informes de SCTP. Los privilegios de privacidad no afectan los informes disponibles en el nodo **Monitor (Supervisar)** > **Reports (Informes)** y, por lo tanto, debe deshabilitar el acceso a los	Cortafuegos: yes (sí) Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilita	Solo lectura	Deshab
	informes si tiene requisitos de privacidad de usuario.				

Acceso detallado a la pestaña Política

Si habilita la opción de política en el perfil de función de administrador, a continuación podrá habilitar, deshabilitar o proporcionar acceso de solo lectura a nodos específicos dentro de la pestaña según fuera necesario para la función que esté definiendo. Al habilitar el acceso a un tipo de política específico, habilita la capacidad de ver, añadir o eliminar reglas de política. Al habilitar un acceso de solo lectura a una política específica, habilita al administrador para que pueda ver la base de reglas de política correspondiente, pero no añadir ni eliminar reglas. Al deshabilitar el acceso a un tipo de política específico, impide que el administrador vea la base de reglas de política.

Dado que la política basada en usuarios específicos (por nombre de usuario o dirección IP) debe definirse explícitamente, los ajustes de privacidad que deshabiliten la capacidad de ver direcciones IP completas o nombres de usuario no se aplican a la pestaña Policy (Política). Por lo tanto, solamente debería permitir el acceso a la pestaña Política a administradores excluidos de restricciones de privacidad de usuario.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Security	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de seguridad. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de seguridad, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
NAT	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de NAT. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas NAT, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
QoS	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de QoS. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas QoS, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
Reenvío basado en políticas	Active este privilegio para permitir que el administrador visualice, añada o elimine las reglas de reenvío basado en políticas (Policy-Based Forwarding, PBF). Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas,	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	pero no modificarlas. Para impedir que el administrador vea la base de reglas PBF, deshabilite este privilegio.			
descifrado	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de descripción. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de descripción, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
Inspección de túnel	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de inspección de túnel. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de inspección de túnel, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
Cancelación de aplicación	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de política de cancelación de aplicación. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de cancelación de aplicación, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
Autenticación	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de política de autenticación. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de autenticación, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)
Protección DoS	Habilite este privilegio para permitir que el administrador vea, añada y/o elimine reglas de protección DoS. Establezca el privilegio como de solo lectura si desea que el administrador pueda ver las reglas, pero no modificarlas. Para impedir que el administrador vea la base de reglas de protección DoS, deshabilite este privilegio.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Acceso detallado a la pestaña Objetos

Un objeto es un contenedor que agrupa valores de filtros de políticas específicos (como direcciones IP, URL, aplicaciones o servicios) para una definición de reglas simplificada. Por ejemplo, un objeto de dirección puede contener definiciones de direcciones IP específicas para servidores web y de aplicaciones en su zona DMZ.

Al decidir si desea permitir el acceso a la pestaña de objetos en su totalidad, determine si el administrador tendrá responsabilidades de definición de políticas. Si no, probablemente el administrador no necesite acceder a la pestaña. Sin embargo, si el administrador necesitara crear políticas, podrá habilitar el acceso a la pestaña y, a continuación, otorgar privilegios de acceso detallados a nivel del nodo.

Al habilitar el acceso a un nodo específico, usted otorga al administrador el privilegio de ver, añadir y eliminar el tipo de objeto correspondiente. Al otorgar un acceso de solo lectura, permitirá que el administrador vea los objetos ya definidos, pero no podrá crear o eliminar ninguno. Al deshabilitar un nodo, impide que el administrador vea el nodo en la interfaz web.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
addresses	Especifica si el administrador puede ver, añadir o eliminar objetos de direcciones para su uso en una política de seguridad.	yes (sí)	yes (sí)	yes (sí)
Grupos de direcciones	Especifica si el administrador puede ver, añadir o eliminar objetos de grupos de direcciones para su uso en una política de seguridad.	yes (sí)	yes (sí)	yes (sí)
regions	Especifica si el administrador puede ver, añadir o eliminar objetos de regiones para su uso en una política de seguridad, de descifrado o DoS.	yes (sí)	yes (sí)	yes (sí)
applications	Especifica si el administrador puede ver, añadir o eliminar objetos de aplicaciones para su uso en una política.	yes (sí)	yes (sí)	yes (sí)
Grupos de aplicaciones	Especifica si el administrador puede ver, añadir o eliminar objetos de grupo de aplicaciones para su uso en una política.	yes (sí)	yes (sí)	yes (sí)
Filtros de aplicación	Especifica si el administrador puede ver, añadir o eliminar filtros de aplicación para la simplificación de búsquedas repetidas.	yes (sí)	yes (sí)	yes (sí)
Services	Especifica si el administrador puede ver, añadir o eliminar objetos de servicio para su uso en la creación de reglas de políticas que limiten los números de puertos que puede utilizar una aplicación.	yes (sí)	yes (sí)	yes (sí)
Grupos de servicios	Especifica si el administrador puede ver, añadir o eliminar objetos de grupos de servicio para su uso en una política de seguridad.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Etiquetas	Especifica si el administrador puede ver, añadir o eliminar etiquetas que se hayan definido en el cortafuegos.	yes (sí)	yes (sí)	yes (sí)
GlobalProtect	Especifica si el administrador puede ver, añadir o eliminar objetos y perfiles HIP. Puede restringir el acceso a ambos tipos de objetos a nivel de GlobalProtect, o bien proporcionar un control más detallado habilitando el privilegio GlobalProtect y restringiendo el acceso a objetos HIP o perfiles HIP.	yes (sí)	No	yes (sí)
Objetos HIP	Especifica si el administrador puede ver, añadir o eliminar objetos HIP, que se utilizan para definir perfiles HIP. Los objetos HIP también generan logs de coincidencias HIP.	yes (sí)	yes (sí)	yes (sí)
Aplicaciones sin cliente	Especifica si el administrador puede ver, añadir, modificar o eliminar aplicaciones de VPN sin cliente de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
Grupos de aplicaciones sin cliente	Especifica si el administrador puede ver, añadir, modificar o eliminar grupos de aplicaciones de VPN sin cliente de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
perfiles de HIP	Especifica si el administrador puede ver, añadir o eliminar perfiles HIP para su uso en una política de seguridad y/o para generar logs de coincidencias HIP.	yes (sí)	yes (sí)	yes (sí)
Listas dinámicas externas	Especifica si el administrador puede ver, añadir o eliminar listas dinámicas externas para su uso en una política de seguridad.	yes (sí)	yes (sí)	yes (sí)
Objetos personalizados	Especifica si el administrador puede ver las firmas personalizadas de spyware y vulnerabilidad. Puede restringir el acceso para habilitar o deshabilitar el acceso a todas las firmas personalizadas a este nivel, o bien proporcionar un control más detallado habilitando el privilegio Objetos personalizados y, a continuación, restringiendo el acceso a cada tipo de firma.	yes (sí)	No	yes (sí)
Patrones de datos	Especifica si el administrador puede ver, añadir o eliminar firmas de patrones de datos personalizadas para su uso en la creación de perfiles de protección contra vulnerabilidades personalizados.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Spyware	Especifica si el administrador puede ver, añadir o eliminar firmas de spyware personalizadas para su uso en la creación de perfiles personalizados de protección contra vulnerabilidades.	yes (sí)	yes (sí)	yes (sí)
vulnerabilidad	Especifica si el administrador puede ver, añadir o eliminar firmas de vulnerabilidad personalizadas para su uso en la creación de perfiles personalizados de protección contra vulnerabilidades.	yes (sí)	yes (sí)	yes (sí)
URL Category (Categoría de URL)	Especifica si el administrador puede ver, añadir o eliminar categorías de URL personalizadas para su uso en una política.	yes (sí)	yes (sí)	yes (sí)
Perfiles de seguridad	Especifica si el administrador puede ver perfiles de seguridad. Puede restringir el acceso para habilitar o deshabilitar el acceso a todos los perfiles de seguridad a este nivel, o bien proporcionar un control más detallado habilitando el privilegio Perfiles de seguridad y, a continuación, restringiendo el acceso a cada tipo de perfil.	yes (sí)	No	yes (sí)
Antivirus	Especifica si el administrador puede ver, añadir o eliminar perfiles de antivirus.	yes (sí)	yes (sí)	yes (sí)
Antispyware	Especifica si el administrador puede ver, añadir o eliminar perfiles de antivirus.	yes (sí)	yes (sí)	yes (sí)
Protección contra vulnerabilidades	Especifica si el administrador puede ver, añadir o eliminar perfiles de protección contra vulnerabilidades.	yes (sí)	yes (sí)	yes (sí)
Filtrado de URLs	Especifica si el administrador puede ver, añadir o eliminar perfiles de filtrado de URL.	yes (sí)	yes (sí)	yes (sí)
Bloqueo de archivos	Especifica si el administrador puede ver, añadir o eliminar perfiles de bloqueo de archivos.	yes (sí)	yes (sí)	yes (sí)
Análisis de WildFire	Especifica si el administrador puede ver, añadir o eliminar perfiles de análisis de WildFire.	yes (sí)	yes (sí)	yes (sí)
Data Filtering	Especifica si el administrador puede ver, añadir o eliminar perfiles de filtrado de datos.	yes (sí)	yes (sí)	yes (sí)
Protección DoS	Especifica si el administrador puede ver, añadir o eliminar perfiles de protección DoS.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Protección de GTP	Especifica si el operador de la red móvil puede ver, añadir o eliminar perfiles de protección de GTP.	yes (sí)	yes (sí)	yes (sí)
Protección de SCTP	Especifica si el operador de la red móvil puede ver, añadir o eliminar perfiles de protección del Protocolo de transmisión de control de secuencias (Stream Control Transmission Protocol, SCTP).	yes (sí)	yes (sí)	yes (sí)
Grupos de perfiles de seguridad	Especifica si el administrador puede ver, añadir o eliminar grupos de perfiles de seguridad.	yes (sí)	yes (sí)	yes (sí)
Log Forwarding	Especifica si el administrador puede ver, añadir o eliminar perfiles de reenvío de logs.	yes (sí)	yes (sí)	yes (sí)
Autenticación	Especifica si el administrador puede ver, añadir o eliminar objetos de aplicación de autenticación.	yes (sí)	yes (sí)	yes (sí)
Perfil de descifrado	Especifica si el administrador puede ver, añadir o eliminar perfiles de descifrado.	yes (sí)	yes (sí)	yes (sí)
Programaciones	Especifica si el administrador puede ver, añadir o eliminar programaciones para limitar una política de seguridad a una fecha y/o intervalo de tiempo específico.	yes (sí)	yes (sí)	yes (sí)

Acceso detallado a la pestaña Red

Al decidir si desea permitir el acceso a la pestaña **Network (Red)** en su totalidad, determine si el administrador tendrá responsabilidades de administración de red, incluida la administración de GlobalProtect. Si no, probablemente el administrador no necesite acceder a la pestaña.

También puede definir el acceso a la pestaña **Network (Red)** a nivel de nodo. Al habilitar el acceso a un nodo específico, usted otorga al administrador el privilegio de ver, añadir y eliminar las configuraciones de red correspondientes. Al tener un acceso de solo lectura el administrador puede visualizar la configuración ya definida, pero no crear ni eliminar ninguna. Al deshabilitar un nodo, impide que el administrador vea el nodo en la interfaz web.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Interfaces	Especifica si el administrador puede ver, añadir o eliminar configuraciones de interfaces.	yes (sí)	yes (sí)	yes (sí)
Zonas	Especifica si el administrador puede ver, añadir o eliminar zonas.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
vlans	Especifica si el administrador puede ver, añadir o eliminar VLAN.	yes (sí)	yes (sí)	yes (sí)
Cables virtuales	Especifica si el administrador puede ver, añadir o eliminar cables virtuales.	yes (sí)	yes (sí)	yes (sí)
Enrutadores virtuales	Especifica si el administrador puede ver, añadir, modificar o eliminar enrutadores virtuales.	yes (sí)	yes (sí)	yes (sí)
Túneles IPSec	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de túneles de IPSec.	yes (sí)	yes (sí)	yes (sí)
Túneles GRE	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de túneles de GRE.	yes (sí)	yes (sí)	yes (sí)
DHCP	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de servidor DHCP y retransmisión DHCP.	yes (sí)	yes (sí)	yes (sí)
Proxy Dns	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de proxy DNS.	yes (sí)	yes (sí)	yes (sí)
GlobalProtect	Especifica si el administrador puede ver, añadir o modificar configuraciones de portal y puerta de enlace de GlobalProtect. Puede deshabilitar el acceso a las funciones de GlobalProtect por completo, o bien puede habilitar el privilegio GlobalProtect y, a continuación, restringir la función a las áreas de configuración del portal o del puerta de enlace.	yes (sí)	No	yes (sí)
Portales	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de portal de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
Gateways	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de puerta de enlace de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
MDM	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de servidor MDM de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
Lista de bloqueo de dispositivos	Especifica si el administrador puede ver, añadir, modificar o eliminar listas de bloqueo de dispositivos.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Aplicaciones sin cliente	Especifica si el administrador puede ver, añadir, modificar o eliminar aplicaciones de VPN sin cliente de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
Grupos de aplicaciones sin cliente	Especifica si el administrador puede ver, añadir, modificar o eliminar grupos de aplicaciones de VPN sin cliente de GlobalProtect.	yes (sí)	yes (sí)	yes (sí)
QoS	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de QoS.	yes (sí)	yes (sí)	yes (sí)
LLDP	Especifica si el administrador puede ver, añadir, modificar o eliminar configuraciones de LLDP.	yes (sí)	yes (sí)	yes (sí)
Perfiles de red	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de red descritos a continuación.	yes (sí)	No	yes (sí)
Criptográfico de IPSec de GlobalProtect	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **GlobalProtect IPSec Crypto (Criptográfico de IPSec de GlobalProtect)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo o configurar algoritmos para la autenticación y cifrado en túneles VPN entre una puerta de enlace y clientes de GlobalProtect. Si establece este privilegio como de solo lectura, el administrador podrá ver los perfiles de criptográficos IPSec de GlobalProtect pero no podrá añadirlo ni editarlos.	yes (sí)	yes (sí)	yes (sí)
Puertas de enlace de IKE	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)**. Si deshabilita este privilegio, el administrador no verá el nodo **IKE Gateways (Puertas de enlace de IKE)** ni definirá puertas de enlace que incluyan la información de configuración necesaria para realizar la negociación del protocolo IKE con la puerta de enlace del peer. Si el estado del privilegio está establecido como de solo lectura, podrá ver los gateways de IKE actualmente configuradas, pero no podrá añadir ni editar gateways.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Criptográfico de IPSec	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico de IPSec)**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico de IPSec)** ni especificará protocolos y algoritmos para la identificación, autenticación y cifrado en túneles de VPN basándose en la negociación de SA de IPSec. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración criptográfica de IPSec actualmente establecida, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Criptográfico de IKE	Controla el modo en que los dispositivos intercambian información para garantizar una comunicación segura. Especifique los protocolos y algoritmos para la identificación, autenticación y cifrado en túneles de VPN basándose en la negociación de SA de IPSec (IKEv1 de fase 1).	yes (sí)	yes (sí)	yes (sí)
Monitor (Supervisar)	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **Monitor (Supervisar)**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **Monitor (Supervisar)** ni podrá crear o editar un perfil de supervisión que se utilice para supervisar túneles de IPSec y supervisar un dispositivo de siguiente salto para reglas de reenvío basadas en políticas (PBF). Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración de perfil de supervisión actualmente definida, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Gestión de interfaz	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** ni podrá especificar los protocolos que se utilizan para gestionar el cortafuegos. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración de perfil de gestión de interfaz	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitación	Solo lectura	Deshabilita
	actualmente definida, pero no podrá añadir ni editar una configuración.			
Protección de zona	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** ni podrá configurar un perfil que determine cómo responde el cortafuegos ante ataques desde zonas de seguridad especificadas. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración de perfil de protección de zona actualmente definida, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Perfil de QoS	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **QoS**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **QoS** ni podrá configurar un perfil de QoS que determine cómo se tratan las clases de tráfico de QoS. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración de perfil de QoS actualmente definida, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Perfil de LLDP	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **LLDP**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **LLDP** ni podrá configurar un perfil LLDP que controle si las interfaces del cortafuegos pueden participar en el protocolo de detección de nivel de enlace. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración de perfil de LLDP actualmente definida, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Perfil BFD	Controla el acceso al nodo **Network Profiles (Perfiles de red)** > **BFD Profile (Perfil BFD)**. Si deshabilita este privilegio, el administrador no verá el nodo **Network Profiles (Perfiles de red)** > **BFD Profile (Perfil**	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	BFD) ni podrá configurar un perfil BFD. Un perfil de detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) le permite configurar los ajustes BFD para aplicar a una o más rutas o protocolos de enrutamiento. Por lo tanto, BFD detecta un enlace erróneo o peer BFD y permite una conmutación por error sumamente rápida. Si el estado del privilegio está establecido como de solo lectura, podrá ver el perfil BFD actualmente configurado, pero no podrá añadir ni editar un perfil BFD.			

Acceso detallado a la pestaña Dispositivo

Para definir los privilegios de acceso detallados de la pestaña **Device (Dispositivo)**, cuando cree o edite un perfil de función de administrador (**Device [Dispositivo]** > **Admin Roles [Funciones de administrador]**), desplácese hacia abajo hasta el nodo **Device (Dispositivo)** en la pestaña **WebUI (Interfaz web)**.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Configuración	Controla el acceso al nodo **Configuración**. Si deshabilita este privilegio, el administrador no ve el nodo **Setup (Configuración)** ni tiene acceso a la información de configuración de todo el cortafuegos, como datos de configuración de la gestión, las operaciones, el servicio, las sesiones, Content-ID o WildFire. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
Gestión	Controla el acceso al nodo **Management**. Si deshabilita este privilegio, el administrador no podrá configurar los ajustes tales como el nombre de host, el dominio, la zona horaria, la autenticación, la creación de logs e informes, las conexiones a Panorama, el banner, los mensajes y la configuración de complejidad de contraseña, entre otros. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
Operaciones	Controla el acceso a los nodos **Operations (Operaciones)** y **Telemetry and Threat**	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	Intelligence (Información de telemetría y amenazas). Si deshabilita este privilegio, el administrador no podrá realizar las siguientes tareas: • Cargar configuraciones de cortafuegos. • Guarde o restaure la configuración del cortafuegos. *Este privilegio solo se aplica a las opciones Device (Dispositivo) > Operations (Operaciones). Los privilegios Save (Guardar) y Commit (Confirmar) controlan si el administrador puede guardar o restaurar las configuraciones con las opciones Config (Configuración) > Save (Guardar) y Config (Configuración) > Revert (Restaurar).* • Crear grupos personalizados. • Configurar la supervisión de SNMP de la configuración del cortafuegos. • Configurar la función de servicio de estadísticas. • Realizar la configuración de **Telemetry and Threat Intelligence (Inteligencia de telemetría y amenazas)**. Solo los administradores con la función de superusuario predefinida pueden exportar o importar configuraciones de cortafuegos y apagar el cortafuegos. Solo los administradores con función de superusuario o administrador de dispositivo predefinida pueden reiniciar el cortafuegos o reiniciar el plano de datos. Los administradores con una función que permite acceder solo a sistemas virtuales específicos no pueden cargar, guardar o restaurar la configuración del cortafuegos con las opciones **Device (Dispositivo)** > **Operations (Operaciones)**.			
Services	Controla el acceso al nodo **Services (Servicios)**. Si deshabilita este privilegio, el administrador no podrá configurar servicios para los	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	servidores DNS, un servidor de actualización, un servidor proxy o servidores NTP, ni configurar rutas de servicio. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.			
Content-ID	Controla el acceso al nodo **Content-ID**. Si deshabilita este privilegio, el administrador no podrá configurar el filtrado URL o Content-ID. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
WildFire	Controla el acceso al nodo **WildFire**. Si deshabilita este privilegio, el administrador no podrá configurar los ajustes de WildFire. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
session	Controla el acceso al nodo **Session (Sesión)**. Si deshabilita este privilegio, el administrador no podrá configurar los ajustes de sesión ni los tiempos de espera para TCP, UDP o ICMP, ni configurar el cifrado o los ajustes de sesión VPN. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
HSM	Controla el acceso al nodo **HSM**. Si deshabilita este privilegio, el administrador no podrá configurar un módulo de seguridad de hardware. Si el estado del privilegio está establecido como de solo lectura, podrá ver la configuración actual, pero no podrá realizar ningún cambio.	yes (sí)	yes (sí)	yes (sí)
High Availability	Controla el acceso al nodo **High Availability (Alta disponibilidad)**. Si deshabilita este privilegio, el administrador no verá el nodo **High Availability** ni tendrá acceso a información de configuración de alta	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	disponibilidad de todo el cortafuegos, como información de configuración general o supervisión de enlaces y rutas. Si establece este privilegio como de solo lectura, el administrador podrá ver información de configuración de alta disponibilidad del cortafuegos, pero no tendrá permiso para realizar ningún procedimiento de configuración.			
Auditoría de configuraciones	Controla el acceso al nodo **Config Audit (Auditoría de configuraciones)**. Si deshabilita este privilegio, el administrador no verá el nodo **Config Audit (Auditoría de configuraciones)** ni tendrá acceso a la información de configuración de todo el cortafuegos.	yes (sí)	No	yes (sí)
Administradores	Controla el acceso al nodo **Administrators (Administradores)**. Esta función solo puede permitirse para acceso a solo lectura. Si deshabilita este privilegio, el administrador no verá el nodo **Administrators (Administradores)** ni tendrá acceso a información sobre su propia cuenta de administrador. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de configuración de su propia cuenta de administrador. No verá información sobre las cuentas de otros administradores configuradas en el cortafuegos.	No	yes (sí)	yes (sí)
Funciones de gestor	Controla el acceso al nodo **Funciones de gestor**. Esta función solo puede permitirse para acceso a solo lectura. Si deshabilita este privilegio, el administrador no verá el nodo **Admin Roles (Funciones de administrador)** ni tendrá acceso a la información de todo el cortafuegos sobre la configuración de perfiles de función de administrador. Si establece este privilegio como de solo lectura, podrá ver la información de configuración de todas las funciones de administrador configuradas en el dispositivo.	No	yes (sí)	yes (sí)
Perfil de autenticación	Controla el acceso al nodo **Authentication Profile (Perfil de autenticación)**. Si	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	deshabilita este privilegio, el administrador no verá el nodo **Authentication Profile (Perfil de autenticación)** ni podrá crear o editar perfiles de autenticación que especifiquen la configuración de autenticación RADIUS, TACACS+, LDAP, Kerberos o SAML, autenticación multifactor (MFA), o autenticación de la base de datos local. PAN-OS utiliza perfiles de autenticación para autenticar administradores del cortafuegos y usuarios finales del portal de autenticación o GlobalProtect. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Authentication Profile (Perfil de autenticación)**, pero no podrá crear ni editar perfiles de autenticación.			
Secuencia de autenticación	Controla el acceso al nodo **Secuencia de autenticación**. Si deshabilita este privilegio, el administrador no verá el nodo**Secuencia de autenticación** ni podrá crear o editar una secuencia de autenticación. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Authentication Profile (Perfil de autenticación)**, pero no podrá crear ni editar una secuencia de autenticación.	yes (sí)	yes (sí)	yes (sí)
Virtual Systems	Controla el acceso al nodo **Sistemas virtuales**. Si deshabilita este privilegio, el administrador no verá ni podrá configurar sistemas virtuales. Si el estado del privilegio está establecido como de solo lectura, podrá ver los sistemas virtuales actualmente configurados, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)
Gateways compartidos	Controla el acceso al nodo **Puertas de enlace compartidas**. Los gateways compartidas permiten que los sistemas virtuales compartan una interfaz común para las comunicaciones externas. Si deshabilita este privilegio, el administrador no verá ni podrá configurar gateways compartidos. Si el estado del privilegio está establecido como de solo lectura, podrá ver los gateways compartidos actualmente configurados, pero no podrá añadir ni editar una configuración.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Identificación de usuarios	Controla el acceso al nodo **Identificación de usuarios**. Si deshabilita este privilegio, el administrador no verá el nodo **User Identification (Identificación de usuario)** ni tendrá acceso a la información de configuración de identificación de usuarios de todo el cortafuegos, como asignación de usuarios, seguridad de conexión, agentes de User-ID, agentes de servidor de terminal, configuración de asignación de grupos o configuración de portal de autenticación. Si establece este privilegio como de solo lectura, el administrador podrá ver información de configuración del cortafuegos, pero no tendrá permiso para realizar ningún procedimiento de configuración.	yes (sí)	yes (sí)	yes (sí)
Origen de información de VM	Controla el acceso al nodo **VM Information Source (Origen de información de VM)** que le permite configurar el agente de User-ID de Windows/cortafuegos que recopilará el inventario de VM automáticamente. Si deshabilita este privilegio, el administrador no verá el nodo **VM Information Source (Origen de información de VM)**. Si establece este privilegio como de solo lectura, el administrador podrá ver los orígenes de información de VM configurados, pero no podrá añadir, editar ni eliminar ningún origen. *Este privilegio no está disponible para los administradores Grupo de dispositivos y plantilla.*	yes (sí)	yes (sí)	yes (sí)
Gestión de certificados	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de certificados descritos a continuación.	yes (sí)	No	yes (sí)
certificates	Controla el acceso al nodo **Certificates (Certificados)**. Si deshabilita este privilegio, el administrador no verá el nodo **Certificates (Certificados)** ni podrá configurar o acceder a información relativa a certificados de dispositivos o entidades de certificación de confianza predeterminadas. Si establece este privilegio como de solo lectura, el administrador podrá ver información de configuración de certificados	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitación	Solo lectura	Deshabilita
	para el cortafuegos, pero no tendrá permiso para realizar ningún procedimiento de configuración.			
Perfil del certificado	Controla el acceso al nodo **Certificate Profile (Perfil del certificado)**. Si deshabilita este privilegio, el administrador no verá el nodo **Certificate Profile (Perfil del certificado)** ni podrá crear perfiles del certificado. Si establece este privilegio como de solo lectura, el administrador podrá ver perfiles del certificado actualmente configurados para el cortafuegos, pero no tendrá permiso para crear o editar un perfil del certificado.	yes (sí)	yes (sí)	yes (sí)
OCSP responder	Controla el acceso al nodo **OCSP responder**. Si deshabilita este privilegio, el administrador no verá el nodo **OCSP responder (Respondedor OCSP)** ni podrá definir un servidor que se utilizará para comprobar el estado de revocación de los certificados emitidos por el cortafuegos. Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **OCSP Responder (Respondedor OCSP)** del cortafuegos, pero no tendrá permiso para crear o editar una configuración de respondedor OCSP.	yes (sí)	yes (sí)	yes (sí)
Perfil de servicio SSL/TLS	Controla el acceso al nodo **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**. Si deshabilita este privilegio, el administrador no verá el nodo o configurará un perfil que especifica una versión o rango de versiones de protocolo y un certificado para los servicios de cortafuego que usen SSL/TLS. Si establece este privilegio como de solo lectura, el administrador podrá ver los perfiles de servicio SSL/TLS existentes, pero no puede crearlos ni editarlos.	yes (sí)	yes (sí)	yes (sí)
SCEP	Controla el acceso al nodo **SCEP**. Si deshabilita este privilegio, el administrador no verá el nodo ni podrá definir un perfil que especifique los ajustes de protocolo de inscripción de certificados simple (simple certificate enrollment protocol, SCEP) para emitir certificados de dispositivo únicos.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	Si establece este privilegio como de solo lectura, el administrador podrá ver los perfiles de SCEP existentes, pero no puede crearlos ni editarlos.			
Exclusión de descifrado SSL	Controla el acceso al nodo **SSL Decryption Exclusion (Exclusiones de descifrado SSL)**. Si deshabilita este privilegio, el administrador no verá el nodo ni podrá ver las exclusiones personalizadas de adición de cifrado SSL. Si establece este privilegio como de solo lectura, el administrador verá las excepciones de cifrado SSL existentes, pero no podrá crearlas ni editarlas.	yes (sí)	yes (sí)	yes (sí)
Páginas de respuesta	Controla el acceso al nodo **Response Pages (Páginas de respuesta)**. Si deshabilita este privilegio, el administrador no verá el nodo **Response Page (Páginas de respuesta)** ni podrá definir un mensaje HTML personalizado que se descarga y se visualiza en lugar de una página web o archivo solicitado. Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Response Page (Página de respuesta)** del cortafuegos, pero no tendrá permiso para crear o editar la configuración de una página de respuesta.	yes (sí)	yes (sí)	yes (sí)
Configuración de log	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de log descritos a continuación.	yes (sí)	No	yes (sí)
Sistema	Controla el acceso al nodo **Log Settings (Configuración de log)** > **System (Sistema)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **System (Sistema)** ni especificar los logs del sistema que el cortafuegos reenvía a Panorama o a los servicios externos (como un servidor syslog). Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **System (Sistema)** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.	yes (sí)	yes (sí)	yes (sí)
Configuración	Controla el acceso al nodo **Log Settings (Configuración de log)** > **Configuration**	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	(Configuración). Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **Configuration (Configuración)** ni especificar los logs de configuración que el cortafuegos reenvía a Panorama o a los servicios externos (como un servidor syslog). Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **Configuration (Configuración)** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.			
User-ID	Controla el acceso al nodo **Log Settings (Configuración de log)** > **User-ID (ID de usuario)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **User-ID (ID de usuario)** ni especificar los logs de User-ID que el cortafuegos reenvía a Panorama o a los servicios externos (como un servidor syslog). Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **User-ID (ID de usuario)** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.	yes (sí)	yes (sí)	yes (sí)
Coincidencia HIP	Controla el acceso al nodo **Log Settings (Configuración de log)** > **HIP Match (Coincidencias HIP)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **HIP Match (Coincidencias HIP)** ni especificar el perfil de información de host (Host Information Profile, HIP) que coincide con los logs que el cortafuegos reenvía a Panorama o a los servicios externos (como un servidor syslog). Los logs de coincidencia HIP ofrecen información sobre las reglas de la política de seguridad que se aplican a los endpoints de GlobalProtect. Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **HIP** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
GlobalProtect	Controla el acceso al nodo **Log Settings (Configuración de log)** > **GlobalProtect**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **GlobalProtect** ni especificar los logs de GlobalProtect que el cortafuegos reenvía a Panorama o a los servicios externos (como un servidor Syslog). Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **GlobalProtect** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.	yes (sí)	yes (sí)	yes (sí)
Correlación	Controla el acceso al nodo **Log Settings (Configuración de log)** > **Correlation (Correlación)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **Correlation (Correlación)** ni agregar, eliminar o modificar la configuración de reenvío de logs de correlación, o etiquetar direcciones IP de origen o de destino. Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **Correlation (Correlación)** del cortafuegos, pero no tendrá permiso para agregar, editar o eliminar la configuración.	yes (sí)	yes (sí)	yes (sí)
Configuración de alarma	Controla el acceso al nodo **Log Settings (Configuración de log)** > **Alarm Settings (Configuración de alarma)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Log Settings (Configuración de log)** > **Alarm Settings (Configuración de alarma)** ni configurar las notificaciones que genera el cortafuegos cuando se encuentran coincidencias con una regla (o un grupo de reglas) de la política de seguridad de manera repetida dentro de un período de tiempo configurable. Si establece este privilegio como de solo lectura, el administrador podrá ver la configuración de **Log Settings (Configuración de log)** > **Alarm Settings (Configuración de alarma)** del cortafuegos, pero no tendrá permiso para editar la configuración.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitación	Solo lectura	Deshabilita
Gestionar logs	Controla el acceso al nodo **Log Settings (Configuración de log)** > **Manage Logs (Gestionar logs)**. Si deshabilita este privilegio, el administrador no verá el nodo **Log Settings (Configuración de log)** > **Manage Logs (Gestionar logs)** ni podrá borrar los logs indicados. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Log Settings (Configuración de log)** > **Manage Logs (Gestionar logs)**, pero no podrá borrar ninguno de los logs.	yes (sí)	yes (sí)	yes (sí)
Perfiles de servidores	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de perfiles de servidor descritos a continuación.	yes (sí)	No	yes (sí)
SNMP Trap	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **SNMP Trap (Trampa SNMP)**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **SNMP Trap (Trampa SNMP)** ni podrá especificar uno o más destinos de la captura de SNMP que deben utilizarse en las entradas de log del sistema. Si define este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **SNMP Trap Logs (Logs de trampa SNMP)**, pero no podrá especificar los destinos de la captura de SNMP.	yes (sí)	yes (sí)	yes (sí)
Syslog	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **Syslog**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **Syslog** ni podrá especificar uno o más servidores syslog. Si define este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **Syslog**, pero no podrá especificar los servidores syslog.	yes (sí)	yes (sí)	yes (sí)
EMAIL	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **Email (Correo electrónico)**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **Email (Correo**	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitación	Solo lectura	Deshabilita
	electrónico) ni podrá configurar un perfil de correo electrónico que pueda utilizarse para habilitar las notificaciones de correo electrónico para las entradas de log del sistema y la configuración. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **Email (Correo electrónico)**, pero no podrá configurar un perfil de correo electrónico.			
HTTP	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **HTTP**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **HTTP** ni podrá configurar un perfil de servidor HTTP que pueda utilizarse para habilitar los logs que reenvían entradas de log a destinos HTTP. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **HTTP**, pero no podrá configurar un perfil de servidor HTTP.	yes (sí)	yes (sí)	yes (sí)
Netflow	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **Netflow**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **Netflow** ni podrá definir un perfil de servidor de NetFlow, que especifica la frecuencia de la exportación, además de los servidores NetFlow que recibirán los datos exportados. Si define este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **Netflow**, pero no podrá definir un perfil de Netflow.	yes (sí)	yes (sí)	yes (sí)
RADIUS	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **RADIUS**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **RADIUS** ni podrá configurar los servidores RADIUS que se identifican en perfiles de autenticación. Si define este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** >	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	RADIUS, pero no podrá configurar los servidores RADIUS.			
TACACS+	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **TACACS+**. Si deshabilita este privilegio, el administrador no verá el nodo ni podrá configurar los ajustes para los servidores TACACS+ a los que se hace referencia en los perfiles de autenticación. Si establece este privilegio como de solo lectura, el administrador podrá ver los perfiles de servidor TACACS+ existentes, pero no puede añadirlos ni editarlos.	yes (sí)	yes (sí)	yes (sí)
LDAP:	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **LDAP**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **LDAP** ni podrá configurar los servidores LDAP que se utilizarán para la autenticación con los perfiles de autenticación. Si define este privilegio como de solo lectura, el administrador verá la información de **Server Profiles (Perfiles de servidor)** > **LDAP**, pero no podrá configurar los servidores LDAP.	yes (sí)	yes (sí)	yes (sí)
Kerberos	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **Kerberos**. Si deshabilita este privilegio, el administrador no verá el nodo **Server Profiles (Perfiles de servidor)** > **Kerberos** ni podrá configurar un servidor Kerberos que permite a los usuarios autenticarse de manera nativa en un controlador de dominios. Si define este privilegio como de solo lectura, el administrador podrá ver **Server Profiles (Perfiles de servidor)** > **Kerberos**, pero no podrá configurar los servidores Kerberos.	yes (sí)	yes (sí)	yes (sí)
Proveedor de identidad SAML	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)**. Si desactiva este privilegio, el administrador no podrá ver el nodo ni configurar los perfiles de servidor del proveedor de identidad (IdP) SAML. Si establece este privilegio como de solo lectura, el administrador podrá ver la	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	información de **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)**, pero no podrá configurar los perfiles de servidor del IdP SAML.			
Autenticación de múltiples factores	Controla el acceso al nodo **Server Profiles (Perfiles de servidor)** > **Multi Factor Authentication (Autenticación multifactor)**. Si desactiva este privilegio, el administrador no podrá ver el nodo ni configurar los perfiles de servidor de autenticación multifactor (MFA). Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)**, pero no podrá configurar los perfiles de servidor de MFA.			
Base de datos de usuario local	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de base de datos de usuario local descritos a continuación.	yes (sí)	No	yes (sí)
Usuarios	Controla el acceso al nodo **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)**. Si deshabilita este privilegio, el administrador no verá el nodo **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)** ni configurará una base de datos local en el cortafuegos para almacenar información de autenticación para usuarios con acceso remoto, administradores de cortafuegos y usuarios del portal de autenticación. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)**, pero no podrá configurar una base de datos local en el cortafuegos para almacenar información de autenticación.	yes (sí)	yes (sí)	yes (sí)
Grupos de usuarios	Controla el acceso al nodo **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)**. Si deshabilita este privilegio, el administrador no verá el nodo **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)** ni podrá añadir información de grupos de usuarios a la base de datos local.	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitación	Solo lectura	Deshabilita
	Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Local User Database (Base de datos de usuario local)** > **Users (Usuarios)**, pero no podrá añadir información de grupos de usuarios a la base de datos local.			
Dominio de acceso	Controla el acceso al nodo **Access Domain (Dominio de acceso)**. Si deshabilita este privilegio, el administrador no verá el nodo **Access Domain** ni podrá crear o editar un dominio de acceso. Si define este privilegio como de solo lectura, el administrador podrá ver la información de **Access Domain (Dominio de acceso)**, pero no se puede crear ni editar un dominio de acceso.	yes (sí)	yes (sí)	yes (sí)
Programación de la exportación de logs	Controla el acceso al nodo **Scheduled Log Export (Exportación de logs programada)**. Si deshabilita este privilegio, el administrador no verá el nodo **Scheduled Log Export (Exportación de logs programada)** ni podrá programar exportaciones de logs y guardarlas en un servidor de protocolo de transferencia de archivos (File Transfer Protocol, FTP) en formato CSV o utilizar copias seguras (Secure Copy, SCP) para transferir datos de forma segura entre el cortafuegos y un host remoto. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Scheduled Log Export Profile (Perfil de programación de la exportación de logs)**, pero no podrá programar la exportación de logs.	yes (sí)	No	yes (sí)
Software	Controla el acceso al nodo **Software**. Si deshabilita este privilegio, el administrador no verá el nodo **Software**, no verá las versiones más recientes del software PAN-OS disponibles desde Palo Alto Networks, no leerá las notas de cada versión ni seleccionará una versión para su descarga e instalación. Si establece este privilegio como de solo lectura, el administrador podrá ver la información de **Software**, pero no podrá descargar ni instalar software.	yes (sí)	yes (sí)	yes (sí)
Cliente de GlobalProtect	Controla el acceso al nodo **Cliente de GlobalProtect**. Si deshabilita este privilegio, el administrador no verá el nodo **GlobalProtect**	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	Client (Cliente de GlobalProtect), no verá las versiones de GlobalProtect disponibles, no descargará el código ni activará la aplicación de GlobalProtect. Si establece este privilegio como de solo lectura, el administrador podrá ver las versiones de **GlobalProtect Client (Cliente de GlobalProtect)** disponibles, pero no podrá descargar ni instalar el software de la aplicación.			
Actualizaciones dinámicas	Controla el acceso al nodo **Dynamic Updates (Actualizaciones dinámicas)**. Si deshabilita este privilegio, el administrador no verá el nodo **Dynamic Updates (Actualizaciones dinámicas)**, no podrá ver las actualizaciones más recientes, no podrá leer las notas de versión de cada actualización ni podrá seleccionar una actualización para su carga e instalación. Si establece este privilegio como de solo lectura, el administrador podrá ver las versiones de **Dynamic Updates (Actualizaciones dinámicas)** disponibles y leer las notas de versión, pero no podrá cargar ni instalar el software.	yes (sí)	yes (sí)	yes (sí)
Licencias	Controla el acceso al nodo **Licenses (Licencias)**. Si deshabilita este privilegio, el administrador no verá el nodo **Licenses (Licencias)** ni podrá ver las licencias instaladas o las licencias activas. Si establece este privilegio como de solo lectura, el administrador podrá ver las **Licenses (Licencias)** instaladas, pero no podrá realizar funciones de gestión de licencias.	yes (sí)	yes (sí)	yes (sí)
Soporte	Controla el acceso al nodo **Support (Asistencia técnica)**. Si deshabilita este privilegio, el administrador no podrá ver el nodo **Support (Asistencia técnica)**, activar la asistencia ni acceder a las alertas de producción y seguridad de Palo Alto Networks. Si establece este privilegio como de solo lectura, el administrador podrá ver el nodo **Support (Asistencia técnica)** y acceder a alertas de producción y seguridad, pero no podrá activar la asistencia técnica. Solo los administradores con la función de superusuario predefinida pueden utilizar	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	el nodo **Support (Asistencia técnica)** para generar archivos de asistencia técnica, o generar y descargar archivos de volcado de estadísticas y de núcleo.			
Clave maestra y diagnóstico	Controla el acceso al nodo **Master Key and Diagnostics (Clave maestra y diagnóstico)**. Si deshabilita este privilegio, el administrador no verá el nodo **Master Key and Diagnostics (Clave maestra y diagnóstico)** ni podrá especificar una clave maestra para cifrar claves privadas en el cortafuegos. Si establece este privilegio como de solo lectura, el administrador podrá ver el nodo **Master Key and Diagnostics (Clave maestra y diagnóstico)** y ver información sobre claves maestras que se han especificado, pero no podrá añadir ni editar una nueva configuración de clave maestra.	yes (sí)	yes (sí)	yes (sí)

Definición de ajustes de privacidad de usuario en el perfil de función de administrador

Para definir los datos privados de usuario final a los que tendrá acceso un administrador, cuando cree o edite un perfil de función de administrador (**Device [Dispositivo]** > **Admin Roles [Funciones de administrador]**), desplácese hacia abajo hasta la opción **Privacy (Privacidad)** en la pestaña **WebUI (Interfaz web)**.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Privacidad	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes de privacidad descritos a continuación.	yes (sí)	n/c	yes (sí)
Mostrar direcciones IP completas	Cuando la opción está deshabilitada, las direcciones IP completas obtenidas a través del tráfico que pasa por el cortafuegos de Palo Alto Networks no se muestran en logs ni informes. En lugar de las direcciones IP que suelen mostrarse, aparecerá la subred relevante. *Los informes programados que se muestran en la interfaz mediante Monitor (Supervisar) > Reports (Informes) y los informes que se envían a través*	yes (sí)	n/c	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	de correos electrónicos programados seguirán mostrando direcciones IP completas. Debido a esta excepción, se recomienda deshabilitar los siguientes ajustes de la pestaña Monitor (Supervisión): Informes personalizados, Informes de aplicación, Informes de amenazas, Informes de filtrado de URL, Informes de tráfico y Programador de correo electrónico.			
Visualización de los nombres de usuario en los logs e informes	Cuando la opción está deshabilitada, los nombres de usuario obtenidos a través del tráfico que pasa por el cortafuegos de Palo Alto Networks no se muestran en logs ni informes. Las columnas donde normalmente aparecerían los nombres de usuario están vacías.  *Los informes programados que se muestran en la interfaz mediante Monitor (Supervisar) > Reports (Informes) o los informes que se envían mediante el programador de correo electrónico seguirán mostrando nombres de usuario. Debido a esta excepción, recomendamos deshabilitar los siguientes ajustes en la pestaña Supervisar: Informes personalizados, Informes de aplicación, Informes de amenazas, Informes de filtrado de URL, Informes de tráfico y Programador de correo electrónico.*	yes (sí)	n/c	yes (sí)
Ver archivos de PCAP	Cuando la opción está deshabilitada, los archivos de captura de paquetes que suelen estar disponibles en los logs de tráfico, amenaza y filtrado de datos no se muestran.	yes (sí)	n/c	yes (sí)

© 2020 Palo Alto Networks, Inc.

Restricción del acceso de administrador a funciones de confirmación y validación

Para restringir el acceso con el fin de confirmar (y anular), guardar y validar las funciones cuando crea o edita un perfil de función de administrador (**Device [Dispositivo]** > **Admin Roles [Funciones de administrador]**), desplácese hacia abajo hasta las opciones **Commit (Confirmar)**, **Save (Guardar)** y **Validate (Validar)** en la pestaña **WebUI**.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Commit (Confirmar)	Establece el estado predeterminado en habilitado o deshabilitado para todos los privilegios de confirmación y restauración que se describen a continuación.	yes (sí)	n/c	yes (sí)
Dispositivo	Cuando se encuentra deshabilitado, un administrador no puede confirmar o restaurar cambios que cualquier administrador haya realizado en la configuración del cortafuegos, lo que incluye sus propios cambios.	yes (sí)	n/c	yes (sí)
Confirmación para otros administradores	Cuando se encuentra deshabilitado, un administrador no puede confirmar o restaurar cambios que otros administradores hayan realizado en la configuración del cortafuegos.	yes (sí)	n/c	yes (sí)
Guardar	Establece el estado predeterminado en habilitado o deshabilitado para todos los privilegios de guardado de operación que se describen a continuación.	yes (sí)	n/c	yes (sí)
Guardado parcial	Cuando se encuentra deshabilitado, un administrador no puede guardar cambios que cualquier administrador haya realizado en la configuración del cortafuegos, lo que incluye sus propios cambios.	yes (sí)	n/c	yes (sí)
Guardar para otros administradores	Cuando se encuentra deshabilitado, un administrador no puede guardar cambios que otros administradores hayan realizado en la configuración del cortafuegos.	yes (sí)	n/c	yes (sí)
Validar	Cuando la opción está deshabilitada, un administrador no puede validar una configuración.	yes (sí)	n/c	yes (sí)

Acceso detallado a ajustes globales

Para definir la configuración global a la que tendrá acceso un administrador, cuando cree o edite un perfil de función de administrador (**Device [Dispositivo]** > **Admin Roles [Funciones de administrador]**), desplácese hacia abajo hasta la opción **Privacy (Privacidad)** en la pestaña **WebUI (Interfaz web)**.

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Global	Establece el estado predeterminado para habilitar o deshabilitar para todos los ajustes globales descritos a continuación. En este momento, este ajuste solamente es efectivo para Alarmas del sistema.	yes (sí)	n/c	yes (sí)
Alarmas del sistema	Cuando la opción está deshabilitada, un administrador no puede ver ni reconocer alarmas que se generen.	yes (sí)	n/c	yes (sí)

Concesión de acceso granular a la pestaña Panorama

La siguiente tabla muestra los niveles de acceso de pestaña **Panorama** y las funciones de administrador Panorama personalizado para los que están disponibles. Los administradores del cortafuegos no pueden acceder a ninguno de esos privilegios.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
Configuración	Especifica si el administrador puede ver o editar la información de configuración de Panorama, incluida la información de **Management (Gestión)**, **Operations (Operaciones)** y **Telemetry (Telemetría)**, **Services (Servicios)**, Content-ID, **WildFire**, sesión o **HSM**. Si este privilegio: • se define como de solo lectura, el administrador puede ver la información pero no editarla. • se deshabilita, el administrador no podrá ver ni editar la información.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
High Availability	Especifica si el administrador puede ver y gestionar los ajustes de alta disponibilidad (HA) para el servidor de gestión de Panorama. Si define este privilegio como de solo lectura, el administrador puede ver la información de configuración de HA para el servidor de gestión de Panorama pero no puede gestionar la configuración.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes de configuración de HA para el servidor de gestión de Panorama.				
Auditoría de configuraciones	Especifica si el administrador puede ejecutar las auditorías de configuración de Panorama. Si deshabilita este privilegio, el administrador no podrá ejecutar las auditorías de configuración de Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Administradores	Especifica si el administrador puede ver los detalles de la cuenta de administrador de Panorama. No puede habilitar el acceso completo a esta función: solo un acceso de solo lectura. (Solo los administradores con Panorama con una función dinámica pueden añadir, editar o eliminar administradores de Panorama.) Con un acceso de solo lectura, el administrador puede ver la información sobre su cuenta, pero ninguna otra cuenta de administrador de Panorama. Si deshabilita este privilegio, el administrador no puede ver información sobre ninguna cuenta de administrador de Panorama, incluyendo la suya propia.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	No	yes (sí)	yes (sí)
Funciones de gestor	Especifica si el administrador puede ver las funciones de administrador de Panorama. No puede habilitar el acceso completo a esta función: solo un acceso de solo lectura. (Solo los administradores con Panorama con una función dinámica pueden añadir, editar o eliminar funciones personalizadas de Panorama.) Con un acceso de solo lectura, el administrador puede ver configuraciones de función de administrador de Panorama, pero no puede configurarlas.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	No	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las funciones de administrador de Panorama.				
Dominio de acceso	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar los dominios de acceso de los administradores de Panorama. (Este privilegio solo controla el acceso a la configuración de dominios de acceso, no el acceso a los contextos de cortafuegos, grupos de dispositivos y plantillas que se han asignado a los dominios de acceso.) Si define este privilegio como de solo lectura, el administrador puede ver las configuraciones de dominio de acceso de Panorama, pero no gestionarlas. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las configuraciones de dominio de acceso de Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No *Puede asignar dominios de acceso a administradores de grupo de dispositivos y plantilla para que puedan acceder a los datos de supervisión y configuración en los contextos de cortafuegos, grupos de dispositivos y plantillas que se han asignado a esos dominios de acceso.*	yes (sí)	yes (sí)	yes (sí)
Perfil de autenticación	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar los perfiles de autenticación de los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	autenticación de Panorama pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de autenticación de Panorama.				
Secuencia de autenticación	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar las secuencias de autenticación de los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar las secuencias de autenticación de Panorama pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las secuencias de autenticación de Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Identificación de usuarios	Especifica si el administrador puede configurar la seguridad de conexión de User-ID y ver, añadir, editar o eliminar puntos de redistribución de datos (como agentes de User-ID). Si configura este privilegio como de solo lectura, el administrador puede ver los ajustes de la conexión de seguridad de User-ID y los puntos de redistribución, pero no puede gestionar la configuración. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes de la seguridad de conexión de User-ID ni los puntos de redistribución.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Dispositivos gestionados	Especifica si el administrador puede ver, añadir, editar o eliminar cortafuegos como dispositivos gestionados, e instalar actualizaciones de contenido o software en ellos. Si define este privilegio como de solo lectura, el administrador	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí) (No para las funciones de Grupo de	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	puede ver los cortafuegos gestionados, pero no añadirlos, eliminarlos, etiquetarlos ni instalar actualizaciones. Si deshabilita a este privilegio, el administrador no podrá ver, añadir, editar, etiquetar ni eliminar cortafuegos gestionados ni instalarles actualizaciones. *Un administrador con privilegios de implementación de dispositivo podrá seguir usando las opciones Panorama > Device Deployment (Implementación de dispositivo) para instalar actualizaciones en cortafuegos gestionados.*		dispositivo y plantilla)		
Plantillas	Especifica si el administrador puede ver, editar, añadir o eliminar plantillas y pilas de plantillas. Si define este privilegio como de solo lectura, el administrador puede ver las configuraciones de plantilla y pila, pero no gestionarlas. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las configuraciones de plantilla y pila.	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí) *Los administradores de grupo de dispositivos y plantilla solo pueden ver las plantillas y pilas que se encuentran en los dominios de acceso asignados a esos administradores.*	yes (sí) (No para los administradores de Grupo de dispositivo y plantilla)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
Grupos de dispositivos	Especifica si el administrador puede ver, editar, añadir o eliminar grupos de dispositivos. Si define este privilegio como de solo lectura, el administrador puede ver las configuraciones de grupo de dispositivos, pero no gestionarlas. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las configuraciones de grupos de dispositivos.	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí) *Los administradores de grupo de dispositivos y plantilla solo pueden ver los grupos de dispositivos que se encuentran en los dominios de acceso asignados a esos administradores.*	yes (sí)	yes (sí)	yes (sí)
Recopiladores gestionados	Especifica si el administrador puede ver, editar, añadir o eliminar recopiladores gestionados. Si define este privilegio como de solo lectura, el administrador puede ver las configuraciones de recopiladores gestionados, pero no gestionarlas. Si deshabilita este privilegio, el administrador no podrá ver, editar, añadir ni eliminar las configuraciones de recopiladores gestionados. *Un administrador con privilegios de implementación de dispositivo podrá seguir usando las opciones Panorama > Device Deployment (Implementación de dispositivo)*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	para instalar actualizaciones en recopiladores gestionados.				
Grupos de recopiladores	Especifica si el administrador puede ver, editar, añadir o eliminar grupos de recopiladores. Si define este privilegio como de solo lectura, el administrador puede ver los grupos de recopiladores, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los grupos de recopiladores.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Administrador de servicios VMWare	Especifica si el administrador puede ver y editar ajustes de VMware Service Manager. Si define este privilegio como de solo lectura, el administrador puede ver los ajustes, pero no realizar ningún procedimiento operativo o de configuración relacionado. Si deshabilita este privilegio, el administrador no puede ver los ajustes ni realizar ningún procedimiento operativo o de configuración relacionado.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Gestión de certificados	Define el estado predeterminado, habilitado o deshabilitado de todos los privilegios de gestión de certificados de Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
certificates	Especifica si el administrador puede ver, editar, generar, eliminar, revocar, renovar o exportar certificados. Este privilegio también especifica si el administrador puede importar o exportar claves HA. Si define este privilegio como de solo lectura, el administrador puede ver los certificados de	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Panorama, pero no gestionar los certificados o las claves HA. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los certificados de Panorama ni las claves HA.				
Perfil del certificado	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar los perfiles de certificados de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de certificado de Panorama, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de certificados de Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Perfil de servicio SSL/TLS	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar los perfiles de servicios SSL/TLS. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servicio de SSL/TLS, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servicio SSL/TLS.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Configuración de log	Define el estado predeterminado, habilitado o deshabilitado de todos los privilegios de ajuste de logs.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Sistema	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de sistema a servicios externos (syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	puede ver los ajustes de reenvío de logs de sistema, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *Este privilegio se aplica únicamente a los logs de sistema que genera Panorama y los recopiladores de logs. El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups) controla el reenvío de logs de sistema que los recopiladores de log reciben de los cortafuegos. El privilegio Device (Dispositivo)Log Settings (Configuración de log) > System (Sistema) controla el reenvío de logs desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de log).*				
Configurar	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de configuración a servicios externos (syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	de logs de configuración, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *Este privilegio se aplica únicamente a los logs de configuración que genera Panorama y los recopiladores de logs. El privilegio* Collector Groups (Grupos de recopiladores) *(Panorama > Collector Groups) controla el reenvío de logs de configuración que los recopiladores de log reciben de los cortafuegos. El privilegio Device (Dispositivo)Log Settings (Configuración de log) > Configuration (Configuración) controla el reenvío de logs desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).*				
User-ID	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de User-ID a servicios externos (syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	de logs de configuración, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *Este privilegio se aplica únicamente a los logs de User-ID que genera Panorama y los recopiladores de logs. El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups) controla el reenvío de logs de User-ID que los recopiladores de log reciben de los cortafuegos. El privilegio Device (Dispositivo)Log Settings (Configuración de log) > User-ID (ID de usuario) controla el reenvío de logs desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).*				
Coincidencia HIP	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de coincidencia HIP desde un dispositivo virtual Panorama en modo heredado a servicios externos (Syslog, correo electrónico o servidores de captura de SNMP). Si define este privilegio como de solo lectura, el administrador	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	puede ver los ajustes de reenvío de logs de coincidencia HIP, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups) controla el reenvío de logs de coincidencia HIP que los recopiladores de log reciben de los cortafuegos. El privilegio Device (Dispositivo)Log Settings (Configuración de log) > HIP Match (Coincidencia de HIP) controla el reenvío de logs desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).*				
GlobalProtect	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de GlobalProtect desde un dispositivo virtual Panorama en modo heredado a servicios externos (syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío de logs de GlobalProtect, pero no gestionarlos.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups (Grupos de recopiladores)) controla el reenvío de logs de GlobalProtect que los recopiladores de log reciben de los cortafuegos. El privilegio Device (Dispositivo) > Log Settings (Configuración de log) > GlobalProtect controla el reenvío de logs desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).*				
Correlación	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de correlación desde un dispositivo virtual Panorama en modo heredado a servicios externos (Syslog, correo electrónico o servidores de captura de SNMP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío de logs de correlación, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups) controla el reenvío de logs de correlación desde un dispositivo serie M de Panorama o dispositivo virtual Panorama en modo Panorama.				
Tráfico	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de tráfico desde un dispositivo virtual Panorama en modo heredado a servicios externos (Syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío de logs de tráfico, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups) controla el reenvío de logs de tráfico que los recopiladores de log reciben de los cortafuegos. El privilegio {0>Log Forwarding (Reenvío de logs)<0} ({0>{0>Objects*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	[Objetos]<0} {0>Log Forwarding<0}<0}) controla el reenvío desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).				
threat	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de amenazas desde un dispositivo virtual Panorama en modo heredado a servicios externos (Syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío de logs de amenazas, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes. *El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups [Grupos de recopiladores]) controla el reenvío de logs de amenaza que los recopiladores de log reciben de los cortafuegos. El privilegio {0>Log Forwarding (Reenvío de logs)<0} ({0>{0>Objects [Objetos]<0}*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	{0>Log Forwarding<0}<0}) controla el reenvío desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).				
WildFire	Especifica si el administrador puede ver y configurar los ajustes que controlan el reenvío de los logs de WildFire desde un dispositivo virtual Panorama en modo heredado a servicios externos (Syslog, correo electrónico, servidores de captura de SNMP o servidores HTTP). Si define este privilegio como de solo lectura, el administrador puede ver los ajustes de reenvío de logs de WildFire, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los ajustes.  *El privilegio Collector Groups (Grupos de recopiladores) (Panorama > Collector Groups [Grupos de recopiladores]) controla el reenvío de logs de WildFire que los recopiladores de log reciben de los cortafuegos. El privilegio {0>Log Forwarding (Reenvío de logs)<0} ({0>{0>Objects [Objetos]<0} {0>Log*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Forwarding<0}<0}) controla el reenvío desde los cortafuegos directamente a servicios externos (sin agregación en los recopiladores de logs).				
Perfiles de servidores	Define el estado predeterminado, habilitado o deshabilitado de todos los privilegios de perfil de servidor.  *Estos privilegios solo pertenecen a los perfiles de servidor que se usan para reenviar logs de Panorama o los recopiladores de logs, y los perfiles de servidor que se usan para autenticar a los administradores de Panorama. Los privilegios Device (Dispositivo) > Server Profiles (Perfiles de servidor) controlan el acceso a los perfiles de servidor que se usan para reenviar logs directamente desde los cortafuegos a servicios externos y para autenticar administradores de cortafuegos.*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
SNMP Trap	Especifica si el administrador puede ver y configurar perfiles de servidor de captura de SNMP. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	servidor de captura de SNMP, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor de captura de SNMP.				
Syslog	Especifica si el administrador puede ver y configurar perfiles de servidor Syslog. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor de Syslog pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor de Syslog.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
EMAIL	Especifica si el administrador puede ver y configurar perfiles de servidor de correo electrónico. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor de correo electrónico, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor de correo electrónico.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
RADIUS	Especifica si el administrador puede ver y configurar los perfiles de servidor RADIUS que se usan para autenticar a los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor de RADIUS, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor de RADIUS.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
TACACS+	Especifica si el administrador puede ver y configurar los perfiles de servidor TACACS+ que se usan para autenticar a los administradores de Panorama. Si deshabilita este privilegio, el administrador no verá el nodo ni podrá configurar los ajustes para los servidores TACACS+ a los que se hace referencia en los perfiles de autenticación. Si establece este privilegio como de solo lectura, el administrador podrá ver los perfiles de servidor TACACS+ existentes, pero no puede añadirlos ni editarlos.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
LDAP:	Especifica si el administrador puede ver y configurar los perfiles de servidor LDAP que se usan para autenticar a los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor LDAP, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor LDAP.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Kerberos	Especifica si el administrador puede ver y configurar los perfiles de servidor Kerberos que se usan para autenticar a los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor Kerberos, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor Kerberos.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
Proveedor de identidad SAML	Especifica si el administrador puede ver y configurar los perfiles de servidor de proveedor de identidad (IdP) SAML que se usan para autenticar a los administradores de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar los perfiles de servidor IdP SAML, pero no gestionarlos. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar los perfiles de servidor IdP SAML.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Exportación de configuración programada	Especifica si el administrador puede ver, añadir, editar, eliminar o duplicar las exportaciones de configuración programada de Panorama. Si define este privilegio como de solo lectura, el administrador puede visualizar las exportaciones programadas de Panorama, pero no gestionarlas. Si deshabilita este privilegio, el administrador no podrá ver ni gestionar las exportaciones programadas.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	No	yes (sí)
Software	Especifica si el administrador puede: ver información sobre las actualizaciones de software instaladas en el servidor de gestión de Panorama; descargar, cargar o instalar actualizaciones; y ver las notas de la versión asociadas. Si define este privilegio como de solo lectura, el administrador puede ver información sobre las actualizaciones de software de Panorama y ver las notas de versión asociadas, pero no puede realizar ninguna operación relacionada. Si deshabilita este privilegio, el administrador no puede ver las	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	actualizaciones de software de Panorama, consultar las notas de versión asociadas ni realizar ninguna operación relacionada. *El privilegio Panorama > Device Deployment (Implementación de dispositivo) > Software controla el acceso al software PAN-OS implementado en cortafuegos y el software Panorama implementado en recopiladores de log dedicados.*				
Actualizaciones dinámicas	Especifica si el administrador puede: ver información sobre las actualizaciones de contenido instaladas en el servidor de gestión de Panorama (por ejemplo, actualizaciones de WildFire); descargar, cargar, instalar o revertir las actualizaciones; y ver las notas de la versión asociadas. Si define este privilegio como de solo lectura, el administrador puede ver información sobre las actualizaciones de contenido de Panorama y ver las notas de versión asociadas, pero no puede realizar ninguna operación relacionada. Si deshabilita este privilegio, el administrador no puede ver las actualizaciones de contenido de Panorama, consultar las notas de versión asociadas ni realizar ninguna operación relacionada. *El privilegio Panorama > Device Deployment*	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	(Implementación de dispositivo) > Dynamic Updates (Actualizaciones dinámicas) *controla el acceso a las actualizaciones de contenido implementadas en los cortafuegos y los recopiladores de log dedicados.*				
Soporte	Especifica si el administrador puede: ver información de la licencia de asistencia de Panorama, alertas de productos y de seguridad; habilitar una licencia de asistencia; y gestionar casos. Solo un administrador con función de superusuario puede generar archivos de asistencia técnica. Si define este privilegio como de solo lectura, el administrador puede ver información de asistencia de Panorama, alertas de productos y de seguridad; pero no activar una licencia de asistencia, generar archivos de asistencia tecnológica ni gestionar casos. Si deshabilita este privilegio, el administrador no puede: ver información de asistencia de Panorama, alertas de productos y de seguridad; activar una licencia de asistencia, generar archivos de asistencia tecnológica ni gestionar casos.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)
Implementación de dispositivo	Establece el estado predeterminado, habilitado o deshabilitado, para todos los privilegios asociados con las licencias de implementación y las actualizaciones de software o contenido en los cortafuegos y recopiladores de logs. *Los privilegios Panorama >*	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	Software *y* *Panorama* > Dynamic Updates (Actualizaciones dinámicas) *controlan las actualizaciones de software y contenido instaladas en un servidor de gestión de Panorama.*				
Software	Especifica si el administrador puede: ver información sobre las actualizaciones de software instaladas en cortafuegos y recopiladores de logs; descargar, cargar o instalar actualizaciones; y ver las notas de la versión asociadas. Si define este privilegio como de solo lectura, el administrador puede ver información sobre las actualizaciones de software de Panorama y ver las notas de versión asociadas, pero no puede implementar las actualizaciones en cortafuegos o recopiladores de logs dedicados. Si deshabilita este privilegio, el administrador no podrá ver información sobre las actualizaciones de software ni las notas de versión asociadas, como tampoco podrá implementar las actualizaciones en el cortafuegos o los recopiladores de logs dedicados.	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Cliente de GlobalProtect	Especifica si el administrador puede: ver información sobre las actualizaciones de software de la aplicación de GlobalProtect sobre cortafuegos; descargar, cargar o activar actualizaciones; y ver las notas de la versión asociadas. Si define este privilegio como de solo lectura, el administrador	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	puede ver información sobre las actualizaciones de software de la aplicación de GlobalProtect y ver las notas de versión asociadas, pero no puede activar las actualizaciones en cortafuegos. Si deshabilita este privilegio, el administrador no puede ver información sobre las actualizaciones de software de la aplicación de GlobalProtect, ver las notas de versión asociadas, ni activar las actualizaciones en cortafuegos.				
Actualizaciones dinámicas	Especifica si el administrador puede: ver información sobre las actualizaciones de contenido (por ejemplo, actualizaciones de aplicaciones) instaladas en cortafuegos y recopiladores de logs dedicados; descargar, cargar o instalar actualizaciones, y ver las notas de la versión asociadas. Si define este privilegio como de solo lectura, el administrador puede ver información sobre las actualizaciones de contenido de Panorama y ver las notas de versión asociadas, pero no puede implementar las actualizaciones en cortafuegos o recopiladores de logs dedicados. Si deshabilita este privilegio, el administrador no podrá ver información sobre las actualizaciones de contenido ni las notas de versión asociadas, como tampoco podrá implementar las actualizaciones en el cortafuegos o los recopiladores de logs dedicados.	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)
Licencias	Especifica si el administrador puede ver, actualizar y activar licencias de cortafuegos. Si define este privilegio como de solo lectura, el administrador puede ver las licencias de	Panorama: yes (sí) Plantilla/grupo de dispositivos: yes (sí)	yes (sí)	yes (sí)	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Disponibilidad de la función de administrador	Habilitac	Solo lectur	Deshab
	cortafuegos pero no actualizar ni activar esas licencias. Si desactiva este privilegio, el administrador no podrá ver, actualizar ni activar licencias de cortafuegos.				
Clave maestra y diagnóstico	Especifica si el administrador puede ver y configurar una clave maestra con la que cifrar claves privadas en Panorama. Si define este privilegio como de solo lectura, el administrador puede ver la configuración de clave maestra de Panorama, pero no cambiarla. Si deshabilita este privilegio, el administrador no podrá ver ni editar la configuración de clave maestra Panorama.	Panorama: yes (sí) Plantilla/grupo de dispositivos: No	yes (sí)	yes (sí)	yes (sí)

Privilegios de Acceso a la interfaz web de Panorama

Las funciones personalizadas de administrador de Panorama le permiten definir el acceso a las opciones de Panorama y le dan la capacidad de dar acceso únicamente a los grupos de dispositivos y plantillas (pestañas **Políticas**, **Objetos**, **Red** y **Dispositivo**).

Las funciones de administrador que puede crear son **Panorama** y **Device Group and Template**. No puede conceder privilegios de acceso al CLI a un perfil de función de administrador **Device Group and Template**. Si asigna privilegios de superusuario para el CLI a un perfil de función de administrador **Panorama**, los administradores con esa función pueden acceder a todas las funciones, independientemente de los privilegios de interfaz web que asigne.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Dashboard (Panel)	Controla el acceso a la pestaña **Panel**. Si deshabilita este privilegio, el administrador no verá la pestaña ni tendrá acceso a ninguno de los widgets del panel.	yes (sí)	No	yes (sí)
ACC	Controla el acceso al Centro de control de aplicaciones (Application Command Center, ACC). Si deshabilita este privilegio, la pestaña **ACC** no aparecerá en la interfaz web. Recuerde que si desea proteger la privacidad de sus usuarios y a la vez seguir proporcionando acceso al ACC,	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	puede deshabilitar la opción {0>**Privacy (Privacidad)Show Full IP Addresses (Mostrar direcciones IP completas)**<0} y/o la opción **Show User Names In Logs And Reports (Mostrar nombres de usuario en logs e informes)**.			
Monitor (Supervisar)	Controla el acceso a la pestaña **Monitor (Supervisar)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Monitor (Supervisar)** ni tendrá acceso a ninguno de los logs, capturas de paquetes, información de sesión, informes o Appscope. Para obtener un control más detallado sobre qué información de supervisión puede ver el administrador, deje la opción Monitor (Supervisar) habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Monitor (Supervisar).	yes (sí)	No	yes (sí)
Políticas	Controla el acceso a la pestaña **Políticas**. Si deshabilita este privilegio, el administrador no verá la pestaña **Políticas** ni tendrá acceso a ninguna información de política. Para obtener un control más detallado sobre qué información de políticas puede ver el administrador; por ejemplo, para habilitar el acceso a un tipo de política específico o para habilitar el acceso de solo lectura a información de políticas, deje la opción **Policies (Políticas)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Policy (Política).	yes (sí)	No	yes (sí)
Objetos	Controla el acceso a la pestaña **Objects (Objetos)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Objects (Objetos)** ni tendrá acceso a ninguno de los objetos, perfiles de seguridad, perfiles de reenvío de logs, perfiles de descifrado o programaciones. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Objects (Objetos)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Objects (Objetos).	yes (sí)	No	yes (sí)
network	Controla el acceso a la pestaña **Network (Red)**. Si deshabilita este privilegio, el	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	administrador no verá la pestaña **Network (Red)** ni tendrá acceso a ninguna información de configuración de interfaz, zona, VLAN, Virtual Wire, enrutador virtual, túnel de IPSec, DHCP, proxy DNS, GlobalProtect o QoS o a los perfiles de red. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Networks (Red)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Network (Red).			
Dispositivo	Controla el acceso a la pestaña **Device (Dispositivo)**. Si deshabilita este privilegio, el administrador no verá la pestaña **Device (Dispositivo)** ni tendrá acceso a ninguna información de configuración de todo el cortafuegos, como información de configuración de User-ID, alta disponibilidad, perfil de servidor o certificado. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Device (Dispositivo)** habilitada y, a continuación, habilite o deshabilite nodos específicos en la pestaña como se describe en Acceso detallado a la pestaña Device (Dispositivo). *No puede habilitar el acceso a los nodos Admin Roles (Funciones de administrador) o Administrators (Administradores) para un administrador basado en funciones, aunque habilite un acceso completo a la pestaña Device (Dispositivo).*	yes (sí)	No	yes (sí)
Panorama	Controla el acceso a la pestaña **Panorama**. Si deshabilita este privilegio, el administrador no verá la pestaña **Panorama** y no tendrá acceso a ninguna información de configuración en Panorama, como los Dispositivos gestionados, Recopiladores gestionados o Grupos de recopiladores. Para obtener un control más detallado sobre qué objetos puede ver el administrador, deje la opción **Panorama** habilitada y, a continuación, habilite o deshabilite nodos específicos en la	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
	pestaña como se describe en Acceso detallado a la pestaña Panorama.			
Privacidad	Controla el acceso a los ajustes de privacidad descritos en Definición de los ajustes de privacidad en el perfil de rol de administrador.	yes (sí)	No	yes (sí)
Validar	Cuando la opción está deshabilitada, un administrador no puede validar una configuración.	yes (sí)	No	yes (sí)
Guardar	Establece el estado predeterminado (habilitado o deshabilitado) para todos los privilegios de la función guardar que se describen a continuación (Guardado parcial y guardar para otros administradores).	yes (sí)	No	yes (sí)
• Guardado parcial	Cuando la opción está deshabilitada, un administrador no puede guardar ningún cambio que cualquier administrador haya realizado a la configuración de Panorama.	yes (sí)	No	yes (sí)
• Guardar para otros administradores	Cuando la opción está deshabilitada, un administrador no puede guardar ningún cambio que otros administradores hayan realizado a la configuración de Panorama.	yes (sí)	No	yes (sí)
Commit (Confirmar)	Configura el estado por defecto (habilitado o deshabilitado) para todos los privilegios de confirmación, envío y reversión que se describen a continuación (Panorama, grupos de dispositivos, plantillas, forzar valores de plantilla, grupos de recopiladores, clústeres de dispositivos WildFire).	yes (sí)	No	yes (sí)
• Panorama	Cuando la opción está deshabilitada, un administrador no puede confirmar ni revertir los cambios en la configuración que realicen los administradores, incluidos sus propios cambios.	yes (sí)	No	yes (sí)
• Confirmación para otros administradores	Cuando la opción está deshabilitada, un administrador no puede confirmar ni revertir los cambios en la configuración que realicen otros administradores.	yes (sí)	No	yes (sí)
Grupos de dispositivos	Cuando la opción está deshabilitada, un administrador no puede enviar los cambios a los grupos de dispositivos.	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Nivel de acceso	Description (Descripción)	Habilitació	Solo lectura	Deshabilita
Plantillas	Cuando la opción está deshabilitada, un administrador no puede enviar los cambios a las plantillas.	yes (sí)	No	yes (sí)
Forzar valores de plantilla	Este privilegio controla el acceso a la opción **Force Template Values (Forzar valores de plantilla)** del cuadro de diálogo Push Scope Selection (Selección del alcance del envío). Cuando la opción está deshabilitada, el administrador no puede reemplazar los ajustes invalidados en las configuraciones de cortafuegos locales con ajustes que Panorama envía de una plantilla. *Si envía una configuración con la opción Force Template Values (Forzar valores de plantilla) habilitada, todos los valores anulados del cortafuegos se reemplazarán por valores de la plantilla. Antes de usar esta opción, verifique los valores anulados en los cortafuegos para asegurarse de que la compilación no derive en interrupciones imprevistas de la red o en problemas causados por el reemplazo de los valores anulados.*	yes (sí)	No	yes (sí)
Grupos de recopiladores	Cuando la opción está deshabilitada, un administrador no puede enviar ningún cambio a los grupos de recopiladores.	yes (sí)	No	yes (sí)
Clústeres de dispositivos WildFire	Cuando la opción está deshabilitada, un administrador no puede enviar los cambios a los clústeres de dispositivos WildFire.	yes (sí)	No	yes (sí)
Tareas	Cuando la opción está deshabilitada, un administrador no puede acceder al Gestor de tareas.	yes (sí)	No	yes (sí)
Global	Controla el acceso a los ajustes globales (alarmas del sistema) que se describen en Acceso detallado a los ajustes globales.	yes (sí)	No	yes (sí)

© 2020 Palo Alto Networks, Inc.

Referencia: Uso de número de puerto

Las siguientes tablas enumeran los puertos que usan los cortafuegos de Palo Alto Networks para comunicarse entre sí o con otros servicios de la red.

- Puertos usados para funciones de gestión
- Puertos usados para HA
- Puertos usados para Panorama
- Puertos usados para GlobalProtect
- Puertos usados para User-ID

Puertos usados para funciones de gestión

El cortafuegos y Panorama utilizan los siguientes puertos para las funciones de gestión.

Puerto de destino	Protocolo	Description (Descripción)
22	TCP	Se usa para comunicarse desde un sistema cliente con la interfaz CLI del cortafuegos.
80	TCP	El puerto que escucha el cortafuegos para recibir actualizaciones del protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) cuando actúa como un respondedor OCSP.
123	UDP	Puerto que usa el cortafuegos para las actualizaciones NTP.
443	TCP	Se usa para comunicarse desde un sistema cliente con la interfaz web del cortafuegos. Este también es el puerto que el cortafuegos y el agente de User-ID escucha para recibir actualizaciones cuando realiza la Habilitación de la supervisión de VM para el registro de cambios en la red virtual. Este es el único puerto que se usa para la supervisión de un entorno AWS. Para supervisar un entorno VMware vCenter/ESXi, el puerto de escucha cambia de forma predeterminada a 443, aunque puede configurarse.
162	UDP	Puerto que el cortafuegos, Panorama o un recopilador de logs utiliza para el Reenvío de capturas a un administrador SNMP. *No es necesario que este puerto esté abierto en el cortafuegos de Palo Alto Networks. Debe configurar el protocolo simple de administración de redes (SNMP) para que escuche en este puerto. Si desea información detallada, consulte la documentación de software de gestión de SNMP.*
161	UDP	Puerto que escucha el cortafuegos para las solicitudes de sondeo (mensajes GET) del gestor SNMP.

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
514 514 6514	TCP UDP SSL	Puerto que utilizan el cortafuegos, Panorama o el recopilador de logs para enviar logs a un servidor Syslog si realiza la Configuración de la supervisión de Syslog; así como los puertos que escucha el agente de User-ID integrado en PAN-OS o el agente de User-ID basado en Windows para los mensajes de syslog de autenticación.
2055	UDP	Puerto predeterminado que utiliza el cortafuegos para enviar registros de NetFlow a un recopilador de NetFlow si realiza la Configuración de exportaciones de NetFlow, aunque esto puede configurarse.
5008	TCP	Puerto que el gestor de seguridad móvil de GlobalProtect escucha para recibir solicitudes HIP de las Gateways de GlobalProtect. Si está usando un sistema MDM de terceros, puede configurar el gateway para que use un puerto distinto, tal y como requiera el proveedor de MDM.
6081 6082	TLS 1.2 TCP	Puertos utilizados para el portal de autenticación de User-ID™: 6081 para el portal de autenticación sin un perfil de servidor SSL/TLS y 6082 para el portal de autenticación con un perfil de servidor SSL/TLS.
10443	SSL	Puerto que usa el cortafuegos y Panorama para proporcionar información contextual sobre una amenaza o realizar un cambio de su investigación sobre amenazas hacia Threat Vault y AutoFocus sin inconvenientes.

Puertos usados para HA

Los cortafuegos configurados como peers de alta disponibilidad (High Availability, HA) deben poder comunicarse entre sí para mantener la información de estado (enlace de control HA1) y sincronizar los datos (enlace de datos HA2). En las implementaciones de HA activa/activa, las implementaciones de los cortafuegos peer también deben reenviar paquetes a los peer HA que posee la sesión. El enlace HA3 es un enlace de capa 2 (MAC en MAC) y no admite cifrado ni direcciones de capa 3.

Puerto de destino	Protocolo	Description (Descripción)
28769 28260	TCP TCP	Se usa para el enlace de control HA1 para una comunicación de texto clara entre los cortafuegos de peer de HA. El enlace de HA1 es un enlace de capa 3 y requiere una dirección IP.
28	TCP	Se usa para el enlace de control HA1 para una comunicación cifrada (SSH en TCP) entre los cortafuegos de peer de HA.
28770	TCP	Puerto de escucha para enlaces de copia de seguridad HA1.
28771	TCP	Usado para copias de seguridad de heartbeat. Palo Alto Networks recomienda habilitar la copia de seguridad de heartbeat en la interfaz

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
		de MGT si usa un puerto en banda para HA1 o los enlaces de copia de seguridad HA1.
99 29281	IP UDP	Se usa para el enlace HA2 para sincronizar sesiones, reenviar tablas, las asociaciones de la seguridad IPSec y las tablas de ARP entre los cortafuegos en un par de HA. El flujo de datos en el enlace HA2 siempre es unidireccional (excepto para el mantenimiento de HA2); fluye desde el cortafuegos activo (activo/pasivo), o el activo-principal (activo/activo) hacia el cortafuegos pasivo (activo/pasivo) o activo secundario (activo/activo). El enlace de HA2 es un enlace de capa 2 y utiliza el tipo ether 0x7261 de manera predeterminada. El enlace de datos HA también puede configurarse para usar el IP (número de protocolo 99) o UDP (puerto 29281) como el transporte, y por lo tanto permite que el enlace de datos de HA abarque las subredes.

Puertos usados para Panorama

Panorama utiliza los siguientes puertos.

Puerto de destino	Protocolo	Description (Descripción)
22	TCP	Se usa para comunicarse desde un sistema cliente con la interfaz CLI de Panorama.
443	TCP	Se usa para comunicarse desde un sistema cliente con la interfaz web de Panorama.
444	TCP	Se utiliza para la comunicación entre Panorama y Cortex Data Lake.
3978	TCP	Se usa para la comunicación entre Panorama y los cortafuegos gestionados o recopiladores de logs, así como para la comunicación entre los recopiladores gestionados en un grupo de recopiladores: • Para la comunicación entre Panorama y los cortafuegos, se trata de una conexión bidireccional en la que los cortafuegos reenvían logs a Panorama y Panorama envía los cambios de configuración a los cortafuegos. Los comandos de cambio de contexto se envían a través de la misma conexión. • Los recopiladores de logs usan este puerto de destino para reenviar los logs a Panorama. • Para una comunicación con el recopilador de logs predeterminado en un dispositivo serie M en modo Panorama y para la comunicación con los recopiladores de logs dedicados.
28443	TCP	Se usa para los dispositivos gestionados (cortafuegos y recopilador de logs) para recuperar actualizaciones de software y de contenido de Panorama.

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
		Solo los dispositivos que ejecutan versiones de PAN-OS 8.x y superiores recuperan actualizaciones de Panorama mediante este puerto. En el caso de los dispositivos que ejecutan versiones anteriores, Panorama envía los paquetes de actualización mediante el puerto 3978.
28769 (5.1 o posterior) 28260 (5.0 o posterior) 49160 (5.0 o posterior)	TCP TCP TCP	Se usa para una conectividad HA y la sincronización entre los peers HA de Panorama usando una comunicación de texto clara. Cualquiera de los peers puede iniciar la comunicación.
28	TCP	Se usa para una conectividad HA y la sincronización entre los peers HA de Panorama usando una comunicación cifrada (SSH en TCP). Cualquiera de los peers puede iniciar la comunicación. Se usa para la comunicación entre recopiladores de logs en un grupo de recopiladores para la distribución de logs.
28270 (6.0 o posterior) 49190 (5.1 o posterior)	TCP	Se usa para la comunicación entre recopiladores de logs en un grupo de recopiladores para la distribución de logs.
2049	TCP	La usa el dispositivo virtual Panorama para escribir logs en el almacén de datos NFS.
10443	SSL	Puerto que usa Panorama para proporcionar información contextual sobre una amenaza o realizar un cambio de su investigación sobre amenazas hacia Threat Vault y AutoFocus sin inconvenientes.
23000 a 23999	TCP, UDP o SSL	Se usa para la comunicación de syslog entre Panorama y los componentes de ESM de las capturas.

Puertos usados para GlobalProtect

GlobalProtect utiliza los siguientes puertos.

Puerto de destino	Protocolo	Description (Descripción)
443	TCP	Se utiliza para las comunicaciones entre las aplicaciones y los portales de GlobalProtect, o para las aplicaciones y las puertas de enlace de GlobalProtect, y para las conexiones de túnel SSL. Las puertas de enlace de GlobalProtect también utilizan este puerto para recopilar información del host de las aplicaciones de GlobalProtect

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
		y realizar comprobaciones del perfil de información del host (host information profile, HIP).
4501	UDP	Se usa para las conexiones de túnel IPSec entre aplicaciones y puertas de enlace de GlobalProtect.

Para encontrar consejos sobre cómo usar una interfaz de bucle invertido para proporcionar acceso a GlobalProtect a través de diferentes puertos y direcciones, consulte ¿Se puede configurar la página del portal de GlobalProtect para acceder a ella desde cualquier puerto?

Puertos usados para User-ID

User-ID es una función que permite la asignación de direcciones IP de usuario a nombres de usuario y miembros de grupo, que permite políticas basadas en grupos o usuarios y visibilidad sobre las actividades de sus usuarios en su red (por ejemplo, para poder rastrear con rapidez a un usuario que puede ser víctima de una amenaza). Para realizar esta asignación, el cortafuegos, el agente de User-ID (instalado en un sistema basado en Windows o el agente integrado de PAN-OS que funciona en el cortafuegos) o el agente de servidor de terminal debe poder conectarse con los servicios de directorio de su red para realizar la Asignación de grupos y la Asignación de usuarios. Además, si los agentes funcionan en sistemas externos al cortafuegos, deben poder conectar con el cortafuegos para comunicar la dirección IP con las asignaciones de nombre de usuario al cortafuegos. La siguiente tabla muestra los requisitos de comunicación para User-ID junto con los números de puerto necesarios para establecer las conexiones.

Puerto de destino	Protocolo	Description (Descripción)
389	TCP	Puerto que utiliza el cortafuegos para conectarse con un servidor LDAP (texto normal o seguridad de la capa de transporte de inicio, Start TLS [TLS de inicio]) para la Asignación de usuarios a grupos.
3268	TCP	Puerto que utiliza el cortafuegos para conectarse con el servidor del catálogo global de Active Directory (texto normal o Start TLS [TLS de inicio]) para la Asignación de usuarios a grupos.
636	TCP	Puerto que utiliza el cortafuegos para las conexiones de LDAP sobre SSL con un servidor LDAP para la Asignación de usuarios a grupos.
3269	TCP	Puerto que utiliza el cortafuegos para las conexiones de LDAP sobre SSL con un servidor de catálogo global de Active Directory para la Asignación de usuarios a grupos.
514 6514	TCP UDP SSL	Puerto que escucha el agente User-ID para los mensajes de syslog de autenticación si realiza la Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios. El puerto depende del tipo de agente y protocolo. • Agente User-ID integrado en PAN-OS: puerto 6514 para SSL y puerto 514 para UDP. • Agente User-ID basado en Windows: puerto 514 para TCP y UDP.

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
5007	TCP	Puerto que escucha el cortafuegos para obtener información de asignación de usuarios desde User-ID o el agente de servidor de terminal. El agente envía la asignación de dirección IP y nombre de usuario junto con una marca de tiempo cuando sabe de una asignación nueva o actualizada. Además, conecta con el cortafuegos a intervalos regulares para actualizar las actualizaciones conocidas.
5006	TCP	Puerto que escucha el agente User-ID para las solicitudes de API de XML. El origen de esta comunicación suele ser el sistema que ejecuta una secuencia de comandos que invoque la API.
88	UDP/TCP	Puerto que usa el agente User-ID para autenticarse en un servidor Kerberos. El dispositivo prueba UDP en primer lugar y luego vuelve a TCP.
1812	UDP	Puerto que usa el agente User-ID para autenticarse en un servidor RADIUS.
49	TCP	Puerto que usa el agente User-ID para autenticarse en un servidor TACACS+.
135	TCP	Puerto que usa el agente User-ID para establecer conexiones WMI basadas en TCP con el asignador de extremos de llamada a procedimiento remoto (RPC) de Microsoft. El asignador de extremos asigna al agente un puerto asignado aleatoriamente en el intervalo de puertos 49152-65535. El agente usa esta conexión para crear consultas RPC para las tablas de sesión y los logs de seguridad del servidor AD o servidor Exchange. Este es también el puerto que se usa para acceder a servicios de terminal. El agente User-ID también usa este puerto para conectar con sistemas cliente y realizar sondeos de Windows Management Instrumentation (WMI).
139	TCP	Puerto que usa el agente User-ID para establecer conexiones NetBIOS basadas en TCP con el servidor AD, de modo que pueda enviar consultas RPC sobre logs de seguridad e información de sesión. El agente User-ID también usa este puerto para conectar con sistemas cliente para sondeos de NetBIOS (admitidos únicamente en el agente User-ID basado en Windows).
445	TCP	Puerto que usa el agente User-ID para conectar con Active Directory (AD) mediante conexiones SMB basadas en TCP al servidor AD para acceder a la información de inicio de sesión de usuario (administrador de trabajos de impresión y Net Logon).
5985	HTTP	Puerto que usa el agente de User-ID para supervisar los logs de seguridad y la información de las sesiones con el protocolo WinRM por HTTP.

© 2020 Palo Alto Networks, Inc.

Puerto de destino	Protocolo	Description (Descripción)
5986	HTTPS	Puerto que usa el agente de User-ID para supervisar los logs de seguridad y la información de las sesiones con el protocolo WinRM por HTTPS.

© 2020 Palo Alto Networks, Inc.

Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica

El restablecimiento del cortafuegos a los ajustes predeterminados de fábrica producirá la pérdida de todos los ajustes y logs de configuración.

STEP 1 | Configure una conexión de consola con el cortafuegos.

1. Conecte un cable en serie desde su ordenador hasta el puerto de la consola y conéctese al cortafuegos usando el software de emulación de terminal (9600-8-N-1).

   Si su ordenador no tiene un puerto de serie de 9 clavijas, use un conector de puerto USB a serie.

2. Introduzca sus credenciales de inicio de sesión.
3. Introduzca el siguiente comando del CLI:

   `debug system maintenance-mode`

   El cortafuegos se reinicia en el modo de mantenimiento.

STEP 2 | Restablezca el sistema a los ajustes predeterminados de fábrica.

1. Cuando el dispositivo se reinicie, pulse **`Intro`** para continuar hacia el menú de modo de mantenimiento.
2. Seleccione **`Restablecimiento de la configuración predeterminada de fábrica`** y pulse **`Intro`**.
3. De nuevo, seleccione **`Restablecimiento de la configuración predeterminada de fábrica`** y pulse **`Intro`**.

   El cortafuegos se reinicia sin ningún ajuste de configuración. El nombre de usuario y contraseña predeterminados para iniciar sesión en el cortafuegos es admin/admin.

   Para realizar una configuración inicial del cortafuegos y configurar la conectividad de red, consulte Integración del cortafuegos en la red de gestión.

© 2020 Palo Alto Networks, Inc.

Arranque del cortafuegos

El arranque acelera el proceso de configuración y obtención de licencia del cortafuegos para ponerlo en funcionamiento en la red con o sin acceso a Internet. El arranque le permite elegir entre configurar el cortafuegos con un archivo de configuración básica (init-cfg.txt) para poder conectarlo a Panorama y obtener la configuración completa, o configurar completamente el cortafuegos con la configuración básica y el archivo opcional bootstrap.xml.

- Soporte de la unidad Flash USB
- Archivos init-cfg.txt de muestra
- Preparación de una unidad Fash USB para el arranque de un cortafuegos
- Arranque de un cortafuegos usando una unidad Flash USB

Soporte de la unidad Flash USB

La unidad flash USB que arranca el cortafuegos de Palo Alto Networks basado en hardware debe admitir uno de los siguientes formatos:

- Tabla de asignación de archivos 32 (FAT32)
- Tercer sistema de archivos extendido (ext3)

El cortafuegos puede arrancar desde las siguientes unidades flash con conectividad USB 2.0 o USB 3.0.

Unidades flash USB compatibles
Kingston • Kingston SE9 8 GB (2.0) • Kingston SE9 16 GB (3.0) • Kingston SE9 32 GB (3.0)
SanDisk • SanDisk Cruzer Fit CZ33 8 GB (2.0) • SanDisk Cruzer Fit CZ33 16 GB (2.0) • SanDisk Cruzer Fit CZ33 16 GB (2.0) • SanDisk Cruzer CZ33 32 GB (2.0) • SanDisk Cruzer Fit CZ33 32 GB (3.0)
Silicon Power • Silicon Power Jewel 32 GB (3.0) • Silicon Power Jewel 16 GB (3.0)
PNY • PNY Attache 16 GB (2.0) • PNY Attache 32 GB (3.0)

Archivos init-cfg.txt de muestra

El archivo init-cfg.txt es necesario para el proceso de arranque; este archivo es un archivo de configuración básica que usted crea usando un editor de texto. Para crear este archivo, consulte Creación del archivo init-

© 2020 Palo Alto Networks, Inc.

cfg.txt. Los siguientes archivos init-cfg.txt de ejemplo muestran los parámetros que admite el archivo; los parámetros que debe proporcionar se muestran en negrita.

Archivo init-cfg.txt de muestra (dirección IP estática)	Archivo init-cfg.txt de muestra (cliente DHCP)
type=static **ip-address=10.5.107.19** **default-gateway=10.5.107.1** **netmask=255.255.255.0** **ipv6-address=2001:400:f00::1/64** **ipv6-default-gateway=2001:400:f00::2** hostname=Ca-FW-DC1 panorama-server=10.5.107.20 panorama-server-2=10.5.107.21 tplname=FINANCE_TG4 dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame dhcp-send-hostname=no dhcp-send-client-id=no dhcp-accept-server-hostname=no dhcp-accept-server-domain=no	**type=dhcp-client** ip-address= default-gateway= netmask= ipv6-address= ipv6-default-gateway= hostname=Ca-FW-DC1 panorama-server=10.5.107.20 panorama-server-2=10.5.107.21 tplname=FINANCE_TG4 dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame dhcp-send-hostname=yes dhcp-send-client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-domain=yes

La tabla siguiente describe los campos del archivo init-cfg.txt: El tipo es obligatorio; si el tipo es estático, la dirección IP, la puerta de enlace por defecto y la máscara de red son obligatorias, o la dirección IPv6 y la puerta de enlace por defecto IPv6 son obligatorias.

Campo	Description (Descripción)
tipo	(Obligatorio) Tipo de dirección IP de gestión estática o dhcp-client.
dirección-ip	(Obligatorio para dirección de gestión estática IPv4) Dirección IPv4. El cortafuegos ignora este campo si el tipo es dhcp-client.
default-gateway	(Obligatorio para la dirección de gestión estática IPv4) Puerta de enlace IPv4 por defecto para la interfaz de gestión. El cortafuegos ignora este campo si el tipo es dhcp-client.
Máscara de red	(Obligatorio para dirección de gestión estática IPv4) Máscara de red IPv4. El cortafuegos ignora este campo si el tipo es dhcp-client.
ipv6-address	(Obligatorio para la dirección de gestión estática IPv6) Dirección IPv4 y extensión del /prefijo de la interfaz de gestión. El cortafuegos ignora este campo si el tipo es dhcp-client.
ipv6-default-gateway	(Obligatorio para la dirección de gestión estática IPv6) Puerta de enlace IPv6 por defecto para la interfaz de gestión. El cortafuegos ignora este campo si el tipo es dhcp-client.
hostname	(Opcional) Nombre de host para el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
panorama-server	(Recomendado) Dirección IPv4 o IPv6 del servidor Panorama principal.
panorama-server-2	(Opcional) Dirección IPv4 o IPv6 del servidor Panorama secundario.
Tplname	(Recomendado) Nombre de la plantilla de Panorama.
Dgname	(Recomendado) Nombre del grupo de dispositivos Panorama.
dns-primary	(Opcional) Dirección IPv4 o IPv6 del servidor DNS primario.
dns-secondary	(Opcional) Dirección IPv4 o IPv6 del servidor DNS secundario.
vm-auth-key	(Cortafuegos serie VM únicamente) Clave de autenticación de equipo virtual.
op-command-modes	(Opcional) Introduzca varios sistemas virtuales, trama gigante o ambos separados por coma únicamente. Habilita sistemas virtuales múltiples y tramas gigantes durante el arranque.
dhcp-send-hostname	(Tipo de cliente DHCP únicamente) El servidor DHCP determina un valor de sí o no. En caso afirmativo, el cortafuegos envía su nombre de host al servidor DHCP.
dhcp-send-client-id	(Tipo de cliente DHCP únicamente) El servidor DHCP determina un valor afirmativo o negativo. En caso afirmativo, el cortafuegos envía su ID de cliente al servidor DHCP.
dhcp-accept-server-hostname	(Tipo de cliente DHCP únicamente) El servidor DHCP determina un valor afirmativo o negativo. En caso afirmativo, el cortafuegos acepta el nombre de host del servidor DHCP.
dhcp-accept-server-domain	(Tipo de cliente DHCP únicamente) El servidor DHCP determina un valor afirmativo o negativo. En caso afirmativo, el cortafuegos acepta el servidor DNS del servidor DHCP.

Preparación de una unidad Fash USB para el arranque de un cortafuegos

Puede usar una unidad flash USB para arrancar un cortafuegos físico. No obstante, para hacerlo, debe ejecutar PAN-OS 7.1.0 o una imagen posterior y restablecer el cortafuegos a los ajustes predeterminados de fábrica. Por motivos de seguridad, arranque un cortafuegos únicamente cuando este tenga la configuración de fábrica o cuando todos los datos privados se hayan eliminado.

STEP 1 | Obtenga los números de serie (serial numbers, S/N) y los códigos de autorización para admitir suscripciones de su correo electrónico de cumplimiento de pedido.

STEP 2 | Registre los S/N de los cortafuegos nuevos en el portal del servicio de atención al cliente.

1. Vaya a support.paloaltonetworks.com, inicie sesión y seleccione **Assets (Activos)** > **Devices (Dispositivos)** > **Register New Device (Registrar nuevo dispositivo)** > **Register device using**

© 2020 Palo Alto Networks, Inc.

Serial Number or Authorization Code (Registrar dispositivo con el número de serie o código de autorización).

2. Siga los pasos para registrar el cortafuegos.
3. Haga clic en **Submit (Enviar)** para enviar.

STEP 3 | Active los códigos de autorización en el portal del servicio de atención al cliente, que crea las claves de licencia.

1. Visite support.paloaltonetworks.com, inicie sesión y seleccione **Assets (Activos)** > **Devices (Dispositivos)** en el panel de navegación izquierdo.
2. Para cada número de serie (serial number, S/N) de dispositivo que acabe de registrar, haga clic en el enlace **Action (Acción)** (el icono de lapíz).
3. En Activate Licenses (Activar licencias), seleccione **Activate Auth-Code (Activar código de autenticación)**.
4. Introduzca el **Authorization code (Código de autorización)** y haga clic en **Agree (Acepto)** y **Submit (Enviar)**.

STEP 4 | Añada los S/N en Panorama.

Complete el paso 1 en Añadir un cortafuegos como dispositivo gestionado en la Guía del administrador en Panorama.

STEP 5 | Cree el archivo init-cfg.txt.

Cree el archivo init-cfg.txt, un archivo obligatorio que proporciona parámetros de arranque. Los campos se describen en archivos de muestra init-cfg.txt.



Si falta el archivo init-cfg.txt, el proceso de arranque no se realizará y el cortafuegos se iniciará con la configuración por defecto en la secuencia de inicio normal.

No hay espacios entre la clave y el valor en cada campo; no añada espacios ya que pueden causar errores durante el análisis en el lado del servidor de gestión.

Puede tener varios archivos init-cfg.txt (uno para cada sitio remoto diferente) si antepone el S/N.al nombre de archivo. Por ejemplo:

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

Si nada precede al nombre de archivo, el cortafuegos utiliza el archivo init-cfg.txt y continúa con el arranque.

STEP 6 | (Opcional) Cree el archivo bootstrap.xml.

El archivo bootstrap.xml opcional es una configuración de cortafuegos completa que puede exportar de un cortafuegos de producción existente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones) y** > **Export named configuration snapshot (Exportar instantáneas de configuración con nombre)**.
2. Seleccione en **Name** el nombre de la configuración guardada o en ejecución.
3. Haga clic en **OK (Aceptar)**.
4. Cambie el nombre del archivo a **`bootstrap.xml`**.

STEP 7 | Cree y descargue el lote de arranque en el portal del servicio de atención al cliente.

Para un cortafuegos físico, el lote de arranque requiere solo los directorios de /licencia y /config.

Use uno de los siguientes métodos para crear y descargar el lote de arranque:

© 2020 Palo Alto Networks, Inc.

- Use el **Método 1** para crear un paquete de arranque específico de un sitio remoto (tiene solo un archivo init-cfg.txt).
- Use el **Método 2** para crear un paquete de arranque para varios sitios.

Método 1

1. En su sistema local, ingrese en support.paloaltonetworks.com e inicie sesión.
2. Seleccione **Assets**.
3. Seleccione el S/N del cortafuegos que desea arrancar.
4. Seleccione **Bootstrap Container**.
5. Haga clic en **Select**.
6. Cargue y **Open (Abra)** el archivo init-cfg.txt que acaba de crear.
7. (Opcional) Seleccione el archivo bootstrap.xml que creó y haga clic en **Upload Files (Cargar archivos)**.

   Debe usar un archivo bootstrap.xml de un cortafuegos del mismo modelo y versión de PAN-OS.
8. Seleccione **Bootstrap Container Download** para descargar un archivo tar.gz con el nombre **`bootstrap_<S/N>_<date>.tar.gz`** en su sistema local. Este contenedor de arranque incluye las claves de licencia asociadas con el S/N del cortafuegos.

Método 2

Cree un archivo tar.gz en su sistema local con dos directorios de nivel superior: /license y /config. Incluya todas las licencias y todos los archivos init-cfg.txt con S/N antepuestos a los nombres de archivo.

Los archivos de clave de licencia que descarga del portal del servicio de atención al cliente tienen el S/N en el nombre de archivo de la licencia. PAN-OS comprueba el S/N en el nombre de archivo al compararlo con el S/N del cortafuegos mientras ejecuta el proceso de arranque.

STEP 8 | Importe el archivo tar.gz que ha creado (a un cortafuegos que ejecute PAN-OS 7.1.0 o una imagen posterior) usando Secure Copy (SCP) o TFTP.

Acceda a la CLI e introduzca los siguientes comandos:

- **`tftp import bootstrap-bundle file <path and filename> from <host IP address>`**

  Por ejemplo:

  `tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3`
- **`scp import bootstrap-bundle from <<usuario>@<host>:<ruta al archivo>>`**

  Por ejemplo:

  `scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz`

STEP 9 | Prepare la unidad flash USB.

1. Introduzca la unidad flash USB en el cortafuegos que haya usado en el paso anterior.
2. Introduzca el siguiente comando operativo de CLI usando su nombre de archivo ta.gz en lugar de "**`pa5000.tar.gz`**". Este comando formatea la unidad flash USB, descomprime el archivo y valida la unidad flash USB

   `request system bootstrap-usb prepare from pa5000.tar.gz`
3. Pulse **`y`** para continuar. El siguiente mensaje aparece cuando la unidad USB está lista:

   `USB prepare completed successfully.`
4. Quite la unidad flash USB del cortafuegos.

© 2020 Palo Alto Networks, Inc.

5. Puede preparar todas las unidades flash USB que necesite.

STEP 10 | Entregue la unidad flash USB a su sitio remoto.

Si utilizó el Método 2 para crear el lote de arranque, puede usar el mismo contenido de la unidad flash USB para arrancar los cortafuegos en varios sitios remotos. Puede traducir el contenido a varias unidades flash USB o a una sola unidad flash USB utilizada varias veces.

Arranque de un cortafuegos usando una unidad Flash USB

Una vez que reciba un cortafuegos de Palo Alto Networks y una unidad flash USB que contenga los archivos de arranque, puede arrancar el cortafuegos.



Los sistemas operativos de Microsoft Windows y Apple Mac no pueden leer la unidad flash USB de arranque debido a que la unidad está formateada por un sistema de archivo ext4. Debe instalar un software de terceros o usar un sistema Linux para leer la unidad USB.

STEP 1 | El cortafuegos debe estar en estado de fábrica por defecto o debe tener todos los datos privados eliminados.

STEP 2 | Para garantizar la conectividad con su sede corporativa central, conecte el cortafuegos mediante la interfaz de gestión (MGT) usando un cable Ethernet conectado a una de las siguientes opciones:

- Un módem de subida.
- Un puerto en el conmutador o enrutador.
- Una toma Ethernet en la pared.

STEP 3 | Introduzca la unidad flash USB en el puerto USB del cortafuegos y encienda el cortafuegos. El cortafuegos en estado de fábrica por defecto arranca desde la unidad flash USB.

La luz de estado del cortafuegos cambia de amarillo a verde cuando el cortafuegos está configurado; la autoconfirmación se ha realizado correctamente.

STEP 4 | Verifique que el arranque se haya completado. Puede ver logs de estado básicos en la consola durante el arranque y puede verificar que el proceso se haya completado.

1. Si incluyó valores de Panorama (panorama-server, tplname y dgname) en su archivo init-cfg.txt, compruebe los dispositivos gestionados de Panorama, el grupo de dispositivos y el nombre de la plantilla.
2. Verifique la configuración general del sistema accediendo a la interfaz web y seleccionando **Dashboard (Panel)** > **Widgets** > **System (Sistema)** o utilizando los comandos operativos de la CLI **`show system info`** y **`show config running`**.
3. Verifique la instalación de la licencia seleccionando **Device (Dispositivo)** > **Licenses (Licencias)** o utilizando el comando operativo de la CLI **`request license info`**.
4. Si tiene Panorama configurado, gestione las versiones de contenido y las versiones del software desde Panorama. Si no tiene Panorama configurado, utilice la interfaz web para gestionar versiones de contenido y versiones de software.

© 2020 Palo Alto Networks, Inc.

Telemetría de dispositivos

La telemetría de dispositivos recopila datos sobre su cortafuegos o Panorama de nueva generación y los comparte con Palo Alto Networks mediante la carga de los datos en Cortex Data Lake. Estos datos se utilizan para impulsar aplicaciones de telemetría y para compartir inteligencia sobre amenazas.

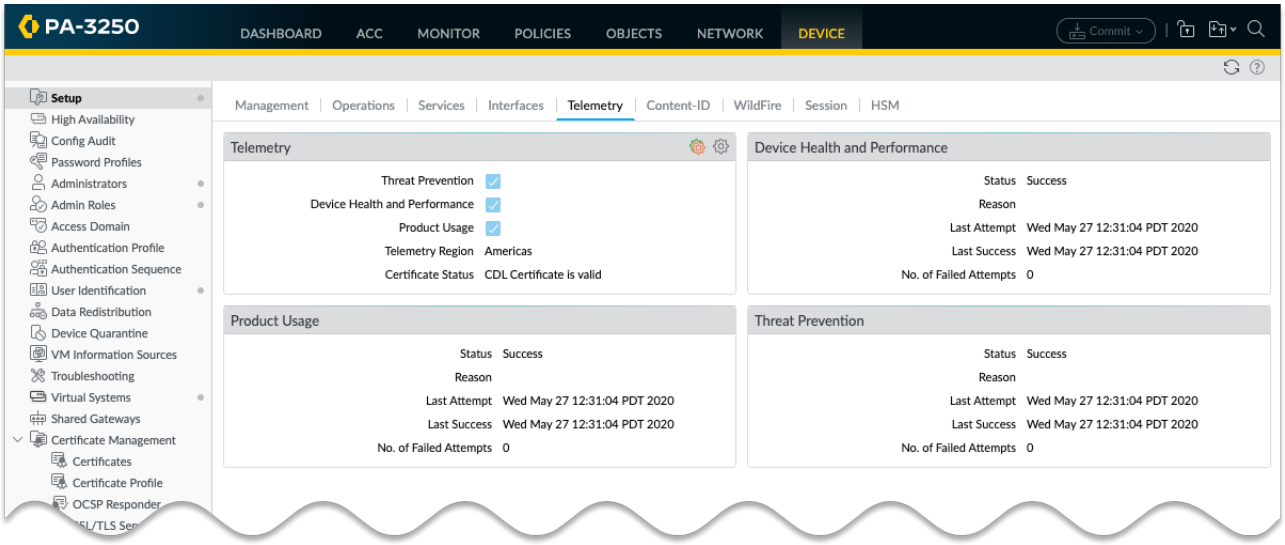
- Descripción general de telemetría de dispositivos
- Recopilación de telemetría de dispositivos e intervalos de transmisión
- Gestión de telemetría de dispositivos
- Supervisión de telemetría de dispositivos
- Muestra de los datos que recopila la telemetría de dispositivos

© 2020 Palo Alto Networks, Inc.

Descripción general de telemetría de dispositivos

La telemetría de dispositivos recopila datos sobre su cortafuegos o Panorama de nueva generación y los comparte con Palo Alto Networks mediante la carga de los datos en Cortex Data Lake. Estos datos se utilizan para alimentar aplicaciones de telemetría, que son aplicaciones basadas en la nube que facilitan la supervisión y la gestión de sus cortafuegos y soluciones Panorama de nueva generación. Las aplicaciones mejoran la visibilidad del estado, el rendimiento, la planificación de la capacidad y la configuración del dispositivo. A través de esas aplicaciones, podrá maximizar los beneficios de los que disfruta en cuanto a los productos y servicios que ofrece Palo Alto Networks.

Los datos de telemetría también se utilizan para compartir inteligencia sobre amenazas y proporcionar una prevención de intrusiones mejorada, una evaluación de firmas de amenazas y una detección mejorada de malware dentro del filtrado de URL PAN-DB, firmas de comando y control (C2) basadas en DNS y WildFire.



Los datos de telemetría se recopilan y almacenan localmente en su dispositivo durante un período limitado. Estos datos se comparten con Palo Alto Networks solo si configura una región de destino para los datos. Si su organización tiene una licencia de Cortex Data Lake, solo puede enviar los datos a la misma región donde se encuentre su instancia de Cortex Data Lake. Si su organización no tiene una licencia de Cortex Data Lake, debe instalar un certificado de dispositivo para compartir esos datos. En este caso, puede elegir cualquier región disponible, aunque debe cumplir con todas las leyes locales aplicables con respecto a la privacidad y el almacenamiento de datos.

Los datos de telemetría se recopilan y comparten con Palo Alto Networks en intervalos de recopilación predefinidos. Puede habilitar/deshabilitar categorías de datos para controlar si los datos se recopilan y comparten. También puede supervisar el estado actual de la recopilación y transmisión de datos.

Finalmente, puede obtener una muestra en vivo de los datos que su cortafuegos está recopilando para fines de telemetría. Para obtener una descripción completa de todas las métricas de telemetría que se pueden compartir con Palo Alto Networks, incluida la implicación de privacidad para cada métrica, consulte la Guía de referencia de métricas de telemetría de dispositivos PAN-OS.

© 2020 Palo Alto Networks, Inc.

Recopilación de telemetría de dispositivos e intervalos de transmisión

PAN-OS recopila y envía datos de telemetría en intervalos fijos. La recopilación se define métrica por métrica y puede ser una de las siguientes:

- Cada 20 minutos.
- Cada 4 horas.
- Una vez por semana.

La telemetría se recopila en paquetes de datos. Cada paquete es una agregación de todos los datos recopilados hasta el punto de transmisión de datos. Estos paquetes se almacenan en el dispositivo hasta un evento de transmisión, que se produce una vez cada 4 horas. Una vez que se envía el paquete correctamente a Palo Alto Networks, se elimina del dispositivo.

Si se produce un error al enviar un paquete a Palo Alto Networks, el cortafuegos espera 10 minutos y, a continuación, vuelve a intentarlo. El cortafuegos seguirá intentando enviar el paquete hasta que sea correcto o necesite espacio de almacenamiento para recopilar nuevos datos de telemetría.

En cada intervalo de transmisión regular, el cortafuegos comenzará con el envío de los paquetes programados para ese evento. Después de una transferencia correcta de esos paquetes, el cortafuegos enviará cualquier paquete fallido que pueda haber almacenado de eventos de transmisión anteriores.

© 2020 Palo Alto Networks, Inc.

Gestión de telemetría de dispositivos

Para gestionar la telemetría de dispositivos, puede realizar los siguientes procedimientos:

- Habilitación de telemetría de dispositivos
- Deshabilitación de telemetría de dispositivos
- Gestión de datos que recopila la telemetría de dispositivos
- Gestión de telemetría de dispositivos histórica

Habilitación de telemetría de dispositivos

De forma predeterminada, su dispositivo no comparte datos con Palo Alto Networks. Si el uso compartido está habilitado, puede dejar de compartir toda la telemetría del dispositivo. Para ello, diríjase a **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**, desactive la casilla **Enable Telemetry (Habilitar telemetría)** y, a continuación, confirme el cambio.

Para habilitar la telemetría de dispositivos para que los datos se compartan con Palo Alto Networks, realice el siguiente procedimiento:

STEP 1 | Habilite Cortex Data Lake.

1. Si su organización no tiene una licencia de Cortex Data Lake, instale un certificado de dispositivo si aún no hay uno instalado en su dispositivo.

   Si su organización tiene una licencia de Cortex Data Lake, asegúrese de que esté activada.
2. Asegúrese de que su red esté configurada correctamente para que el cortafuegos pueda enviar datos a Cortex Data Lake.

STEP 2 | Desplácese a **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**.

STEP 3 | Edite el widget de **telemetría**.

STEP 4 | En **Telemetry Destination (Destino de telemetría)**, seleccione su región. Si su organización está usando Cortex Data Lake, debe utilizar la región configurada en Cortex Data Lake.

STEP 5 | Haga clic en **OK (Aceptar)** y, a continuación, confirme los cambios.

Deshabilitación de telemetría de dispositivos

Si su cortafuegos de nueva generación está configurado para compartir datos con Palo Alto Networks, puede deshabilitar el uso compartido de la siguiente manera:

STEP 1 | Desplácese a **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**.

STEP 2 | Edite el widget de **telemetría**.

STEP 3 | Desactive la casilla **Enable Telemetry (Habilitar telemetría)**.

STEP 4 | Haga clic en **OK (Aceptar)** y, a continuación, confirme los cambios.

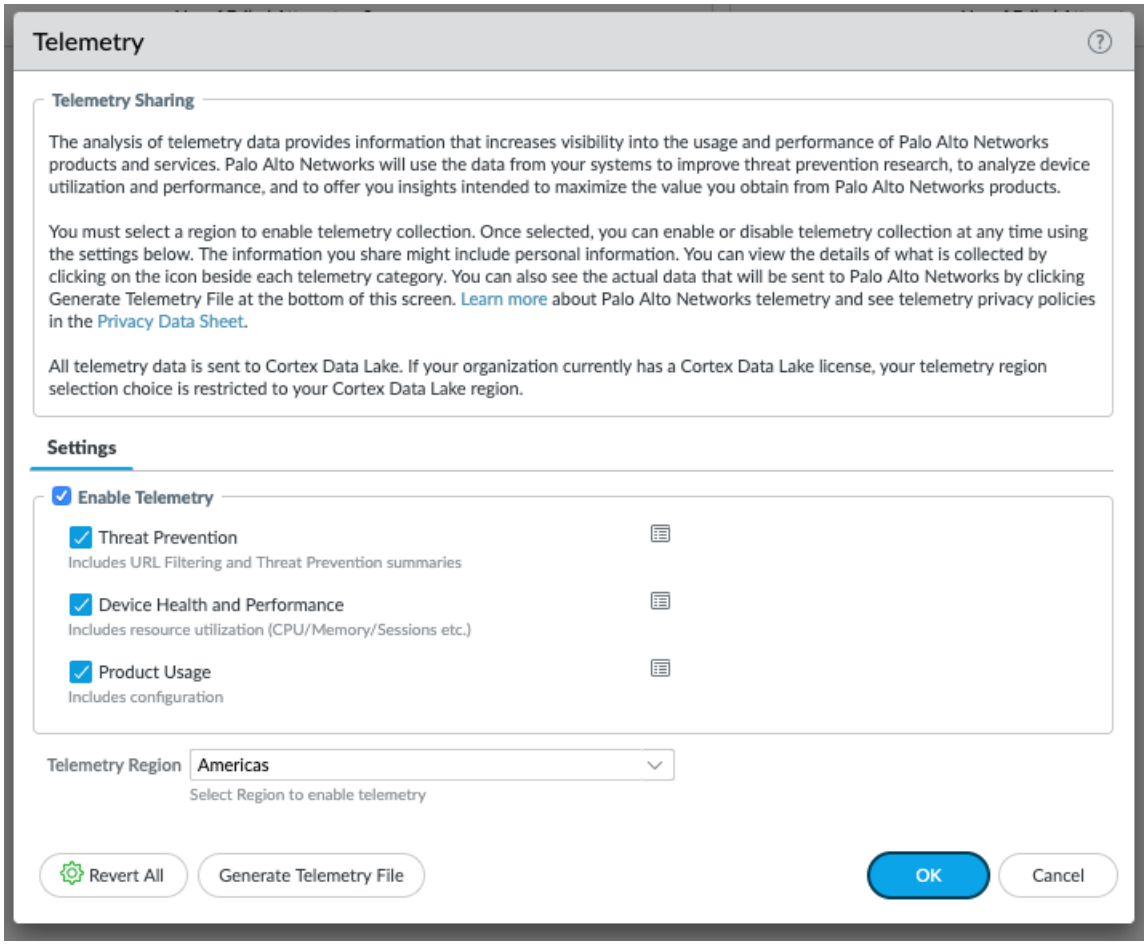
STEP 5 | Todos los datos de telemetría almacenados actualmente en Cortex Data Lake se borran automáticamente un año después de que su cortafuegos los cargue. Opcionalmente, si no desea que los datos se almacenen en Cortex Data Lake durante este período después de

© 2020 Palo Alto Networks, Inc.

deshabilitar la telemetría, abra un vale de soporte y solicite a Palo Alto Networks que borre sus datos de telemetría.

Gestión de datos que recopila la telemetría de dispositivos

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)** para ver las categorías de telemetría recopiladas actualmente. Para cambiar estas categorías, edite el widget de telemetría. Anule la selección de las categorías que no desee que el cortafuegos recopile, seleccione **OK (Aceptar)** y luego confirme el cambio.



Para dejar de compartir la telemetría de todos los dispositivos, desactive la casilla Enable Telemetry (Habilitar telemetría) y confirme el cambio.

Gestión de telemetría de dispositivos histórica

La telemetría de dispositivos cambió significativamente para la versión 10.0 de PAN-OS. Antes de la versión 10.0, los datos de telemetría eran de interés principalmente para fines de inteligencia de amenazas. A partir de 10.0, las métricas de inteligencia de amenazas siguen siendo una gran parte de los datos recopilados por el dispositivo, pero también se recopilan muchos más datos relacionados con el estado, el rendimiento y la configuración del dispositivo.

En otras palabras, la telemetría de dispositivos PAN-OS 10.0 amplía los datos que se recopilaron para versiones anteriores. PAN-OS 10.0 también envía datos de telemetría a una ubicación en la nube diferente a la de versiones anteriores. Sin embargo, el soporte histórico de telemetría todavía existe para los

© 2020 Palo Alto Networks, Inc.

cortafuegos de nueva generación que ejecutan PAN-OS 10.0. La única diferencia es que la interfaz de usuario de telemetría del dispositivo 10.0 no es capaz de gestionar esta recopilación de datos históricos.

Si tiene un cortafuegos de nueva generación existente y tiene habilitada alguna de las categorías históricas de datos de telemetría, cuando actualice a PAN-OS 10.0, su cortafuegos continuará recopilando y compartiendo esa información. Si desea desactivar este uso compartido de datos de telemetría, use los siguientes comandos de la CLI:

```
set deviceconfig system update-schedule statistics-service application-
reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-information no
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap no
set deviceconfig system update-schedule statistics-service passive-dns-
monitoring no
set deviceconfig system update-schedule statistics-service url-reports no
set deviceconfig system update-schedule statistics-service health-
performance-reports no
set deviceconfig system update-schedule statistics-service file-
identification-reports no
```

Si tiene un cortafuegos 10.0 y este uso compartido de telemetría está desactivado, pero desea compartir estos datos con Palo Alto Networks, puede activarlo mediante:

```
set deviceconfig system update-schedule statistics-service application-
reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-information yes
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap yes
set deviceconfig system update-schedule statistics-service passive-dns-
monitoring yes
set deviceconfig system update-schedule statistics-service url-reports yes
set deviceconfig system update-schedule statistics-service health-
performance-reports yes
set deviceconfig system update-schedule statistics-service file-
identification-reports yes
```

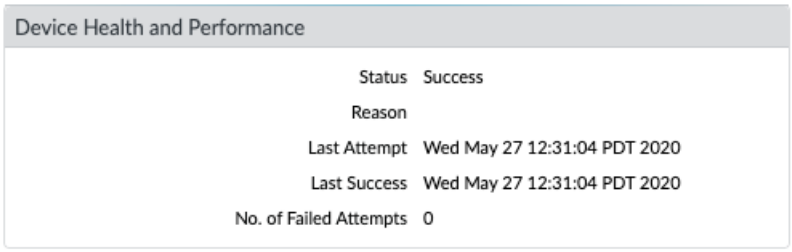
Puede ver si su dispositivo recopila y comparte esos datos históricos de telemetría mediante el siguiente comando de la CLI:

```
show deviceconfig system update-schedule statistics-service
```


© 2020 Palo Alto Networks, Inc.

Supervisión de telemetría de dispositivos

PAN-OS le muestra el estado de uso compartido de cada categoría de telemetría. Los widgets para cada categoría de métricas están disponibles en **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)**.



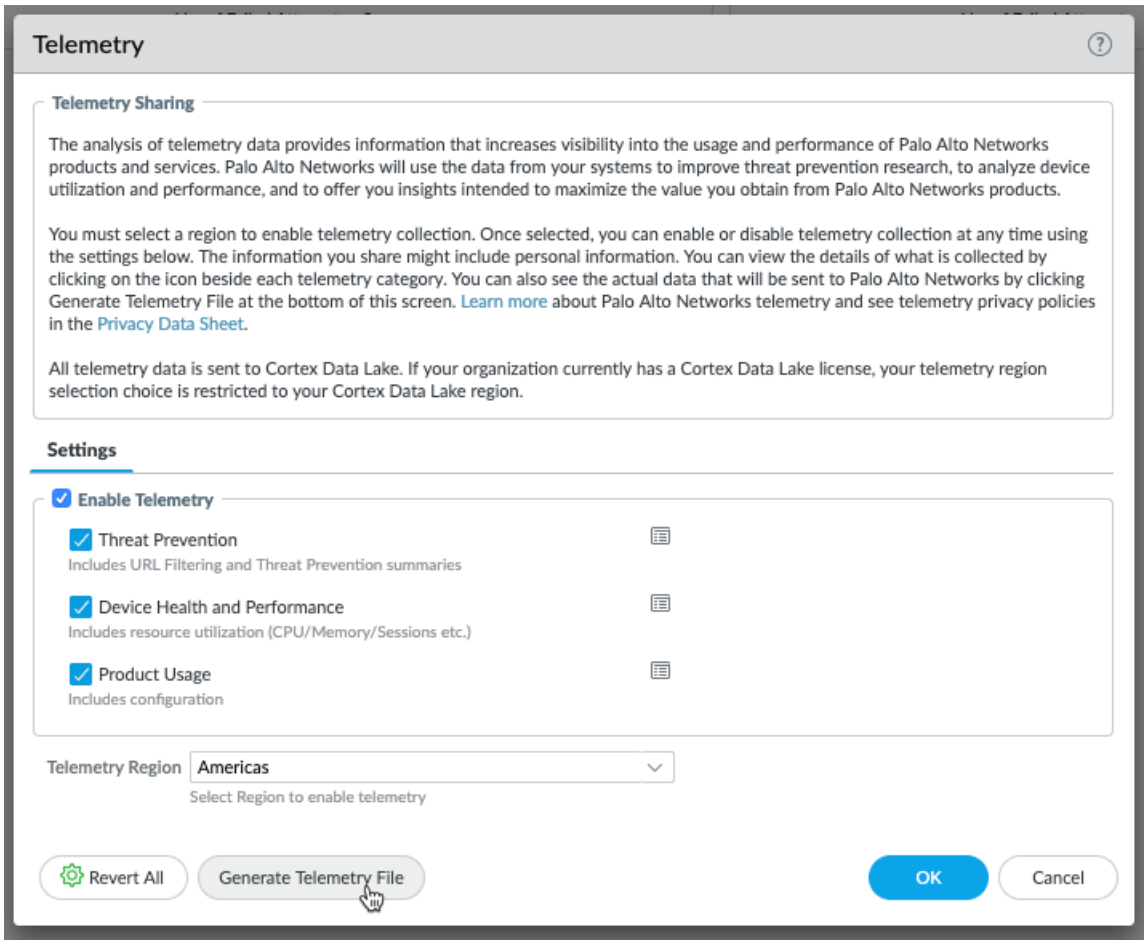
En el caso de un fallo, su dispositivo volverá a intentar el envío en la próxima hora de transmisión. Si el problema persiste, verifique que sus dispositivos estén configurados correctamente para enviar datos a Cortex Data Lake:

- Si su organización tiene una licencia de Cortex Data Lake, asegúrese de que su licencia de Cortex Data Lake esté activada y que su cortafuegos esté configurado para usar Cortex Data Lake.
- Si su organización no tiene una licencia de Cortex Data Lake, asegúrese de haber instalado un certificado de dispositivoy de que su red esté configurada para permitir el tráfico a Cortex Data Lake.

© 2020 Palo Alto Networks, Inc.

Muestra de los datos que recopila la telemetría de dispositivos

Puede descargar un ejemplo en vivo de los datos que la telemetría del dispositivo recopila y comparte con Palo Alto Networks. Para ello, diríjase a **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)** y edite el widget de **telemetría**. A continuación, haga clic en **Generate Telemetry File (Generar archivo de telemetría)**.



La recopilación de datos tardará unos minutos, según la velocidad de su cortafuegos. Cuando se complete el proceso, haga clic en **Download Device Telemetry Data (Descargar datos de telemetría del dispositivo)**. El paquete de telemetría es una tar ball comprimida y se coloca en el directorio de descarga de su navegador predeterminado.

Para obtener una descripción de cada métrica que la telemetría de dispositivos recopila y comparte con Palo Alto Networks, consulte la Guía de referencia de métricas de telemetría de dispositivos de PAN-OS.

© 2020 Palo Alto Networks, Inc.

Autenticación

La autenticación se utiliza para proteger los servicios y las aplicaciones mediante la verificación de las identidades de los usuarios, de modo que únicamente los usuarios legítimos puedan acceder a ellos. Varias funciones del cortafuegos y de Panorama requieren una autenticación. Los administradores se autentican para acceder a la interfaz de web, CLI o API de XML del cortafuegos y de Panorama. Los usuarios finales se autentican en el portal de autenticación o en GlobalProtect para acceder a varios servicios y aplicaciones. Puede seleccionar entre varios servicios de autenticación para proteger su red y para adaptar su infraestructura de seguridad existente, y garantizar una experiencia de usuario fluida.

Si tiene una infraestructura de clave pública, puede implementar certificados para permitir la autenticación sin que los usuarios deban responder manualmente a los desafíos del inicio de sesión (consulte Gestión de certificados). De manera alternativa, o además de los certificados, puede implementar una autenticación interactiva, que requiere que los usuarios se autentiquen utilizando uno o más métodos. Los siguientes temas describen cómo implementar, probar y solucionar los problemas de los diferentes tipos de autenticación interactiva:

- Tipos de autenticación
- Planificación de su implementación de autenticación
- Configuración de la autenticación multifactor
- Configuración de la autenticación SAML
- Configuración de un inicio de sesión único de Kerberos
- Configuración de la autenticación del servidor Kerberos
- Configuración de la autenticación TACACS+
- Configuración de la autenticación RADIUS
- Configuración de la autenticación LDAP
- Tiempos de espera de conexión de los servidores de autenticación
- Configuración de la autenticación de la base de datos local
- Configuración de una secuencia y perfil de autenticación
- Comprobación de la conectividad del servidor de autenticación
- Política de autenticación
- Solución de problemas de autenticación

© 2020 Palo Alto Networks, Inc.

Tipos de autenticación

- Servicios de autenticación externos
- Autenticación de múltiples factores
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP:
- Autenticación local

Servicios de autenticación externos

El cortafuegos y Panorama pueden utilizar servidores externos para controlar el acceso administrativo a la interfaz web y el acceso del usuario final a los servicios o las aplicaciones mediante el portal de autenticación y GlobalProtect. En este contexto, los servicios de autenticación que no son locales en el cortafuegos o Panorama se consideran externos, independientemente de si el servicio es interno (como Kerberos) o externo (como un proveedor de identidad SAML) en relación a su red. Los tipos de servidor que pueden integrar el cortafuegos y Panorama incluirán autenticación multifactor (MFA), SAML, Kerberos, TACACS+, RADIUS y LDAP. A pesar de que puede utilizar los servicios de autenticación local que admiten el cortafuegos y Panorama, por lo general, se recomiendan los servicios externos debido a que ofrecen lo siguiente:

- Gestión central de todas las cuentas de usuario en un almacenamiento de identidades externo. Todos los servicios externos compatibles proporcionan esta opción a los usuarios finales y administradores.
- Gestión central de la autorización de las cuentas (asignación de funciones y dominios de acceso). SAML, TACACS+ y RADIUS admiten esta opción para los administradores.
- Inicio de sesión único (SSO), que permite a los usuarios autenticarse solo una vez para acceder a varios servicios y aplicaciones. SAML y Kerberos admiten el SSO.
- Múltiples desafíos de autenticación de diferentes tipos (factores) para proteger los servicios y las aplicaciones más delicados. Los servicios de MFA admiten esta opción.

La autenticación mediante un servicio externo requiere un perfil de servidor que defina cómo el cortafuegos se conecta al servicio. Puede asignar el perfil del servidor a los perfiles de autenticación, lo que define la configuración que personaliza para cada aplicación y conjunto de usuarios. Por ejemplo, puede configurar un perfil de autenticación para los administradores que acceden a la interfaz web y otro perfil para los usuarios finales que acceden al portal de GlobalProtect. Para obtener información detallada, consulte Configuración de una secuencia y perfil de autenticación.

Autenticación de múltiples factores

Puede realizar la Configuración de la autenticación multifactor (MFA) para garantizar que cada usuario se autentique utilizando varios métodos to (factores) cuando accede a servicios y aplicaciones más delicados. Por ejemplo, puede obligar a los usuarios a introducir una contraseña de inicio de sesión e introducir un código de verificación que reciben por teléfono antes de permitir el acceso a documentos financieros importantes. Este enfoque ayuda a evitar que los atacantes accedan a cada servicio y aplicación en su red solo con robar las contraseñas. Evidentemente, no todos los servicios y aplicaciones requieren el mismo nivel de protección, y es posible que la MFA no sea necesaria para los servicios y aplicaciones menos delicados a los que los usuarios acceden con frecuencia. Para permitir una variedad de necesidades de seguridad, puede realizar la Configuración de la política de autenticación para configurar las reglas de la política de autenticación que activan la MFA o un factor de autenticación único (como las credenciales

© 2020 Palo Alto Networks, Inc.

de inicio de sesión o los certificados) en función de los servicios, las aplicaciones y los usuarios finales específicos.

Cuando seleccione la cantidad y los tipos de factores de autenticación que aplicará, debe comprender cómo afecta la evaluación de la política a la experiencia del usuario. Cuando un usuario solicita un servicio o aplicación, el cortafuegos evalúa la política de autenticación. Si la solicitud coincide con una regla de la política de autenticación con MFA habilitada, el cortafuegos muestra un formulario web del portal de autenticación, de modo que los usuarios puedan autenticarse para el primer factor. Si la autenticación se produce correctamente, el cortafuegos muestra una página de inicio de sesión de MFA para cada factor adicional. Algunos servicios de MFA le solicitan al usuario seleccionar un factor de dos a cuatro, lo que es útil cuando algunos factores no se encuentran disponibles. Si la autenticación se produce correctamente en todos los factores, el cortafuegos evalúa la política de seguridad para el servicio o aplicación solicitado.



Para reducir la frecuencia de los desafíos de autenticación que interrumpen el flujo de trabajo del usuario, configure el primer factor para que utilice el inicio de sesión único (single sign-on, SSO) de Kerberos o SAML.

Para implementar la MFA de GlobalProtect, consulte la Configuración de GlobalProtect para facilitar las notificaciones de la autenticación multifactor.

No puede utilizar los perfiles de autenticación de MFA en las secuencias de autenticación.

Para la autenticación de usuario final por medio de la política de autenticación, el cortafuegos integra directamente varias plataformas de MFA (Duo v2, Okta Adaptive, PingID y SecurID de RSA), además de la integración a través de RADIUS o SAML para el resto de las plataformas de MFA. Para la autenticación de usuario remoto en portales y puertas de enlace de GlobalProtect y para la autenticación de administrador en Panorama y la interfaz web de PAN-OS, el cortafuegos se integra con proveedores de MFA utilizando únicamente RADIUS y SAML.

El cortafuegos admite los siguientes factores de MFA:

Factor	Description (Descripción)
Enviar	Un dispositivo de extremo (como un teléfono o tableta) le pide al usuario que permita o deniegue la autenticación.
Servicio de mensajes cortos (SMS)	Un mensaje de SMS en el dispositivo de extremo le pide al usuario que permita o deniegue la autenticación. En algunos casos, el dispositivo de extremo proporciona un código que el usuario debe introducir en la página de inicio de sesión de MFA.
Voz	Una llamada telefónica automatizada le pide al usuario que se autentique presionando una clave en el teléfono o introduciendo un código en la página de inicio de MFA.
Contraseña de una sola vez (One-time password, OTP)	Un dispositivo de extremo proporciona una cadena alfanumérica generada automáticamente que el usuario introduce en la página de inicio de sesión de MFA para habilitar la autenticación para una transacción o sesión única.

SAML

Puede utilizar el lenguaje de marcado para confirmaciones de seguridad (Security Assertion Markup Language, SAML) 2.0 para autenticar a los administradores que acceder a la interfaz web del cortafuegos o de Panorama, y a los usuarios finales que acceden a aplicaciones web internas o externas a su organización. En entornos donde cada usuario accede a varias aplicaciones y la autenticación de cada uno impediría la

© 2020 Palo Alto Networks, Inc.

producción de usuario, puede configurar el inicio de sesión único (SSO) de SAML para permitir un inicio de sesión para acceder a varias aplicaciones. De igual modo, el cierre de sesión único (single logout, SLO) de SAML le permite a un usuario finalizar sesiones de varias aplicaciones cerrando la sesión de una sola sesión. El SSO está disponible para los administradores que acceden a la interfaz web y a los usuarios finales que acceden a las aplicaciones mediante GlobalProtect o el portal de autenticación. El SLO está disponible para los administradores y los usuarios finales de GlobalProtect, pero no para los usuarios finales del portal de autenticación. Cuando configura la autenticación de SAML en el cortafuegos o en Panorama, puede especificar los atributos de SAML para la autorización de administrador. Los atributos de SAML le permiten cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, lo que, por lo general, es más sencillo que volver a configurar el cortafuegos y Panorama.

Los administradores no pueden utilizar SAML para autenticarse en la CLI del cortafuegos o de Panorama.

No puede utilizar los perfiles de autenticación de SAML en las secuencias de autenticación.

La autenticación de SAML requiere un *proveedor de servicios* (el cortafuegos o Panorama), que controla el acceso a las aplicaciones y un *proveedor de identidad* (identity provider, IdP) como PingFederate, que autentica usuarios. Cuando un usuario solicita un servicio o aplicación, el cortafuegos o Panorama intercepta la solicitud y redirige el usuario al IdP para que se autentique. Luego, el IdP autentica al usuario y devuelve una *confirmación SAML*, que indica que la autenticación fue correcta o no. La autenticación de SAML para los usuarios finales del portal de autenticación muestra la autenticación de SAML para un usuario final que accede a las aplicaciones mediante el portal de autenticación.

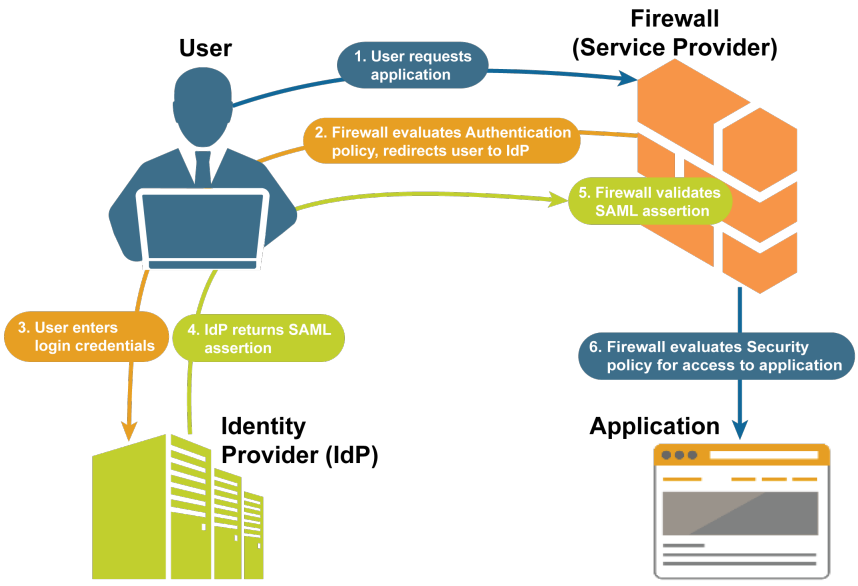


Figure 1: Autenticación SAML para usuarios finales del portal de autenticación

Kerberos

Kerberos es un protocolo de autenticación que permite un intercambio seguro de información entre las partes mediante una red insegura utilizando claves únicas (denominadas vales) para identificar a las partes. El cortafuegos y Panorama admiten dos tipos de autenticación de Kerberos para los administradores y los usuarios finales:

- **Autenticación de servidor Kerberos:** un perfil de servidor Kerberos permite a los usuarios autenticarse de manera nativa en un controlador de dominio de Active Directory o un servidor de autenticación compatible con Kerberos V5. Este método de autenticación es interactivo y requiere que los usuarios

© 2020 Palo Alto Networks, Inc.

introduzcan nombres de usuario y contraseñas. Para obtener los pasos de la configuración, consulte Configuración de la autenticación del servidor Kerberos.

- **Inicio de sesión único (SSO) de Kerberos:** una red que admita un SSO de Kerberos V5 pide al usuario que inicie sesión únicamente para el acceso inicial a la red (por ejemplo, iniciando sesión en Microsoft Windows). Tras este inicio de sesión inicial, el usuario podrá acceder a cualquier servicio basado en el explorador de la red (por ejemplo, la interfaz web del cortafuegos) sin tener que iniciar sesión de nuevo hasta que venza la sesión con SSO. (Su administrador de Kerberos define la duración de las sesiones con SSO.) Si habilita el SSO de Kerberos y los servicios de autenticación externa (como un servidor TACACS +), el cortafuegos primero prueba el SSO y, solo si falla, vuelve al servicio externo para la autenticación. Para admitir el SSO de Kerberos, su red requiere:
  - Una infraestructura Kerberos, que incluya un centro de distribución de claves (key distribution center,KDC) con un servidor de autenticación (authentication server, AS) y servicios de concesión de tickets (ticket-granting service, TGS).
  - Una cuenta de Kerberos para el cortafuegos o Panorama que autentique usuarios. Se requiere una cuenta para crear un keytab de Kerberos, que es un archivo que contiene el nombre principal y una contraseña con hash del cortafuegos o Panorama. El proceso de SSO requiere un keytab.

  Para obtener los pasos de la configuración, consulte Configuración de un inicio de sesión único de Kerberos.

  El SSO de Kerberos se encuentra disponible solo para los servicios y las aplicaciones internas de su entorno de Kerberos. Para habilitar el SSO para los servicios y las aplicaciones externas, utilice SAML.

TACACS+

El sistema de control de acceso del controlador de acceso a terminales (Terminal Access Controller Access-Control System Plus, TACACS+) es una familia de protocolos que permiten la autenticación y la autorización mediante un servidor centralizado. TACACS+ cifra nombres de usuario y contraseñas, lo que lo convierte en una opción más segura que RADIUS, que solo cifra contraseñas. TACACS+ es más fiable dado que utiliza TCP, mientras que RADIUS utiliza UDP. Puede configurar la autenticación TACACS+ para los usuarios finales o los administradores en el cortafuegos y para los administradores en Panorama. De manera opcional, puede utilizar los VSA de TACACS+ para gestionar la autorización del administrador. Los VSA de TACACS+ le permiten cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, en lugar de volver a configurar el cortafuegos y Panorama.

El cortafuegos y Panorama admiten los siguientes atributos y VSA de TACACS+. Consulte su documentación de servidor TACACS+ para obtener información sobre los pasos necesarios para definir estos VSA en el servidor TACACS+.

Nombre	Valor
service	Este atributo es necesario para identificar los VSA como específicos de Palo Alto Networks. Debe establecer el valor en **`PaloAlto`**.
Protocol	Este atributo es necesario para identificar los VSA como específicos de los dispositivos de Palo Alto Networks. Debe establecer el valor en **`firewall (cortafuegos)`**.
PaloAlto-Admin-Role	Un nombre de función de administración predeterminada (dinámica) o un nombre de función de administración personalizada en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Nombre	Valor
PaloAlto-Admin-Access-Domain	El nombre de un dominio de acceso para los administradores de cortafuegos (configurados en la página **Device [Dispositivo]** > **Access Domains [Dominios de acceso]**). Defina este VSA si el cortafuegos tiene múltiples sistemas virtuales.
PaloAlto-Panorama-Admin-Role	Un nombre de función de administración predeterminada (dinámica) o un nombre de función de administración personalizada en Panorama.
PaloAlto-Panorama-Admin-Access-Domain	El nombre de un dominio de acceso para los administradores de grupo de dispositivo y plantilla (configurados en la página **Panorama** > **Access Domains [Dominios de acceso]**).
PaloAlto-User-Group	El nombre de un grupo de usuarios en la lista de permitidos de un perfil de autenticación.

RADIUS

El servicio de autenticación remota telefónica de usuario (RADIUS) es un protocolo de red ampliamente admitido que brinda autenticación y autorización centralizadas. Puede configurar la autenticación RADIUS para los usuarios finales o los administradores en el cortafuegos y para los administradores en Panorama. De manera opcional, puede utilizar los atributos específicos del proveedor (Vendor-Specific Attributes, VSA) de RADIUS para gestionar la autorización del administrador. Los VSA de RADIUS le permiten cambiar con rapidez las funciones, los dominios de acceso y los grupos de usuarios de administradores en su servicio de directorio, en lugar de volver a configurar el cortafuegos y Panorama. Además, puede configurar el cortafuegos para utilizar un servidor RADIUS para lo siguiente:

- Recolección de VSA de los endpoints de GlobalProtect.
- Implementación de la autenticación multifactor.

Al enviar solicitudes de autenticación a un servidor RADIUS, el cortafuegos y Panorama utilizan el nombre de perfil de autenticación como el servidor de acceso de red (network access server, NAS), incluso si el perfil está asignado a una secuencia de autenticación para el servicio (como el acceso administrativo a la interfaz web) que inicia el proceso de autenticación.

El cortafuegos y Panorama admiten los siguientes VSA de RADIUS. Para definir VSA en un servidor RADIUS, debe especificar el código de proveedor (25461 para cortafuegos o Panorama de Palo Alto Networks) y el nombre y número de VSA. Algunos VSA también requieren un valor. Consulte su documentación de servidor RADIUS para obtener información sobre los pasos necesarios para definir estos VSA.

Como alternativa, puede descargar el diccionario de RADIUS de Palo Alto Networks, en el cual se definen los atributos de autenticación que emplean el cortafuegos de Palo Alto Networks y el servidor RADIUS para comunicarse entre sí, e instalarlo en dicho servidor para asignar los atributos a los datos binarios de RADIUS.

Si predefine las funciones dinámicas de administrador para los usuarios en el servidor, especifíquelas en minúscula; por ejemplo, escriba ***`superuser (superusuario)`****, no* ***`SuperUser (SuperUsuario)`****.*

Cuando configure las opciones avanzadas de proveedor en un servidor de control de acceso seguro de Cisco (Cisco Secure Access Control Server, ACS), debe establecer Vendor

© 2020 Palo Alto Networks, Inc.

Length Field Size (Tamaño del campo longitud de proveedor) y Vendor Type Field Size (Tamaño del campo de tipo de proveedor) en ***1****. De lo contrario, la autenticación fallará.*

Nombre	Número	Valor
VSA para la autenticación y la gestión de cuentas de administrador		
PaloAlto-Admin-Role	1	Un nombre de función de administración predeterminada (dinámica) o un nombre de función de administración personalizada en el cortafuegos.
PaloAlto-Admin-Access-Domain	2	El nombre de un dominio de acceso para los administradores de cortafuegos (configurados en la página **Device [Dispositivo]** > **Access Domains [Dominios de acceso]**). Defina este VSA si el cortafuegos tiene múltiples sistemas virtuales.
PaloAlto-Panorama-Admin-Role	3	Un nombre de función de administración predeterminada (dinámica) o un nombre de función de administración personalizada en Panorama.
PaloAlto-Panorama-Admin-Access-Domain	4	El nombre de un dominio de acceso para los administradores de grupo de dispositivo y plantilla (configurados en la página **Panorama** > **Access Domains [Dominios de acceso]**).
PaloAlto-User-Group	5	El nombre de un grupo de usuarios al que hace referencia un perfil de autenticación.
VSA enviados desde los endpoints de GlobalProtect al servidor RADIUS		
PaloAlto-User-Domain	6	No especifique un valor cuando defina estos VSA.
PaloAlto-Client-Source-IP	7	
PaloAlto-Client-OS	8	
PaloAlto-Client-Hostname	9	
PaloAlto-GlobalProtect-Client-Version	10	

LDAP:

El protocolo ligero de acceso a directorios (LDAP) es un protocolo estándar para acceder a directorios de información. Puede realizar la Configuración de la autenticación LDAP para los usuarios finales y para los administradores del cortafuegos y de Panorama.

La configuración del cortafuegos para conectarse a un servidor LDAP también le permite definir las reglas de la política en función de los usuarios y los grupos de usuarios, en lugar de solo las direcciones IP. Para obtener información sobre los pasos, consulte Asignación de usuarios a grupos y Habilitación de política basada en usuarios y grupos.

© 2020 Palo Alto Networks, Inc.

Autenticación local

A pesar de que el cortafuegos y Panorama ofrecen autenticación local a administradores y usuarios finales, se recomiendan los servicios de autenticación externa en la mayoría de los casos debido a que proporcionan una gestión central de las cuentas. Sin embargo, es posible que requiera cuentas de usuario especiales que no gestiona mediante los servidores del directorio que la organización reserva para las cuentas regulares. Por ejemplo, puede definir una cuenta de superusuario local en el cortafuegos para poder acceder al cortafuegos incluso aunque el servidor del directorio no funcione. En estos casos, puede utilizar los siguientes métodos de autenticación local:

- **(Solo en el cortafuegos) Autenticación de base de datos local:** para realizar la Configuración de la autenticación de la base de datos local, cree una base de datos que funcione localmente en el cortafuegos y contenga las cuentas de usuario (nombres de usuario y contraseñas, o contraseñas con hash) y los grupos de usuarios. Este tipo de autenticación es útil para la creación de cuentas de usuario que reutilizan las credenciales de las cuentas Unix existentes en casos donde solo conoce las contraseñas con hash, no las contraseñas en texto normal. Dado que la autenticación de base de datos local se asocia con los perfiles de autenticación, puede incluir implementaciones donde diferentes conjuntos de usuarios requieren diferentes configuraciones de autenticación, como el SSO de Kerberos o la autenticación multifactor. (Para obtener información detallada, consulte Configuración de una secuencia y perfil de autenticación). En el caso de las cuentas que utilizan contraseñas en texto normal, también puede realizar el paso Defina la complejidad de la contraseña y la configuración del vencimiento. Este método de autenticación se encuentra disponible para los administradores que acceden al cortafuegos (pero no a Panorama) y para los usuarios finales que acceden a servicios y aplicaciones mediante el portal de autenticación o GlobalProtect.
- **Autenticación local sin una base de datos:** puede configurar cuentas administrativas del cortafuegos o cuentas administrativas de Panorama sin crear una base de datos de los usuarios y los grupos de usuarios que se ejecute localmente en el cortafuegos o en Panorama. Dado que este método no está asociado a los perfiles de autenticación, no puede combinarlo con el SSO de Kerberos o la MFA. Sin embargo, este es el único método de autenticación que permite perfiles de contraseña, lo que le permite asociar cuentas individuales con configuración de vencimiento de contraseña que se diferencia de la configuración global. (Si desea información detallada, consulte Defina la complejidad de la contraseña y la configuración del vencimiento)

© 2020 Palo Alto Networks, Inc.

Planificación de su implementación de autenticación

A continuación, se muestran las preguntas clave que deben considerarse antes de implementar una solución de autenticación para los administradores que acceden al cortafuegos y a los usuarios finales que acceden a los servicios y aplicaciones mediante el portal de autenticación.

En el caso de los usuarios finales y los administradores, considere las siguientes interrogantes:

- ¿Cómo puede aprovechar su infraestructura de seguridad existente? Por lo general, integrar el cortafuegos con una infraestructura existente es más rápido y económico que establecer una solución separada nueva solo para los servicios del cortafuegos. El cortafuegos se puede integrar con autenticación multifactor, SAML, Kerberos, TACACS+, RADIUS, y servidores LDAP. Si sus usuarios acceden a los servicios y aplicaciones externos a su red, puede utilizar SAML para integrar el cortafuegos con un proveedor de identidad (IdP) que controla el acceso a los servicios y aplicaciones externos e internos.
- ¿Cómo se puede optimizar la experiencia de usuario? Si no desea que los usuarios se autentiquen manualmente y no cuenta con una infraestructura de clave pública, puede implementar la autenticación de certificados. Otra opción es implementar el inicio de sesión único (single sign-on, SSO) de Kerberos o SAML, de modo que los usuarios puedan acceder a varios servicios y aplicaciones tras iniciar sesión en uno. Si su red requiere seguridad adicional, puede combinar la autenticación de certificados con la autenticación interactiva (desafío-respuesta).
- ¿Requiere cuentas de usuario especiales que no gestiona mediante los servidores del directorio que la organización reserva para las cuentas regulares? Por ejemplo, puede definir una cuenta de superusuario local en el cortafuegos para poder acceder al cortafuegos incluso aunque el servidor del directorio no funcione. Puede configurar la autenticación local para estas cuentas con fines especiales.



Suelen ser preferibles los servicios de autenticación externos en lugar de los de autenticación local porque ofrecen gestión central de cuentas, servicios de autenticación fiables y, por lo general, funciones de creación de logs y solución de problemas.

Solo en el caso de los usuarios finales, considere lo siguiente:

- ¿Qué servicios y aplicaciones son más delicados que otros? Por ejemplo, es posible que desee una autenticación más sólida para los documentos financieros clave que para los motores de búsqueda. Para proteger los servicios y aplicaciones más delicados, puede configurar la Autenticación multifactor (Multi-Factor Authentication, MFA) para garantizar que cada usuario se autentique utilizando varios métodos (factores) cuando accede a esos servicios y aplicaciones. Para responder a distintas necesidades de seguridad, realice la Configuración de la política de autenticación para configurar las reglas de la política de autenticación que desencadenan la MFA o la autenticación de factor único (como las credenciales de inicio de sesión o los certificados) en función de los servicios, las aplicaciones y los usuarios finales específicos. Entre las otras maneras de reducir la superficie de ataque, se encuentran la segmentación de la red y los grupos de usuario para aplicaciones permitidas.

En el caso de solo los administradores, considere lo siguiente:

- ¿Utiliza un servidor externo para gestionar centralmente la autorización de todas las cuentas administrativas? Si define los atributos específicos del proveedor (Vendor-Specific Attributes, VSA) en el servidor externo, puede cambiar con rapidez las asignaciones de funciones administrativas mediante el servicio de su directorio en lugar de volver a configurar el cortafuegos. Los VSA también le permiten especificar los dominios de acceso para los administradores de cortafuegos con varios sistemas virtuales. SAML, TACACS+ y RADIUS admiten autorización externa.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación multifactor

Para usar la autenticación multifactor (Multi-Factor Authentication, MFA) para proteger servicios y aplicaciones sensibles, debe configurar el portal de autenticación para que muestre un formulario web para el primer factor de autenticación y registrar marcas de tiempo de autenticación. El cortafuegos utiliza las marcas de tiempo para evaluar los tiempos de espera para las reglas de política de autenticación. Para habilitar los factores de autenticación adicionales, puede integrar el cortafuegos con proveedores MFA a través de RADIUS o API de proveedor. Después de evaluar la política de autenticación, el cortafuegos evalúa la política de seguridad, por lo que se deben configurar reglas para ambos tipos de política.

Palo Alto Networks proporciona soporte a proveedores MFA a través de actualizaciones de contenido de aplicaciones. Esto significa que si utiliza Panorama para enviar configuraciones de grupo de dispositivos a los cortafuegos, debe instalar las mismas actualizaciones de aplicaciones en los cortafuegos que en Panorama para evitar discrepancias en el soporte del proveedor.

Solo se admiten integraciones de API de proveedor de MFA en la autenticación de usuario final a través de la política de autenticación. Para la autenticación de usuario remoto en portales o puertas de enlace de GlobalProtect o para la autenticación de administrador en PAN-OS o la interfaz web de Panorama, solo puede utilizar proveedores de MFA compatibles con RADIUS o SAML; los servicios de MFA en las API de proveedor no son compatibles en estos casos de uso.

STEP 1 | Configure el portal de autenticación en el modo **Redirect (Redirigir)** para mostrar un formulario web para el primer factor de autenticación, registrar marcas de tiempo de autenticación y actualizar asignaciones de usuario.

STEP 2 | Configure uno de los siguientes perfiles de servidor para definir de qué manera el cortafuegos se conectará con el servicio que autentica a los usuarios para el primer factor de autenticación.

- Añada un perfil de servidor RADIUS. Esto es necesario si el cortafuegos se integra con un proveedor MFA a través de RADIUS. En ese caso, el proveedor MFA proporciona el primero y todos los factores de autenticación adicionales para que usted pueda omitir el paso siguiente (configuración de un perfil de servidor MFA). Si el cortafuegos se integra con un proveedor MFA a través de una API, se puede usar un perfil de servidor RADIUS para el primer factor, pero se necesitan los perfiles de servidor MFA para los factores adicionales.
- Añada un perfil de servidor SAML IdP.
- Añada un perfil de servidor Kerberos.
- Añada un perfil de servidor TACACS+.
- Añada un perfil de servidor LDAP.

En la mayoría de los casos, se recomienda un servicio externo para el primer factor de autenticación. Sin embargo, puede realizar la configuración de autenticación de base de datos local como alternativa.

STEP 3 | Añada un perfil de servidor MFA.

El perfil define de qué manera el cortafuegos se conecta con el servidor MFA. Añada un perfil separado para cada factor de autenticación después del primer factor. El cortafuegos se integra con estos servidores MFA a través de API de proveedores. Puede especificar hasta tres factores adicionales. Cada proveedor MFA proporciona un factor, si bien algunos proveedores permiten a los usuarios elegir un factor entre varios.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Multi Factor Authentication (Autenticación multifactor)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un nombre en **Name (Nombre)** para identificar el servidor MFA.
3. Seleccione el **Certificate Profile (Perfil del certificado)** que el cortafuegos utilizará para validar el certificado del servidor MFA al establecer una conexión segura con el servidor MFA.
4. Seleccione el **MFA Vendor (Proveedor MFA)** que implementó.
5. Configure el **Value (Valor)** de cada atributo de proveedor.

   Los atributos definen de qué manera el cortafuegos se conecta con el servidor MFA. Cada **Type (Tipo)** de proveedor requiere diferentes atributos y valores; consulte la documentación de su proveedor para obtener detalles.
6. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 4 | Configure un perfil de autenticación.

El perfil define el orden de los factores de autenticación a los que los usuarios deben responder.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
3. Seleccione el **Type (Tipo)** para el primer factor de autenticación y seleccione el **Server Profile (Perfil de servidor)** correspondiente.
4. Seleccione **Factors (Factores)**, **Enable Additional Authentication Factors (Habilitar factores de autenticación adicionales)** y luego **Add (Añadir)** para añadir los perfiles de servidor MFA que configuró.

   El cortafuegos invocará cada servicio MFA en el orden enumerado, desde arriba hacia abajo.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 5 | Configure un objeto de cumplimiento de autenticación.

El objeto asocia cada perfil de autenticación con un método de portal de autenticación. El método determina si el primer desafío de autenticación (factor) es transparente o requiere una respuesta del usuario.

Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró e introduzca un **Message (Mensaje)** que indique a los usuarios cómo autenticarse con el primer factor. El mensaje se muestra en el formulario web del portal de autenticación.



Si usted configura el Authentication Method (Método de autenticación) en browser-challenge (comprobación del navegador), el formulario web del portal de autenticación se muestra solo si la autenticación SSO de Kerberos falla. De lo contrario, la autenticación para el primer factor es automática, los usuarios no verán el formulario web.

STEP 6 | Configure una regla de política de autenticación.

La regla debe coincidir con los servicios y aplicaciones que usted desea proteger y los usuarios que deben autenticarse.

1. Seleccione **Policies (Políticas)** > **Authentication (Autenticación)** y luego **Add (Añadir)** para añadir una regla.
2. Introduzca un nombre en **Name** para identificar la regla.
3. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir zonas específicas, o seleccione **Any (Cualquiera)** para seleccionar cualquier zona o dirección IP.

   La regla se aplica únicamente al tráfico proveniente de las direcciones IP identificadas o de las interfaces en las zonas especificadas.

© 2020 Palo Alto Networks, Inc.

4. Seleccione **User (Usuario)** y seleccione o añada, haciendo clic en **Add (Añadir)**, los grupos de usuario a los cuales se aplica la regla (el valor predeterminado es **any [cualquiera]**).
5. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir zonas y direcciones IP específicas, o seleccione **Any (Cualquiera)** para seleccionar cualquier zona o dirección IP.

   La direcciones IP pueden ser recursos (como servidores) para los cuales usted desea controlar el acceso.
6. Seleccione **Service/URL Category (Categoría de URL/servicio)** y seleccione o añada, haciendo clic en **Add (Añadir)**, los servicios y grupos de servicio para los cuales la regla controla el acceso (el valor predeterminado es **service-http**).
7. Seleccione o añada, haciendo clic en **Add (Añadir)**, las categorías URL para las cuales la regla controla el acceso (el valor predeterminado es **any [cualquiera]**). Por ejemplo, puede crear una categoría URL personalizada que especifique sus sitios internos más sensibles.
8. Seleccione **Actions (Acciones)** y seleccione el objeto de **Authentication Enforcement (Cumplimiento de la autenticación)** que creó.
9. Especifique el periodo de **Timeout (Tiempo de espera)** en minutos (el valor predeterminado es 60) durante el cual el cortafuegos indica al usuario que se autentique solo una vez para el acceso repetido a los servicios y aplicaciones.

   Timeout (Tiempo de espera) es un término medio entre una seguridad más estricta (menos tiempo entre los mensajes de autenticación) y la experiencia del usuario (más tiempo entre los mensajes de autenticación). Una autenticación más frecuente a menudo es la opción correcta para acceder a sistemas críticos y áreas sensibles, tales como un centro de datos. Una autenticación menos frecuente a menudo es la opción correcta en el perímetro de red y para empresas en las cuales la experiencia del usuario es un factor clave.
10. Haga clic en **OK (Aceptar)** para guardar la regla.

STEP 7 | Personalice la página de inicio de sesión de MFA.

El cortafuegos muestra esta página para indicar a los usuarios cómo autenticarse para los factores MFA e indicar el estado de autenticación (en curso, correcto o fallido).

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** y seleccione **MFA Login Page (Página de inicio de sesión de MFA)**.
2. Seleccione la página de respuesta **Predefined (Predefinida)** y **Export (Exporte)** la página a su sistema cliente.
3. En su sistema cliente, use un editor HTML para personalizar la página de respuesta descargada y guardarla con un nombre de archivo único.
4. Regrese al cuadro de diálogo MFA Login Page (Página de inicio MFA) en el cortafuegos, seleccione **Import (Importar)** para importar su página personalizada, **Browse (Examinar)** para seleccionar **Import File (Importar archivo)**, luego seleccione el **Destination (Destino)** (sistema virtual o ubicación **shared [compartida]**), haga clic en **OK (Aceptar)**, y luego haga clic en **Close (Cerrar)**.

STEP 8 | Configure una regla de política de seguridad que permita a los usuarios acceder a los servicios y aplicaciones que requieren autenticación.

1. Creación de una regla de política de seguridad.
2. **Commit (Confirmar)** los cambios.

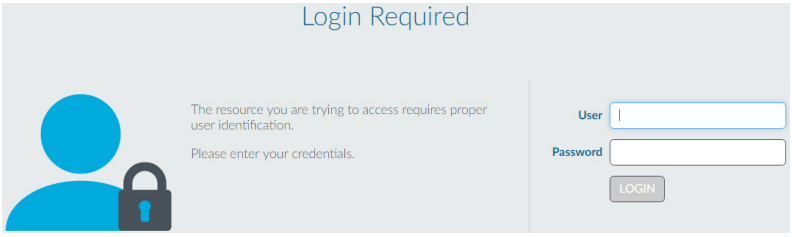
   El motor de correlación automatizado en el cortafuegos utiliza varios objetos de correlación para detectar eventos en su red que podrían indicar abuso de credenciales en relación con MFA. Para revisar los eventos, seleccione **Monitor (Supervisar) Automated Correlation Engine (Motor de correlación automatizado) Correlated Events (Eventos correlacionados)**.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Verifique que el cortafuegos aplique la MFA.

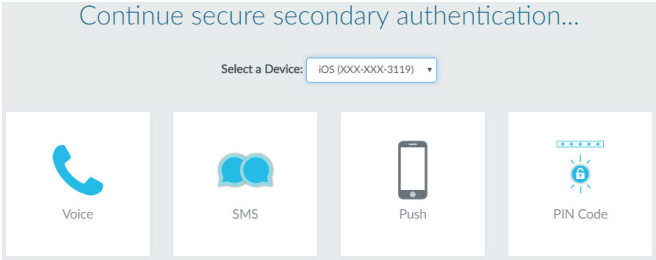
1. Inicie sesión en su red como uno de los usuarios de origen especificados en la regla de autenticación.
2. Solicite un servicio o aplicación que coincida con uno de los servicios o aplicaciones especificados en la regla.

   El cortafuegos muestra el formulario web del portal de autenticación para el primer factor de autenticación. La página contiene el mensaje que introdujo en el objeto de cumplimiento de la autenticación. Por ejemplo:



3. Introduzca sus credenciales para el primer desafío de autenticación.

   El cortafuegos luego muestra una página de inicio de sesión de MFA para el siguiente factor de autenticación. Por ejemplo, el servicio MFA puede indicarle que seleccione el método de autenticación por voz, SMS, inserción o código PIN (OTP). Si selecciona el método push (inserción), el teléfono le indicará que apruebe la autenticación.



4. Autentíquese con el siguiente factor.

   El cortafuegos muestra un mensaje de autenticación correcta o fallida. Si la autenticación se realizó correctamente, el cortafuegos muestra una página de inicio de sesión de MFA para el siguiente factor de autenticación, si hubiera.

   Repita este paso para cada factor MFA. Una vez que se ha autenticado para todos los factores, el cortafuegos evalúa la política de seguridad para determinar si permitirá el acceso al servicio o aplicación.
5. Finalice la sesión para el servicio o aplicación a los que acaba de acceder.
6. Inicie una nueva sesión para el mismo servicio o aplicación. Asegúrese de realizar este paso dentro del periodo de **Timeout (Tiempo de espera)** que configuró en la regla de autenticación.

   El cortafuegos permite el acceso sin una nueva autenticación.
7. Espere hasta que el periodo de **Timeout (Tiempo de espera)** caduque y solicite el mismo servicio o aplicación.

   El cortafuegos le solicita que vuelva a autenticarse.

Configuración de la MFA entre SecurID de RSA y el cortafuegos

La autenticación multifactor le permite proteger los activos de la empresa utilizando varios factores a fin de verificar la identidad de un usuario antes de permitirle acceder a los recursos de la red. Para permitir la autenticación multifactor (multi-factor authentication, MFA) entre el cortafuegos y el servicio de autenticación de acceso en la nube de SecurID de RSA, debe configurar el servicio SecurID de RSA, de

© 2020 Palo Alto Networks, Inc.

modo que posea los detalles que necesita para configurar el cortafuegos a fin de que autentique a los usuarios utilizando varios factores. Tras realizar la configuración necesaria en la consola de acceso de SecurID de RSA, puede configurar el cortafuegos para que se integre a SecurID de RSA.

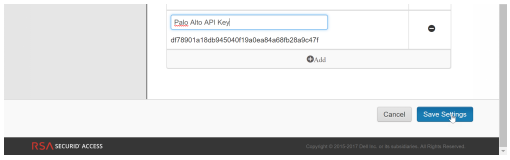
El cortafuegos de nueva generación de Palo Alto Networks se integra con el servicio de autenticación de acceso en la nube de SecurID de RSA. La integración de API de MFA con SecurID de RSA solo es compatible con los servicios basados en la nube y no admite la autenticación en dos factores del Administrador de autenticación local cuando el segundo factor usa la API específica del proveedor. La versión de contenido mínima necesaria para esta integración es 752 y PAN-OS 8.0.2.

- Obtenga información detallada sobre la autenticación de acceso en la nube de SecurID de RSA
- Configure el cortafuegos para la MFA con SecurID de RSA

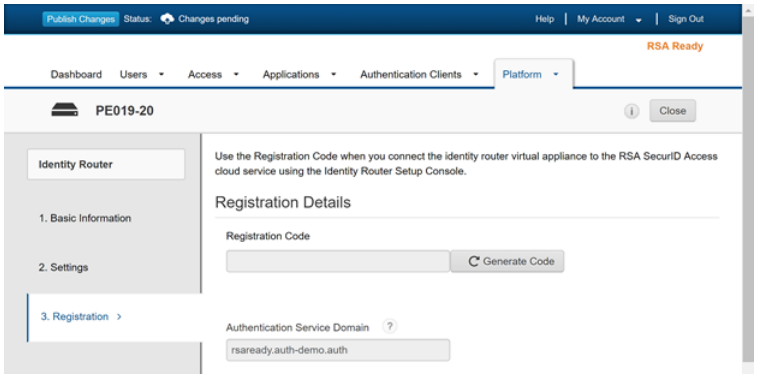
Obtenga información detallada sobre la autenticación de acceso en la nube de SecurID de RSA

Para pasar las solicitudes de autenticación de usuario con seguridad desde y hacia el cortafuegos y el servicio de autenticación de acceso en la nube de SecurID de RSA, primero debe dirigirse a la consola de acceso de SecurID de RSA y configurar la ID de acceso de RSA, la URL de servicio de autenticación y la clave de cliente de la API que el cortafuegos necesita para autenticarse e interactuar con el servicio. Además, el cortafuegos requiere la ID de política de acceso que utiliza el método de autenticación de RSA Approve o de código token de RSA para autenticarse en el origen de identidad.

- **Genere la clave de la API de SecurID de RSA**: inicie sesión en la consola de acceso de SecurID de RSA y seleccione **My Account (Mi cuenta)** > **Company Settings (Ajustes de la empresa)** > **Authentication API Keys (Claves de API de autenticación)**. Haga clic en **Add (Añadir)** para añadir una clave nueva y haga clic en **Save Settings (Guardar configuración)** y en **Publish Changes (Publicar cambios)**.

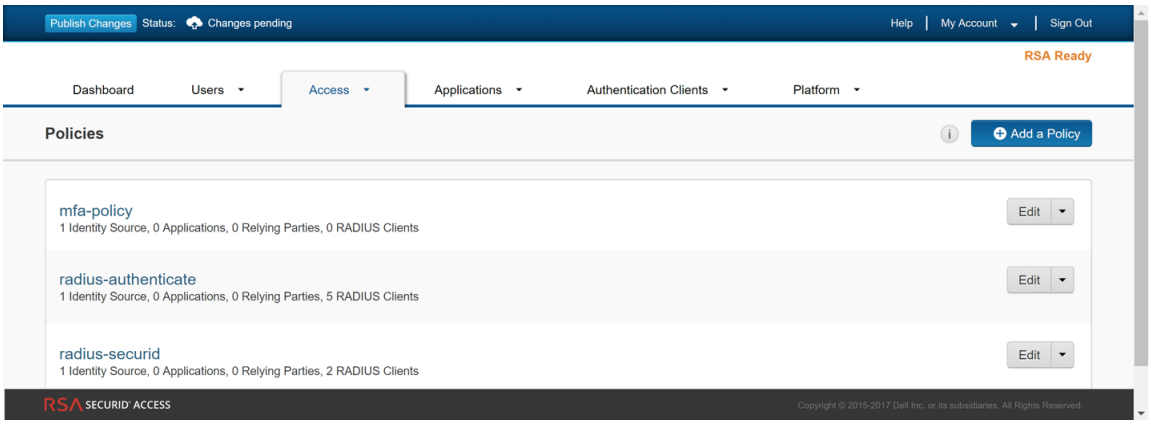


- **Obtenga la API del endpoint de acceso de SecurID de RSA (dominio de servicio de autenticación) a la que el cortafuegos debe conectarse**: seleccione **Platform (Plataforma)** > **Identity Routers (Enrutador de identidad)**, seleccione un enrutador de identidad para **Edit (Editar)** y anote el **Authentication Service Domain (Dominio de servicio de autenticación)**. En este ejemplo, es https://rsaready.auth-demo.auth.



© 2020 Palo Alto Networks, Inc.

- **Obtener la ID de la política de acceso**: seleccione **Access (Acceso)** > **Policies (Políticas)** y anote el nombre de la política de acceso que permitirá al cortafuegos actuar como cliente de autenticación para el servicio SecurID de RSA. La política debe configurarse para que utilice únicamente los métodos de autenticación de RSA Approve o de código token de RSA.



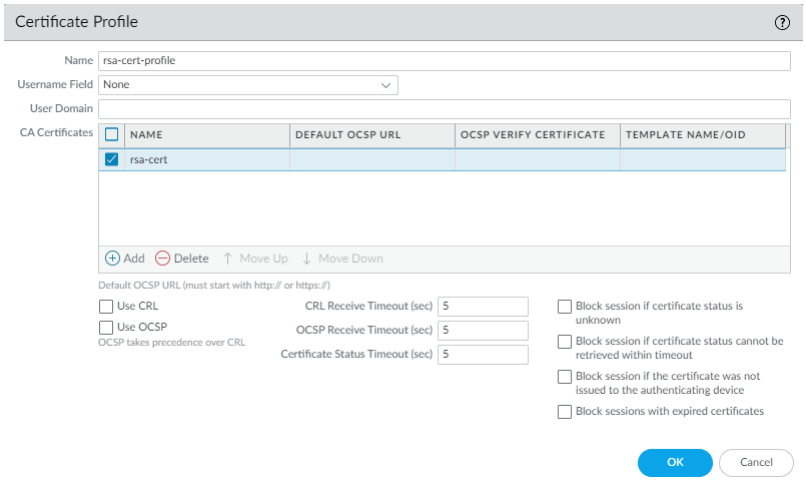
Configure el cortafuegos para la MFA con SecurID de RSA

Después de la Obtención de información detallada sobre la autenticación de acceso en la nube de SecurID de RSA, configure el cortafuegos para que le solicite a los usuarios un token de SecurID de RSA cuando se invoque la MFA.

STEP 1 | Configure el cortafuegos para que confíe en certificados SSL proporcionados por la API de acceso de endpoint de SecurID de RSA.

1. Exporte el certificado SSL desde el endpoint de acceso de SecurID de RSA e impórtelo al cortafuegos.

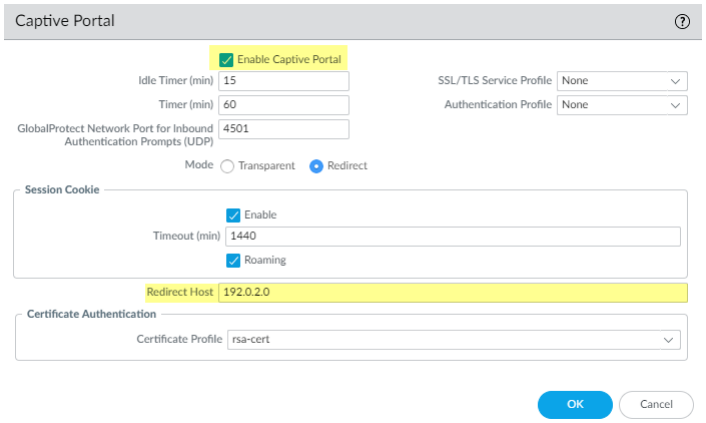
   Para habilitar la confianza entre el cortafuegos y la API del endpoint de acceso de SecurID de RSA, debe importar un certificado autofirmado o el certificado de CA que se utilizó para firmar el certificado.
2. Realice la configuración de un perfil de certificado (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **Certificate Profile [Perfil de certificados]** y haga clic en **Add [Añadir]**).



STEP 2 | Configure el portal de autenticación (**Device [Dispositivo]** > **User Identification [Identificación de usuario]** > **Captive Portal Settings [Ajustes del portal de autenticación]**) en el modo de redireccionamiento para mostrar un formulario web de autenticación de SecureID de RSA. Asegúrese de especificar el Redirect Host (Host de redireccionamiento) como una dirección IP

© 2020 Palo Alto Networks, Inc.

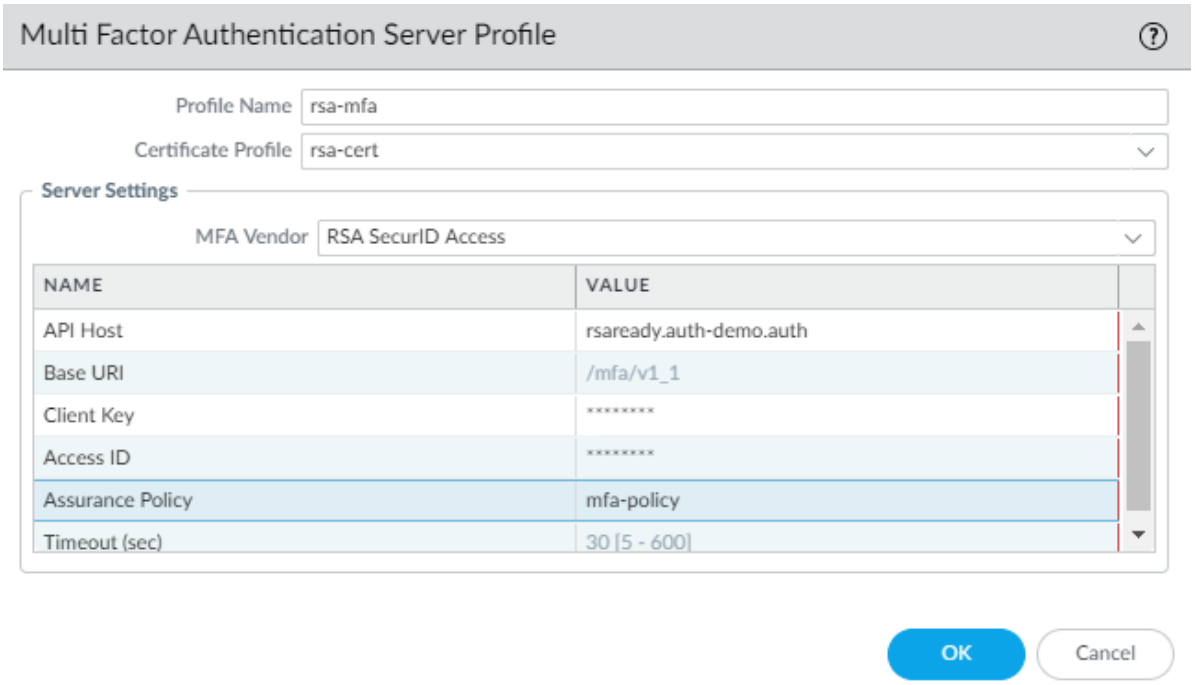
o un nombre de host (sin punto en su nombre) que resuelve a la dirección IP de la interfaz de capa 3 del cortafuegos a la que se redirigirán las solicitudes web.



STEP 3 | Configure un perfil de servidor de autenticación multifactor para especificar cómo se debe conectar el cortafuegos con el servicio en la nube de SecurID de RSA **(Device [Dispositivo]** > **Server Profiles [Perfiles de servidor]** > **Multi Factor Authentication [Autenticación multifactor]** y haga clic en **Add [Añadir]**).

1. Introduzca un **Name (Nombre)** para identificar el servidor de MFA.
2. Seleccione el **Certificate Profile (Perfil de certificado)** que creó previamente, rsa-cert-profile en este ejemplo. El cortafuegos utilizará este certificado cuando establezca una conexión segura con el servicio en la nube de SecurID de RSA.
3. En el menú desplegable **MFA Vendor (Proveedor de MFA)**, seleccione **RSA SecurID Access (Acceso de SecurID de RSA)**.
4. Configure el **Value (Valor)** de cada atributo que observó en la Obtención de información detallada sobre la autenticación de acceso en la nube de SecurID de RSA:
   - **API Host (Host de API)**: introduzca el nombre de host o la dirección IP del endpoint de la API de acceso de SecurID de RSA al que debe conectarse el cortafuegos, rsaready.auth-demo.auth en este ejemplo.
   - **Base URI (URI básico)**: no modifique el valor predeterminado (/mfa/v1_1)
   - **Client Key (Clave de cliente)**: introduzca la clave de cliente de SecurID de RSA.
   - **Access ID (ID de acceso)**: introduzca la ID de acceso de SecurID de RSA.
   - **Assurance Policy (Política de garantías)**: introduzca el nombre de la política de acceso de SecurID de RSA, mfa-policy en este ejemplo.
   - **Timeout (Tiempo de espera)**: el valor predeterminado es de 30 segundos.

© 2020 Palo Alto Networks, Inc.

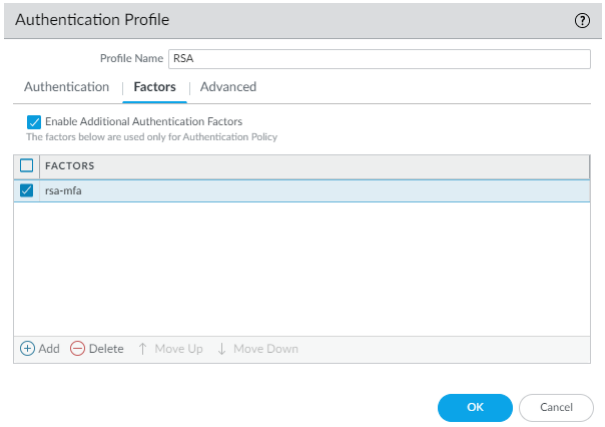


5. Guarde el perfil.

STEP 4 | Configure un perfil de autenticación (**Device [Dispositivo]** > **Authentication Profile [Perfil de autenticación]** y haga clic en **Add [Añadir]**).

El perfil define el orden de los factores de autenticación a los que los usuarios deben responder.

1. Seleccione el **Type (Tipo)** para el primer factor de autenticación y seleccione el **Server Profile (Perfil de servidor)** correspondiente.
2. Seleccione **Factors (Factores)**, **Enable Additional Authentication Factors (Habilitar factores de autenticación adicionales)** y haga clic en **Add (Añadir)** para añadir el perfil de servidor rsa-mfa que creó antes en este ejemplo.

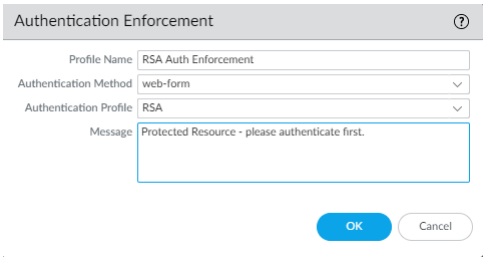


3. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 5 | Configure un objeto de cumplimiento de autenticación. (**Objects [Objetos] Authentication [Autenticación]** y haga clic en **Add (Añadir)**).

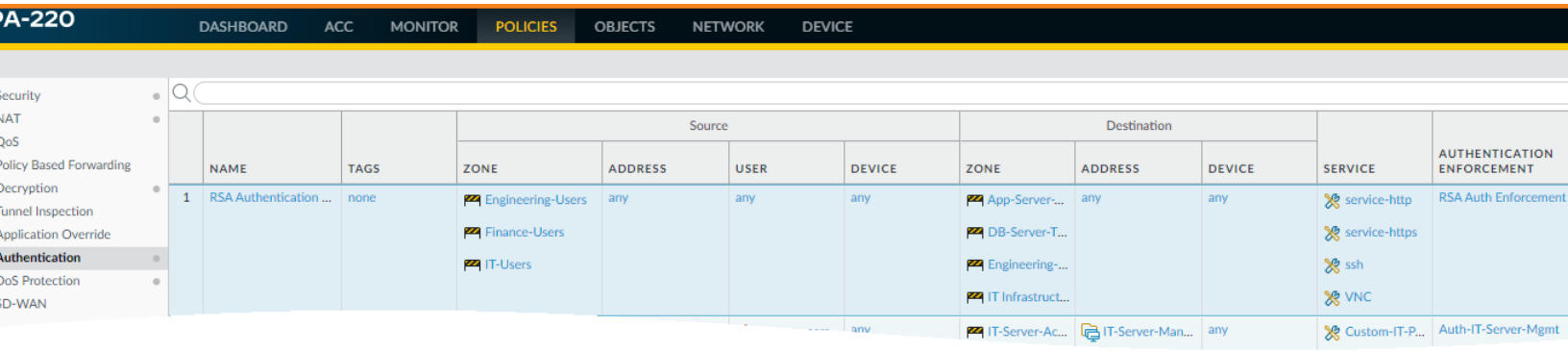
Asegúrese de seleccionar el perfil de autenticación que acaba de definir, RSA en este ejemplo.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Configure una regla de política de autenticación. (**Policies [Políticas] Authentication [Autenticación]** y haga clic en **Add (Añadir)**).

La regla de la política de autenticación debe coincidir con los servicios y las aplicaciones que desea proteger, especificar los usuarios que debe autenticar, e incluir el objeto de aplicación de autenticación que activa el perfil de autenticación. En este ejemplo, el acceso de SecurID de RSA autentica a todos los usuarios que acceden a tráfico HTTP, HTTPS, SSH y VNC con el objeto de aplicación de autenticación denominado RSA Auth Enforcement (Aplicación de autenticación de RSA) (en **Actions [Acciones]**, seleccione el objeto de **Authentication Enforcement [Aplicación de autenticación]**).

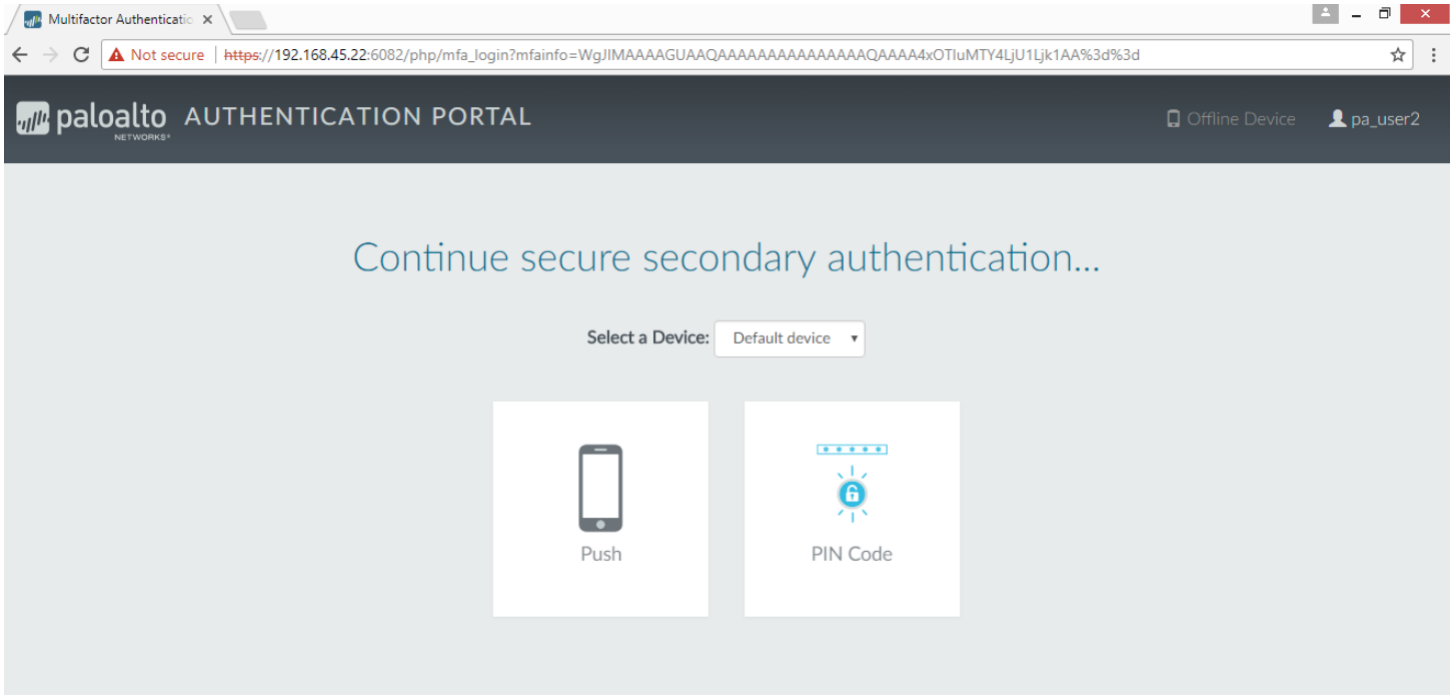


STEP 7 | Haga clic en **Commit (Confirmar)** para confirmar los cambios en el cortafuegos.

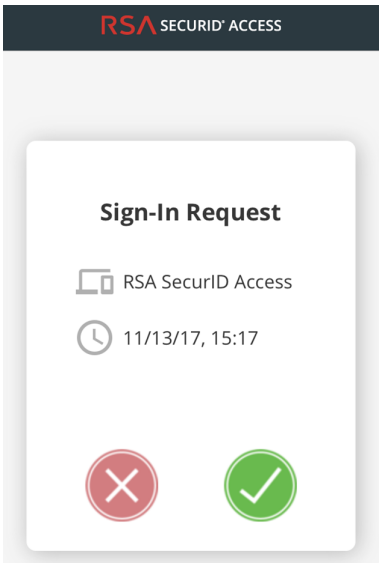
STEP 8 | Verifique que los usuarios en su red estén protegidos con SecurID de RSA utilizando el método de autenticación por inserción o código PIN que habilitó.

1. **Autenticación de inserción**
    1. Solicite a un usuario de su red que inicie un navegador web y que acceda a un sitio web. Se debe mostrar la página del portal de autenticación con la dirección IP o nombre de host para el host de redireccionamiento que definió antes.
    2. Verifique que el usuario introduzca las credenciales para el primer factor de autenticación y continúe con el segundo factor de autenticación, y seleccione **Push (Inserción)**.

© 2020 Palo Alto Networks, Inc.



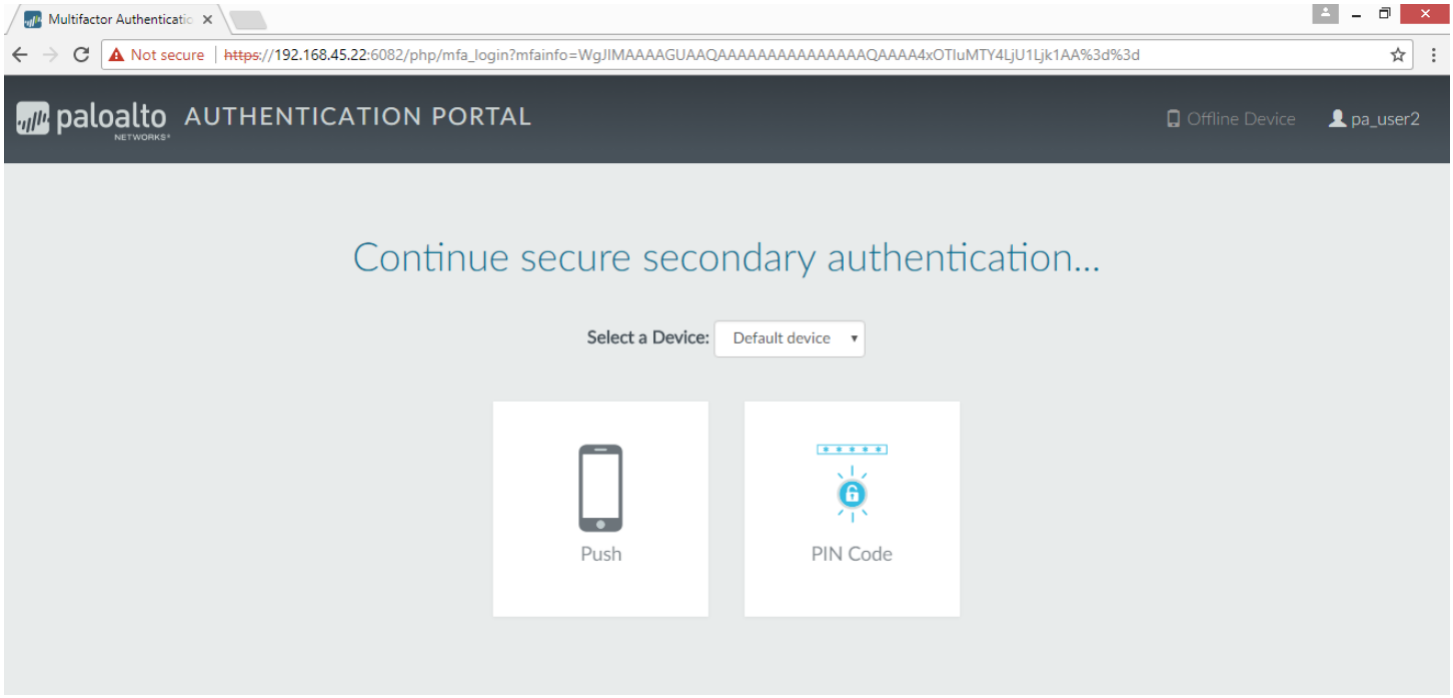
3. Compruebe que se muestre una **Sign-In request (Solicitud de inicio de sesión)** en la aplicación de acceso de SecurID de RSA en el dispositivo móvil del usuario.
4. Solicite al usuario que haga clic en **Accept (Aceptar)** para aceptar la solicitud de inicio de sesión en el dispositivo móvil y espere unos segundos a que el cortafuegos reciba la notificación de la autenticación correcta. El usuario debe poder acceder al sitio web solicitado.



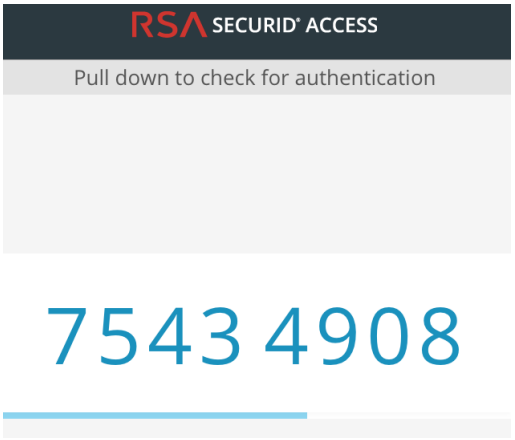
Para probar un fallo de autenticación, haga clic en Decline (Rechazar) para rechazar la solicitud de inicio de sesión en el dispositivo móvil.

2. **Autenticación con código PIN**
   1. Solicite a un usuario de su red que inicie un navegador web y que acceda a un sitio web. Se debe mostrar la página del portal de autenticación con la dirección IP o nombre de host para el host de redireccionamiento que definió antes.
   2. Verifique que el usuario introduzca las credenciales para el primer factor de autenticación y continúe con el segundo factor de autenticación, y seleccione **PIN Code (Código PIN)**.

© 2020 Palo Alto Networks, Inc.



3. Compruebe que se muestre un **PIN Code (Código PIN)** en la aplicación de acceso de SecurID de RSA en el dispositivo móvil del usuario.



4. Solicite al usuario que copie el código PIN en el mensaje **Enter the PIN... (Introduzca el PIN...)** del navegador web y haga clic en **Submit (Enviar)**. Espere unos segundos a que el cortafuegos reciba la notificación de la autenticación correcta. El usuario debe poder acceder al sitio web solicitado.

Configuración de la MFA entre Okta y el cortafuegos

La autenticación multifactor le permite proteger los activos de la empresa utilizando varios factores para verificar la identidad de los usuarios antes de permitirles acceder a los recursos de la red.

Para habilitar la autenticación multifactor (multi-factor authentication, MFA) entre el cortafuegos y el servicio de administración de identidades de Okta, revise lo siguiente:

- Configuración de Okta
- Configuración del cortafuegos para integrarse con Okta
- Verificación de MFA con Okta

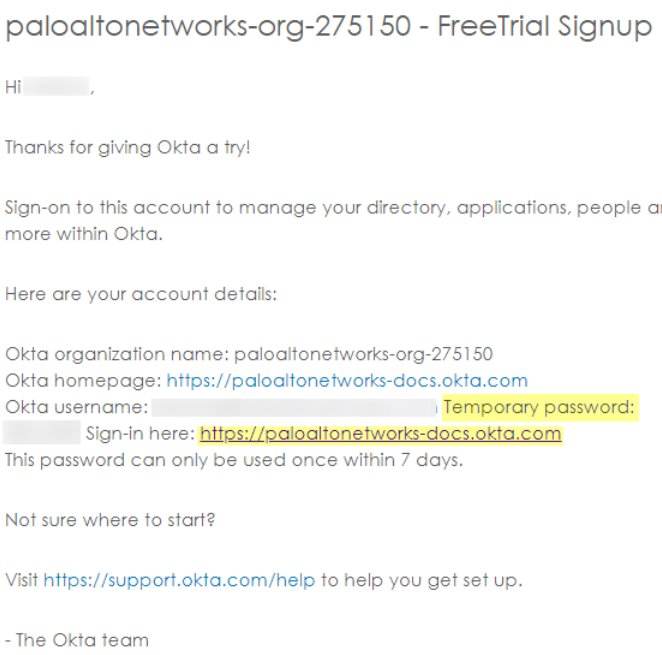
© 2020 Palo Alto Networks, Inc.

Configuración de Okta

Inicie sesión en el portal de administrador de Okta para crear sus cuentas de usuario, defina la política de MFA de Okta y obtenga la información del token requerido para configurar MFA con Okta en el cortafuegos.

STEP 1 | Cree una cuenta de usuario administrador de Okta.

1. Introduzca su nombre y dirección de correo electrónico, luego haga clic en **Get Started (Comenzar)**.
2. Haga clic en el enlace del correo electrónico de confirmación y use la contraseña temporal incluida para iniciar sesión en el portal de administrador de Okta.


paloaltonetworks-org-275150 - FreeTrial Signup

Hi ,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: Temporary password:
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

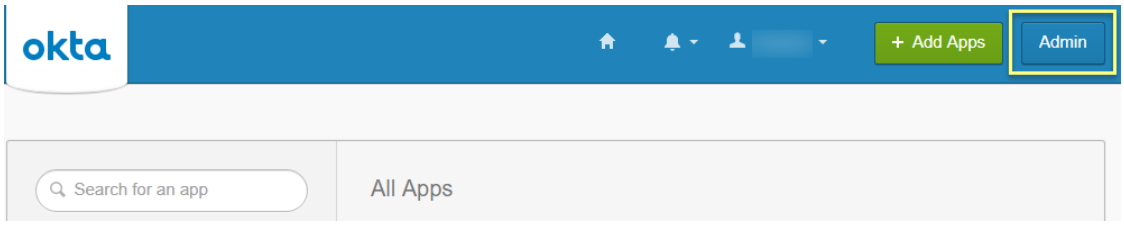
Visit https://support.okta.com/help to help you get set up.

- The Okta team

3. Cree una contraseña nueva que incluya al menos 8 caracteres, una letra en minúscula, una letra en mayúscula, un número y no incluya ninguna parte de su nombre de usuario.
4. Seleccione una pregunta para recordar la contraseña e introduzca la respuesta.
5. Seleccione una imagen de seguridad, luego haga clic en **Create My Account (Crear mi cuenta)**.

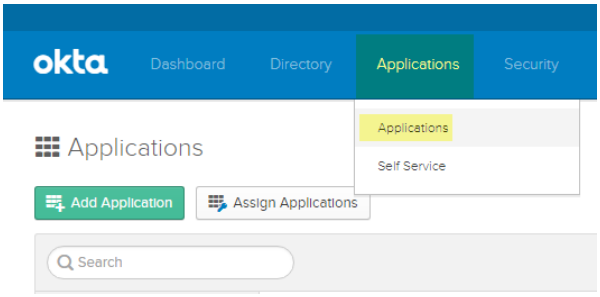
STEP 2 | Configure su servicio de Okta.

Si inicia sesión y no se le redirige al portal de administrador de Okta, seleccione Admin (Administrador) en la parte superior derecha.

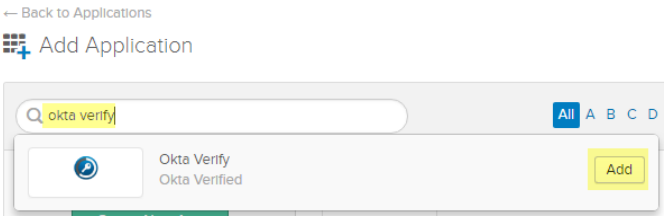


1. Desde el panel de Okta, inicie sesión con sus credenciales de administrador de Okta, luego seleccione **Applications (Aplicaciones)** > **Applications (Aplicaciones)**.

© 2020 Palo Alto Networks, Inc.

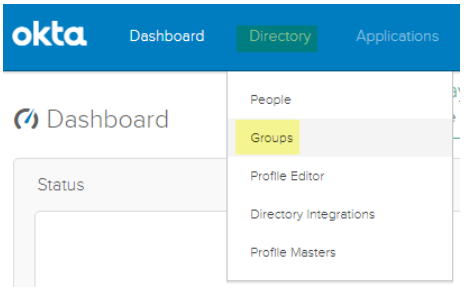


2. Seleccione **Add Application (Añadir aplicación)**.
3. Busque **`Okta Verify`**.
4. Seleccione **Add (Añadir)** y luego **Done (Listo)**.

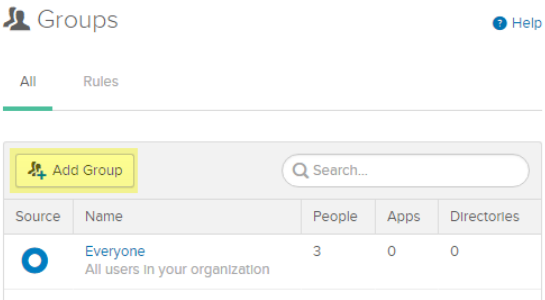


STEP 3 | Cree uno o más grupos de usuarios para clasificar a sus usuarios (por ejemplo, por dispositivo, política o departamento) y asigne la aplicación de Okta Verify.

1. Seleccione **Directory (Directorio)** > **Groups (Grupos)**.

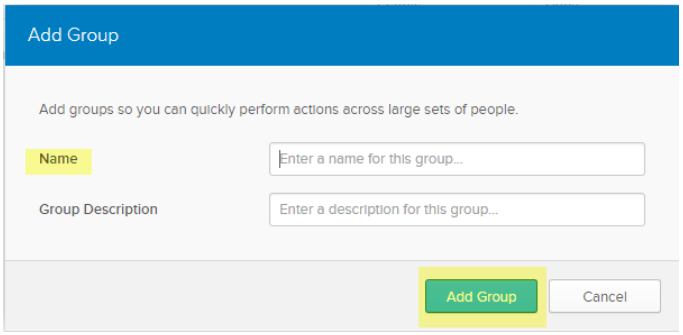


2. Haga clic en **Add Group (Añadir grupo)**.



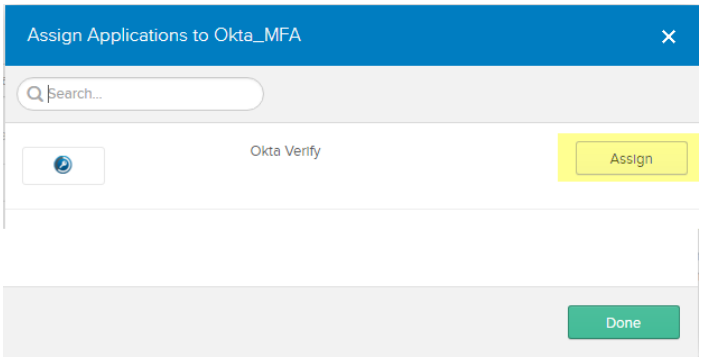
3. Introduzca el nombre del grupo en **Name (Nombre)** y de manera opcional, una **Group Description (Descripción de grupo)**, luego seleccione **Add Group (Añadir grupo)**.

© 2020 Palo Alto Networks, Inc.



*El grupo predeterminado **Todos** incluye a todos los usuarios configurados para su organización durante el primer paso de la Configuración de Okta.*

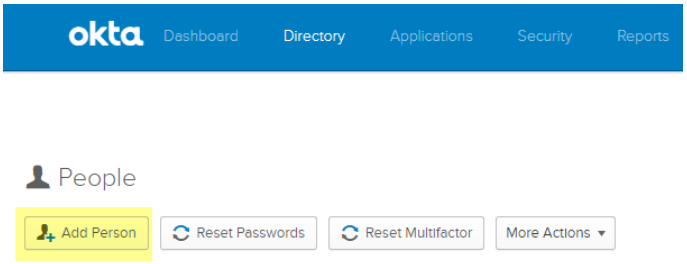
4. Seleccione el grupo que ha creado y, a continuación, seleccione **Manage Apps (Administrar aplicaciones)**.
5. Seleccione **Assign (Asignar)** para asignar la aplicación de Okta Verify que añadió en el paso 2.



6. Después de que la aplicación muestre **Assigned (Asignada)**, haga clic en **Done (Listo)**.
7. Repita este proceso para todos los grupos que usarán la aplicación de Okta Verify para MFA.

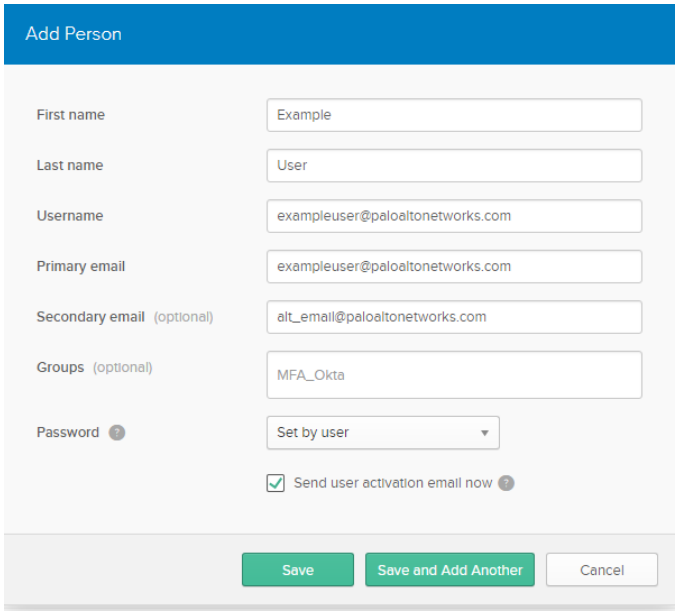
STEP 4 | Añada usuarios y asígnelos a un grupo.

1. Desde el panel de Okta, seleccione **Directory (Directorio)** > **People (Personas)** > **Add Person (Añadir persona)**.



2. Introduzca el nombre, apellido y nombre de usuario de la persona en **First Name (Nombre)**, **Last Name (Apellido)** y **Username (Nombre de usuario)**. El nombre de usuario debe coincidir con el **Primary email (Correo electrónico principal)**, que se completa de manera automática, y el nombre de usuario introducido en el cortafuegos. De manera opcional, puede introducir una dirección de correo electrónico alternativa para el usuario como **Secondary Email (Correo electrónico secundario)**.

© 2020 Palo Alto Networks, Inc.



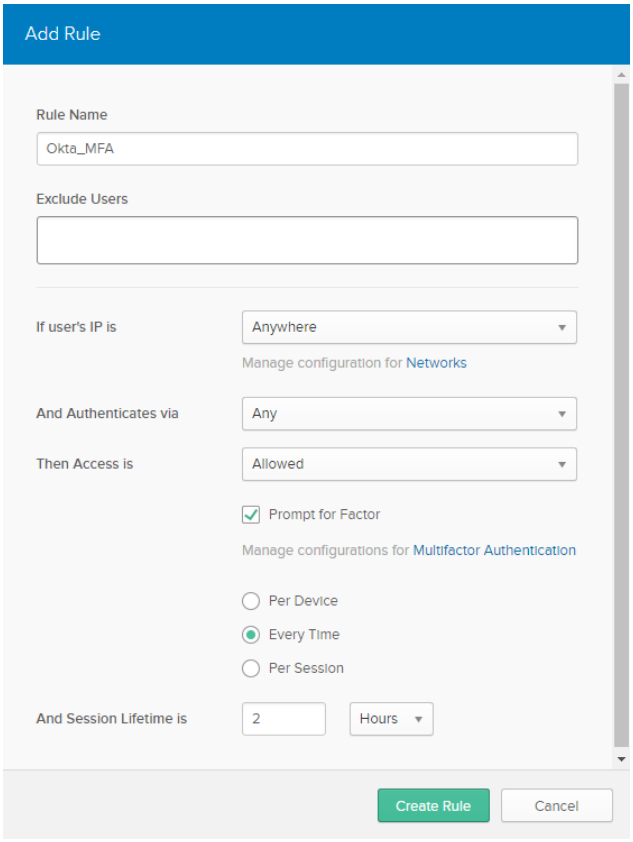
3. Introduzca el nombre del grupo o **Groups (Grupos)** para asociarlo con este usuario. Cuando comience a escribir, el nombre del grupo se completa automáticamente.
4. Marque **Send user activation email now (Enviar correo electrónico de activación de usuario ahora)**, luego seleccione **Save (Guardar)** para añadir un único usuario o **Save and Add Another (Guardar y añadir otro usuario)** para continuar añadiendo usuarios.

STEP 5 | Asigne una política de prueba a los usuarios.

1. Seleccione **Security (Seguridad)** > **Authentication (Autenticación)** > **Sign On (Inicio de sesión)**.

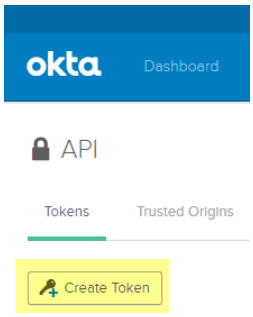
   Existe una **Default Policy (Política predeterminada)** con una **Default Rule (Regla predeterminada)** que no solicita a los usuarios que inicien sesión con MFA.
2. Introduzca el **Rule Name (Nombre de regla)** y marque **Prompt for Factor (Solicitar factor)** para aplicar la solicitud de MFA y seleccione el tipo de solicitud (**Per Device [Por dispositivo]**, **Every Time [Siempre]** o **Per Session [Por sesión]**), luego haga clic en **Create Rule (Crear regla)**.

© 2020 Palo Alto Networks, Inc.

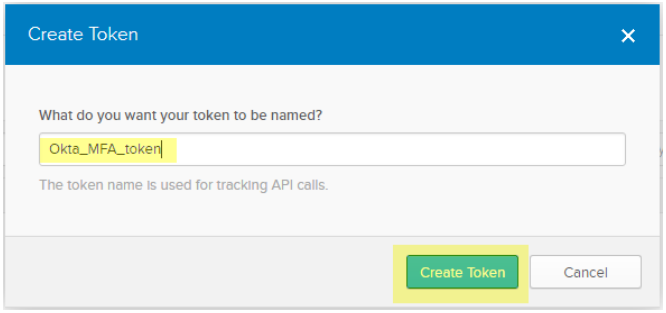


STEP 6 | Registre la información del token de autenticación de Okta en un lugar seguro porque solo se muestra una vez.

1. Seleccione **Security (Seguridad)** > **API** > **Tokens**.
2. Seleccione **Create Token (Crear token)**.



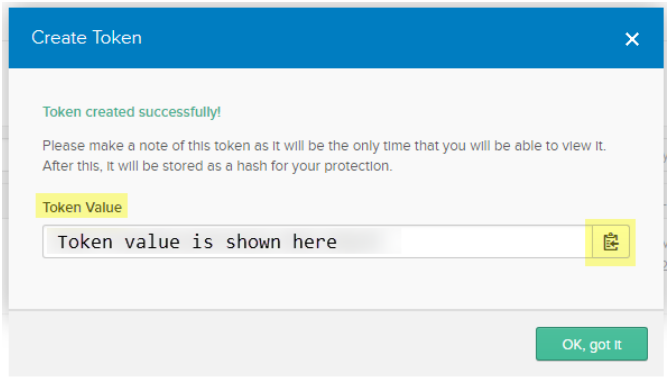
3. Introduzca el nombre del token, luego haga clic en **Create Token (Crear token)**.



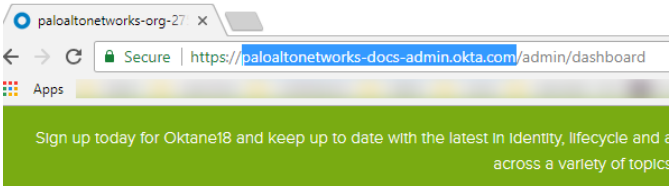
4. Copie el **Token Value (Valor de token)**.

© 2020 Palo Alto Networks, Inc.

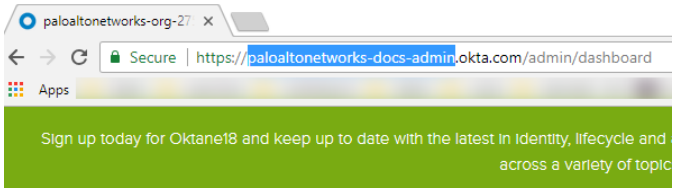
Puede hacer clic en el botón **Copy to clipboard (Copiar al portapapeles)** para copiar el valor del token en su portapapeles.



5. En la URL del panel del administrador de Okta, copie la parte de la URL después de **`https://`** hasta **`/admin`** para usarla como el **API host (Host de la API)**.



6. Omita el dominio **`okta.com`** de esta URL para usarlo como la **Organization (Organización)**.



Por ejemplo, en la URL del panel de administrador de Okta anterior, **`https://paloaltonetworks-doc-admin.okta.com/admin/dashboard`**:

- El nombre de host de la API es **`paloaltonetworks-doc-admin.okta.com`**.
- La organización es **`paloaltonetworks-doc-admin`**.

STEP 7 | Exporte todos los certificados en la cadena de certificados mediante la codificación Base-64:

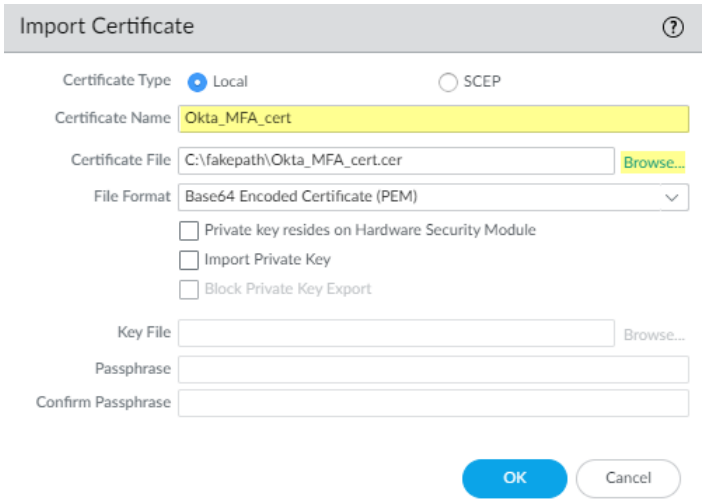
1. En función de su explorador, use uno de los siguientes métodos para exportar todos los certificados en la cadena.
   - **Chrome**: presione **`F12`**, luego seleccione **Security (Seguridad)** > **View Certificate (Ver certificado)** > **Details (Detalles)** > **Copy to File (Copiar al archivo)**.
   - **Firefox**: seleccione **Options (Opciones)** > **Privacy & Security (Privacidad y seguridad)** > **View Certificates (Ver certificados)** > **Export (Exportar)**.
   - **Internet Explorer**: seleccione **Settings (Configuración)** > **Internet Options (Opciones de Internet)** > **Content (Contenido)** > **Certificates (Certificados)** > **Export (Exportar)**.
2. Use el asistente de exportación de certificados para exportar todos los certificados en la cadena y seleccione **Base-64 encoded X.509 (Codificación X.509 de Base-64)** como el formato.

Configuración del cortafuegos para integrarse con Okta

Como requisito previo, confirme que asignó todos los usuarios que desea que se autentiquen con Okta.

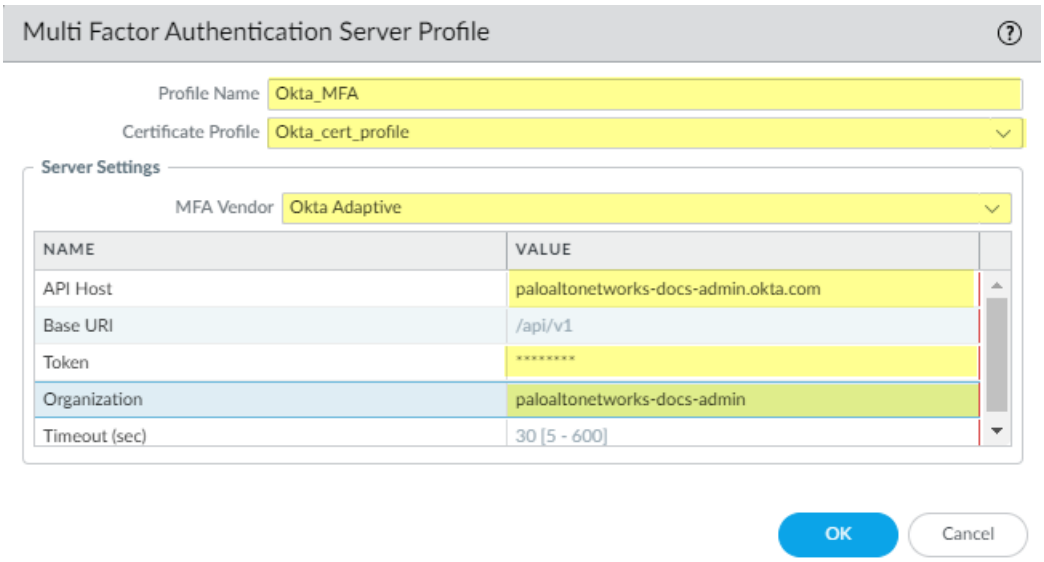
© 2020 Palo Alto Networks, Inc.

STEP 1 | Importe todos los certificados en la cadena de certificados en el cortafuegos y añada los certificados de CA importados (raíz e intermedio) a un perfil del certificado.



STEP 2 | Añada un **Multi Factor Authentication Server Profile (Perfil de servidor de autenticación multifactor)** para Okta.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Multi Factor Authentication (Autenticación multifactor)**.
2. Haga clic en **Add (Añadir)** para añadir un perfil de servidor de MFA.

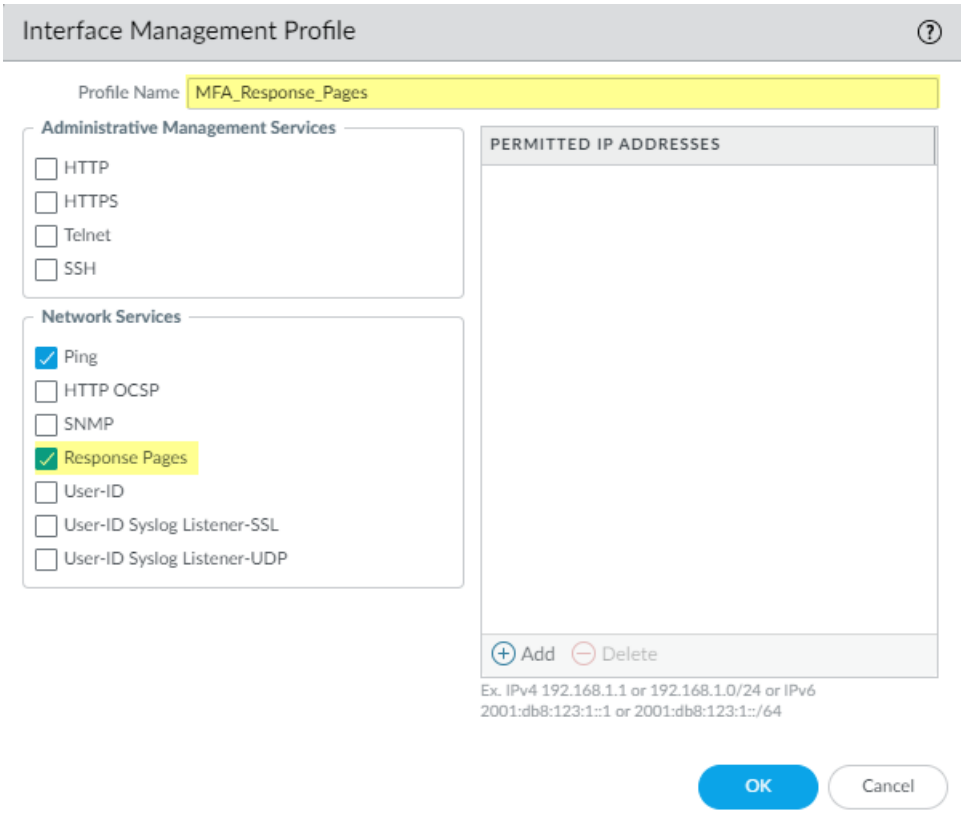


3. Introduzca un **Profile Name (Nombre de perfil)**.
4. Seleccione el **Certificate Profile (Perfil de certificado)** que creó en el paso 1 en Configuración del cortafuegos para integrarse con Okta.
5. Seleccione **Okta Adaptive** como el **MFA Vendor (Proveedor de MFA)**.
6. Introduzca el **API Host (Host de la API)**, **Token** y **Organization (Organización)** del paso 4 en Configuración del cortafuegos para integrarse con Okta.

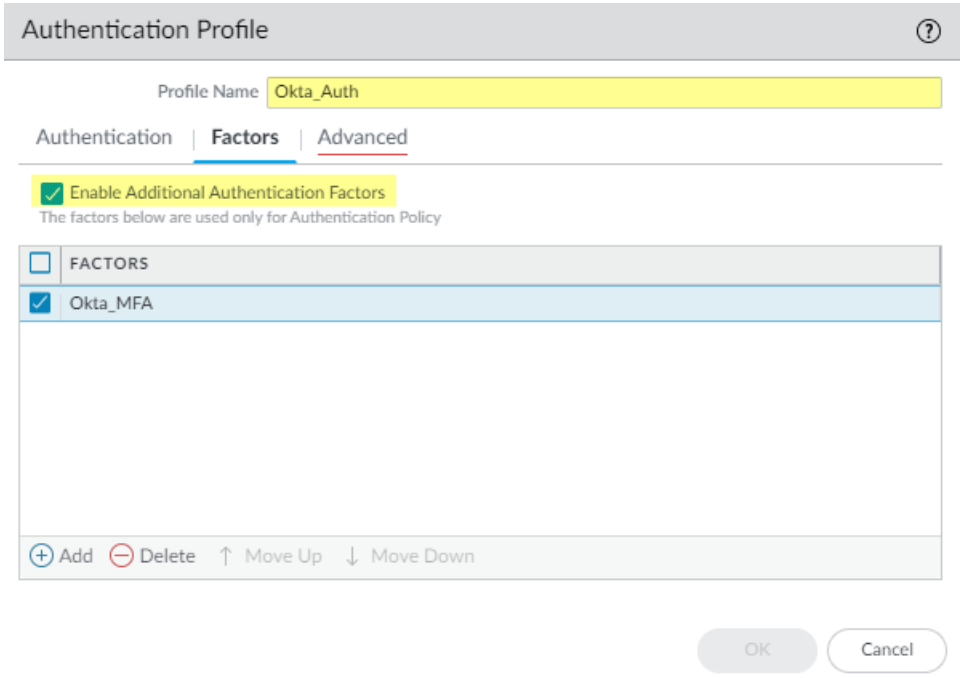
STEP 3 | Configure el portal de autenticación con **Redirect Mode (Modo de redireccionamiento)** para redirigir a los usuarios a la comprobación del proveedor de MFA.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Habilite las páginas de respuesta en el perfil de gestión de interfaces para redirigir a los usuarios a la comprobación de la página de respuesta.



STEP 5 | Cree un perfil de autenticación y añada el proveedor de MFA como un **Factor** (consulte la Configuración de autenticación multifactor del paso 3).



© 2020 Palo Alto Networks, Inc.

STEP 6 | Habilite el ID del usuario en la zona de origen para exigir a los usuarios identificados que respondan a la comprobación mediante el proveedor de MFA.

STEP 7 | Cree un objeto de ejecución de autenticación para usar el proveedor de MFA y crear una regla de política de autenticación (consulte Configuración de la política de autenticación, en los pasos 4 y 5).

STEP 8 | **Commit (Confirmar)** los cambios.

Verificación de MFA con Okta

STEP 1 | Verifique que los usuarios hayan recibido sus correos electrónicos de inscripción, activado sus cuentas y descargado la aplicación de Okta Verify en sus dispositivos.

STEP 2 | Visite el sitio web que mostrará la comprobación de la página de respuesta.



Si está usando un certificado autofirmado en lugar de un certificado asignado por PKI de su organización, se muestra una advertencia de seguridad en la que los usuarios deben hacer clic para acceder a la comprobación.

STEP 3 | Inicie sesión en la página de respuesta con las credenciales de Okta.

STEP 4 | Confirme que el dispositivo recibe la notificación push de la comprobación.

STEP 5 | Confirme que los usuarios puedan acceder correctamente a la página después de autenticar la comprobación aceptando la notificación push en sus dispositivos.

Configuración de la MFA entre Duo y el cortafuegos

La autenticación multifactor (Multi-factor authentication, MFA) le permite proteger los activos de la empresa utilizando varios factores para verificar la identidad de los usuarios antes de permitirles acceder a los recursos de la red. Existen varias formas de usar el servicio de gestión de identidad de Duo para realizar la autenticación con el cortafuegos:

- La autenticación de dos factores para los inicios de sesión de VPN con la puerta de enlace de GlobalProtect y un perfil de servidor RADIUS (admitido en PAN-OS 7.0 y versiones posteriores).
- La integración basada en la API con el portal de autenticación y un perfil de servidor de MFA (no requiere un proxy de autenticación de Duo o IdP de SAML; admitido en PAN-OS 8.0 y versiones posteriores).
- La integración de SAML para servidores locales (admitido en PAN-OS 8.0 y versiones posteriores).

Para permitir que MFA de SAML entre el cortafuegos y Duo asegure el acceso administrativo al cortafuegos:

- Configuración de Duo para MFA de SAML con la puerta de enlace de acceso de Duo
- Configuración del cortafuegos para integrarse con Duo
- Verificación de MFA con Duo

Configuración de Duo para MFA de SAML con la puerta de enlace de acceso de Duo

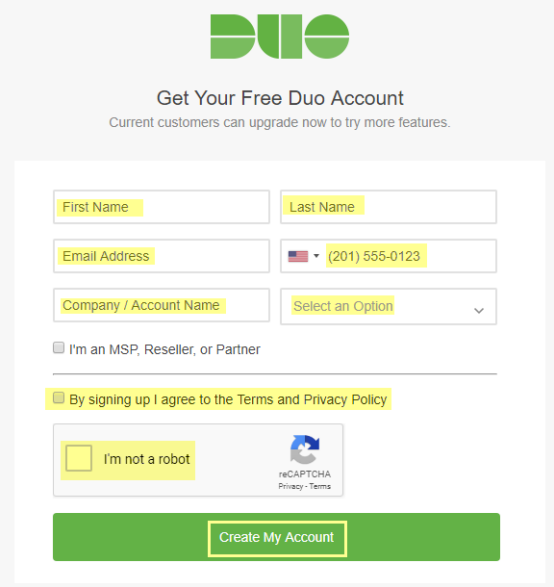
Antes de comenzar, verifique que implementó la puerta de enlace de acceso de Duo (Duo Access Gateway, DAG) en un servidor local en su zona de DMZ.

© 2020 Palo Alto Networks, Inc.

Cree su cuenta de administrador de Duo y configure la puerta de enlace de acceso de Duo para autenticar a sus usuarios antes de que puedan acceder a los recursos.

STEP 1 | Cree su cuenta de administrador de Duo.

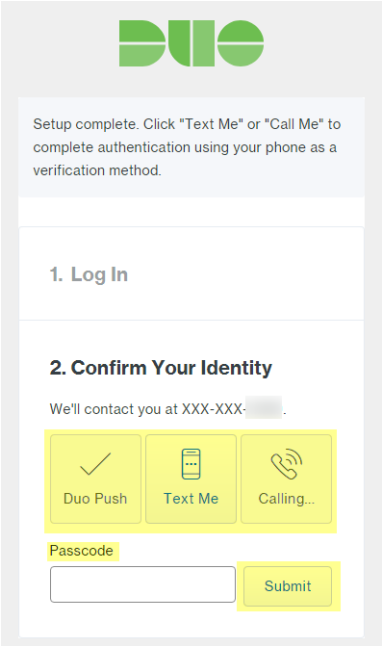
1. En la página de creación de cuenta de Duo, introduzca **First Name (Nombre)**, **Last Name (Apellido)**, **Email Address (Dirección de correo electrónico)**, **Cell Phone Number (Número de móvil)**, **Company / Account Name (Nombre de la empresa/cuenta)** y seleccione la cantidad de empleados de la organización.
2. Acepte las condiciones y la política de privacidad y responda a la comprobación reCAPTCHA en **Create My Account (Crear mi cuenta)**.



STEP 2 | Verifique su cuenta de administrador de Duo.

1. Seleccione el método de verificación de autenticación (**Duo Push [Notificación push de Duo]**, **Text Me [Mensaje de texto]** o **Calling... [Llamada]**).
2. Introduzca el **Passcode (Código de acceso)** que recibe y haga clic en **Submit (Enviar)** para verificar su cuenta.

© 2020 Palo Alto Networks, Inc.

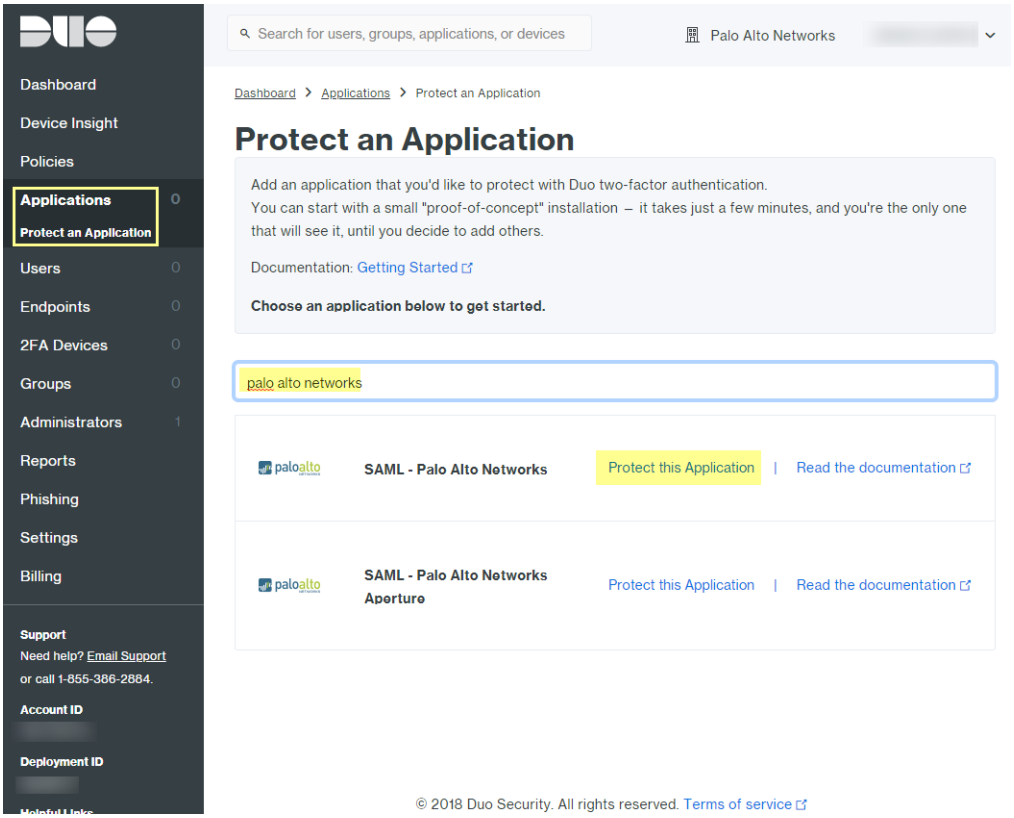


STEP 3 | Configure el servicio de Duo para SAML.

Después de crear su configuración, descargue el archivo de configuración en la parte superior de la página.

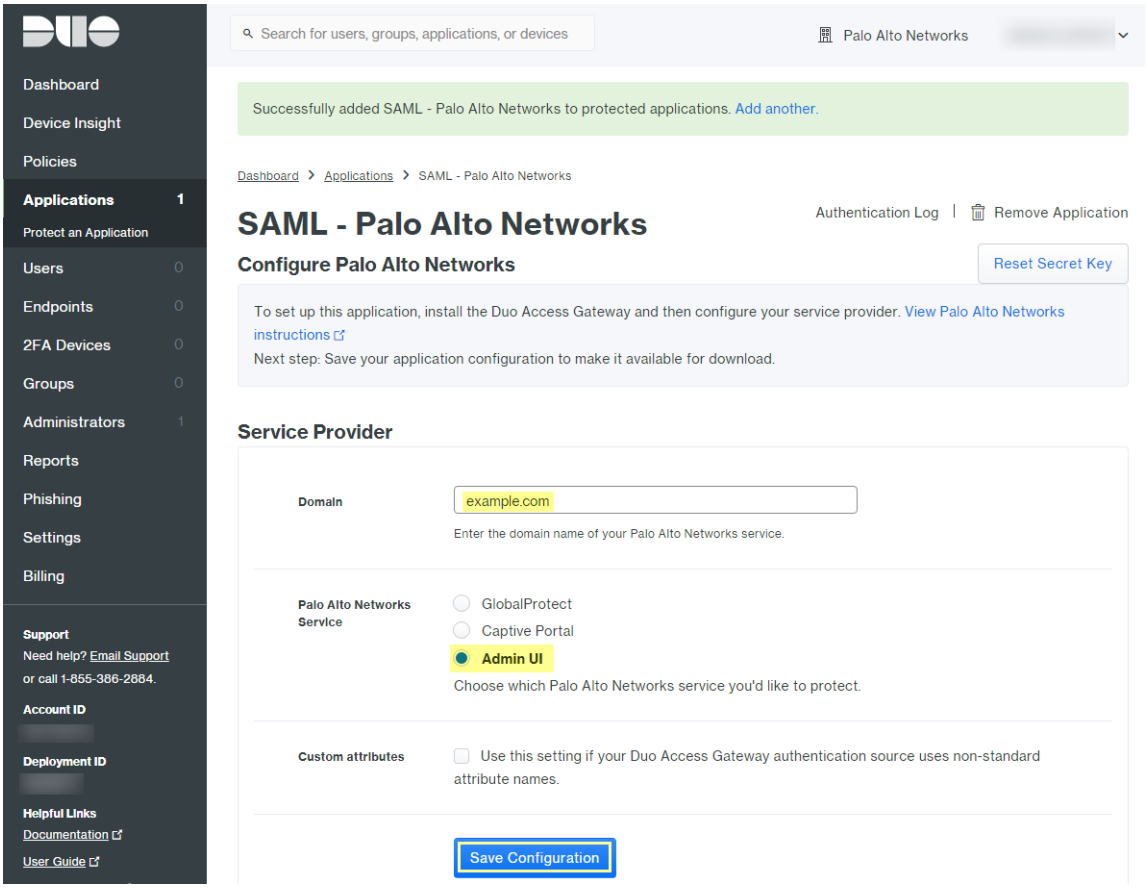
1. En el panel de administrador de Duo, seleccione **Applications (Aplicaciones)** > **Protect an Application (Proteger una aplicación)**.
2. Introduzca **`Palo Alto Networks`** para buscar aplicaciones.
3. Localice **SAML - Palo Alto Networks** en la lista de resultados, luego seleccione **Protect this Application (Proteger esta aplicación)**.

© 2020 Palo Alto Networks, Inc.



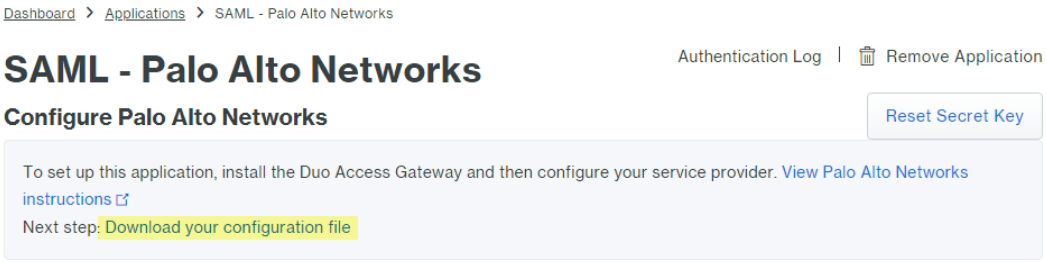
4. Introduzca el **Domain (Dominio)**.
5. Seleccione **Admin UI (IU de administrador)** como el **Palo Alto Networks Service (Servicio de Palo Alto Networks)**.
6. Configure su **Policy (Política)** y otra **Settings (Configuración)**, y haga clic en **Save Configuration (Guardar cambios)**.

© 2020 Palo Alto Networks, Inc.



7. Seleccione **Download your configuration file (Descargar su archivo de configuración)**.

   El enlace para descargar el archivo se encuentra en la parte superior de la página.



STEP 4 | Suba el archivo de configuración a la Puerta de enlace de acceso de Duo (Duo Access Gateway, DAG).

1. En la consola de administrador de DAG, seleccione **Applications (Aplicaciones)**.
2. Haga clic en **Choose File (Elegir archivo)** y seleccione el archivo de configuración que descargó, luego haga clic en **Upload (Subir)** para subirlo.
3. En **Settings (Configuración)** > **Session Management (Gestión de la sesión)**, deshabilite **User agent binding (Vinculación de agente y usuario)**, y luego haga clic en **Save Settings (Guardar configuración)**.

STEP 5 | En la consola de administrador de DAG, configure el servidor de Active Directory u OpenLDAP como el origen de la autenticación y descargue el archivo de metadatos.

1. Inicie sesión en la consola de administrador de DAG.

© 2020 Palo Alto Networks, Inc.

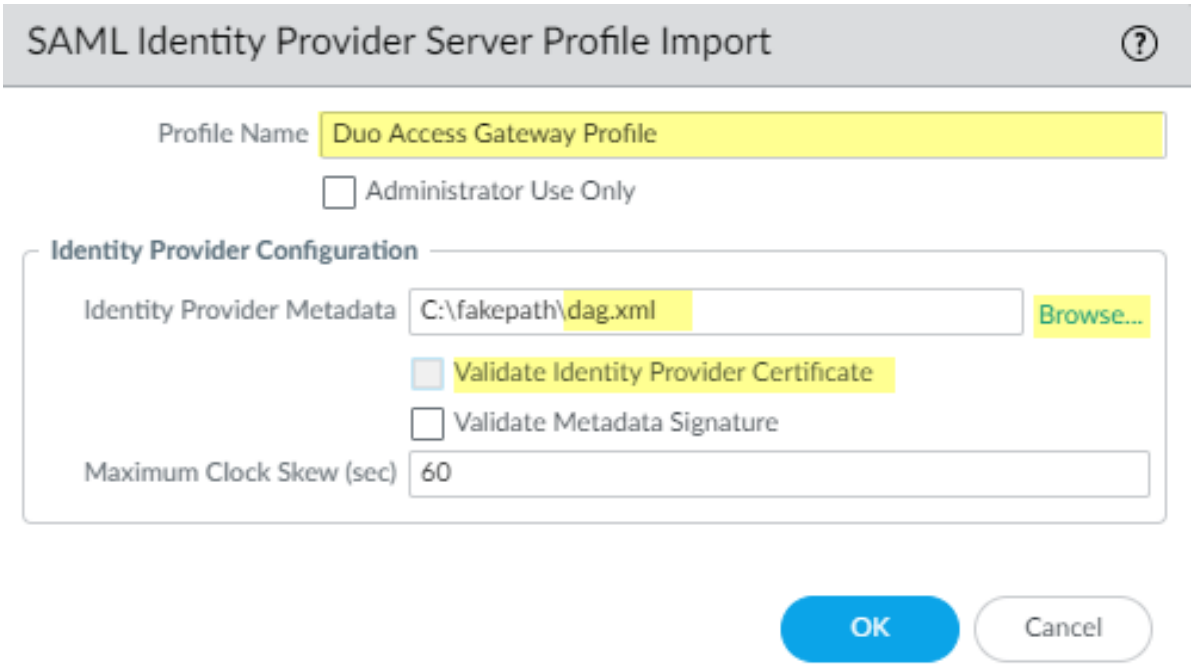
2. En **Authentication Source (Origen de autenticación)** > **Set Active Source (Configurar origen activo)**, seleccione el **Source type (Tipo de origen)** (Active Directory u OpenLDAP) y haga clic en **Set Active Source (Configurar origen activo)**.
3. En **Configure Sources (Configurar orígenes)**, introduzca los **Attributes (Atributos)**.
   - Para Active Directory, introduzca `mail,sAMAccountName,userPrincipalName,objectGUID`.
   - Para OpenLDAP, introduzca `mail,uid`.
   - Para los atributos personalizados, adjúntelos al final de la lista y separe cada atributo con una coma. No elimine ningún atributo existente.
4. Haga clic en **Save Settings (Guardar configuración)** para guardar la configuración.
5. Seleccione **Applications (Aplicaciones)** > **Metadata (Metadatos)**, y luego haga clic en **Download XML metadata (Descargar metadatos XML)** para descargar los metadatos XML que deberá importar al cortafuegos.

   El archivo se nombrará dag.xml. Debido a que este archivo incluye información confidencial para autenticar su cuenta de Duo con el cortafuegos, asegúrese de conservarlo en un lugar seguro para evitar el riesgo de comprometer la información.

Configuración del cortafuegos para integrarse con Duo

STEP 1 | Importe los metadatos de Duo.

1. Inicie sesión en la interfaz web del cortafuegos.
2. En el cortafuegos, seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles del servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)** > **Import (Importar)**.
3. Introduzca el **Profile Name (Nombre de perfil)**.
4. Seleccione **Browse (Examinar)** para buscar el archivo de **Identity Provider Metadata (Metadatos de proveedor de identidad)** (**dag.xml**).
5. Si Duo Access Gateway proporciona un certificado autofirmado como certificado de firma para el IdP, no puede **validar el certificado de proveedor de identidad**. En este caso, asegúrese utilizar PAN-OS 10.0 para reducir la exposición a CVE-2020-2021.

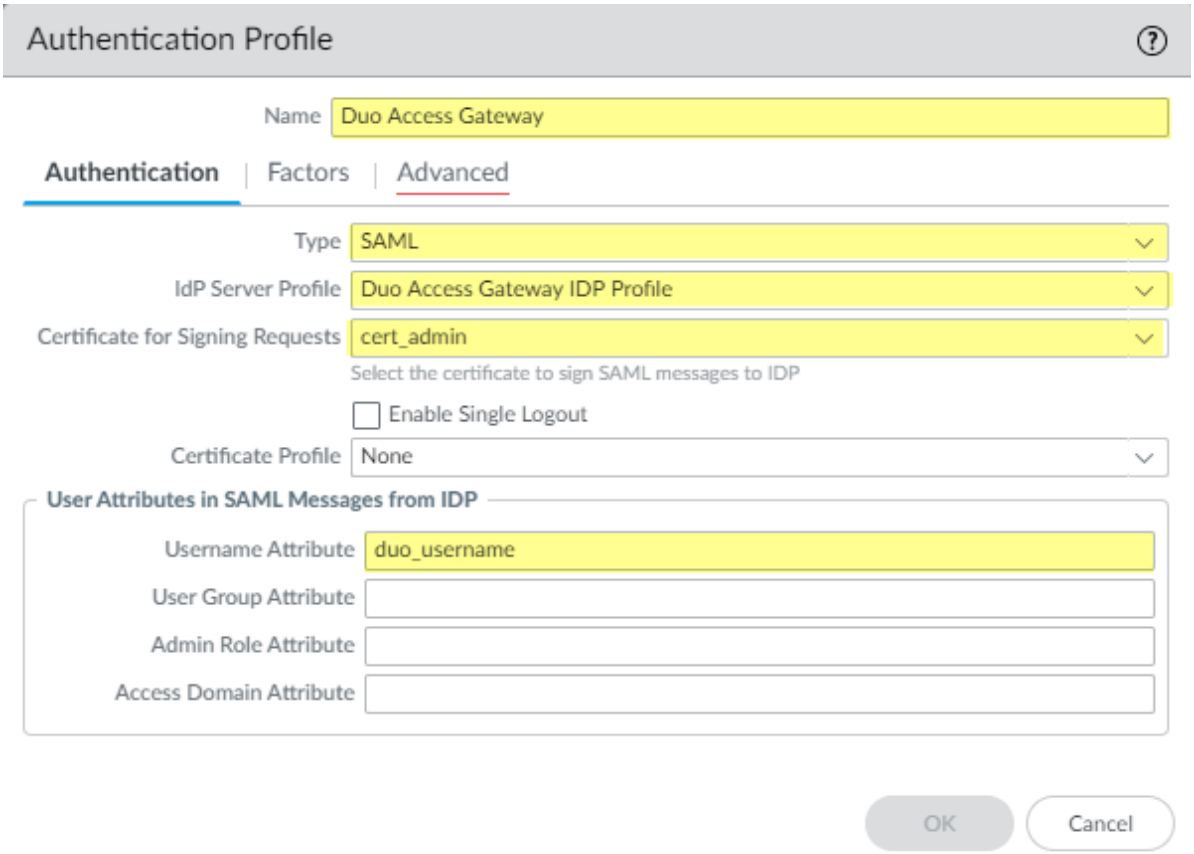


© 2020 Palo Alto Networks, Inc.

STEP 2 | Añada un perfil de autenticación.

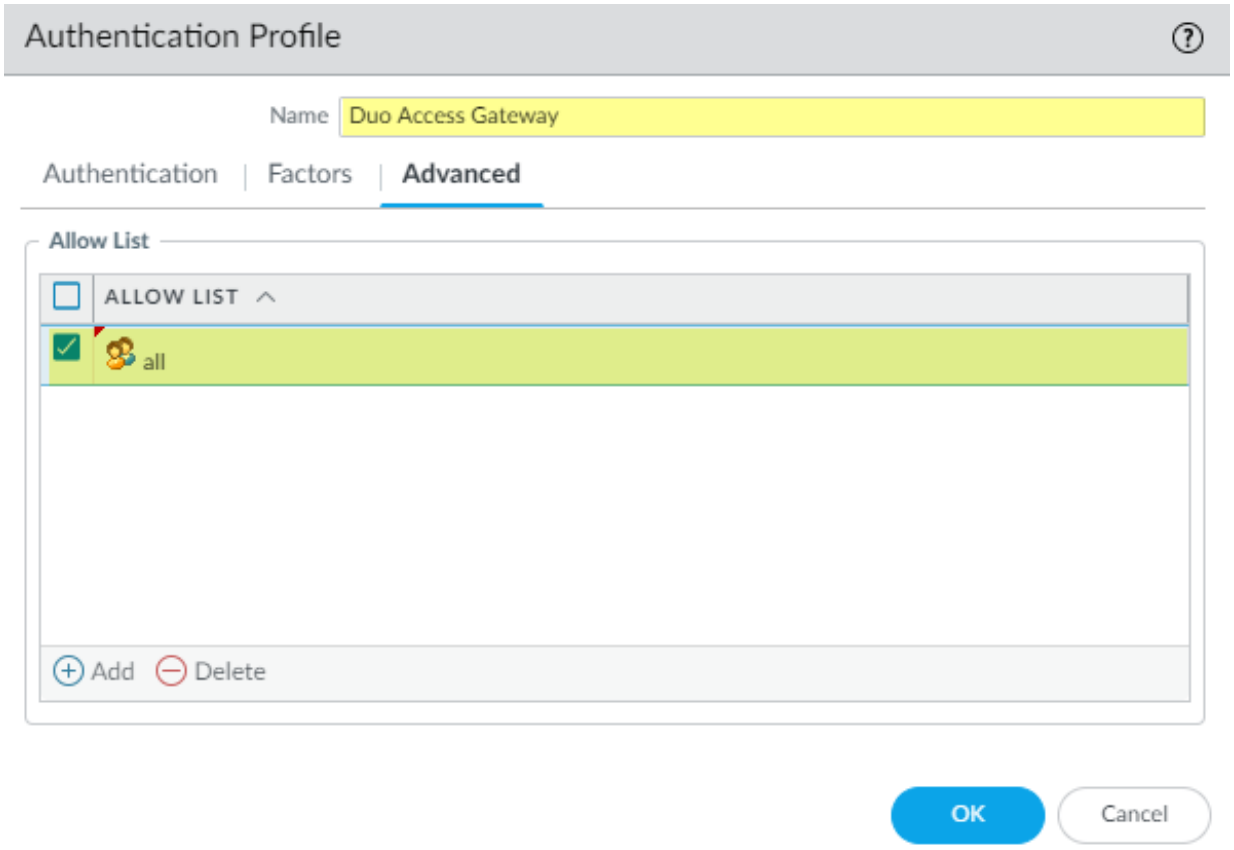
El perfil de autenticación permite que Duo sea el proveedor de identidad que valida las credenciales de inicio de sesión del administrador.

1. Haga clic en **Add (Añadir)** para añadir un **Authentication Profile (Perfil de autenticación)**.
2. Introduzca el **Name (Nombre)** del perfil.
3. Seleccione **SAML** como el tipo de autenticación en **Type (Tipo)**.
4. Seleccione **Duo Access Gateway Profile (Perfil de puerta de enlace de acceso de DUo)** como el **IdP Server Profile (Perfil de servidor IdP)**.
5. Seleccione el certificado que desea usar para la comunicación SAML con la puerta de enlace de acceso de Duo para el **Certificate for Signing Requests (Certificado para solicitudes de firma)**.
6. Introduzca **`user.username`** como el **Username Attribute (Atributo de nombre de usuario)**.



7. Seleccione **Advanced (Avanzado)** para añadir una lista de permisos en **Add (Añadir)**.
8. Seleccione **all (todos)** y luego haga clic en **OK (Aceptar)**.
9. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

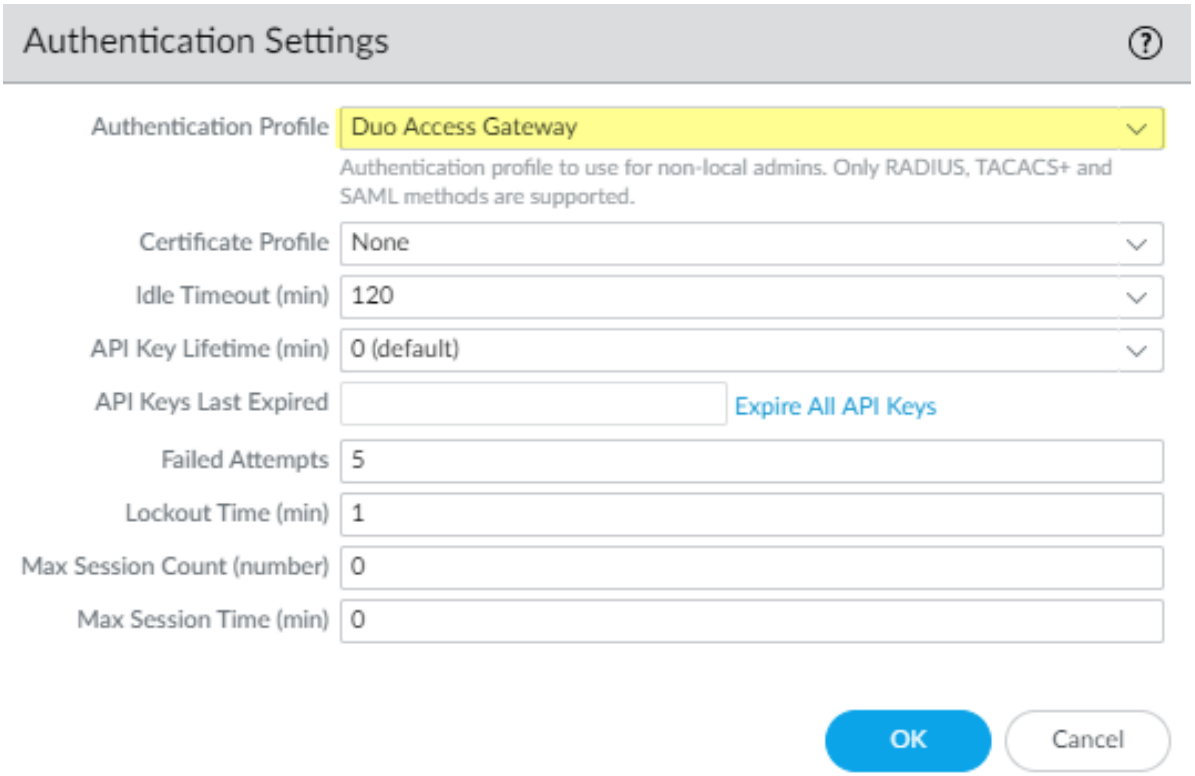
© 2020 Palo Alto Networks, Inc.



STEP 3 | Especifique la configuración de autenticación que usa el cortafuegos para la autenticación SAML con Duo.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite los ajustes de **Authentication Settings (Configuración de autenticación)**.
2. Seleccione **Duo Access Gateway (Puerta de enlace de acceso de Duo)** como el **Authentication Profile (Perfil de autenticación)** y, luego, haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

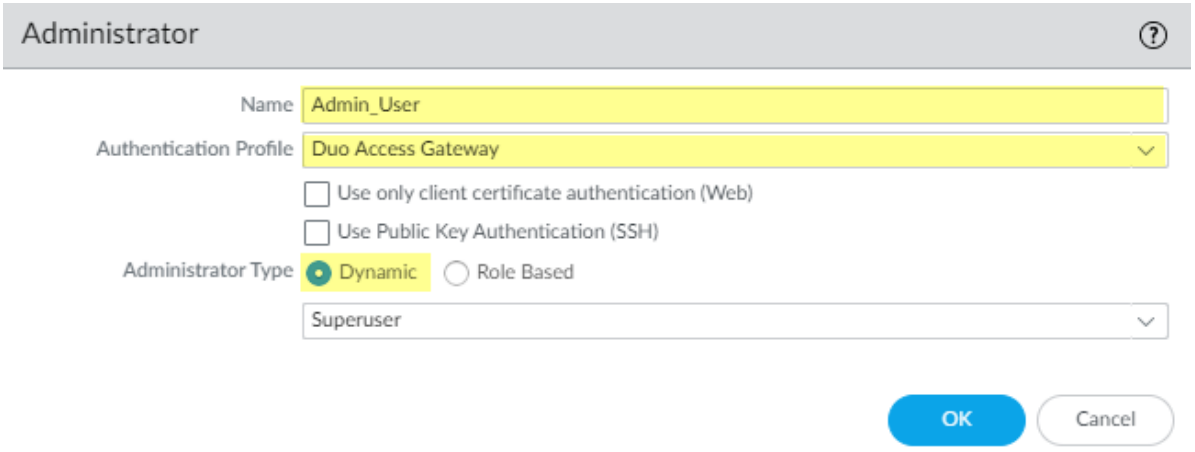


3. **Commit (Confirmar)** los cambios.

STEP 4 | Añada cuentas para los administradores que se autenticarán en el cortafuegos con Duo.

1. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)** y **Add (Añadir)** para añadir una cuenta.
2. Introduzca un nombre de usuario en **Name**.
3. Seleccione **Duo Access Gateway (Puerta de enlace de acceso de Duo)** como el **Authentication Profile (Perfil de autenticación)**.
4. Seleccione **Administrator Type (Tipo de administrador)** y, a continuación, haga clic en **OK (Aceptar)**.

   Seleccione **Role Based (Basado en la función)** si desea usar una función personalizada para el usuario. De lo contrario, seleccione **Dynamic (Dinámico)**. Para solicitar que los administradores inicien sesión mediante SSO con Duo, asigne el perfil de autenticación a todos los administradores actuales.



© 2020 Palo Alto Networks, Inc.

Verificación de MFA con Duo

STEP 1 | Inicie sesión en la interfaz web del cortafuegos.

STEP 2 | Configure **Use Single Sign-on (Usar inicio de sesión único)** y haga clic en **Continue (Continuar)**.

STEP 3 | Introduzca las credenciales de inicio de sesión en la página de inicio de sesión de la puerta de enlace de acceso de Duo.

STEP 4 | Seleccione un método de autenticación (notificación push, llamada telefónica o código de acceso).

Cuando se autentique correctamente, se le redirigirá a la interfaz web del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación SAML

Para configurar el inicio de sesión único (single sign-on, SSO) de SAML y el cierre de sesión único (single logout, SLO), debe registrar el cortafuegos y el IdP entre sí para habilitar la comunicación entre ellos. Si el IdP proporciona un archivo de metadatos que contiene información de registro, usted puede importarlo en el cortafuegos para registrar el IdP y crear un perfil de servidor IdP. El perfil de servidor define cómo conectarse con el IdP y especifica el certificado que el IdP utiliza para firmar los mensajes de SAML. También puede usar un certificado para que el cortafuegos firme los mensajes de SAML. El uso de certificados es un requisito para garantizar las comunicaciones entre el cortafuegos y el IdP.

Palo Alto Networks requiere HTTPS para garantizar la confidencialidad de todas las transacciones SAML en lugar de enfoques alternativos, como aserciones SAML cifradas. Para garantizar la integridad de todos los mensajes procesados en una transacción SAML, Palo Alto Networks recomienda fehacientemente solicitar certificados digitales para firmar todos los mensajes criptográficamente.

El siguiente procedimiento describe cómo configurar la autenticación SAML para usuarios finales y administradores de cortafuegos. También puede configurar la autenticación SAML para los administradores de Panorama.



El SSO está disponible para los administradores y para los usuarios finales de GlobalProtect y el portal de autenticación. El SLO está disponible para los administradores y los usuarios finales de GlobalProtect, pero no para los usuarios finales del portal de autenticación.

Los administradores pueden utilizar SAML para autenticarse en la interfaz web del cortafuegos, pero no en la CLI.

STEP 1 | Obtenga los certificados que el IdP y el cortafuegos utilizarán para firmar los mensajes de SAML.

Si los certificados no especifican atributos de uso clave, todos los usos se permitirán de manera predeterminada, incluidos los mensajes de firmas. En este caso, usted puede obtener certificados mediante cualquier método.

Si el certificado especifica atributos de uso de clave, uno de los atributos debe ser la firma digital, que no está disponible en los certificados que usted genera en el cortafuegos o en Panorama. En este caso, debe importar los certificados:

- **Certificado que el cortafuegos utiliza para firmar mensajes de SAML:** importe el certificado desde la autoridad de certificados (certificate authority, CA) de su empresa o una CA de terceros.
- **Certificado que el IdP utiliza para firmar mensajes de SAML** (obligatorio para todas las implementaciones): importe un archivos de metadatos que contenga el certificado del IdP (consulte el paso a continuación). El certificado de IdP se limita a los siguientes algoritmos:

  Public key algorithms (Algoritmos de clave pública): RSA (1.024 bits o mayor) y ECDSA (todos los tamaños). Un cortafuegos en modo FIPS / CC admite RSA (2.048 bits o más) y ECDSA (todos los tamaños).

  Signature algorithms (Algoritmos de firma): SHA1, SHA256, SHA384 y SHA512. Un cortafuegos en modo FIPS / CC soporta SHA256, SHA384 y SHA512.

STEP 2 | Añada un perfil de servidor SAML IdP.

El perfil de servidor registra el IdP en el cortafuegos y define cómo se conectan.

© 2020 Palo Alto Networks, Inc.

En este ejemplo, usted importa un archivos de metadatos de SAML desde el IdP, de manera que el cortafuegos puede crear automáticamente un perfil de servidor y completar la información de conexión, registro y certificado de IdP.



Si el IdP no proporciona un archivo de metadatos, seleccione Device (Dispositivo) > Server Profiles (Perfiles de servidor) > SAML Identity Provider (Proveedor de identidad de SAML) y Add (Añadir) para añadir el perfil de servidor, e ingrese manualmente la información (consulte a su administrador de IdP para obtener los valores).

1. Exporte el archivo de metadatos de SAML desde el IdP a un sistema cliente desde el que pueda cargar los metadatos en el cortafuegos.

   El certificado especificado en el archivo debe reunir los requisitos enumerados en el paso anterior. Consulte su documentación de IdP para obtener instrucciones sobre cómo exportar el archivo.
2. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **SAML Identity Provider (Proveedor de identidad SAML)** en Panorama™ e **importe** el archivo de metadatos en el cortafuegos.
3. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
4. Seleccione **Browse (Examinar)** para buscar el archivo de **Identity Provider Metadata (Metadatos de proveedor de identidad)**.
5. Seleccione **Validate Identity Provider Certificate (Validar certificado de proveedor de identidad)** (predeterminado) para validar la cadena de confianza y, opcionalmente, el estado de la revocación del certificado IdP.

   Para habilitar esta opción, una entidad de certificación (Certificate Authority, CA) debe emitir el certificado de firma de su IdP. Debe crear un perfil del certificado que tenga la CA que emitió el certificado de firma del IdP. En el perfil de autenticación, seleccione el perfil de servidor SAML y el perfil del certificado para validar el certificado IdP.

   Si su certificado de firma IdP es un certificado autofirmado, no hay cadena de confianza; como resultado, no puede habilitar esta opción. El cortafuegos siempre valida la firma de las respuestas o aserciones de SAML con el certificado de proveedor de identidad que configure, tanto si habilita como si no la opción **Validar Certificado de Proveedor de Identidad)**. Si su IdP proporciona un certificado autofirmado, asegúrese de que está utilizando PAN-OS 10.0 para reducir la exposición a CVE-2020-2021.

   Valide el certificado para verificar que no se ha visto comprometido y para reforzar la seguridad.
6. Ingrese el **Maximum Clock Skew (Desplazamiento de reloj máximo)**, que es la diferencia permitida en segundos entre los tiempos del sistema del IdP y el cortafuegos al momento en que el cortafuegos valida los mensajes de IdP (el valor predeterminado es 60; el intervalo es de 1 a 900). Si la diferencia supera este valor, la autenticación falla.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.
8. Haga clic en el nombre del perfil de servidor para que aparezcan los ajustes del perfil. Verifique que la información importada sea correcta y modifíquela si fuera necesario.
9. Tanto si importa los metadatos de IdP como si especifica manualmente la información de IdP, asegúrese siempre de que el certificado de firma de su proveedor de identidad de SAML sea el **certificado de proveedor de identidad** para su perfil de servidor y que su IdP envíe respuestas y aserciones de SAML firmadas, o ambas.

STEP 3 | Configure un perfil de autenticación.

El perfil define los ajustes de autenticación que son comunes a un conjunto de usuarios.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Configure el **Type (Tipo)** en **SAML**.
4. Seleccione el **IdP Server Profile (Perfil de servidor IdP)** que configuró.
5. Seleccione el **Certificate for Signing Requests (Certificado para las solicitudes de firma)**.

   El cortafuegos utiliza este certificado para firmar mensajes que envía al IdP. Puede importar un certificado generado por su CA de la empresa o puede generar un certificado mediante la CA raíz que se generó en el cortafuegos o Panorama.
6. (Opcional) **Enable Single Logout (Habilitar cierre de sesión único)** (está inhabilitado de manera predeterminada).
7. Seleccione el **Certificate Profile (Perfil de certificado)** que el cortafuegos utilizará para validar el **Identity Provider Certificate (Certificado de proveedor de identidad)**.
8. Ingrese el **Username Attribute (Atributo de nombre de usuario)** que los mensajes de IdP utilizan para identificar a los usuarios (el valor predeterminado es **`username [nombre de usuario]`**).

   *Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba **`superreader (superlector)`**, no **`SuperReader (SuperLector)`**. Si gestiona la autorización de administrador en el almacén de identidades, especifique el Admin Role Attribute (Atributo de rol de administrador) y también el Access Domain Attribute (Atributo de dominio de acceso).*
9. Seleccione **Advanced (Avanzado)** y haga clic en **Add (Añadir)** para añadir los usuarios y grupos que pueden autenticarse con este perfil de autenticación.
10. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 4 | Asigne el perfil de autenticación a las aplicaciones de cortafuegos que requieren autenticación.

1. Asigne el perfil de autenticación a lo siguiente:
   - Cuentas de administrador que usted gestiona a nivel local en el cortafuegos. En este ejemplo, configure una cuenta de administrador de cortafuegos antes de verificar la configuración de SAML posteriormente en este procedimiento.
   - Las cuentas de administrador que usted gestiona externamente en el almacén de identidades de IdP. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, modifique los ajustes de autenticación y seleccione el **Authentication Profile (Perfil de autenticación)** que configuró.
   - Las reglas de política de autenticación que aseguran los servicios y aplicaciones a los que los usuarios finales acceden a través del portal de autenticación. Consulte Configuración de la política de autenticación.
   - Portales y puertas de enlace de GlobalProtect a los que acceden los usuarios finales.
2. **Commit (Confirmar)** los cambios.

   El cortafuegos valida el **Identity Provider Certificate (Certificado de proveedor de identidad)** que usted asignó al perfil de servidor IdP SAML.

STEP 5 | Cree un archivo de metadatos SAML para registrar la aplicación del cortafuegos (acceso de gestión, portal de autenticación o GlobalProtect) en el IdP.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y, en la columna Authentication (Autenticación) del perfil de autenticación que configuró, haga clic en **Metadata (Metadatos)**.
2. En la lista desplegable **Service (Servicio)**, seleccione la aplicación que desee registrar:
   - **management (gestión)** (predeterminado): proporciona acceso de administrador a la interfaz web.

© 2020 Palo Alto Networks, Inc.

- **authentication-portal**: acceso de usuario final a servicios y aplicaciones a través del portal de autenticación.
- **global-protect**: proporciona acceso al usuario final para los servicios y aplicaciones a través de GlobalProtect.

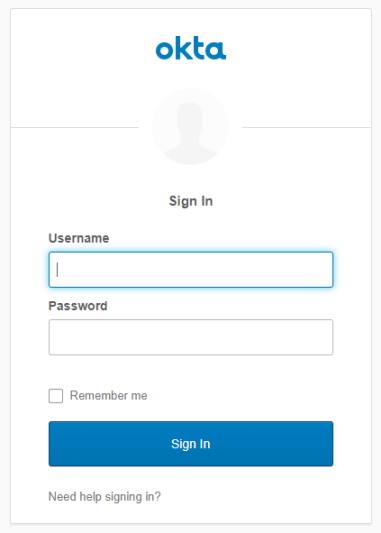
3. (Portal de autenticación o GlobalProtect únicamente) para el **Vsysname Combo (Combinación de nombre de sistema virtual)**, seleccione el sistema virtual en el que están definidos los ajustes del portal de autenticación o el portal de GlobalProtect.
4. Ingrese la interfaz, la dirección IP o el nombre de host según la aplicación que registrará:
   - **management (gestión)**: para **Management Choice (Opción de gestión)**, seleccione **Interface (Interfaz)** (predeterminado) y seleccione una interfaz que esté habilitada para el acceso de gestión a la interfaz web. La selección predeterminada es la dirección IP de la interfaz MGT.
   - **authentication-portal**: para el **IP Hostname (Nombre de host IP)**, ingrese la dirección IP o el nombre de host del **Redirect Host (Host de redireccionamiento)** (consulte **Device [Dispositivo]** > **User Identification [Identificación de usuario]** > **Authentication Portal Settings [Configuración del portal de autenticación]**).
   - **global-protect**: para el **IP Hostname (Nombre de host IP)**, ingrese el nombre de host o dirección IP del portal o la puerta de enlace de GlobalProtect.
5. Haga clic en **OK (Aceptar)** y guarde el archivo de metadatos en su sistema cliente.
6. Importe el archivo de metadatos en el servidor de IdP para registrar la aplicación del cortafuegos. Consulte la documentación del IdP para obtener instrucciones.

STEP 6 | Verifique que los usuarios puedan autenticarse usando el SSO de SAML.

Por ejemplo, para verificar que SAML funcione para el acceso a la interfaz web usando una cuenta de administrador local:

1. Vaya a la URL de la interfaz web del cortafuegos.
2. Haga clic en **Use Single Sign-On (Usar inicio de sesión único)**.
3. Ingrese el nombre de usuario del administrador.
4. Haga clic en **Continue (Continuar)**.

   El cortafuegos lo redirigirá para autenticarse en el IdP, que muestra una página de inicio de sesión. Por ejemplo:



5. Inicie sesión usando su nombre de usuario y contraseña de SSO.

   Una vez autenticado correctamente en el IdP, será redirigido nuevamente al cortafuegos, que mostrará la interfaz web.

© 2020 Palo Alto Networks, Inc.

6. Utilice su cuenta de administrador de cortafuegos para solicitar acceso a otra aplicación de SSO.
   El acceso correcto indica que la autenticación de SSO SAML se realizó correctamente.

© 2020 Palo Alto Networks, Inc.

Configuración de un inicio de sesión único de Kerberos

Panorama y los cortafuegos de Palo Alto Networks admiten el inicio de sesión único (single sign-on, SSO) de Kerberos 5 para autenticar a los administradores en la interfaz web y a los usuarios finales en el portal de autenticación. Si el SSO de Kerberos está habilitado, el usuario solo debe iniciar sesión durante el acceso inicial a su red (como iniciar sesión en Microsoft Windows). Tras este inicio de sesión inicial, el usuario podrá acceder a cualquier servicio basado en el explorador de la red (por ejemplo, la interfaz web del cortafuegos) sin tener que iniciar sesión de nuevo hasta que venza la sesión con SSO.

STEP 1 | Cree un keytab de Kerberos.

El keytab es un archivo que contiene el nombre y la contraseña principales del cortafuegos, y es necesario para el proceso de SSO. Cuando configura Kerberos en el perfil y la secuencia de autenticación, el cortafuegos busca en primer lugar un nombre de host de SSO de Kerberos. Si proporciona un nombre de host, el cortafuegos busca en los keytab un nombre principal de servicio que coincida con dicho nombre y utiliza solo ese keytab para el descifrado. Si no proporciona ningún nombre de host, el cortafuegos prueba cada keytab de la secuencia de autenticación hasta que se logre la correcta autenticación con Kerberos.

Si el nombre de host de SSO de Kerberos se incluye en la solicitud enviada al cortafuegos, el nombre de host debe coincidir con el nombre principal del servicio del keytab; de lo contrario, la solicitud de autenticación de Kerberos no se envía.

1. Inicie sesión en el servidor de Active Directory y abra un símbolo del sistema.
2. Especifique el siguiente comando para registrar el nombre principal del servicio (Service Principal Name, SPN) para GlobalProtect o el portal de autenticación, donde <*portal_fqdn*> y <*service_account_username*> son variables.

   setspn -s HTTP/<*portal_fqdn*> <*service_account_username*>
3. Cree una cuenta de Kerberos para el cortafuegos. Consulte la documentación de Kerberos para obtener información sobre los pasos.
4. Inicie sesión en el KDC y abra una línea de comandos.
5. Especifique el siguiente comando, donde <*portal_fqdn*>, <*kerberos_realm*>, <*netbios_name*>, <*service_account_username*>, <*password*>, <*filename*> y <*algorithm*> son variables.

   ktpass /princ HTTP <*portal_fqdn*>@<*kerberos_realm*> /mapuser <*netbios_name*>\<*service_account_username*> /pass <*password*>/out <*filename*>.keytab /ptype KRB5_NT_PRINCIPAL /crypto <*algorithm*>

   *El valor <kerberos_realm> debe estar en mayúsculas (por ejemplo, especifique **AD1.EXAMPLE.COM**, no **ad1.example.com**).*

   *Si el cortafuegos está en modo FIPS/CC, el algoritmo debe ser **aes128-cts-hmac-sha1-96** o **aes256-cts-hmac-sha1-96**. De lo contrario, puede usar también des3-cbc-sha1 o arcfour-hmac. Para utilizar un algoritmo Advanced Encryption Standard (estándar de cifrado avanzado, AES), el nivel funcional del KDC debe ser Windows Server 2012 o posterior y debe habilitar el cifrado AES para la cuenta del cortafuegos.*

   El algoritmo del keytab tiene que coincidir con el algoritmo del ticket de servicio que el TGS (servicio de concesión de vales) emite a los clientes. Su administrador de Kerberos determina qué algoritmos usan los tickets de servicio.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Realice la Configuración de una secuencia y perfil de autenticación para definir la configuración de Kerberos y otras opciones de autenticación que son comunes a un conjunto de usuarios.

- Introduzca el **dominio de Kerberos** (normalmente es el dominio DNS de los usuarios, solo que el dominio está en mayúsculas).
- Seleccione **Import (Importar)** en el **Kerberos Keytab (Keytab de Kerberos)** que creó para el cortafuegos.

STEP 3 | Asigne el perfil de autenticación a la aplicación del cortafuegos que requiera autenticación.

- Acceso administrativo a la interfaz web: realice la Configuración de una cuenta administrativa de cortafuegos y asigne el perfil de autenticación que configuró.
- Acceso de los usuarios finales a los servicios y las aplicaciones: asigne el perfil de autenticación que configuró a un objeto de ejecución de autenticación. Durante la configuración del objeto, configure el **Authentication Method (Método de autenticación)** como **browser-challenge (Desafío del explorador)**. Asigne el objeto a las reglas de la política de autenticación. Para obtener información sobre todo el procedimiento de configuración de la autenticación para los usuarios finales, consulte la Configuración de la política de autenticación.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación del servidor Kerberos

Puede utilizar Kerberos para autenticar de forma nativa los usuarios finales y los administradores del cortafuegos o de Panorama para un controlador de dominio de Active Directory o un servidor de autenticación Kerberos compatible con V5. Este método de autenticación es interactivo y requiere que los usuarios introduzcan nombres de usuario y contraseñas.

Para usar un servidor Kerberos para la autenticación, debe poderse acceder al servidor a través de una dirección IPv4. Las direcciones IPv6 no son compatibles.

STEP 1 | Añada un perfil de servidor Kerberos.

El perfil define cómo el cortafuegos se conecta al servidor de Kerberos.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Kerberos** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **Kerberos** en Panorama™ y **añada** un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. **Add (Añada)** cada servidor y especifique un **Name (Nombre)** (para identificar el servidor), la dirección IPv4 o FQDN del **Kerberos Server (servidor de Kerberos)** y un número de **Port (Puerto)** opcional para la comunicación con el servidor (el valor predeterminado es 88).

   Si utiliza un objeto de dirección FQDN para identificar al servidor y, posteriormente, cambia la dirección, debe confirmar el cambio para que se aplique la nueva dirección de servidor.
4. Haga clic en **OK (Aceptar)** para guardar los cambios en el perfil.

STEP 2 | Asigne el perfil del servidor para realizar la Configuración de una secuencia y perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de usuarios.

STEP 3 | Asigne el perfil de autenticación a la aplicación del cortafuegos que requiera autenticación.

- Acceso administrativo a la interfaz web: realice la Configuración de una cuenta administrativa de cortafuegos y asigne el perfil de autenticación que configuró.
- Acceso de los usuarios finales a los servicios y las aplicaciones: asigne el perfil de autenticación que configuró a un objeto de ejecución de autenticación y asigne el objeto a las reglas de la política de autenticación. Para obtener información sobre todo el procedimiento de configuración de la autenticación para los usuarios finales, consulte la Configuración de la política de autenticación.

STEP 4 | Verifique que el cortafuegos pueda comprobar la conectividad con el servidor de autenticación para autenticar a los usuarios.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación TACACS+

Puede configurar la autenticación TACACS+ para los usuarios finales y el cortafuegos, o los administradores de Panorama. También puede usar un servidor TACACS+ para gestionar la autorización de administrador (función y asignaciones de dominio de acceso) al definir los atributos específicos del proveedor (Vendor-Specific Attributes, VSA). Configure un perfil de servidor TACACS+ para todos los usuarios que defina cómo se conectan el cortafuegos o Panorama al servidor. A continuación, asigne el perfil de servidor a un perfil de autenticación en cada conjunto de usuarios que necesite una configuración común de autenticación. Lo que haga con el perfil de autenticación dependerá de los usuarios que el servidor TACACS+ autentique:

- **Usuarios finales**: asigne el perfil de autenticación a un objeto de cumplimiento de autenticación y asigne el objeto a reglas de política de autenticación. Para conocer el procedimiento completo, consulte Configuración de la política de autenticación.
- **Cuentas administrativas con autorización gestionada a nivel local en el cortafuegos o Panorama**: asigne el perfil de autenticación a las cuentas del administrador del cortafuegos o administrador de Panorama.
- **Cuentas administrativas con autorización gestionada en el servidor TACACS+:** el siguiente procedimiento describe cómo configurar la autenticación y autorización de TACACS+ para los administradores el cortafuegos. Para los administradores de Panorama, consulte Configuración de autenticación TACACS+ para administradores de Panorama.

STEP 1 | Añada un perfil de servidor TACACS+.

El perfil define de qué manera el cortafuegos se conecta con el servidor TACACS+.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **TACACS+** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACAS+** en Panorama™ y **añada** un perfil.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. (Opcional) Seleccione **Administrator Use Only (Solo uso de administrador)** para restringir el acceso a administradores.
4. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 20).
5. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **CHAP**) que el cortafuegos utiliza para autenticarse en el servidor TACACS+.

   Seleccione CHAP si el servidor TACACS+ admite ese protocolo; es más seguro que PAP.
6. Seleccione **Add (Añadir)** para añadir cada servidor TACACS+ e ingrese lo siguiente:
   - Un nombre en **Name** para identificar el servidor.
   - La dirección IP o FQDN del **servidor TACACS+**. Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección de servidor tenga efecto.
   - **Secret (Secreto)**/**Confirm Secret (Confirmar secreto)** (clave para cifrar nombres de usuario y contraseñas).
   - El **Port (Puerto)** del servidor para las solicitudes de autenticación (el valor predeterminado es 49).
7. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Asigne el perfil del servidor TACACS+ a un perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de usuarios.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir un perfil.

© 2020 Palo Alto Networks, Inc.

2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Configure el **Type (Tipo)** en **TACACS+**.
4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.
5. Seleccione **Retrieve user group from TACACS+ (Recuperar grupo de usuarios desde TACACS+)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor TACACS+.

   El cortafuegos coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los usuarios y grupos que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 3 | Configure el cortafuegos para que utilice el perfil de autenticación para todos los administradores.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite los ajustes de Authentication Settings (Configuración de autenticación).
2. Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró y haga clic en **OK (Aceptar)**.

STEP 4 | Configure los roles y dominios de acceso que definen los ajustes de autorización para los administradores.

Si ya definió VSA TACACS+ en el servidor TACACS+, los nombres que especifique para los roles y dominios de acceso en el cortafuegos deben coincidir con los valores de VSA.

1. Configure un perfil de rol de administrador si el administrador utilizará un rol personalizado en lugar de un rol predefinido (dinámico).
2. Configure un dominio de acceso si el cortafuegos tiene más de un sistema virtual: seleccione **Device (Dispositivo)** > **Access Domain (Dominio de acceso)**, y luego **Add (Añadir)** para añadir un dominio de acceso, ingrese un nombre en **Name (Nombre)** para identificar el dominio de acceso, y seleccione **Add (Añadir)** para añadir cada sistema virtual al que accederá el administrador. Luego haga clic en **OK (Aceptar)**.

STEP 5 | Seleccione **Commit (Confirmar)** para aplicar los cambios y luego actívelos en el cortafuegos.

STEP 6 | Configure el servidor TACACS+ para que autentique y autorice administradores.

Consulte la documentación de su servidor TACACS+ a fin de obtener instrucciones específicas para realizar los siguientes pasos:

1. Añada la dirección IP o el nombre de host del cortafuegos como el cliente TACACS+.
2. Añada las cuentas de administrador.

   Si seleccionó CHAP como el Authentication Protocol (Protocolo de autenticación), debe definir cuentas con contraseñas cifradas de manera reversible. De lo contrario, la autenticación CHAP fallará.
3. Defina VSA TACACS+ para el rol, dominio de acceso y grupo de usuario de cada administrador.

   Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba ***`superuser (superusuario)`****, no* ***`SuperUser (SuperUsuario)`****.*

STEP 7 | Verifique que el servidor TACACS+ realice la autenticación y autorización de los administradores.

© 2020 Palo Alto Networks, Inc.

1. Inicie sesión en la interfaz web del cortafuegos usando una cuenta de administrador que haya añadido al servidor TACACS+.
2. Verifique que pueda acceder solo a las páginas de la interfaz web que están permitidas para el rol que usted asoció con el administrador.
3. En las pestañas **Monitor (Supervisar)**, **Policies (Políticas)** y **Objects (Objetos)**, verifique que puede acceder únicamente a los sistemas virtuales que están permitidos para el dominio de acceso que asoció con el administrador.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación RADIUS

Puede configurar la autenticación RADIUS para los usuarios finales y el cortafuegos, o los administradores de Panorama. Para los administradores, puede usar RADIUS para gestionar la autorización (función y asignaciones de dominio de acceso) al definir los atributos específicos del proveedor (Vendor-Specific Attributes, VSA). También puede usar RADIUS para implementar la autenticación multifactor (Multi-Factor Authentication, MFA) para los administradores e usuarios finales. Para habilitar la autenticación con RADIUS, configure un perfil de servidor RADIUS que defina cómo se conectan el cortafuegos o Panorama al servidor (consulte el paso 1 a continuación). A continuación, asigne el perfil de servidor a un perfil de autenticación en cada conjunto de usuarios que necesite una configuración común de autenticación (consulte el paso 5 a continuación). Lo que haga con el perfil de autenticación dependerá de los usuarios que el servidor RADIUS autentique:

- **Usuarios finales**: asigne el perfil de autenticación a un objeto de cumplimiento de autenticación y asigne el objeto a reglas de política de autenticación. Para conocer el procedimiento completo, consulte Configuración de la política de autenticación.



También puede configurar sistemas cliente para que envíen atributos específicos del proveedor (Vendor-Specific Attributes, VSA) de RADIUS al servidor RADIUS asignando el perfil de autenticación a un portal o puerta de enlace de GlobalProtect. Los administradores de RADIUS luego pueden realizar tareas administrativas en función de dichos VSA.

- **Cuentas administrativas con autorización gestionada a nivel local en el cortafuegos o Panorama**: asigne el perfil de autenticación a las cuentas del administrador del cortafuegos o administrador de Panorama.
- **Cuentas administrativas con autorización gestionada en el servidor RADIUS:** el siguiente procedimiento describe cómo configurar la autenticación y autorización de RADIUS para los administradores el cortafuegos. Para los administradores de Panorama, consulte Configuración de autenticación RADIUS para administradores de Panorama.

STEP 1 | Añada un perfil de servidor RADIUS.

El perfil define de qué manera el cortafuegos se conecta con el servidor RADIUS.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **RADIUS** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** en Panorama™ y **añada** un perfil.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. (Opcional) Seleccione **Administrator Use Only (Solo uso de administrador)** para restringir el acceso a administradores.
4. Introduzca un intervalo de **Timeout (Tiempo de espera)** en segundos después del cual la solicitud de autenticación vence (el valor predeterminado es 3; el intervalo es de 1 a 120).

   Si utiliza el perfil del servidor para integrar el cortafuegos con un servicio MFA, ingrese un intervalo que proporcione a los usuarios tiempo suficiente para autenticarse. Por ejemplo, si el servicio MFA solicita una única contraseña (OTP), los usuarios necesitan tiempo para ver la OTP en su dispositivo de endpoint y, a continuación, introducir la OTP en la página de inicio de sesión de MFA.
5. Especifique el número de **reintentos**.
6. Seleccione el **Authentication Protocol (Protocolo de autenticación)** (el valor predeterminado es **PEAP-MSCHAPv2**) que el cortafuegos utiliza para autenticarse en el servidor RADIUS.

   En función de los factores que desee utilizar para autenticar a los usuarios en su entorno de autenticación multifactor (multi-factor authentication, MFA), seleccione el protocolo de autenticación adecuado:

© 2020 Palo Alto Networks, Inc.

- **Nombre de usuario, contraseña e inserción (una solicitud fuera de banda activada automáticamente)**: compatible con todos los protocolos de autenticación
- **Inserción, contraseña, token y PIN (cuando la contraseña, el token o el PIN se brindan en conjunto)**: compatible con PAP, PEAP con GTC y EAP-TTLS con PAP
- **Nombre de usuario, contraseña, token, PIN y respuesta a desafío (cuando la contraseña, el token o el PIN se brindan en conjunto)**: compatible con PAP y PEAP con GTC

Si selecciona un método de autenticación de EAP (PEAP-MSCHAPv2, PEAP con GTC o EAP-TTLS con PAP), confirme que su servidor RADIUS admita seguridad de capa de transporte (Transport Layer Security, TLS) 1.1 o superior, y que las entidades de certificación (Certificate authorities, CA) del servidor RADIUS se incluyan en el perfil de certificado asociado al perfil del servidor RADIUS. Si selecciona un método de EAP y no asocia el perfil de certificado configurado correctamente con el perfil RADIUS, la autenticación falla.

7. Seleccione **Add (Añadir)** para añadir cada servidor RADIUS e ingrese lo siguiente:
   - Un nombre en **Name** para identificar el servidor.
   - La dirección IP o FQDN del **servidor RADIUS**. Si utiliza un FQDN para identificar el servidor y, posteriormente, cambia la dirección, debe confirmar el cambio para que entre en vigor la nueva dirección del servidor.
   - La clave para cifrar las contraseñas en **Secret (Secreto)** y **Confirm Secret (Confirmar secreto)**, con una longitud máxima de 64 caracteres.
   - El **Port (Puerto)** del servidor para las solicitudes de autenticación (el valor predeterminado es 1812).
8. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

Para lograr redundancia, añada varios servidores RADIUS en la secuencia que desea que el cortafuegos los utilice. Si seleccionó un método de EAP, configure una secuencia de autenticación para garantizar que los usuarios puedan responder al desafío de autenticación. No existen métodos alternativos de autenticación para el EAP: si el usuario falla el desafío de autenticación y no configuró una secuencia de autenticación que permita otro método de autenticación, la autenticación falla.

STEP 2 | Si utiliza PEAP-MSCHAPv2 con GlobalProtect, seleccione **Allow users to change passwords after expiry (Permitir a los usuarios cambiar contraseñas tras el vencimiento)** para permitir que los usuarios de GlobalProtect cambien las contraseñas vencidas para iniciar sesión.

STEP 3 | (PEAP-MSCHAPv2, PEAP con GTC o EAP-TTLS con PAP únicamente) Para hacer anónima la identidad del usuario en el túnel externo que se crea tras la autenticación en el servidor, seleccione **Make Outer Identity Anonymous (Hacer anónima la identidad externa)**.



Debe configurar el servidor RADIUS, de modo que toda la cadena permita el acceso a usuarios anónimos. Es posible que algunas configuraciones de servidor RADIUS no admitan ID externas anónimas y que deba anular esta selección. Cuando lo hace, el servidor RADIUS transmite nombres de usuario en texto sin cifrar.

STEP 4 | Si selecciona un método de autenticación de EAP, seleccione un perfil de certificado.

STEP 5 | Asigne el perfil del servidor RADIUS a un perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de usuarios.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
3. Configure el **Type (Tipo)** en **RADIUS**.
4. Seleccione el **Server Profile (Perfil de servidor)** que configuró.

© 2020 Palo Alto Networks, Inc.

5. Seleccione **Retrieve user group from RADIUS (Recuperar grupo de usuarios desde RADIUS)** para recopilar información de grupo de usuarios desde los VSA definidos en el servidor RADIUS.

   El cortafuegos coteja la información del grupo con los grupos que usted especifica en la lista de permitidos del perfil de autenticación.
6. Seleccione **Advanced (Avanzado)** y, en la lista de permitidos, haga clic en **Add (Añadir)** y añada los usuarios y grupos que pueden autenticarse con este perfil de autenticación.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 6 | Configure el cortafuegos para que utilice el perfil de autenticación para todos los administradores.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite los ajustes de Authentication Settings (Configuración de autenticación).
2. Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró y haga clic en **OK (Aceptar)**.

STEP 7 | Configure los roles y dominios de acceso que definen los ajustes de autorización para los administradores.

Si ya definió VSA RADIUS en el servidor RADIUS, los nombres que especifique para los roles y dominios de acceso en el cortafuegos deben coincidir con los valores de VSA.

1. Configure un perfil de rol de administrador si el administrador utiliza un rol personalizado en lugar de un rol predefinido (dinámico).
2. Configure un dominio de acceso si el cortafuegos tiene más de un sistema virtual:
   1. Seleccione **Device (Dispositivo)** > **Access Domain (Dominio de acceso)** y luego **Add (Añadir)** para añadir un dominio de acceso, e ingrese un nombre en **Name (Nombre)** para identificar el dominio de acceso.
   2. Seleccione **Add (Añadir)** para añadir cada sistema virtual al que accederá el administrador y luego haga clic en **OK (Aceptar)**.

STEP 8 | Seleccione **Commit (Confirmar)** para aplicar los cambios y luego actívelos en el cortafuegos.

STEP 9 | Configure el servidor RADIUS para que autentique y autorice administradores.

Consulte la documentación de su servidor RADIUS a fin de obtener instrucciones específicas para realizar los siguientes pasos:

1. Añada la dirección IP o nombre de host del cortafuegos como el cliente RADIUS.
2. Añada las cuentas de administrador.

   Si el perfil de servidor RADIUS especifica CHAP como el Authentication Protocol (Protocolo de autenticación), debe definir cuentas con contraseñas cifradas de manera reversible. De lo contrario, la autenticación CHAP fallará.
3. Defina el código de proveedor para el cortafuegos (25461) y defina los VSA RADIUS para el rol, el dominio de acceso y el grupo de usuario de cada administrador.

   Si predefine las funciones dinámicas de administrador para los usuarios, especifíquelas en minúscula; por ejemplo, escriba **`superuser (superusuario)`**, no **`SuperUser (SuperUsuario)`**.

   *Al configurar las opciones de proveedor avanzadas en ACS, debe configurar tanto el Vendor Length Field Size (Tamaño de campo de longitud de proveedor) como el Vendor Type Field Size (Tamaño de campo de tipo de proveedor) en **`1`**. De lo contrario, la autenticación fallará.*
4. Si seleccionó un método de EAP, el cortafuegos valida el servidor, pero no el cliente. Para garantizar la validez del cliente, restrinja a los clientes por dirección IP y subdominio.

© 2020 Palo Alto Networks, Inc.

STEP 10 | Verifique que el servidor RADIUS realice la autenticación y autorización de los administradores.

1. Inicie sesión en la interfaz web del cortafuegos usando una cuenta de administrador que haya añadido al servidor RADIUS.
2. Verifique que pueda acceder solo a las páginas de la interfaz web que están permitidas para el rol que usted asoció con el administrador.
3. En las pestañas **Monitor (Supervisar)**, **Policies (Políticas)** y **Objects (Objetos)**, verifique que puede acceder únicamente a los sistemas virtuales que están permitidos para el dominio de acceso que asoció con el administrador.
4. En **Monitor (Supervisión)** > **Authentication (Autenticación)**, verifique el **Authentication Protocol (Protocolo de autenticación)**.
5. Pruebe la conexión y la validez del perfil de certificado utilizando el siguiente comando de la CLI:

```
admin@PA-220 > test authentication authentication-profile auth-profile
 username <username> password <password>
```


© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación LDAP

Puede utilizar LDAP para autenticar a los usuarios finales que acceden a aplicaciones y servicios mediante el portal de autenticación, y autenticar a los administradores del cortafuegos o de Panorama que acceden a la interfaz de web.

También puede conectarse a un servidor LDAP para definir las reglas de la política en función de los grupos de usuarios. Si desea información detallada, consulte la Asignación de usuarios a grupos*.*

STEP 1 | Añada un perfil de servidor LDAP.

El perfil define cómo el cortafuegos se conecta al servidor LDAP.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **LDAP** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **LDAP** en Panorama™ y **añada** un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. (Solo sistemas virtuales múltiples) Seleccione la **ubicación** en la que está disponible el perfil.
4. (Opcional) Seleccione **Administrator Use Only (Solo uso de administrador)** para restringir el acceso a administradores.
5. **Add (Añada)** los servidores LDAP (máximo de cuatro). Para cada servidor, ingrese un nombre en **Name** (para identificar al servidor), una dirección IP del **LDAP Server (Servidor LDAP)** o FQDN, y un **Port (Puerto)** para el servidor (el valor predeterminado es 389).

   Si utiliza un objeto de dirección FQDN para identificar el servidor y posteriormente cambia la dirección, debe confirmar el cambio para que la nueva dirección de servidor tenga efecto.
6. Seleccione el **Type (Tipo)** de servidor.
7. Seleccione el **DN base**.

   Para identificar el DN base de su directorio, abra el complemento de la consola de administración de Microsoft **Active Directory Domains and Trusts (Dominios y confianzas de Active Directory)** y use el nombre del dominio de nivel superior.
8. Introduzca **Bind DN (DN de enlace)** y **Password (Contraseña)** para permitir que el servicio de autenticación autentique el cortafuegos.

   La cuenta DN de enlace debe tener permiso para leer el directorio LDAP.
9. Ingrese el **Bind Timeout (Tiempo de espera de enlace)** y el **Search Timeout (Tiempo de espera de búsqueda)** en segundos (el valor predeterminado es 30 para ambos).
10. Especifique el **intervalo de reintento** en segundos (el valor predeterminado es 60).
11. Habilite la opción para **requerir una conexión segura SSL/ TLS** (habilitada de manera predeterminada). El protocolo que usa el endpoint depende del puerto del servidor:
    - 389 (predeterminado): TLS (específicamente, el dispositivo usa la operación StartTLS, que actualiza la conexión de texto no cifrado inicial a TLS).
    - 636—SSL
    - Cualquier otro puerto: El dispositivo intenta primer usar TLS. Si el servidor de directorio no admite TLS, el dispositivo cambia a SSL.
12. (Opcional) Para mayor seguridad, habilite la opción **Verify Server Certificate for SSL sessions (Verificar el certificado del servidor para las sesiones SSL)** de modo que el endpoint verifique el certificado que el servidor de directorio presenta para las conexiones SSL/TLS. Para habilitar la

© 2020 Palo Alto Networks, Inc.

verificación, debe seleccionar también la opción **Require SSL/TLS secured connection (Requerir conexión segura de SSL/TLS)**. Para que la verificación se realice correctamente, el certificado debe reunir una de las siguientes condiciones:

- Está en la lista de certificados de dispositivo: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**. Si es necesario, importe el certificado al dispositivo.
- El firmante del certificado está en la lista de autoridades de certificación confiables: **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Autoridades de certificados de confianza por defecto)**.

13. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Asigne el perfil del servidor para realizar la Configuración de una secuencia y perfil de autenticación para definir varias configuraciones de autenticación.

STEP 3 | Asigne el perfil de autenticación a la aplicación del cortafuegos que requiera autenticación.

- **Acceso administrativo a la interfaz web**: realice la Configuración de una cuenta administrativa de cortafuegos y asigne el perfil de autenticación que configuró.
- **Acceso de los usuarios finales a los servicios y las aplicaciones**: para obtener información sobre todo el procedimiento de configuración de la autenticación para los usuarios finales, consulte la Configuración de la política de autenticación.

STEP 4 | Verifique que el cortafuegos pueda comprobar la conectividad con el servidor de autenticación para autenticar a los usuarios.

© 2020 Palo Alto Networks, Inc.

Tiempos de espera de conexión de los servidores de autenticación

Puede configurar el cortafuegos para utilizar Servicios de autenticación externa para los administradores de autenticación que acceden al cortafuegos o Panorama, y los usuarios finales que acceden a servicios o aplicaciones mediante el portal de autenticación. Para garantizar que el cortafuegos no desperdicie recursos por intentar alcanzar continuamente un servidor de autenticación que es inalcanzable, puede configurar un intervalo de tiempo de espera tras el cual el cortafuegos deja de intentar la conexión. Configure el tiempo de espera en los perfiles del servidor que definen cómo el cortafuegos se conecta a los servidores de autenticación. Cuando selecciona valores de tiempo de espera, su objetivo es proporcionar un equilibrio entre la necesidad de conservar los recursos del cortafuegos y ser responsable de demoras normales de red que afectan a la rapidez con la que los servidores de autenticación responden al cortafuegos.

- Directrices de configuración de tiempo de espera de autenticación
- Modificación del tiempo de espera de servidor web de PAN-OS
- Modificación del tiempo de espera de sesión del portal de autenticación

Directrices de configuración de tiempo de espera de autenticación

A continuación, se muestran algunas de las directrices de configuración del tiempo de espera para los intentos del cortafuegos de conectarse con servicios de autenticación externa.

- Además del tiempo de espera que configura en los perfiles del servidor para los servidores específicos, el cortafuegos tiene un tiempo de espera global de servidor web de PAN-OS. El tiempo de espera global se aplica cuando el cortafuegos se conecta a cualquier servidor externo para autenticar el acceso administrativo a la interfaz web del cortafuego o a la API de XML de PAN-OS, y el acceso de usuario final a las aplicaciones o servicios mediante el portal de autenticación. El tiempo de espera global predeterminado es de 30 segundos (rango: 3 a 125). El valor debe ser igual o superior al tiempo total durante el cual cualquier perfil de servidor permite los intentos de conexión. El tiempo total en un perfil de servidor es el valor de tiempo de espera multiplicado por la cantidad de reintentos y la cantidad de servidores. Por ejemplo, si un perfil de servidor RADIUS especifica un tiempo de espera de 3 segundos, 3 reintentos y 4 servidores, la cantidad total de tiempo que brinda el perfil para los intentos de conexión es de 36 segundos (3 x 3 x 4). Realice la Modificación del tiempo de espera de servidor web de PAN-OS si es necesario.

  No cambie el tiempo de espera de servidor web de PAN-OS a menos que observe fallos de autenticación. Si establece un valor de tiempo de espera demasiado alto, es posible que se degrade el rendimiento del cortafuegos o que el cortafuegos descarte solicitudes de autenticación. Puede revisar los fallos de autenticación en los logs de autenticación.
- El cortafuegos aplica un tiempo de espera a la sesión en el portal de autenticación que define cuánto tiempo pueden dedicar los usuarios finales a la respuesta del desafío de autenticación en un formulario web del portal de autenticación. El formulario web se muestra cuando los usuarios solicitan servicios o aplicaciones que coinciden con una regla de la política de autenticación. El tiempo de espera predeterminado de la sesión es de 30 segundos (rango: 1 a 1.599.999). El valor debe ser igual o superior al tiempo de espera del servidor web de PAN-OS. Modificación del tiempo de espera de sesión del portal de autenticación, si fuese necesario. Tenga en cuenta que es posible que aumentar los valores de tiempo de espera del servidor web de PAN-OS y de sesión del portal de autenticación degrade el rendimiento del cortafuegos o provoque el descarte de las solicitudes de autenticación.

  El tiempo de espera de sesión del portal de autenticación no se relaciona con los temporizadores que determinan por cuánto tiempo el cortafuegos retiene las asignaciones de direcciones IP a nombres de usuario.

© 2020 Palo Alto Networks, Inc.

- Los valores de tiempo de espera se acumulan en las secuencias de autenticación. Por ejemplo, considere el caso de una secuencia de autenticación con dos perfiles de autenticación. Un perfil de autenticación especifica un perfil de servidor RADIUS con 3 segundos de tiempo de espera, 3 reintentos y 4 servidores. El otro perfil de autenticación especifica un perfil de servidor TACACS+ con 3 segundos de tiempo de espera y 2 servidores. El período más prolongado posible durante el cual el cortafuegos puede intentar autenticar las cuentas de usuario con esa secuencia de autenticación es 42 segundos: 36 segundos para el perfil de servidor RADIUS, además de 6 segundos para el perfil de servidor TACACS+.
- El valor de tiempo de espera no configurable para los servidores de Kerberos es de 17 segundos en cada servidor, que se especifica en el perfil de servidor de Kerberos.
- Para configurar los valores de tiempo de espera y la configuración relacionada de otros tipos de servidores, consulte:
  - Añada un perfil de servidor MFA.
  - Añada un perfil de servidor SAML IdP.
  - Añada un perfil de servidor TACACS+.
  - Añada un perfil de servidor RADIUS.
  - Añada un perfil de servidor LDAP.

Modificación del tiempo de espera de servidor web de PAN-OS

El tiempo de espera del servidor web de PAN-OS debe ser igual o mayor al tiempo de espera en cualquier perfil de servidor de autenticación multiplicado por la cantidad de reintentos y la cantidad de servidores en ese perfil.

No cambie el tiempo de espera de servidor web de PAN-OS a menos que observe fallos de autenticación. Si establece un valor de tiempo de espera demasiado alto, es posible que se degrade el rendimiento del cortafuegos o que el cortafuegos descarte solicitudes de autenticación. Puede revisar los fallos de autenticación en los logs de autenticación.

STEP 1 | Acceda a la CLI del cortafuegos.

STEP 2 | Establezca el tiempo de espera del servidor web de PAN-OS introduciendo los siguientes comandos, donde ***<value>*** es la cantidad de segundos (predeterminado: 30; rango: 3 a 125).

```
> configure
# set deviceconfig setting l3-service timeout <value>
# commit
```

Modificación del tiempo de espera de sesión del portal de autenticación

El valor de tiempo de espera de la sesión del portal de autenticación debe ser igual o superior al tiempo de espera del servidor web de PAN-OS. Para obtener información detallada, consulte Tiempos de espera de conexión de los servidores de autenticación.

Cuanto más eleve los tiempos de espera de sesión del servidor web de PAN-OS y el portal de autenticación, más lentamente responderá el portal de autenticación a los usuarios.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique los tiempos de espera de la sesión.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Introduzca un nuevo valor en segundos en el **portal de autenticación** (el valor predeterminado es 30; el intervalo es de 1 a 1 599 999) y haga clic en **OK (Aceptar)**.

STEP 3 | **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Configuración de la autenticación de la base de datos local

Puede configurar una base de datos de usuarios que sea local en el cortafuegos para autenticar a los administradores que acceder a la interfaz web del cortafuegos y para autenticar a los usuarios finales que acceden a las aplicaciones mediante el portal de autenticación o GlobalProtect. Realice los siguientes pasos para configurar la autenticación local con una base de datos local.

Por lo general, se recomiendan los servicios de autenticación externos en lugar de los de autenticación local debido a que proporcionan el beneficio de la gestión central de las cuentas.

Además, puede configurar la autenticación local sin una base de datos, pero solo para los administradores de cortafuegos o de Panorama.

STEP 1 | Añada la cuenta de usuario a la base de datos local.

1. Seleccione **Device (Dispositivo)** > **Local User Database (Base de datos de usuarios locales)** > **Users (Usuarios)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** para el administrador.
3. Introduzca una contraseña en **Password (Contraseña)** y luego en **Confirm Password (Confirmar contraseña)**, o introduzca una contraseña con hash en **Password Hash (Hash de contraseña)**.
4. Seleccione **Enable (Habilitar)** para habilitar la cuenta (habilitado por defecto) y haga clic en **OK (Aceptar)**.

STEP 2 | Añada el grupo de usuarios a la base de datos local.

Esto es obligatorio si sus usuarios requieren pertenencia a un grupo.

1. Seleccione **Device (Dispositivo)** > **Local User Database (Base de datos de usuarios locales)** > **User Groups (Grupos de usuarios)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name** para identificar al grupo.
3. Seleccione **Add** para añadir cada usuario que sea miembro del grupo y luego haga clic en **OK**.

STEP 3 | Configure un perfil de autenticación.

El perfil de autenticación define los ajustes de autenticación que son comunes a un conjunto de usuarios. Configure el **Type (Tipo)** de autenticación en **Local Database (Base de datos local)**.

STEP 4 | Asigne el perfil de autenticación a una cuenta administrativa o a una regla de la política de autenticación para los usuarios finales.

- **Administradores**: Configuración de una cuenta administrativa de cortafuegos:

  Especifique en **Name (Nombre)** el nombre de un usuario que definió previamente en este procedimiento.

  Asigne el **Authentication Profile (Perfil de autenticación)** que configuró para la cuenta.

- **Usuarios finales:** para conocer el procedimiento completo para configurar la autenticación para los usuarios finales, consulte Configuración de la política de autenticación.

STEP 5 | Verifique que el cortafuegos pueda comprobar la conectividad con el servidor de autenticación para autenticar a los usuarios.

© 2020 Palo Alto Networks, Inc.

Configuración de una secuencia y perfil de autenticación

Un perfil de autenticación define el servicio de autenticación que valida las credenciales de inicio de sesión de los administradores que acceden a la interfaz web del cortafuegos y a los usuarios finales que acceden a las aplicaciones a través del portal de autenticación o GlobalProtect. El servicio puede ser la Autenticación local que proporciona el cortafuegos o Servicios de autenticación externa. El perfil de autenticación también define las opciones como el inicio de sesión único (single sign-on, SSO) de Kerberos.

Algunas redes tienen múltiples bases de datos (como TACACS+ y LDAP) para distintos usuarios y grupos de usuarios. Para autenticar usuarios en esos casos, configure una *secuencia de autenticación*: una clasificación ordenada de perfiles de autenticación con los que el cortafuegos compara al usuario durante el inicio de sesión. El cortafuegos compara cada perfil en orden hasta que uno autentica correctamente al usuario. Solo se impide el acceso del usuario si falla la autenticación con todos los perfiles definidos en la secuencia. La secuencia puede especificar los perfiles de autenticación que se basan en un servicio de autenticación que el cortafuegos admite, excepto la autenticación multifactor (Multi-Factor Authentication, MFA) y SAML.

STEP 1 | (Solo servicio externo) Habilite al cortafuegos para que se conecte con un servidor externo para autenticar a los usuarios:

1. Configure el servidor externo. Consulte la documentación de su servidor para obtener las instrucciones.
2. Configure un perfil de servidor para el tipo de servicio de autenticación que utiliza.
   - Añada un perfil de servidor RADIUS.

     Si el cortafuegos se integra con un servicio MFA a través de RADIUS, debe añadir un perfil de servidor RADIUS. En este caso, el servicio MFA proporciona todos los factores de autenticación. Si el cortafuegos se integra con un servicio MFA a través de una API de proveedor, se puede seguir usando un perfil de servidor RADIUS para el primer factor, pero se necesitan los perfiles de servidor MFA para los factores adicionales.

   - Añada un perfil de servidor MFA.
   - Añada un perfil de servidor SAML IdP.
   - Añada un perfil de servidor Kerberos.
   - Añada un perfil de servidor TACACS+.
   - Añada un perfil de servidor LDAP.

STEP 2 | (Autenticación de base de datos local únicamente) Configure una base de datos de usuario que sea local para el cortafuegos.

Realice estos pasos para cada usuario y grupo de usuarios para los cuales desea configurar la autenticación local en función de un almacén de identidades de usuario que sea local para el cortafuegos:

1. Añada la cuenta de usuario a la base de datos local.
2. (Opcional) Añada el grupo de usuarios a la base de datos local.

STEP 3 | (Kerberos SSO únicamente) Cree un keytab Kerberos para el cortafuegos si el inicio de sesión único (SSO) de Kerberos es el servicio de autenticación primario.

© 2020 Palo Alto Networks, Inc.

Cree un keytab de Kerberos. Un keytab es un archivo que contiene información de cuenta de Kerberos para el cortafuegos. Para respaldar el SSO de Kerberos, su red debe contar con una infraestructura Kerberos.

STEP 4 | Configure un perfil de autenticación.

Defina una de las siguientes opciones, o ambas:

- **SSO de Kerberos:** el cortafuegos prueba la autenticación de SSO en primer lugar. Si falla, volverá al **tipo** de autenticación especificado.
- **Autenticación externa o autenticación de base de datos local:** el cortafuegos solicita al usuario que introduzca las credenciales de inicio de sesión y utiliza un servicio externo o base de datos local para autenticar al usuario.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y luego **Add (Añadir)** para añadir el perfil de autenticación.
2. Introduzca un **Name (Nombre)** para identificar el perfil de autenticación.
3. Seleccione el **Type (Tipo)** de servicio de autenticación.

   Si utiliza autenticación multifactor, el tipo seleccionado se aplica únicamente al primer factor de autenticación. En la pestaña **Factors (Factores)**, puede seleccionar factores MFA adicionales.

   Si selecciona **RADIUS**, **TACACS+**, **LDAP** o **Kerberos**, elija el **Server Profile (Perfil de servidor)**.

   Si selecciona **LDAP**, seleccione el **Server Profile (Perfil de servidor)** y defina el **Login Attribute (Atributo de inicio de sesión)**. Para Active Directory, introduzca **sAMAccountName** como valor.

   Si selecciona **SAML**, seleccione el **IdP Server Profile (Perfil de servidor IdP)**.
4. Si desea activar el SSO de Kerberos, introduzca el **Kerberos Realm** (normalmente es el dominio DNS de los usuarios, excepto por que el dominio está en MAYÚSCULAS) y seleccione **Import (Import)** para importar el **Kerberos Keytab** que ha creado para el cortafuegos o Panorama.
5. (MFA únicamente) Seleccione **Factors (Factores)**, **Enable Additional Authentication Factors (Habilitar factores de autenticación adicionales)** y luego **Add (Añadir)** para añadir los perfiles de servidor MFA que configuró.

   El cortafuegos invocará cada servicio MFA en el orden enumerado, desde arriba hacia abajo.
6. Seleccione **Advanced (Avanzado)** y **Add (Añadir)** para añadir los usuarios y grupos que se pueden autenticar con este perfil.

   Puede seleccionar usuarios y grupos de la base de datos local o, si ha configurado el cortafuegos en Map Users to Groups (Asignar usuarios a grupos) de un servicio de directorio basado en LDAP, como Active Directory. De manera predeterminada, la lista está vacía, por lo que ningún usuario se puede autenticar.

   También puede seleccionar grupos personalizados definidos en una configuración de asignación de grupo.
7. (Opcional) Para modificar los datos del usuario antes de que el cortafuegos envíe la solicitud de autenticación al servidor, configure **Username Modifier (Modificador de nombre de usuario)**.

   - **%USERDOMAIN%\%USERINPUT%**: si el origen no incluye el dominio (por ejemplo, utiliza sAMAccountName), el cortafuegos añade el dominio del usuario que haya especificado delante del nombre del usuario. Si el origen incluye el dominio, el cortafuegos lo sustituye por el valor indicado en **User Domain (Dominio de usuario)**. Si se deja en blanco **User Domain (Dominio de usuario)**, el cortafuegos elimina el dominio de los datos del usuario que recibe del origen antes de enviar la solicitud al servidor de autenticación.

     No emplee esta opción para realizar la autenticación en servidores LDAP, ya que no admiten el uso de barras invertidas en sAMAccountName.

© 2020 Palo Alto Networks, Inc.

- **%USERINPUT%** (predeterminado): el cortafuegos envía los datos del usuario al servidor de autenticación con el mismo formato con el que los recibe del origen.
- **%USERINPUT%@%USERDOMAIN%**: si el origen no incluye el dominio, el cortafuegos añade el valor de **User Domain (Dominio de usuario)** detrás del nombre del usuario. Si el origen incluye el dominio, el cortafuegos lo sustituye por el valor indicado en **User Domain (Dominio de usuario)**. Si se deja en blanco **User Domain (Dominio de usuario)**, el cortafuegos elimina el dominio de los datos del usuario que recibe del origen antes de enviar la solicitud al servidor de autenticación.
- **None (Ninguno)**: si introduce manualmente este valor:
  - Para los perfiles de servidores LDAP y Kerberos, el cortafuegos utiliza el dominio que recibe del origen para seleccionar el perfil de autenticación adecuado y, luego, lo elimina cuando envía la solicitud de autenticación al servidor. Eso permite incluir el dominio del usuario en la secuencia de autenticación y eliminarlo antes de que cortafuegos envíe la solicitud de autenticación al servidor. Por ejemplo, si utiliza un perfil de servidor LDAP y sAMAccountName como atributo, emplee esta opción para que el cortafuegos no envíe el dominio al servidor de autenticación, que solo espera un nombre de usuario, no un dominio.
  - Para los perfiles de servidores RADIUS:
    - Si el origen envía los datos del usuario con el formato **`dominio\nombre-usuario`**, el cortafuegos los remite al servidor con el mismo formato.
    - Si el origen envía los datos del usuario con el formato **`nombre-usuario@dominio`**, el cortafuegos los cambia al formato normalizado **`dominio\nombre-usuario`** antes de enviarlos al servidor.
    - Si el origen solo envía el nombre de usuario, el cortafuegos añade el dominio del usuario que haya especificado antes de enviar los datos al servidor con el formato **`dominio\nombre-usuario`**.
  - Para las bases de datos locales, TACACS+ y SAML, el cortafuegos envía los datos del usuario al servidor de autenticación con el mismo formato con el que los recibe del origen.

8. Haga clic en **OK (Aceptar)** para guardar el perfil de autenticación.

STEP 5 | Configure una secuencia de autenticación.

Es obligatorio si desea que el cortafuegos pruebe múltiples perfiles de autenticación para autenticar usuarios. El cortafuegos evalúa los perfiles en orden descendente hasta que un perfil autentica correctamente al usuario.

1. Seleccione **Device (Dispositivo)** > **Authentication Sequence (Secuencia de autenticación)** y luego **Add (Añadir)** para añadir la secuencia de autenticación.
2. Introduzca un **nombre** para identificar la secuencia de autenticación.

   Para acelerar el proceso de autenticación, seleccione Use domain to determine authentication profile (Usar dominio para determinar el perfil de autenticación): el cortafuegos comparará el nombre del dominio que introduzca el usuario durante el inicio de sesión con el dominio de usuario o el dominio Kerberos de un perfil de autenticación de la secuencia, y luego usará ese perfil para autenticar al usuario. Si el cortafuegos no encuentra una coincidencia o si usted deshabilita la opción, el cortafuegos probará los perfiles en orden descendente.
3. Seleccione **Add** para añadir un perfil de autenticación. Para cambiar el orden de evaluación de los perfiles, seleccione un perfil y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**.
4. Haga clic en **OK (Aceptar)** para guardar la secuencia de autenticación.

STEP 6 | Asigne el perfil de autenticación o secuencia a una cuenta administrativa para los administradores del cortafuegos o a la política de autenticación para los usuarios finales.

© 2020 Palo Alto Networks, Inc.

- **Administradores:** asigne el perfil de autenticación según cómo gestiona la autorización del administrador:

  Autorización gestionada localmente en el cortafuegos: configure una cuenta de administrador de cortafuegos.

  Autorización gestionada en un servidor SAML, TACACS+ o RADIUS: seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, modifique los ajustes de autenticación y seleccione el **Authentication Profile (Perfil de autenticación)**.
- **Usuarios finales:** para conocer el procedimiento completo para configurar la autenticación para los usuarios finales, consulte Configuración de la política de autenticación.

STEP 7 | Verifique que el cortafuegos pueda comprobar la conectividad con el servidor de autenticación para autenticar a los usuarios.

© 2020 Palo Alto Networks, Inc.

Comprobación de la conectividad del servidor de autenticación

La función de comprobación de autenticación le permite comprobar si el cortafuegos o Panorama puede comunicarse con el servidor de autenticación especificado en un perfil de autenticación y si una solicitud de autenticación se produce correctamente para un usuario específico. Puede comprobar los perfiles de autenticación que autentican a los administradores que acceder a la interfaz web o que autentican a los usuarios finales que acceden a las aplicaciones mediante GlobalProtect o el portal de autenticación. Puede realizar pruebas de autenticación con la configuración del candidato para comprobar que la configuración sea correcta antes de confirmarla.

STEP 1 | Configure un perfil de autenticación. No es necesario que confirme la configuración del perfil de autenticación o el perfil de servidor antes de realizar la prueba.

STEP 2 | Inicie sesión en la CLI del cortafuegos.

STEP 3 | (Cortafuegos con varios sistemas virtuales) Defina el sistema virtual de destino al que accederá el comando de comprobación.

Esto necesario en el caso de los cortafuegos con varios sistemas virtuales para que el comando de autenticación de comprobación pueda ubicar el usuario que comprobará.

Defina el sistema virtual de destino ingresando lo siguiente:

```
admin@PA-325060> set system setting target-vsys <vsys-name>
```

Por ejemplo, si el usuario se define en vsys2, introduzca lo siguiente:

```
admin@PA-3250> set system setting target-vsys vsys2
```

*La opción **target-vsys** depende de la sesión de inicio de sesión; el cortafuegos borra la opción cuando cierra sesión.*

STEP 4 | Compruebe el perfil de autenticación introduciendo el siguiente comando:

```
admin@PA-3250> test authentication authentication-profile <authentication-
profile-name> username <username> password
```

Por ejemplo, para probar un perfil de autenticación denominado **my-profile** para un usuario denominado **bsimpson**, introduzca lo siguiente:

```
admin@PA-3250> test authentication authentication-profile my-profile
 username bsimpson password
```

*Cuando ejecuta el comando **test**, los nombres de los perfiles de autenticación y los perfiles de servidor distinguen entre mayúsculas y minúsculas. Además, si un perfil de autenticación tiene definido un modificador de nombre de usuario, debe escribir el modificador con el nombre de usuario. Por ejemplo, si agrega el modificador de nombre de usuario %USERINPUT%@%USERDOMAIN% para un usuario llamado bsimpson y el*

© 2020 Palo Alto Networks, Inc.

nombre de dominio es mydomain.com, escriba bsimpson@mydomain.com como nombre de usuario. Esto garantiza que el cortafuegos envíe las credenciales correctas al servidor de autenticación. En este ejemplo, mydomain.com es el dominio que define en el campo User Domain (Dominio de usuario) en el perfil de autenticación.

STEP 5 | Vea los resultados de la prueba.

Si el perfil de autenticación se configura correctamente, los resultados indican `Autenticación correcta`. Si hay un problema de configuración, los resultados muestran información que le ayuda a solucionar los problemas de configuración.



Los resultados varían en función de varios factores relacionados con el tipo de autenticación que está comprobando, así como el tipo de problema. Por ejemplo, RADIUS y TACACS+ usan diferentes bibliotecas subyacentes, de modo que un mismo problema que exista en ambos tipos producirá diferentes errores. Además, si hay un problema en la red, como el uso de una dirección IP o puerto incorrecto en el perfil del servidor de autenticación, el error de salida no es específico. Esto se debe a que el comando de prueba no puede realizar el protocolo inicial entre el cortafuegos y el servidor de autenticación para determinar detalles sobre el problema.

© 2020 Palo Alto Networks, Inc.

Política de autenticación

La política de autenticación le permite autenticar a los usuarios finales antes de que accedan a los servicios y las aplicaciones. Cada vez que un usuario solicita un servicio o aplicación (como al visitar una página web), el cortafuegos evalúa la política de autenticación. Según la regla de la política de autenticación correspondiente, el cortafuegos le pide al usuario que se autentique con uno o más métodos (factores), como inicio de sesión y contraseña, voz, SMS, envío o autenticación de contraseñas de una sola vez (OTP). En el caso del primer factor, los usuarios se autentican mediante un formulario web en el portal de autenticación. En el caso de los factores adicionales, los usuarios se autentican mediante una página de inicio con autenticación multifactor (MFA).



Para implementar la política de autenticación de GlobalProtect, consulte la Configuración de GlobalProtect para facilitar las notificaciones de la autenticación multifactor*.*

Después de que el usuario se autentique en todos los factores, el cortafuegos evaluará la Política de seguridad para determinar si se debe permitir el acceso al servicio o aplicación.

Para reducir la frecuencia de los desafíos de autenticación que interrumpen el flujo de trabajo del usuario, puede especificar el período de tiempo de espera durante el cual el usuario se autentica únicamente para el acceso inicial a los servicios y las aplicaciones, no para el próximo acceso. La política de autenticación se integra con el portal de autenticación para registrar las marcas de tiempo que se utilizan para evaluar el tiempo de espera y para permitir políticas e informes basados en los usuarios.

En función de la información del usuario que recoge el cortafuegos durante la autenticación, User-ID crea una nueva asignación de dirección IP a nombre de usuario o actualiza la asignación existente para ese usuario (si la información de la asignación se modificó). El cortafuegos genera logs de User-ID para registrar las adiciones y las actualizaciones. Además, el cortafuegos genera un log de autenticación para cada solicitud que corresponda a una regla de autenticación. Si prefiere la supervisión centralizada, puede configurar informes basados en User-ID o logs de autenticación, y enviar los logs a Panorama o a servicios externos como haría en el caso de otros tipos de logs.

- Marcas de tiempo de la autenticación
- Configuración de la información de autenticación

Marcas de tiempo de la autenticación

Cuando se configura una regla de la política de autenticación, puede especificar el período de tiempo de espera durante el cual el usuario se autentica únicamente para el acceso inicial a los servicios y las aplicaciones, no para el próximo acceso. Su objetivo es especificar un tiempo de espera que brinde un equilibrio entre la necesidad de proteger los servicios y las aplicaciones, y la necesidad de minimizar las interrupciones en el flujo de trabajo del usuario. Cuando un usuario se autentica, el cortafuegos registra una marca de tiempo para el primer desafío de autenticación (factor) y una marca de tiempo para cada los factores de autenticación multifactor (MFA) adicionales. Cuando, posteriormente, el usuario solicita servicios y aplicaciones que correspondan a la regla de autenticación, el cortafuegos evalúa el tiempo de espera especificado en la regla asociada a cada marca de tiempo. Esto significa que el cortafuegos vuelve a emitir desafíos de autenticación para cada factor cuando se venzan los tiempos de espera. Si realiza la Redistribución de las asignaciones de usuario y la autenticación de las marcas de tiempo, todos los cortafuegos aplicarán los tiempos de espera de la política de autenticación de manera uniforme para todos los usuarios.



El cortafuegos registra una marca de tiempo independiente para cada proveedor de MFA. Por ejemplo, si utiliza servidores Duo v2 *y PingID para emitir desafíos para factores de MFA, el cortafuegos registra una marca de tiempo para la respuesta de factor Duo y una marca de tiempo para el factor de PingID.*

© 2020 Palo Alto Networks, Inc.

En el período del tiempo de espera, un usuario que se autentica correctamente para una regla de autenticación puede acceder a los servicios o las aplicaciones que protegen otras reglas. Sin embargo, esta portabilidad se aplica únicamente a las reglas que activan los mismos factores de autenticación. Por ejemplo, un usuario que se autentica correctamente para un regla que activa la autenticación TACACS+ debe autentificarse nuevamente para una regla que active una autenticación SAML, incluso si las solicitudes de acceso se encuentran dentro del período de tiempo de espera para ambas reglas.

Cuando se evalúa el tiempo de espera en cada regla de autenticación y el temporizador global definido en la configuración del portal de autenticación (consulte Configuración del portal de autenticación), el cortafuegos le pide al usuario que se vuelva a autenticar para la configuración que venza primero. Tras la nueva autenticación, el cortafuegos registra las nuevas marcas de tiempo de autenticación para las reglas y vuelve a establecer el recuento de tiempo del temporizador del portal de autenticación. Por lo tanto, para habilitar diferentes períodos de tiempo de espera para diferentes reglas de autenticación, establezca el temporizador del portal de autenticación en un valor similar o mayor al tiempo de espera de cualquier regla.

Configuración de la información de autenticación

Siga los pasos a continuación para configurar la política de autenticación para los usuarios finales que acceden a servicios a través del portal de autenticación. Antes de comenzar, asegúrese de que su Política de seguridad permita a los usuarios acceder a los servicios y categorías de URL que requieren autenticación.

STEP 1 | Configuración del portal de autenticación. Si utiliza servicios de autenticación Multi-Factor (Multi-Factor Authentication, MFA) para autenticar usuarios, debe configurar el **Mode (Modo)** en **Redirect (Redirigir)**.

STEP 2 | Configure el cortafuegos para usar uno de los siguientes servicios para autenticar a los usuarios.

- Servicios de autenticación externa: configure un perfil de servidor para definir de qué manera el cortafuegos se conecta con el servicio.
- Autenticación de la base de datos local: añada cada cuenta de usuario a la base de datos de usuario local en el cortafuegos.
- Inicio de sesión único (SSO) de Kerberos: cree un keytab Kerberos para el cortafuegos. Opcionalmente, puede configurar el cortafuegos para usar el SSO de Kerberos como el servicio de autenticación primario y, si se producen fallos del SSO, volver al servicio externo o la autenticación de la base de datos local.

STEP 3 | Configure un perfil y secuencia de autenticación para cada conjunto de usuarios y reglas de política de autenticación que requieran los mismos servicios y ajustes de autenticación.

Seleccione el **Type (Tipo)** de servicio de autenticación y los ajustes relacionados:

- **Servicio externo**: seleccione el **Type (Tipo)** de servidor externo y seleccione el **Server Profile (Perfil de servidor)** que creó para él.
- **Autenticación de base de datos local**: configure el **Type (Tipo)** en **Local Database (Base de datos local)**. En la configuración **Advanced (Avanzado)**, seleccione **Add (Añadir)** para añadir los usuarios de portal de autenticación y los grupos de usuario que creó.
- **SSO de Kerberos**: especifique el **Kerberos Realm (Dominio Kerberos)** y seleccione **Import (Importar)** para importar el **Kerberos Keytab**.

STEP 4 | Configure un objeto de cumplimiento de autenticación.

El objeto asocia cada perfil de autenticación con un método de portal de autenticación. El método determina si el primer desafío de autenticación (factor) es transparente o requiere una respuesta del usuario.

1. Seleccione **Objects (Objetos)** > **Authentication (Autenticación)** y **Add (Añadir)** para añadir un objeto.

© 2020 Palo Alto Networks, Inc.

2. Introduzca un nombre en **Name** para identificar el objeto.
3. Seleccione un **Authentication Method (Método de autenticación)** para el **Type (Tipo)** de servicio de autenticación que especificó en el perfil de autenticación:
   - **browser-challenge (comprobación del navegador)** : seleccione este método si desea que el navegador del cliente responda al primer factor de autenticación, en lugar de solicitar al usuario que ingrese sus credenciales de inicio de sesión. Para este método, debe configurar el SSO de Kerberos en el perfil de autenticación. Si la comprobación del navegador falla, el cortafuegos vuelve al método **web-form**.
   - **web-form**: seleccione este método si desea que el cortafuegos muestre un formulario web de portal de autenticación para los usuarios que ingresan las credenciales de inicio de sesión.
4. Seleccione el **Authentication Profile (Perfil de autenticación)** que configuró.
5. Introduzca el **Message (Mensaje)** que el formulario web del portal de autenticación mostrará para indicar a los usuarios cómo autenticarse con el primer factor de autenticación.
6. Haga clic en **OK (Aceptar)** para guardar el objeto.

STEP 5 | Configure una regla de política de autenticación.

Configure un perfil para cada conjunto de usuarios, servicios y categorías de URL que requieran los mismos servicios y ajustes de autenticación.

El cortafuegos no aplica el tiempo de espera del portal de autenticación si su política de autenticación utiliza objetos de cumplimiento de autenticación predeterminados (por ejemplo, default-browser-challenge). Para requerir que los usuarios se vuelvan a autenticar después del tiempo de espera del portal de autenticación, clone la regla para el objeto de autenticación predeterminado y muévala antes de la regla existente para el objeto de autenticación predeterminado.

1. Seleccione **Policies (Políticas)** > **Authentication (Autenticación)** y luego **Add (Añadir)** para añadir una regla.
2. Introduzca un nombre en **Name** para identificar la regla.
3. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir zonas específicas, o seleccione **Any (Cualquiera)** para seleccionar cualquier zona o dirección IP.

   La regla se aplica únicamente al tráfico proveniente de las direcciones IP identificadas o de las interfaces en las zonas especificadas.
4. Seleccione **User (Usuario)** y seleccione o añada, haciendo clic en **Add (Añadir)**, los grupos de usuario a los cuales se aplica la regla (el valor predeterminado es **any [cualquiera]**).
5. Seleccione o añada, haciendo clic en **Add (Añadir)**, los perfiles de información de hosts a los cuales se aplica la regla (el valor predeterminado es **any [cualquiera]**).
6. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir zonas y direcciones IP específicas, o seleccione **Any (Cualquiera)** para seleccionar cualquier zona o dirección IP.

   La direcciones IP pueden ser recursos (como servidores) para los cuales usted desea controlar el acceso.
7. Seleccione **Service/URL Category (Categoría de URL/servicio)** y seleccione o añada, haciendo clic en **Add (Añadir)**, los servicios y grupos de servicio para los cuales la regla controla el acceso (el valor predeterminado es **service-http**).
8. Seleccione o añada, haciendo clic en **Add (Añadir)**, las categorías URL para las cuales la regla controla el acceso (el valor predeterminado es **any [cualquiera]**). Por ejemplo, puede crear una categoría URL personalizada que especifique sus sitios internos más sensibles.
9. Seleccione **Actions (Acciones)** y seleccione el objeto de **Authentication Enforcement (Cumplimiento de la autenticación)** que creó.

© 2020 Palo Alto Networks, Inc.

10. Especifique el periodo de **Timeout (Tiempo de espera)** en minutos (el valor predeterminado es 60) durante el cual el cortafuegos indica al usuario que se autentique solo una vez para el acceso repetido a los servicios y aplicaciones.

   Timeout (Tiempo de espera) es un término medio entre una seguridad más estricta (menos tiempo entre los mensajes de autenticación) y la experiencia del usuario (más tiempo entre los mensajes de autenticación). Una autenticación más frecuente a menudo es la opción correcta para acceder a sistemas críticos y áreas sensibles, tales como un centro de datos. Una autenticación menos frecuente a menudo es la opción correcta en el perímetro de red y para empresas en las cuales la experiencia del usuario es un factor clave.

11. Haga clic en **OK (Aceptar)** para guardar la regla.

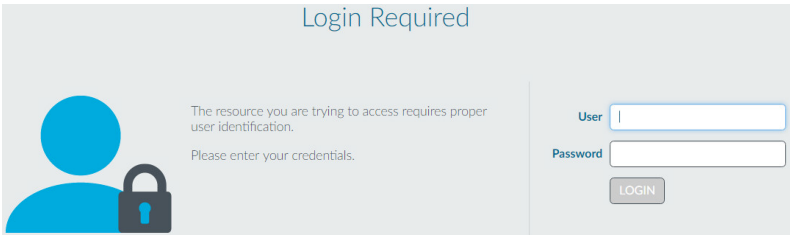
STEP 6 | (MFA únicamente) Personalice la página de inicio de sesión de MFA.

El cortafuegos muestra esta página para que los usuarios puedan autenticarse para cualquier factor MFA adicional.

STEP 7 | Verifique que el cortafuegos aplique la política de autenticación.

1. Inicie sesión en su red como uno de los usuarios de origen especificados en la regla de la política de autenticación.
2. Solicite un servicio o categoría de URL que coincida con lo que especificó en la regla.

   El cortafuegos muestra el formulario web del portal de autenticación para el primer factor de autenticación. Por ejemplo:



   Si configuró el cortafuegos para que utilice uno o más servicios MFA, autentíquese para los factores de autenticación adicionales.

3. Finalice la sesión para la URL o servicio a los que acaba de acceder.
4. Inicie una nueva sesión para el mismo servicio o aplicación. Asegúrese de realizar este paso dentro del periodo de **Timeout (Tiempo de espera)** que configuró en la regla de autenticación.

   El cortafuegos permite el acceso sin una nueva autenticación.
5. Espere hasta que el periodo de **Timeout (Tiempo de espera)** caduque y solicite el mismo servicio o aplicación.

   El cortafuegos le solicita que vuelva a autenticarse.

STEP 8 | (Opcional) Redistribución de las marcas de tiempo de autenticación y datos a otros cortafuegos que hacen cumplir la política de autenticación para garantizar que todos apliquen los tiempos de espera de manera coherente para todos los usuarios.

© 2020 Palo Alto Networks, Inc.

Solución de problemas de autenticación

Cuando los usuarios no pueden autenticarse en un cortafuegos de Palo Alto Networks o en Panorama, o el proceso de autenticación tarda más de lo esperado, un análisis de la información de autenticación puede ayudar a determinar si el fallo o retraso se deben a las siguientes variables:

- Comportamiento del usuario: Por ejemplo, los usuarios quedan bloqueados tras introducir credenciales erróneas o cuando hay un alto volumen de usuarios intentando acceder de manera simultánea.
- Problemas de red o del sistema: Por ejemplo, cuando un servidor de autenticación no es accesible.
- Problemas de configuración: Por ejemplo, la Lista de permitidas de un perfil de autenticación no tiene todos los usuarios que debería.

Los siguientes comandos de la CLI muestran información que puede ayudarle a resolver estos problemas:

Tarea	Comando

Muestra el número de cuentas de usuario bloqueadas asociadas con el perfil de autenticación (**auth-profile**), la secuencia de autenticación (**is-seq**) o el sistema virtual (**vsys**).
 	
Para desbloquear usuarios, utilice el siguiente comando operativo:
 	
`> request authentication [unlock-admin | unlock-user]`
	`PA-220> show authentication locked-users`
	`{`
	`vsys <value> |`
	`auth-profile <value> |`
	`is-seq`
	`{yes | no}`
	`{auth-profile | vsys} <value>`
	`}`

Use el comando **debug authentication** para solucionar problemas con eventos de autenticación.
 	
Use las opciones **show** para mostrar estadísticas de solicitud de autenticación y en nivel de depuración actual:
 	
• **show** muestra el nivel de depuración actual para el servicio de autenticación (authd).
• **show-active-requests** muestra la cantidad de comprobaciones activas de solicitudes de autenticación, listas de permitidos, cuentas de usuario bloqueadas y solicitudes de autenticación multifactor (Multi-Factor Authentication, MFA).
• **show-pending-requests** muestra la cantidad de comprobaciones pendientes de solicitudes de autenticación, listas de permitidos, cuentas de usuario bloqueadas y solicitudes de MFA.
• **connection-show** muestra las estadísticas de respuestas y solicitudes de autenticación para
	`PA-220> debug authentication`
	`{`
	`on {debug | dump | error | info | warn} |`
	`show |`
	`show-active-requests |`
	`show-pending-requests |`
	`connection-show |`
	`{`
	`connection-id |`
	`protocol-type`
	`{`
	`Kerberos connection-id <value> |`
	`LDAP connection-id <value> |`
	`RADIUS connection-id <value> |`
	`TACACS+ connection-id <value> |`
	`}`
	`connection-debug-on |`
	`{`
	`connection-id |`
	`debug-prefix |`

© 2020 Palo Alto Networks, Inc.

Tarea	Comando
todos los servidores de autenticación o de un tipo de protocolo específico. Use las opciones de **`connection-debug`** para habilitar o deshabilitar la depuración de autenticación: • Use la opción **`on`** para habilitar o bien **`off`** para deshabilitar la depuración de autenticación. • Use la opción **`connection-debug-on`** para habilitar o bien **`connection-debug-off`** para deshabilitar la depuración de todos los servidores de autenticación o para un tipo de protocolo específico.	`protocol-type { Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-off | { connection-id | protocol-type { Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-on }`
Pruebe la conexión y la validez del perfil de certificado.	`PA-220> test authentication authentication-profile auth-profile username <username>password <password>`
Solucione los problemas de una autenticación específica utilizando la **Authentication ID (ID de autenticación)** que se muestra en **Monitor (Supervisar)** > **Logs (Logs)** > **Authentication (Autenticación)**.	`PA-220> grep <Authentication ID>`

Gestión de certificados

Los siguientes temas describen los distintos certificados y claves que utilizan los cortafuegos y Panorama de Palo Alto Networks®, así como el modo de obtenerlos y gestionarlos:

- Claves y certificados
- Entidades de certificación (CA) de confianza predeterminadas
- Revocación de certificados
- Implementación de certificados
- Configuración de la verificación del estado de revocación de certificados
- Configuración de la clave maestra
- Cifrado de la clave maestra
- Obtención de certificados
- Exportación de un certificado y una clave privada
- Configuración de un perfil de certificado
- Configuración de un perfil de servicio SSL/TLS
- Configuración de un perfil de servicio SSH
- Sustitución del certificado para el tráfico de gestión entrante
- Configuración del tamaño de clave para los certificados de servidor proxy SSL de reenvío
- Revocación y renovación de certificados
- Claves seguras con módulos de seguridad de hardware

© 2020 Palo Alto Networks, Inc.

Claves y certificados

Para garantizar la confianza entre las partes de una sesión de comunicación segura, los cortafuegos y Panorama de Palo Alto Networks utilizan certificados digitales. Cada certificado contiene una clave criptográfica para cifrar el texto sin formato o descifrar el texto cifrado. Cada certificado también incluye una firma digital para autenticar la identidad del emisor. Este debe estar incluido en la lista de entidades de certificación (CA) de confianza de la parte que realiza la autenticación. De manera opcional, la parte que realiza la autenticación verifica que el emisor no haya revocado el certificado (consulte Revocación de certificados).

Panorama y los cortafuegos de Palo Alto Networks utilizan certificados en las siguientes aplicaciones:

- Autenticación de usuarios para el portal de autenticación, la autenticación multifactor (MFA, Multi-factor Authentication) y el acceso a la interfaz web de un cortafuegos o Panorama.
- Autenticación de dispositivos para VPN de GlobalProtect (de usuario remoto a sitio o gran escala).
- Autenticación de dispositivos para VPN de sitio a sitio de IPSec con intercambio de claves de Internet (IKE).
- Validación de listas dinámicas externas (external dynamic list, EDL).
- Acceso a los agentes de User-ID y de TS.
- Descifrado de tráfico SSL entrante y saliente.

  Un cortafuegos descifra el tráfico para aplicar reglas de políticas y, a continuación, vuelve a cifrarlo antes de reenviar el tráfico al destino definitivo. Para el tráfico saliente, el cortafuegos actúa como servidor proxy de reenvío, estableciendo una conexión SSL/TLS con el servidor de destino. Para proteger una conexión entre sí mismo y el cliente, el cortafuegos utiliza un *certificado de firma* para generar automáticamente una copia del certificado del servidor de destino.

La tabla siguiente describe las claves y los certificados que utilizan Panorama y los cortafuegos de Palo Alto Networks. Una práctica recomendada es utilizar diferentes claves y certificados para cada uso.

Table 1: Claves/certificados de dispositivo de Palo Alto Networks

Uso de clave/ certificado	Description (Descripción)
Acceso administrativo	Un acceso seguro a las interfaces de administración de cortafuegos o Panorama (acceso HTTPS a la interfaz web) requiere un certificado de servidor para la interfaz MGT (o una interfaz designada en el plano de datos si el cortafuegos o Panorama no utiliza una interfaz de gestión) y, opcionalmente, un certificado para autenticar al administrador.
Portal de autenticación	En las implementaciones en las que la política de autenticación identifique a los usuarios que accedan a recursos HTTPS, designe un certificado de servidor para la interfaz de portal de autenticación. Si configura el portal de autenticación para que utilice certificados para identificar a los usuarios (en lugar de, o además de la autenticación interactiva), implemente también certificados cliente. Para obtener más información sobre el portal de autenticación, consulte Asignación de direcciones IP a nombres de usuario mediante un portal de autenticación.
Reenvío fiable	Para el tráfico SSL/TLS saliente, si un cortafuegos que actúa como proxy de reenvío confía en la CA que firmó el certificado del servidor de destino, el cortafuegos utiliza el certificado de CA fiable de reenvío para generar una copia del certificado del servidor de destino y enviarla al cliente. Para

© 2020 Palo Alto Networks, Inc.

Uso de clave/ certificado	Description (Descripción)
	configurar el tamaño de la clave privada, configure el tamaño de clave para los certificados de servidor proxy SSL de reenvío. Para mayor seguridad, almacene la clave en un módulo de seguridad de hardware (si desea información detallada, consulte Claves seguras con un módulo de seguridad de hardware).
Reenvío no fiable	Para el tráfico SSL/TLS saliente, si un cortafuegos que actúa como proxy de reenvío no confía en la CA que firmó el certificado del servidor de destino, el cortafuegos utiliza el certificado de CA no fiable de reenvío para generar una copia del certificado del servidor de destino y enviarla al cliente.
Inspección de entrada SSL	Claves que descifran el tráfico SSL/TLS entrante para su inspección y la aplicación de la política. Para esta aplicación, importe en el cortafuegos una clave privada para cada servidor que esté sujeto a una inspección entrante SSL/TLS. Consulte Configuración de la inspección de entrada SSL. *Desde la versión PAN-OS 8.0, los cortafuegos emplean el algoritmo Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) para realizar comprobaciones estrictas de los certificados. Eso significa que, si el cortafuegos usa un certificado intermedio, debe volver a importarlo al cortafuegos desde el servidor web después de actualizar a PAN-OS 8.0 o a una versión posterior y combinar el certificado del servidor con el certificado intermedio (es decir, instalar un certificado encadenado). Si no lo hace, fallan las sesiones de inspección de entrada de SSL que incluyen un certificado intermedio en la cadena. Para instalar un certificado encadenado:* 1. *Abra cada uno de los archivos de certificado (.cer) en un editor de texto, como el Bloc de notas.* 2. *Pegue todos los certificados seguidos con el certificado del servidor en primer lugar.* 3. *Guarde los cambios como un archivo de texto (.txt) o de certificado (.cer); tenga en cuenta que el nombre no puede incluir espacios en blanco.* 4. *Importe el certificado combinado (encadenado) al cortafuegos.*
Certificado SSL de exclusión	Certificados de servidores que deben excluirse del descifrado SSL/TLS. Por ejemplo, si habilita el descifrado SSL pero su red incluye servidores para los que el cortafuegos no debería descifrar el tráfico (por ejemplo, servicios web para sus sistemas de RR.'A0;HH.), importe los correspondientes certificados en el cortafuegos y configúrelos como certificados SSL de exclusión. Consulte Exclusiones de descifrado.
GlobalProtect	Todas las interacciones entre componentes de GlobalProtect se producen en conexiones de SSL/TLS. Por lo tanto, como parte de la implementación de GlobalProtect, implemente certificados de servidor para todos los portales, gateways y gestores de seguridad móvil de GlobalProtect. Opcionalmente, implemente certificados también para los usuarios que realizan la autenticación.

© 2020 Palo Alto Networks, Inc.

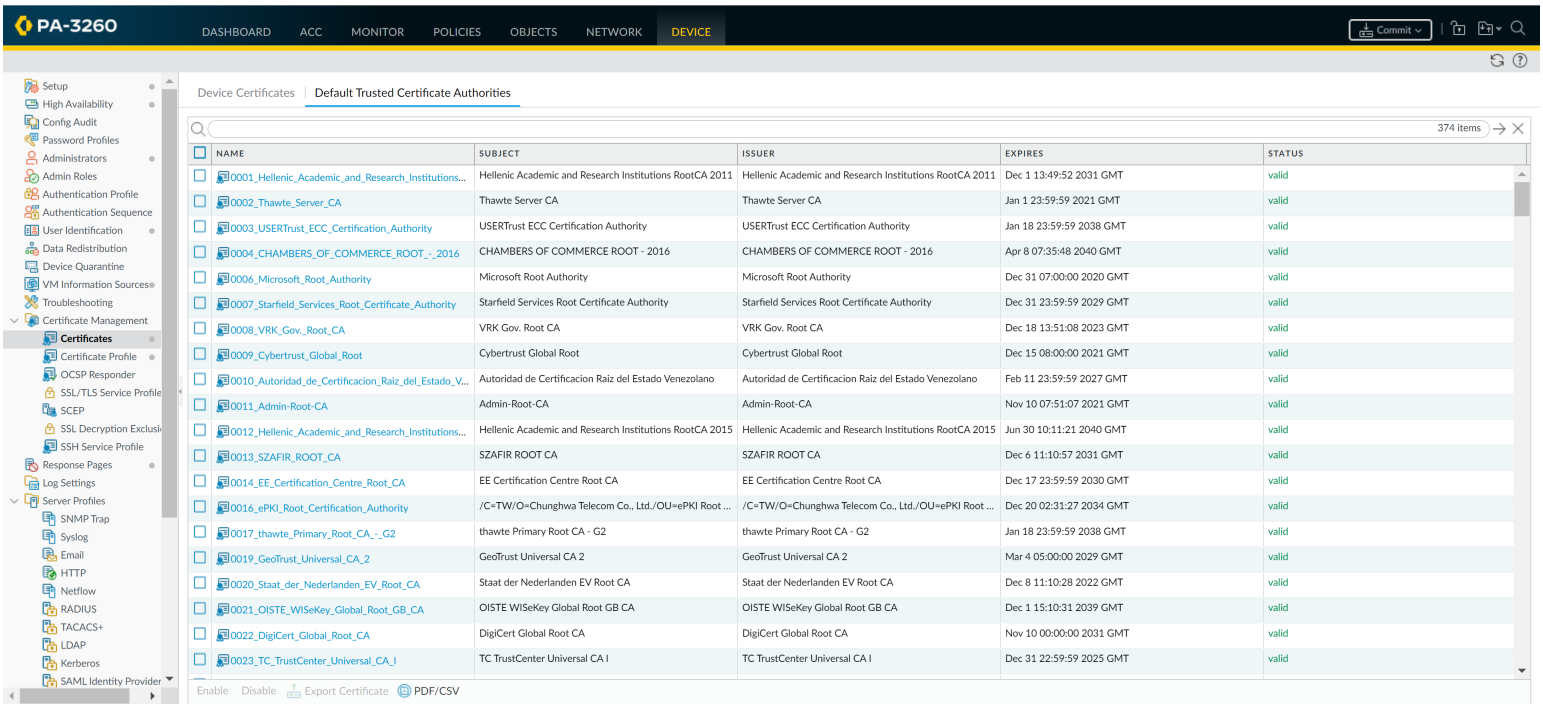
Uso de clave/ certificado	Description (Descripción)
	 *La característica de VPN de gran escala (Large Scale VPN, LSVPN) de GobalProtect requiere un certificado con firma CA.*
VPN de sitio a sitio (IKE)	En una implementación de VPN de sitio a sitio de IPSec, los dispositivos de peer utilizan gateways de intercambio de claves de Internet (IKE) para establecer un canal seguro. Las gateways de IKE utilizan certificados o claves precompartidas para autenticar los peers entre sí. Los certificados o las claves se configuran y asignan al definir una gateway de IKE en un cortafuegos. Consulte Descripción general de VPN de sitio a sitio.
Clave maestra	El cortafuegos utiliza una clave maestra para cifrar todas las claves privadas y contraseñas. Si su red requiere una ubicación segura para almacenar claves privadas, puede utilizar una clave de cifrado (ajuste) almacenada en un módulo de seguridad de hardware (HSM) para cifrar la clave maestra. Para conocer más detalles, consulte Cifrado de una clave maestra utilizando un HSM.
Syslog seguro	Certificado para habilitar conexiones seguras entre el cortafuegos y un servidor Syslog. Consulte Descripciones de los campos de Syslog.
CA raíz de confianza	Designación de un certificado raíz emitido por una CA en la que confía el cortafuegos. El cortafuegos puede utilizar un certificado de CA raíz autofirmado para emitir certificados automáticamente para otras aplicaciones (por ejemplo, proxy de reenvío SSL). Asimismo, si un cortafuegos debe establecer conexiones seguras con otros cortafuegos, la CA raíz que emite sus certificados debe estar incluida en la lista de CA raíz de confianza del cortafuegos.
Comunicación interdispositivo	De manera predeterminada, Panorama, los cortafuegos y los recopiladores de logs usan un conjunto de certificados predefinidos para las conexiones SSL/TLS utilizadas para la gestión y el reenvío de logs. Sin embargo, usted puede mejorar esta conexión al implementar certificados personalizados a los dispositivos en su implementación. Estos certificados también pueden usarse para garantizar la conexión SSL/TLS entre los peers HA de Panorama.

© 2020 Palo Alto Networks, Inc.

Entidades de certificación (CA) de confianza predeterminadas

El cortafuegos confía en las entidades de certificación (Certificate Authorities, CA) más frecuentes de manera predeterminada. Estos proveedores de certificados de confianza son responsables de emitir los certificados que requiere el cortafuegos para asegurar conexiones a internet.

Para ver y gestionar la lista de CA en las que confía el cortafuegos, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Entidades de certificación de confianza predeterminadas)**:



Las únicas CA adicionales que es posible que desee añadir son las CA empresariales de confianza que requiere su organización; consulte Obtención de certificados.

© 2020 Palo Alto Networks, Inc.

Revocación de certificados

Panorama y los cortafuegos de Palo Alto Networks utilizan certificados digitales para garantizar la confianza entre las partes de una sesión de comunicación segura. La configuración de un cortafuegos o Panorama para que compruebe el estado de revocación de certificados ofrece seguridad adicional. Una parte que presente un certificado revocado no es fiable. Cuando un certificado forma parte de una cadena, el cortafuegos o Panorama comprueban el estado de cada certificado de la cadena, excepto el certificado de CA raíz, cuyo estado de revocación no puede verificar el dispositivo.

Diversas circunstancias pueden invalidar un certificado antes de la fecha de vencimiento. Algunos ejemplos son un cambio de nombre, un cambio de asociación entre el sujeto y la entidad de certificación (por ejemplo, un empleado cuyo contrato se resuelva) y la revelación (confirmada o sospechada) de la clave privada. En estas circunstancias, la entidad de certificación que emitió el certificado deberá revocarlo.

Panorama y los cortafuegos de Palo Alto Networks admiten los siguientes métodos para verificar el estado de revocación de certificados. Si configura los dos métodos, el cortafuegos o Panorama primero intentará utilizar el método OCSP; si el servidor OCSP no está disponible, utilizará el método CRL.

- Lista de revocación de certificados (CRL)
- Protocolo de estado de certificado en línea (OCSP)



En PAN-OS, la verificación del estado de revocación de certificados es una función opcional. Para verificar que no se haya revocado el certificado, se recomienda habilitarla en los perfiles de certificados, que definen la autenticación de usuarios y dispositivos en el portal de autenticación, GlobalProtect, la VPN de sitio a sitio de IPSec o el acceso a la interfaz web del cortafuegos o Panorama.

Lista de revocación de certificados (CRL)

Cada entidad de certificación (CA) emite periódicamente una lista de revocación de certificados (CRL) en un repositorio público. La CRL identifica los certificados revocados por su número de serie. Después de que la CA revoque un certificado, la siguiente actualización de la CRL incluirá el número de serie de ese certificado.

El cortafuegos de Palo Alto Networks descarga y guarda en caché la última emisión de la CRL de cada CA incluida en la lista de CA de confianza del cortafuegos. El almacenamiento en caché solamente se aplica a certificados validados; si un cortafuegos nunca validó un certificado, el cortafuegos no almacenará la CRL para la CA de emisión. Asimismo, la caché solamente almacena una CRL hasta que vence.

El cortafuegos admite las CRL solo en formato de reglas de codificación distinguida (DER). Si el cortafuegos descarga una CRL en cualquier otro formato (como en formato de correo con privacidad mejorada o PEM), cualquier proceso de verificación de revocaciones que use esa CRL fallará cuando un usuario realice una actividad que active el proceso (por ejemplo, el envío de datos SSL salientes). El cortafuegos generará un log de sistema para el fallo de verificación. Si la verificación se aplicaba a un certificado SSL, el cortafuegos también mostrará la página de respuesta de notificación de errores de certificados SSL al usuario.



Si configura varios puntos de distribución de CRL (CRL distribution point, CDP) y el cortafuegos no logra acceder al primero, no comprueba los demás. Para redirigir las solicitudes de CRL que no sean válidas, configure un proxy DNS *como servidor alternativo.*

Para usar CRL para comprobar el estado de verificación de los certificados usados para el descifrado de tráfico SSL/TLS entrante/saliente, consulte la Configuración de la verificación de estado de certificados usados para el descifrado de SSL/TLS.

Para utilizar las CRL para verificar el estado de revocación de certificados que autentiquen usuarios y dispositivos, configure un perfil de certificado y asígnelo a las interfaces específicas de la aplicación: portal de autenticación, GlobalProtect (de usuario remoto a sitio o gran escala), VPN de sitio a sitio de IPSec o

© 2020 Palo Alto Networks, Inc.

acceso a la interfaz web de Panorama o cortafuegos de Palo Alto Networks. Si desea información detallada, consulte la Configuración de la verificación del estado de revocación de los certificados.

Protocolo de estado de certificado en línea (OCSP)

Al establecer una sesión SSL/TLS, los clientes pueden utilizar el protocolo de estado de certificado en línea (OCSP) para comprobar el estado de revocación del certificado de autenticación. El cliente de autenticación envía una solicitud que contiene el número de serie del certificado al respondedor OCSP (servidor). El respondedor busca en la base de datos de la entidad de certificación (CA) que emitió el certificado y devuelve una respuesta con el estado (correcto, revocado o desconocido) al cliente. La ventaja del método OCSP es que puede verificar el estado en tiempo real, en lugar de depender de la frecuencia de emisión (cada hora, diariamente o semanalmente) de las CRL.

El cortafuegos de Palo Alto Networks descarga y guarda en caché información de estado de OCSP de cada CA incluida en la lista de CA de confianza del cortafuegos. El almacenamiento en caché solamente se aplica a certificados validados; si un cortafuegos nunca validó un certificado, la caché del cortafuegos no almacenará la información de OCSP para la CA de emisión. Si su empresa tiene su propia infraestructura de clave pública (PKI), puede configurar el cortafuegos como un respondedor OCSP (consulte Configuración de un respondedor OCSP).

Para utilizar el OCSP para verificar el estado de revocación de certificados cuando el cortafuegos funcione como proxy SSL de reenvío, realice los pasos que se indican en Configuración de la verificación de estado de certificados usados para el descifrado de SSL/TLS.

Las siguientes aplicaciones utilizan certificados para autenticar usuarios y/o dispositivos: portal de autenticación, GlobalProtect (de usuario remoto a sitio o gran escala), VPN de sitio a sitio de IPSec y acceso a la interfaz web de Panorama o cortafuegos de Palo Alto Networks. Para utilizar OCSP para verificar el estado de revocación de los certificados:

- Configure un respondedor OCSP (si configura el cortafuegos como un respondedor OCSP).
- Habilite el servicio OCSP de HTTP en el cortafuegos (si configura el cortafuegos como un respondedor OCSP).
- Cree u obtenga un certificado para cada aplicación.
- Configure un perfil de certificado para cada aplicación.
- Asigne el perfil de certificado a la aplicación relevante.

Para cubrir situaciones en las que el OCSP responder no esté disponible, configure la CRL como método de retroceso. Si desea información detallada, consulte la Configuración de la verificación del estado de revocación de los certificados.

© 2020 Palo Alto Networks, Inc.

Implementación de certificados

Los enfoques básicos de implementación de certificados para Panorama o cortafuegos de Palo Alto Networks son los siguientes:

- **Obtenga certificados de una CA externa de confianza**: La ventaja de obtener un certificado de una entidad de certificación (CA) externa de confianza como VeriSign o GoDaddy es que los clientes finales ya confiarán en el certificado debido a que los exploradores comunes incluyen certificados de CA raíz de CA conocidas en sus almacenes de certificados raíz de confianza. Por lo tanto, para aplicaciones que requieran que los clientes finales establezcan conexiones seguras con Panorama o el cortafuegos de Palo Alto Networks, adquiera un certificado de una CA en la que confíen los clientes finales para no tener que implementar previamente certificados de CA raíz en los clientes finales. (Algunas de estas aplicaciones son un portal de GlobalProtect o gestor de seguridad móvil de GlobalProtect.) Sin embargo, observe que la mayoría de las CA externas no pueden emitir certificados de firma. Por lo tanto, este tipo de certificado no es adecuado para las aplicaciones (por ejemplo, descifrado SSL/TLS y VPN a gran escala) que requieran que el cortafuegos emita certificados. Consulte Obtención de un certificado desde una CA externa.
- **Obtenga certificados de una CA de empresa**: Las empresas que tengan su propia CA interna podrán utilizarla para emitir certificados para aplicaciones de cortafuegos e importarlos en el cortafuegos. La ventaja es que los clientes finales probablemente ya confíen en la CA de empresa. Puede generar los certificados necesarios e importarlos en el cortafuegos o generar una solicitud de firma de certificado (CSR) en el cortafuegos y enviarla a la CA de empresa para que la firme. La ventaja de este método es que la clave privada no abandona el cortafuegos. Un CA de empresa también puede emitir un certificado de firma, que el cortafuegos utiliza para generar certificados automáticamente (por ejemplo, para VPN a gran escala de GlobalProtect o sitios que requieran un descifrado SSL/TLS). Consulte Importación de un certificado y una clave privada.
- **Genere certificados autofirmados:** puede implementar la Creación de un certificado de CA raíz autofirmado en el cortafuegos y utilizarlo para emitir certificados automáticamente para otras aplicaciones de cortafuegos.



Si utiliza este método para generar certificados para una aplicación que requiera que un cliente final confíe en el certificado, los usuarios finales verán un error de certificado debido a que el certificado de CA raíz no está en su almacén de certificados raíz de confianza. Para evitar esto, implemente el certificado de CA raíz autofirmado en todos los sistemas de usuario final. Puede implementar los certificados manualmente o utilizar un método de implementación centralizado como un objeto de directiva de grupo (GPO) de Active Directory.

© 2020 Palo Alto Networks, Inc.

Configuración de la verificación del estado de revocación de certificados

Para verificar el estado de revocación de los certificados, el cortafuegos utiliza el protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) y/o listas de revocación de certificados (certificate revocation lists, CRL). Para obtener información detallada sobre estos métodos, consulte Revocación de certificados. Si configura ambos métodos, el cortafuegos primero intentará utilizar el OCSP y solamente volverá al método CRL si el respondedor OCSP no está disponible. Si su empresa tiene su propia infraestructura de clave pública (public key infrastructure, PKI), puede configurar el cortafuegos para que funcione como el respondedor OCSP.

Los siguientes temas describen cómo configurar el cortafuegos para verificar el estado de revocación de certificados:

- Configuración de un OCSP responder
- Configuración de la verificación del estado de revocación de los certificados
- Configuración de la verificación del estado de revocación de certificados utilizados para el descifrado SSL/TLS

Configuración de un OCSP responder

Para utilizar el protocolo de estado de certificado en línea (OCSP) para verificar el estado de revocación de certificados, debe configurar el cortafuegos para que acceda a un respondedor OCSP (servidor). La entidad que administra el respondedor OCSP puede ser una entidad de certificación (certificate authority, CA) externa. Si su empresa tiene su propia infraestructura de clave pública (public key infrastructure, PKI), puede usar respondedores OCSP externos o puede configurar el cortafuegos como un respondedor OCSP. Si desea información detallada sobre OCSP, consulte la Revocación de certificados.

STEP 1 | Defina un respondedor OCSP externo o configure el cortafuegos como un respondedor OCSP.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **OCSP Responder (Respondedor OCSP)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Nombre** para identificar al respondedor (hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, espacios, guiones y guiones bajos.
3. Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.
4. En el campo **Host Name**, introduzca el nombre de host (recomendado) o la dirección IP del respondedor OCSP. Puede introducir una dirección IPv4 o IPv6. A partir de este valor, PAN-OS deriva automáticamente una URL y la añade al certificado que se está verificando.

   Si configura el propio cortafuegos como respondedor OCSP, el nombre de host debe resolverse en una dirección IP de la interfaz que utiliza el cortafuegos para servicios de OCSP.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Si desea que el cortafuegos use la interfaz de gestión para la interfaz del respondedor OCSP, habilite la comunicación de OCSP en el cortafuegos. De lo contrario, continúe con el paso siguiente para configurar una interfaz alternativa.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
2. En la sección Configuración de interfaz de gestión, edite para seleccionar la casilla de verificación **HTTP OCSP** y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Para usar una interfaz alternativa como la interfaz del respondedor OCSP, añada un perfil de gestión de interfaz a la interfaz utilizada para servicios de OCSP.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)**.
2. Haga clic en **Añadir** para crear un nuevo perfil o haga clic en el nombre de un perfil existente.
3. Seleccione la casilla de verificación **OCSP de HTTP** y haga clic en **ACEPTAR**.
4. Seleccione **Network (Red)** > **Interfaces** y haga clic en el nombre de la interfaz que el cortafuegos utilizará para los servicios OCSP. El **Host Name (Nombre de host)** OCSP que se especifica en el paso 1 debe dirigir a una dirección IP en esta interfaz.
5. Seleccione **Advanced (Avanzada)** > **Other info (Otra información)** y seleccione el perfil de gestión de interfaz que configuró.
6. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de la verificación del estado de revocación de los certificados

El cortafuegos y Panorama utilizan certificados para autenticar usuarios y dispositivos para aplicaciones tales como portal de autenticación, GlobalProtect, VPN de sitio a sitio de IPSec y acceso a la interfaz web de Panorama o el cortafuegos de Palo Alto Networks. Para mejorar la seguridad, la práctica recomendada es configurar el cortafuegos o Panorama para que verifiquen el estado de revocación de certificados que utilicen para la autenticación de dispositivos/usuarios.

STEP 1 | Realice la Configuración de un perfil de certificado para cada aplicación.

Asigne uno o más certificados CA raíz al perfil y seleccione el modo en que el cortafuegos verifica el estado de revocación de certificados.

Si desea información detallada de los certificados que utilizan las distintas aplicaciones, consulte Claves y certificados.

STEP 2 | Asigne los perfiles de certificados a las aplicaciones relevantes.

Los pasos para asignar un perfil de certificado dependen de la aplicación que lo requiera.

Configuración de la verificación del estado de revocación de certificados utilizados para el descifrado SSL/TLS

El cortafuegos descifra el tráfico SSL/TLS entrante y saliente para inspeccionar el tráfico en busca de amenazas. Cuando cree una regla de la política de seguridad que permita el tráfico y aplique perfiles de seguridad a la regla, cree una regla de política de descifrado análoga para descifrar ese tráfico. Si no descifra el tráfico, el cortafuegos no puede utilizar los perfiles de seguridad para inspeccionar el tráfico (no puede inspeccionar lo que no puede ver). El cortafuegos vuelve a cifrar el tráfico antes de reenviarlo. (Consulte Inspección entrante de SSL y Proxy de reenvío SSL.) Puede configurar el cortafuegos para comprobar el estado de revocación de los certificados usados para la descripción como sigue.

Si habilita la verificación del estado de revocación de certificados de descifrado SSL/TLS, añadirá tiempo al proceso de establecimiento de la sesión. El primer intento de acceder a un sitio puede fallar si la verificación no termina antes de que se acabe el tiempo de espera de la sesión. Por estos motivos, la verificación está deshabilitada de manera predeterminada.

STEP 1 | Defina los intervalos de tiempo de espera específicos de servicio para las solicitudes de estado de revocación.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y, en la sección Session Features (Características de la sesión), seleccione **Decryption Certificate Revocation Settings (Configuración de revocación de certificado de descifrado)**.
2. Realice uno de los dos pasos siguientes o ambos, en función de si el cortafuegos utilizará el Protocolo de estado de certificado en línea (OCSP) o el método de Lista de revocación de certificados (CRL) para verificar el estado de revocación de los certificados. Si el cortafuegos utiliza ambos, primero intentará utilizar OCSP; si el respondedor OCSP no está disponible, entonces el cortafuegos intentará utilizar el método CRL.
   - En la sección CRL, seleccione la casilla de verificación **Habilitar** e introduzca el **Tiempo de espera de recepción**. Este es el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta del servicio CRL.
   - En la sección OCSP, seleccione la casilla de verificación **Habilitar** e introduzca el **Tiempo de espera de recepción**. Este es el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta del OCSP responder.

   Según el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** que especifique en el paso 2, es posible que el cortafuegos registre un tiempo de espera antes de que pase cualquiera de los intervalos de **Receive Timeout (Tiempo de espera de recepción)** o ambos.

STEP 2 | Defina el intervalo de tiempo de espera total para las solicitudes de estado de revocación.

Introduzca el **Tiempo de espera del estado del certificado**. Este es el intervalo (1 a 60 segundos) tras el cual el cortafuegos deja de esperar una respuesta de cualquier servicio de estado de certificado y aplica la lógica de bloqueo de sesión que puede definir de manera opcional en el paso 3. El **Certificate Status Timeout (Tiempo de espera del estado del certificado)** se relaciona con el **Receive Timeout (Tiempo de espera de recepción)** de OCSP/CRL de la manera siguiente:

- Si habilita tanto OCSP como CRL: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o la suma de los dos valores de **Receive Timeout (Tiempo de espera de recepción)**.
- Si habilita únicamente OCSP: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o el valor de **Receive Timeout (Tiempo de espera de recepción)** de OCSP.
- Si habilita únicamente CRL: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o el valor de **Receive Timeout (Tiempo de espera de recepción)** de CRL.

STEP 3 | Defina el comportamiento de bloqueo para el estado de certificado desconocido o un tiempo de espera de solicitud de estado de revocación.

Si desea que el cortafuegos bloquee sesiones SSL/TLS cuando el servicio OCSP o CRL devuelva el estado de revocación de certificados Desconocido, seleccione la casilla de verificación **Block Session With Unknown Certificate Status (Bloquear sesión con estado de certificado desconocido)**. De lo contrario, el cortafuegos continuará con la sesión.

Si desea que el cortafuegos bloquee sesiones SSL/TLS después de que registre un tiempo de espera de solicitud, seleccione la casilla de verificación **Bloquear sesión al agotar el tiempo de espera de comprobación de estado de certificado**. De lo contrario, el cortafuegos continuará con la sesión.

STEP 4 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de la clave maestra

Cada servidor de gestión de cortafuegos o de Panorama tiene una clave maestra predeterminada que cifra todas las claves privadas y contraseñas en la configuración para protegerlas (como la clave privada que se utiliza para el descifrado proxy de reenvío SSL).



Cambie la clave maestra predeterminada tan pronto como sea posible para asegurarse de que utiliza una clave maestra única para el cifrado.

En las configuraciones de alta disponibilidad (high availability, HA), debe utilizar la misma clave maestra en ambos cortafuegos o las dos instancias de Panorama del par. De lo contrario, la sincronización de HA no funcionará.

Además, si utiliza Panorama para gestionar su cortafuegos, debe utilizar la misma clave maestra en Panorama y todos los cortafuegos gestionados, de modo que Panorama pueda enviar configuraciones a los cortafuegos.

Asegúrese de almacenar la clave maestra en una ubicación segura. No puede recuperar la clave maestra y la única manera de restaurar la clave maestra predeterminada es mediante el Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica.

STEP 1 | Realice una copia de seguridad de configuración.

STEP 2 | (Solo en configuraciones de HA) Deshabilite la HA.

Es obligatorio realizar este paso antes de implementar una clave maestra nueva en un par de cortafuegos de HA. Si no deshabilita la HA antes de implementarla, Panorama pierde la conectividad al cortafuegos principal.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración.
2. Quite la marca del ajuste **Enable HA (Habilitar HA)** para deshabilitarla y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

STEP 3 | Seleccione **Device (Dispositivo)** > **Master Key and Diagnostics (Clave maestra y diagnóstico)** y edite la sección Master Key (Clave maestra).

STEP 4 | Introduzca la **Clave maestra actual**, si existe.

STEP 5 | Defina una **New Master Key (Nueva clave maestra)** y, a continuación, seleccione la acción **Confirm New Master Key (Confirmar clave maestra)**. La clave debe contener exactamente 16 caracteres.

STEP 6 | En los campos **Days (Días)** o **Hours (Horas)** de **Lifetime (Duración)**, especifique cuánto tiempo pasa antes de que venza la clave maestra.

Debe configurar una nueva clave maestra antes de que expire la clave actual. Si la clave maestra expira, el cortafuegos o Panorama se reiniciarán automáticamente en el modo Mantenimiento. Luego, deberá realizar el Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica.



Establezca la duración en dos años o menos, según la cantidad de cifrados que realice el dispositivo. Cuantos más cifrados realice un dispositivo, más corta será la duración que debe establecer. La consideración fundamental es no quedarse sin cifrados únicos antes

© 2020 Palo Alto Networks, Inc.

de cambiar la clave maestra. Cada clave maestra puede proporcionar hasta 2^{32} cifrados únicos basados en el valor de la clave maestra y el valor del vector de inicialización (IV, Initialization Vector). Después de 2^{32} cifrados únicos, los cifrados se repiten (ya no son únicos), lo que representa un riesgo para la seguridad.

Establezca un valor de Time for Reminder (Tiempo para el recordatorio) (consulte el siguiente paso) para la clave maestra y, cuando se produzca la notificación de recordatorio, cambie la clave maestra.

STEP 7 | Introduzca un **Time for Reminder (Período restante)** que especifique el número de **Days (Días)** y **Hours (Horas)** antes de que la clave maestra venza cuando el cortafuegos genere una alarma de vencimiento. El cortafuegos abre automáticamente el cuadro de diálogo System Alarms (Alarmas de sistema) para mostrar la alarma.



Configure el recordatorio para que disponga de tiempo suficiente como para configurar una nueva clave maestra antes de que caduque en una ventana de mantenimiento programada. Cuando el tiempo para el recordatorio caduque y el cortafuegos o Panorama envíe un log de notificación, cambie la clave maestra. No espere a que la duración caduque. Para dispositivos agrupados, realice un seguimiento de todos los dispositivos (por ejemplo, cortafuegos que administra Panorama y pares de HA de cortafuegos) y, cuando el valor del recordatorio expire para cualquier dispositivo del grupo, cambie la clave maestra.

Para asegurarse de que se muestre la alarma de vencimiento, seleccione Device (Dispositivo) > Log Settings (Configuración del registro), edite la configuración de las alarmas y haga clic en Enable Alarms (Habilitar alarmas).

STEP 8 | Marque **Auto Renew Master Key (Renovar clave maestra automáticamente)** para configurar el cortafuegos de modo que cambie la clave de forma automática. Para configurar **Auto Renew With Same Master Key (Renovar la misma clave maestra automáticamente)**, especifique cada cuánto se renueva la misma clave en **Days (Días)** o **Hours (Horas)**. Si se amplía la vigencia de la clave, el cortafuegos permanece operativo y sigue protegiendo la red; no implica que no deba configurar una clave nueva si la clave maestra existente vence pronto.

La renovación automática de la clave maestra tiene beneficios y riesgos. El beneficio es que ampliar la **duración** de la clave maestra le protegerá contra fallos al cambiar la clave maestra antes de que expire. El riesgo es que los cifrados se repitan y provoquen un riesgo de seguridad si el número de cifrados que realiza el dispositivo con la clave maestra supera el número de cifrados únicos que la clave maestra puede generar (2^{32} cifrados únicos).



Si la clave maestra caduca (no la renueva automáticamente y no la reemplaza de manera oportuna), el dispositivo entra en modo de mantenimiento.



Si habilita la opción Auto Renew Master Key (Renovación automática de la clave maestra), configúrela para que el tiempo total (duración más el tiempo de renovación automática) no provoque que el dispositivo se quede sin cifrados únicos. Por ejemplo, si cree que el dispositivo consumirá el número de cifrados únicos de la clave maestra en dos años y medio, puede establecer la duración en dos años, establecer el tiempo para el recordatorio en 60 días y configurar la renovación automática de la clave maestra en 60-90 días para ofrecer tiempo adicional para configurar una nueva clave maestra antes de que se extinga la duración. Sin embargo, lo recomendable sigue siendo cambiar la clave maestra antes de que expire la duración para garantizar que ningún dispositivo repita los cifrados.

© 2020 Palo Alto Networks, Inc.

Cuando configure la renovación automática de la clave maestra tras su vencimiento, tenga en cuenta cuántos días faltan hasta el siguiente intervalo de mantenimiento.

STEP 9 | (Opcional) Si desea mayor seguridad, seleccione si desea utilizar un **HSM** para cifrar la clave maestra. Para conocer más detalles, consulte Cifrado de una clave maestra utilizando un HSM.

STEP 10 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 11 | (Solo en configuraciones de HA) Vuelva a habilitar la HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración.
2. Marque **Enable HA (Habilitar HA)** y haga clic en **OK (Aceptar)**.
3. Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

© 2020 Palo Alto Networks, Inc.

Cifrado de la clave maestra

En dispositivos físicos y virtuales de Palo Alto Networks, puede configurar la clave maestra para usar el algoritmo de cifrado AES-256-CBC o AES-256-GCM (introducido en PAN-OS 10.0) para cifrar datos como claves y contraseñas. AES-256-GCM proporciona un cifrado más fuerte que AES-256-CBC y mejora su estrategia de seguridad. También incluye un control de integridad incorporado. La clave maestra utiliza el algoritmo de cifrado configurado para cifrar los datos confidenciales almacenados en el cortafuegos y en Panorama. Cuando configura el algoritmo de cifrado en AES-256-GCM, puede seguir usando un HSM para cifrar la clave maestra con una clave de cifrado almacenada en el HSM.

El algoritmo de cifrado predeterminado que utiliza la clave maestra para cifrar los datos es AES-256-CBC, el mismo algoritmo que usaba la clave maestra antes de PAN-OS 10.0. AES-256-CBC es el nivel de cifrado predeterminado porque cuando gestiona cortafuegos con Panorama, los cortafuegos gestionados pueden estar en diferentes versiones de PAN-OS, y los cortafuegos en versiones de PAN-OS anteriores a PAN-OS 10.0 no son compatibles con AES-256- GCM. Por eso, Panorama debe utilizar el nivel más bajo de cifrado que pueden utilizar sus dispositivos gestionados. Por ejemplo, si algunos dispositivos gestionados ejecutan PAN-OS 10.0 y algunos ejecutan versiones anteriores, Panorama debe usar AES-256-CBC. Sin embargo, si todos los dispositivos gestionados ejecutan PAN-OS 10.0 o posterior, Panorama y todos sus dispositivos gestionados pueden usar AES-256-GCM.

Utilice el mismo nivel de cifrado en Panorama y sus dispositivos gestionados y utilice el mismo nivel de cifrado en los pares de cortafuegos. Actualice los dispositivos para utilizar el algoritmo de cifrado más seguro posible. Si todos los dispositivos gestionados por Panorama ejecutan PAN-OS 10.0, use AES-256-GCM en todos los dispositivos. La configuración de los dispositivos gestionados o emparejados que utilizan diferentes niveles de cifrado puede desincronizarse.

Cuando cambie el algoritmo de cifrado a AES-256-GCM, los dispositivos lo utilizarán en lugar de AES-256-CBC para cifrar datos confidenciales. Cuando cambie de un algoritmo a otro, también podrá especificar si:

- Volver a cifrar los datos cifrados existentes con el nuevo algoritmo.
- Dejar los datos existentes cifrados con el antiguo algoritmo de cifrado y utilizar el nuevo algoritmo solo para cifrados nuevos (futuros).

De forma predeterminada, cuando cambie el algoritmo de cifrado, el dispositivo utilizará el nuevo algoritmo para volver a cifrar los datos cifrados existentes, así como para cifrar los datos nuevos. Si gestiona dispositivos con Panorama, es posible que estén en diferentes versiones de PAN-OS y que no admitan los algoritmos de cifrado más recientes. Asegúrese de comprender qué algoritmos de cifrado admiten Panorama y sus dispositivos gestionados antes de cambiar el algoritmo de cifrado o volver a cifrar los datos que ya se han cifrado.

- Configuración del nivel de cifrado de la clave maestra
- Cifrado de la clave maestra en un par de HA de cortafuegos
- Logs de cifrado de la clave maestra
- Cifrados de la clave maestra únicos para AES-256-GCM

Configuración del nivel de cifrado de la clave maestra

Configure el nivel de algoritmo de cifrado de clave maestra y decida si vuelve a cifrar todos los datos cifrados actualmente con un nuevo nivel de algoritmo de cifrado mediante la CLI. Dependiendo del orden de las palabras clave, puede cambiar el nivel de cifrado o realizar ese procedimiento y también especificar si volver a cifrar los datos previamente cifrados.

© 2020 Palo Alto Networks, Inc.

El siguiente comando operativo de la CLI permite cambiar el nivel de cifrado y volver a cifrar automáticamente todos los datos cifrados actualmente con el nivel de cifrado especificado:

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

El siguiente comando operativo de la CLI permite cambiar el nivel de cifrado y especificar si volver a cifrar todos los datos cifrados actualmente con el nuevo nivel de cifrado:

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|1|2>
```

Palabra clave	Opciones
level	**0** = Se utiliza el algoritmo predeterminado (AES-256-CBC) para cifrar datos. **1** = Se utiliza el algoritmo AES-256-CBC para cifrar datos. **2** = Se utiliza el algoritmo AES-256-GCM para cifrar datos. El cortafuegos vuelve a cifrar todos los datos cifrados actualmente y encripta nuevos datos confidenciales mediante el algoritmo especificado. Si no desea volver a cifrar los datos cifrados existentes con el nuevo algoritmo, especifique **re-encrypt no** en la cadena de comandos. Esto evita que el cortafuegos vuelva a cifrar automáticamente los datos que el cortafuegos ya ha cifrado. *Solo use AES-256-GCM cuando Panorama y todos sus dispositivos gestionados (o ambos dispositivos en un par de HA) utilicen PAN-OS 10.0 o superior y configuren todos los dispositivos para usar AES-256-GCM. Los dispositivos administrados o emparejados que usen diferentes niveles de cifrado pueden perder la sincronización.*
re-encrypt	**no** = No se vuelven a cifrar los datos actualmente cifrados. El cortafuegos no vuelve a cifrar los datos actualmente cifrados. Los datos cifrados actualmente permanecen encriptados con cualquier algoritmo que el cortafuegos haya usado originalmente para cifrar los datos. El cortafuegos usa el algoritmo especificado solo para cifrar datos confidenciales en el futuro. **yes** = Se vuelve a cifrar los datos cifrados actualmente con el algoritmo especificado y se utiliza ese algoritmo para cifrar datos confidenciales en el futuro.

Utilice el comando operativo de la CLI **show system masterkey-properties** para verificar el algoritmo de cifrado (nivel) configurado actualmente en el dispositivo, por ejemplo:

© 2020 Palo Alto Networks, Inc.

```
admin@PA-NGFW>show system masterkey-properties
```

```
Master key expires at: unspecified
Reminders will begin at: unspecified
Master key on hsm: no
Automatically renew master key lifetime: 0
Encryption Level: 1
```

El resultado muestra que el nivel de cifrado actual es 1, que es AES-256-CBC.

Si cambia a una versión anterior de PAN-OS, el dispositivo revierte automáticamente el algoritmo de cifrado a un nivel que admite la versión de PAN-OS anterior y vuelve a encriptar automáticamente los datos cifrados mediante ese nivel para que el dispositivo pueda descifrar y usar los datos según sea necesario. Por ejemplo, si su dispositivo funciona con PAN-OS 10.0 y utiliza AES-256-GCM como el algoritmo de cifrado (que no es compatible con versiones anteriores de PAN-OS) y cambia a PAN-OS 9.1, el dispositivo vuelve a encriptar los datos cifrados en AES-256-CBC, que es compatible con PAN-OS 9.1.

Cifrado de la clave maestra en un par de HA de cortafuegos

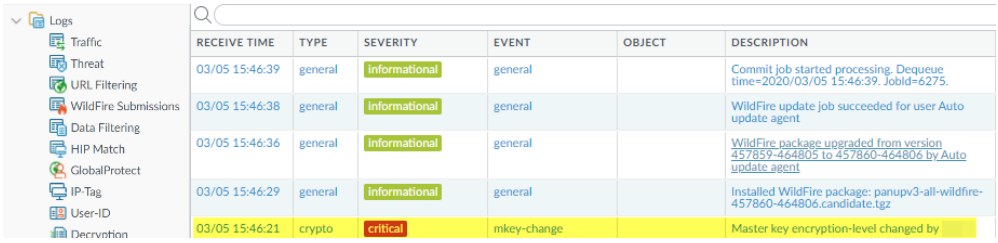
Para usar el nivel de cifrado AES-256-GCM en un par de cortafuegos de alta disponibilidad (HA, High Availability), ambos cortafuegos deben ejecutar PAN-OS 10.0 para que los dos admitan AES-256-GCM. Si alguno de los cortafuegos del par de HA ejecuta una versión anterior a PAN-OS 10.0, no podrá utilizar AES-256-GCM. Cuando ambos cortafuegos estén en PAN-OS 10.0, los dos podrá decodificar las claves de cifrado AES-256-CBC o AES-256-GCM, por lo que podrán usar el nivel de cifrado. Sin embargo, ambos cortafuegos deben usar el mismo nivel de cifrado para evitar la posibilidad de perder la sincronización.

Utilice el cifrado AES-256-GCM en ambos cortafuegos en el par de HA. Tanto si usa AES-256-GCM como AES-256-CBC, utilice el mismo algoritmo en ambos cortafuegos.

No es necesario deshabilitar HA para cambiar el nivel de cifrado en un cortafuegos en un par de HA en el que ambos cortafuegos ejecutan PAN-OS 10.0.

Logs de cifrado de la clave maestra

El cortafuegos genera un log del sistema (**Monitor [Supervisar]** > **Logs** > **System [Sistema]**) cuando cambia el algoritmo de cifrado de clave maestra (nivel).



Para ver todos los logs del sistema para el cifrado de clave maestra, cree un filtro que muestre todos los logs del **tipo** crypto: **`(subtype eq crypto)`**.

Cifrados de la clave maestra únicos para AES-256-GCM

La clave maestra solo puede generar un número finito de cifrados únicos antes de que se agoten las combinaciones únicas y deba repetir los cifrados. El cortafuegos crea cifrados únicos mediante el algoritmo

© 2020 Palo Alto Networks, Inc.

de cifrado AES-256-GCM con un vector de inicialización (IV, Initialization Vector). Un IV es un número arbitrario que solo debe usarse una vez para crear un cifrado para garantizar que cada cifrado sea único.

Los cifrados que utilizan la clave maestra y el IV deben ser únicos para evitar ataques de falsificación. El cortafuegos cumple con el requisito de exclusividad de que la probabilidad de que el cifrado autenticado se cree alguna vez con el mismo IV y la misma clave en dos o más conjuntos distintos de datos de entrada no sea superior a 2^{32}.

Cuando el IV atraviesa todos sus valores únicos, el valor de IV se repite. Cuando el valor de IV se repite, el uso de la misma clave maestra y el valor de IV repetido para cifrar los datos significa que el cifrado es el mismo que el utilizado anteriormente en otros datos. Cambie la clave maestra antes de que el sistema se quede sin cifrados únicos para evitar que el cortafuegos utilice el mismo cifrado (combinación de clave maestra y valor IV) en más de una pieza de datos confidenciales. Las combinaciones de cifrado únicas nunca deben repetirse ni reutilizarse.

Para realizar un seguimiento de cuándo necesita cambiar la clave maestra, configure los valores **Lifetime (Duración)** y **Reminder (Recordatorio)** en cada dispositivo (**Device (Dispositivo)** > **Master Key and Diagnostics (Clave maestra y diagnóstico)** y edite la clave maestra). Establezca los valores de forma conservadora, en función del volumen esperado de cifrados de clave maestra, para garantizar que todos los cifrados sean únicos y que no se repitan ni se reutilizan combinaciones de cifrado.

© 2020 Palo Alto Networks, Inc.

Obtención de certificados

- Creación de un certificado de CA raíz autofirmado
- Generar un certificado
- Importación de un certificado y una clave privada
- Obtención de un certificado desde una CA externa
- Instalación de un certificado del dispositivo
- Implementación de certificados utilizando SCEP

Creación de un certificado de CA raíz autofirmado

Un certificado de una entidad de certificación (CA) raíz autofirmado es el certificado de mayor nivel de una cadena de certificados. Un cortafuegos puede utilizar este certificado para emitir certificados automáticamente para otros usos. Por ejemplo, el cortafuegos emite certificados para el descifrado SSL/TLS y para dispositivos satélite de una VPN a gran escala de GlobalProtect.

Al establecer una conexión segura con el cortafuegos, el cliente remoto debe confiar en la CA raíz que emitió el certificado. De lo contrario, el explorador del cliente mostrará una advertencia indicando que el certificado no es válido y podría (dependiendo de la configuración de seguridad) bloquear la conexión. Para evitar esto, después de generar el certificado de CA raíz autofirmado, impórtelo en los sistemas cliente.

En un cortafuegos o Panorama de Palo Alto Networks, solo puede generar certificados autofirmados si son certificados de CA.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 2 | Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.

STEP 3 | Haga clic en **Generate (Generar)**.

STEP 4 | Introduzca el nombre en **Certificate Name (Nombre de certificado)**, por ejemplo, `GlobalProtect_CA`. Puede tener hasta 63 caracteres en el cortafuegos y hasta 31 caracteres en Panorama. Además, se distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, guiones y guiones bajos.

STEP 5 | En el campo **Common Name (Nombre común)**, introduzca el FQDN (recomendado) o la dirección IP de la interfaz en la que configurará el servicio que utilizará este certificado.

STEP 6 | Si el dispositivo tiene más de un vsys y desea que el certificado esté disponible para todos los vsys, seleccione la casilla de verificación **Shared (Uso compartido)**.

STEP 7 | Deje el campo **Firmado por** en blanco para designar el certificado como autofirmado.

STEP 8 | (Obligatorio) Seleccione la casilla de verificación **Certificate Authority (Autoridad de certificado)**.

STEP 9 | Deje en blanco el campo **OCSP Responder**; la verificación del estado de revocación de certificados no se aplica a certificados de CA raíz.

© 2020 Palo Alto Networks, Inc.

STEP 10 | Haga clic en **Generar** y **Confirmar**.

Generar un certificado

Los cortafuegos y Panorama de Palo Alto Networks utilizan certificados para autenticar clientes, servidores, usuarios y dispositivos en varias aplicaciones, incluido el descifrado SSL/TLS, portal de autenticación, GlobalProtect, VPN de sitio a sitio de IPSec y acceso a la interfaz web del cortafuegos/Panorama. Genere certificados para cada uso: si desea obtener información detallada, consulte Claves y certificados.

Para generar un certificado, debe realizar la Creación de un certificado de CA raíz autofirmado o importar uno (Importación de un certificado y una clave privada) para firmarlo. Para utilizar el protocolo de estado de certificado en línea (OCSP) para verificar el estado de revocación de certificados, realice la Configuración de un respondedor OCSP antes de generar el certificado.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 2 | Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.

STEP 3 | Haga clic en **Generate (Generar)**.

STEP 4 | Seleccione **Local** (valor predeterminado) como el **Certificate Type (Tipo de certificado)**, a menos que desee implementar certificados SCEP en endpoints GlobalProtect.

STEP 5 | Introduzca un **Certificate Name (Nombre de certificado)**. Puede tener hasta 63 caracteres en el cortafuegos y hasta 31 caracteres en Panorama. Además, se distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, guiones y guiones bajos.

STEP 6 | En el campo **Common Name (Nombre común)**, introduzca el FQDN (recomendado) o la dirección IP de la interfaz en la que configurará el servicio que utilizará este certificado.

STEP 7 | Si el dispositivo tiene más de un vsys y desea que el certificado esté disponible para todos los vsys, seleccione la casilla de verificación **Shared (Uso compartido)**.

STEP 8 | En el campo **Signed By (Firmado por)**, seleccione el certificado de CA raíz que emitirá el certificado.

STEP 9 | (Opcional) Seleccione un **OCSP Responder**.

STEP 10 | Para el **Algorithm** de generación de claves, seleccione **RSA** (por defecto) o **Elliptical Curve DSA** (DSA de curva elíptica, ECDSA). ECDSA se recomienda para navegadores de clientes y sistemas operativos compatibles.

> *Los cortafuegos que ejecutan la versión PAN-OS 6.1 o anteriores eliminarán cualquier certificado de ECDSA que envíe desde Panorama™, y ningún certificado RSA firmado por una entidad de certificación (CA) ECDSA será válido en esos cortafuegos.*

No puede utilizar un módulo de seguridad de hardware (HSM) para almacenar claves ECDSA utilizadas para el descifrado de SSL/TLS.

STEP 11 | Seleccione el **Number of Bits** para definir la extensión de la clave del certificado. Mientras más alto sea el número más seguro será, pero requerirá más tiempo de procesamiento.

© 2020 Palo Alto Networks, Inc.

STEP 12 | Seleccione el algoritmo **Digest (Resumen)**. Las opciones son las siguientes, de mayor a menor seguridad: **sha512**, **sha384**, **sha256** (predeterminado), **sha1** y **md5**.

Los certificados de cliente que se emplean al solicitar servicios de cortafuegos que se basan en TLSv1.2 (como el acceso de administrador a la interfaz web) no pueden tener sha512 como un algoritmo de resumen. Los certificados de cliente deben utilizar un algoritmo de resumen más bajo (como sha384) o debe limitar la Max Version (Versión máx.) a TLSv1.1 cuando realiza la Configuración de un perfil de servicio SSL/TLS *de los servicios de cortafuegos.*

STEP 13 | En **Expiration**, escriba la cantidad de días (por defecto es 365) durante los cuales es válido el certificado.

STEP 14 | (Opcional) Seleccione **Add** para añadir **Certificate Attributes (Atributos de certificados)** para identificar de manera exclusiva el cortafuegos y el servicio que vaya a utilizar el certificado.

Si añade el atributo Host Name (Nombre de host), que es el nombre de DNS, es recomendable que coincida con Common Name (Nombre común) porque el nombre de host rellena el campo Subject Alternate Name (Nombre alternativo de asunto) *(SAN) del certificado, el cual es obligatorio en algunos navegadores para especificar los dominios que protege el certificado. En GlobalProtect, es obligatorio que coincidan Host Name (Nombre de host) y Common Name (Nombre común).*

STEP 15 | Haga clic en **Generate** y en la pestaña Device Certificates, haga clic en el nombre del certificado.

Independientemente de la zona horaria del cortafuegos, siempre se muestra la hora del meridiano de Greenwich (Greenwich Mean Time, GMT) para la validez del certificado y las fechas/horas de vencimiento.

STEP 16 | Seleccione las casillas de verificación que se correspondan con el uso que se pretende dar al certificado en el cortafuegos.

Por ejemplo, si el cortafuegos va a utilizar este certificado para asegurar el reenvío de syslogs a un servidor syslog externo, seleccione la casilla de verificación **Certificate for Secure Syslog (Certificado de syslog seguro)**.

STEP 17 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Importación de un certificado y una clave privada

Si su empresa tiene su propia infraestructura de clave pública (PKI), puede importar un certificado y una clave privada en el cortafuegos desde la entidad de certificación (CA) de su empresa. Los certificados de CA de empresa (a diferencia de la mayoría de certificados adquiridos a una CA externa de confianza) pueden emitir automáticamente certificados de CA para aplicaciones como el descifrado SSL/TLS o VPN a gran escala.

En un cortafuegos o Panorama de Palo Alto Networks, usted solo puede importar certificados autofirmados si son certificados de CA.

En lugar de importar un certificado de CA raíz autofirmado en todos los sistemas cliente, la práctica recomendada es importar un certificado desde la CA de la empresa, dado que los clientes ya mantienen una relación de confianza con la CA de la empresa, lo cual simplifica la implementación.

© 2020 Palo Alto Networks, Inc.

Si el certificado que va a importar forma parte de una cadena de certificados, la práctica recomendada es importar toda la cadena.

STEP 1 | Desde la CA de la empresa, exporte el certificado y la clave privada que el cortafuegos utilizará para la autenticación.

Al exportar una clave privada, debe introducir una frase de contraseña para cifrar la clave para su transporte. Asegúrese de que el sistema de gestión puede acceder a los archivos del certificado y clave. Al importar la clave en el cortafuegos, debe introducir la misma frase de contraseña para descifrarla.

STEP 2 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 3 | Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.

STEP 4 | Haga clic en **Import (Importar)** e introduzca un **Certificate Name (Nombre de certificado)**. Puede tener hasta 63 caracteres en el cortafuegos y hasta 31 caracteres en Panorama. Además, se distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, guiones y guiones bajos.

STEP 5 | Para que el certificado esté disponible para todos los sistemas virtuales, seleccione la casilla de verificación Compartido. Esta casilla de verificación solo aparece si el cortafuegos admite múltiples sistemas virtuales.

STEP 6 | Introduzca la ruta y el nombre del **Archivo de certificado** que recibió de la CA o seleccione **Examinar** para buscar el archivo.

STEP 7 | Seleccione un **File Format (Formato de archivo)**:

- **Clave privada cifrada y certificado (PKCS12)**: Este es el formato predeterminado y más común, en el que la clave y el certificado están en un único contenedor (**Archivo del certificado**). Si un módulo de seguridad de hardware (HSM) va a almacenar la clave privada para este certificado, seleccione la casilla de verificación **La clave privada reside en el módulo de seguridad de hardware**.
- **Certificado codificado en Base64 (PEM)**: Debe importar la clave independientemente del certificado. Si un módulo de seguridad de hardware (HSM) almacena la clave privada para este certificado, seleccione la casilla de verificación **Private key resides on Hardware Security Module (La clave privada reside en el módulo de seguridad de hardware)** y omita el siguiente paso. De lo contrario, seleccione la casilla de verificación **Import Private Key (Importar clave privada)**, introduzca el archivo de clave en **Key File (Archivo de clave)** o haga clic en **Browse (Explorar)** para buscarlo y realice el siguiente paso.

STEP 8 | Introduzca y vuelva a introducir (confirme) la Frase de contraseña utilizada para cifrar la clave privada.

STEP 9 | Haga clic en **OK (Aceptar)**. La página Device Certificates (Certificados de dispositivos) muestra el certificado importado.

Obtención de un certificado desde una CA externa

La ventaja de obtener un certificado de una entidad de certificación (CA) externa es que la clave privada no abandona el cortafuegos. Para obtener un certificado desde una CA externa, genere una solicitud de firma de certificado (CSR) y envíela a la CA. Después de que la CA emita un certificado con los atributos especiales, impórtelo en el cortafuegos. La CA puede ser una CA pública conocida o una CA de la empresa.

© 2020 Palo Alto Networks, Inc.

Para utilizar el protocolo de estado de certificación en línea (OCSP) para comprobar el estado de revocación del certificado, realice la Configuración de un respondedor OCSP antes de generar la CSR.

STEP 1 | Solicite el certificado de una CA externa.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.
2. Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.
3. Haga clic en **Generate (Generar)**.
4. Introduzca un **Certificate Name (Nombre de certificado)**. Puede tener hasta 63 caracteres en el cortafuegos y hasta 31 caracteres en Panorama. Además, se distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, guiones y guiones bajos.
5. En el campo **Common Name (Nombre común)**, introduzca el FQDN (recomendado) o la dirección IP de la interfaz en la que configurará el servicio que utilizará este certificado.
6. Si el dispositivo tiene más de un vsys y desea que el certificado esté disponible para todos los vsys, seleccione la casilla de verificación **Shared (Uso compartido)**.
7. En el campo **Signed By (Firmado por)**, seleccione **External Authority (CSR) (Autoridad externa [CSR])**.
8. Si es aplicable, seleccione un **OCSP responder**.
9. (Opcional) Seleccione **Add** para añadir **Certificate Attributes (Atributos de certificados)** para identificar de manera exclusiva el cortafuegos y el servicio que vaya a utilizar el certificado.

   Si añade el atributo Host Name (Nombre de host), debe coincidir con Common Name (Nombre común) (es obligatorio en GlobalProtect). El nombre de host cumplimenta el campo Nombre alternativo del asunto (SAN) del certificado.
10. Haga clic en **Generate (Generar)**. La pestaña **Device Certificates (Certificados de dispositivos)** muestra la CSR con el estado `pending (pendiente)`.

STEP 2 | Envíe la CSR a la CA.

1. Seleccione la CSR y haga clic en **Export (Exportar)** para guardar el archivo .csr en un equipo local.
2. Cargue el archivo .csr en la CA.

STEP 3 | Importe el certificado.

1. Cuando la CA envíe el certificado firmado en respuesta a la CSR, vuelva a la pestaña **Certificados de dispositivos** y haga clic en **Importar**.
2. Introduzca el nombre del certificado en **Certificate Name (Nombre de certificado)**, que se utiliza para generar la CSR.
3. Introduzca la ruta y el nombre del **Archivo del certificado** PEM que envió la CA o seleccione **Examinar** para buscarlo.
4. Haga clic en **OK (Aceptar)**. La pestaña **Certificados de dispositivos** muestra el certificado de un estado de `válido`.

STEP 4 | Configure el certificado.

1. Haga clic en el **Name (Nombre)** del certificado.
2. Seleccione las casillas de verificación que se correspondan con el uso que se pretende dar al certificado en el cortafuegos. Por ejemplo, si el cortafuegos va a utilizar este certificado para asegurar el reenvío de syslogs a un servidor syslog externo, seleccione la casilla de verificación **Certificate for Secure Syslog (Certificado de syslog seguro)**.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Instalación de un certificado del dispositivo

Su cortafuegos de nueva generación puede aprovechar los servicios en la nube como la telemetría de dispositivos y la IoT. Para hacer esto, debe instalar un certificado de dispositivo para autenticar correctamente el cortafuegos con el portal de soporte al cliente (CSP, Customer Support Portal) de Palo Alto Networks para aprovechar estos servicios en la nube. Las circunstancias bajo las que se requiere un certificado de dispositivo diferirán de una función a otra. Por lo tanto, instale un certificado de dispositivo solo si la documentación de configuración de la función le indica que debe hacerlo.

Solo necesita instalar un certificado de dispositivo una vez. Las funciones que usan certificados de dispositivo utilizarán el certificado instalado en su cortafuegos si ya existe.

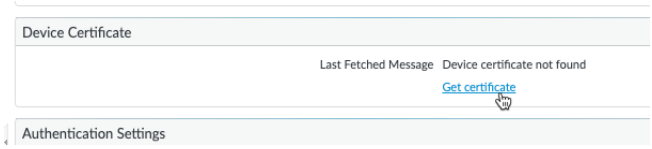
Puede instalar un certificado de dispositivo en cortafuegos gestionados por Panorama. Si desea instalar un certificado de dispositivo directamente en un único cortafuegos de nueva generación (es decir, *no* utiliza Panorama), realice los siguientes pasos:

STEP 1 | Genere la contraseña de un solo uso (One Time Password, OTP).

1. Inicie sesión en el Portal de atención al cliente.
2. Seleccione **Assets (Activos)** > **Device Certificates (Certificados del dispositivo)** y **Generate OTP (Generar OTP)**.
3. Para el **tipo de dispositivo**, seleccione **Generate OTP for Next-Gen Firewalls (Generar OTP para cortafuegos de nueva generación)**.
4. Seleccione el número de serie de su **dispositivo PAN OS**.
5. **Genere el OTP** y cópielo.

STEP 2 | Inicie sesión en su cortafuegos de nueva generación como usuario administrador.

STEP 3 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Device Certificate (Certificado del dispositivo)** y **Get certificate (Obtener certificado)**.



STEP 4 | Pegue la **contraseña de un solo uso** generada y haga clic en **OK (Aceptar)**.

STEP 5 | Su cortafuegos de nueva generación recupera e instala correctamente el certificado.

Implementación de certificados utilizando SCEP

Si tiene un servidor de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) en la PKI de su empresa, puede configurar un perfil SCEP para automatizar la generación y la distribución de certificados cliente únicos. El funcionamiento de SCEP es dinámico, ya que la PKI de la empresa genera un certificado específico del usuario cuando el cliente SCEP lo solicita y envía el certificado al cliente SCEP. El cliente SCEP luego implementa de manera transparente el certificado en el cliente.

Puede utilizar un perfil SCEP con GlobalProtect para asignar certificados cliente para usuarios específicos a cada usuario de GlobalProtect. En este caso de uso, el portal de GlobalProtect actúa como un cliente SCEP para el servidor SCEP en la PKI de su empresa. Además, puede utilizar un perfil SCEP para asignar certificados cliente a dispositivos Palo Alto Networks para una autenticación mutua con otros dispositivos Palo Alto Networks a fin de obtener acceso de gestión y comunicación entre dispositivos.

STEP 1 | Cree un perfil de SCEP.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **SCEP** y luego **Add (Añadir)** para añadir un nuevo perfil.
2. Introduzca un nombre en **Name (Nombre)** para identificar el perfil de SCEP.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.

STEP 2 | (**Opcional**) Para que la generación de certificados basada en SCEP sea más segura, configure un mecanismo de respuesta de comprobación de SCEP entre la PKI y el portal de cada solicitud de certificado.

Después de configurar este mecanismo, su operación es invisible, y no requerirá que realice otras acciones.

Para cumplir con los estándares federales de EE. UU. de procesamiento de la información (U.S. Federal Information Processing Standard, FIPS), utilice una comprobación SCEP **Dynamic (Dinámica)** y especifique una **Server URL (URL de servidor)** que utilice HTTPS.

Seleccione una de las siguientes opciones:

- **None (Ninguna)**: (**valor por defecto**) el servidor SCEP no comprueba el portal antes de emitir un certificado.
- **Fixed**: obtenga la contraseña de comprobación de inscripción desde el servidor SCEP en la infraestructura de PKI y luego introduzca la contraseña en el campo Password.
- **Dynamic (Dinámica)**: introduzca un nombre de usuario y contraseña de su elección (posiblemente las credenciales del administrador de PKI) y la **Server URL (URL de servidor)** de SCEP donde el portal-cliente envía estas credenciales. El portal utiliza las credenciales para autenticarse con el servidor SCEP, que genera de manera transparente una contraseña OTP para el portal tras cada solicitud de certificado. (Puede ver este cambio de OTP después de una actualización de pantalla en el campo `The enrollment challengepassword is (La contraseña de comprobación de inscripción es)` en cada solicitud de certificado). La PKI aprueba cada contraseña nueva de manera transparente en el portal, el cual luego utiliza la contraseña para su solicitud de certificado.

STEP 3 | Especifique los ajustes para la conexión entre el servidor SCEP y el portal para habilitar el portal para que solicite y reciba certificados cliente.

Usted puede incluir información adicional sobre el usuario o dispositivo cliente al especificar tokens en el nombre de asunto del certificado en el campo **Subject**.

El portal incluye el valor de token y la ID de host en la solicitud CSR para el servidor SCEP.

1. Configure la **Server URL (URL de servidor)** que usa el portal para conectarse con el servidor SCEP en la PKI (por ejemplo, `http://10.200.101.1/certsrv/mscep/`).
2. Introduzca una cadena (hasta 255 caracteres de extensión) en el campo **CA-IDENT Name (Nombre CA-IDENT)** para identificar el servidor SCEP.
3. Escriba un nombre de **Subject (Asunto)** para los certificados generados por el servidor SCEP. El nombre de asunto debe ser un nombre distintivo con el formato <**`attribute`**>=<**`value`**> y debe incluir un atributo de nombre común (CN) (`CN=<`**`variable`**`>`). El CN admite las siguientes tokens dinámicos:
   - `$USERNAME`: utilice este token para permitir que el portal solicite certificados para un usuario específico. Para utilizar esta variable con GlobalProtect, también debe realizar la Habilitación de la asignación de grupos. El nombre de usuario introducido por el usuario debe coincidir con el nombre en la tabla de asignación de grupos de usuarios.
   - `$EMAILADDRESS`: utilice este token para solicitar certificados asociados con una dirección de correo electrónico específica. Para usar esta variable, también debe Habilitar la asignación de grupos y configurar los **Mail Attributes (Atributos de correo)** en la sección Dominios de correo del

© 2020 Palo Alto Networks, Inc.

perfil del servidor. Si GlobalProtect no puede identificar una dirección de correo electrónico para el usuario, genera una ID único y rellena el CN con ese valor.

- `$HOSTID`: para solicitar certificados únicamente para el dispositivo, especifique el token de ID de host. Cuando un usuario intenta iniciar sesión en el portal, el endpoint envía información de identificación que incluye su valor de ID de host. El valor de ID de host varía según el tipo de dispositivo, ya sea la GUID (Windows), dirección MAC de la interfaz (Mac), ID Android (dispositivos Android), UDID (dispositivos iOS) o un nombre único que asigne GlobalProtect (Chrome).
- `$UDID`: utilice el atributo de nombre común de UDID para solicitar certificados basados en el UDID de dispositivo del cliente para GlobalProtect o el número de serie del dispositivo a fin de realizar una autenticación mutua entre dispositivos Palo Alto Networks.

Cuando el portal de GlobalProtect envíe los ajustes SCEP al agente, la parte de CN del nombre de asunto se sustituirá por el valor real (nombre de usuario, ID de host o dirección de correo electrónico) del propietario del certificado (por ejemplo, **`O=acme,CN=johndoe`**).

4. Seleccione **Subject Alternative Name Type (Tipo de nombre de asunto alternativo)**:

   *Utilice entradas estáticas para el tipo de Nombre Alternativo del Asunto. El cortafuegos no admite tokens dinámicos como **`$USERNAME`**.*

   - **RFC 822 Name (Nombre RFC 822)**: introduzca el nombre del correo electrónico en el asunto o la extensión de nombre alternativo de asunto del certificado.
   - **DNS Name (Nombre de DNS)**: ingrese el nombre de DNS usado para evaluar los certificados.
   - **Uniform Resource Identifier (Identificador uniforme de recursos)**: introduzca el nombre del recurso desde el cual el cliente obtendrá el certificado.
   - **None (Ninguno)**: no especifique atributos para el certificado.

STEP 4 | (**Opcional**) Configure ajustes criptográficos para el certificado.

- Seleccione la extensión de la clave (**Number of Bits**) del certificado.

  Si el cortafuegos está en modo FIPS-CC y el algoritmo de generación de claves es RSA. Las claves RSA deben ser de 2.048 bits o más.
- Seleccione el **Digest for CSR (Resumen para CSR)**, que indica el algoritmo de resumen para la solicitud de firma de certificado (certificate signing request, CSR): sha1, sha256 o sha384.

STEP 5 | (**Opcional**) Configure los usos permitidos del certificado, ya sea para firma o cifrado.

- Para usar este certificado para la firma, seleccione la casilla de verificación **Use as digital signature**. Esto habilita el extremo para usar la clave privada en el certificado a fin de validar una firma digital.
- Para usar este certificado para cifrado, seleccione la casilla de verificación **Use for key encipherment (Usar para cifrado de clave)**. Esto habilita al cliente para usar la clave privada en el certificado para cifrar los datos intercambiados en la conexión HTTPS establecida con los certificados emitidos por el servidor SCEP.

STEP 6 | (**Opcional**) Para garantizar que el portal se conecte al servidor SCEP correcto, introduzca la huella digital de certificado CA en **CA Certificate Fingerprint (Huella de certificado de CA)**. Obtenga esta huella en el campo Thumbprint (Huella digital) de la interfaz del servidor SCEP.

1. Introduzca la URL para la IU administrativa del servidor SCEP (por ejemplo, **`http://<hostname or IP>/CertSrv/mscep_admin/`**).
2. Copie la huella e introdúzcala en el campo **CA Certificate Fingerprint (Huella de certificado de CA)**.

STEP 7 | Habilite la autenticación SSL mutua entre el servidor SCEP y el cortafuegos. Esto es necesario para cumplir con los estándares federales de EE. UU. de procesamiento de la información (U.S. Federal Information Processing Standard, FIPS).

© 2020 Palo Alto Networks, Inc.

La operación de FIPS-CC se indica en la página de inicio de sesión del cortafuegos y en la barra de estado del cortafuegos.

Seleccione el **CA Certificate (Certificado de CA)** raíz del servidor SCEP. De manera opcional, puede habilitar la autenticación SSL mutua entre el servidor SCEP y el cortafuegos seleccionado un **Client Certificate (Certificado de cliente)**.

STEP 8 | Guarde y confirme la configuración.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes y cierre la configuración de SCEP.
2. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

El portal intenta solicitar un certificado de CA usando los ajustes del perfil SCEP y lo guarda en el cortafuegos que aloja al portal. Si se obtiene correctamente, el certificado de CA se muestra en **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.

STEP 9 | (**Opcional**) Si después de guardar el perfil SCEP, el portal no puede obtener el certificado, usted puede generar manualmente una solicitud de firma de certificado (CSR) del portal.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)**.
2. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
3. Seleccione el **SCEP Profile (Perfil SCEP)** para usar para enviar una CSR a la PKI de su empresa.
4. Haga clic en **OK** para enviar la solicitud y generar el certificado.

© 2020 Palo Alto Networks, Inc.

Exportación de un certificado y una clave privada

Palo Alto Networks le recomienda usar una infraestructura de clave pública de empresa (PKI) para distribuir un certificado y una clave privada en su organización. Sin embargo, si es necesario también puede exportar un certificado y una clave privada desde el cortafuegos o Panorama. Puede usar un certificado y una clave privada exportados en los siguientes casos:

- Configuración de una autenticación de administrador basada en certificados en la interfaz web
- Habilitación de SSL entre componentes de LSVPN de GlobalProtect para configurar la autenticación de agente/aplicación de GlobalProtect en los portales y puertas de enlace
- SSL Forward Proxy decryption (Descifrado del proxy SSL de reenvío)
- Obtención de un certificado desde una CA externa

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 2 | Si el cortafuegos tiene más de un sistema virtual (virtual system, vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para el certificado.

STEP 3 | Seleccione el certificado, haga clic en **Export (Exportar)** y seleccione un **File Format (Formato de archivo)**:

- **Base64 Encoded Certificate (PEM) (Certificado codificado en Base64)**: es el formato por defecto. Se trata del formato más común y más ampliamente aceptado de Internet. Si desea que el archivo exportado incluya la clave privada, seleccione la casilla de verificación **Export Private Key**.
- **Encrypted Private Key and Certificate (PKCS12)**: este formato es más seguro que PEM, pero no es tan común o tan ampliamente admitido. El archivo exportado incluirá automáticamente la clave privada.
- **Binary Encoded Certificate (DER) (Certificado codificado binario)**: este es el formato que admite la mayor cantidad de tipos de sistemas operativos. Puede exportar el certificado únicamente, no la clave: para ello, ignore la casilla de verificación **Export Private Key** y los campos de frase de contraseña.

STEP 4 | Escriba una frase de contraseña en **Passphrase (Frase de contrseña)** y repítala en **Confirm Passphrase (Confirmar frase de contrseña)** para cifrar la clave privada si el valor de **File Format (Formato de archivo)** es PKCS12 o si es PEM y ha seleccionado la casilla de verificación **Export Private Key (Exportar clave privada)**. Usará esta frase de contraseña cuando importe el certificado y la clave en sistemas cliente.

STEP 5 | Haga clic en **OK** y guarde el archivo de clave o certificado en su ordenador.

© 2020 Palo Alto Networks, Inc.

Configuración de un perfil de certificado

Los perfiles de certificados definen la autenticación de usuarios y dispositivos para el portal de autenticación, la autenticación multifactor (MFA, Multi-Factor Authentication), GlobalProtect, la VPN de sitio a sitio de IPSec, la validación de listas dinámicas externas (EDL, External Dynamic List), el DNS dinámico (DDNS, Dynamic DNS), el acceso a los agentes de User-ID y de TS, y el acceso a la interfaz web de Panorama o los cortafuegos de Palo Alto Networks. Los perfiles especifican qué certificados deben utilizarse, cómo verificar el estado de revocación de certificados y cómo restringe el acceso dicho estado. Configure un perfil de certificado para cada aplicación.



Para verificar que no se haya revocado el certificado, se recomienda habilitar el protocolo de estado de certificados en línea (online certificate status protocol, OCSP) y la verificación del estado de las listas de revocación de certificados (certificate revocation list, CRL) en los perfiles de certificados. Habilite tanto OCSP como las CRL para que el cortafuegos use estas en caso de que el servidor OCSP no esté disponible. Si desea información detallada sobre estos métodos, consulte Revocación de certificado*.*

STEP 1 | Obtenga los certificados de la entidad de certificación (CA) que asignará.

Realice uno de los pasos siguientes para obtener los certificados de CA que asignará al perfil. Debe asignar al menos uno.

- Generar un certificado.
- Exporte un certificado de la CA de su empresa y, a continuación, impórtelo al cortafuegos (consulte el paso 3).

STEP 2 | Identifique el perfil de certificado.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** para identificar el perfil. El nombre debe ser único, puede tener hasta 63 caracteres en el cortafuegos y hasta 31 caracteres en Panorama y solo puede incluir letras, números, espacios, guiones y guiones bajos. Además, se distingue entre mayúsculas y minúsculas.
3. Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.

STEP 3 | Asigne uno o más certificados.

Realice los siguientes pasos para cada certificado de CA:

1. En la tabla Certificados de CA, haga clic en **Añadir**.
2. Seleccione un **CA Certificate (Certificado de CA)**. Otra opción es importar un certificado al hacer clic en **Import**, introducir un **Certificate Name**, seleccionar **Browse** y buscar el **Certificate File** que ha exportado desde su CA de empresa y hacer clic en **OK**.
3. (**Opcional**) Si el cortafuegos utiliza OCSP para verificar el estado de revocación de certificados, configure los siguientes campos para cancelar el comportamiento predeterminado. Para la mayoría de las implementaciones, estos campos no son aplicables.
   - De manera predeterminada, el cortafuegos usa el "Acceso a la información de entidad" (Authority Information Access, AIA) del certificado para extraer los datos del respondedor del OCSP. Para cancelar la información de AIA, introduzca una **Default OCSP URL (URL de OCSP predeterminada)** (que comience con `http://` o `https://`).
   - De manera predeterminada, el cortafuegos utiliza el certificado seleccionado en el campo **CA Certificate (Certificado de CA)** para validar las respuestas de OCSP. Para utilizar un certificado

© 2020 Palo Alto Networks, Inc.

diferente para la validación, selecciónelo en el campo **OCSP Verify CA Certificate (Verificación de certificado CA con OCSP)**.

4. Haga clic en **OK (Aceptar)**. La tabla Certificados de CA muestra el certificado asignado.

STEP 4 | Defina los métodos para verificar el estado de revocación de certificados y el comportamiento de bloqueo asociado.

1. Seleccione **Utilizar CRL** y/o **Utilizar OCSP**. Si selecciona ambos, el cortafuegos probará primero con OCSP y volverá al método CRL solo si respondedor OCSP no está disponible.
2. Dependiendo del método de verificación, introduzca el **CRL Receive Timeout (Tiempo de espera de recepción de CRL)** y/o **OCSP Receive Timeout (Tiempo de espera de recepción de OCSP)**. Estos son los intervalos (1-60 segundos) tras los cuales el cortafuegos deja de esperar una respuesta del servicio CRL/OCSP.
3. Introduzca el **Tiempo de espera del estado del certificado**. Este es el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta de cualquier servicio de estado de certificado y aplica la lógica de bloqueo de sesión que defina. El **Certificate Status Timeout (Tiempo de espera del estado del certificado)** se relaciona con el **Receive Timeout (Tiempo de espera de recepción)** de OCSP/CRL de la manera siguiente:
   - Si habilita tanto OCSP como CRL: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o la suma de los dos valores de **Receive Timeout (Tiempo de espera de recepción)**.
   - Si habilita únicamente OCSP: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o el valor de **Receive Timeout (Tiempo de espera de recepción)** de OCSP.
   - Si habilita únicamente CRL: El cortafuegos registra un tiempo de espera de solicitud después de que pase el menor de dos intervalos: el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** o el valor de **Receive Timeout (Tiempo de espera de recepción)** de CRL.
4. Si desea que el cortafuegos bloquee sesiones cuando el servicio OCSP o CRL devuelva el estado de revocación de certificados desconocido, seleccione la casilla de verificación **Block session if certificate status is unknown (Bloquear una sesión si el estado del certificado es desconocido)**. De lo contrario, el cortafuegos permitirá las sesiones.
5. Si desea que el cortafuegos bloquee sesiones después de que registre un tiempo de espera de solicitud de OCSP o CRL, seleccione **Block session if certificate status cannot be retrieved within timeout (Bloquear una sesión si no se puede recuperar el estado del certificado dentro del tiempo de espera)**. De lo contrario, el cortafuegos permitirá las sesiones.
6. (**GlobalProtect únicamente**) Si desea que el cortafuegos bloquee las sesiones cuando el atributo de número de serie en el asunto del certificado del cliente no coincida con la ID de host que la aplicación de GlobalProtect informa al endpoint, seleccione **Block sessions if the certificate was not issued to the authenticating device (Bloquear las sesiones si el certificado no se emitió para el dispositivo de autenticación)**.

STEP 5 | Haga clic en **OK (Aceptar)** y luego en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de un perfil de servicio SSL/TLS

Los cortafuegos y Panorama de Palo Alto Networks utilizan perfiles de servicio SSL/TLS para especificar un certificado y las versiones permitidas del protocolo para los servicios SSL/TLS. Los cortafuegos y Panorama usan SSL/TLS para el portal de autenticación, portales y puertas de enlace de GlobalProtect, tráfico entrante de la interfaz de gestión (MGT), la función Cancelación de administrador de URL y el servicio de escucha de syslog User-ID™. Mediante la definición de versiones de protocolo, puede usar un perfil para restringir los conjuntos de cifras disponibles para proteger la comunicación con los clientes que solicitan los servicios. Esto mejora la seguridad de la red al habilitar el cortafuegos o Panorama para evitar las versiones de SSL/TLS que tienen debilidades conocidas. Si una solicitud de servicio involucra una versión de protocolo que está fuera del rango especificado, el cortafuegos o Panorama regresa a la versión anterior o actualiza la conexión a una versión compatible.

En los sistemas cliente que solicitan servicios de cortafuegos, la lista de certificados de confianza (CTL) debe incluir el certificado de autoridad de certificación (CA) que emitió el certificado especificado en el perfil de servicio SSL/TLS. De lo contrario, los usuarios observarán un error de certificado cuando soliciten servicios de cortafuegos. La mayoría de los certificados de CA externos están presentes de forma predeterminada en los exploradores de cliente. Si el emisor es un certificado de CA generado por una empresa o cortafuegos, debe implementar ese certificado de CA en los CTL en los navegadores de cliente.

STEP 1 | Para cada servicio deseado, genere o importe un certificado en el cortafuegos (consulte Obtención de certificados).

Utilice solo certificados firmados, no certificados de CA en perfiles de servicio SSL/TLS.

STEP 2 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.

STEP 3 | Si el cortafuegos tiene más de un sistema virtual (virtual system, vsys), seleccione la ubicación en **Location (Ubicación)** (vsys o **Shared [Compartida]**) en la que el perfil está disponible.

STEP 4 | Haga clic en **Add** e introduzca un nombre en **Name** para identificar el perfil.

STEP 5 | Seleccione el **Certificate** que acaba de obtener.

STEP 6 | Defina el intervalo de protocolos que puede usar el servicio:

- En **Min Version**, seleccione la versión de TLS más antigua permitida: **TLSv1.0** (por defecto), **TLSv1.1** o **TLSv1.2**.
- En **Max Version**, seleccione la versión de TLS más reciente permitida: **TLSv1.0**, **TLSv1.1**, **TLSv1.2** o **Max** (última versión disponible). El valor por defecto es **Max**.

Se recomienda configurar Min Version (Versión mínima) a TLSv1.2 y Max Version (Versión máxima) a Max (Máx.).

En los cortafuegos en modo FIPS/CC que ejecutan PAN-OS 8.0 o una versión posterior, TLSv1.1 es la versión TLS más antigua compatible; no seleccione TLSv1.0.

© 2020 Palo Alto Networks, Inc.

Los certificados de cliente utilizados al solicitar servicios de cortafuegos que dependen de TLS v. 1.2 no pueden tener SHA512 como algoritmo de resumen. Los certificados de cliente deben utilizar un algoritmo de resumen más bajo (como SHA384) o limitar la Max Version (Versión máx.) a TLSv1.1 para los servicios de cortafuegos.

STEP 7 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de un perfil de servicio SSH

Los perfiles de servicio SSH le permiten personalizar los parámetros SSH para mejorar la seguridad y la integridad de las conexiones SSH a sus dispositivos de gestión y alta disponibilidad (HA, High Availability) de Palo Alto Networks. De forma predeterminada, SSH admite todos los cifrados, algoritmos de intercambio de claves y códigos de autenticación de mensajes, lo que hace que su conexión sea vulnerable a ataques. Con un perfil de servicio SSH, puede restringir los algoritmos que admite el servidor SSH. También puede generar una nueva clave de host y especificar el volumen de datos, el tiempo y los umbrales basados en paquetes para la regeneración e intercambio de claves de sesión SSH.

Según la instancia del servidor SSH, configure un perfil de servicio de administración o SSH de HA. Puede configurar perfiles desde el cortafuegos o la interfaz web de Panorama™ (si aplica la configuración a través de varios cortafuegos o dispositivos) o la CLI.

Puede configurar un máximo de cuatro perfiles de administración y cuatro de servidor de HA.

Para utilizar la misma configuración de conexión SSH para cada recopilador de logs dedicado (dispositivo virtual de M-Series o Panorama en modo de recopilador de logs) en un grupo de recopiladores, configure un perfil de servicio SSH desde el servidor de gestión Panorama, confirme los cambios en Panorama y, a continuación, envíe la configuración a los recopiladores de logs. También puede realizar estos pasos desde la CLI mediante los comandos ***`set log-collector-group <name> general-setting management ssh`***.

- Creación de un perfil de administración SSH
- Creación de un perfil de HA SSH

Creación de un perfil de administración SSH

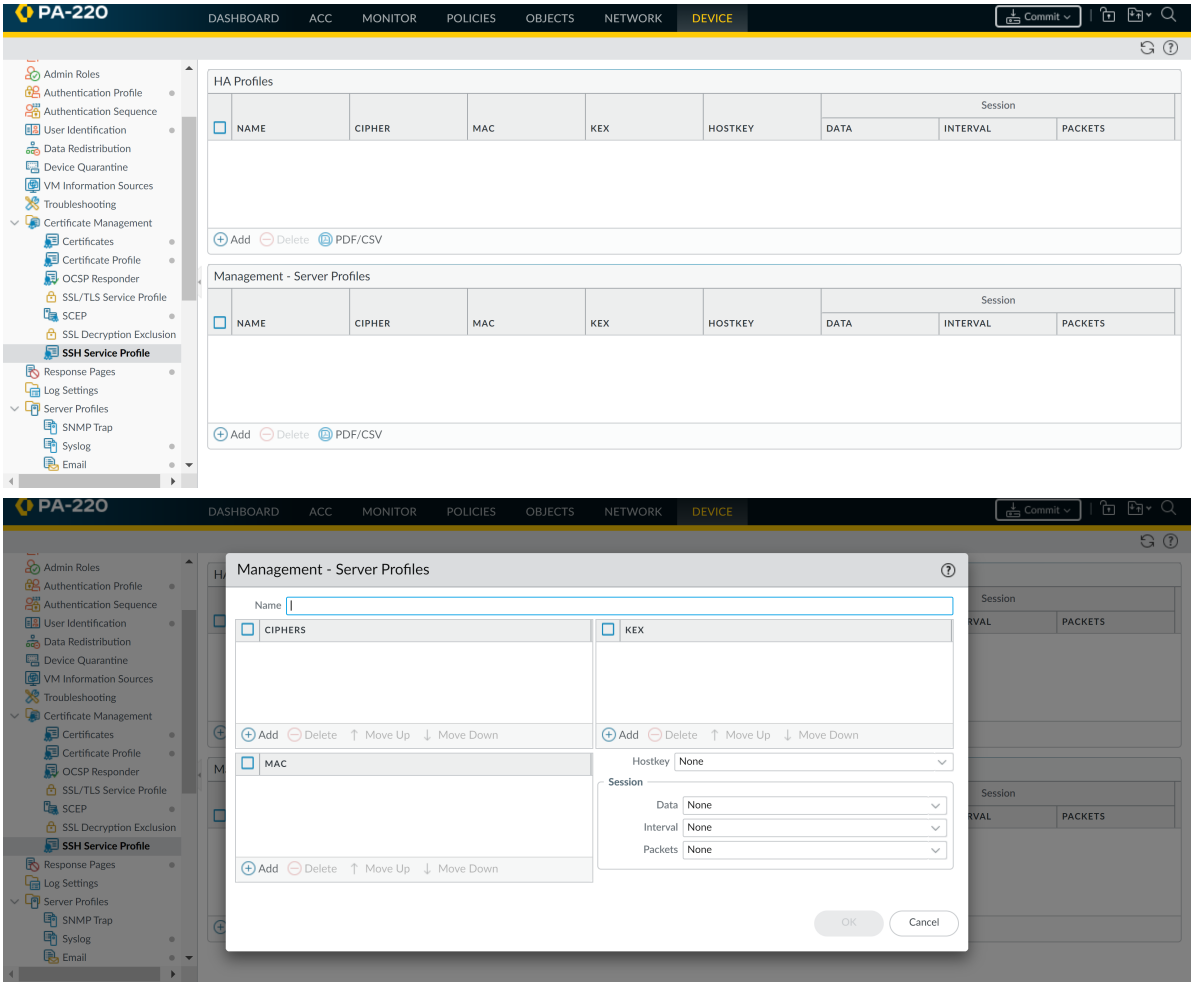
Debe crear un perfil de administración SSH para personalizar la configuración SSH para las conexiones de gestión.

Puede configurar o actualizar un perfil de gestión existente desde su CLI.

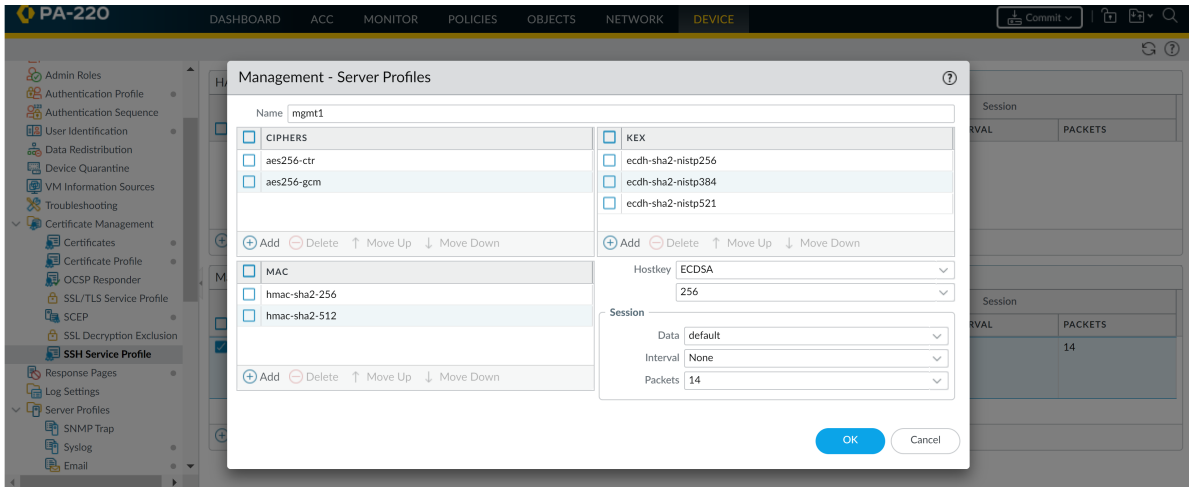
STEP 1 | Cree un perfil de servidor de gestión.

1. Seleccione **Device (Dispositivo)** > **Certification Management (Administración de certificaciones)** > **SSH Service Profile (Perfil de servicio SSH)**.
2. **Añada** un perfil de servidor de gestión.

© 2020 Palo Alto Networks, Inc.



3. Introduzca un **Name (Nombre)** para identificar el perfil.
4. (Opcional) **Añada** los cifrados, los códigos de autenticación de mensajes o algoritmos de intercambio de clave que admitirá el perfil.
5. (Opcional) Seleccione una **clave de host** y la longitud de clave.
6. (Opcional) Especifique valores para los parámetros de reclave de sesión SSH: **Data (Datos)**, **Interval (Intervalo)** y **Packets (Paquetes)**.

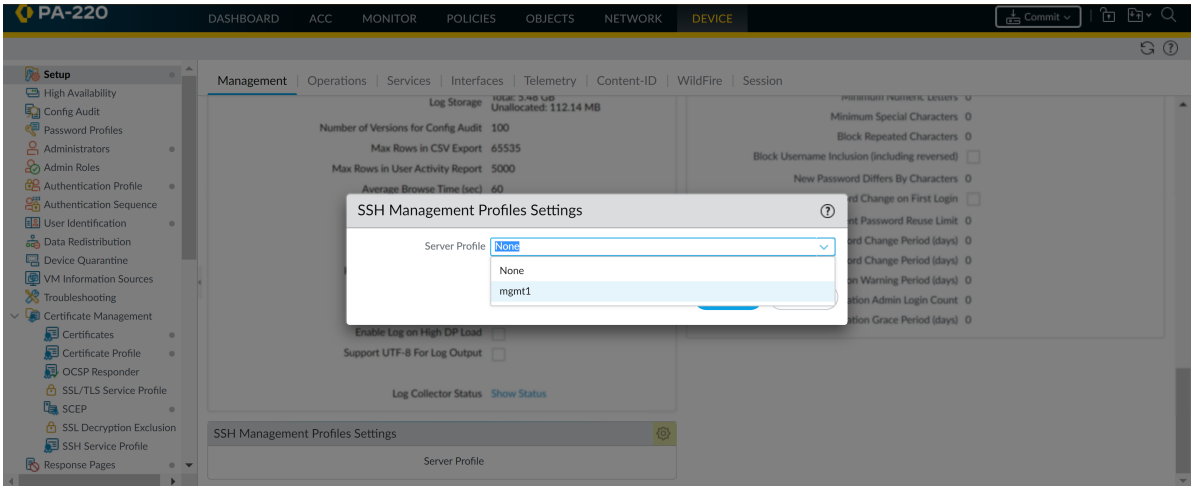


7. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Seleccione un perfil de gestión que aplicar.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**. En SSH Management Profiles Settings (Configuración de perfiles de gestión SSH), seleccione un perfil existente.



2. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para aplicar los cambios.

STEP 3 | Reinicie el servicio SSH de gestión desde la CLI para aplicar el perfil.

Debe reiniciar la conexión cada vez que aplique un nuevo perfil o realice cambios en un perfil en uso; con este procedimiento se reiniciará el dispositivo. Las nuevas configuraciones no afectarán a las sesiones activas. El perfil se aplicará a las conexiones (o sesiones) posteriores.

1. admin@PA-3260> **`set ssh service-restart mgmt`**

Creación de un perfil de HA SSH

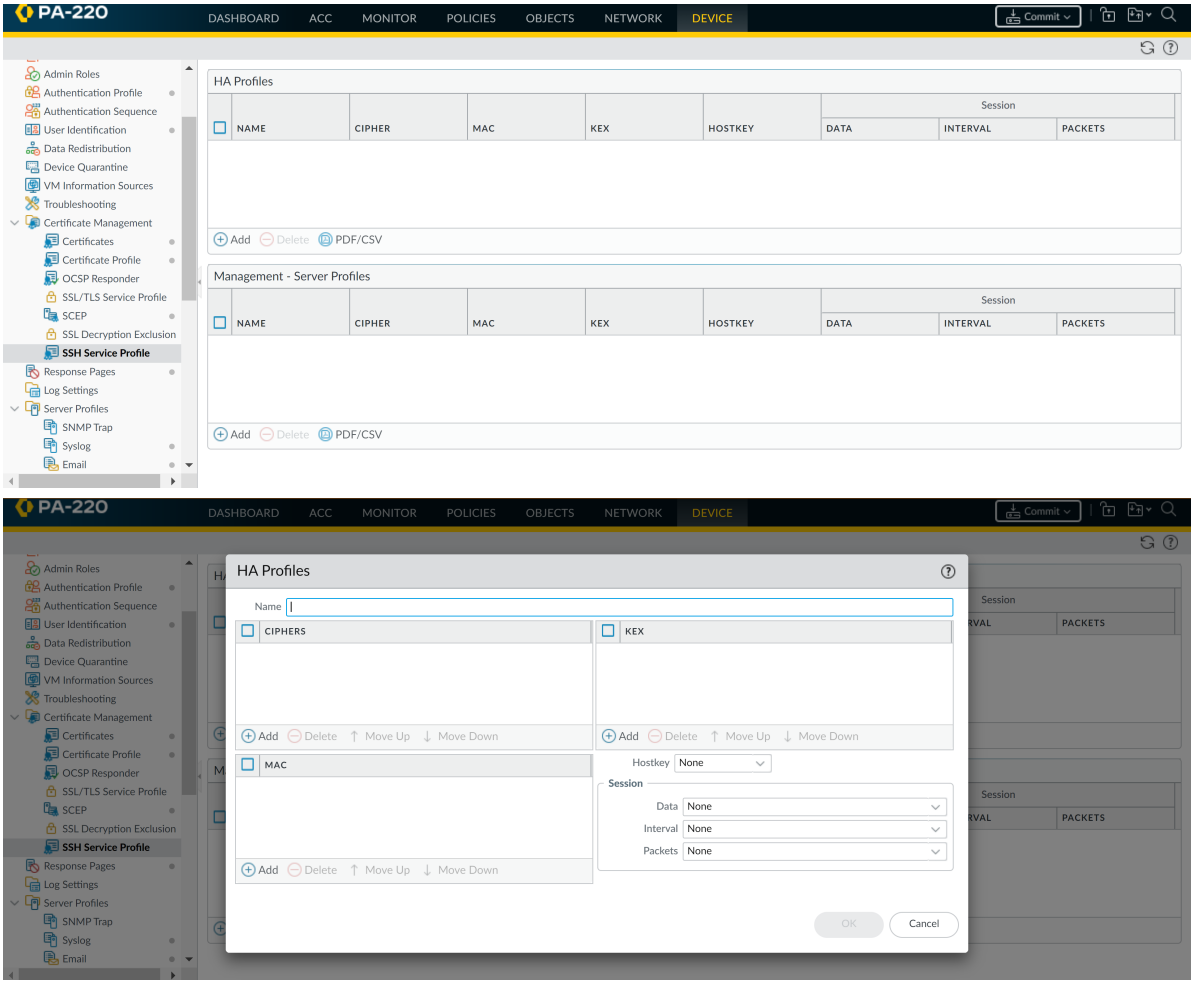
Para proteger las comunicaciones SSH entre dispositivos en un par de HA, debe crear un perfil de HA SSH. Para poder crear un perfil, debe establecer una conexión de HA entre los dispositivos. Si no se ha establecido una conexión de HA, debe habilitar el cifrado en la conexión del enlace de control, exportar la clave de HA a una ubicación de la red e importarla al peer. (Consulte Configuración de la HA activa/pasiva o Configuración de la HA activa/activa).

Puede configurar o actualizar un perfil de HA existente desde su CLI.

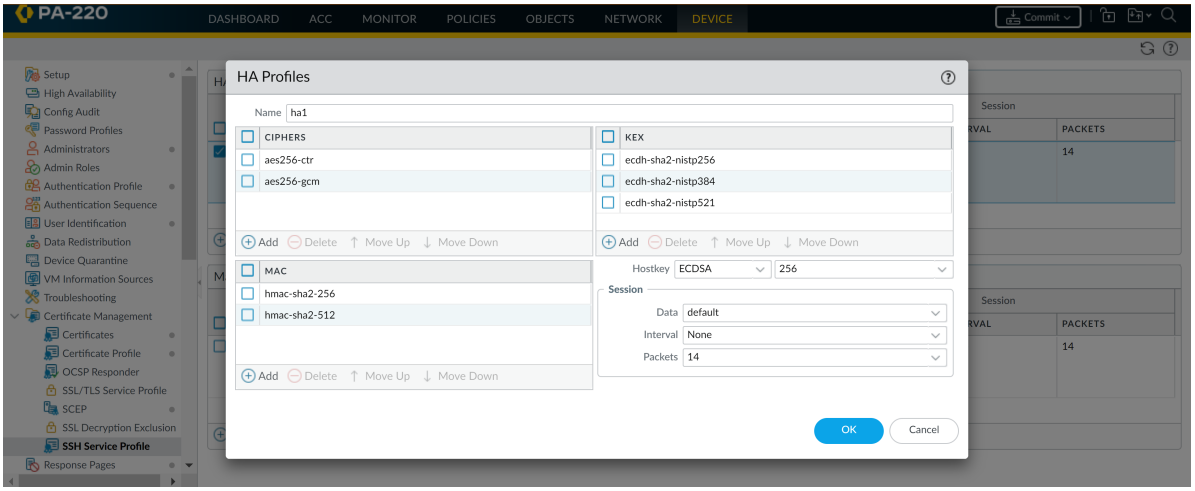
STEP 1 | Cree un perfil de HA.

1. Seleccione **Device (Dispositivo)** > **Certification Management (Administración de certificaciones)** > **SSH Service Profile (Perfil de servicio SSH)**.
2. **Añada** un perfil de HA.

© 2020 Palo Alto Networks, Inc.



3. Introduzca un **Name (Nombre)** para identificar el perfil.
4. (Opcional) **Añada** los cifrados, los códigos de autenticación de mensajes o algoritmos de intercambio de clave que admitirá el perfil.
5. (Opcional) Seleccione una **clave de host** y la longitud de clave.
6. (Opcional) Especifique valores para los parámetros de reclave de sesión SSH: **Data (Datos)**, **Interval (Intervalo)** y **Packets (Paquetes)**.

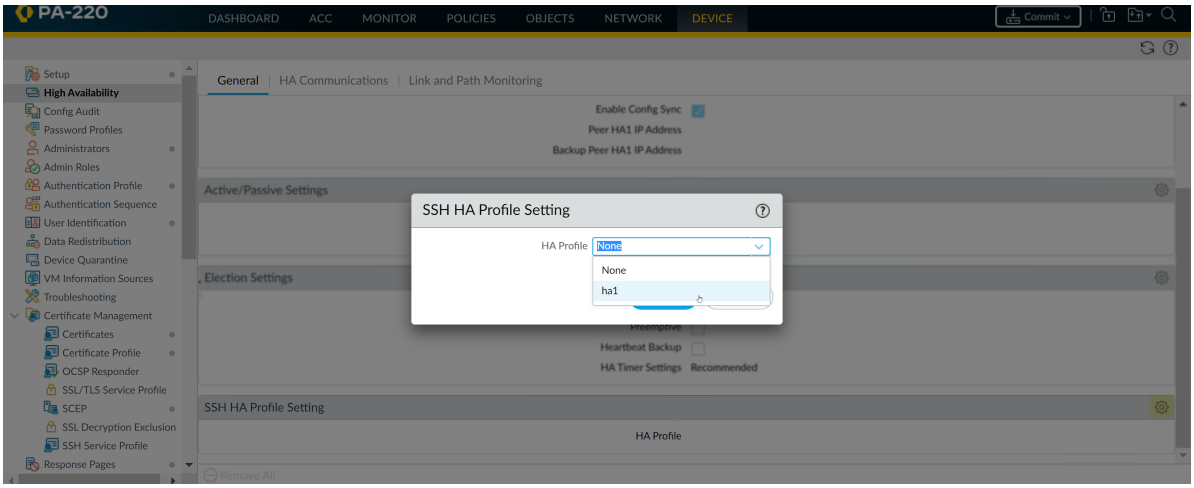


7. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Seleccione un perfil de HA que aplicar.

1. Seleccione **Dispositivo** > **Alta disponibilidad** > **General**. En SSH HA Profile Setting (Configuración de perfil de HA SSH), seleccione un perfil existente.



2. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para aplicar los cambios.

STEP 3 | Reinicie el servicio SSH de HA1 desde la CLI para aplicar el perfil.

Debe reiniciar la conexión cada vez que aplique un nuevo perfil o realice cambios en un perfil en uso; con este procedimiento se reiniciará el dispositivo. La nueva configuración no afectará a las sesiones activas. El perfil se aplicará a las conexiones (o sesiones) posteriores.

1. admin@PA-3260> **`set ssh service-restart ha`**

Puede utilizar los siguientes comandos si se ha establecido la conexión entre el par de HA y desea minimizar el tiempo de inactividad inherente al reinicio del servicio SSH. Si no se ha establecido una conexión de HA, debe reiniciar el servicio SSH.

- *(HA1 Backup is configured) admin@PA-3260>* ***`request high-availability session-reestablish`***
- *(Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3260>* ***`request high-availability session-reestablish force`***

  Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***`force (forzar)`*** *no funciona.*

© 2020 Palo Alto Networks, Inc.

Sustitución del certificado para el tráfico de gestión entrante

Cuando inicia por primera vez el cortafuegos o Panorama, estos generan automáticamente un certificado predeterminado que habilita el acceso HTTPS a la interfaz web y a la API de XML en la interfaz de gestión (MGT) y (solo en el cortafuegos) en cualquier otra interfaz que admita el tráfico de gestión HTTPS (para obtener información detallada, consulte Uso de los perfiles de gestión de interfaz para restringir el acceso). Para mejorar la seguridad del tráfico de gestión entrante, reemplace el certificado por defecto por un nuevo certificado emitido específicamente para su organización.



No puede ver, modificar ni eliminar el certificado por defecto.

Para proteger el tráfico de gestión, también debe realizar la Configuración de cuentas administrativas y autenticación*.*

STEP 1 | Obtenga el certificado que autenticará el cortafuegos o Panorama para los sistemas cliente de administradores.

Puede simplificar su implementación de certificados mediante el uso de un certificado en el que los sistemas clientes ya confíen. Por lo tanto, le recomendamos que realice una Importación de un certificado y una clave privada de su autoridad de certificación (certificate authority, CA) de la empresa o la Obtención de un certificado desde una CA externa; el almacén de certificados raíz de confianza de los sistemas cliente probablemente ya tenga el certificado CA raíz asociado que garantiza confianza.



Si realiza la Generación de un certificado *en el cortafuegos o Panorama, los administradores verán un error de certificado debido a que el certificado CA raíz no está en el almacén de certificados raíz de confianza de los sistemas cliente. Para evitar esto, implemente el certificado de CA raíz autofirmado en todos los sistemas cliente.*



Independientemente de cómo obtenga el certificado, recomendamos un algoritmo Digest de sha256 o mayor para la seguridad mejorada.

STEP 2 | Configuración de un perfil de servicio SSL/TLS.

Seleccione el **Certificate** que acaba de obtener.



Para una seguridad mejorada, recomendamos que configure Min Version (Versión mínima) (la versión más antigua permitida de TLS) a TLSv1.2 para el tráfico de gestión entrante. También recomendamos que use un perfil de servicio SSL/TLS diferente para cada cortafuegos o servicio de Panorama en lugar de reutilizar este perfil para todos los servicios.

STEP 3 | Aplique el perfil de servicio SSL/TS al tráfico de gestión entrante.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite {0>General Settings (Configuración general)<0}.
2. Seleccione el **perfil de servicio SSL/TLS** que acaba de configurar.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración del tamaño de clave para los certificados de servidor proxy SSL de reenvío

Cuando responde a un cliente en una sesión de Proxy de reenvío SSL, el cortafuegos crea una copia del certificado que le presenta el servidor de destino y lo usa para establecer su conexión con el cliente. Por defecto, el cortafuegos genera certificados con el mismo tamaño de clave que el certificado que le ha presentado el servidor de destino. Sin embargo, puede cambiar el tamaño de la clave para el certificado generado por el cortafuegos de la siguiente manera:

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y, en la sección Decryption Settings (Configuración de descifrado), haga clic en **SSL Forward Proxy Settings (Configuración de proxy de reenvío de SSL)**.

STEP 2 | Seleccione un tamaño de clave en **Key Size**:

- **Defined by destination host (Definido por host de destino)**: el cortafuegos determina el tamaño de clave y el algoritmo de hash de los certificados que genera para establecer las sesiones de proxy SSL con clientes en función del certificado del servidor de destino. Si el servidor de destino usa una clave RSA de 1024 bits, el cortafuegos genera un certificado con esa clave. Si el servidor de destino usa un tamaño de clave superior a 1024 bits (por ejemplo, 2048 bits o 4096 bits), el cortafuegos genera un certificado que usará una clave RSA de 2048 bits Si el servidor de destino usa un algoritmo de hash SHA-1, el cortafuegos genera un certificado con ese algoritmo. Si el servidor de destino usa un algoritmo de hash más potente que SHA-1, el cortafuegos genera un certificado con el algoritmo SHA-256. Es el ajuste predeterminado.
- **1024-bit RSA**: el cortafuegos genera certificados que usan una clave RSA de 1.024 bits y un algoritmo de hash SHA-1 independientemente del tamaño de clave de los certificados del servidor de destino. A fecha de 31 de diciembre de 2013, las entidades de certificación (CA) públicas y navegadores más populares han limitado la compatibilidad con los certificados X.509 que utilizan claves de menos de 2.048 bits. En el futuro, en función de los ajustes de seguridad, cuando aparezcan esas claves el navegador puede advertir al usuario o bloquear la sesión SSL/TLS por completo.
- **2048-bit RSA**: el cortafuegos genera certificados que usan una clave RSA de 2048 bits y un algoritmo de hash SHA-256 independientemente del tamaño de clave de los certificados del servidor de destino. Las CA públicas y los navegadores más populares admiten claves de 2.048 bits, que proporcionan más seguridad que las claves de 1.024 bits.

El cambio del ajuste del tamaño de la clave borra la caché del certificado actual.

STEP 3 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Revocación y renovación de certificados

- Revocación de un certificado
- Renovación de un certificado

Revocación de un certificado

Diversas circunstancias pueden invalidar un certificado antes de la fecha de vencimiento. Algunos ejemplos son un cambio de nombre, un cambio de asociación entre el sujeto y la entidad de certificación (por ejemplo, un empleado cuyo contrato se resuelva) y la revelación (confirmada o sospechada) de la clave privada. En estas circunstancias, la entidad de certificación (CA) que emitió el certificado deberá revocarlo. La siguiente tarea describe cómo revocar un certificado para el que el cortafuegos sea la CA.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 2 | Si el cortafuegos admite varios sistemas virtuales, la pestaña muestra el menú desplegable **Location**. Seleccione el sistema virtual al que pertenece el certificado.

STEP 3 | Seleccione el certificado que desea revocar.

STEP 4 | Haga clic en **Revoke (Revocar)**. PAN-OS inmediatamente establece el estado del certificado como revocado y añade el número de serie a la caché del respondedor del protocolo de estado de certificado en línea (OCSP) o la lista de revocación de certificados (CRL). No necesita realizar una compilación.

Renovación de un certificado

Si un certificado vence, o lo hará pronto, puede restablecer el periodo de validez. Si una autoridad de certificación (certificate authority, CA) externa firmó el certificado y el cortafuegos utiliza el protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) para verificar el estado de revocación de certificados, el cortafuegos utilizará información del respondedor OCSP para actualizar el estado del certificado (consulte Configuración de un respondedor OCSP). Si el cortafuegos es la CA que emitió el certificado, el cortafuegos lo sustituirá por un nuevo certificado que tenga un número de serie diferente pero los mismos atributos que el certificado anterior.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

STEP 2 | Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la ubicación en **Location** (vsys o **Shared**) para esta configuración.

STEP 3 | Seleccione el certificado que desea renovar y haga clic en **Renovar**.

STEP 4 | Introduzca un **Nuevo intervalo de vencimiento** (en días).

STEP 5 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Claves seguras con módulos de seguridad de hardware

Un módulo de seguridad de hardware (HSM) es un dispositivo físico que gestiona claves digitales. Un HSM proporciona un almacenamiento seguro y la generación de claves digitales. Ofrece tanto protección lógica como física de estos materiales ante un uso no autorizado y posibles atacantes.

Los clientes HSM integrados con cortafuegos y Panorama de Palo Alto Networks habilitan una seguridad mejorada para las claves privadas utilizadas en el descifrado SSL/TLS (tanto el proxy SSL de reenvío como la inspección de entrada SSL). Además, puede utilizar el HSM para cifrar claves maestras.

Los siguientes temas describen cómo integrar un HSM con su cortafuegos o Panorama:

- Configuración de la conectividad con un HSM
- Cifrado de una clave maestra utilizando un HSM
- Almacenamiento de claves privadas en un HSM
- Gestión de la implementación del HSM

Configuración de la conectividad con un HSM

Hay clientes HSM integrados en los cortafuegos PA-3200 Series, PA-5200 Series, PA-7000 Series y VM-Series, así como en el servidor de gestión Panorama (dispositivos virtuales y M-Series) para su uso con los siguientes proveedores de HSM:

- **nCipher nShield Connect**: las versiones de cliente admitidas dependen de la versión de PAN-OS:
  - PAN-OS 10.0 es compatible con la versión de cliente 12.40.2 (compatible con versiones anteriores hasta la versión de cliente 11.50 para dispositivos más antiguos).
  - PAN-OS 9.1, 9.0 y 8.1 son compatibles con la versión de cliente 12.30.
  - Las versiones PAN-OS 8.0 y anteriores admiten la versión de cliente 11.62.
- **SafeNet Network:** las versiones de cliente admitidas dependen de la versión de PAN-OS:
  - PAN-OS 10.0 es compatible con las versiones de cliente 5.4.2 y 7.2.
  - PAN-OS 9.1 y 9.0 son compatibles con las versiones de cliente 5.4.2 y 6.3.
  - PAN-OS 8.1 son compatibles con las versiones de cliente 5.4.2 y 6.2.2.
  - Las versiones PAN-OS 8.0.2 y las versiones posteriores a PAN-OS 8.0 (también PAN-OS 7.1.10 y versiones PAN-OS 7.1 posteriores): versiones de cliente 5.2.1, 5.4.2 y 6.2.2.

La versión del servidor HSM debe ser compatible con estas versiones de cliente. Consulte la documentación del proveedor del HSM para conocer la matriz de compatibilidad de la versión de servidor cliente. En el cortafuegos o en Panorama, utilice el siguiente procedimiento para seleccionar la versión de cliente SafeNet Network compatible con su servidor de HSM SafeNet.



Es posible que cambiar a una versión anterior de los servidores de HSM no sea una opción luego de actualizarlas.

- Configuración de la conectividad con un HSM SafeNet Network
- Configuración de la conectividad con un HSM nCipher nShield Connect

- Instale el gestor de paquetes RPM de cliente de SafeNet.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y haga clic en **Select HSM Client Version (Seleccionar la versión de cliente de HSM)** (ajustes de las Operaciones de seguridad de hardware).
2. Seleccione **Version 5.4.2 (Versión 5.4.2)** (valor predeterminado) o **7.2**, según corresponda para su versión de servidor de HSM.
3. Haga clic en **OK (Aceptar)**.
4. (Obligatorio solo si cambia la versión de HSM en el cortafuegos) Si se produce el cambio de versión correctamente, el cortafuegos le solicita realizar un reinicio para cambiar a la nueva versión de HSM. Si se le solicita que reinicie, haga clic en **Yes (Sí)**.
5. Si la clave maestra no está en el cortafuegos, la actualización de la versión de cliente fallará. Haga clic en **Close (Cerrar)** para cerrar el mensaje y hacer local la clave maestra del cortafuegos:
   - Edite el Hardware Security Module Provider (Proveedor de módulo de seguridad de hardware) y deshabilite (desmarque) la opción **Master Key Secured by HSM (Clave maestra asegurada por HSM)**.
   - Haga clic en **OK (Aceptar)**.
   - Seleccione **Device (Dispositivo)** > **Master Key and Diagnostics (Clave maestra y diagnóstico)** y edite la Master Key (Clave maestra).
   - Introduzca la **Current Master Key (Clave maestra actual)**; puede introducir la misma clave en **New Master Key (Nueva clave maestra)** y hacer clic en **Confirm New Master Key (Confirmar nueva clave maestra)**.
   - Haga clic en **OK (Aceptar)**.
   - Repita los primeros cuatro pasos para **Select HSM Client Version (Seleccionar la versión de cliente de HSM)** y vuelva a reiniciar.

Configuración de la conectividad con un HSM SafeNet Network

Para configurar la conectividad entre el cortafuegos de Palo Alto Networks (cliente HSM) y un servidor HSM de SafeNet Network, debe especificar la dirección IP del servidor, ingresar una contraseña para autenticar el cortafuegos en el servidor y registrar el cortafuegos con el servidor. Antes de configurar su cliente HSM, cree una partición para el cortafuegos en el servidor HSM y confirme que la versión de cliente de SafeNet Network en el cortafuegos sea compatible con su servidor HSM de SafeNet Network (consulte Configuración de la conectividad con un HSM).

Antes de la conexión de HSM y el cortafuegos, el HSM autentica el cortafuegos según la dirección IP del cortafuegos. Por lo tanto, debe configurar el cortafuegos para que utilice una dirección IP estática, no una dirección dinámica asignada a través de DHCP. Las operaciones en el HSM dejan de funcionar si la dirección IP del cortafuegos cambia durante el tiempo de ejecución.

Las configuraciones del HSM no están sincronizadas entre peers de cortafuegos en alta disponibilidad (HA). Por consiguiente, deberá configurar el HSM por separado en cada uno de los peers. En configuraciones de HA activa/pasiva, deberá realizar manualmente una conmutación por error para configurar y autenticar cada peer de HA individualmente en el HSM. Después de realizar esta conmutación manual inicial, la interacción del usuario no será necesaria para que la conmutación por error funcione adecuadamente.

STEP 1 | Defina los ajustes de conexión para cada HSM SafeNet Network.

1. Inicie sesión en la interfaz web del cortafuegos y seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM**.
2. Modifique los ajustes de proveedor de módulo de seguridad de hardware y establezca el **Provider Configured (Proveedor configurado)** en **SafeNet Network HSM (HSM de SafeNet Network)**.

© 2020 Palo Alto Networks, Inc.

3. Seleccione **Add (Añadir)** para añadir cada servidor HSM de la siguiente manera. Una configuración HSM de alta disponibilidad (high availability, HA) requiere, al menos, dos servidores; es posible tener un clúster de hasta 16 servidores HSM. Todos los servidores HSM en el clúster deben ejecutar la misma versión de SafeNet y se deben autenticar por separado. Debe utilizar un clúster SafeNet únicamente cuando desee replicar las claves del clúster. De manera alternativa, puede añadir hasta 16 servidores HSM SafeNet para que funcionen por separado.
   1. Introduzca un **Module Name (Nombre de módulo)** (una cadena ASCII de hasta 31 caracteres) para el servidor HSM.
   2. Ingrese una dirección IPv4 como **Server Address (Dirección de servidor)** HSM.
4. (HA únicamente) Seleccione **High Availability (Alta disponibilidad)**, especifique el valor de **Auto Recovery Retry (Reintento de recuperación automática)** (número máximo de veces que el cliente HSM intenta recuperar la conexión con un servidor HSM antes de pasar a otro servidor HSM de peer de HA; el intervalo es 0 a 500; el valor predeterminado es 0) e introduzca un **High Availability Group Name (Nombre de grupo de alta disponibilidad)** (una cadena ASCII de hasta 31 caracteres de longitud).

   Si configura dos o más servidores HSM, se recomienda habilitar la High Availability (Alta disponibilidad). De lo contrario, el cortafuegos no utiliza los servidores HSM adicionales.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 2 | (Opcional) Configure una ruta de servicio para conectarse a HSM si no desea que el cortafuegos se conecte a través de la interfaz de gestión (opción predeterminada).

*Si configura una ruta de servicio para HSM, la ejecución del comando CLI **`clear session all`** borrará todas las sesiones HSM existentes, y hará que todos los estados del HSM se desconecten y luego se conecten nuevamente. Durante los segundos que necesita el HSM para recuperarse, fallarán todas las operaciones de SSL/TLS.*

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.
2. Seleccione **Customize (Personalizar)** para personalizar una ruta de servicio. La pestaña **IPv4** está activa de manera predeterminada.
3. Haga clic en **HSM** en la columna Service (Servicio).
4. Seleccione una **Source Interface (Interfaz de origen)** para el HSM.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 3 | Configure el cortafuegos para autenticarlo con el HSM.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** y **Setup Hardware Security Module (Configurar módulo de seguridad de hardware)**.
2. Seleccione el **Server Name (Nombre de servidor)** de HSM.
3. Seleccione **Automatic (Automático)** o **Manual** para su autenticación y certificado de confianza.
4. Introduzca la Contraseña de administrador para autenticar el cortafuegos para el HSM.
5. Haga clic en **OK (Aceptar)**.

   El cortafuegos intenta realizar una autenticación con el HSM y muestra un mensaje de estado.
6. Haga clic en **OK (Aceptar)** nuevamente.

STEP 4 | Registre el cortafuegos como cliente HSM con el servidor HSM y asígnelo a una partición en el servidor HSM.

*Si el HSM ya tiene un cortafuegos con el mismo <cl-name> ya registrado, primero debe eliminar el registro duplicado ejecutando el comando **`client delete -client <cl-`***

© 2020 Palo Alto Networks, Inc.

***name>**, donde <cl-name> es el nombre del cliente registrado (cortafuegos) que desea eliminar.*

1. Inicie sesión en el HSM desde un sistema remoto.
2. Registre el cortafuegos usando el comando de CLI **`client register -c <cl-name> -ip <fw-ip-addr>`**, donde *<cl-name>* es un nombre que usted asigna al cortafuegos para usar en HSM y *<fw-ip-addr>* es la dirección IP de ese cortafuegos.
3. Asigne una partición al cortafuegos usando el comando de CLI **`client assignpartition -c <cl-name> -p <partition-name>`**, donde *<cl-name>* es el nombre que asignó al cortafuegos con el comando **`client register`** y *<partition-name>* es el nombre de la partición configurada anteriormente que desea asignar a este cortafuegos.

STEP 5 | Configure el cortafuegos para conectarlo a la partición del HSM.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y actualice ( ) la pantalla.
2. Seleccione **Setup HSM Partition (Configurar partición HSM)** (ajustes de las Operaciones de seguridad de hardware).
3. Introduzca la Contraseña de partición para autenticar el cortafuegos para la partición del HSM.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | (HA únicamente) Repita la autenticación anterior y los pasos de conexión de partición para añadir el HSM al grupo HA existente.

Si elimina el HSM de su configuración, repita el paso de conexión de partición anterior para quitar el HSM eliminado del grupo HA.

STEP 7 | Verifique la conectividad del cortafuegos y la autenticación con el HSM.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y compruebe la autenticación y el estado de conexión:
   - **Verde:** el cortafuegos se autenticó correctamente y está conectado al HSM.
   - **Rojo:** el cortafuegos no se autenticó correctamente al HSM o la conectividad de red con el HSM no está activa.
2. Consulte las siguientes columnas en Hardware Security Module Status (Estado de módulo de seguridad de hardware) para determinar el estado de autenticación:
   - **Serial Number (Número de serie)**: el número de serie de la partición HSM si el HSM se ha autenticado con éxito en el HSM.
   - **Partition (Partición)**: nombre de la partición del HSM que se asignó al cortafuegos.
   - **Module State (Estado de módulo)**: estado actual de la conexión con HSM. El valor es siempre `Authenticated` (Autenticado) si Hardware Security Module Status (Estado de módulo de seguridad de hardware) muestra el HSM.

Configuración de la conectividad con un HSM nCipher nShield Connect

Debe configurar un sistema de archivo remoto (remote filesystem, RF) como un núcleo para sincronizar los datos clave para todos los cortafuegos (clientes HSM) de su organización que utilizan el HSM nCipher nShield Connect. Para garantizar que la versión de cliente de nShield Connect en el cortafuegos sea compatible con su servidor de nShield Connect, consulte Configuración de la conectividad con un HSM.

Antes de la conexión del HSM y el cortafuegos, el HSM autentica el cortafuegos según las direcciones IP del cortafuegos. Por lo tanto, debe configurar el cortafuegos para que utilice direcciones IP estáticas, no direcciones dinámicas asignadas a través de DHCP. (Las operaciones en el HSM dejan de funcionar si la dirección IP del cortafuegos cambia durante el tiempo de ejecución).

© 2020 Palo Alto Networks, Inc.

Las configuraciones del HSM no están sincronizadas entre peers de cortafuegos en alta disponibilidad (HA). Por consiguiente, deberá configurar el HSM por separado en cada uno de los peers. En configuraciones de HA activa/pasiva, deberá realizar manualmente una conmutación por error para configurar y autenticar cada peer de HA individualmente en el HSM. Después de realizar esta conmutación manual inicial, la interacción del usuario no será necesaria para que la conmutación por error funcione adecuadamente.

STEP 1 | Defina los ajustes de conexión para cada HSM nCipher nShield Connect.

1. Inicie sesión en la interfaz web del cortafuegos y seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM**.
2. Modifique los ajustes de proveedor de módulo de seguridad de hardware y configure el **Provider Configured (Proveedor configurado)** en **nShield Connect**.
3. Seleccione **Add (Añadir)** para añadir cada servidor HSM de la siguiente manera. Una configuración HSM de HA requiere dos servidores.
    1. Especifique un nombre en **Module Name (Nombre del módulo)** para el servidor HSM. Puede ser cualquier cadena ASCII con una longitud de hasta 31 caracteres.
    2. Ingrese una dirección IPv4 como **Server Address (Dirección de servidor)** HSM.
4. Imtroduzca una dirección IPv4 para la **Remote Filesystem Address (Dirección de sistema de archivos remoto)**.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 2 | (Opcional) Configure una ruta de servicio para conectarse a HSM si no desea que el cortafuegos se conecte a través de la interfaz de gestión (opción predeterminada).

Si configura una ruta de servicio para HSM, la ejecución del comando CLI ***`clear session all`*** *borrará todas las sesiones HSM existentes, y hará que todos los estados del HSM se desconecten y luego se conecten nuevamente. Durante los segundos que necesita el HSM para recuperarse, fallarán todas las operaciones de SSL/TLS.*

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.
2. Seleccione **Customize (Personalizar)** para personalizar una ruta de servicio. La pestaña **IPv4** está activa de manera predeterminada.
3. Haga clic en **HSM** en la columna Service (Servicio).
4. Seleccione una **Source Interface (Interfaz de origen)** para el HSM.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 3 | Registre el cortafuegos como cliente HSM con el servidor HSM.

Este paso describe brevemente el procedimiento para utilizar la interfaz del panel frontal del HSM nShield Connect. Si desea información más detallada, consulte la documentación de nCipher.

1. Inicie sesión en la pantalla del panel frontal de la unidad HSM nCipher nShield Connect.
2. En el panel frontal de la unidad, utilice el botón de navegación de la derecha para seleccionar **System (Sistema)** > **System configuration (Configuración del sistema)** > **Client config (Configuración de cliente)** > **New client (Nuevo cliente)**.
3. Introduzca la dirección IP del cortafuegos.
4. Seleccione **System (Sistema)** > **System configuration (Configuración del sistema)** > **Client config (Configuración del cliente)** > **Remote file system (Sistema de archivos remotos)** e introduzca la dirección IP del equipo cliente donde configure el RFS.

STEP 4 | Configure el RFS para que acepte las conexiones del cortafuegos.

© 2020 Palo Alto Networks, Inc.

1. Inicie sesión en el RFS desde un cliente Linux.
2. Obtenga el número de serie electrónico (electronic serial number, ESN) y el hash de la clave K_{NETI}, que autentica el HSM en los clientes mediante la ejecución del comando de CLI **anonkneti *<ip-address>***, donde *<ip-address>* es la dirección IP de HSM.

   Por ejemplo:

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   En este ejemplo, `B1E2-2D4C-E6A2` es el ESN y `5a2e5107e70d525615a903f6391ad72b1c03352c` es el hash de la clave K_{NETI}.
3. Utilice el siguiente comando de una cuenta de superusuario para configurar el RFS:

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   La *<ip-address>* es la dirección IP de HSM, *<ESN>* es el número de serie electrónico y *<hash-Kneti-key>* es el hash de la clave K_{NETI}.

   El siguiente ejemplo utiliza los valores obtenidos mediante este procedimiento:

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. Utilice el siguiente comando para permitir los envíos del cliente HSM en el RFS:

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   donde *<FW-IPaddress>* es la dirección IP del cortafuegos.

STEP 5 | Autentique el cortafuegos en el HSM.

1. En la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y **Setup Hardware Security Module (Configurar módulo de seguridad de hardware)**.
2. Haga clic en **OK (Aceptar)**.

   El cortafuegos intenta realizar una autenticación con el HSM y muestra un mensaje de estado.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Sincronice el cortafuegos con el RFS al seleccionar **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y **Synchronize with Remote Filesystem (Sincronizar con el sistema de archivo remoto)**.

STEP 7 | Verifique la conectividad del cortafuegos y la autenticación con el HSM.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y compruebe la autenticación y el estado de conexión:
   - **Verde:** el cortafuegos se autenticó correctamente y está conectado al HSM.
   - **Rojo:** el cortafuegos no se autenticó correctamente al HSM o la conectividad de red con el HSM no está activa.
2. Consulte la sección Hardware Security Module Status (Estado de módulo de seguridad de hardware) para determinar el estado de autenticación.

© 2020 Palo Alto Networks, Inc.

- **Name (Nombre)**: nombre del servidor HSM.
- **IP address (Dirección IP)**: dirección IP del servidor HSM.
- **Module State (Estado de módulo)**: estado actual de la conexión con HSM: `Authenticated (Autenticado)` o `Not Authenticated (No autenticado)`.

Cifrado de una clave maestra utilizando un HSM

Una clave maestra cifra todas las claves privadas y las contraseñas en el cortafuegos y Panorama. Si tiene requisitos de seguridad para almacenar sus claves privadas en una ubicación segura, puede cifrar la clave maestra utilizando una clave de cifrado que se almacene en un HSM. A continuación, el cortafuegos o Panorama solicita al HSM que descifre la clave maestra cuando sea necesaria para descifrar una contraseña o clave privada en el cortafuegos. Normalmente, el HSM se encuentra en una ubicación de alta seguridad separada del cortafuegos o de Panorama para mayor seguridad.

El HSM cifra la clave maestra mediante una clave de empaquetamiento. Para garantizar la seguridad, debe cambiar (actualizar) con regularidad esta clave de empaquetamiento.

Los cortafuegos configurados en modo FIPS/CC no admiten cifrado de clave maestra con HSM.

Los siguientes temas describen cómo descifrar la clave maestra inicialmente y cómo actualizar el cifrado de la clave maestra:

- Cifrado de la clave maestra
- Actualización del cifrado de la clave maestra

Cifrado de la clave maestra

Si no ha cifrado anteriormente la clave maestra de un cortafuegos, utilice el siguiente procedimiento para cifrarla. Utilice este procedimiento la primera vez que cifre una clave o si define una nueva clave maestra y desea descifrarla. Si desea actualizar el cifrado de una clave cifrada anteriormente, consulte Actualización del cifrado de la clave maestra.

STEP 1 | Seleccione **Device (Dispositivo)** > **Master Key and Diagnostics (Clave maestra y diagnósticos)**.

STEP 2 | Especifique la clave que se utiliza actualmente para cifrar todas las claves privadas y contraseñas del cortafuegos en el campo **Master Key (Clave maestra)**.

STEP 3 | Si está cambiando la clave maestra, introduzca la nueva clave maestra y confírmela.

STEP 4 | Seleccione la casilla de verificación **HSM**.

- **Life Time (Duración):** el número de días y horas tras el cual vence la clave maestra (el rango es de 1 a 730 días).
- **Time for Reminder (Período restante):** el número de días y horas antes del vencimiento, en cuyo momento se notificará al usuario del vencimiento inminente (el rango es de 1 a 365).

STEP 5 | Haga clic en **OK (Aceptar)**.

Actualización del cifrado de la clave maestra

La práctica recomendada es actualizar periódicamente el cifrado de clave maestra rotando la clave de empaquetamiento que lo cifra. La frecuencia de la rotación depende de su aplicación. La clave de empaquetamiento permanece en su HSM. El siguiente comando es el mismo para los HSM SafeNet Network y nCipher nShield Connect.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Inicie sesión en la CLI del cortafuegos.

STEP 2 | Utilice el siguiente comando de la CLI para rotar la clave de ajuste para la clave maestra de un HSM:

```
> request hsm mkey-wrapping-key-rotation
```

Si la clave maestra está cifrada en el HSM, el comando de la CLI generará una nueva clave de ajuste en el HSM y cifrará la clave maestra con la nueva clave de ajuste.

Si la clave maestra no está cifrada en el HSM, el comando de la CLI generará una nueva clave de ajuste en el HSM para su uso en el futuro.

Este comando no elimina la clave de ajuste anterior.

Almacenamiento de claves privadas en un HSM

Para una mayor seguridad, puede usar un HSM para asegurar las claves privadas que se usan en el descifrado SSL/TLS para:

- SSL forward proxy (Proxy SSL de reenvío): el HSM puede almacenar la clave privada del certificado de reenvío fiable que se utiliza para firmar certificados en operaciones de proxy SSL/TLS. A continuación, el cortafuegos enviará los certificados que genere durante estas operaciones al HSM para su firma antes de reenviarlos al cliente.
- SSL inbound inspection (Inspección de entrada SSL): el HSM puede almacenar las claves privadas de los servidores internos de los que está haciendo una inspección entrante de SSL/TLS.

Si utiliza algoritmos de intercambio de claves DHE o ECDHE para permitir la compatibilidad del secreto perfecto y permanente (perfect forward secrecy, PFS) para el descifrado SSL, puede utilizar un HSM para almacenar las claves privadas para la inspección entrante de SSL. También puede utilizar un HSM para almacenar claves ECDSA utilizadas para el descifrado de proxy SSL de reenvío o inspección entrante de SSL a no ser que use TLSv1.3. Para el tráfico TLSv1.3, PAN-OS admite HSM solo para el proxy SSL de reenvío. No es compatible con HSM para la inspección de SSL entrante.

STEP 1 | En el HSM, importe o genere el certificado y la clave privada utilizada en su implementación de descifrado.

Para obtener instrucciones sobre la importación o generación de un certificado y una clave privada en el HSM, consulte su documentación del HSM.

STEP 2 | (Solo nCipher nShield Connect) Sincronice los datos clave desde el sistema de archivos remoto nCipher nShield con el cortafuegos.

La sincronización con el HSM de SafeNet Network es automática.

1. Acceda a la interfaz web del cortafuegos y seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM**.
2. Seleccione **Synchronize with Remote Filesystem (Sincronizar con sistema de archivos remoto)** (ajustes de Operaciones de seguridad de hardware).

STEP 3 | Importe el certificado que corresponde a la clave almacenada en HSM.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)**.

© 2020 Palo Alto Networks, Inc.

2. Introduzca el **Certificate Name (Nombre de certificado)**.
3. Seleccione **Browse (Explorar)** para buscar el **Certificate File (Archivo de certificado)** en el HSM.
4. Seleccione un **File Format (Formato de archivo)**.
5. Seleccione **Private Key resides on Hardware Security Module (La clave privada reside en el módulo de seguridad de hardware)**.
6. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 4 | (Solo certificados de reenvío fiables) Habilite el certificado para su uso en el proxy SSL/TLS de reenvío.

1. Abra el certificado que importó en el paso 3 para editarlo.
2. Seleccione **Forward Trust Certificate (Certificados de reenvío fiables)**.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 5 | Compruebe que ha importado con éxito el certificado en el cortafuegos.

Localice el certificado que importó en el paso 3 y consulte el icono en la columna Key (Clave):

- **Icono de bloqueo**: la clave privada del certificado está en el HSM.
- **Icono de error**: la clave privada no está en el HSM o el HSM no está autenticado o conectado adecuadamente.

Gestión de la implementación del HSM

Puede realizar las siguientes tareas para gestionar la implementación del HSM:

- Visualice los ajustes de configuración del HSM.

  Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM**.

- Muestre la información detallada del HSM.

  Seleccione **Show Detailed Information (Mostrar información detallada)** en la sección Hardware Security Operations (Operaciones de seguridad de hardware).

  Aparecerá información relativa a los servidores HSM, el estado de HA del HSM y el hardware del HSM.

- Exporte el archivo de compatibilidad.

  Seleccione **Export Support File (Exportar archivo de asistencia)** en la sección Hardware Security Operations (Operaciones de seguridad de hardware).

  Se creará un archivo de prueba para ayudar en la asistencia a los clientes cuando se trate de solucionar un problema con una configuración del HSM en el cortafuegos.

- Restablezca la configuración del HSM.

  Seleccione **Reset HSM Configuration (Restablecer configuración de HSM)** en la sección Hardware Security Operations (Operaciones de seguridad de hardware).

  Seleccionar esta opción elimina todas las conexiones del HSM. Todos los procedimientos de autenticación deberán repetirse después de utilizar esta opción.

High Availability

La alta disponibilidad (HA, High Availability) es una implementación en la que dos cortafuegos se colocan en un grupo y o hasta 16 cortafuegos se colocan en un clúster de HA y su configuración se sincroniza para prevenir el fallo de un único punto en su red. La conexión de heartbeat entre los peers del cortafuegos garantiza una conmutación por error sin problemas en el caso de que falle un peer. La configuración de HA proporciona redundancia y le permite garantizar la continuidad de la actividad comercial.

- Descripción general de la alta disponibilidad
- Conceptos de HA
- Configuración de la HA activo/pasivo
- Configuración de HA activa/activa
- Descripción general de agrupación en clústeres de HA
- Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA
- Configuración de la agrupación en clústeres de HA
- Actualización de las claves de SSH de HA1 y configuración de sus opciones
- Estados del cortafuegos HA
- Referencia: sincronización HA
- Hoja de referencia de la CLI: HA

© 2020 Palo Alto Networks, Inc.

Descripción general de la alta disponibilidad

Puede configurar dos cortafuegos de Palo Alto Networks como un par de HA o configurar hasta 16 cortafuegos como miembros pares de un clúster de HA. Los peers del clúster pueden ser pares de HA o cortafuegos independientes. La HA le permite reducir al mínimo la inactividad al garantizar que haya un cortafuegos alternativo disponible en el caso de que falle el cortafuegos peer. Los cortafuegos en un clúster o par de HA dedicados o internos en el cortafuegos para sincronizar datos (configuraciones de red, objeto y política) y mantener la información de estado. Los peers no comparten información de la configuración específica de los cortafuegos, como la dirección IP de la interfaz de gestión o perfiles de administrador, la configuración específica de HA, datos de log y el Centro de comando de aplicación (ACC).

Para obtener una vista consolidada de aplicaciones y logs a través del clúster en HA, deberá utilizar Panorama, el sistema de gestión centralizado de Palo Alto Networks. Consulte Cambio de contexto—Cortafuegos o Panorama en la Guía del administrador de Panorama. Consulte los Requisitos para la HA activa/pasiva y los Requisitos previos para la HA activa/activa. Se recomienda encarecidamente que utilice Panorama para aprovisionar miembros del clúster de HA. Consulte las Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA.

Cuando se produce un fallo en un cortafuegos en un clúster o par de HA y el cortafuegos del peer toma el control de la tarea de proteger el tráfico, el evento se denomina una conmutación por error. Las condiciones que activan una conmutación por error son las siguientes:

- Falla una o más de las interfaces supervisadas. (Supervisión de enlaces)
- No se puede llegar a uno o más de los destinos especificados en el cortafuegos. (Supervisión de rutas)
- El cortafuegos no responde a sondeos de heartbeat. (Sondeos de heartbeat y mensajes de saludo)
- Un chip o componente de software crítico falla, lo que se conoce como supervisión del estado de la ruta del paquete.

Los cortafuegos de Palo Alto Networks admiten alta disponibilidad activo/activo o activo/pasivo de estado con sincronización de sesión y configuración, con algunas excepciones.

- Los cortafuegos VM-Series en Azure y los cortafuegos VM-Series en AWS solo admiten la HA con peers activo/pasivo.

  En AWS no se admite la HA si implementa el cortafuegos con el servicio Amazon Elastic Load Balancing (ELB), el cual se encarga de ofrecer las funciones de conmutación por error.
- Los cortafuegos VM-Series en Google Cloud Platform no admiten la HA.

Empiece por comprender los conceptos de HA y la Descripción general de agrupación en clústeres de HA si va a configurar la agrupación en clústeres de HA.

© 2020 Palo Alto Networks, Inc.

Conceptos de HA

Los siguientes temas ofrecen información conceptual sobre cómo funciona la HA en un cortafuegos de Palo Alto Networks:

- Modos de HA
- Enlaces de HA y enlaces de backup
- Prioridad y preferencia de dispositivos
- Conmutación por error
- Negociación previa de LACP y LLDP para HA activa/pasiva
- Dirección IP flotante y dirección MAC virtual
- Distribución de carga de ARP
- Redundancia basada en la ruta
- Temporizadores de HA
- Propietario de sesión
- Configuración de sesión
- NAT en modo HA activa/activa
- ECMP en modo HA activa/activa

Modos de HA

Puede configurar los cortafuegos en un par de HA en uno de dos modos:

- **Activo/pasivo**: Un dispositivo gestiona activamente el tráfico mientras que el otro está sincronizado y listo para pasar al estado activo en el caso de que se produjera un fallo. En este modo, ambos cortafuegos comparten los mismos ajustes de configuración y uno gestiona activamente el tráfico hasta que se produce un fallo de ruta, enlace, sistema o red. Cuando el cortafuegos activo falla, el cortafuegos pasivo pasa al estado activo y toma el control sin interrupciones, y aplica las mismas políticas para mantener la seguridad de red. El HA activo/pasivo es compatible con las implementaciones de Virtual Wire, capa 2 y capa 3.
- **Activo/Activo**: ambos cortafuegos están activos, procesan el tráfico y trabajan sincronizadamente para gestionar la configuración y la pertenencia de la sesión. Ambos cortafuegos mantienen individualmente las tablas de sesión y las tablas de enrutamiento y se sincronizan entre sí. El HA activo/activo es compatible con las implementaciones de Virtual Wire y capa 3.

  En el modo activo/activo HA, el cortafuegos no admite el cliente DHCP. Además, solo el cortafuegos activo-primario puede funcionar como retransmisión DHCP. Si el cortafuegos activo-secundario recibe paquetes de difusión de DHCP, los descarta.

  Una configuración activo/activo no equilibra la carga del tráfico. Si bien puede compartir la carga al enviar el tráfico al peer, no se produce el equilibrio de la carga. Algunas maneras de compartir la carga de sesiones con ambos cortafuegos incluyen el uso de ECMP, varios ISP y equilibradores de carga.

Al decidir si usar el modo activo/pasivo o activo/activo, tenga en cuenta las siguientes diferencias:

- El modo activo/pasivo tiene un diseño simple;.Es considerablemente más sencillo solucionar problemas de enrutamiento y flujo de tráfico en el modo activo/pasivo. El modo activo/pasivo admite una implementación de capa 2; el modo activo/activo no.
- El modo activo/activo requiere conceptos de diseño avanzados, lo que puede derivar en redes más complejas. Según cómo implemente el modo HA activo/activo, es posible que se necesite una configuración adicional, tal como la activación de protocolos de red en ambos cortafuegos, la replicación de grupos NAT y la implementación de direcciones IP flotantes para brindar una conmutación por error apropiada. Debido a que ambos cortafuegos procesan activamente el tráfico, los cortafuegos usan

© 2020 Palo Alto Networks, Inc.

conceptos adicionales de propiedad de sesión y configuración de sesión para realizar la inspección de contenido de capa 7. El modo activo/activo se recomienda si cada cortafuegos necesita sus propias instancias de enrutamiento y usted necesita una redundancia completa en tiempo real de los dos cortafuegos en todo momento. El modo activo/activo posee una conmutación por error más rápida y puede manejar mejor los flujos de tráfico que el modo activo/pasivo, debido a que ambos cortafuegos están procesando el tráfico de manera activa.



En el modo activo/activo, el par HA puede usarse para procesar temporalmente más tráfico de lo que un cortafuegos maneja normalmente. Sin embargo, esta no debe ser la norma, ya que el fallo de un cortafuegos hace que todo el tráfico se redireccione hacia el otro cortafuegos en el par HA. Su diseño debe permitir que el otro cortafuegos procese la capacidad máxima de sus cargas de tráfico con inspección de contenido habilitada. Si el diseño excede la capacidad del otro cortafuegos, se puede producir una alta latencia o el fallo de la aplicación.

Si desea información sobre cómo configurar sus cortafuegos en el modo activo/pasivo, consulte Configuración de la HA activa/pasiva. Si desea información sobre cómo configurar sus cortafuegos en el modo activo/activo, consulte Configuración de la HA activa/activa.

En un clúster de HA, todos los miembros se consideran activos; No existe un concepto de cortafuegos pasivos excepto los pares de HA en los clústeres, que pueden mantener su relación activo/pasivo después de agregarlos a un clúster de HA.

Enlaces de HA y enlaces de backup

Los cortafuegos configurados en un par de alta disponibilidad (high availability, HA) usan enlaces de HA para sincronizar los datos y mantener la información sobre el estado. Algunos modelos del cortafuegos tienen puertos de HA específicos, como enlace de control (HA1) y enlace de datos (HA2), mientras que otros requieren que utilice los puertos internos como enlaces de HA.

- En los cortafuegos con puertos de HA dedicados, utilice estos puertos para gestionar la comunicación y la sincronización entre los cortafuegos. Si desea información detallada, consulte Puertos de HA en cortafuegos Palo Alto Networks.
- En los cortafuegos sin puertos de HA dedicados, como PA-220 y PA-220R, se recomienda utilizar el puerto de gestión para el puerto de HA1 y el puerto de plano de datos para la copia de seguridad de HA1.



Para los cortafuegos sin puertos de HA dedicados, decida qué puertos usar para la copia de seguridad HA1 y HA1 en función de su entorno y conozca cuáles son los menos utilizados y los menos congestionados. Asigne HA1 a la mejor interfaz y la copia de seguridad de HA1 a la otra.

Los peers de HA en un clúster de HA pueden ser una combinación de miembros independientes y pares de HA. Los miembros del clúster HA utilizan un enlace HA4 y un enlace de reserva HA4 para realizar la sincronización del estado de la sesión. HA1 (enlace de control), HA2 (enlace de datos) y HA3 (enlace de reenvío de paquetes) no se admiten entre miembros del clúster que no son pares de HA.

Enlaces de HA y enlaces de backup	Description (Descripción)
Enlace de control	El enlace de HA1 se utiliza para intercambiar saludos, heartbeats e información de estado de HA, así como la sincronización del plano de gestión para el enrutamiento e información de User-ID. Los cortafuegos también usan este enlace para sincronizar cambios de configuración con su peer. El enlace de HA1 es un enlace de capa 3 y requiere una dirección IP.

© 2020 Palo Alto Networks, Inc.

Enlaces de HA y enlaces de backup	Description (Descripción)
	ICMP se utiliza para intercambiar heartbeats entre peers de HA. Puertos usados para HA1 y TCP: puertos TCP 28769 y 28260 para una comunicación con texto no cifrado; puerto 28 para una comunicación cifrada (SSH sobre TCP). Si habilita el cifrado en el enlace de HA1, también puede seguir el procedimiento Actualización de las claves de SSH de HA1 y configuración de sus opciones.
Enlace de datos	El enlace de HA2 se utiliza para sincronizar sesiones, reenviar tablas, asociaciones de seguridad de IPSec y tablas de ARP entre cortafuegos de un clúster en HA. El flujo de datos del enlace de HA2 siempre es unidireccional (excepto en la conexión persistente de HA2); fluye desde el cortafuegos activo o activo-principal al cortafuegos pasivo o pasivo-secundario. El enlace de HA2 es un enlace de capa 2 y utiliza el tipo ether 0x7261 de manera predeterminada. Puertos used for HA2: el enlace de datos de HA puede configurarse para utilizar IP (número de protocolo 99) o UDP (puerto 29281) como transporte, lo que permite que el enlace de datos de HA utilice subredes.
Vínculos de reserva HA1 y HA2	Proporcionan redundancia para los enlaces de HA1 y HA2. Los puertos internos se pueden utilizar como enlaces de respaldo para las conexiones HA1 y HA2 cuando los enlaces de respaldo dedicados no están disponibles. Tenga en cuenta las siguientes directrices al configurar enlaces de HA de backup: • Las direcciones IP de los enlaces de HA principal y backup no deben solaparse entre sí. • Los enlaces de backup de HA deben encontrarse en una subred diferente de la de los enlaces de HA principales. • Los puertos de backup de HA1 y HA2 deben configurarse en puertos físicos separados. El enlace de backup de HA1 utiliza los puertos 28770 y 28260. • Los cortafuegos PA-3200 Series no admiten direcciones IPv6 para el enlace de copia de seguridad de HA1. Utilice direcciones IPv4. *Palo Alto Networks recomienda habilitar el backup de heartbeat (que utiliza el puerto 28771 en la interfaz MGT) si utiliza un puerto interno para los enlaces de HA1 o backup de HA1.*
Enlace de reenvío de paquete	Además de los enlaces de HA1 y HA2, las implementaciones activa/activa también requieren un enlace HA3 dedicado. Los cortafuegos utilizan este enlace para el reenvío de paquetes al peer durante la configuración de la sesión y el flujo de tráfico asimétrico. El enlace de HA3 es un enlace de capa 2 que utiliza encapsulación MAC-in-MAC. No admite direcciones o cifrado de capa 3. Los cortafuegos de la serie PA-7000 sincronizan las sesiones de los NPC uno por uno. En los cortafuegos PA-800 Series, PA-3200 Series y PA-5200 Series, puede configurar interfaces agregadas como enlace de HA3. Las interfaces agregadas también pueden proporcionar redundancia para el enlace HA3; usted no puede configurar enlaces de copia de seguridad para el enlace HA3. En los cortafuegos serie PA-3200 PA-5200 y PA-7000, los

© 2020 Palo Alto Networks, Inc.

Enlaces de HA y enlaces de backup	Description (Descripción)
	puertos HSCI dedicados admiten el enlace HA3. El cortafuegos añade un encabezado de paquete exclusivo a los paquetes que cruzan el enlace HA3, por lo que la MTU en este enlace debe ser superior a la extensión máxima del paquete reenviado.
Enlace HA4 y enlace de reserva HA4	El enlace HA4 y el enlace de reserva HA4 realizan la sincronización de la caché de sesión entre todos los miembros del clúster de HA que tienen el mismo ID de clúster. El enlace HA4 entre los miembros del clúster detecta fallos de conectividad entre los miembros del clúster al enviar y recibir mensajes de conexión persistente de capa 2. Vea el estado de los enlaces de reserva HA4 y HA4 en el panel del cortafuegos.

Puertos de HA en cortafuegos Palo Alto Networks.

Cuando conecta dos cortafuegos Palo Alto Networks® en una configuración de alta disponibilidad (high availability, HA), recomendamos que utilice los puertos de HA dedicados para los enlaces de HA y enlaces de copia de seguridad. Estos puertos dedicados incluyen: los puertos HA1 con etiquetas HA1, HA1-A, y HA1-B que se utilizan para el control de HA y el tráfico de sincronización; y los puertos HA2 y de interconexión de bastidor de alta velocidad (High Speed Chassis Interconnect, HSCI) que se utilizan para el tráfico de configuración de sesiones de HA. Los cortafuegos serie PA-5200 poseen puertos auxiliares multipropósito con etiquetas AUX-1 y AUX-2 que puede configurar para el tráfico de HA1.

También puede configurar el puerto HSCI para HA3, que se utiliza para el reenvío de paquetes al cortafuegos del peer durante la configuración de la sesión y el flujo asimétrico de tráfico (únicamente HA activo/activo). El puerto HSCI puede utilizarse para tráfico HA2, tráfico HA3 o ambos.

Los enlaces de HA1 y AUX proporcionan sincronización para las funciones que residen en el plano de gestión. Utilizar las interfaces de HA específicas del plano de gestión es más eficaz que utilizar los puertos internos, ya que así se elimina la necesidad de pasar los paquetes de sincronización a través del plano de datos.

Si el cortafuegos no posee puertos de HA dedicados, puede configurar los puertos de datos como interfaces de HA. Si el cortafuegos posee puertos de HA dedicados, pero no posee un puerto de respaldo de HA dedicado, también puede configurar los puertos de datos como respaldo para los puertos de HA dedicados.

Siempre que sea posible, conecte los puertos de HA directamente entre los dos cortafuegos en un par de HA (no a través de un conmutador o enrutador) para evitar problemas en el enlace de HA y la comunicación que puedan ocasionarse si se produce un problema de red.

Utilice la siguiente tabla para obtener más información sobre los puertos de HA dedicados y cómo conectarse a los enlaces de HA y enlaces de respaldo:

Modelo	Puertos dedicados del panel frontal
Cortafuegos de PA-800 Series	• **HA1 y HA2**: puertos Ethernet de 10 Mbps/100 Mbps/1000 Mbps que se utilizan para HA1 y HA2 en ambos modos de HA. • **Para tráfico de HA1**: conecte el puerto HA1 del primer cortafuegos directamente al puerto HA1 del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.

© 2020 Palo Alto Networks, Inc.

Modelo	Puertos dedicados del panel frontal
	• **Para tráfico de HA2**: conecte el puerto HA2 del primer cortafuegos directamente al puerto HA2 del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.

Cortafuegos de PA-3200 Series	• **HA1-A y HA1-B**: puertos Ethernet de 10 Mbps/100 Mbps/1000 Mbps que se utilizan con el tráfico de HA1 en ambos modos de HA.
	  • **Para tráfico de HA1**: conecte el puerto HA1-A del primer cortafuegos directamente al puerto HA1-A del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	  • **Para un respaldo de la conexión de HA1-A**: conecte el puerto HA1-B del primer cortafuegos directamente al puerto HA1-B del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	
	  *Si el plano de datos del cortafuegos se reinicia debido a un fallo o a un reinicio manual, el enlace HA1-B también se reiniciará. Si esto ocurre y el enlace de HA1-A no está conectado ni configurado, se produce una condición de división. Por lo tanto, recomendamos que conecte y configure los puertos de HA1-A y los puertos de HA1-B para proporcionar redundancia y evitar problemas de división.*
	
	  *Puede reasignar los puertos SFP del cortafuegos como puertos HA1-A y HA1-B a través de PAN-OS o Panorama.*
	
	• **HSCI**: el puerto HSCI es una interfaz SFP+ de capa 1 que conecta dos cortafuegos serie PA-3200 en una configuración de HA. Utilice este puerto para una conexión de HA2, una conexión de HA3 o ambas.
	
	El tráfico que se transporta en los puertos HSCI es tráfico sin formato de capa 1, que no es enrutable o conmutable. Por lo tanto, debe conectar los puertos HSCI directamente entre sí (desde el puerto HSCI del primer cortafuegos al puerto HSCI del segundo cortafuegos).

Cortafuegos PA-5200 Series	• **HA1-A y HA1-B**: puertos Ethernet de 10 Mbps/100 Mbps/1000 Mbps que se utilizan con el tráfico de HA1 en ambos modos de HA.
	  • **Para tráfico de HA1**: conecte el puerto HA1-A del primer cortafuegos directamente al puerto HA1-A del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	  • **Para un respaldo de la conexión de HA1-A**: conecte el puerto HA1-B del primer cortafuegos directamente al puerto HA1-B del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	
	• **HSCI**: el puerto HSCI es una interfaz de capa 1 que conecta dos cortafuegos serie PA-5200 en una configuración de HA. Utilice este puerto para una conexión de HA2, una conexión de HA3 o ambas.

© 2020 Palo Alto Networks, Inc.

Modelo	Puertos dedicados del panel frontal
	El puerto HSCI en el cortafuegos PA-5220 es un puerto QSFP+ y el puerto HSCI en los cortafuegos PA-5250, PA-5260 y PA-5280 es un puerto QSFP28. El tráfico que se transporta en el puerto HSCI es tráfico sin formato de capa 1, que no es enrutable o conmutable. Por lo tanto, debe conectar los puertos HSCI directamente entre sí (desde el puerto HSCI del primer cortafuegos al puerto HSCI del segundo cortafuegos).

Cortafuegos serie PA-5200 (continuación)	• **AUX-1 y AUX-2**: los puertos SFP+ auxiliares son puertos multipropósito que puede configurar para HA1, funciones de gestión o reenvío de logs a Panorama. Utilice estos puertos cuando necesite una conexión de fibra para una de estas funciones.
	  • **Para tráfico de HA1**: conecte el puerto AUX-1 del primer cortafuegos directamente al puerto AUX-1 del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	  • **Para un respaldo de la conexión de AUX-1**: conecte el puerto AUX-2 del primer cortafuegos directamente al puerto AUX-2 del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.

Cortafuegos PA-7000 Series	• **HA1-A y HA1-B**: puertos Ethernet de 10 Mbps/100 Mbps/1000 Mbps que se utilizan con el tráfico de HA1 en ambos modos de HA.
	  • **Para tráfico de HA1**: conecte el puerto HA1-A del primer cortafuegos directamente al puerto HA1-A del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	  • **Para un respaldo de la conexión de HA1-A**: conecte el puerto HA1-B del primer cortafuegos directamente al puerto HA1-B del segundo cortafuegos del par, o bien conéctelos juntos a través de un conmutador o enrutador.
	
	No puede configurar una conexión de HA1 en los puertos de datos de NPC ni en el puerto de gestión (MGT).
	• **HSCI-A y HSCI-B**: los puertos HSCI son interfaces SFP+ de capa 1 que conectan dos cortafuegos serie PA-7000 en una configuración de HA. Utilice estos puertos para una conexión de HA2, una conexión de HA3 o ambas.
	
	El tráfico que se transporta en los puertos HSCI es tráfico sin formato de capa 1, que no es enrutable o conmutable. Por lo tanto, debe conectar estos puertos de la siguiente manera:
	  • **Para tráfico de HA2 y HA3**: conecte el puerto HSCI-A en el primer cortafuegos directamente al puerto HSCI-A en el segundo cortafuegos.

© 2020 Palo Alto Networks, Inc.

Modelo	Puertos dedicados del panel frontal
	Para el tráfico de HA2 o HA2/HA3, los cortafuegos serie PA-7000 sincronizan las sesiones en las NPC una a una. • **Para un respaldo de la conexión HSCI-A**: debe conectar el puerto HSCI en el primer cortafuegos directamente al puerto HSCI del segundo cortafuegos. *Los enlaces HA2 y de reserva de HA2 se pueden configurar para usar una interfaz de plano de datos en lugar de los puertos HSCI. Sin embargo, si se configura de esta manera, los enlaces HA2 y de reserva HA2 deben usar interfaces de plano de datos. Una combinación de un puerto de plano de datos y un puerto HSCI para HA2 o reserva de HA2 generará en un error de confirmación. Esto se aplica a PA-7050-SMC, PA-7080-SMC, PA-7050-SMC-B y PA-7080-SMC-B.*

Prioridad y preferencia de dispositivos

Puede asignar un valor de *prioridad de dispositivo* a los cortafuegos de un par de alta disponibilidad (high availability, HA) si desea indicar el preferido para asumir la función activa. Si necesita utilizar un cortafuegos específico del clúster en HA para proteger de manera activa el tráfico, debe habilitar el comportamiento de preemption en ambos cortafuegos y asignar un valor de prioridad de dispositivo para cada cortafuegos. Se designa como activo el cortafuegos que tiene el valor numérico más bajo y, por lo tanto, la *prioridad más alta*. El otro cortafuegos es el pasivo.

Se aplica lo mismo a los pares activo/activo de HA, aunque se emplea el *ID de dispositivo* para asignarle una prioridad. Cuanto menor es el valor numérico del ID del dispositivo, mayor es la prioridad. El cortafuegos con más prioridad se convierte en activo-principal y su peer, en activo-secundario.

De manera predeterminada, la preemption está deshabilitada en los cortafuegos y debe habilitarse en ambos cortafuegos. Cuando se habilita, el comportamiento de preemption permite que el cortafuegos con la *mayor prioridad* (valor numérico más bajo) vuelva a estar activo o activo-principal cuando se recupere de un fallo. Cuando se produce una preferencia, el evento se registra en los logs del sistema.

Conmutación por error

Cuando se produce un fallo en un cortafuegos y el peer en el par de HA (o un peer en el clúster de HA) asume la tarea de asegurar el tráfico, el evento se denomina *conmutación por error*. Una conmutación por error se activa, por ejemplo, cuando falla una métrica supervisada en un cortafuegos en el par HA. Las métricas que supervisa el cortafuegos para detectar un fallo en el cortafuegos son las siguientes:

- **Sondeos de heartbeat y mensajes de saludo**

  Los cortafuegos utilizan mensajes de saludo y heartbeats para comprobar que el cortafuegos peer responde y está operativo. Los mensajes de saludo se envían desde un peer al otro en el *intervalo de saludo* configurado para comprobar el estado del cortafuegos. El heartbeat es un ping ICMP para el peer de HA a través del enlace de control y el peer responde al ping para establecer que los cortafuegos están conectados y responden. De manera predeterminada, el intervalo para el heartbeat es de 1.000 milisegundos. Un ping se envía cada 1.000 milisegundos y si se detectan tres pérdidas de heartbeat consecutivas, se produce un error. Si desea información detallada sobre los temporizadores de HA que activan una conmutación por error, consulte Temporizadores de HA.

© 2020 Palo Alto Networks, Inc.

- **Supervisión de enlaces**

  Puede especificar un grupo de interfaces físicas que el cortafuegos supervisará (un grupo de enlaces) y el cortafuegos supervisará el estado de cada enlace en el grupo (enlace activado o desactivado). Determine la condición de fallo para el grupo de enlaces: **Any (Cualquier)** enlace inactivo o **All (Todos)** los enlaces inactivos en el grupo constituyen un fallo del grupo de vínculos (pero no necesariamente una conmutación por error).

  Puede crear varios grupos de enlaces. Por lo tanto, también debe determinar la condición de fallo del conjunto de grupos de enlaces: **Any (Cualquier)** grupo de enlaces falla o **All (Todos)**los grupos de enlaces fallan, lo que determina cuándo se activa una conmutación por error. El comportamiento predeterminado es que el fallo de **cualquier** enlace de **cualquier** grupo de enlaces haga que el cortafuegos cambie el estado de HA a no funcional (o al estado provisional en el modo activo/activo) para indicar el fallo de un objeto supervisado.
- **Monitorización de rutas**

  Puede especificar un grupo de direcciones IP de destino que el cortafuegos se encargará de supervisar. El cortafuegos supervisa la ruta completa a través de la red a direcciones IP de misión crítica mediante pings ICMP para verificar la accesibilidad de la dirección IP. El intervalo predeterminado para pings es de 200 ms. Una dirección IP se considera inalcanzable cuando fallan 10 pings consecutivos (valor predeterminado). Especifique la condición de fallo para las direcciones IP en un grupo de IP de destino: **Any (Cualquier)** dirección IP inaccesible o **All (Todas)** las direcciones IP inaccesibles en el grupo. Puede especificar varios grupos de IP de destino para un grupo de ruta para un cable virtual, VLAN o enrutador virtual; especifique la condición de fallo de los grupos de IP de destino en un grupo de rutas: **Any (Cualquier)** o **All (Todas)**, lo que constituye una fallo en el grupo de rutas. Puede configurar varios grupos de rutas de cables virtuales, grupos de rutas de VLAN y grupos de rutas de enrutadores virtuales.

  Determine también la condición de fallo global: **Any (Cualquier)** grupo de rutas falla o **All (Todos)**los grupos de rutas fallan, lo que determina cuándo se activa una conmutación por error. El comportamiento predeterminado es que **cualquier** dirección IP que se vuelva inaccesible en **cualquier** grupo de IP de destino en **cualquier** ruta de enrutador virtual, VLAN o cable virtual hará que el cortafuegos cambie el estado de HA a no funcional (o al estado provisional en modo activo/activo) para indicar un fallo de un objeto supervisado.

Además de los activadores de conmutación por error enumerados anteriormente, también se produce una conmutación por error cuando el administrador suspende el cortafuegos o si se produce un adelantamiento.

En los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series, se puede producir una conmutación por error si falla una comprobación de estado interna. Esta comprobación de estado no es configurable y se habilita para verificar los componentes críticos del cortafuegos, tales como las FPGA y CPU. Además, las comprobaciones de estado general se producen en cualquier plataforma que produzca un error.

A continuación, se describe lo que ocurre si se produce un fallo de la tarjeta de procesamiento de red (NPC, Network Processing Card) en un cortafuegos de PA-7000 Series miembro de un clúster de HA:

- Si la NPC que se está utilizando para mantener la caché de la sesión de agrupación en clúster de HA (una copia de las sesiones de los otros miembros) deja de funcionar, el cortafuegos también dejará de funcionar. Si esto ocurre, el dispositivo de distribución de sesiones (como equilibrador de carga) debe detectar que el cortafuegos está inactivo y distribuir la carga de la sesión a los otros miembros del clúster.
- Si la NPC de un miembro del clúster deja de funcionar y no se habilita la supervisión de enlaces o la supervisión de ruta en esa NPC, el miembro del cortafuegos de PA-7000 Series permanecerá activo, pero con una capacidad inferior, ya que hay una NPC inactiva.
- Si la NPC de un miembro del clúster deja de funcionar y se habilita la supervisión de enlaces o de rutas en esa NPC, el cortafuegos de PA-7000 Series dejará de funcionar y el dispositivo de distribución de sesiones (como equilibrador de carga) deberá detectar que el cortafuegos está inactivo y distribuir la carga de la sesión a los otros miembros del clúster.

© 2020 Palo Alto Networks, Inc.

Negociación previa de LACP y LLDP para HA activa/pasiva

Si un cortafuegos utiliza LACP o LLDP, la negociación de estos protocolos tras la conmutación por error previene una conmutación por error de fracciones de segundo. Sin embargo, puede habilitar una interfaz en un cortafuegos pasivo para negociar LACP y LLDP antes de la conmutación por error. Por lo tanto, un cortafuegos en estado HA Passive (Pasivo) o Non-functional (No funcional) puede comunicarse con los dispositivos cercanos utilizando LACP o LLDP. Dicha negociación previa acelera la conmutación por error.

Todos los modelos de cortafuegos, excepto los VM-Series, admiten una configuración de negociación previa, que depende de si la interfaz Ethernet o AE está en una implementación de capa 2, capa 3 o cable virtual. Un cortafuegos HA pasivo maneja los paquetes LACP y LLDP de una de las dos maneras siguientes:

- **Activo**: el cortafuegos tiene LACP o LLDP configurados en la interfaz y participa activamente en la negociación previa de LACP o LLDP, respectivamente.
- **Pasivo**: LACP o LLDP no están configurados en la interfaz y el cortafuegos no participa en el protocolo, pero permite que los peers en cada lado del cortafuegos negocien previamente LACP o LLDP respectivamente.

La siguiente tabla muestra qué implementaciones son compatibles con las interfaces Ethernet de agregación (AE, Aggregate Ethernet) y Ethernet.

Implementación de interfaz	Interfaz AE	Interfaz Ethernet
LACP en capa 2	Activo	No compatible
LACP en capa 3	Activo	No compatible
LACP en cable virtual	No compatible	Pasivo
LLDP en capa 2	Activo	Activo
LLDP en capa 3	Activo	Activo
LLDP en cable virtual	Activo	• Activo si el propio LLDP está configurado. • Pasivo si el propio LLDP no está configurado.

La negociación previa no se admite en subinterfaces o en interfaces de túnel.

Para configurar la negociación previa de LACP o LLDP, consulte el paso (Opcional) Habilite LACP and LLDP Pre-Negotiation for Active/Passive HA (Negociación previa de LACP y LLDP para la HA activa/pasiva) para una conmutación por error más rápida si su red utiliza LACP o LLDP.

Dirección IP flotante y dirección MAC virtual

En una implementación de capa 3 del modo HA activo/activo, usted puede asignar direcciones IP flotantes, que se mueven de un cortafuegos HA a otro si un enlace o cortafuegos falla. La interfaz en el cortafuegos que posee la dirección IP flotante responde a solicitudes de ARP con una dirección MAC virtual.

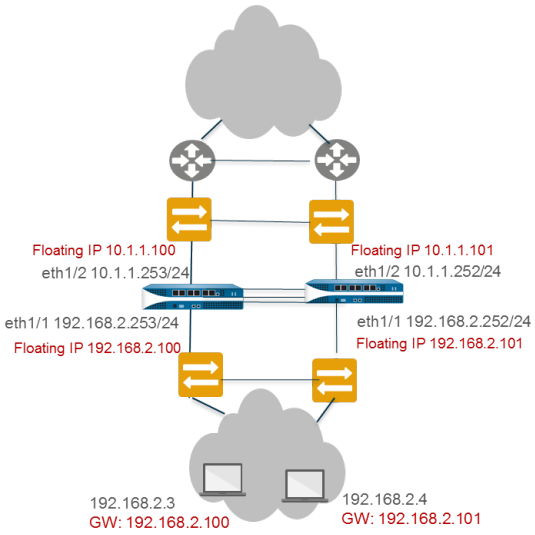
Las direcciones IP flotantes se recomiendan cuando necesita funcionalidades tales como el protocolo de redundancia de enrutador virtual (Virtual Router Redundancy Protocol, VRRP). Las direcciones IP flotantes también pueden usarse para implementar VPN y NAT de origen, lo que permite conexiones persistentes cuando el cortafuegos que ofrece esos servicios falla.

© 2020 Palo Alto Networks, Inc.

Como se muestra en la siguiente figura, cada interfaz de cortafuegos HA tiene su propia dirección IP y dirección IP flotante. La dirección IP de la interfaz sigue siendo local para el cortafuegos, pero, si este falla, la dirección IP flotante se mueve entre los cortafuegos. Usted configura los hosts de destino para usar una dirección IP flotante como la puerta de enlace por defecto, lo que le permite cargar el tráfico de equilibrio a los dos peers HA. También puede usar equilibradores de carga externos para cargar el tráfico de equilibrio.

Si un enlace o cortafuegos falla o un evento de supervisión de ruta produce un fallo, la dirección IP flotante y la dirección MAC virtual se mueven hacia el cortafuegos funcional. (En la siguiente figura , cada cortafuegos tiene dos direcciones IP flotantes y direcciones MAC virtuales; todas migran si el cortafuegos falla). El cortafuegos en funcionamiento envía un ARP gratuito para actualizar las tablas MAC de los conmutadores conectados para informar del cambio en la dirección IP flotante y la propiedad de la dirección MAC para redireccionar el tráfico hacia él.

Una vez que se recupera el cortafuegos fallido, la dirección IP flotante y la dirección MAC virtual regresan por defecto al cortafuegos con el ID de dispositivo [0 o 1] al que está vinculada la dirección IP. Específicamente, una vez que el cortafuegos fallido se recupera, este vuelve a estar en línea. El cortafuegos actualmente activo determina que el cortafuegos está nuevamente en línea y comprueba si la dirección IP flotante que está manejando pertenece originalmente a él o al otro cortafuegos. Si la dirección IP flotante estaba vinculada originalmente al otro ID de dispositivo, el cortafuegos automáticamente la devuelve. (Para conocer una alternativa a este comportamiento predeterminado, consulte Caso de uso: configuración HA activa/activa con dirección IP flotante enlazada a cortafuegos activo-principal).



Cada cortafuegos del par HA crea una dirección MAC virtual para cada una de sus interfaces que posee una dirección IP flotante o dirección IP de uso compartido de carga de ARP.

El formato de la dirección MAC virtual (de los cortafuegos que no sean PA-7000, PA-5200 y PA-3200 Series) es 00-1B-17-00-xx-yy, donde 00-1B-17 es el ID del proveedor (Palo Alto Networks en este caso); 00, un valor fijo; xx, el ID del dispositivo y el ID del grupo (como se muestra en la siguiente figura); e yy, el ID de la interfaz:

7	6	5 4 3 2 1 0	7 6 5 4 3 2 1 0
ID de dispositivo	0	ID de grupo	ID de interfaz

El formato de la dirección MAC virtual de los cortafuegos PA-7000, PA-5200 y PA-3200 Series es B4-0C-25-xx-xx-xx, donde B4-0C-25 es el ID del proveedor (Palo Alto Networks en este caso) y los 24 bits siguientes indican el ID del dispositivo, el ID del grupo y el ID de la interfaz, tal como figura a continuación:

© 2020 Palo Alto Networks, Inc.

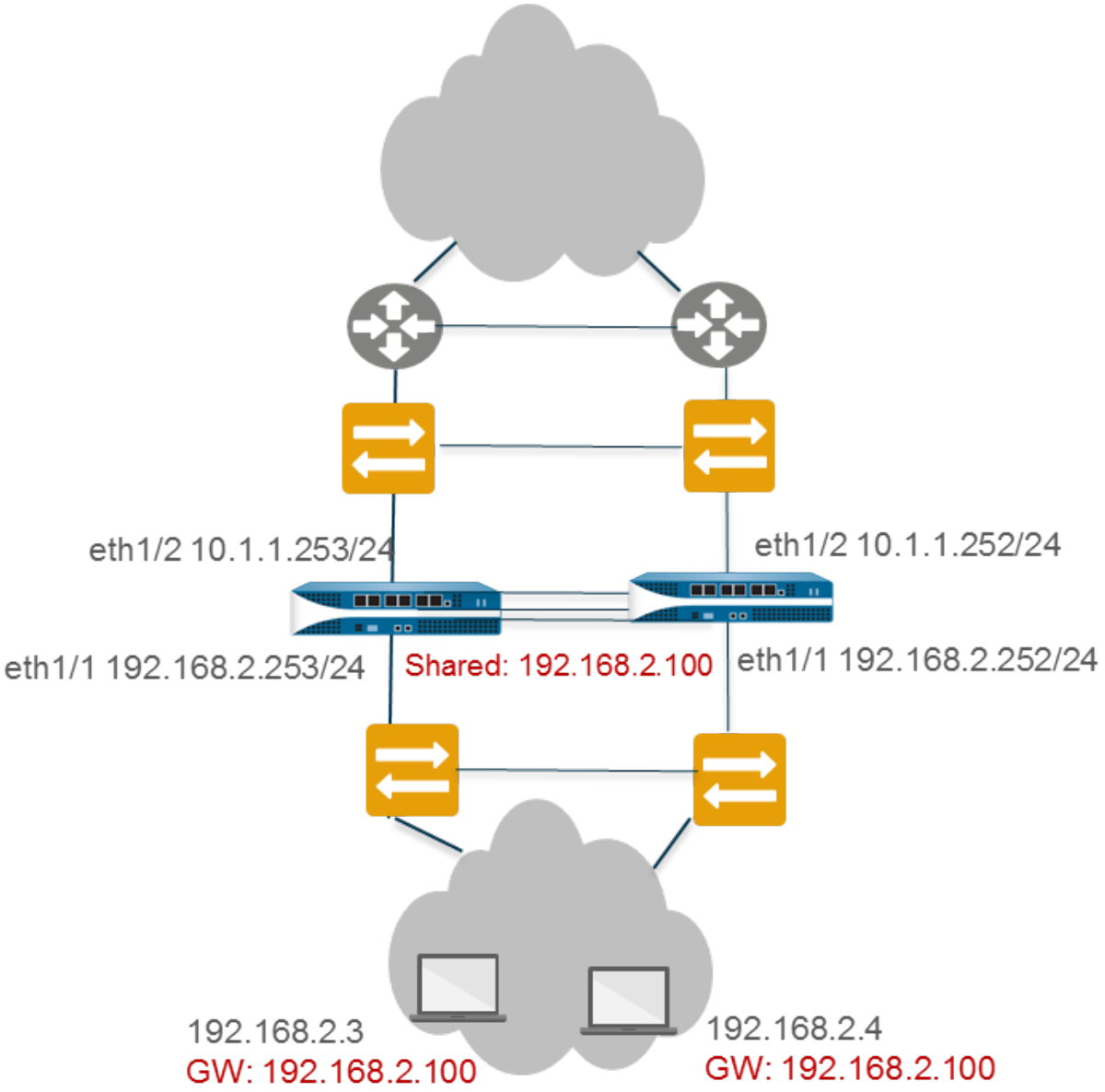
7 6 5	4	3 2 1 0 7 6	5 4 3 2	1 0 7 6 5 4 3 2 1 0
111	ID de dispositivo	ID de grupo	0000	ID de interfaz

Cuando un cortafuegos activo toma el control, envía ARP gratuitos de cada una de sus interfaces conectadas para informar a los conmutadores de capa 2 conectados de la nueva ubicación de la dirección MAC virtual. Para configurar direcciones IP flotantes, consulte Caso de uso: configuración de HA activa/activa con direcciones IP flotantes.

Distribución de carga de ARP

En una implementación de interfaz de capa y configuración HA activa/activa, la distribución de carga de ARP permite que los cortafuegos compartan una dirección IP y proporcionen servicios de puerta de enlace. Use la distribución de carga de ARP únicamente cuando no haya ningún dispositivo de capa 3 entre el cortafuegos y los hosts de destino; es decir, cuando los hosts de destino utilicen el cortafuegos como la puerta de enlace por defecto.

© 2020 Palo Alto Networks, Inc.



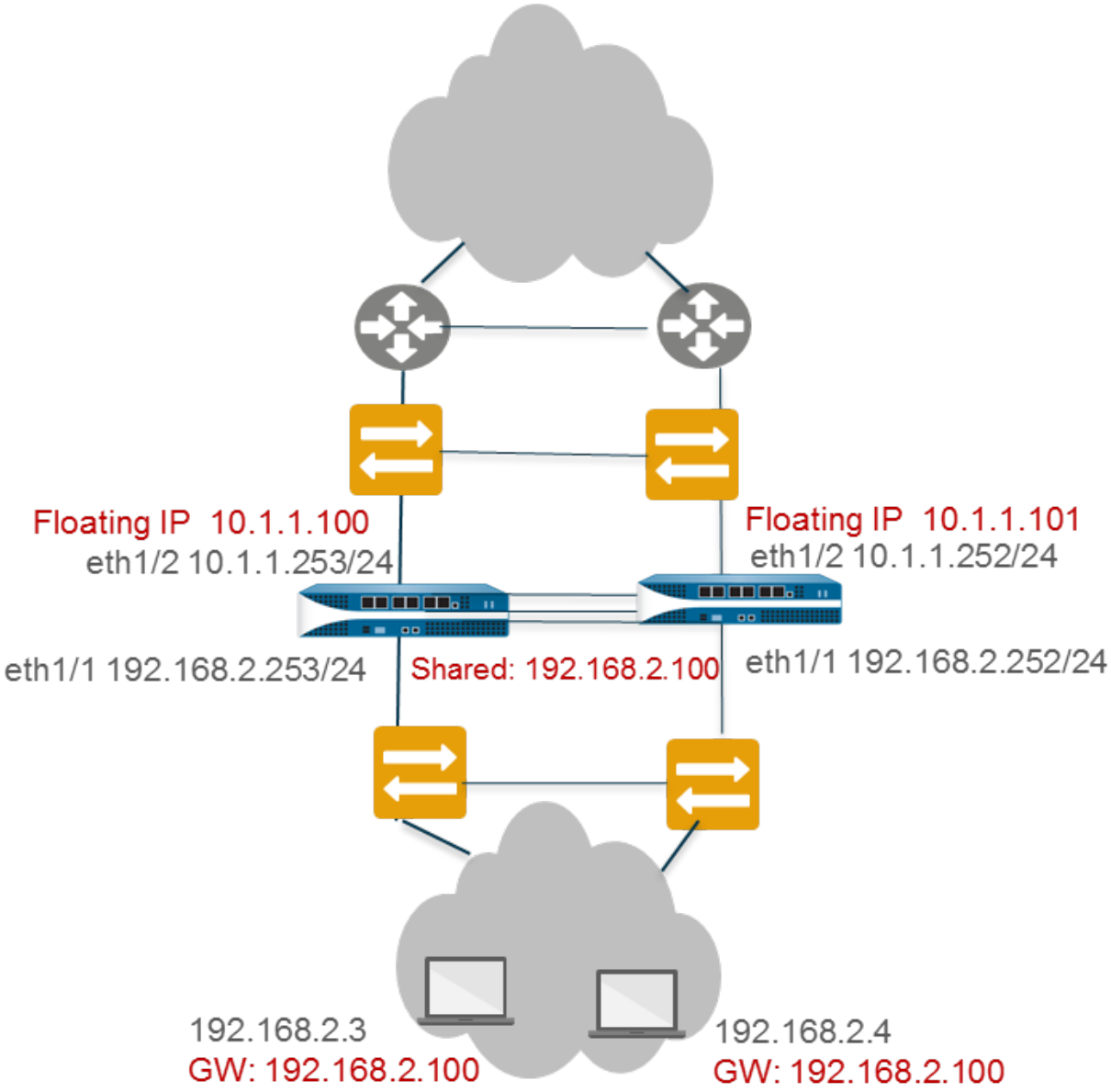
En este escenario, todos los hosts se configuran con una única dirección IP de puerta de enlace. Uno de los cortafuegos responde a solicitudes de ARP para la dirección IP de puerta de enlace con su dirección MAC virtual. Cada cortafuegos posee una dirección MAC virtual única generada para la dirección IP compartida. El algoritmo de carga compartida que controla qué cortafuegos responderá a la solicitud de ARP es configurable; se determina mediante el cálculo del hash o módulo de la dirección IP de origen de la solicitud de ARP.

Después de que el host de destino recibe la respuesta de ARP de la puerta de enlace, captura la dirección MAC y todo el tráfico del host se envía a través del cortafuegos que respondió con la dirección MAC virtual durante el periodo de almacenamiento en caché del ARP. El periodo de almacenamiento en caché del ARP depende del sistema operativo del host de destino.

Si un enlace o cortafuegos falla, la dirección IP flotante y la dirección MAC virtual se mueven hacia el cortafuegos funcional. El cortafuegos funcional envía ARP gratuitos para actualizar la tabla MAC de los conmutadores conectados para redirigir hacia él el tráfico desde el cortafuegos fallido. Consulte Caso de uso: configuración de alta disponibilidad activa/activa con uso compartido de carga de ARP.

© 2020 Palo Alto Networks, Inc.

Puede configurar interfaces en el lado WAN de los cortafuegos HA con direcciones IP flotantes y configurar interfaces en el lado LAN de los cortafuegos HA con una dirección IP compartida para la distribución de carga de ARP. Por ejemplo, la siguiente figura ilustra las direcciones IP flotantes para los enrutadores perimetrales WAN anteriores y una dirección de distribución de carga ARP para los hosts en el segmento LAN.

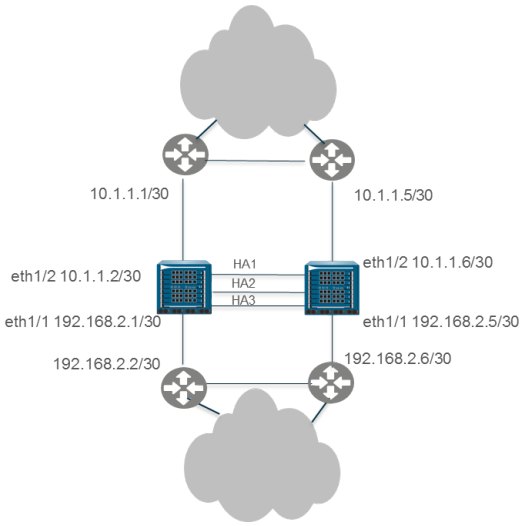


Redundancia basada en la ruta

En una implementación de interfaz de capa 3 y una configuración activa/activa, los cortafuegos están conectados a enrutadores, no a conmutadores. Los cortafuegos usan protocolos de enrutamiento dinámico para determinar la mejor ruta (ruta asimétrica) y para compartir la carga entre el par HA. En ese caso no se necesita ninguna dirección IP. Si un enlace, ruta supervisada o cortafuegos falla, o si la detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) detecta un fallo de enlace, el protocolo de enrutamiento (RIP, OSPF o BGP) se encarga del nuevo enrutamiento del tráfico hacia el cortafuegos en funcionamiento. Usted configura cada interfaz de cortafuegos con una nueva dirección IP única. Las direcciones IP siguen siendo locales para el cortafuegos en el que están configuradas; no se mueven entre

© 2020 Palo Alto Networks, Inc.

dispositivos cuando un cortafuegos falla. Consulte Caso de uso: configuración de HA activa/activa con redundancia basada en la ruta.



Temporizadores de HA

Los temporizadores de alta disponibilidad (high availability, HA) facilitan que el cortafuegos detecte un fallo y active una conmutación por error. Para reducir la complejidad al configurar temporizadores de un par de HA, puede seleccionar uno de los tres perfiles: **Recomendada**, **Agresivo** y **Avanzado**. Estos perfiles cumplimentan automáticamente los valores óptimos del temporizador de HA para la plataforma de cortafuegos específica con el fin de habilitar una implementación de HA más rápida.

Utilice el perfil **Recommended (Recomendado)** para ajustes comunes del temporizador de conmutación por error y el perfil **Aggressive (Agresivo)** para ajustes más rápidos del temporizador de conmutación por error. El perfil **Advanced (Avanzado)** le permite personalizar los valores del temporizador para que se adapten a sus requisitos de red.

La siguiente tabla describe cada temporizador incluido en los perfiles y los valores preestablecidos actuales (recomendados/agresivos) de los diferentes modelos de hardware; estos valores se indican únicamente como referencia y pueden cambiar en versiones posteriores.

Los temporizadores que afectan a los miembros de un clúster HA se describen en Configuración de la agrupación en clústeres de HA.

Temporizadores	Description (Descripción)	PA-7000 Series PA-5200 Series Serie PA-3200	PA-800 Series PA-220 VM-SERIES	Dispositivo virtual Panorama Panorama M-Series
Tiempo de espera ascendente tras fallo de supervisor (ms)	Intervalo durante el cual el cortafuegos permanecerá activo tras un fallo de supervisor de ruta o supervisor de enlace. Se recomienda este ajuste para evitar una conmutación por error de HA debido a los	0/0	0/0	0/0

© 2020 Palo Alto Networks, Inc.

Temporizadores	Description (Descripción)	PA-7000 Series PA-5200 Series Serie PA-3200	PA-800 Series PA-220 VM-SERIES	Dispositivo virtual Panorama Panorama M-Series
	flaps ocasionales de los dispositivos vecinos.			
Preemption Hold Time (min)	Tiempo que un cortafuegos pasivo o secundario activo esperará antes de tomar el control como dispositivo activo o principal activo.	1/1	1/1	1/1
Intervalo de heartbeat (ms)	Frecuencia con la que los peers de HA intercambian mensajes de heartbeat en forma de un ICMP (ping).	1000/1000	2000/1000	2000/1000
Tiempo de espera de promoción (ms)	Tiempo que el cortafuegos pasivo (en el modo activo/pasivo) o el cortafuegos secundario activo (en el modo activo/activo) esperará antes de tomar el control como cortafuegos activo o principal activo después de perder las comunicaciones con el peer de HA. Este tiempo de espera únicamente comenzará después de haber realizado una declaración de fallo de peer.	2000/500	2000/500	2000/500
Tiempo de espera principal adicional (ms)	Intervalo de tiempo en milisegundos que se aplica al mismo evento que Monitor Fail Hold Up Time (Tiempo de espera activo tras un fallo de supervisor) (el intervalo es de 0 a 60 000; el valor predeterminado es 500). El intervalo de tiempo adicional únicamente se aplica al cortafuegos activo en el modo activo/pasivo y al cortafuegos principal activo en el	500/500	500/500	7000/5000

© 2020 Palo Alto Networks, Inc.

Temporizadores	Description (Descripción)	PA-7000 Series PA-5200 Series Serie PA-3200	PA-800 Series PA-220 VM-SERIES	Dispositivo virtual Panorama Panorama M-Series
	modo activo/activo. Se recomienda este temporizador para evitar una conmutación por error cuando ambos cortafuegos experimentan el mismo fallo de supervisor de enlace/ruta simultáneamente.			
Hello Interval (ms)	Intervalo de tiempo en milisegundos entre los paquetes de saludo enviados para verificar que la funcionalidad de HA del otro cortafuegos está operativo (el intervalo es de 8000 a 60 000; el valor predeterminado es 8000).	8000/8000	8000/8000	8000/8000
N.º máximo de flaps	Se cuenta un flap cuando se produce una de las siguientes situaciones: • Un cortafuegos con preferencia deja el estado activo dentro de los 20 minutos posteriores a su activación. • Un enlace o ruta no puede permanecer activo durante 10 minutos después de empezar a funcionar. En el caso de un una preferencia errónea o un bucle no funcional, este valor indica el número máximo de flaps permitidos antes de suspender el cortafuegos (el intervalo es de 0 a 16; el valor predeterminado es 3).	3/3	3/3	No aplicable

© 2020 Palo Alto Networks, Inc.

Propietario de sesión

En una configuración HA activa/activa, ambos cortafuegos están activos simultáneamente, lo que significa que los paquetes pueden distribuirse entre ellos. Dicha distribución requiere que los cortafuegos desempeñen dos funciones: propiedad de la función y configuración de la sesión. En general, cada cortafuegos del par desempeña una de estas funciones, con lo cual se evitan condiciones de carrera que pueden producirse en entornos enrutados asimétricamente.

Puede configurar el propietario de las sesiones bien como el cortafuegos que recibe el primer paquete de una nueva sesión desde el host de destino, o bien como el cortafuegos que está en estado activo-primario (el dispositivo principal). Si el dispositivo principal está configurado, pero el cortafuegos que recibe el primer paquete no está en estado activo-primario, el cortafuegos reenvía el paquete al cortafuegos peer (el propietario de la sesión) mediante el enlace HA3.

El propietario de la sesión realiza todo el procesamiento de capa 7, tal como App-ID, Content-ID y exploración en busca de amenazas para la sesión. El propietario de la sesión también genera todos los logs de tráfico para la sesión.

Si el propietario de la sesión falla, el cortafuegos peer se convierte en el propietario de la sesión. Las sesiones existentes conmutan por error al cortafuegos en funcionamiento y no hay procesamiento de capa 7 disponible para esas sesiones. Cuando un cortafuegos se recupera de un fallo, por defecto, todas las sesiones de su propiedad antes del fallo regresan al cortafuegos original; el procesamiento de capa 7 no se reanuda.

Si usted configura la propiedad de la sesión en el dispositivo principal, la configuración de la sesión regresa por defecto al dispositivo principal también.

Palo Alto Networks recomienda configurar el propietario de sesión en el primer paquete y la configuración de sesión en el módulo IP, a menos que se indique lo contrario en un caso de uso específico. Si configura el propietario de sesión en el primer paquete, se reduce el tráfico en el enlace de HA3 y permite distribuir la carga del plano de datos entre los peers.

La configuración del propietario de sesión y configuración de sesión en el dispositivo principal hace que el cortafuegos activo-principal realice todo el procesamiento del tráfico. Podría configurar esto por uno de los siguientes motivos:

- *Está solucionando problemas y capturando logs y capturas de paquetes, por lo que el paquete que se está procesando no se divide entre los cortafuegos.*
- *Desea forzar el par HA activo/activo para que funcione como un par HA activo/pasivo. Consulte* Caso de uso: Configuración HA activa/activa con dirección IP flotante enlazada a cortafuegos activo-principal*.*

Configuración de sesión

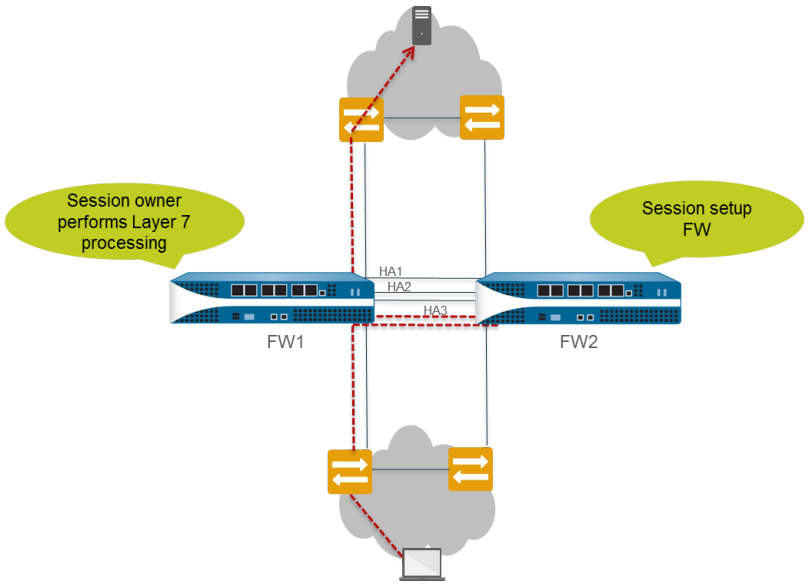
El cortafuegos de configuración de sesión realiza el procesamiento de capa 2 a capa 4 necesario para configurar una nueva sesión. El cortafuegos de configuración de sesión también realiza NAT usando el grupo NAT del propietario de sesión. Usted determina el cortafuegos de configuración de sesión en una configuración activa/activa al seleccionar una de las siguientes opciones de distribución de carga de configuración de sesión.

© 2020 Palo Alto Networks, Inc.

Opción de configuración de sesión	Description (Descripción)
IP Modulo	El cortafuegos distribuye la carga de configuración de sesión sobre la base de la paridad de la dirección IP de origen. Este es un método determinista para compartir la configuración de la sesión.
IP Hash (Hash de IP)	El cortafuegos utiliza un hash de las direcciones IP de origen y destino para distribuir las responsabilidades de configuración de la sesión.
Primary Device (Dispositivo principal)	El cortafuegos activo-principal siempre configura la sesión; solo el cortafuegos lleva a cabo todas las responsabilidades de configuración de la sesión.
First Packet (Primer paquete)	El cortafuegos que recibe el primer paquete de una sesión realiza la configuración de la sesión.

- *Si desea compartir la carga de las responsabilidades de propietario de la sesión y configuración de la sesión, configure el propietario de la sesión en First Packet y la configuración de la sesión en IP modulo. Estos son los ajustes recomendados.*
- *Si desea solucionar problemas o capturar logs o capturas de paquetes, o si desea que un par HA activo/activo funcione como un par HA activo/pasivo, configure el propietario de la sesión y la configuración de la sesión en el dispositivo principal, para que el dispositivo activo-principal realice todo el procesamiento del tráfico. Consulte* Caso de uso: configuración HA activa/activa con dirección IP flotante enlazada a cortafuegos activo-principal.

El cortafuegos utiliza el enlace HA3 para enviar paquetes a su peer para la configuración de la sesión si fuera necesario. La siguiente figura y texto describen la ruta de un paquete que el cortafuegos FW1 recibe para una nueva sesión. Las líneas de puntos rojos indican que el cortafuegos FW1 reenvía el paquete al FW2 y el FW2 devuelve el paquete al FW1 por el enlace HA3.



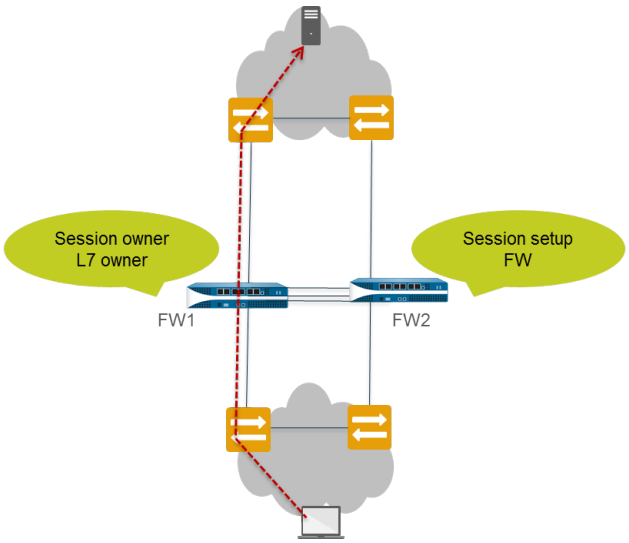
- El host de destino envía un paquete a FW1.
- El FW1 examina el contenido del paquete para determinar si coincide con una sesión existente. Si no hay coincidencia con ninguna sesión, el FW1 determina que ha recibido el primer paquete para una

© 2020 Palo Alto Networks, Inc.

nueva sesión y, por lo tanto, se convierte en el propietario de la sesión (suponiendo que **Session Owner Selection** está configurado en **First Packet**).

- FW1 utiliza la opción de distribución de carga de configuración de la sesión para identificar el cortafuegos de configuración de la sesión. En este ejemplo, FW2 está configurado para realizar la configuración de la sesión.
- FW1 utiliza el enlace HA3 para enviar el primer paquete a FW2.
- FW2 configura la sesión y devuelve el paquete a FW1 para el procesamiento de capa 7, si hubiera.
- FW1 luego reenvía el paquete por la interfaz de salida hacia el destino.

La siguiente figura y texto describen la ruta de un paquete que coincide con una sesión existente:



- El host de destino envía un paquete a FW1.
- El FW1 examina el contenido del paquete para determinar si coincide con una sesión existente. Si la sesión coincide con una sesión existente, FW1 procesa el paquete y lo envía por la interfaz de salida hacia el destino.

NAT en modo HA activa/activa

En una configuración HA activa/activa:

- Debe vincular cada regla NAT de IP dinámica (Dynamic IP, DIP) y regla NAT de IP dinámica y puerto (Dynamic IP and Port, DIPP) con el ID de dispositivo 0 o ID de dispositivo 1.
- Debe vincular cada regla NAT estática al ID de dispositivo 0, ID de dispositivo 1, ambos ID de dispositivo, o el cortafuegos en estado activo-principal.

Por lo tanto, cuando uno de los cortafuegos crea una nueva sesión, la vinculación del ID de dispositivo **0** o **1** determina qué reglas NAT coinciden con el cortafuegos. La vinculación del dispositivo debe incluir al cortafuegos propietario de la sesión para que la regla coincida.

El cortafuegos de configuración de la sesión realiza la búsqueda de coincidencia de la política NAT, pero las reglas NAT se evalúan en función del propietario de la sesión. La sesión se traduce de acuerdo con las reglas de NAT que están vinculadas con el dispositivo propietario de sesión. Al realizar la búsqueda de coincidencias con la política NAT, un cortafuegos omite todas las reglas de NAT que no están vinculadas con el cortafuegos propietario de sesión.

Por ejemplo, supongamos que el cortafuegos con ID de dispositivo 1 es el propietario de la sesión y el cortafuegos de configuración de sesión. Cuando el cortafuegos con ID de dispositivo 1 intenta que la sesión coincida con una regla de NAT, ignora todas las reglas vinculadas al ID de dispositivo 0. El cortafuegos

© 2020 Palo Alto Networks, Inc.

realiza la traducción NAT únicamente si el propietario de sesión y el ID de dispositivo en la regla NAT coinciden.

En una situación típica, usted crea reglas NAT específicas del dispositivo cuando los cortafuegos peer utilizan diferentes direcciones IP para la traducción.

Si uno de los cortafuegos peer falla, el cortafuegos activo continúa procesando el tráfico para las sesiones sincronizadas del cortafuegos fallido, incluido el tráfico NAT. En una configuración NAT de origen, cuando un cortafuegos falla:

- La dirección IP flotante que se utiliza como la dirección IP traducida de la regla NAT se transfiere al cortafuegos operativo. Por lo tanto, las sesiones existentes que conmutan por error continúan utilizando esta dirección IP.
- Todas las nuevas sesiones usarán las reglas NAT específicas del dispositivo que pertenecen originalmente al cortafuegos operativo. Es decir, el cortafuegos operativo traduce las nuevas sesiones usando solo las reglas NAT que coinciden con su ID de dispositivo e ignora las reglas NAT vinculadas con el ID del dispositivo fallido.

Para obtener ejemplos de HA activo/activo con NAT, consulte:

- Caso de uso: Configuración de HA activa/activa con NAT DIPP de origen usando direcciones IP flotantes
- Caso de uso: Configuración de grupos de direcciones IP NAT de origen separadas para cortafuegos HA activo/activo.
- Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino
- Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino en capa 3

ECMP en modo HA activa/activa

Cuando un peer HA activo/activo falla, sus sesiones se transfieren al nuevo cortafuegos activo-principal, que intenta usar la misma interfaz de salida que estaba usando el cortafuegos que falló. Si el cortafuegos detecta que la interfaz está entre las rutas ECMP, las sesiones transferidas tomarán la misma ruta e interfaz de salida. Este comportamiento se produce independientemente del algoritmo de ECMP en uso; se recomienda utilizar la misma interfaz.

Solo en el caso de que ninguna ruta de ECMP coincida con la interfaz de salida original, el cortafuegos activo-principal seleccionará una nueva ruta ECMP.

Si no configuró las mismas interfaces en los peers activo/activo, cuando se produzca una conmutación por error, el cortafuegos activo-principal seleccionará la mejor ruta desde la tabla FIB. En consecuencia, las sesiones existentes pueden no distribuirse de acuerdo con el algoritmo de ECMP.

© 2020 Palo Alto Networks, Inc.

Configuración de la HA activo/pasivo

- Requisitos para la HA activa/pasiva
- Directrices de configuración para la HA activo/pasivo
- Configuración de la HA activa/pasiva
- Definición de las condiciones de conmutación por error de HA
- Verificación de conmutación por error

Requisitos para la HA activa/pasiva

Para configurar la alta disponibilidad en sus cortafuegos de Palo Alto Networks, necesitará un par de cortafuegos que reúnan los siguientes requisitos:

- **El mismo modelo**: Ambos cortafuegos del par deben tener el mismo modelo de hardware o de máquina virtual.
- **La misma versión de PAN-OS**: Ambos cortafuegos deben ejecutar la misma versión de PAN-OS y estar actualizados en las bases de datos de la aplicación, URL y amenazas.
- La misma capacidad de múltiples sistemas virtuales: ambos cortafuegos deben tener la función **Multi Virtual System Capability** habilitada o no habilitada. Cuando está habilitada, cada cortafuegos requiere sus propias licencias de sistemas virtuales múltiples.
- **El mismo tipo de interfaces**: enlaces de HA específicos o una combinación del puerto de gestión y los puertos internos que se establecen para la HA de *tipo de interfaz*.
  - Determine la dirección IP de la conexión de HA1 (control) entre peers de HA. La dirección IP de HA1 de ambos peers debe estar en la misma subred si están conectados directamente o si están conectados al mismo conmutador.

    En el caso de cortafuegos sin puertos de HA específicos, puede utilizar el puerto de gestión para la conexión de control. Al utilizar el puerto de gestión obtiene un enlace de comunicación directa entre los planos de gestión de ambos cortafuegos. Sin embargo, dado que los puertos de gestión no tienen cables directos entre los peers, asegúrese de que tiene una ruta que conecte estas dos interfaces a través de su red.
  - Si utiliza la capa 3 como método de transporte para la conexión de HA2 (datos), determine la dirección IP para el enlace de HA2. Utilice la capa 3 únicamente si la conexión de HA2 debe comunicarse a través de una red enrutada. La subred IP de los enlaces de HA2 no debe solaparse con la de los enlaces de HA1 ni con ninguna otra subred asignada a los puertos de datos del cortafuegos.
- **El mismo conjunto de licencias**: Las licencias son exclusivas para cada cortafuegos y no se pueden compartir entre los cortafuegos. Por lo tanto, debe obtener licencias idénticas para ambos cortafuegos. Si los dos cortafuegos no tienen un conjunto idéntico de licencias, no podrán sincronizar información de configuración ni mantener la paridad para una conmutación por error sin problemas.



Si ya cuenta con un cortafuegos y desea añadir uno nuevo para HA, pero este ya está configurado, se recomienda el Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica *del nuevo cortafuegos. Esto garantizará que el nuevo cortafuegos tenga una configuración limpia. Después de configurar la HA, deberá sincronizar la configuración del cortafuegos principal con el cortafuegos recién introducido con la configuración limpia.*

Directrices de configuración para la HA activo/pasivo

Para establecer un par activo (PeerA) pasivo (PeerB) en HA, debe configurar algunas opciones de manera idéntica en ambos cortafuegos y algunas de manera independiente (no coincidentes) en cada cortafuegos.

© 2020 Palo Alto Networks, Inc.

Estos ajustes de HA no se sincronizan entre los cortafuegos. Si desea información detallada sobre qué se sincroniza y qué no, consulte Referencia: Sincronización HA.

La siguiente lista de verificación enumera los ajustes que debe configurar de manera idéntica en ambos cortafuegos:

- Usted debe habilitar HA en ambos cortafuegos.
- Debe configurar el mismo valor de ID de grupo en ambos cortafuegos. El cortafuegos utiliza el valor de ID de grupo para crear una dirección MAC virtual para todas las interfaces configuradas. Consulte la dirección IP flotante y la dirección MAC virtual para obtener información sobre las direcciones MAC virtuales. Cuando un nuevo cortafuegos activo toma el control, se envían mensajes ARP gratuitos desde cada una de las interfaces conectadas para informar a los conmutadores de capa 2 la nueva ubicación de la dirección MAC.
- Si está utilizando puertos internos como enlaces HA, debe configurar las interfaces para los enlaces HA1 y HA2 en el tipo HA.
- Establezca el modo HA como Activo Pasivo en ambos cortafuegos.
- Si se le solicita, habilite la preferencia en ambos cortafuegos. Sin embargo, el valor de prioridad de dispositivo no debe ser idéntico.
- Si fuera necesario, configure el cifrado del enlace HA1 (para la comunicación entre los peers de HA) en ambos cortafuegos.
- Basándose en la combinación de puertos de HA1 y backup de HA1 que está utilizando, utilice las siguientes recomendaciones para decidir si debería habilitar el backup de heartbeat:

  La funcionalidad HA (copia de seguridad de HA1 y HA1) no es compatible en la interfaz de gestión si está configurada para el direccionamiento DHCP (el tipo de IP está configurado como cliente DHCP). Las excepciones son AWS y Azure, donde la interfaz de gestión está configurada como cliente DHCP y admite enlaces de copia de seguridad HA1 y HA1.

  - HA1: Puerto de HA1 específico

    Backup de HA1: Puerto de HA1 específico

    Recomendación: Habilitar backup de heartbeat
  - HA1: Puerto de HA1 específico

    Backup de HA1: Puerto interno

    Recomendación: Habilitar backup de heartbeat
  - HA1: Puerto de HA1 específico

    Backup de HA1: puerto de gestión

    Recomendación: No habilitar backup de heartbeat
  - HA1: Puerto interno

    Backup de HA1: Puerto interno

    Recomendación: Habilitar backup de heartbeat
  - HA1: puerto de gestión

    Backup de HA1: Puerto interno

    Recomendación: No habilitar backup de heartbeat

La siguiente tabla enumera los ajustes de HA que debe configurar de manera independiente en ambos cortafuegos. Consulte Referencia: Sincronización HA para obtener más información sobre otros ajustes de configuración que no se sincronizan automáticamente entre peers.

© 2020 Palo Alto Networks, Inc.

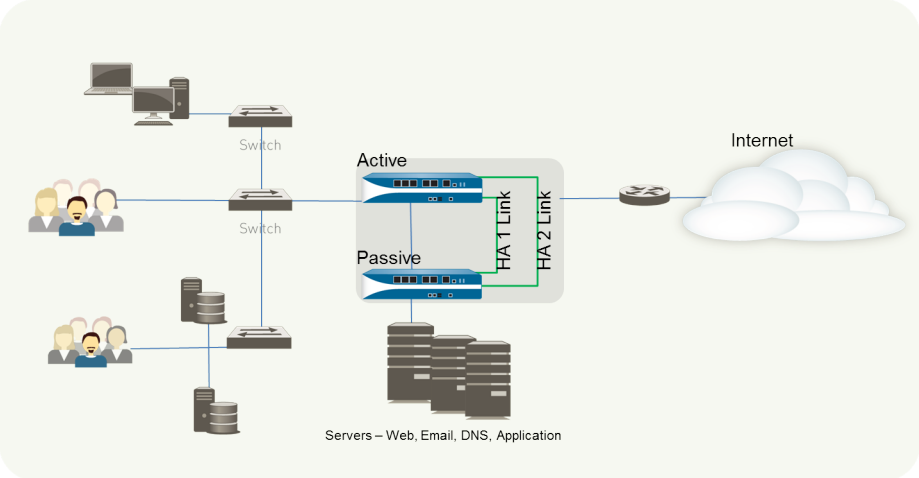
Ajustes de configuración independientes	PeerA	PeerB
Enlace de control	Dirección IP del enlace de HA1 configurado en este cortafuegos (PeerA).	Dirección IP del enlace de HA1 configurado en este cortafuegos (PeerB).
	En el caso de cortafuegos sin puertos de HA específicos, utilice la dirección IP del puerto de gestión para el enlace de control.	
Enlace de datos La información de enlace de datos se sincroniza entre los cortafuegos después de habilitar la HA y establecer el enlace de control entre los cortafuegos.	De manera predeterminada, el enlace de HA2 utiliza Ethernet/capa 2. Si utiliza una conexión de capa 3, configure la dirección IP para el enlace de datos de este cortafuegos (PeerA).	De manera predeterminada, el enlace de HA2 utiliza Ethernet/capa 2. Si utiliza una conexión de capa 3, configure la dirección IP para el enlace de datos de este cortafuegos (PeerB).
Prioridad de dispositivo (obligatorio si se habilita la preemption)	El cortafuegos que tiene la intención de activar debe tener un valor numérico más bajo que su peer. Por lo tanto, si PeerA va a funcionar como el cortafuegos activo, mantenga el valor predeterminado de 100 y aumente el valor de PeerB. Si los cortafuegos tienen el mismo valor de prioridad de dispositivo, usan la misma dirección MAC de su HA1 como separador.	Si PeerB es pasivo, establezca el valor de prioridad de dispositivo con un número mayor que el de PeerA. Por ejemplo, establezca el valor como 110.
Supervisión de enlaces: Supervise una o más interfaces físicas que gestionen el tráfico vital de este cortafuegos y defina la condición de fallo.	Seleccione las interfaces físicas del cortafuegos que desea supervisar y defina la condición de fallo (todas o alguna) que activará una conmutación por error.	Seleccione un conjunto similar de interfaces físicas que desearía supervisar y defina la condición de fallo (todas o alguna) que activará una conmutación por error.
Supervisión de rutas: Supervise una o más direcciones IP de destino en las que el cortafuegos pueda utilizar pings ICMP para verificar la capacidad de respuesta.	Defina la condición de fallo (todas o alguna), el intervalo de ping y el recuento de pings. Esto es de especial utilidad para supervisar la disponibilidad de otros dispositivos de red interconectados. Por ejemplo, supervise la disponibilidad de un enrutador que se conecte a un servidor, la conectividad del propio servidor o cualquier otro dispositivo vital que se encuentre en el flujo del tráfico.	Seleccione un conjunto similar de dispositivos o direcciones IP de destino que se puedan supervisar para determinar la activación de una conmutación por error para PeerB. Defina la condición de fallo (todas o alguna), el intervalo de ping y el recuento de pings.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración independientes	PeerA	PeerB
	Asegúrese de que no sea probable que el nodo/dispositivo que está supervisando no responda, especialmente bajo carga, ya que esto podría provocar un fallo de supervisión de rutas y activar una conmutación por error.	

Configuración de la HA activa/pasiva

El siguiente procedimiento muestra cómo configurar un par de cortafuegos en una implementación activa/pasiva como se muestra en la topología del ejemplo siguiente.



Para configurar un par HA activo/pasivo, primero complete el siguiente flujo de trabajo en el primer cortafuegos y luego repita los pasos en el segundo cortafuegos.

STEP 1 | Conecte los puertos de HA para establecer una conexión física entre los cortafuegos.

- En el caso de cortafuegos con puertos de HA específicos, utilice un cable Ethernet para conectar los puertos de HA1 y HA2 específicos de los peers. Utilice un cable cruzado si los cortafuegos están conectados directamente entre sí.
- En el caso de cortafuegos sin puertos de HA específicos, seleccione dos interfaces de datos para el enlace de HA2 y el enlace de HA1 de backup. A continuación, utilice un cable Ethernet para conectar estas interfaces de HA internas entre ambos cortafuegos.

Utilice el puerto de gestión para el enlace de HA1 y asegúrese de que los puertos de gestión pueden conectarse entre sí a través de su red.

STEP 2 | Habilite los pings en el puerto de gestión.

La habilitación de los pings permite que el puerto de gestión intercambie información de backup de heartbeat.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de interfaz de gestión.
2. Seleccione **Ping** como servicio permitido en la interfaz.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Si el cortafuegos no tiene puertos de HA específicos, configure los puertos de datos para que funcionen como puertos de HA.

En el caso de cortafuegos con puertos de HA específicos, vaya al siguiente paso.

1. Seleccone **Network (Red)** > **Interfaces**.
2. Confirme que el enlace está activado en los puertos que desee utilizar.
3. Seleccione la interfaz y establezca el **Interface Type (Tipo de interfaz)** como **HA**.
4. Establezca los ajustes **Link Speed (Velocidad de enlace)** y **Link Duplex (Dúplex de enlace)** según corresponda.

STEP 4 | Establezca el modo HA y el ID de grupo.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Establezca un **ID de grupo** y, de manera opcional, una **descripción** para el par. El ID de grupo exclusivamente cada clúster en HA en su red. Si tiene varios pares HA que comparten el mismo dominio de difusión, debe establecer un ID de grupo exclusivo para cada par.
3. Establezca el modo como **Active Passive (Activo Pasivo)**.

STEP 5 | Configure la conexión del enlace de control.

Este ejemplo muestra un puerto interno configurado con el tipo de interfaz HA.

En el caso de cortafuegos que utilicen el puerto de gestión como el enlace de control, la información de dirección IP se cumplimenta previamente de manera automática.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la sección Control Link (HA1) (Enlace de control [HA1]).
2. Seleccione el **Port** al que ha conectado el cable para utilizarlo como el enlace HA1.
3. Establezca la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.

   Si las interfaces HA1 están en subredes separadas, introduzca la dirección IP de la **Gateway (Puerta de enlace)**. No añada una dirección de puerta de enlace si los cortafuegos están conectados directamente o están en la misma VLAN.

STEP 6 | (Opcional) Habilite el cifrado para la conexión del enlace de control.

Esto suele utilizarse para proteger el enlace si los dos cortafuegos no están conectados directamente, es decir, si los puertos están conectados a un conmutador o un enrutador.

1. Exporte la clave de HA desde un cortafuegos e impórtela al cortafuegos peer.
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
   2. Seleccione **Export HA key (Exportar clave de HA)**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el peer.
   3. En el cortafuegos del peer, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)** y seleccione **Import HA key (Importar clave HA)** para desplazarse hasta la ubicación donde guardó la clave e importarla en el peer.
   4. Repita este procedimiento en el segundo cortafuegos para intercambiar las claves de HA en ambos dispositivos.
2. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Control Link (HA1) (Enlace de control [HA1]).
3. Seleccione **Encryption Enabled**.

© 2020 Palo Alto Networks, Inc.

Si habilita el cifrado, cuando termine de configurar los cortafuegos de HA, puede seguir el procedimiento Actualización de las claves de SSH de HA1 y configuración de sus opciones.

STEP 7 | Configure la conexión del enlace de control de backup.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la sección Control Link (HA1 Backup) (Enlace de control [copia de seguridad de HA1]).
2. Seleccione la interfaz de copia de seguridad de HA1 y configure la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.

Los cortafuegos PA-3200 Series no admiten direcciones IPv6 para el enlace de control de copia de seguridad de HA1. Utilice direcciones IPv4.

STEP 8 | Configure la conexión del enlace de datos (HA2) y la conexión de HA2 de backup entre los cortafuegos.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la sección Data Link (HA2) (Enlace de datos [HA2]).
2. Seleccione el **Port** para la conexión del enlace de datos.
3. Seleccione el método **Transport (Transporte)**. El valor predeterminado es **Ethernet** y funcionará cuando el par de HA se conecte directamente o a través de un conmutador. Si necesita enrutar el tráfico del enlace de datos a través de la red, seleccione IP o UDP como modo de transporte.
4. Si utiliza IP o UDP como método de transporte, introduzca la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.
5. Verifique que se ha seleccionado **Habilitar sincronización de sesión**.
6. Seleccione **HA2 Keep-alive (Conexión persistente de HA2)** para habilitar la supervisión del enlace de datos de HA2 entre los peers de HA. Si se produce un fallo basado en el umbral establecido (el valor predeterminado son 10.000 ms), se producirá la acción definida. En el caso de una configuración activo/pasivo, se generará un mensaje de log de sistema crítico cuando se produzca un fallo de conexión persistente de HA2.

   Puede configurar la opción Conexión persistente de HA2 en ambos cortafuegos o solamente un cortafuegos del clúster en HA. Si la opción se habilita únicamente en un cortafuegos, solamente ese cortafuegos enviará los mensajes de conexión persistente. Si se produce un fallo, se notificará al otro cortafuegos.
7. Edite la sección **Data Link (HA2 Backup) (Enlace de datos [copia de seguridad de HA2])**, seleccione la interfaz y añada la **IPv4/IPv6 Address (Dirección IPv4/Ipv6)** y la **Netmask (Máscara de red)**.

STEP 9 | Habilite el backup del heartbeat si su enlace de control utiliza un puerto de HA específico o un puerto interno.

No necesita habilitar el backup del heartbeat si está utilizando el puerto de gestión para el enlace de control.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Seleccione **Heartbeat Backup (Copia de seguridad de heartbeat)**.

   Para permitir la transmisión de heartbeats entre los cortafuegos, deberá verificar que el puerto de gestión entre ambos peers puede enrutarse del uno al otro.

Habilitar el backup de heartbeat también le permite evitar una situación de síndrome de cerebro dividido. El síndrome de cerebro dividido se produce cuando el enlace HA1 deja de funcionar y provoca que el cortafuegos se omita, pese a que el

© 2020 Palo Alto Networks, Inc.

cortafuegos sigue funcionando. En tales situaciones, cada peer cree que el otro ha dejado de funcionar e intenta iniciar los servicios que están en funcionamiento, causando un síndrome de cerebro dividido. Si el enlace de backup de heartbeat está habilitado, se evita el síndrome de cerebro dividido, ya que los heartbeats redundantes y los mensajes de saludo se transmiten a través del puerto de gestión.

STEP 10 | Establezca la prioridad de dispositivo y habilite la preemption.

Este ajuste únicamente es necesario si desea asegurarse de que un cortafuegos específico es el dispositivo activo preferido. Para obtener más información, consulte Prioridad de dispositivo y preferencia.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Establezca el valor numérico de **Device Priority (Prioridad de dispositivo)**. Asegúrese de establecer un valor numérico más bajo en el cortafuegos al que desee asignar una mayor prioridad.

   Si ambos cortafuegos tienen el mismo valor de prioridad de dispositivo, el cortafuegos con la dirección MAC más baja en el enlace de control de HA1 será el cortafuegos activo.
3. Seleccione **Preemptive (Preferente)**.

   Debe habilitar la preemption tanto en el cortafuegos activo como en el pasivo.

STEP 11 | (Opcional) Modifique los HA Timers (Temporizadores HA).

De manera predeterminada, el perfil del temporizador de HA se establece como el perfil **Recommended (Recomendado)** y es adecuado para la mayoría de implementaciones de HA.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Seleccione el perfil **Agresivo** para activar la conmutación por error más rápido; seleccione **Avanzado** para definir valores personalizados para activar la conmutación por error en su configuración.

   Para ver el valor preestablecido para un temporizador concreto incluido en un perfil, seleccione Advanced (Avanzado) y haga clic en Load Recommended (Carga recomendada) o Load Aggressive (Carga intensiva). Los valores preestablecidos para su modelo de hardware aparecerán en la pantalla.

STEP 12 | (Opcional) Modifique el estado del enlace de los puertos de HA del cortafuegos pasivo.

El estado de enlace pasivo es shutdown (apagar) de manera predeterminada. Cuando habilite HA, el estado de enlace de los puertos de HA del cortafuegos activo será de color verde; los del cortafuegos pasivo estarán desactivados y se mostrarán de color rojo.

La configuración del estado de enlace como **Auto** permite reducir la cantidad de tiempo que tarda el cortafuegos pasivo en tomar el control cuando se produce una conmutación por error y le permite supervisar el estado del enlace.

Para habilitar el estado de enlace del cortafuegos pasivo para que permanezca activado y refleje el estado de cableado de la interfaz física:

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite la configuración activa pasiva.
2. Establezca **Estado de los enlaces en el pasivo (Passive Link State)** como **Auto (Automático)**.

   La opción automática reduce la cantidad de tiempo que tarda el cortafuegos pasivo en tomar el control cuando se produce una conmutación por error.

© 2020 Palo Alto Networks, Inc.

Aunque la interfaz se muestre de color verde (cableada y activada), seguirá descartando todo el tráfico hasta que se active una conmutación por error.

Cuando modifique el estado de enlace pasivo, asegúrese de que los dispositivos adyacentes no reenvían el tráfico al cortafuegos pasivo basándose únicamente en el estado de enlace del cortafuegos.

STEP 13 | Habilite la HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.
3. Seleccione **Enable Config Sync**. Este ajuste habilita la sincronización de los ajustes de configuración entre los cortafuegos activo y pasivo.
4. Introduzca la dirección IP asignada al enlace de control del peer en **Peer HA1 IP Address**.

   En el caso de cortafuegos sin puertos de HA específicos, si el peer utiliza el puerto de gestión para el enlace de HA1, introduzca la dirección IP del puerto de gestión del peer.
5. Introduzca **Dirección IP de HA1 de copia de seguridad**.

STEP 14 | (Opcional) Habilite LACP and LLDP Pre-Negotiation for Active/Passive HA (Negociación previa de LACP y LLDP para la HA activa/pasiva) para una conmutación por error más rápida si su red utiliza LACP o LLDP.

Habilite LACP y LLDP antes de configurar la negociación previa de HA para el protocolo si desea que la negociación previa funcione en modo activo.

1. Asegúrese de configurar el estado del enlace como **Auto (Automático)** en el paso 12.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Para habilitar la negociación previa activa de LACP:
   1. Seleccione una interfaz AE en una implementación de capa 2 o capa 3.
   2. Seleccione la pestaña **LACP**.
   3. Seleccione **Enable in HA Passive State (Habilitar en estado pasivo HA)**.
   4. Haga clic en **OK (Aceptar)**.

      No puede seleccionar también Same System MAC Address for Active-Passive HA debido a que la negociación previa requiere direcciones MAC de interfaz únicas en los cortafuegos activo y pasivo.
4. Para habilitar la negociación previa pasiva de LACP:
   1. Seleccione una interfaz Ethernet en una implementación de Virtual Wire.
   2. Seleccione la pestaña **Advanced (Avanzado)**.
   3. Seleccione la pestaña **LACP**.
   4. Seleccione **Enable in HA Passive State (Habilitar en estado pasivo HA)**.
   5. Haga clic en **OK (Aceptar)**.
5. Para habilitar la negociación previa activa de LLDP:
   1. Seleccione una interfaz Ethernet en una implementación de capa 2, capa 3 o Virtual Wire.
   2. Seleccione la pestaña **Advanced (Avanzado)**.
   3. Seleccione la pestaña **LLDP**.
   4. Seleccione **Enable in HA Passive State (Habilitar en estado pasivo HA)**.
   5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

Si desea permitir la negociación previa pasiva de LLDP para una implementación de cable virtual, realice el paso 14.e pero no habilite LLDP.

STEP 15 | Guarde los cambios de configuración.

Haga clic en **Commit (Confirmar)**.

STEP 16 | Cuando termine de configurar ambos cortafuegos, verifique que los dispositivos están emparejados en la HA activo/pasivo.

1. Acceda al **Dashboard** de ambos dispositivos y visualice el widget High Availability.
2. En el cortafuegos activo, haga clic en el enlace **Sync to peer**.
3. Confirme que los cortafuegos están emparejados y sincronizados, como se muestra a continuación:
   - En el cortafuegos pasivo: el estado del cortafuegos local debería mostrar **passive (pasivo)** y Running Config (Config. en ejecución) debería mostrar **synchronized (sincronizada)**.
   - En el cortafuegos activo: El estado del cortafuegos local debería mostrar **active (activo)** y Running Config (Config. en ejecución) debería mostrar **synchronized (sincronizada)**.

Definición de las condiciones de conmutación por error de HA

Realice la siguiente tarea para usar la supervisión de enlaces o supervisión de rutas para definir condiciones de Conmutación por error y establecer qué causará un error en un cortafuegos en un par de cortafuegos de HA, un evento en el que la tarea de protección de tráfico pasa del cortafuegos previamente activo a su par de HA. La Descripción general de la alta disponibilidad describe las condiciones que causan un error.

Puede supervisar varios grupos de rutas de IP por enrutador virtual, VLAN o cable virtual. Puede habilitar cada grupo de ruta con una o más direcciones IP y dar a cada uno sus propias condiciones de fallo de peer. Además, puede establecer estas condiciones de fallo tanto en el nivel de grupo de ruta como en el nivel de enrutador virtual o VLAN o grupo de cable virtual más amplio mediante las verificaciones de fallos "cualquiera" o "todas" para determinar el estado del cortafuegos activo.

Cuando actualice a PAN-OS 10.0, el cortafuegos transferirá automáticamente sus direcciones IP de destino supervisadas actualmente a un grupo de destino recién creado y le dará a ese grupo un nombre de supervisión de ruta predeterminado. El nuevo grupo de destino conservará su condición de conmutación por error anterior en el nivel del grupo de ruta.

Asegúrese de eliminar todas las configuraciones de supervisión de ruta de VLAN en HA activo/activo antes de actualizar a PAN-OS 10.0, ya que la supervisión de ruta de VLAN no es compatible con el emparejamiento de HA activo/activo en PAN-OS 10.0; retener una configuración de HA activa/activa anterior da como resultado un fallo de confirmación automática.

Antes de habilitar la supervisión de rutas, debe configurar sus enrutadores virtuales, VLAN o cables virtuales o una combinación de estos componentes de red lógicos. La supervisión de rutas en enrutadores virtuales y cables virtuales es compatible con implementaciones de HA activas/activas y activas/pasivas; sin embargo, la supervisión de rutas en las VLAN solo se admite en pares activos/pasivos.

Antes de habilitar la supervisión de rutas, también debe realizar las siguientes acciones:

- Comprobar la accesibilidad de los grupos de IP de destino en sus enrutadores virtuales.
- Asegurarse de que las VLAN (para las que desea habilitar la supervisión de rutas) incluyan interfaces configuradas.
- Obtener la dirección IP de origen que utilizará para recibir pings de la dirección IP de destino adecuada.

© 2020 Palo Alto Networks, Inc.

Si está utilizando SNMPv3 para supervisar los cortafuegos, tenga en cuenta que el ID de motor de SNMPv3 es exclusivo para cada cortafuegos; EngineID no se sincroniza entre el clúster en HA y, por lo tanto, le permite supervisar independientemente cada cortafuegos del clúster en HA. Para obtener información sobre la configuración de SNMP, consulte Reenvío de capturas a un administrador SNMP*. Como EngineID se genera utilizando el número de serie del cortafuegos, en el cortafuegos VM-Series deberá aplicar una licencia válida para obtener un EngineID exclusivo para cada cortafuegos.*

STEP 1 | Para configurar la supervisión de enlaces de HA, especifique un grupo de interfaces físicas para que el cortafuegos lo supervise (enlace hacia arriba o hacia abajo).

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Link and Path Monitoring (Supervisión de enlaces y rutas)**.
2. En la sección Link Monitoring (Supervisión de enlaces), **añada** un grupo de enlaces por **nombre**.
3. Seleccione **Enabled (Habilitado)** para habilitar el grupo de enlaces.
4. Seleccione la **condición de fallo** para las interfaces en el grupo de enlaces: **Any (Cualquiera)** (valor predeterminado) o **All (Todos)**.
5. **Añada** la **interfaces** que supervisar.
6. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Modifique la condición de fallo para el conjunto de grupos de enlaces configurados en el cortafuegos.

De manera predeterminada, el cortafuegos activará una conmutación por error cuando falle el grupo de enlaces supervisado.

1. Edite la sección **Link Monitoring (Supervisión de enlaces)**.
2. Establezca la **condición de fallo** en **Any (Cualquiera)** (valor predeterminado) o **All (Todos)**.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Para configurar la supervisión de la ruta de HA para un cable virtual, VLAN o enrutador virtual, especifique las direcciones IP de destino en las que el cortafuegos hará ping para verificar la conectividad de la red.

1. En la sección Path Monitoring (Supervisión de ruta), seleccione **Add Virtual Wire Path (Añadir ruta de cables virtual)**, **Add VLAN Path (Añadir ruta de WLAN)** o **Add Virtual Router Path (Añadir enrutador virtual)**.
2. Especifique un **nombre** para el grupo de rutas de enrutador virtual, VLAN o cable virtual.
3. (Solo en ruta de cable virtual o ruta de VLAN) Especifique la dirección **IP de origen** que se utilizará para hacer ping en la dirección IP de destino a través del cable virtual o VLAN.
4. Seleccione **Enabled (Habilitado)** para habilitar el grupo de rutas.
5. Seleccione la **condición de fallo** que genere una fallo para este grupo de rutas: **Any (Cualquiera)** (valor predeterminado) para emitir un fallo cuando uno o más grupos de IP de destino en este grupo de ruta fallen o **All (Todos)** para emitir un fallo cuando fallen todos los grupos de IP de destino en este grupo de rutas.
6. Especifique el **intervalo de ping** en milisegundos; el intervalo entre los mensajes ICMP enviados a la dirección IP de destino (el intervalo es de 200 a 60 000; el valor predeterminado es 200).
7. Especifique el **recuento de pings** de los pings que deben fallar antes de declarar una fallo (el intervalo es de 3 a 10; el valor predeterminado es 10).
8. **Añada** y especifique un nombre de **grupo IP de destino**.
9. **Añada** una o más direcciones **IP de destino** en las que hacer ping.
10. Seleccione **Enabled (Habilitado)** para habilitar la supervisión de la ruta para el grupo de IP de destino.
11. Seleccione la **condición de fallo** que genere una fallo para este grupo de IP de destino: **Any (Cualquiera)** (valor predeterminado) para emitir un error cuando una o más direcciones IP enumeradas

© 2020 Palo Alto Networks, Inc.

no están disponibles o **All (Todo)** para emitir un error cuando todas las direcciones IP enumeradas no están disponibles.

12. Haga clic en **OK (Aceptar)** dos veces.
13. (Solo en Panorama) Seleccione la plantilla de Panorama adecuada para enviar la configuración de supervisión de ruta a su dispositivo.

STEP 4 | (Opcional) Modifique la condición de fallo para el conjunto de grupos de rutas configurados en el cortafuegos.

De manera predeterminada, el cortafuegos activará una conmutación por error cuando falle el grupo de rutas supervisado.

1. Edite la sección **Path Monitoring (Supervisión de rutas)**.
2. Seleccione **Enabled (Habilitado)** para habilitar la supervisión de rutas en el dispositivo.
3. Establezca la **condición de fallo** en **Any (Cualquiera)** (valor predeterminado) para emitir un fallo para este cortafuegos cuando uno o más enrutadores virtuales, VLAN o cables virtuales supervisados estén inactivos. Seleccione **Todo** para emitir un fallo para este cortafuegos cuando todos los enrutadores virtuales supervisados, VLAN o cables virtuales estén inactivos.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Seleccione **Confirmar**.

Verificación de conmutación por error

Para comprobar que su configuración de HA funciona correctamente, active una conmutación por error manual y verifique que los cortafuegos cambian de estado correctamente.

STEP 1 | Suspenda el cortafuegos activo.

Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Operational Commands (Comandos operativos)** y haga clic en el enlace **Suspend local device (Suspender dispositivo local)**.

STEP 2 | Verifique que el cortafuegos pasivo ha tomado el control como activo.

En el **Dashboard (Panel)**, verifique que el estado del cortafuegos pasivo cambie a **active (activo)** en el widget High Availability.

STEP 3 | Restablezca el cortafuegos suspendido a un estado funcional. Espere un par de minutos y, a continuación, verifique que se ha producido un adelantamiento, si la opción **Preemptive (Preferente)** se ha habilitado.

1. En el cortafuegos que ha suspendido previamente, seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Operational Commands (Comandos operativos)** y haga clic en **Make local device functional (Hacer dispositivo local funcional)**.
2. En el widget High Availability (Alta disponibilidad) del **Dashboard (Panel)**, confirme que el cortafuegos ha tomado el control como cortafuegos activo y que el peer ahora está en un estado pasivo.

© 2020 Palo Alto Networks, Inc.

Configuración de HA activa/activa

- Requisitos previos para la HA activa/activa
- Configuración de la HA activa/activa
- Determinación del caso de uso activo/activo

Requisitos previos para la HA activa/activa

Para configurar la HA activa/activa en sus cortafuegos, necesitará un par de cortafuegos que reúnan los siguientes requisitos:

- **El mismo modelo**: ambos cortafuegos del par deben ser del mismo modelo de hardware.
- **La misma versión de PAN-OS**: ambos cortafuegos deben ejecutar la misma versión de PAN-OS y estar actualizados en las bases de datos de la aplicación, URL y amenazas.
- La misma capacidad de múltiples sistemas virtuales: ambos cortafuegos deben tener la función **Multi Virtual System Capability (Capacidad de sistema multivirtual)** habilitada o no habilitada. Cuando está habilitada, cada cortafuegos requiere sus propias licencias de sistemas virtuales múltiples.
- **El mismo tipo de interfaces**: enlaces de HA específicos o una combinación del puerto de gestión y los puertos internos que se establecen para la HA de *tipo de interfaz*.
  - Las interfaces HA deben estar configuradas con direcciones IP estáticas únicamente, no con direcciones IP obtenidas de DHCP (excepto AWS, que pueden usar direcciones DHCP). Determine la dirección IP de la conexión de HA1 (control) entre peers de HA. La dirección IP de HA1 de ambos peers debe estar en la misma subred si están conectados directamente o si están conectados al mismo conmutador.

    En el caso de cortafuegos sin puertos de HA específicos, puede utilizar el puerto de gestión para la conexión de control. Al utilizar el puerto de gestión obtiene un enlace de comunicación directa entre los planos de gestión de ambos cortafuegos. Sin embargo, dado que los puertos de gestión no tienen cables directos entre los peers, asegúrese de que tiene una ruta que conecte estas dos interfaces a través de su red.
  - Si utiliza la capa 3 como método de transporte para la conexión de HA2 (datos), determine la dirección IP para el enlace de HA2. Utilice la capa 3 únicamente si la conexión de HA2 debe comunicarse a través de una red enrutada. La subred IP de los enlaces de HA2 no debe solaparse con la de los enlaces de HA1 ni con ninguna otra subred asignada a los puertos de datos del cortafuegos.
  - Cada cortafuegos necesita una interfaz dedicada para el enlace HA3. Los cortafuegos serie PA-7000 utilizan el puerto HSCI para HA3. Los cortafuegos serie PA-5200 pueden utilizar el puerto HSCI para HA3 o puede configurar interfaces agregadas en los puertos del plano de datos para HA3 para redundancia. En las plataformas restantes, puede configurar interfaces agregadas en los puertos del plano de datos como el enlace HA3 para redundancia.
- **El mismo conjunto de licencias**: Las licencias son exclusivas para cada cortafuegos y no se pueden compartir entre los cortafuegos. Por lo tanto, debe obtener licencias idénticas para ambos cortafuegos. Si los dos cortafuegos no tienen un conjunto idéntico de licencias, no podrán sincronizar información de configuración ni mantener la paridad para una conmutación por error sin problemas.



Si ya tiene un cortafuegos y desea añadir uno nuevo para HA pero este ya está configurado, se recomienda que realice el Restablecimiento del cortafuegos a los ajustes predeterminados de fábrica *en el nuevo cortafuegos. Esto garantizará que el nuevo cortafuegos tenga una configuración limpia. Después de configurar la HA, deberá sincronizar la configuración del cortafuegos principal con el cortafuegos recién introducido con la configuración limpia. También deberá configurar las direcciones IP locales.*

© 2020 Palo Alto Networks, Inc.

Configuración de la HA activa/activa

El siguiente procedimiento describe el flujo de trabajo básico para configurar sus cortafuegos en una configuración activa/activa. Sin embargo, antes de comenzar, Determine su caso de uso activo/activo para los ejemplos de configuración que más se adecuen a su entorno de red específico.

Si hay un conmutador entre los cortafuegos de HA, los puertos de conmutación que conectan el enlace de HA3 deben admitir tramas gigantes para manejar la sobrecarga asociada a la encapsulación de MAC en MAC en dicho enlace.

Para configurar activo/activo, primero complete los siguientes pasos en un peer y luego complételos en el segundo peer, y asegúrese de que configure la ID de dispositivo en valores diferentes (0 o 1) en cada peer.

STEP 1 | Conecte los puertos de HA para establecer una conexión física entre los cortafuegos.

Para cada caso de uso, los cortafuegos podrían ser cualquier modelo de hardware; elija el paso HA3 que corresponda a su modelo.

- En el caso de cortafuegos con puertos de HA específicos, utilice un cable Ethernet para conectar los puertos de HA1 y HA2 específicos de los peers. Utilice un cable cruzado si los cortafuegos están conectados directamente entre sí.
- En el caso de cortafuegos sin puertos de HA específicos, seleccione dos interfaces de datos para el enlace de HA2 y el enlace de HA1 de backup. A continuación, utilice un cable Ethernet para conectar estas interfaces de HA internas entre ambos cortafuegos. Utilice el puerto de gestión para el enlace de HA1 y asegúrese de que los puertos de gestión pueden conectarse entre sí a través de su red.
- Para HA3:
  - En los cortafuegos de la serie PA-7000, conecte la interconexión de bastidor de alta velocidad (High Speed Chassis Interconnect, HSCI) en el primer bastidor con la HSCI-A en el segundo bastidor, y la HSCI-B en el primer bastidor con la HSCI-B en el segundo bastidor.
  - En los cortafuegos PA-5200 Series (que cuentan con un puerto HSCI), conéctese con el puerto HSCI del primer bastidor con el puerto HSCI en el segundo bastidor. También puede utilizar los puertos de datos para los cortafuegos HA3 en los cortafuegos de la serie PA-5200.
  - En los cortafuegos PA-3200 Series (que cuentan con un puerto HSCI), conéctese con el puerto HSCI del primer bastidor con el puerto HSCI en el segundo bastidor.
  - En cualquier otro modelo de hardware, use interfaces de plano de datos para HA3.

STEP 2 | Habilite los pings en el puerto de gestión.

La habilitación de los pings permite que el puerto de gestión intercambie información de backup de heartbeat.

1. En **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, edite los ajustes de la interfaz de gestión.
2. Seleccione **Ping** como servicio permitido en la interfaz.

STEP 3 | Si el cortafuegos no tiene puertos de HA específicos, configure los puertos de datos para que funcionen como puertos de HA.

En el caso de cortafuegos con puertos de HA específicos, vaya al siguiente paso.

1. Seleccone **Network (Red)** > **Interfaces**.
2. Confirme que el enlace está activado en los puertos que desee utilizar.
3. Seleccione la interfaz y establezca el **Interface Type (Tipo de interfaz)** como **HA**.

© 2020 Palo Alto Networks, Inc.

4. Establezca los ajustes **Link Speed (Velocidad de enlace)** y **Link Duplex (Dúplex de enlace)** según corresponda.

STEP 4 | Habilite la HA activa/activa y configure el ID de grupo.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.
3. Introduzca un **Group ID**, que debe ser el mismo para ambos cortafuegos. El cortafuegos utiliza el ID de grupo para calcular la dirección MAC virtual (el intervalo es 1-63).
4. (Opcional) Introduzca una **descripción**.
5. Para **Mode (Modo)**, seleccione **Active Active (Activo activo)**.

STEP 5 | Configure el ID del dispositivo, habilite la sincronización e identifique el enlace de control en el cortafuegos peer.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Setup (Configuración).
2. Seleccione **Device ID (ID de dispositivo)** de la siguiente manera:
   - Al configurar el primer peer, establezca la **Device ID (ID de dispositivo)** en **0**.
   - Al configurar el segundo peer, establezca la **Device ID (ID de dispositivo)** en **1**.
3. Seleccione **Enable Config Sync**. Este ajuste es obligatorio para sincronizar las dos configuraciones de cortafuegos (habilitado por defecto).
4. Introduzca la **Peer HA1 IP Address (Dirección IP de HA del peer)**, que es la dirección IP del enlace de control HA1 del cortafuegos del peer.
5. (Opcional) Introduzca una **Backup Peer HA1 IP Address (Dirección IP de HA1 de backup)**, que es la dirección IP del enlace de control de rcopia de seguridad del cortafuegos del peer.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | Determine si el cortafuegos con el ID de dispositivo más bajo reemplaza al cortafuegos activo-principal tras la recuperación después de un fallo.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Seleccione **Preemptive (Preferente)** para que el cortafuegos con el ID de dispositivo más bajo reanude automáticamente el funcionamiento activo-principal después de que cualquiera de los cortafuegos se recuperen de un fallo. Ambos cortafuegos deben tener la opción **Preemptive (Preferente)** seleccionada para que se produzca el reemplazo.

   Deje **Preemptive (Preferente)** sin seleccionar si desea que la función activa-principal continúe con el cortafuegos actual hasta que usted convierta manualmente el cortafuegos recuperado en el cortafuegos activo-principal.

STEP 7 | Habilite el backup del heartbeat si su enlace de control utiliza un puerto de HA específico o un puerto interno.

No necesita habilitar la copia de seguridad de heartbeat si está utilizando el puerto de gestión para el enlace de control.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Seleccione **Heartbeat Backup (Copia de seguridad de heartbeat)**.

   Para permitir la transmisión de heartbeats entre los cortafuegos, deberá verificar que el puerto de gestión entre ambos peers puede enrutarse del uno al otro.

© 2020 Palo Alto Networks, Inc.

Habilitar la copia de seguridad de heartbeat le permite evitar una situación de síndrome de cerebro dividido. El síndrome de cerebro dividido se produce cuando el enlace HA1 deja de funcionar y provoca que el cortafuegos omita heartbeats, pese a que el cortafuegos sigue funcionando. En tales situaciones, cada peer cree que el otro ha dejado de funcionar e intenta iniciar los servicios que están en funcionamiento, lo que produce un síndrome de cerebro dividido. Al habilitar la copia de seguridad de heartbeat se evita el síndrome de cerebro dividido, ya que los heartbeats redundantes y los mensajes de saludo se transmiten a través del puerto de gestión.

STEP 8 | (Opcional) Modifique los HA Timers (Temporizadores HA).

De manera predeterminada, el perfil del temporizador de HA se establece como el perfil **Recommended (Recomendado)** y es adecuado para la mayoría de implementaciones de HA.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Seleccione **Aggressive (Intensivo)** para activar la conmutación por error más rápido. Seleccione **Advanced** para definir los valores personalizados y así activar la conmutación por error en su configuración.

   Para ver el valor preestablecido para un temporizador concreto incluido en un perfil, seleccione Advanced (Avanzado) y haga clic en Load Recommended (Carga recomendada) o Load Aggressive (Carga intensiva). Los valores preestablecidos para su modelo de hardware aparecerán en la pantalla.

STEP 9 | Configure la conexión del enlace de control.

Este ejemplo muestra un puerto interno configurado con el tipo de interfaz HA.

En el caso de cortafuegos que utilicen el puerto de gestión como el enlace de control, la información de dirección IP se cumplimenta previamente de manera automática.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Control Link (HA1) (Enlace de control [HA1]).
2. Seleccione el **Port** al que ha conectado el cable para utilizarlo como el enlace HA1.
3. Establezca la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.

   Si las interfaces HA1 están en subredes separadas, introduzca la dirección IP de la **Gateway (Puerta de enlace)**. No añada una dirección de puerta de enlace si los cortafuegos están conectados directamente.

STEP 10 | (Opcional) Habilite el cifrado para la conexión del enlace de control.

Esto suele utilizarse para proteger el enlace si los dos cortafuegos no están conectados directamente, es decir, si los puertos están conectados a un conmutador o un enrutador.

1. Exporte la clave de HA desde un cortafuegos e impórtela al cortafuegos peer.
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
   2. Seleccione **Export HA key (Exportar clave de HA)**. Guarde la clave de HA en una ubicación de red a la que pueda acceder el peer.
   3. En el cortafuegos del peer, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)** y seleccione **Import HA key (Importar clave HA)** para desplazarse hasta la ubicación donde guardó la clave e importarla en el peer.
2. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Control Link (HA1) (Enlace de control [HA1]).

© 2020 Palo Alto Networks, Inc.

3. Seleccione **Encryption Enabled**.



Si habilita el cifrado, cuando termine de configurar los cortafuegos de HA, puede seguir el procedimiento Actualización de las claves de SSH de HA1 y configuración de sus opciones*.*

STEP 11 | Configure la conexión del enlace de control de backup.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Control Link (HA1 Backup) (Enlace de control [copia de seguridad HA1]).
2. Seleccione la interfaz de copia de seguridad de HA1 y configure la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.



Los cortafuegos PA-3200 Series no admiten direcciones IPv6 para el enlace de control de copia de seguridad de HA1. Utilice direcciones IPv4.

STEP 12 | Configure la conexión del enlace de datos (HA2) y la conexión de HA2 de backup entre los cortafuegos.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Data Link (HA2) (Enlace de datos [HA2]).
2. Seleccione el **Port** para la conexión del enlace de datos.
3. Seleccione el método **Transport (Transporte)**. El valor predeterminado es **Ethernet** y funcionará cuando el par de HA se conecte directamente o a través de un conmutador. Si necesita enrutar el tráfico del enlace de datos a través de la red, seleccione IP o UDP como modo de transporte.
4. Si utiliza IP o UDP como método de transporte, introduzca la **IPv4/IPv6 Address (Dirección IPv4/IPv6)** y la **Netmask (Máscara de red)**.
5. Verifique que se ha seleccionado **Habilitar sincronización de sesión**.
6. Seleccione **HA2 Keep-alive (Conexión persistente de HA2)** para habilitar la supervisión del enlace de datos de HA2 entre los peers de HA. Si se produce un fallo basado en el umbral establecido (el valor predeterminado son 10.000 ms), se producirá la acción definida. Cuando se produce un fallo de conexión persistente de HA2, según la configuración, el sistema genera un mensaje de log de sistema crítico o provoca una división del plano de datos.



Puede configurar la conexión persistente de HA2 en ambos cortafuegos del par de HA o en uno de ellos. Si habilita esta opción solo en uno, ese cortafuegos es el único que envía los mensajes de conexión persistente. Si se produce un fallo, se notifica al otro cortafuegos.



La división provoca que los planos de datos de ambos peers funcionen de manera independiente, si bien el estado de alta disponibilidad sigue siendo activo-principal y activo-secundario. Aunque se configure la división del plano de datos en uno solo de los cortafuegos, también se aplica al otro dispositivo.

7. Edite la sección **Data Link (HA2 Backup) (Enlace de datos [copia de seguridad de HA2])**, seleccione la interfaz y añada la **IPv4/IPv6 Address (Dirección IPv4/Ipv6)** y la **Netmask (Máscara de red)**.
8. Haga clic en **OK (Aceptar)**.

STEP 13 | Configure el enlace HA3 para el reenvío de paquetes.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)** y edite Packet Forwarding (Reenvío de paquetes).
2. Para **HA3 Interface (Interfaz HA3)**, seleccione la interfaz que planea usar para reenviar paquetes entre los peers de HA activo/activo. Debe ser una interfaz dedicada con capacidad para el transporte de capa 2 y estar configurada en **Interface Type HA**.

© 2020 Palo Alto Networks, Inc.

3. Seleccione **VR Sync** para forzar la sincronización de todos los enrutadores virtuales configurados en los peers de HA. Use esta opción cuando el enrutador virtual no esté configurado para los protocolos de enrutamiento dinámico. Ambos peers deben conectarse al mismo enrutador de siguiente salto a través de una red conmutada y deben utilizar únicamente rutas estáticas.
4. Seleccione **QoS Sync** para sincronizar la selección de perfil de QoS en todas las interfaces físicas. Utilice esta opción cuando ambos peers tengan velocidades de enlace similares y requieran los mismos perfiles de QoS en todas las interfaces físicas. Este ajuste afecta a la sincronización de la configuración de QoS en la pestaña **Network (Red)**. La política de QoS se sincroniza independientemente de este ajuste.

STEP 14 | (Opcional) Modifique el tiempo de espera tentativa.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)** y edite Packet Forwarding (Reenvío de paquetes).
2. En **Tentative Hold Time (sec) (Tiempo de espera provisional [s])**, introduzca el número de segundos que permanece el cortafuegos en el estado Tentative (Provisional) tras recuperarse de un fallo (el intervalo es de 10 a 600 y el valor predeterminado, 60).

STEP 15 | Configure Session Owner (Responsable de la sesión) y Session Setup (Configuración de la sesión).

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)** y edite Packet Forwarding (Reenvío de paquetes).
2. En **Session Owner Selection**, seleccione una de las opciones siguientes:
   - **First Packet**: el cortafuegos que recibe el primer paquete de una nueva sesión es el propietario de la sesión (configuración recomendada). Este ajuste minimiza el tráfico por HA3 y distribuye la carga de tráfico por los peers.
   - **Primary Device**: el cortafuegos que está en estado activo-principal es el propietario de la sesión.
3. En **Session Setup (Configuración de la sesión)**, seleccione una de las opciones siguientes:
   - **IP Modulo (Módulo IP)**: el cortafuegos realiza una operación XOR en las direcciones IP de origen y destino del paquete; en función del resultado, elige el peer de HA que debe configurar la sesión.
   - **Primary Device (Dispositivo principal)**: El cortafuegos activo principal configura todas las sesiones.
   - **First Packet (Primer paquete)**: el cortafuegos que recibe el primer paquete de una nueva sesión realiza la configuración de la sesión (configuración recomendada).

     Comience con First Packet (Primer paquete) para Session Owner (Propietario de la sesión) y Session Setup (Configuración de la sesión) y, luego, según la distribución de carga, cambie a una de las otras opciones.
   - **IP Hash**: el cortafuegos utiliza un hash de la dirección IP de origen o una combinación de las direcciones IP de origen y destino para distribuir las responsabilidades de configuración de la sesión.
4. Haga clic en **OK (Aceptar)**.

STEP 16 | Configure direcciones virtuales de HA.

Necesita una dirección virtual para usar una Floating IP Address and Virtual MAC Address (Dirección IP flotante y dirección MAC virtual) o ARP Load-Sharing (Distribución de la carga de ARP).

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)**, seleccione **Add (Añadir)** para añadir una dirección virtual.
2. Introduzca o seleccione una **Interface (Interfaz)**.
3. Seleccione la pestaña **IPv4** o **IPv6** y haga clic en **Add**.
4. Introduzca una **IPv4 Address (Dirección IPv4)** o **IPv6 Address (Dirección IPv6)**.
5. Para **Type**:

© 2020 Palo Alto Networks, Inc.

- Seleccione **Floating** para configurar la dirección IP virtual como una dirección IP virtual flotante.
- Seleccione **ARP Load Sharing (Distribución de la carga ARP)** para configurar la dirección IP virtual como una dirección IP compartida y continúe con Configure ARP Load-Sharing (Configuración de la distribución de carga de ARP).

STEP 17 | Configure la dirección IP flotante.

1. No seleccione **Floating IP bound to the Active-Primary device (Vinculación de IP flotante al dispositivo activo-principal)** a menos que desee que el par HA activo/activo se comporte como un par HA activo/pasivo.
2. Para **Device 0 Priority (Prioridad de dispositivo 0)** y **Device 1 Priority (Prioridad de dispositivo 1)**, introduzca la prioridad para el cortafuegos configurado con el ID de dispositivo 0 y el ID de dispositivo 1, respectivamente. Las prioridades relativas determinan qué peer es propietario de la dirección IP flotante que acaba de configurar (el intervalo es de 0 a 255). El cortafuegos con el valor de prioridad más bajo (prioridad más alta) es propietario de la dirección IP flotante.
3. Seleccione **Failover address if link state is down (Dirección de conmutación por error si el estado del enlace es desconectado)** para hacer que el cortafuegos use la dirección de conmutación por error cuando el estado del enlace en la interfaz sea desconectado.
4. Haga clic en **OK (Aceptar)**.

STEP 18 | Configure ARP Load-Sharing (Distribución de la carga de ARP).

El algoritmo de selección del dispositivo determina qué cortafuegos HA responde a las solicitudes ARP para proporcionar la distribución de carga.

1. En **Device Selection Algorithm (Algoritmo de selección del dispositivo)**, seleccione una de las opciones siguientes:
   - **IP Modulo (Módulo IP)**: el cortafuegos que responderá a las solicitudes de ARP basándose en la paridad de la dirección IP de los solicitantes de ARP.
   - **IP Hash (Hash IP)**: el cortafuegos que responderá a las solicitudes de ARP basándose en un hash de la dirección IP de los solicitantes de ARP.
2. Haga clic en **OK (Aceptar)**.

STEP 19 | Defina las condiciones de conmutación por error de HA.

STEP 20 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Determinación del caso de uso activo/activo

Determine qué tipo de caso de uso tiene y luego seleccione el procedimiento correspondiente para configurar HA activa/activa.

Si está usando Redundancia basada en la ruta, Dirección IP flotante y dirección MAC virtual o Distribución de carga de ARP, seleccione el procedimiento correspondiente.

- Caso de uso: Configuración de HA activa/activa con redundancia basada en la ruta
- Caso de uso: Configuración de HA activa/activa con direcciones IP flotantes
- Caso de uso: Configuración de HA activa/activa con distribución de carga ARP

Si desea una implementación HA activa/activa de capa 3 que se comporte como una implementación activa/pasiva, seleccione el siguiente procedimiento:

- Caso de uso: Configuración HA activa/activa con dirección IP flotante enlazada a cortafuegos activo-principal

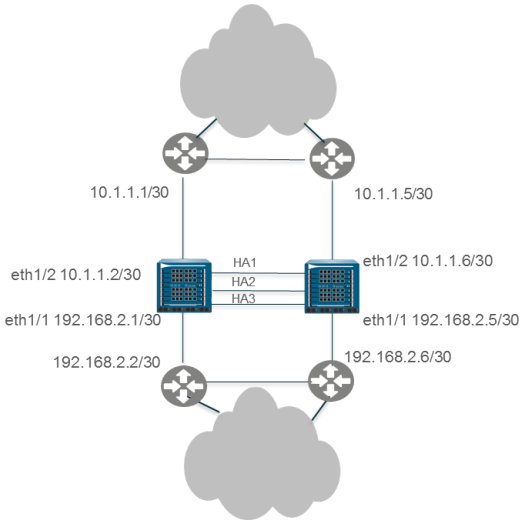
Si está configurando NAT en modo HA activa/activa, consulte los siguientes procedimientos:

© 2020 Palo Alto Networks, Inc.

- Caso de uso: Configuración de HA activa/activa con NAT DIPP de origen usando direcciones IP flotantes
- Caso de uso: Configuración de grupos de direcciones IP NAT de origen separadas para cortafuegos HA activo/activo
- Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino
- Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino en capa 3

Caso de uso: Configuración de HA activa/activa con redundancia basada en la ruta

La siguiente topología de capa 3 ilustra dos cortafuegos PA-7050 en un entorno de HA activa/activa que utiliza redundancia basada en la ruta. Los cortafuegos pertenecen a un área OSPF. Cuando un enlace o cortafuegos falla, OSPF maneja la redundancia al redireccionar el tráfico hacia el cortafuegos en funcionamiento.



STEP 1 | Configuración de la HA activa/activa.

Realice el paso 1 al paso 15.

STEP 2 | Configure OSPF.

Consulte OSPF.

STEP 3 | Defina las condiciones de conmutación por error de HA.

Defina las condiciones de conmutación por error de HA.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

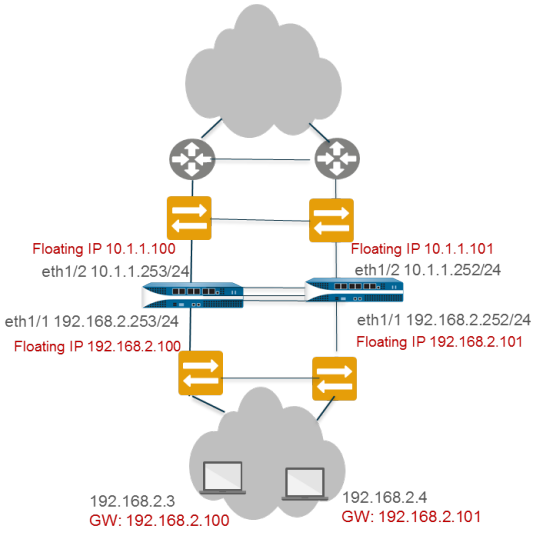
STEP 5 | Configure el cortafuegos del peer de la misma manera, excepto en el paso 5, si seleccionó el ID de dispositivo **0** para el primer cortafuegos, seleccione el ID de dispositivo **1** para el cortafuegos del peer.

Caso de uso: Configuración de HA activa/activa con direcciones IP flotantes

En este ejemplo de interfaz de capa 3, los cortafuegos HA se conectan a conmutadores y usan las direcciones IP flotantes para manejar fallos de enlace o cortafuegos. Los hosts de destino están

© 2020 Palo Alto Networks, Inc.

configurados cada uno con una puerta de enlace, que es la dirección IP flotante de uno de los cortafuegos HA. Consulte Dirección IP flotante y dirección MAC virtual.



STEP 1 | Configuración de la HA activa/activa.

Realice el paso 1 al paso 15.

STEP 2 | Configure direcciones virtuales de HA.

Necesita una dirección virtual para utilizar una dirección IP flotante y dirección MAC virtual.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)**, seleccione **Add (Añadir)** para añadir una dirección virtual.
2. Introduzca o seleccione una **Interface (Interfaz)**.
3. Seleccione la pestaña **IPv4** o **IPv6** y haga clic en **Add**.
4. Introduzca una **IPv4 Address (Dirección IPv4)** o **IPv6 Address (Dirección IPv6)**.
5. En **Type (Tipo)**, seleccione **Floating (Flotante)**, para configurar la dirección IP virtual como una dirección IP flotante.

STEP 3 | Configure la dirección IP flotante.

1. No seleccione **Floating IP bound to the Active-Primary device (IP flotante vinculada al dispositivo activo-principal)**.
2. Para **Device 0 Priority (Prioridad de dispositivo 0)** y **Device 1 Priority (Prioridad de dispositivo 1)**, introduzca la prioridad para el cortafuegos configurado con el ID de dispositivo 0 y el ID de dispositivo 1, respectivamente. Las prioridades relativas determinan qué peer es propietario de la dirección IP flotante que acaba de configurar (el intervalo es de 0 a 255). El cortafuegos con el valor de prioridad más bajo (prioridad más alta) es propietario de la dirección IP flotante.
3. Seleccione **Failover address if link state is down (Dirección de conmutación por error si el estado del enlace es desconectado)** para hacer que el cortafuegos use la dirección de conmutación por error cuando el estado del enlace en la interfaz sea desconectado.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

Realice el paso 19 de la Configuración HA activa/activa.

STEP 5 | Definición de las condiciones de conmutación por error de HA

© 2020 Palo Alto Networks, Inc.

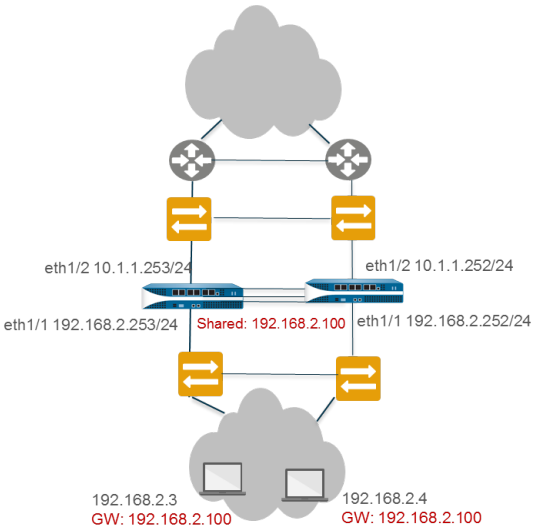
STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 7 | Configure el cortafuegos del peer de la misma manera, excepto que con la selección de un ID de dispositivo diferente.

Por ejemplo, si seleccionó el ID de dispositivo **0** para el primer cortafuegos, seleccione el ID de dispositivo **1** para el cortafuegos del peer.

Caso de uso: Configuración de HA activa/activa con distribución de carga ARP

En este ejemplo, los hosts de una implementación de capa 3 necesitan servicios de puerta de enlace de los cortafuegos HA. Los cortafuegos están configurados con una sola dirección IP compartida, que permite el Uso compartido de carga de ARP. Los hosts de destino están configurados con la misma puerta de enlace, que es la dirección IP compartida de los cortafuegos HA.



STEP 1 | Realice los pasos del 1 al 15 de la Configuración de la HA activa/activa.

STEP 2 | Configure direcciones virtuales de HA.

La dirección virtual es la dirección IP compartida que permite el Uso compartido de carga de ARP.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Configuración activa/activa)** > **Virtual Address (Dirección virtual)** y haga clic en **Add (Añadir)**.
2. Introduzca o seleccione una **Interface (Interfaz)**.
3. Seleccione la pestaña **IPv4** o **IPv6** y haga clic en **Add**.
4. Introduzca una **IPv4 Address (Dirección IPv4)** o **IPv6 Address (Dirección IPv6)**.
5. En **Type (Tipo)**, seleccione **ARP Load Sharing (Uso compartido de carga de ARP)**, que permite que ambos peers utilicen la dirección IP virtual para el Uso compartido de carga de ARP.

STEP 3 | Configure ARP Load-Sharing (Distribución de la carga de ARP).

El algoritmo de selección del dispositivo determina qué cortafuegos HA responde a las solicitudes ARP para proporcionar la distribución de carga.

1. En **Device Selection Algorithm (Algoritmo de selección del dispositivo)**, seleccione una de las opciones siguientes:

© 2020 Palo Alto Networks, Inc.

- **IP Modulo (Módulo IP)**: el cortafuegos que responderá a las solicitudes de ARP basándose en la paridad de la dirección IP de los solicitantes de ARP.
- **IP Hash (Hash IP)**: el cortafuegos que responderá a las solicitudes de ARP basándose en un hash de la dirección IP de los solicitantes de ARP.

2. Haga clic en **OK (Aceptar)**.

STEP 4 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

STEP 5 | Definición de las condiciones de conmutación por error de HA

STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 7 | Configure el cortafuegos del peer de la misma manera, excepto que con la selección de un ID de dispositivo diferente.

Por ejemplo, si seleccionó el ID de dispositivo **0** para el primer cortafuegos, seleccione el ID de dispositivo **1** para el cortafuegos del peer.

Caso de uso: Configuración HA activa/activa con dirección IP flotante enlazada a cortafuegos activo-principal

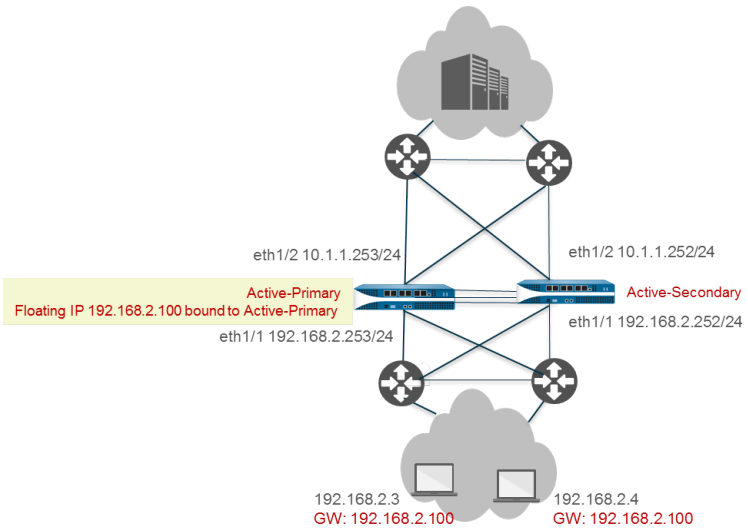
En centros de datos de misión crítica, puede configurar que ambos cortafuegos de HA de capa 3 participen en la supervisión de la ruta, para que puedan detectar fallos en la ruta antes de ambos cortafuegos. Además, usted prefiere controlar si y cuándo la dirección IP flotante regresa al cortafuegos recuperado después de que vuelva a activarse, y no la dirección IP flotante que regresa al ID de dispositivo al cual está vinculada. (Dicho comportamiento predeterminado se describe en Dirección IP flotante y dirección MAC virtual).

En este caso de uso, usted controla cuándo la dirección IP flotante y, por lo tanto, la función activa-principal regresan al peer HA recuperado. Los cortafuegos HA activo/activo comparten una sola dirección IP flotante que usted vincula con cualquier cortafuegos que esté en estado activo-principal. Con solo una dirección IP flotante el tráfico de red fluye predominantemente hacia un solo cortafuegos, por lo que esta implementación activa/activa funciona como una implementación activa/pasiva.

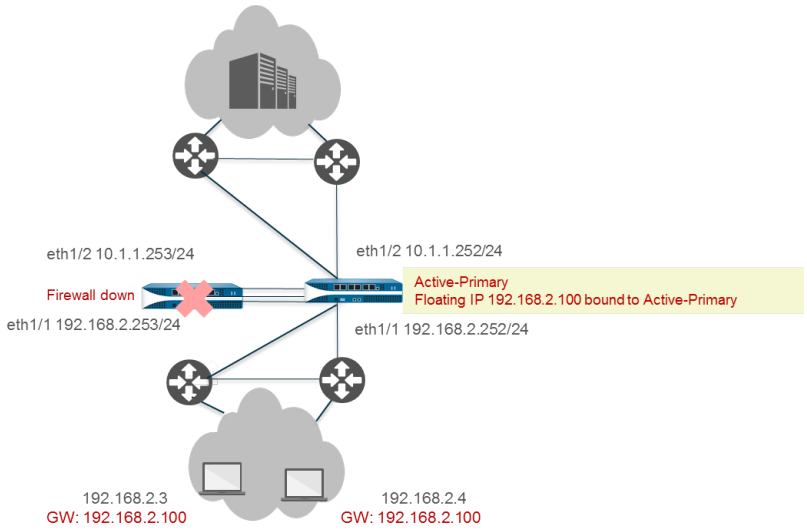
En este caso de uso, los conmutadores Cisco Nexus 7010 con PortChannels virtuales (virtual PortChannels, vPC) que operan en capa 3 se conectan a los cortafuegos. Debe configurar los conmutadores de capa 3 (peers de enrutador) antes y después de los cortafuegos con una preferencia de ruta hacia la dirección IP flotante. Es decir, debe diseñar su red de manera que las tablas de ruta de los peers de enrutador tengan la mejor ruta hacia la dirección IP flotante. Este ejemplo utiliza rutas estáticas con las métricas apropiadas, de manera que la ruta hacia la dirección IP flotante utiliza una métrica más baja (la ruta hacia la dirección IP flotante es la preferida) y recibe el tráfico. Una alternativa al uso de rutas estáticas sería diseñar la red para que redistribuya la dirección IP flotante en el protocolo de enrutamiento OSPF (si está usando OSPF).

La siguiente topología ilustra la dirección IP flotante vinculada al cortafuegos activo-principal, que inicialmente es el peer A, el cortafuegos de la izquierda.

© 2020 Palo Alto Networks, Inc.



Tras una conmutación por error, el cortafuegos activo-principal (peer A) deja de funcionar y el cortafuegos activo-secundario (peer B) toma el control como peer activo-principal, la dirección IP flotante pasa al peer B (se muestra en la siguiente figura). El peer B sigue siendo el cortafuegos activo-principal y el tráfico continúa fluyendo hacia el peer B, incluso aunque el peer A se recupere y se convierta en el cortafuegos activo-secundario. Usted decide si convertirá el peer A en el cortafuegos activo-principal nuevamente y cuándo.



La vinculación de la dirección IP flotante con el cortafuegos activo-principal le brinda mayor control sobre la manera en que el cortafuegos determina la propiedad de la dirección IP flotante a medida que se mueve entre diferentes estados HA de cortafuegos. Se obtienen las siguientes ventajas:

- Puede tener una configuración HA activa/activa para la supervisión de ruta de ambos cortafuegos, pero tener la función de los cortafuegos como una configuración HA activa/pasiva debido a que el tráfico direccionado hacia la dirección IP flotante siempre va hacia el cortafuegos activo-principal.

Cuando desactiva la preferencia en ambos cortafuegos, tiene los siguientes beneficios adicionales:

- La dirección IP flotante no se mueve hacia atrás y hacia adelante entre los cortafuegos HA si el cortafuegos activo-secundario alterna entre activo e inactivo.
- Puede revisar la funcionalidad del cortafuegos recuperado y los componentes adyacentes antes de dirigir el tráfico manualmente otra vez, y puede realizar esto en un tiempo de inactividad adecuado.

© 2020 Palo Alto Networks, Inc.

- Usted controla qué cortafuegos es propietario de la dirección IP flotante, de manera que mantiene todo el flujo de sesiones nuevas y existentes en el cortafuegos activo-principal, con lo cual minimiza el tráfico en el enlace HA3.



- *Recomendamos que configure la supervisión del enlace HA en las interfaces que admiten las direcciones IP flotantes para permitir que cada peer HA detecte rápidamente un fallo del enlace y realice una conmutación por error hacia su peer. Ambos peers HA deben tener supervisión de enlace para que funcione.*
- *Recomendamos que configure la supervisión de ruta HA para notificar a cada peer HA cuando una ruta haya fallado, para que los cortafuegos puedan realizar la conmutación por error hacia su peer. Debido a que la dirección IP flotante siempre está vinculada a un cortafuegos activo-principal, el cortafuegos no puede realizar automáticamente una conmutación por error hacia el peer cuando una ruta deja de funcionar y la supervisión de ruta no está habilitada.*



No puede configurar NAT para una dirección IP flotante que está vinculada a un cortafuegos activo-principal.

STEP 1 | Realice los pasos del 1 al 5 de la Configuración de la HA activa/activa.

STEP 2 | (Opcional) Deshabilite la preferencia.



Al deshabilitar la preferencia usted controla por completo cuándo el cortafuegos recuperado se convierte en el cortafuegos activo-principal.

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Election Settings (Configuración de elección).
2. Desmarque **Preemptive** si está habilitado.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Realice los pasos del 7 al 14 de la Configuración de la HA activa/activa.

STEP 4 | Configure Session Owner (Responsable de la sesión) y Session Setup (Configuración de la sesión).

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)** y edite Packet Forwarding (Reenvío de paquetes).
2. Para **Session Owner Selection (Selección del responsable de la sesión)**, le recomendamos que seleccione **Primary Device (Dispositivo principal)**. El cortafuegos que está en estado activo-principal es el propietario de la sesión.

   O bien, para **Session Owner Selection (Selección del responsable de la sesión)** puede seleccionar **First Packet (Primer paquete)** y luego para **Session Setup (Configuración de la sesión)**, seleccione **Primary Device (Dispositivo principal)** o **First Packet (Primer paquete)**.
3. Para **Session Setup (Configuración de sesión)**, seleccione **Primary Device (Dispositivo principal)**: el cortafuegos activo-principal configura todas las sesiones. Este es el ajuste recomendado si desea que su configuración activa/activa se comporte como una configuración activa/pasiva, debido a que mantiene toda la actividad en el cortafuegos activo-principal.

   También debe diseñar la red para eliminar la posibilidad de flujo de tráfico asimétrico hacia el par HA. Si no lo hace y el tráfico va hacia el cortafuegos activo-secundario, configurar Session Owner Selection (Selección del responsable de la sesión) y Session Setup (Configuración de la sesión) en Primary Device (Dispositivo principal)

© 2020 Palo Alto Networks, Inc.

hace que el tráfico atraviese HA3 para llegar al cortafuegos activo-principal para la propiedad de la sesión y la configuración de la sesión.

4. Haga clic en **OK (Aceptar)**.

STEP 5 | Configure direcciones virtuales de HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Configuración activa/activa)** > **Virtual Address (Dirección virtual)** y haga clic en **Add (Añadir)**.
2. Introduzca o seleccione una **Interface (Interfaz)**.
3. Seleccione la pestaña **IPv4** o **IPv6** y **Add (Añadir)** para añadir una **IPv4 Address (Dirección IPv4)**o **IPv6 Address (Dirección IPv6)**.
4. En **Type (Tipo)**, seleccione **Floating (Flotante)**, para configurar la dirección IP virtual como una dirección IP flotante.
5. Haga clic en **OK (Aceptar)**.

STEP 6 | Vincule la dirección IP flotante con el cortafuegos activo-principal.

1. Seleccione **Floating IP bound to the Active-Primary device (IP flotante vinculada al dispositivo activo-principal)**.
2. Seleccione **Failover address if link state is down (Dirección de conmutación por error si el estado del enlace es desconectado)** para hacer que el cortafuegos use la dirección de conmutación por error cuando el estado del enlace en la interfaz sea desconectado.
3. Haga clic en **OK (Aceptar)**.

STEP 7 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 9 | Configure el cortafuegos del peer de la misma manera, excepto que con la selección de un ID de dispositivo diferente.

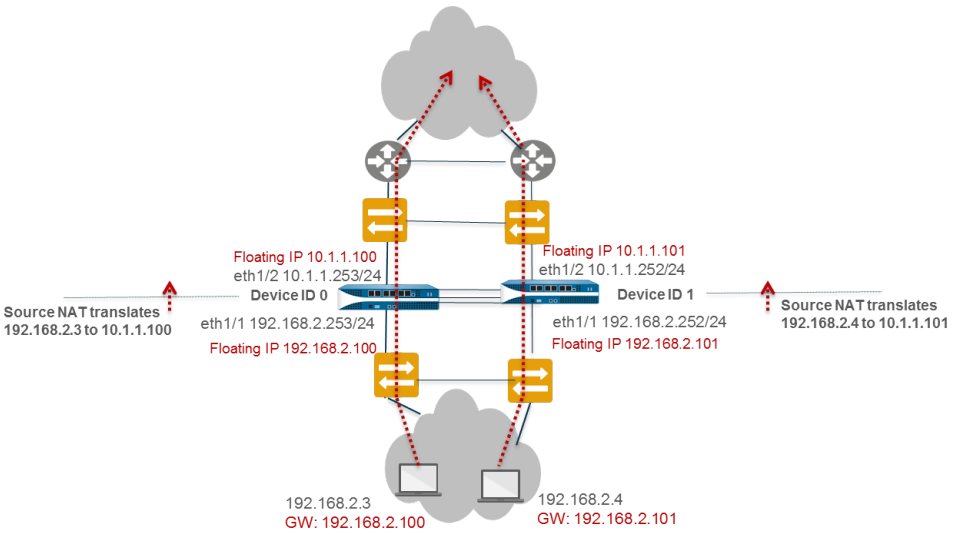
Por ejemplo, si seleccionó el ID de dispositivo **0** para el primer cortafuegos, seleccione el ID de dispositivo **1** para el cortafuegos del peer.

Caso de uso: Configuración de HA activa/activa con NAT DIPP de origen usando direcciones IP flotantes

Este ejemplo de interfaz de capa 3 utiliza NAT de origen en el modo HA activo/activo. Los conmutadores de capa 2 crean dominios de difusión para garantizar que los usuarios puedan llegar a todo lo comprendido antes y después de los cortafuegos.

PA-3050-1 tiene el ID de dispositivo 0 y su peer HA, PA-3050-2, tiene el ID de dispositivo 1. En este caso de uso, NAT traduce la dirección IP de origen y el número de puerto en la dirección IP flotante configurada en la interfaz de salida. Cada host se configura con una dirección de puerta de enlace por defecto, que es la dirección IP flotante en Ethernet1/1 de cada cortafuegos. La configuración requiere dos reglas NAT de origen, cada una vinculada a un ID de dispositivo, a pesar de que usted configura ambas reglas NAT en un solo cortafuegos y de que están sincronizadas con el cortafuegos peer.

© 2020 Palo Alto Networks, Inc.



STEP 1 | En los dispositivos PA-3050-2 (ID de dispositivo 1), realice los pasos del 1 al 3 de la Configuración de la HA activa/activa.

STEP 2 | Habilite la HA activa/activa

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.
3. Introduzca un **Group ID**, que debe ser el mismo para ambos cortafuegos. El cortafuegos utiliza el ID de grupo para calcular la dirección MAC virtual (el intervalo es 1-63).
4. Para **Mode (Modo)**, seleccione **Active Active (Activo activo)**.
5. Establezca el **Device ID (ID de dispositivo)** como **1**.
6. Seleccione **Enable Config Sync**. Este ajuste es obligatorio para sincronizar las dos configuraciones de cortafuegos (habilitado por defecto).
7. Introduzca la **Peer HA1 IP Address (Dirección IP de HA del peer)**, que es la dirección IP del enlace de control HA1 del cortafuegos del peer.
8. (Opcional) Introduzca una **Backup Peer HA1 IP Address (Dirección IP de HA1 de backup)**, que es la dirección IP del enlace de control de rcopia de seguridad del cortafuegos del peer.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Configuración de la HA activa/activa.

Complete los pasos del 6 al 14.

STEP 4 | Configure Session Owner (Responsable de la sesión) y Session Setup (Configuración de la sesión).

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)** y edite Packet Forwarding (Reenvío de paquetes).
2. Para **Session Owner Selection (Selección del responsable de la sesión)**, seleccione **First Packet (Primer paquete)**:el cortafuegos que recibe el primer paquete de una nueva sesión es el propietario de la sesión.
3. Para **Session Setup (Configuración de sesión)**, seleccione **IP Modulo (Módulo IP)**: distribuye la carga de configuración de la sesión sobre la base de la paridad de la dirección IP de origen.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Configure direcciones virtuales de HA.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Configuración activa/activa)** > **Virtual Address (Dirección virtual)** y haga clic en **Add (Añadir)**.
2. Seleccione **Interface (Interfaz)** eth1/1.
3. Seleccione **IPv4** y **Add (Añadir)**para añadir una **IPv4 Address** de 10.1.1.101.
4. En **Type (Tipo)**, seleccione **Floating (Flotante)**, para configurar la dirección IP virtual como una dirección IP flotante.

STEP 6 | Configure la dirección IP flotante.

1. No seleccione **Floating IP bound to the Active-Primary device (IP flotante vinculada al dispositivo activo-principal)**.
2. Seleccione **Failover address if link state is down (Dirección de conmutación por error si el estado del enlace es desconectado)** para hacer que el cortafuegos use la dirección de conmutación por error cuando el estado del enlace en la interfaz sea desconectado.
3. Haga clic en **OK (Aceptar)**.

STEP 7 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

STEP 8 | Defina las condiciones de conmutación por error de HA.

STEP 9 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 10 | Configure el cortafuegos del peer, PA-3050-1, con los mismos ajustes, excepto por los siguientes cambios:

- Seleccione **Device ID 0 (ID de dispositivo 0)**.
- Configure una dirección virtual de 10.1.1.100.
- Para **Device 1 Priority (Prioridad de dispositivo 1)**, introduzca 255. Para **Device 0 Priority (Prioridad de dispositivo 0)**, introduzca 0.

En este ejemplo, el ID de dispositivo 0 posee un valor de prioridad baja, por lo cual tiene prioridad alta . Así pues, el cortafuegos con el ID de dispositivo 0 (PA-3050-1) es propietario de la dirección IP 10.1.1.100.

STEP 11 | Antes de salir de PA-3050-1, cree la regla NAT de origen para el ID de dispositivo 0.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para la regla, que en este ejemplo la identifica como una regla NAT de origen para el ID de dispositivo 0.
3. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
4. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**.
5. Para **Destination Zone (Zona de destino)**, seleccione la zona que creó para la red externa.
6. Permita que **Destination Interface (Interfaz de destino)**, **Service (Servicio)**, **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)** queden configuradas en **Any (Cualquiera)**.
7. Para el **Translated Packet (Paquete traducido)**, seleccione **Dynamic IP And Port (IP dinámica y puerto)** para **Translation Type (Tipo de traducción)**.
8. Para **Address Type (Tipo de dirección)**, seleccione **Interface Address (Dirección de interfaz)**, en cuyo caso la dirección traducida será la dirección IP en la interfaz. Seleccione **Interface (Interfaz)** (eth1/1 en este ejemplo) y una **IP Address (Dirección IP)** de la dirección IP flotante 10.1.1.100.
9. En la pestaña **Active/Active HA Binding (Vinculación de HA activa/activa)**, para **Active/Active HA Binding**, seleccione **0** para vincular la regla NAT al ID de dispositivo 0.
10. Haga clic en **OK (Aceptar)**.

STEP 12 | Cree la regla NAT de origen para el ID de dispositivo 1.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para la regla de política, que en este ejemplo permite identificarla como una regla NAT de origen para el ID de dispositivo 1.
3. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
4. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**. Para **Destination Zone (Zona de destino)**, seleccione la zona que creó para la red externa.
5. Permita que **Destination Interface (Interfaz de destino)**, **Service (Servicio)**, **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)** queden configuradas en **Any (Cualquiera)**.
6. Para el **Translated Packet (Paquete traducido)**, seleccione **Dynamic IP And Port (IP dinámica y puerto)** para **Translation Type (Tipo de traducción)**.
7. Para **Address Type (Tipo de dirección)**, seleccione **Interface Address (Dirección de interfaz)**, en cuyo caso la dirección traducida será la dirección IP en la interfaz. Seleccione **Interface (Interfaz)** (eth1/1 en este ejemplo) y una **IP Address (Dirección IP)** de la dirección IP flotante 10.1.1.101.
8. En la pestaña **Active/Active HA Binding (Vinculación de HA activa/activa)**, para **Active/Active HA Binding**, seleccione **1** para vincular la regla NAT al ID de dispositivo 1.
9. Haga clic en **OK (Aceptar)**.

STEP 13 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Caso de uso: Configuración de grupos de direcciones IP NAT de origen separadas para cortafuegos HA activo/activo

Si desea usar grupos de direcciones IP para el NAT en modo HA activa/activa de origen, cada cortafuegos debe tener su propio grupo, que usted luego vinculará a un ID de dispositivo en una regla NAT.

Los objetos de direcciones y reglas NAT se sincronizan (en el modo activo/pasivo y activo/activo), por lo que deben configurarse en solo uno de los cortafuegos del par HA.

Este ejemplo configura un objeto de dirección denominado Dyn-IP-Pool-dev0 que contiene el grupo de direcciones IP 10.1.1.140-10.1.1.150. También configura un objeto de dirección denominado Dyn-IP-Pool-dev1 que contiene el grupo de direcciones IP 10.1.1.160-10.1.1.170. El primer objeto de dirección está vinculado al ID de dispositivo 0; el segundo objeto de dirección está vinculado al ID de dispositivo 1.

STEP 1 | ECree objetos de dirección en un cortafuegos HA.

1. Seleccione **Objects (Objetos)** > **Addresses (Dirección)** y luego haga clic en **Add (Añadir)** para añadir un nombre de objeto de dirección en **Name (Nombre)**, que, en este ejemplo, es Dyn-IP-Pool-dev0.
2. Para **Type (Tipo)**, seleccione **IP Range (Intervalo IP)** e introduzca el intervalo 10.1.1.140-10.1.1.150.
3. Haga clic en **OK (Aceptar)**.
4. Repita este paso para configurar otro objeto de dirección denominado Dyn-IP-Pool-dev1 con el **IP Range (Intervalo IP)** de 10.1.1.160-10.1.1.170.

STEP 2 | Cree la regla NAT de origen para el ID de dispositivo 0.

1. Seleccione **Policies (Política)** > **NAT** y luego, haga clic en **Add (Añadir)** para añadir una regla de política NAT con un nombre en **Name (Nombre)**; por ejemplo, Src-NAT-dev0.
2. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**.
3. Para **Destination Zone (Zona de destino)**, seleccione la zona de destino para la cual desea traducir la dirección de origen, como por ejemplo, Untrust.
4. En **Translated Packet (Paquete traducido)**, para **Translation Type (Tipo de traducción)**, seleccione **Dynamic IP and Port (IP dinámica y puerto)**.

© 2020 Palo Alto Networks, Inc.

5. Para **Translated Address (Dirección traducida)**, seleccione **Add (Añadir)** para añadir el objeto de dirección que creó para el grupo de direcciones que pertenecen al ID de dispositivo 0: Dyn-IP-Pool-dev0.
6. Para **Active/Active HA Binding (Vinculación de HA activa/activa)**, seleccione **0** para vincular la regla NAT al ID de dispositivo 0.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree la regla NAT de origen para el ID de dispositivo 1.

1. Seleccione **Policies (Política)** > **NAT** y luego, haga clic en **Add (Añadir)** para añadir una regla de política NAT con un nombre en **Name (Nombre)**; por ejemplo, Src-NAT-dev1.
2. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**.
3. Para **Destination Zone (Zona de destino)**, seleccione la zona de destino para la cual desea traducir la dirección de origen, como por ejemplo, Untrust.
4. En **Translated Packet (Paquete traducido)**, para **Translation Type (Tipo de traducción)**, seleccione **Dynamic IP and Port (IP dinámica y puerto)**.
5. Para **Translated Address (Dirección traducida)**, seleccione **Add (Añadir)** para añadir el objeto de dirección que creó para el grupo de direcciones que pertenecen al ID de dispositivo 1: Dyn-IP-Pool-dev1.
6. Para **Active/Active HA Binding (Vinculación de HA activa/activa)**, seleccione **1** para vincular la regla NAT al ID de dispositivo 1.
7. Haga clic en **OK (Aceptar)**.

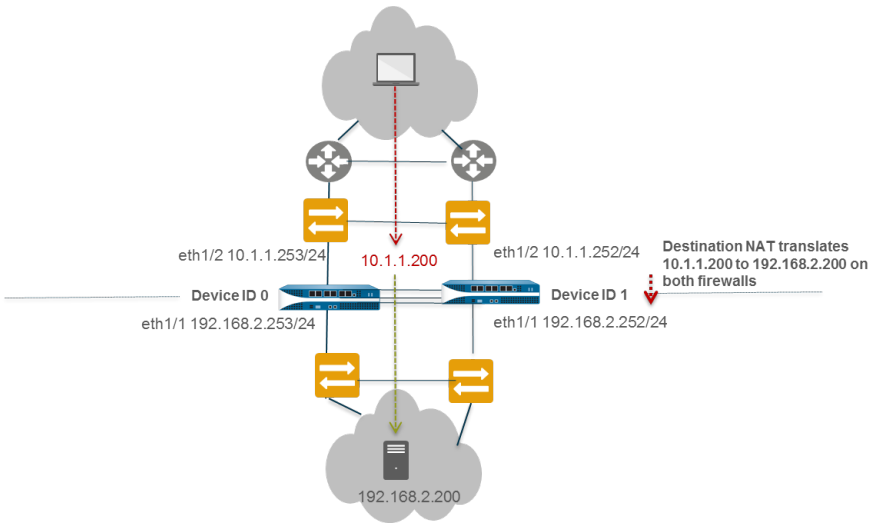
STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino

Este ejemplo de interfaz de capa 3 utiliza NAT en modo HA activa/activa y Uso compartido de carga de ARP con NAT de destino. Ambos cortafuegos HA responden a una solicitud ARP para la dirección NAT de destino con la dirección MAC de la interfaz de salida. La NAT de destino traduce la dirección IP compartida pública (en este ejemplo, 10.1.1.200) a la dirección IP privada del servidor (en este ejemplo, 192.168.2.200).

Cuando los cortafuegos HA reciben tráfico para el destino 10.1.1.200, ambos cortafuegos podrían responder a la solicitud ARP, lo que podría causar la inestabilidad de la red. Para evitar el posible uso, configure el cortafuegos que está en estado activo-principal para que responda a la solicitud ARP mediante la vinculación de la regla NAT de destino con el cortafuegos activo-principal.

© 2020 Palo Alto Networks, Inc.



STEP 1 | En los dispositivos PA-3050-2 (ID de dispositivo 1), realice los pasos del 1 al 3 de la Configuración de la HA activa/activa.

STEP 2 | Habilite la HA activa/activa

1. En **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**, edite Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.
3. Introduzca un **Group ID**, que debe ser el mismo para ambos cortafuegos. El cortafuegos utiliza el ID de grupo para calcular la dirección MAC virtual (el intervalo es 1-63).
4. (Opcional) Introduzca una **descripción**.
5. Para **Mode (Modo)**, seleccione **Active Active (Activo activo)**.
6. En **Device ID (ID de dispositivo)** seleccione **1**.
7. Seleccione **Enable Config Sync**. Este ajuste es obligatorio para sincronizar las dos configuraciones de cortafuegos (habilitado por defecto).
8. Introduzca la **Peer HA1 IP Address (Dirección IP de HA del peer)**, que es la dirección IP del enlace de control HA1 del cortafuegos del peer.
9. (Opcional) Introduzca una **Backup Peer HA1 IP Address (Dirección IP de HA1 de backup)**, que es la dirección IP del enlace de control de rcopia de seguridad del cortafuegos del peer.
10. Haga clic en **OK (Aceptar)**.

STEP 3 | Realice del paso 6 al paso 15 de la Configuración HA activa/activa.

STEP 4 | Configure direcciones virtuales de HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Configuración activa/activa)** > **Virtual Address (Dirección virtual)** y haga clic en **Add (Añadir)**.
2. Seleccione **Interface (Interfaz)** eth1/1.
3. Seleccione **IPv4** y **Add (Añadir)**para añadir una **IPv4 Address** de 10.1.1.200.
4. En **Type (Tipo)**, seleccione **ARP Load Sharing (Uso compartido de carga de ARP)**, lo que configura la dirección IP virtual que utilizarán ambos peers para el ARP Load-Sharing (Uso compartido de carga de ARP).

STEP 5 | Configure ARP Load-Sharing (Distribución de la carga de ARP).

El algoritmo de selección del dispositivo determina qué cortafuegos HA responde a las solicitudes ARP para proporcionar la distribución de carga.

© 2020 Palo Alto Networks, Inc.

1. Para **Device Selection Algorithm (Algoritmo de selección del dispositivo)**, seleccione **IP Modulo (Módulo IP)**. El cortafuegos que responderá a las solicitudes de ARP basándose en la paridad de la dirección IP de los solicitantes de ARP.
2. Haga clic en **OK (Aceptar)**.

STEP 6 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

STEP 7 | Defina las condiciones de conmutación por error de HA.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 9 | Configure el cortafuegos del peer, PA-3050-1 (ID de dispositivo 0), con la misma configuración, excepto en el paso 2, donde debe seleccionar **Device ID 0 (ID de dispositivo 0)**.

STEP 10 | Antes de salir de PA-3050-1 (ID de dispositivo 0), cree la regla NAT de destino para que el cortafuegos activo-principal responda a solicitudes de ARP.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para la regla, que en este ejemplo la identifica como una regla NAT de destino para el ARP de capa 2.
3. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
4. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**.
5. Para **Destination Zone (Zona de destino)**, seleccione la zona Untrust que creó para la red externa.
6. Permita que **Destination Interface (Interfaz de destino)**, **Service (Servicio)** y **Source Address (Dirección de origen)** queden configuradas en **Any (Cualquiera)**.
7. Para **Destination Address (Dirección de destino)**, especifique 10.1.1.200.
8. En **Translated Packet (Paquete traducido)**, Source Address Translation (Traducción de dirección de origen) se queda como **None (Ninguno)**.
9. Para **Destination Address Translation (Traducción de dirección de destino)**, introduzca la dirección IP privada del servidor de destino, que en este ejemplo es 192.168.1.200.
10. En la pestaña **Active/Active HA Binding (Enlace HA activo/activo)**, en **Active/Active HA Binding (Enlace HA activo/activo)**, seleccione **primary (principal)** para vincular la regla NAT con el cortafuegos en estado activo-principal.
11. Haga clic en **OK (Aceptar)**.

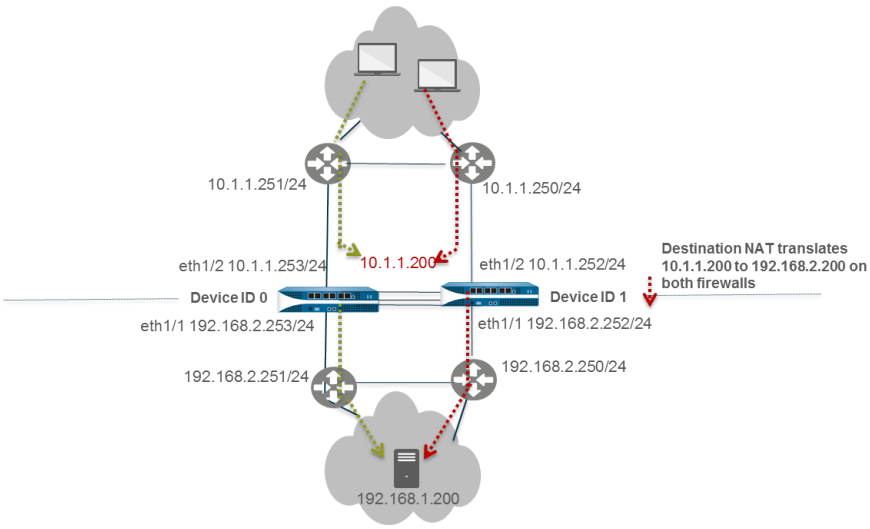
STEP 11 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Caso de uso: Configuración de HA activa/activa para distribución de carga ARP con NAT de destino en capa 3

Este ejemplo de interfaz de capa 3 utiliza NAT en modo HA activa/activa y Uso compartido de carga de ARP. PA-3050-1 tiene el ID de dispositivo 0 y su peer HA, PA-3050-2, tiene el ID de dispositivo 1.

En este caso de uso, ambos cortafuegos HA deben responder a una solicitud ARP para la dirección NAT de destino. El tráfico puede llegar a cualquiera de los cortafuegos de cualquier enrutador WAN en la zona no fiable. La NAT de destino traduce la dirección IP compartida pública a la dirección IP privada del servidor. La configuración requiere una regla NAT de destino vinculada a ambos ID de dispositivo, a fin de que ambos cortafuegos puedan responder a solicitudes ARP.

© 2020 Palo Alto Networks, Inc.



STEP 1 | En los dispositivos PA-3050-2 (ID de dispositivo 1), realice los pasos del 1 al 3 de la Configuración de la HA activa/activa.

STEP 2 | Habilite la HA activa/activa

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración.
2. Seleccione **Enable HA (Habilitar HA)**.
3. Introduzca un **Group ID**, que debe ser el mismo para ambos cortafuegos. El cortafuegos utiliza el ID de grupo para calcular la dirección MAC virtual (el intervalo es 1-63).
4. (Opcional) Introduzca una **descripción**.
5. Para **Mode (Modo)**, seleccione **Active Active (Activo activo)**.
6. En **Device ID (ID de dispositivo)** seleccione **1**.
7. Seleccione **Enable Config Sync**. Este ajuste es obligatorio para sincronizar las dos configuraciones de cortafuegos (habilitado por defecto).
8. Introduzca la **Peer HA1 IP Address (Dirección IP de HA del peer)**, que es la dirección IP del enlace de control HA1 del cortafuegos del peer.
9. (Opcional) Introduzca una **Backup Peer HA1 IP Address (Dirección IP de HA1 de backup)**, que es la dirección IP del enlace de control de rcopia de seguridad del cortafuegos del peer.
10. Haga clic en **OK (Aceptar)**.

STEP 3 | Configuración de la HA activa/activa.

Realice el paso 6 al paso 15.

STEP 4 | Configure direcciones virtuales de HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Configuración activa/activa)** > **Virtual Address (Dirección virtual)** y haga clic en **Add (Añadir)**.
2. Seleccione **Interface (Interfaz)** eth1/2.
3. Seleccione **IPv4** y **Add (Añadir)**para añadir una **IPv4 Address** de 10.1.1.200.
4. En **Type (Tipo)**, seleccione **ARP Load Sharing (Uso compartido de carga de ARP)**, lo que configura la dirección IP virtual que utilizarán ambos peers para el ARP Load-Sharing (Uso compartido de carga de ARP).

STEP 5 | Configure ARP Load-Sharing (Distribución de la carga de ARP).

© 2020 Palo Alto Networks, Inc.

El algoritmo de selección del dispositivo determina qué cortafuegos HA responde a las solicitudes ARP para proporcionar la distribución de carga.

1. En **Device Selection Algorithm (Algoritmo de selección del dispositivo)**, seleccione una de las opciones siguientes:
   - **IP Modulo (Módulo IP)**: el cortafuegos que responderá a las solicitudes de ARP basándose en la paridad de la dirección IP de los solicitantes de ARP.
   - **IP Hash (Hash IP)**: el cortafuegos que responderá a las solicitudes de ARP se basa en un hash de la dirección IP de origen y destino de los solicitantes de ARP.
2. Haga clic en **OK (Aceptar)**.

STEP 6 | Habilite las tramas gigantes en los cortafuegos que no sean de la serie PA-7000.

STEP 7 | Defina las condiciones de conmutación por error de HA.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 9 | Configure el cortafuegos del peer, PA-3050-1 (ID de dispositivo 0), con la misma configuración, pero ajuste la **Device ID (ID de dispositivo)** en **0** en lugar de **1**.

STEP 10 | Antes de salir de PA-3050-1 (ID de dispositivo 0), cree la regla NAT de destino para el ID de dispositivo 0 y el ID de dispositivo 1

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para la regla, que en este ejemplo la identifica como una regla NAT de destino para el ARP de capa 3.
3. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
4. En **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, seleccione **Any (Cualquiera)**.
5. Para **Destination Zone (Zona de destino)**, seleccione la zona Untrust que creó para la red externa.
6. Permita que **Destination Interface (Interfaz de destino)**, **Service (Servicio)** y **Source Address (Dirección de origen)** queden configuradas en **Any (Cualquiera)**.
7. Para **Destination Address (Dirección de destino)**, especifique 10.1.1.200.
8. Para **Translated Packet (Paquete traducido)**, Source Address Translation(Traducción de dirección de origen) queda en None (Ninguno).
9. Para **Destination Address Translation (Traducción de dirección de destino)**, introduzca la dirección IP privada del servidor de destino, que en este ejemplo es 192.168.1.200.
10. En la pestaña **Active/Active HA Binding (Enlace HA activo/activo)**, en **Active/Active HA Binding (Enlace HA activo/activo)**, seleccione**both (Ambos)** para vincular la regla NAT al ID de dispositivo 0 y al ID de dispositivo 1.
11. Haga clic en **OK (Aceptar)**.

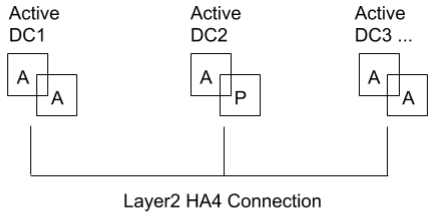
STEP 11 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

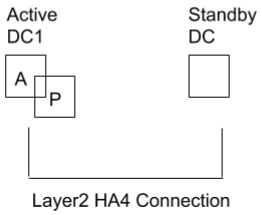
© 2020 Palo Alto Networks, Inc.

Descripción general de agrupación en clústeres de HA

Varios modelos de cortafuegos de Palo Alto Networks® ahora admiten la sincronización del estado de sesión entre el cortafuegos en un clúster de alta disponibilidad (HA, High Availability) de hasta 16 cortafuegos. Los pares del clúster de HA sincronizan sesiones para protegerse contra fallos del centro de datos o un gran punto de inspección de seguridad con cortafuegos escalados horizontalmente. En el caso de una interrupción de la red o un cortafuegos caído, las sesiones conmutan por error a un cortafuegos diferente en el clúster. Dicha sincronización es especialmente útil en los siguientes casos de uso.

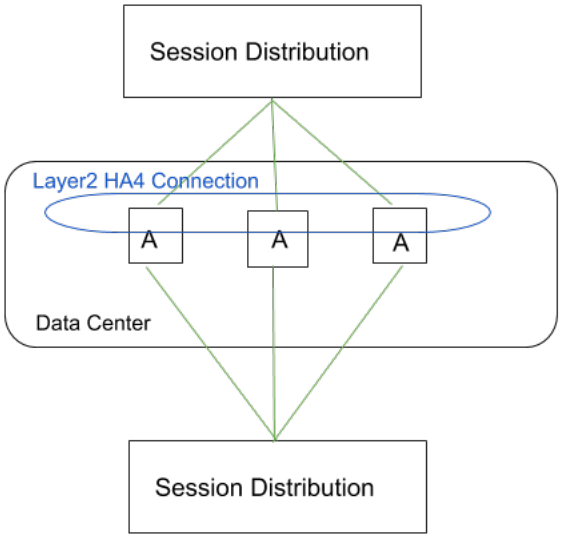
Uno de los casos de uso se produce cuando los pares de HA se distribuyen en varios centros de datos, de modo que no hay un solo punto de fallo dentro de los centros de datos o entre ellos. Un segundo caso de uso de varios centros de datos se produce cuando un centro de datos está activo y el otro está en espera.





Un tercer caso de uso de agrupación en clústeres de HA es el de escalado horizontal, en el que se añaden miembros del clúster de HA a un único centro de datos para escalar la seguridad y garantizar la supervivencia de la sesión.

© 2020 Palo Alto Networks, Inc.



Los clústeres de HA admiten una implementación de cable virtual o de capa 3. Los peers de HA en el clúster pueden ser una combinación de pares de HA y miembros de clúster independientes. En un clúster de HA, todos los miembros se consideran activos; No existe un concepto de cortafuegos pasivos excepto los pares de HA, que pueden mantener su relación activo/pasivo después de agregarlos a un clúster de HA.

Todos los miembros del clúster comparten el estado de la sesión. Cuando un nuevo cortafuegos se une a un clúster de HA, eso activa todos los cortafuegos del clúster para sincronizar todas las sesiones existentes. Las conexiones de reserva HA4 y HA4 son los enlaces de clúster dedicados que sincronizan el estado de la sesión entre todos los miembros del clúster que tienen el mismo ID de clúster. El enlace HA4 entre los miembros del clúster detecta fallos de conectividad entre los miembros del clúster. HA1 (enlace de control), HA2 (enlace de datos) y HA3 (enlace de reenvío de paquetes) no se admiten entre miembros del clúster que no son pares de HA.

Para una sesión normal que no ha fallado, solo el cortafuegos que es el propietario de la sesión crea un log de tráfico. Para una sesión fallida, el nuevo propietario de la sesión (el cortafuegos que recibe el tráfico que ha fallado) crea el log de tráfico.

Los modelos de cortafuegos que admiten la agrupación en clústeres de HA y el número máximo de miembros admitidos por clúster son los siguientes:

Modelo de cortafuegos	Número de miembros admitidos por clúster
Serie PA-3200	6
PA-5200 Series	16
Cortafuegos PA-7000 Series que tienen al menos una de las siguientes tarjetas: PA-7000-100G-NPC, PA-7000-20GQXM-NPC, PA-7000-20GXM-NPC	PA-7080: 4 PA-7050: 6
VM-300	6
VM-500	6

© 2020 Palo Alto Networks, Inc.

Modelo de cortafuegos	Número de miembros admitidos por clúster
VM-700	16

Considere el Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA antes de empezar con Configuración de la agrupación en clústeres de HA.

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA

Estos son los requisitos de aprovisionamiento y las prácticas recomendadas para la agrupación en clústeres de HA.

- Requisitos de aprovisionamiento y prácticas recomendadas
  - Los miembros del clúster de HA deben ser del mismo modelo de cortafuegos y ejecutar la misma versión de PAN-OS®.

    Al actualizar, los miembros del cortafuegos seguirán sincronizando sesiones con un miembro en una versión diferente.
  - Es muy recomendable y una práctica recomendada utilizar Panorama para aprovisionar miembros del clúster de HA para mantener todas las configuraciones y políticas sincronizadas entre todos los miembros del clúster.
  - Los miembros del clúster de HA deben tener licencia para los mismos componentes con el fin de garantizar la aplicación de políticas y las capacidades de inspección de contenido coherentes.
  - Las licencias deben caducar al mismo tiempo para evitar licencias no coincidentes y pérdida de funcionalidad.
  - Todos los miembros del clúster deben ejecutarse con la misma versión de actualizaciones de contenido dinámicas para una aplicación de seguridad coherente.
  - Los miembros del clúster de HA deben compartir los mismos nombres de zona para que las sesiones conmuten correctamente a otro miembro del clúster. Por ejemplo, suponga que las sesiones que van a una zona de entrada llamada **`internal (interna)`** se descartan porque el enlace no funciona. Para que esas sesiones conmuten por error a un peer de cortafuegos de HA en el clúster, ese peer también debe tener una zona denominada **`internal (interna)`**.
  - Los flujos de cliente a servidor y de servidor a cliente deben volver al mismo cortafuegos en condiciones normales (sin fallos) para que se produzca el análisis de contenido de seguridad. El tráfico asimétrico no se eliminará y no se podrá escanear por motivos de seguridad.
- Prácticas recomendadas para la sincronización de sesiones
  - Deben utilizarse interfaces de comunicación de HA dedicadas sobre interfaces de plano de datos. Las interfaces HSCI no se utilizan para HA4. Esto permite la separación del par de HA y la sincronización de sesiones de clúster para garantizar el máximo ancho de banda y fiabilidad para la sincronización de sesiones.
  - HA4 debe tener el tamaño adecuado si utiliza interfaces de plano de datos. Esto garantiza la mejor sincronización del estado de la sesión entre los miembros del clúster
  - La práctica recomendada es tener una red de clúster dedicada para el enlace de comunicaciones HA4 con el fin de garantizar un ancho de banda adecuado y conexiones no congestionadas y de baja latencia entre los miembros del clúster.
  - Diseñe sus redes y realice ingeniería de tráfico para evitar posibles condiciones de carrera, en las que una red dirige el tráfico del propietario de la sesión a un miembro del clúster antes de que la sesión se sincronice correctamente entre los cortafuegos. Las conexiones HA4 de capa 2 deben tener suficiente ancho de banda y baja latencia para permitir la sincronización oportuna entre los miembros de HA. La latencia de HA4 debe ser menor que la latencia en que se incurre cuando los dispositivos de intercambio de tráfico cambian el tráfico entre los miembros del clúster.
  - Diseñe sus redes para minimizar los flujos asimétricos. La configuración de la sesión requiere que un miembro del clúster vea el protocolo de enlace de tres vías TCP completo.
- Prácticas recomendadas de verificación de estado

© 2020 Palo Alto Networks, Inc.

- En los pares de HA en un clúster, configure un par activo/pasivo con enlaces de comunicación de reserva de HA para HA1, HA2 y HA4. Configure un par activo/activo con enlaces de comunicaciones de copia de seguridad de HA para HA1, HA2, HA3 y HA4.
- Configure los enlaces de reserva de HA4 en todos los miembros del clúster.

© 2020 Palo Alto Networks, Inc.

Configuración de la agrupación en clústeres de HA

Obtenga información sobre la agrupación en clústeres de HA y siga las Prácticas recomendadas y aprovisionamiento de la agrupación en clústeres de HA antes de configurar los firewalls de alta disponibilidad como miembros de un clúster.

STEP 1 | Establezca una interfaz como interfaz de HA (para luego asignarla como enlace HA4).

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz; por ejemplo, ethernet1/1.
2. En **Interface Type (Tipo de interfaz)** seleccione la opción **HA**.
3. Asigne la interfaz a una **zona de seguridad**.
4. Haga clic en **OK (Aceptar)**.
5. Repita este paso para configurar otra interfaz que usar como enlace de reserva HA4.

STEP 2 | Habilite la agrupación en clústeres de HA.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la configuración de agrupación en clústeres
2. **Habilite la participación de clústeres**.
3. Especifique el **ID de clúster**, un ID numérico único para un clúster de HA en el que todos los miembros pueden compartir el estado de la sesión; el intervalo es de 1 a 99.
4. Especifique una **descripción del clúster** breve y útil.
5. (Opcional) Cambie el **Tiempo de espera de sincronización del clúster (min)**, que es la cantidad máxima de minutos que el cortafuegos local espera antes de pasar al estado Active (Activo) cuando otro miembro del clúster (por ejemplo, en estado desconocido) impide que el clúster se sincronice por completo; el intervalo es de 0 a 30; el valor predeterminado es 0.
6. (Opcional) Cambie **Monitor Fail Hold Down Time (min) (Supervisar tiempo de retención de fallos)**, que es el número de minutos después de los que se vuelve a probar un enlace descendente para ver si está funcionando; el intervalo es de 1 a 60; el valor predeterminado es 1.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure el enlace HA4.

1. Seleccione **HA Communications (Comunicaciones de HA)** y en la sección Clustering Links (Enlaces de agrupación en clústeres), edite la sección HA4.
2. Seleccione la interfaz que configuró en el primer paso como una interfaz de **HA** para que sea el **puerto** para el enlace HA4; por ejemplo, ethernet1/1.
3. Especifique la **dirección IPv4/IPv6** de la interfaz HA4 local.
4. Introduzca la **Netmask (Máscara de red)**.
5. (Opcional) Cambie el **umbral de conexión persistente de HA4 (ms)** para especificar el intervalo de tiempo dentro del que el cortafuegos debe recibir conexiones persistentes de un miembro del clúster para saber que el miembro del clúster es funcional; el intervalo es de 5000 a 60 000; el valor predeterminado es 10 000.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure el enlace de reserva de HA4.

1. Edite la sección HA4 Backup (Copia de seguridad de HA4).
2. Seleccione la otra interfaz que configuró en el primer paso como una interfaz de **HA** para que sea el **puerto** para el enlace de reserva de HA4.

© 2020 Palo Alto Networks, Inc.

3. Especifique la **dirección IPv4/IPv6** de la interfaz de reserva de HA4 local.
4. Introduzca la **Netmask (Máscara de red)**.
5. Haga clic en **OK (Aceptar)**.

STEP 5 | Especifique todos los miembros del clúster de HA, incluido el miembro local y ambos peers de HA en cualquier par de HA.

1. Seleccione **Cluster Config (Configuración de clúster)**.
2. (En un cortafuegos compatible) **Añada** un **número de serie del dispositivo** del miembro del peer.
3. (En Panorama) **Añada** y seleccione un **dispositivo** del menú desplegable y especifique el **nombre del dispositivo**.
4. Especifique la **dirección IP de HA4** del peer de HA en el clúster.
5. Introduzca la **dirección IP de reserva de HA4** del peer de HA en el clúster.
6. Habilite la **sincronización de sesión** con el peer que identificó.
7. (Opcional) Especifique una **descripción** que resulte útil.
8. Haga clic en **OK (Aceptar)**.
9. Seleccione el dispositivo y **habilítelo**.

STEP 6 | Defina las condiciones de conmutación por error de HA con supervisión de enlaces y rutas.

STEP 7 | Seleccione **Confirmar**.

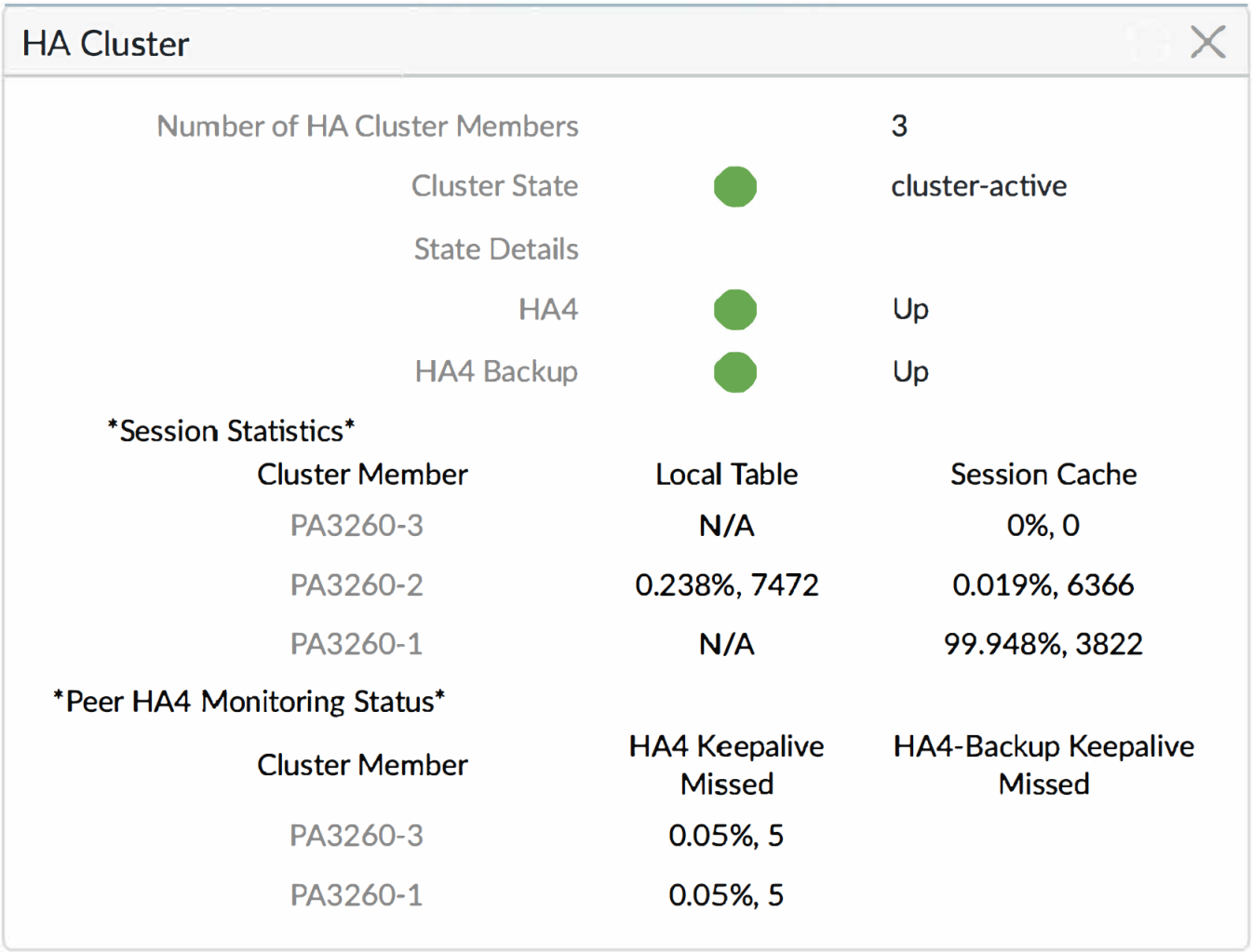
STEP 8 | (Solo Panorama) Actualice la lista de cortafuegos de HA en el clúster de HA.

1. En Templates (Plantillas), seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Cluster Config (Configuración de clúster)**.
2. Haga clic en **Refresh (Actualizar)** en la parte inferior de la pantalla.

STEP 9 | Vea la información del clúster de HA en la interfaz de usuario.

1. Seleccione **Dashboard (Panel)**.
2. Visualice los campos del clúster de HA. La sección superior muestra el estado del clúster y las conexiones HA4 para proporcionar el estado del clúster de un vistazo. Los indicadores de reserva de HA4 y HA4 serán uno de los siguientes: El verde indica que el estado del enlace de los miembros del clúster es Up (Activo). El rojo indica que el estado del enlace de todos los miembros del clúster es Down (Inactivo). El amarillo indica que el estado del enlace de algunos miembros del clúster es Up (Activo) mientras que el estado de otros miembros del clúster es Down (Inactivo). El gris indica que no está configurado. La sección central muestra la capacidad de la tabla de sesión local y la tabla de caché de sesión para que pueda supervisar si las tablas están llenas y planificar las actualizaciones del cortafuegos. La sección inferior muestra errores de comunicación en los enlaces de reserva de HA4 y HA4, lo que significa posibles problemas con la sincronización de información entre miembros.

© 2020 Palo Alto Networks, Inc.



STEP 10 | Acceda a la CLI para ver la información del enlace de HA4 y el clúster de HA y realizar otras tareas de agrupación en clústeres de HA.

© 2020 Palo Alto Networks, Inc.

Actualización de las claves de SSH de HA1 y configuración de sus opciones

Todos los cortafuegos de Palo Alto Networks tienen preconfigurado el Shell seguro (Secure Shell, SSH), y los de alta disponibilidad (HA, High Availability) pueden actuar como servidor y cliente SSH de forma simultánea. Si configura la alta disponibilidad (HA, High Availability) con peers activo/pasivo o con peers activo/activo, puede habilitar el cifrado en la conexión (enlace de control) de HA1 entre los cortafuegos de HA. Le recomendamos que proteja el tráfico HA1 entre los peers de HA con cifrado, especialmente si los cortafuegos no están ubicados en el mismo sitio. Después de habilitar el cifrado en el enlace de control HA1, puede usar la CLI para crear un perfil de servicio SSH y garantizar la conexión entre los cortafuegos de HA.

Los perfiles de servicio SSH le permiten cambiar el tipo de clave de host predeterminado, generar un par nuevo de claves de host SSH pública y privada para el enlace de control de HA1 y configurar otros ajustes de HA1 de SSH. Puede aplicar las nuevas claves de host y las configuraciones establecidas en los cortafuegos sin reiniciar los peers de HA. El cortafuegos restablecerá las sesiones de HA1 con su peer para sincronizar los cambios de configuración. También genera logs del sistema (el subtipo es `ha`) para restablecer las sesiones de copia de reserva de HA1 y HA1.

Los siguientes ejemplos muestran cómo configurar varios ajustes SSH para su HA1 después de habilitar el cifrado y acceder a la CLI. (Consulte Actualización de claves SSH y configuración de opciones de clave para la conexión de la interfaz de gestión para ver ejemplos de perfiles de servidor de gestión SSH).

Debe habilitar el cifrado, que debe funcionar correctamente en un par de HA para poder realizar las siguientes tareas.

Si pretende configurar el enlace de control de HA1 en el modo FIPS-CC, debe definir los parámetros para cambiar automáticamente las claves de las sesiones.

Para utilizar la misma configuración de conexión SSH para cada recopilador de logs dedicado (dispositivo virtual de M-Series o Panorama en modo de recopilador de logs) en un grupo de recopiladores, configure un perfil de servicio SSH desde el servidor de gestión Panorama, confirme los cambios en Panorama y, a continuación, envíe la configuración a los recopiladores de logs. Puede usar los comandos ***`set log-collector-group <name> general-setting management ssh`***.

- Cree un perfil de servicio SSH para ejercer un mayor control sobre las conexiones SSH entre sus cortafuegos de HA.

  Este ejemplo crea un perfil de HA sin configurar ninguna configuración.

  1. admin@PA-3250> **`configure`**
  2. admin@PA-3250# **`set deviceconfig system ssh profiles ha-profiles <name>`**
  3. admin@PA-3250# **`commit`**
  4. admin@PA-3250# **`exit`**
  5. Para verificar que se ha creado el nuevo perfil y ver la configuración de los perfiles existentes:

     admin@PA-3250> **`configure`**

     admin@PA-3250# **`show deviceconfig system ssh profiles`**

© 2020 Palo Alto Networks, Inc.

- (Opcional) Configure el servidor SSH para que use solo los métodos de cifrado especificados para las sesiones de HA1.

  De forma predeterminada, SSH HA1 permite todos los cifrados admitidos para el cifrado de sesiones de HA de la CLI. Mientras establece la conexión, el servidor SSH solo anuncia los cifrados que haya configurado. Si el cliente SSH (peer de HA) intenta conectarse con otro cifrado, el servidor finaliza la conexión.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles *<name>* ciphers *<cipher>***

     aes128-cbc: cifrado AES de 128 bits en modo CBC

     aes128-ctr: cifrado AES de 128 bits en modo CTR

     aes128-gcm: cifrado AES de 128 bits en modo GCM

     aes192-cbc: cifrado AES de 192 bits en modo CBC

     aes192-ctr: cifrado AES de 192 bits en modo CM

     aes256-cbc: cifrado AES de 256 bits en modo CBC

     aes256-ctr: cifrado AES de 256 bits en modo CM

     aes256-gcm: cifrado AES de 256 bits en modo GCM
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
  6. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

     Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los peers de HA. Si hay configurada una copia de seguridad de HA1, la opción force (forzar) no funciona.
  7. Para verificar que los cifrados se hayan actualizado:

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

- (Opcional) Configure el tipo predeterminado de clave de host.

  Si habilita el cifrado en el enlace de control de HA1, el cortafuegos utiliza RSA 2048 como tipo predeterminado de clave de host, a no ser que lo modifique. La conexión SSH de HA1 solo emplea ese `tipo de clave de host predeterminado` para autenticar los peers de HA antes de que establezcan la sesión cifrada entre ellos. Si decide cambiar el tipo predeterminado de clave de host, puede elegir entre ECDSA 256, 384 o 521 y RSA 2048, 3072 o 4096, Cambie el tipo de clave de host predeterminado si prefiere una clave RSA más larga o ECDSA en lugar de RSA. En este ejemplo se configura el tipo predeterminado en una clave ECDSA de 256 bits y se restablece la conexión de HA1 con ella sin reiniciar los peers de HA.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**

© 2020 Palo Alto Networks, Inc.

5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   Ya debe haber una conexión de HA establecida entre los cortafuegos de HA. De lo contrario, debe habilitar el cifrado en la conexión del enlace de control, exportar la clave de HA a una ubicación de la red e importarla al peer. Consulte Configuración de la HA activa/pasiva *o* Configuración de la HA activa/activa*.*
6. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
7. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

   Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***force (forzar)*** *no funciona.*
8. Para verificar que la clave de host se haya actualizado:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey**

- (Opcional) Elimine el cifrado del conjunto seleccionado para SSH por el enlace de control de HA1.

  En este ejemplo se elimina el cifrado AES en modo CBC con claves de 128 bits.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles *<name>* ciphers aes128-cbc**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
  6. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

     Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***force (forzar)*** *no funciona.*
  7. Para verificar que se haya eliminado el cifrado:

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* ciphers**

- (Opcional) Establezca los algoritmos de intercambio de claves de sesión que admitirá el servidor SSH HA1.

  De manera predeterminada, el servidor SSH (cortafuegos de HA) anuncia todos los algoritmos al cliente SSH (cortafuegos de peer de HA).

© 2020 Palo Alto Networks, Inc.

Si utiliza uno de los tipos de claves predeterminados de ECDSA, es recomendable aplicar un algoritmo de claves ECDH.

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles** ***<name>*** **kex** ***<value>***

   diffie-hellman-group14-sha1: grupo Diffie-Hellman 14 con hash SHA1

   ecdh-sha2-nistp256: Elliptic-Curve Diffie-Hellman por NIST P-256 con hash SHA2-256

   ecdh-sha2-nistp384: Elliptic-Curve Diffie-Hellman por NIST P-384 con hash SHA2-384

   ecdh-sha2-nistp521: Elliptic-Curve Diffie-Hellman por NIST P-521 con hash SHA2-521
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
6. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

   Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***force (forzar)*** *no funciona.*
7. Para verificar que se hayan actualizado los algoritmos de intercambio de claves:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- (Opcional) Establezca los códigos de autenticación de mensajes (MAC, Message Authentication Codes) que admitirá el servidor SSH HA1.

  De manera predeterminada, el servidor anuncia todos los algoritmos de MAC al cliente.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles** ***<name>*** **mac** ***<value>***

     hmac-sha1: MAC con hash criptográfico SHA1

     hmac-sha2-256: MAC con hash criptográfico SHA2-256

     hmac-sha2-512: MAC con hash criptográfico SHA2-512
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
  6. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

     Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***force (forzar)*** *no funciona.*
  7. Para verificar que se hayan actualizado los algoritmos MAC:

© 2020 Palo Alto Networks, Inc.

admin@PA-3250> **configure**

admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- (Opcional) Vuelva a generar las claves de host ECDSA o RSA para SSH de HA1 con el fin de sustituir las claves existentes y usarlas para restablecer las sesiones de HA1 entre los peers de HA sin reiniciarlos.

  Los peers de HA emplean las claves de host para autenticarse entre sí. En este ejemplo se vuelve a generar la clave de host predeterminada ECDSA 256.

  Cuando se vuelve a generar la clave de host, no varía el tipo predeterminado. Si desea volver a generar la clave de host predeterminada, debe especificar el tipo predeterminado y la longitud. Si se genera una clave de host que no es del tipo predeterminado, solo se crea una clave que no funciona.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

     Ya debe haber una conexión de HA establecida entre los cortafuegos de HA. De lo contrario, debe habilitar el cifrado en la conexión del enlace de control, exportar la clave de HA a una ubicación de la red e importarla al peer. Consulte Configuración de la HA activa/pasiva *o* Configuración de la HA activa/activa.
  6. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
  7. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

     Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción ***force (forzar)*** *no funciona.*

- (Opcional) Establezca parámetros de regeneración de claves para fijar cuándo se cambian automáticamente las claves de las sesiones en SSH por el enlace de control de HA1.

  Esas claves de sesión sirven para cifrar el tráfico entre los peers de HA. Los parámetros que puede configurar son el volumen de datos (en megabytes), el intervalo de tiempo (segundos) y el recuento de paquetes. Una vez que un parámetro de reintroducción de claves alcanza su valor configurado, SSH inicia un intercambio de claves.

  Resulta útil configurar un parámetro o dos más cuando no sabe con certeza si el primero alcanzará el valor con la rapidez que le interesa cambiar las claves. El primer parámetro en alcanzar su valor configurado solicitará una nueva clave. Después, el cortafuegos restablecerá todos los parámetros de reintroducción.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey data 32**

© 2020 Palo Alto Networks, Inc.

Después de cada cambio de claves, se vuelven a cambiar cuando se transmite el volumen de datos (megabytes) indicado. El predeterminado se basa en el cifrado empleado y oscila entre 1 y 4 GB; el intervalo es de 10 a 4000 MB. También puede especificar el comando **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey data default**, que define el parámetro data (datos) en el valor predeterminado del cifrado que utiliza.

3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey interval 3600**

   Después de cada cambio de claves, se vuelven a cambiar cuando transcurre el intervalo especificado en segundos. El cambio de claves por tiempo está deshabilitado (configurado en none [ninguno]) de forma predeterminada. El intervalo es de 10 a 3600.
4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets 27**

   Después de cada cambio de claves, se vuelven a cambiar cuando se transmite el número de paquetes definido (2^n). Por ejemplo, 14 establece que se transmita un máximo de 2^{14} paquetes antes de que se genere una nueva clave. El valor predeterminado es 2^{28}. El intervalo es de 12 a 27 (de 2^{12} a 2^{27}). También puede especificar **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets default**, que establece el parámetro de paquetes en 2^{28}.

   Elija los parámetros de cambio de claves en función del tipo de tráfico y la velocidad de la red, así como los requisitos de FIPS-CC, si es su caso. No configure parámetros tan bajos que perjudiquen el rendimiento de SSH.
5. admin@PA-3250# **commit**
6. admin@PA-3250# **exit**
7. (HA1 Backup is configured) admin@PA-3250> **request high-availability session-reestablish**
8. (Ninguna copia de seguridad de HA1 configurada o enlace de copia de seguridad de HA1 no disponible) admin@PA-3250> **request high-availability session-reestablish force**

   *Puede forzar que el cortafuegos restablezca las sesiones de HA1 si no hay ninguna copia de seguridad de HA1, lo que provoca una breve situación de división entre los dos peers de HA. Si hay configurada una copia de seguridad de HA1, la opción **force (forzar)** no funciona.*
9. Para verificar los cambios:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* session-rekey**

- Active el perfil. Para ello, selecciónelo y reiniciando el servicio SSH HA1.
  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile *<name>***
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **set ssh service-restart ha**
  6. Para verificar que se está utilizando el perfil correcto:

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh ha**

© 2020 Palo Alto Networks, Inc.

Estados del cortafuegos HA

Un cortafuegos de HA puede tener uno de los siguientes estados:

Estado del cortafuegos HA	Se produce en	Description (Descripción)
Inicial	A/P o A/A	Estado transitorio de un cortafuegos cuando se une al par de HA. El cortafuegos permanece en este estado tras el arranque hasta que descubre a un peer y las negociaciones comienzan. Luego del tiempo de espera, el cortafuegos se vuelve activo si la negociación de HA no ha iniciado.
Activo	A/P	Estado del cortafuegos activo en una configuración activa/pasiva.
Pasivo	A/P	Estado del cortafuegos pasivo en una configuración activa/pasiva. El cortafuegos pasivo está listo para convertirse en un cortafuegos activo sin interrupciones en la red. A pesar de que el cortafuegos pasivo no procesa otro tráfico: • Si se configura el modo automático del estado de enlace pasivo, el cortafuegos pasivo ejecuta protocolos de enrutamiento, supervisa el estado del enlace y la ruta, y el cortafuegos pasivo negociará previamente los paquetes LACP y LLDP si se configuran los paquetes de negociación previa LACP y LLDP, respectivamente. • El cortafuegos pasivo sincroniza el estado del flujo, los objetos del tiempo de ejecución y la configuración. • El cortafuegos pasivo supervisa el estado del cortafuegos activo utilizando el protocolo de saludo.
Activo/principal	A/A	En una configuración activa/activa, el estado del cortafuegos durante el cual este realiza la conexión con los agentes de User-ID, ejecuta el servidor DHCP y la transmisión DHCP, y encuentra coincidencias entre reglas NAT y PBF con la ID del dispositivo del cortafuegos activo-principal. Un cortafuegos en este estado puede poseer sesiones y configurar sesiones.
activa-secundaria	A/A	En una configuración activa/activa, el estado del cortafuegos durante el cual este se conecta a los agentes de User-ID, ejecuta el servidor DHCP y encuentra coincidencias entre reglas NAT y PBF con la ID del dispositivo del cortafuegos activo-secundario. Un cortafuegos en estado activo-secundario no admite transmisión DHCP. Un cortafuegos en este estado puede poseer sesiones y configurar sesiones.
Provisional	A/A	Estado de un cortafuegos (en una configuración activa/activa) provocado por una de las siguientes condiciones: • Fallo de un cortafuegos. • Fallo de un objeto supervisado (un enlace o una ruta). • El cortafuegos permanece suspendido o en estado no funcional. Un cortafuegos en estado provisional sincroniza sesiones y configuraciones del peer.

© 2020 Palo Alto Networks, Inc.

Estado del cortafuegos HA	Se produce en	Description (Descripción)
		• En una implementación de cable virtual, cuando un cortafuegos ingresa a un estado provisional debido a un fallo de ruta y recibe un paquete para reenviar, envía el paquete al cortafuegos del peer mediante el enlace HA3 para su procesamiento. El cortafuegos del peer procesa el paquete y lo devuelve al enlace HA3 hacia el cortafuegos para que se envíe a la interfaz de salida. Este comportamiento conserva la ruta de reenvío en una implementación de cable virtual. • En una implementación de capa 3, cuando un cortafuegos en estado provisional recibe un paquete, envía ese paquete mediante el enlace HA3 para que el cortafuegos del peer posea o configure la sesión. Según la topología de red, el cortafuegos envía el paquete al destino o lo envía al peer en estado provisional para su reenvío. Una vez que la ruta o enlace fallido se borra o a medida que el cortafuegos fallido pasa de un estado provisional a un estado activo-secundario, se activa el **Tentative Hold Time (Tiempo de espera provisional)** y se produce la convergencia del enrutamiento. El cortafuegos intenta crear adyacencias de enrutamiento y completar su tabla de ruta antes de procesar los paquetes. Sin este temporizador, el cortafuegos de recuperación entraría en estado activo-secundario inmediatamente y descartaría de manera silenciosa los paquetes, ya que carecería de las rutas necesarias. Cuando un cortafuegos abandona el estado suspendido, pasa a estado provisional durante el **Tentative Hold Time (Tiempo de espera provisional)** luego de que los enlaces funcionen y puedan procesar los paquetes entrantes. Es posible deshabilitar el **Tentative Hold Time range (Intervalo de tiempo de espera provisional) (s)** (que es de 0 segundos) o dentro del intervalo entre 10 y 600 s; el valor predeterminado es de 60 s.
No funcional	A/P o A/A	Estado de error debido a un fallo en el plano de datos o una falta de coincidencia en la configuración, como un solo cortafuegos configurado para el reenvío de paquetes, la sincronización de VR o la sincronización de QoS. En modo activo/pasivo, todas las causas que se enumeran para el estado provisional causan un estado no funcional.
Suspendido	A/P o A/A	Dispositivo deshabilitado, de modo que no transmite tráfico de datos. Aunque se sigan estableciendo comunicaciones de HA, el dispositivo no participa en el proceso de elección de HA. No puede pasar al estado funcional de HA sin que intervenga el usuario.

© 2020 Palo Alto Networks, Inc.

Referencia: Sincronización HA

Si ha habilitado la sincronización de configuración en ambos peers en un par HA, la mayoría de ajustes de la configuración que establezca en un peer se sincronizará automáticamente en el otro peer al compilar. Para evitar conflictos de configuración, haga siempre cambios de configuración en el peer activo (activo/pasivo) o activo principal (activo/activo) y espere a que los cambios se sincronicen en el peer antes de hacer cualquier cambio de configuración adicional.

Solo las configuraciones confirmadas se sincronizan entre los peers HA. Las confirmaciones en la cola de confirmación en el momento de la sincronización HA no se sincronizarán.

Los siguientes temas identifican qué ajustes de configuración debe establecer en cada cortafuegos de manera independiente (estos ajustes no están sincronizados del peer HA).

- ¿Qué ajustes no se sincronizan en HA Activo/pasivo?
- ¿Qué ajustes no se sincronizan en HA Activo/activo?
- Sincronización de información de tiempos de ejecución del sistema

¿Qué ajustes no se sincronizan en HA Activo/pasivo?

Debe configurar los siguientes ajustes en cada cortafuegos en un par HA en una implementación activo/pasivo. Estos ajustes no se sincronizan de un peer a otro.

Elemento de configuración	¿Qué no se sincroniza en Activo/pasivo?
Configuración de interfaz de gestión	Todos los ajustes de la configuración de gestión deben realizarse individualmente en cada dispositivo, incluidos los siguientes: • **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**: nombre de host, dominio, banner de inicio de sesión, perfil de servicio SSL/TLS (y certificados asociados), zona horaria, configuración regional, fecha, hora, latitud y longitud. • **Device (Dispositivos)** > **Setup (Configuración)** > **Management (Gestión)** > **Management Interface Settings (Configuración de interfaz de gestión):** tipo de IP, dirección IP, máscara de red, puerta de enlace predeterminada, dirección IPv6/longitud de prefijo, puerta de enlace IPv6 predeterminada, velocidad, MTU y servicios (HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, SSL de escucha de Syslog de User-ID, UDP de escucha de Syslog de User-ID).
Capacidad de vsys múltiples	Debe activar la licencia de Virtual Systems en los dos cortafuegos del par a fin de utilizar más sistemas virtuales de los permitidos de manera predeterminada con los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series. Asimismo, debe habilitar **Multi Virtual System Capability (Capacidad para múltiples sistemas virtuales)** en cada cortafuegos (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**).

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en Activo/pasivo?
Ajustes de Panorama	Defina los siguientes ajustes de Panorama en cada cortafuegos (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** > **Panorama Settings [Ajustes de panorama]**). • **Servidores de Panorama** • **Disable Panorama Policy and Objects (Deshabilitar política y objetos de Panorama)** y **Disable Device and Network Template (Deshabilitar plantilla de dispositivo y red)**.
SNMP	Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
Services	**Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
Rutas de servicio globales	**Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de la ruta de servicios)**
Ajustes de telemetría e inteligencia contra amenazas	**Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry and Threat Intelligence (Telemetría e inteligencia contra amenazas)**
Protección de datos	**Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** > **Manage Data Protection (Protección de datos de gestión)**
Tramas gigantes	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Ajustes de sesión)** > **Enable Jumbo Frame (Habilitar trama gigante)**
Protección de búfer de paquetes	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)** > **Packet Buffer Protection (Protección del búfer de paquetes)** **Network (Red)** > **Zones (Zonas)** > **Enable Packet Buffer Protection (Habilitar protección de búfer de paquetes)**
Reenvío de los ajustes de certificados del servidor proxy	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Ajustes de descifrado)** > **SSL Forward Proxy Settings (Ajustes de proxy de reenvío SSL)**
Clave maestra asegurada por HSM	**Device (Dispositivo)** > **Setup (Configuración)** > **HSM** > **Hardware Security Module Provider (Proveedor de módulo de seguridad de hardware)** > **Master Key Secured by HSM (Clave maestra asegurada por HSM)**
Configuración de exportación de logs	**Device (Dispositivo)** > **Scheduled Log Export (Programación de la exportación de logs)**
Actualizaciones de software	En el caso de actualizaciones de software, puede descargarlas e instalarlas por separado en cada dispositivo o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe instalar la actualización en cada peer (**Device [Dispositivo]** > **Software**).

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en Activo/pasivo?
Paquete de agente de GlobalProtect	En el caso de actualizaciones de aplicaciones de GlobalProtect, puede descargarlas e instalarlas por separado en cada cortafuegos, o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe activarlas por separado en cada peer (**Device [Dispositivo]** > **GlobalProtect Client [Cliente de GlobalProtect]**).
Actualizaciones de contenido	En el caso de actualizaciones de contenido, puede descargarlas e instalarlas por separado en cada cortafuegos o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe instalar la actualización en cada peer (**Device [Dispositivo]** > **Dynamic Updates [Actualizaciones dinámicas]**).
Licencias/Suscripciones	**Device (Dispositivo)** > **Licenses (Licencias)**
Suscripción de asistencia	**Device (Dispositivo)** > **Support (Asistencia técnica)**
Clave maestra	La clave maestra debe ser idéntica en cada cortafuegos en el par HA, pero debe introducirla manualmente en cada cortafuegos (**Device [Dispositivo]** > **Master Key and Diagnostics [Clave maestra y diagnóstico]**). Antes de cambiar la clave maestra, debe deshabilitar la sincronización de configuración en ambos peers (**Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **General** > **Setup [Configuración]** y desmarcar la casilla de verificación **Enable Config Sync [Habilitar sincronización de configuración]**) y volver a habilitarla tras cambiar las claves.
Informes, logs y Configuración de panel	Datos de log, Informes y Datos y configuración de panel (visualización de columnas, widgets) no se sincronizan entre peers. En cambio, los ajustes de configuración de informes sí se actualizan.
Configuración de HA	**Device (Dispositivo)** > **High Availability (Alta disponibilidad)**
Rule Usage Data (Datos de uso de reglas)	Los datos de uso de las reglas, como recuento de resultados, fecha de creación y fecha de modificación, no se sincronizan entre los peers. Debe iniciar sesión en cada uno de los cortafuegos para ver su respectivo recuento de resultados de las reglas de las políticas o bien usar Panorama para ver la información sobre los peers de los cortafuegos de HA.
Certificados para la gestión de dispositivos y la comunicación de syslog solo a través de SSL	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** Los certificados utilizados para la gestión de dispositivos o para la comunicación de syslog a través de SSL no se sincronizan con un peer de HA.
Certificados en un perfil de certificado	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**
Perfil de servicio SSL/TLS solo para la gestión de dispositivos	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en Activo/pasivo?
	El perfil de servicio SSL/TLS para la gestión de dispositivos no se sincroniza con un peer de HA.
Device-ID y IoT Security (Seguridad de IoT)	Las asignaciones de dirección IP a dispositivo y las recomendaciones de reglas de políticas no se sincronizan con un peer de HA.

¿Qué ajustes no se sincronizan en HA Activo/activo?

Debe configurar los siguientes ajustes en cada cortafuegos en un par HA en una implementación activo/activo. Estos ajustes no se sincronizan de un peer a otro.

Elemento de configuración	¿Qué no se sincroniza en activo/activo?
Configuración de interfaz de gestión	Debe configurar todos los ajustes de gestión individualmente en cada cortafuegos, incluido lo siguiente: • **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**: nombre de host, dominio, banner de inicio de sesión, perfil de servicio SSL/TLS (y certificados asociados), zona horaria, configuración regional, fecha, hora, latitud y longitud. • **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Management Interface Settings (Ajustes de la interfaz de gestión)**: dirección IP, máscara de red, puerta de enlace predeterminada, dirección IPv6/longitud de prefijo, puerta de enlace IPv6 predeterminada, velocidad, MTU y servicios (HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, SSL de escucha de Syslog de User-ID, UDP de escucha de Syslog de User-ID).
Capacidad de vsys múltiples	Debe activar la licencia de Virtual Systems en los dos cortafuegos del par a fin de utilizar más sistemas virtuales de los permitidos de manera predeterminada con los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series. Asimismo, debe habilitar **Multi Virtual System Capability (Capacidad para múltiples sistemas virtuales)** en cada cortafuegos (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**).
Ajustes de Panorama	Defina los siguientes ajustes de Panorama en cada cortafuegos (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** > **Panorama Settings [Ajustes de panorama]**). • **Servidores de Panorama** • **Disable Panorama Policy and Objects (Deshabilitar política y objetos de Panorama)** y **Disable Device and Network Template (Deshabilitar plantilla de dispositivo y red)**.

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en activo/activo?
SNMP	Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
Services	**Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
Rutas de servicio globales	**Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de la ruta de servicios)**
Ajustes de telemetría e inteligencia contra amenazas	**Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry and Threat Intelligence (Telemetría e inteligencia contra amenazas)**
Protección de datos	**Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** > **Manage Data Protection (Protección de datos de gestión)**
Tramas gigantes	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Ajustes de sesión)** > **Enable Jumbo Frame (Habilitar trama gigante)**
Protección de búfer de paquetes	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)** > **Packet Buffer Protection (Protección del búfer de paquetes)** **Network (Red)** > **Zones (Zonas)** > **Enable Packet Buffer Protection (Habilitar protección de búfer de paquetes)**
Reenvío de los ajustes de certificados del servidor proxy	**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Ajustes de descifrado)** > **SSL Forward Proxy Settings (Ajustes de proxy de reenvío SSL)**
Configuración del HSM.	**Device (Dispositivo)** > **Setup (Configuración)** > **HSM**
Configuración de exportación de logs	**Device (Dispositivo)** > **Scheduled Log Export (Programación de la exportación de logs)**
Actualizaciones de software	En el caso de actualizaciones de software, puede descargarlas e instalarlas por separado en cada dispositivo o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe instalar la actualización en cada peer (**Device [Dispositivo]** > **Software**).
Paquete de agente de GlobalProtect	En el caso de actualizaciones de aplicaciones de GlobalProtect, puede descargarlas e instalarlas por separado en cada cortafuegos, o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe activarlas por separado en cada peer (**Device [Dispositivo]** > **GlobalProtect Client [Cliente de GlobalProtect]**).
Actualizaciones de contenido	En el caso de actualizaciones de contenido, puede descargarlas e instalarlas por separado en cada cortafuegos o descargarlas en un peer y sincronizar la actualización en el otro peer. Debe instalar la actualización en cada peer (**Device [Dispositivo]** > **Dynamic Updates [Actualizaciones dinámicas]**).
Licencias/Suscripciones	**Device (Dispositivo)** > **Licenses (Licencias)**

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en activo/activo?
Suscripción de asistencia	**Device (Dispositivo)** > **Support (Asistencia técnica)**
Dirección IP de interfaz Ethernet	Todos los ajustes de configuración de la interfaz Ethernet se sincronizan, excepto la dirección IP (**Network [Red]** > **Interface [Interfaz]** > **Ethernet**).
Direcciones IP de interfaz de loopback	Todos los ajustes de configuración de la interfaz de bucle invertido se sincronizan, excepto la dirección IP (**Network [Red]** > **Interface** > **Loopback [Bucle invertido]**).
Direcciones IP de interfaz de túnel	Todos los ajustes de configuración de la interfaz de túnel se sincronizan, excepto la dirección IP (**Network [Red]** > **Interface [Interfaz]** > **Tunnel [Túnel]**).
Prioridad del sistema LACP	Cada peer debe tener un único ID de sistema LACP en una implementación activa/activa (**Network [Red]** > **Interface [Interfaz]** > **Ethernet** > **Add Aggregate Group [Añadir grupo de agregación]** > **System Priority [Prioridad del sistema]**)
Dirección IP de interfaz de VLAN	Todos los ajustes de configuración de la interfaz VLAN se sincronizan, excepto la dirección IP (**Network [Red]** > **Interface [Interfaz]** > **VLAN**).
Enrutadores virtuales	La configuración del enrutador virtual se sincroniza solo si ha habilitado la sincronización de VR (**Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **Active/Active Config [Configuración activa/activa]** > **Packet Forwarding [Reenvío de paquetes]**). La necesidad de hacer esto o no viene determinada por el diseño de su red, incluido el hecho de que tenga o no enrutamiento asimétrico.
Túneles IPSec	La sincronización de la configuración del túnel IPSec depende de si ha configurado las direcciones virtuales para usar direcciones IP flotantes (**Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **Active/Active Config [Configuración activa/activa]** > **Virtual Address [Dirección virtual]**). Si ha configurado una dirección IP flotante, estos ajustes se sincronizan automáticamente. De lo contrario, debe configurar esos ajustes independientemente en cada peer.
Configuración de portal de GlobalProtect	La sincronización de la configuración del portal de GlobalProtect depende de si ha configurado las direcciones virtuales para usar direcciones IP flotantes (**Network [Red]** > **GlobalProtect** > **Portals [Portales]**). Si ha configurado una dirección IP flotante, los ajustes de configuración del portal de GlobalProtect se sincronizan automáticamente. De lo contrario, debe configurar los ajustes de este portal independientemente en cada peer.
Configuración del gateway de GlobalProtect	La sincronización de configuración de la puerta de enlace de GlobalProtect depende de si ha configurado las direcciones virtuales para usar direcciones IP flotantes (**Network [Red]** > **GlobalProtect** > **Gateways [Puertas de enlace]**). Si ha configurado una dirección IP flotante, los ajustes de configuración del gateway de GlobalProtect se sincronizan automáticamente. De lo contrario, debe configurar los ajustes del gateway independientemente en cada peer.

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en activo/activo?
QoS	La configuración de QoS se sincroniza solo si ha habilitado **QoS Sync** (**Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **Active/Active Config [Configuración activa/activa]** > **Packet Forwarding [Reenvío de paquetes]**). Puede elegir no sincronizar la QoS si, por ejemplo, tiene un ancho de banda distinto en cada enlace o diferentes latencias en sus proveedores de servicio.
LLDP	En una configuración activa/activa, los datos de cortafuegos individuales o de estado de LLDP no se sincronizan (**Network [Red]** > **Network Profiles [Perfiles de red]** > **LLDP**).
BFD	En una configuración activa/activa, los datos de sesión BFD o de configuración de BFD no se sincronizan (**Network [Red]** > **Network Profiles [Perfiles de red]** > **BFD Profile [Perfil BFD]**).
Puertas de enlace de IKE	La sincronización de configuración de la puerta de enlace de IKE depende de si ha configurado las direcciones virtuales para usar direcciones IP flotantes (**Network [Red]** > **IKE Gateways [Puertas de enlace de IKE]**). Si ha configurado una dirección IP flotante, los ajustes de configuración del gateway de IKE se sincronizan automáticamente. De lo contrario, debe configurar los ajustes del gateway de IKE independientemente en cada peer.
Clave maestra	La clave maestra debe ser idéntica en cada cortafuegos en el par HA, pero debe introducirla manualmente en cada cortafuegos (**Device [Dispositivo]** > **Master Key and Diagnostics [Clave maestra y diagnóstico]**). Antes de cambiar la clave maestra, debe deshabilitar la sincronización de configuración en ambos peers (**Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **General** > **Setup [Configuración]** y desmarcar la casilla de verificación **Enable Config Sync [Habilitar sincronización de configuración]**) y volver a habilitarla tras cambiar las claves.
Informes, logs y Configuración de panel	Los datos de logs, los informes, y los datos y la configuración del panel (visualización de columnas, widgets) no se sincronizan entre peers. En cambio, los ajustes de configuración de informes sí se actualizan.
Configuración de HA	• **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** • (La excepción es **Device [Dispositivo]** > **High Availability [Alta disponibilidad]** > **Active/Active Configuration [Configuración activa/activa]** > **Virtual Addresses [Direcciones virtuales]** que sí se sincroniza).
Rule Usage Data (Datos de uso de reglas)	Los datos de uso de las reglas, como recuento de resultados, fecha de creación y fecha de modificación, no se sincronizan entre los peers. Debe iniciar sesión en cada uno de los cortafuegos para ver su respectivo recuento de resultados de las reglas de las políticas o bien usar Panorama para ver la información sobre los peers de los cortafuegos de HA.
Certificados para la gestión de dispositivos y la comunicación de syslog solo a través de SSL	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** Los certificados utilizados para la gestión de dispositivos o para la comunicación de syslog a través de SSL no se sincronizan con un peer de HA.

© 2020 Palo Alto Networks, Inc.

Elemento de configuración	¿Qué no se sincroniza en activo/activo?
Certificados en un perfil de certificado	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**
Perfil de servicio SSL/TLS solo para la gestión de dispositivos	**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** El perfil de servicio SSL/TLS para la gestión de dispositivos no se sincroniza con un peer de HA.
Device-ID y IoT Security (Seguridad de IoT)	Las asignaciones de dirección IP a dispositivo y las recomendaciones de reglas de políticas no se sincronizan con un peer de HA.

Sincronización de información de tiempos de ejecución del sistema

La siguiente tabla resume la información de tiempo de ejecución del sistema sincronizada entre los peer de HA.

Información de tiempo de ejecución	¿Configuración sincronizada?		Enlace de HA	Detalles
	A/P	A/A		
Plano de administración				
Asignaciones de usuario a grupo	yes (sí)	yes (sí)	HA1	
Asignaciones de usuarios entre sistemas virtuales	yes (sí)	yes (sí)	HA1	
Asignaciones de usuario a dirección IP	yes (sí)	yes (sí)	HA1	
Concesiones DHCP (como servidor)	yes (sí)	yes (sí)	HA1	Si no coinciden las versiones de PAN-OS de los peers de HA, no se sincroniza la información de configuración de concesiones DHCP (como servidor).
Caché de DNS	No	No	n/c	
Actualización de FQDN	No	No	n/c	
Claves de IKE (fase 2)	yes (sí)	yes (sí)	HA1	

© 2020 Palo Alto Networks, Inc.

Información de tiempo de ejecución	¿Configuración sincronizada?		Enlace de HA	Detalles
	A/P	A/A		
Base de información de reenvío (FIB)	yes (sí)	yes (sí)	HA1	
Caché de URL de PAN-DB	yes (sí)	No	HA1	Se sincroniza durante el backup de la base de datos al disco (cada ocho horas, cuando se actualiza la versión de la base de datos de URL) o cuando se reinicia el cortafuegos.
Contenido (sincronización manual)	yes (sí)	yes (sí)	HA1	
PPPoE, concesión de PPPoE	yes (sí)	yes (sí)	HA1	
Configuración y concesión de cliente DHCP	yes (sí)	yes (sí)	HA1	Si no coinciden las versiones de PAN-OS de los peers de HA, no se sincronizan la configuración de clientes DHCP ni la información de configuración de concesiones.
Lista de usuarios que han iniciado sesión en SSL VPN	yes (sí)	yes (sí)	HA1	
Plano de datos				
Tabla de sesiones	yes (sí)	yes (sí)	HA2	• Los peers activos/pasivos no sincronizan ICMP ni la información de sesión del host. • Los peers activos/activos no sincronizan información de sesiones de host, sesiones de multidifusión ni sesiones BFD. *Una sesión de host es una sesión que finaliza en una*

© 2020 Palo Alto Networks, Inc.

Información de tiempo de ejecución	¿Configuración sincronizada?		Enlace de HA	Detalles
	A/P	A/A		
				de las interfaces del cortafuegos, como una sesión ICMP que hace ping en una de las interfaces del cortafuegos o un túnel GP.
Tabla de ARP	yes (sí)	No	HA2	
Tabla de detección de vecinos (ND)	yes (sí)	No	HA2	
Tabla MAC	yes (sí)	No	HA2	
Número de secuencia de IPSec (antirreproducción)	yes (sí)	yes (sí)	HA2	
Entradas de la lista de bloqueo de DoS	No	No	n/c	
MAC virtual	yes (sí)	yes (sí)	HA2	
Asociaciones de SCTP	yes (sí)	No	HA2	

Monitorización

Para prevenir posibles inconvenientes y para acelerar la respuesta ante incidentes cuando se necesite, el cortafuegos ofrece inteligencia sobre patrones de tráfico y usuario usando informes personalizables e informativos. El panel, el Centro de control de aplicaciones (ACC), los informes y los logs del cortafuegos le permiten monitorizar la actividad de su red. Puede monitorizar los logs y filtrar la información para generar informes con vistas predefinidas o personalizadas. Por ejemplo, puede usar las plantillas predefinidas para generar informes sobre las actividades del usuario o analizar los informes y logs para interpretar comportamientos inusuales en la red, y generar un informe personalizado sobre el patrón de tráfico. Para lograr una presentación visualmente atractiva de la actividad de la red, el panel y ACC incluyen widgets, gráficos y tables con los cuales puede interactuar para encontrar la información que necesita. Además, puede configurar el cortafuegos para enviar información monitorizada como notificaciones de correo electrónico, mensajes de syslog, capturas de SNMP y registros NetFlow para servicios externos.

- Uso del panel
- Uso del Centro de control de aplicaciones
- Uso de los informes de App Scope
- Use el motor de correlación automatizada.
- Realización de capturas de paquetes
- Supervisión de aplicaciones y amenazas
- Visualización y gestión de logs
- Supervisión de la lista de bloqueo
- Visualización y gestión de informes
- Visualización de la utilización de las reglas de la política
- Uso de servicios externos para la monitorización
- Configuración de reenvío de logs
- Configuración de alertas de correo electrónico
- Uso de syslog para la monitorización
- Monitorización de SNMP y capturas
- Reenvío de logs a un destino de HTTP
- Monitorización de NetFlow

© 2020 Palo Alto Networks, Inc.

Uso del panel

Los widgets de la pestaña **Dashboard (Panel)** muestran información general del cortafuegos, como la versión de software, el estado operativo de cada interfaz, la utilización de recursos y hasta 10 de las entradas más recientes en los logs de sistema, configuración y amenazas. Todos los widgets disponibles aparecen de forma predeterminada, pero cada administrador puede eliminar y agregar widgets individuales según sea necesario. Haga clic en el icono de actualización para actualizar el panel o un widget individual. Para cambiar el intervalo de actualización automática, seleccione un intervalo del menú desplegable (**1 min**, **2 min**, **5 min** o **Manual**). Para agregar un widget al panel, haga clic en la lista desplegable Widget, seleccione una categoría y luego el nombre del widget. Para eliminar un widget, haga clic en en la barra de títulos. La siguiente tabla describe los widgets del panel.

Gráficos del panel	Descripciones
Aplicaciones principales	Muestra las aplicaciones con la mayoría de sesiones. El tamaño del bloque indica el número relativo de sesiones (pase el ratón sobre el bloque para ver el número) y el color indica el riesgo de seguridad, desde verde (más bajo) a rojo (más alto). Haga clic en una aplicación para ver su perfil de aplicación.
Principales aplicaciones de alto riesgo	Similar a Aplicaciones principales, excepto las que muestran las aplicaciones de mayor riesgo con la mayoría de las sesiones.
Información general	Muestra el nombre del cortafuegos, el modelo, la versión del software de PAN-OS, la aplicación, las amenazas, las versiones de definición del filtro de URL, la fecha y hora actuales y el período transcurrido desde el último reinicio.
Estado de interfaz	Indica si cada interfaz está activa (verde), no está operativa (rojo) o en un estado desconocido (gris).
Logs de amenazas	Muestra el ID de amenaza, la aplicación y la fecha y hora de las 10 últimas entradas en el log Amenazas. El ID de amenaza es una descripción malintencionada una URL que incumple el perfil de filtro de URL.
Logs de configuración	Muestra el nombre de usuario del administrador, el cliente (Web o CLI) y la fecha y hora de las 10 últimas entradas en el log Configuración.
Logs Filtrado de datos	Muestra la descripción y la fecha y hora de los últimos 60 minutos en el log Filtrado de datos.
Registros de filtrado de URL	Muestra la descripción y la fecha y hora de los últimos 60 minutos en el log Filtrado de URL.
Logs del sistema	Muestra la descripción y la fecha y hora de las últimos 10 entradas en el log Sistema. *Una entrada **`Config installed`** indica que se han llevado a cabo cambios en la configuración correctamente.*

© 2020 Palo Alto Networks, Inc.

Gráficos del panel	Descripciones
Recursos del sistema	Muestra el uso de CPU de gestión, el uso de plano de datos y el Número de sesiones que muestra el número de sesiones establecidas a través del cortafuegos.
Administradores registrados	Muestra la dirección IP de origen, el tipo de sesión (Web o CLI) y la hora de inicio de sesión para cada administrador actualmente registrado.
Factor de riesgo de ACC	Muestra el factor de riesgo medio (1 a 5) para el tráfico de red procesado la semana pasada. Los valores mayores indican un mayor riesgo.
High Availability	Si la alta disponibilidad (high availability, HA) está habilitada, indica el estado de HA del dispositivo local y del peer: verde (activo), amarillo (pasivo) o negro (otro). Para obtener más información sobre HA, consulte High Availability.
Bloqueos	Muestra bloqueos de configuración realizados por los administradores.

© 2020 Palo Alto Networks, Inc.

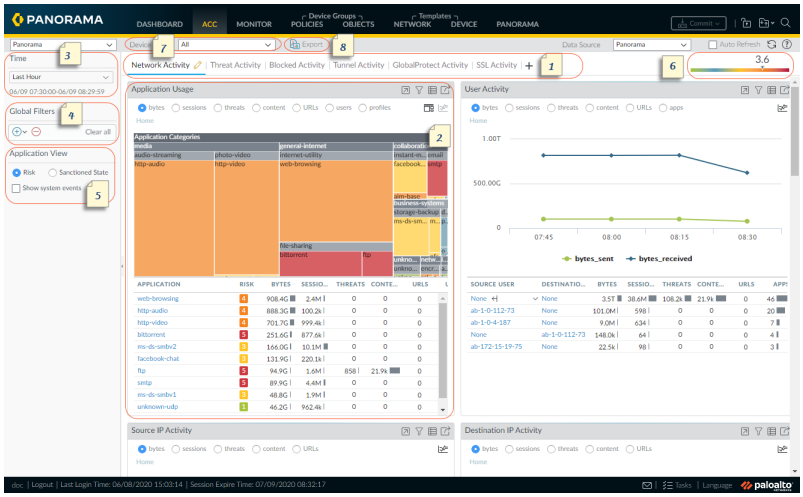
Uso del Centro de control de aplicaciones

El centro de control de aplicaciones (ACC) es un resumen interactivo, y gráfico de las aplicaciones, usuarios, URL, amenazas y contenido que atraviesa su red. El ACC usa los logs del cortafuegos para ofrecer visibilidad de los patrones de tráfico y la información aplicable sobre las amenazas. El diseño del ACC incluye una vista con pestañas de la actividad de la red, la actividad las amenazas y la actividad bloqueada, y cada una de ellas incluye widgets adecuados para una mejor visualización del tráfico de la red. La representación gráfica le permite interactuar con los datos y visualizar las relaciones entre eventos en la red para que pueda detectar anomalías o averiguar formas de mejorar sus reglas de seguridad de red. Para tener una vista personalizada de su red, también puede añadir una pestaña personalizada e incluir widgets que le permitan desglosar la información que le resulte más importante.

- ACC: primer vistazo
- Pestañas de ACC
- Widgets de ACC (Descripciones de widget)
- Filtros de ACC
- Interacción con el ACC
- Caso de uso: ACC: Ruta de descubrimiento de información

ACC: primer vistazo

Ahora vamos a conocer la ACC.



ACC: primer vistazo		
1	**Pestañas**	El ACC incluye tres pestañas predefinidas que ofrecen visibilidad sobre el tráfico de red, la actividad de las amenazas y la actividad bloqueada. Si desea más información sobre cada pestaña, consulte Pestañas de ACC.
2	**Widgets**	Cada pestaña incluye un conjunto predeterminado de widgets que representan mejor los eventos y tendencias asociados a la pestaña. Los widgets le permiten estudiar los datos usando los siguientes filtros:

© 2020 Palo Alto Networks, Inc.

ACC: primer vistazo		
		• bytes (entrada y salida) • sesiones • contenido (archivos y datos) • Categorías de URL • amenazas (y recuentos) Si desea más información sobre cada pestaña, consulte Widgets de ACC.
	**Time**	Los gráficos de cada widget ofrecen una vista de resumen y datos anteriores. Puede elegir un intervalo personalizado o usar los periodos predefinidos que van desde 15 minutos hasta los últimos 90 días o los últimos 30 días naturales. El período de tiempo seleccionado se aplica a todas las pestañas del ACC. El período de tiempo usado para mostrar los datos, por defecto, es el valor **Last Hour** actualizado en intervalos de 15 minutos. El intervalo de fecha y hora se muestran en pantalla, por ejemplo en 11:40, el intervalo de tiempo es 01/12 10:30:00-01/12 11:29:59.
	**Filtros globales**	Los filtros globales le permiten establecer el filtro en todas las pestañas y filtros. Los gráficos aplican los filtros seleccionados antes de representar los datos. Para obtener información sobre cómo utilizar los filtros, consulte Filtros de ACC.
	Vista de la aplicación	La vista de aplicación permite filtrar la vista de ACC por las aplicaciones sancionadas y no sancionadas en uso en la red o por el nivel de riesgo de las aplicaciones en uso en la red. El verde indica las aplicaciones sancionadas, el azul, las aplicaciones no sancionadas, y el amarillo indica las aplicaciones sancionadas parcialmente. Las aplicaciones sancionadas parcialmente son las que tienen un estado de sanción mixto; esto indica que la aplicación está etiquetada como aprobada de manera inconsistente, por ejemplo, es posible que se encuentre sancionada en uno o más sistemas virtuales en un cortafuegos habilitado para varios sistemas virtuales, o en uno o más cortafuegos dentro de un grupo de dispositivos en Panorama.
	**Factor de riesgo**	El factor de riesgo (1=más bajo; 5=más alto) indica el riesgo relativo según las aplicaciones usadas en su red. El factor de riesgos usa diversos factores para evaluar los niveles de riesgo asociados, como si la aplicación puede compartir archivos, tiende a un uso malintencionado o intenta evadir cortafuegos; también los factores de la actividad de amenazas y malware, como a través del número de amenazas bloqueadas, host en riesgo o tráfico hacia los hosts o dominios malintencionados.

© 2020 Palo Alto Networks, Inc.

ACC: primer vistazo		
7	**Source (Origen)**	Los datos que se utilizan en la visualización de ACC. Las opciones varían en el cortafuegos y en Panorama. En el cortafuegos, si está habilitado para varios sistemas virtuales, puede usar el menú desplegable **Virtual System (Sistema virtual)** para cambiar la visualización de ACC de modo que incluya todos los sistemas virtuales o solo un sistema virtual seleccionado. En Panorama, puede seleccionar el menú desplegable **Device Group (Grupo de dispositivos)** para cambiar la visualización de ACC de modo que incluya datos de todos los grupos de dispositivos o solo un grupo de dispositivos seleccionados. Además, en Panorama puede cambiar el **Data Source (Origen de datos)** como datos de **Panorama** o **Remote Device Data (Datos de dispositivo remoto)**. **Remote Device Data** solo está disponible cuando todos los cortafuegos gestionados tienen la versión PAN-OS 7.0.0 o posterior. Cuando filtra la visualización de un grupo de dispositivos específico, los datos de **Panorama** se usan como el origen de datos.
8	**Exportar**	Puede exportar los widgets que se muestran en la pestaña seleccionada actualmente como un PDF. El PDF se descarga y guarda en la carpeta de descargas asociadas con su navegador web en su ordenador.

Pestañas de ACC

El ACC incluye las siguientes pestañas predefinidas para visualizar la actividad de red, la actividad de las amenazas y la actividad bloqueada.

Pestaña	Description (Descripción)
Network Activity (Actividad de red)	Muestra una visualización general del tráfico y la actividad de los usuarios en su red, incluido: • Las aplicaciones principales en uso • Los usuarios que generan más tráfico (con una descripción pormenorizada de los bytes, contenido, amenazas o URL a las que ha accedido el usuario • Las reglas de seguridad más usadas con las que coincide el tráfico Asimismo, puede ver la actividad de la red según la zona de origen o destino, región o direcciones IP, por interfaces de acceso o salida y por información del host GlobalProtect, como los sistemas operativos de los dispositivos más usados en la red.
Threat Activity (Actividad de amenazas)	Muestra una descripción general de las amenazas, centrado en las principales amenazas: vulnerabilidades, spyware, virus, hosts que visitan dominios o URL malintencionados, principales envíos de WildFire

© 2020 Palo Alto Networks, Inc.

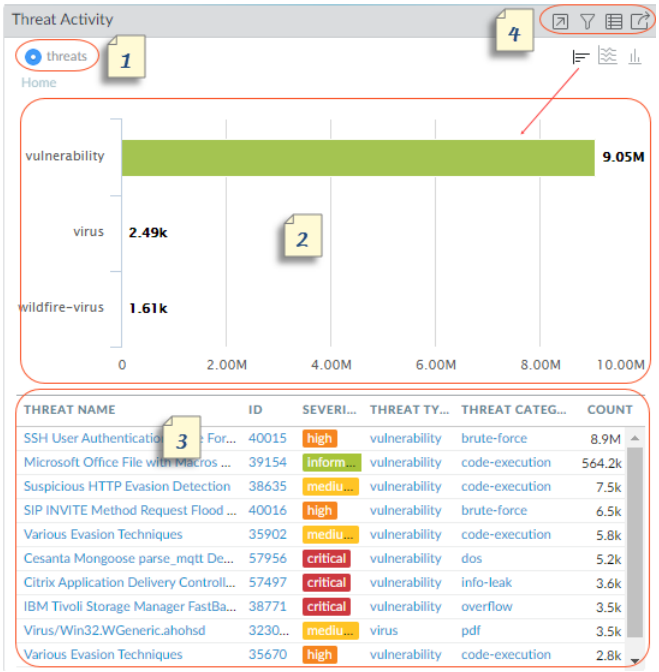
Pestaña	Description (Descripción)
	por tipo de archivo y aplicación y aplicaciones que usan puertos no estándar. El widget Hosts en riesgo de esta pestaña (únicamente algunas plataformas admiten el widget) complementa la detección con mejores técnicas de visualización; utiliza la información de la pestaña de eventos correlacionados (**Automated Correlation Engine [Motor de correlación automatizada]** > **Correlated Events [Eventos correlacionados]**) para presentar una vista agregada de hosts en riesgo en su red en función de las direcciones IP/usuarios de origen y la gravedad.
Actividad bloqueada	Se centra en el tráfico al que se ha impedido entrar en la red. Los widgets de esta pestaña le permiten ver la actividad denegada por nombre de aplicación, nombre de usuario, nombre de amenaza, contenido bloqueado (archivos y datos) por un perfil de bloqueo de archivo. También enumera las principales reglas de seguridad que se compararon para bloquear amenazas, contenido y URL.
Actividad de túnel	Muestra la actividad del tráfico de túnel que el cortafuegos ha inspeccionado en función de las políticas de inspección de túnel. La información incluye el uso del túnel basado en ID de túnel, etiqueta de inspección, protocolos de usuario y túnel tales como Generic Routing Encapsulation (GRE), protocolo de túnel GPRS para datos de usuario (GTP-U) y IPSec no cifrado.
GlobalProtect Activity (Actividad de GlobalProtect)	Muestra una descripción general de la actividad del usuario en su implementación de GlobalProtect. La información incluye el número de usuarios y la cantidad de veces que los usuarios se conectaron, las puertas de enlace a las que se conectaron los usuarios, la cantidad de fallos de conexión y el motivo del fallo, un resumen de los métodos de autenticación, las versiones de la aplicación de GlobalProtect utilizadas y la cantidad de endpoints en cuarentena. Además, esta pestaña muestra un resumen de la vista de gráfico de los dispositivos puestos en cuarentena. Utilice el conmutador de alternancia de la parte superior del gráfico para ver los dispositivos en cuarentena por las acciones que provocaron que GlobalProtect pusiera en cuarentena el dispositivo, el motivo por el que GlobalProtect puso en cuarentena el dispositivo y la ubicación de los dispositivos en cuarentena.
SSL Activity (Actividad de SSL)	Muestra una descripción general de la actividad de descifrado TLS/SSL en el cortafuegos. La información incluye la actividad de descifrado correcta e incorrecta en su red, los motivos de error de descifrado como problemas de protocolo, certificado y versión, versiones de TLS, algoritmos de intercambio de claves y la cantidad y el tipo de tráfico descifrado y no descifrado. Utilice la información de ACC para evaluar cómo está funcionando el descifrado en su red y, a continuación, utilice Log de descifrado para profundizar en los detalles.

También puede Interacción con el ACC para crear pestañas personalizadas con widgets y diseño personalizado que cumplan sus necesidades de supervisión de red, exportar la pestaña y compartirla con otros administradores.

© 2020 Palo Alto Networks, Inc.

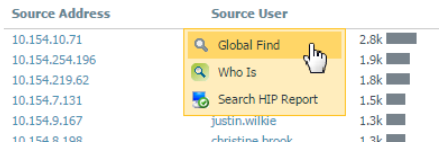
Widgets de ACC

Los widgets de cada pestaña son interactivos; puede definir los Filtros de ACC y desglosar detalles de cada tabla o gráfico, o personalizar los widgets incluidos en la pestaña para centrarse en la información que necesita. Si desea detalles sobre la visualización de cada widget, consulte las Descripciones de los widgets.



Widgets		
1	**Ver**	Puede ordenar los datos por bytes, sesiones, amenazas, recuento, contenido, URL, malintencionados, benignos, archivos, aplicaciones, datos, perfiles, objetos, usuarios. Las opciones disponibles varían según el widget.
2	**Gráfico**	Las opciones de visualización de los gráficos son mapa jerárquico, gráfico de líneas, gráfico de barras horizontales, gráfico de área apilada, gráfico de barra apilada y mapas. Las opciones disponibles varían según el widget; la experiencia de interacción también varía según el tipo de gráfico. Por ejemplo, el widget para aplicaciones que usan puertos no estándar le permite elegir entre un mapa jerárquico y un gráfico de líneas. Para obtener una vista más detallada, haga clic en el gráfico. El área en la que haga clic se convierte en un filtro y le permite acercarse a la selección y ver información más granular para esa selección.
3	**Tabla**	La vista detallada de los datos usados para representar el gráfico se ofrece en una tabla debajo del gráfico. Puede interactuar con la tabla de distintos modos: • Puede hacer clic y establecer un filtro local o un filtro global para un atributo de la tabla. El gráfico se

© 2020 Palo Alto Networks, Inc.

Widgets		
		actualiza y la tabla se ordena según ese filtro local. La información mostrada en el gráfico y la tabla siempre está sincronizada. • Pase el ratón sobre un atributo de la tabla y use las opciones disponibles en el menú desplegable. 
4	**Acciones**	**Maximizar vista**: le permite aumentar el widget y ver la tabla en una pantalla más grande y con más información visualizable. **Configurar filtros locales**: le permite añadir Filtros de ACC para refinar la visualización dentro del widget. Use estos filtros para personalizar los widgets; estas personalizaciones se retienen entre inicios de sesión. **Saltar a logs**: le permite navegar directamente a los logs (pestaña **Monitor [Supervisar]** > **Logs [Logs]** > **<log-type>**). Los logs se filtran usando el periodo que se muestra en el gráfico. Si ha establecido filtros locales y globales, la consulta de log concatena el periodo y los filtros y muestra solo logs que cumplan con el conjunto de filtros combinado. **Exportar**: le permite exportar el gráfico como PDF. El PDF se descarga y se guarda en la máquina local. Se guarda en la carpeta Descargas asociada con su navegador web en su ordenador.

Descripciones de widget

Cada pestaña del ACC incluye un conjunto distinto de widgets.

Widget	Description (Descripción)
Network Activity (Actividad de red): Muestra una descripción general del tráfico y la actividad de los usuarios en su red.	
Application Usage (Uso de aplicación)	La tabla muestra las principales diez aplicaciones que se usan en la red; todas las aplicaciones restantes que se usan en la red se agregan y visualizan como otras. El gráfico muestra todas las aplicaciones por categoría y subcategoría de aplicación y la aplicación. Use este widget para buscar las aplicaciones que se intentan usar en la red, le informa sobre las aplicaciones predominantes según ancho de banda, recuento de sesiones, transferencias de archivos, activación de más amenazas y acceso a URL. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL

© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
	Gráficos disponibles: mapa jerárquico, área, columna, línea (los gráficos varían según el atributo de ordenación seleccionado)
User Activity (Actividad del usuario)	Muestra los diez usuarios más activos de la red que han generado el mayor volumen de tráfico y consumido recursos de red para obtener contenido. Use este widget para monitorizar los principales usuarios según uso ordenado por bytes, sesiones, amenazas, contenido (archivos y patrones) y URL visitadas. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: área, columna, línea (los gráficos varían según el atributo de ordenación seleccionado)
Source IP Activity (Actividad de IP de origen)	Muestra las principales direcciones IP o nombres de host de los dispositivos que han iniciado la actividad en la red. Todos los demás dispositivos se agregan y visualizan como otros. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: área, columna, línea (los gráficos varían según el atributo de ordenación seleccionado)
Destination IP Activity (Actividad de IP de destino)	Muestra las direcciones IP o nombres de host de los diez principales destinos a los que accedieron los usuarios de la red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: área, columna, línea (los gráficos varían según el atributo de ordenación seleccionado)
Source Regions (Regiones de origen)	Muestra las diez principales direcciones (regiones definidas personalizadas o integradas) del mundo desde las que los usuarios iniciaron la actividad en su red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: mapa, barra
Regiones de destino	Muestra las diez principales regiones de destino (regiones definidas personalizadas o integradas) del mundo desde las que los usuarios accedieron al contenido de la red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: mapa, barra
Información de host de GlobalProtect	Muestra información del estado de los hosts en los que se ejecuta el agente GlobalProtect; el sistema de host es un endpoint de GlobalProtect. Esta información se origina desde entradas en el log de coincidencias HIP que se generan cuando los datos enviados por la aplicación de GlobalProtect coinciden con un objeto HIP o un perfil HIP que haya definido en el cortafuegos. Si no tiene log de coincidencias HIP, este widget está en blanco. Para aprender a crear objetos HIP y perfiles HIP, y usarlos como criterios de coincidencias de políticas, consulte Configuración de la aplicación de políticas basadas en HIP. Atributos de ordenación: perfiles, objetos, sistemas operativos

© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
	Gráficos disponibles: barra
Rule Usage (Uso de reglas)	Muestra las diez principales reglas que han iniciado más tráfico en la red. Use este widget para ver las reglas usadas más comúnmente, monitorizar los patrones de uso y para evaluar si las reglas son efectivas para asegurar su red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: línea
Ingress Interfaces (Interfaces de entrada)	Muestra las interfaces de cortafuegos que se usan más para permitir el tráfico en la red. Atributos de ordenación: bytes, bytes enviados, bytes recibidos Gráficos disponibles: línea
Egress Interfaces (Interfaces de salida)	Muestra las interfaces de cortafuegos que más usa el tráfico que sale de la red. Atributos de ordenación: bytes, bytes enviados, bytes recibidos Gráficos disponibles: línea
Source Zones (Zonas de origen)	Muestra las zonas que más se usan para permitir que el tráfico entre en la red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: línea
Destination Zones (Zonas de destino)	Muestra las zonas que más usa el tráfico que sale de la red. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: línea
Threat Activity (Actividad de amenazas): Esta pestaña muestra una descripción general de las amenazas en la red.	
Hosts en riesgo	Muestra los hosts con más probabilidad de estar en riesgo en la red. Este widget resume los eventos desde los logs de correlación. Para cada dirección IP/usuario de origen, incluye el objeto de correlación que activó la coincidencia y el recuento de coincidencias que se agrega desde la correlación de evidencias en los logs de eventos correlacionados. Si desea información detallada, consulte Use el motor de correlación automatizada. Está disponible con PA-5200 Series, PA-7000 Series y Panorama. Atributos de ordenación: gravedad (por defecto)
Hosts Visiting Malicious URLs (Hosts de visitas a URL malintencionadas)	Muestra la frecuencia con la que los hosts (dirección IP/nombres de host) de su red han accedido a URL malintencionadas. Se sabe que esas URL son malware por su categorización en PAN-DB. Atributos de ordenación: recuento Gráficos disponibles: línea

© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
Hosts Resolving Malicious Domains (Hosts de resolución de dominios malintencionados)	Muestra los host que más coinciden con las firmas de DNS; los hosts de la red que intentan resolver el nombre de host o dominio de una URL malintencionada. Esta información se recopila a partir de un análisis de la actividad DNS de su red. Utiliza la monitorización pasiva de DNS, el tráfico DNS generado en la red, la actividad vista en el sandbox si ha configurado un sinkhole de DNS en el cortafuegos, y los informes DNS en orígenes DNS malintencionados que están disponibles en los clientes de Palo Alto Networks. Atributos de ordenación: recuento Gráficos disponibles: línea
Threat Activity (Actividad de amenazas)	Muestra las amenazas que se ven en su red. Esta información se basa en coincidencias de firmas en antivirus, antispyware y perfiles de protección de vulnerabilidad y virus de los que informa WildFire. Atributos de ordenación: amenazas Gráficos disponibles: barra, área, columna
WildFire Activity by Application (Actividad de WildFire por aplicación)	Muestra las aplicaciones con la mayoría de envíos de WildFire. Este widget usa los veredictos de malintencionado/benigno de los logs de envío de WildFire. Atributos de ordenación: malintencionado, benigno Gráficos disponibles: barra, línea
WildFire Activity by File Type (Actividad de WildFire por tipo de archivo)	Muestra un vector de amenazas por tipo de archivo. Este widget muestra los tipos de archivo que han generado la mayoría de envíos de WildFire y usa el veredicto de malintencionado o benigno del log de envíos de WildFire. Si estos datos no están disponibles, el widget está vacío. Atributos de ordenación: malintencionado, benigno Gráficos disponibles: barra, línea
Applications using Non Standard Ports (Aplicaciones que usan puertos no estándar)	Muestra las aplicaciones que entran en su red por puertos no estándar. Si ha migrado sus reglas de cortafuegos de un cortafuegos basado en puerto, use esta información para diseñar reglas de políticas que permitan únicamente el tráfico en el puerto predeterminado de la aplicación. Cuando sea necesario, haga una excepción para permitir el tráfico en un puerto no estándar o cree una aplicación personalizada. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: mapa jerárquico, línea
Rules Allowing Applications On Non Standard (Reglas que permiten aplicaciones en puertos no estándar)	Muestra reglas de políticas de seguridad que permiten aplicaciones en puertos no predeterminados. El gráfico muestra todas las reglas mientras la tabla muestra las diez reglas principales y agrega los datos de las reglas restantes como Otro. Esta información le ayuda a identificar huecos en la seguridad de red permitiéndole evaluar si una aplicación está saltándose puertos o entrando furtivamente en su red. Por ejemplo, puede validar si tiene una regla que permita el tráfico en cualquier puerto excepto el puerto predeterminado para la aplicación. Pongamos, por ejemplo, que tiene una regla que define el

© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
	tráfico DNS en el puerto *predeterminado de la aplicación* (el puerto 53 es el puerto estándar para DNS). Este widget mostrará cualquier regla que admite el tráfico DNS en su red en cualquier puerto excepto el puerto 53. Atributos de ordenación: bytes, sesiones, amenazas, contenido, URL Gráficos disponibles: mapa jerárquico, línea
Blocked Activity (Actividad bloqueada): Esta pestaña se centra en el tráfico bloqueado para que no entre en la red.	
Blocked Application Activity (Actividad de aplicación bloqueada)	Muestra las aplicaciones que se han denegado en su red, y le permite visualizar las amenazas, el contenido y las URL que mantiene fuera de su red. Atributos de ordenación: amenazas, contenido, URL Gráficos disponibles: mapa jerárquico, área, columna
Blocked User Activity (Actividad de usuario bloqueado)	Muestra las solicitudes de usuario que se bloquearon por coincidencia con el perfil de antivirus, antispyware, bloqueo de archivos o filtrado de URL adjunto a la regla de política de seguridad. Atributos de ordenación: amenazas, contenido, URL Gráficos disponibles: barra, área, columna
Blocked Threats (Amenazas bloqueadas)	Muestra las amenazas que se rechazaron con mayor éxito en su red. Estas amenazas se comparan con firmas antivirus, firmas de vulnerabilidad y firmas DNS disponibles a través de las actualizaciones de contenido dinámico en el cortafuegos. Atributos de ordenación: amenazas Gráficos disponibles: barra, área, columna
Contenido bloqueado	Muestra los archivos y datos que se bloquearon para que no entren en la red. El contenido se bloqueó porque la política de seguridad denegó el acceso en función de los criterios definidos en el perfil de seguridad Bloqueo de archivo o un perfil de seguridad de Filtrado de datos. Atributos de ordenación: archivos, datos Gráficos disponibles: barra, área, columna
Security Policies Blocking Activity (Actividad de bloqueo de políticas de seguridad)	Muestra reglas de políticas de seguridad que bloquean o restringen el tráfico de su red. Como su widget muestra las amenazas, el contenido y las URL a las que se denegó acceso a la red, puede usarlos para evaluar la efectividad de las reglas de políticas. Este widget no muestra el tráfico que se bloqueó por las reglas de denegación que se han definido en la política. Atributos de ordenación: amenazas, contenido, URL Gráficos disponibles: barra, área, columna
GlobalProtect Activity (Actividad de GlobalProtect): muestra información de la actividad del usuario en su implementación de GlobalProtect.	

© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
Successful GlobalProtect Connection Activity (Actividad de la conexión de GlobalProtect correcta):	Muestra una vista de gráfico de la actividad de conexión de GlobalProtect durante el periodo seleccionado. Use el botón de la parte superior del gráfico para cambiar entre las estadísticas de conexión por usuarios, portales y puertas de enlace, y ubicación. Atributos de ordenación: usuarios, portales/puertas de enlace, ubicación Gráficos disponibles: barra, línea
Unsuccessful GlobalProtect Connection Activity (Actividad de conexión de GlobalProtect incorrecta)	Muestra una vista de gráfico de la actividad de conexión de GlobalProtect incorrecta durante el periodo seleccionado. Use el botón de la parte superior del gráfico para cambiar entre las estadísticas de conexión por usuarios, portales y puertas de enlace, y ubicación. Para ayudarlo a identificar y solucionar problemas de conexión, puede ver también el cuadro o gráfico de motivos. Para este gráfico, el ACC indica el error, el usuario de origen, la dirección IP pública y demás información para ayudarlo a identificar y resolver el problema rápidamente. Atributos de ordenación: usuarios, portales/puertas de enlace, motivos, ubicación Gráficos disponibles: barra, línea
GlobalProtect Deployment Activity (Actividad de implementación de GlobalProtect)	Muestra un resumen de la vista de gráfico de la implementación. Utilice el botón de la parte superior del gráfico para ver la distribución de usuarios por método de autenticación, versión de la aplicación de GlobalProtect y la versión del sistema operativo. Atributos de ordenación: método de autenticación, versión de la aplicación de globalprotect, sistema operativo Gráficos disponibles: barra, línea
GlobalProtect Quarantine Activity (Actividad de cuarentena de GlobalProtect)	Muestra un resumen de la vista de gráfico de los dispositivos que se han puesto en cuarentena. Utilice el conmutador de alternancia de la parte superior del gráfico para ver los dispositivos en cuarentena por las acciones que provocaron que GlobalProtect pusiera en cuarentena el dispositivo, el motivo por el que GlobalProtect puso en cuarentena el dispositivo y la ubicación de los dispositivos en cuarentena. Atributos de ordenación: acciones, motivo y ubicación Gráficos disponibles: barra, línea
SSL Activity (Actividad de SSL): muestra información sobre la actividad de SSL/TLS en su red.	
Traffic Activity (Actividad de tráfico)	Muestra la actividad de SSL/TLS en comparación con la actividad que no es de SSL/TLS por número total de sesiones o bytes.
SSL/TLS Activity (Actividad de SSL/TLS)	Muestra las conexiones TLS correctas por versión y aplicación TLS o SNI. Este widget le ayuda a comprender cuánto riesgo está asumiendo al permitir versiones del protocolo TLS más débiles. La identificación de aplicaciones y SNI que utilizan protocolos débiles le permite evaluar cada una y decidir si necesita permitir el acceso a ellas por motivos empresariales. Si no necesita la aplicación para fines empresariales, es posible que desee bloquear el tráfico

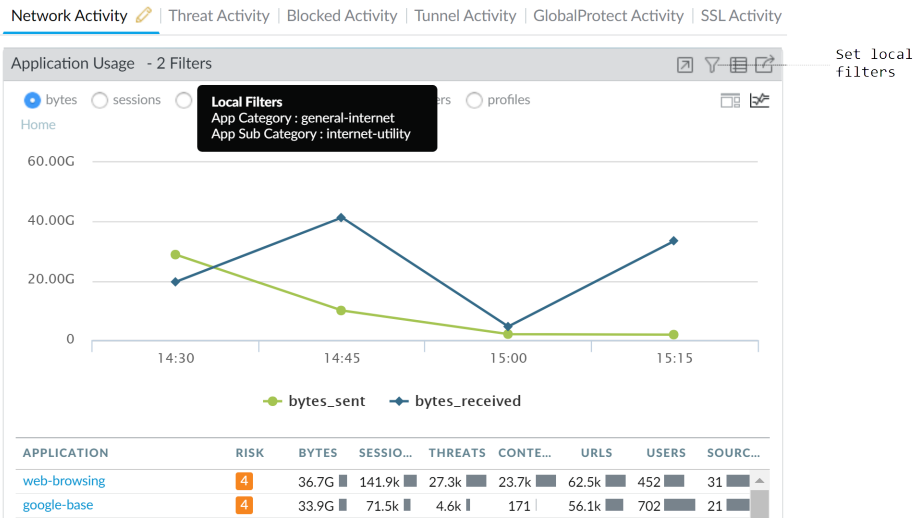
© 2020 Palo Alto Networks, Inc.

Widget	Description (Descripción)
	en lugar de permitirlo. Haga clic en una aplicación o una SNI para profundizar y ver información detallada.
Motivos de error de descripción	Muestra los motivos de los fallos de descifrado, como problemas con el certificado o el protocolo, por SNI. Utilice esta información para detectar problemas causados por una política de descifrado o una configuración incorrecta del perfil o por el tráfico que utiliza protocolos o algoritmos débiles. Haga clic en un motivo de fallo para profundizar y aislar el número de sesiones por SNI o haga clic en un SNI para ver todos los fallos de descifrado para esa SNI.
Actividad de versión de TLS correcta	Muestra la cantidad de tráfico descifrado y no descifrado por sesiones o bytes. El tráfico que no se descifró puede estar exento del descifrado por la política, la configuración incorrecta de políticas o por estar en la lista de exclusión de descifrado (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**).
Actividad de intercambio de claves correcta	Muestra la actividad correcta de intercambio de claves por algoritmo, por aplicación o por SNI. Haga clic en un algoritmo de intercambio de claves para ver la actividad de ese algoritmo o haga clic en una aplicación o SNI para ver la actividad de intercambio de claves para esa aplicación o SNI.

Filtros de ACC

Los gráficos y tablas de los widgets de ACC le permiten usar filtros para restringir el ámbito de datos que se muestra, de modo que puede aislar atributos específicos y analizar información que quiera ver en mayor detalle. El ACC admite el uso simultáneo de filtros globales y widget.

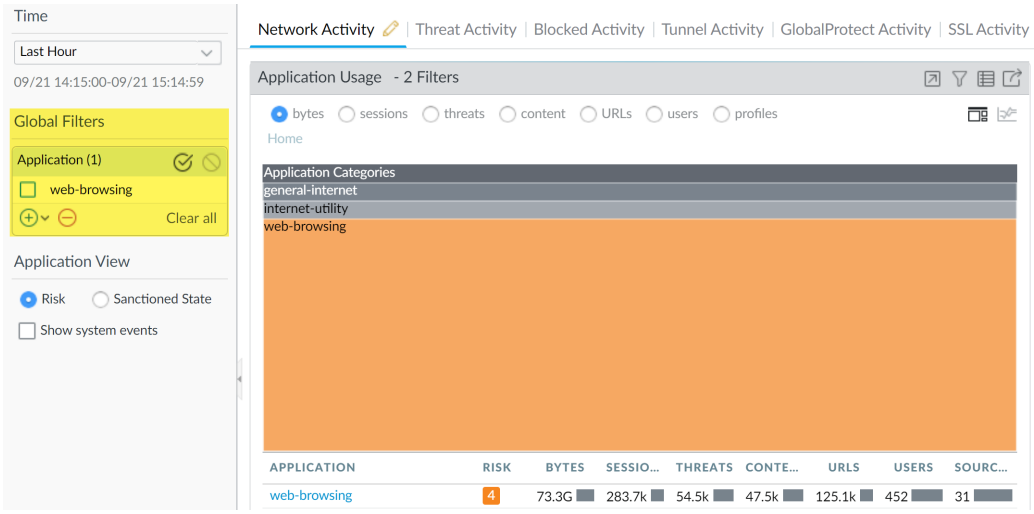
- **Filtros de widget**: Aplica un filtro de widget, que es un filtro que es *local* en un widget específico. Un filtro de widget le permite interactuar con el gráfico y personalizar la vista para que pueda explorar los datos y acceder a la información que quiere monitorizar en un widget específico. Para crear un filtro de widget que sea persistente en los reinicios, debe usar la opción **Set Local Filter (Configurar filtro local)**.



- **Filtros globales**: Aplique filtros globales en todas las pestañas en el ACC. Un filtro global le permite pivotar la vista alrededor de la información que necesita instantáneamente y excluir la información

© 2020 Palo Alto Networks, Inc.

irrelevante para la vista actual. Por ejemplo, para ver todos los eventos relacionados con un usuario y aplicación específicos, puede aplicar el nombre de usuario y la aplicación como un filtro global y ver solo información relativa a ese usuario y aplicación a través de todas las pestañas y widgets en el ACC. Los filtros globales sí se borran al reiniciar.



Puede aplicar los filtros globales de tres formas:

- **Establecer un filtro desde una tabla**: seleccione un atributo desde una tabla en cualquier widget y aplicar el atributo como un filtro global.
- **Add a widget filter to a global filter**: pase el cursor del ratón sobre el atributo y haga clic en la flecha a la derecha del atributo. Esta opción le permite elevar un filtro local utilizado en un widget, y aplicar el atributo de manera global para actualizar la pantalla en todas las pestañas de ACC.
- **Definir un filtro global**: Defina un filtro usando el panel **Global Filters (Filtros globales)** en el ACC.

Consulte Interacción con el ACC si desea obtener detalles sobre el uso de estos filtros.

Interacción con el ACC

Para personalizar y restringir la visualización de ACC, puede añadir, eliminar, exportar e importar pestañas, añadir y eliminar widgets, establecer filtros locales y globales e interactuar con los widgets.

- Añada una pestaña
  1. Seleccione el icono + de la lista de pestañas.
  2. Añada un **View Name**. Este nombre se utilizará como el nombre de la pestaña. Puede añadir hasta 5 pestañas.

- Modifique una pestaña.

  Seleccione la pestaña y haga clic en el icono de lápiz junto al nombre de la pestaña para modificarla. Por ejemplo | Threat Activity .

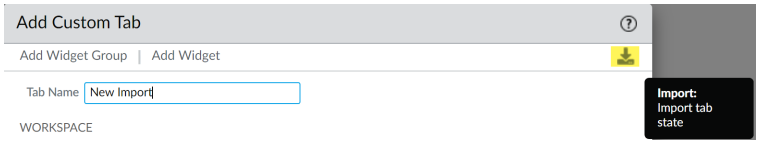
  La edición de una pestaña le permite añadir, eliminar o restablecer los widgets que se muestran en la pestaña. También puede cambiar el diseño de widget de la pestaña.

  Para guardar la pestaña como pestaña predeterminada, seleccione .

- Exporte e importe pestañas.

© 2020 Palo Alto Networks, Inc.

1. Seleccione la pestaña y haga clic en el icono de lápiz junto al nombre de la pestaña para modificarla.
2. Seleccione el icono para exportar la pestaña actual como archivo .txt. Puede compartir este archivo .txt con otro administrador.
3. Para importar la pestaña como una pestaña nueva a otro cortafuegos, seleccione el icono + en la lista de pestañas y añada un nombre y haga clic en el icono importar, y luego busque el archivo .txt.



- Vea qué widgets se incluyen en una pestaña.
  1. Seleccione la pestaña y haga clic en el icono del lápiz para editarlo.
  2. Seleccione el menú desplegable **Add Widget (Añadir widget)** y compruebe los widgets que tienen las casillas de verificación seleccionadas.

- Añadir un widget a un grupo de widgets.
  1. Añada una nueva pestaña o modifique una pestaña predefinida.
  2. Seleccione **Add Widget (Añadir widget)** y marque la casilla de verificación del widget que quiere añadir. Puede seleccionar hasta 12 widgets.
  3. (Opcional) Para crear un diseño de dos columnas, seleccione **Add Widget Group**. Puede arrastrar y soltar los widgets en la vista de dos columnas. Cuando arrastre el widget sobre el diseño, aparecerá un marcador de posición para que suelte el widget.

     No puede ponerle nombre a los grupos de widgets.

- Eliminar una pestaña o un widget/grupo de widgets.
  1. Para eliminar una pestaña personalizada, seleccione la pestaña y haga clic en el icono X. Custom_threat_user_activity

     No puede eliminar una pestaña predefinida.
  2. Para eliminar un widget o grupo de widgets, modifique la pestaña y la sección del espacio de trabajo, haga clic en el icono (X) de la derecha. Esta acción no se puede deshacer.

- Restablezca los widgets predeterminados de una pestaña.

  En una pestaña por defecto, como la pestaña **Blocked Activity**, puede eliminar uno o más widgets. Si quiere restablecer el diseño para que incluya el conjunto predeterminado de widgets de la pestaña, modifique la pestaña y haga clic en **Reset view (Restablecer vista)**.

- Amplíe el zoom sobre los detalles en un área, columna o gráfico de líneas.

  Vea cómo funciona la funcionalidad de ampliación de zoom.

  Haga clic y arrastre un área en el gráfico para ampliar el zoom. Por ejemplo, cuando amplíe el zoom en un gráfico de línea, activa una segunda consulta y el cortafuegos recupera los datos para el periodo de tiempo seleccionado. No es simplemente una magnificación.

- Utilice la lista desplegable de la tabla para buscar más información sobre un atributo.
  1. Pase el ratón sobre un atributo de la tabla para ver el menú desplegable.

© 2020 Palo Alto Networks, Inc.

2. Haga clic en el menú desplegable para ver las opciones disponibles.
   - **Global Find (Búsqueda global)**: permite buscar referencias al atributo (nombre de usuario o dirección IP, nombre de objeto, nombre de regla de política, ID de amenaza o nombre de aplicación) en cualquier lugar de la configuración candidata. Consulte Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama.
   - **Value**: muestra los detalles del ID de amenaza, nombre de aplicación u objeto de dirección.
   - **Who Is**: realiza una búsqueda de nombre de dominio (*WHOIS*) para la dirección IP. Las bases de datos de consulta de búsqueda que almacenan los usuarios registrados o asignados de un recurso de Internet.
   - **Search HIP Report**: usa el nombre de usuario o dirección IP para buscar coincidencias en un informe de coincidencias HIP.

- Defina un filtro local.

  También puede hacer clic en un atributo en la siguiente tabla bajo el gráfico para aplicarlo como un filtro de widget.

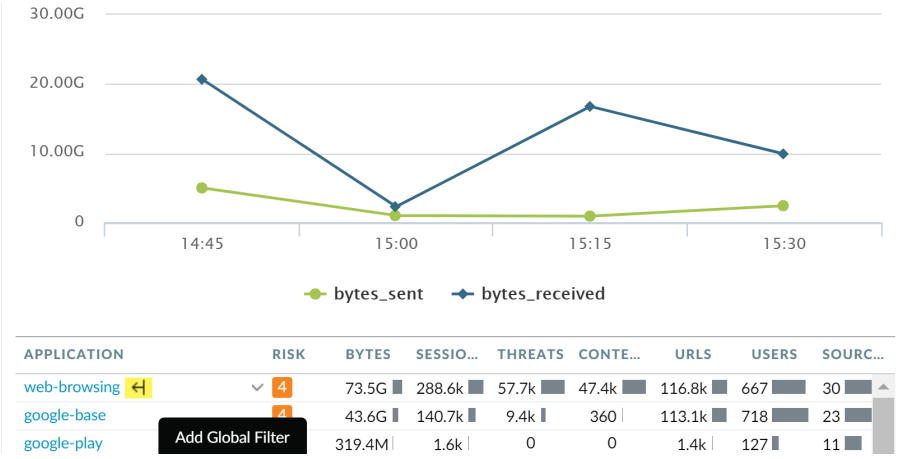
  1. Seleccione un widget y haga clic en el icono .
  2. Haga clic en el icono y añada los filtros que quiere aplicar.
  3. Haga clic en **Apply (Aplicar)**. Estos filtros no se eliminan al reiniciar.

  Los filtros de widget activos se indican junto al nombre de widget.

- Niegue un filtro de widget.
  1. Haga clic en el icono para mostrar el cuadro de diálogo Configurar filtros locales.
  2. Añada un filtro y haga clic en el icono de negación .

- Establecer un filtro global desde una tabla.

  Pase el curso del ratón sobre un atributo en la tabla que hay debajo de la gráfica y haga clic en la flecha que aparece a la derecha del atributo.

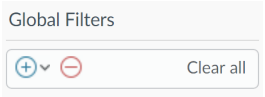


- Establezca un filtro global usando el panel Filtros globales

  Vea los filtros globales en acción.

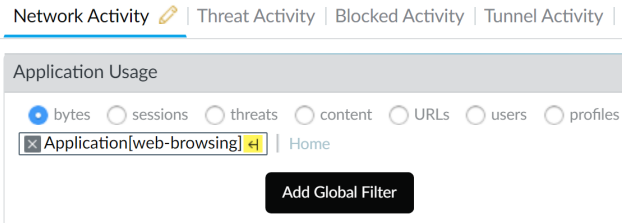
© 2020 Palo Alto Networks, Inc.

1. Encuentre el panel **Global Filters** en la parte izquierda del ACC.



2. Haga clic en el icono para ver la lista de filtros que quiere aplicar.

- Promover un filtro de widget a filtro global.
  1. En cualquier tabla de un widget, haga clic en el enlace de un atributo. Esto define el atributo como un filtro de widget.
  2. Para promover el filtro a filtro global, seleccione la flecha a la derecha del filtro.



- Eliminar un filtro.

  Haga clic en el icono para eliminar un filtro.

  - Para filtros globales: Se encuentra en el panel Filtros globales.
  - Para filtros de widget: Haga clic en el icono para ver el cuadro de diálogo Configurar filtros locales, seleccione el filtro y haga clic en el icono .

- Borrar todos los filtros.

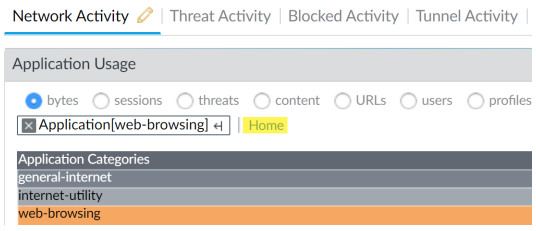
  - Para filtros globales: Haga clic en el botón **Borrar todo** debajo de Filtros globales.
  - Para filtros de widget: Seleccione un widget y haga clic en el icono . Después haga clic en el botón **Clear All** en el cuadro de diálogo Setup Local Filters.

- Vea qué filtros están en uso.

  - Para filtros globales: El número de filtros globales aplicado se muestra en el panel izquierdo, debajo de Filtros globales.
  - Para filtros de widget: El número de filtros de widgets aplicados a un widget se muestran junto al nombre del widget. Para ver los filtros, haga clic en el icono .

- Restablezca la visualización en un widget.

  - Si define un filtro de widget o desglosa un gráfico, haga clic en el enlace **Home** para restablecer la visualización en el widget.



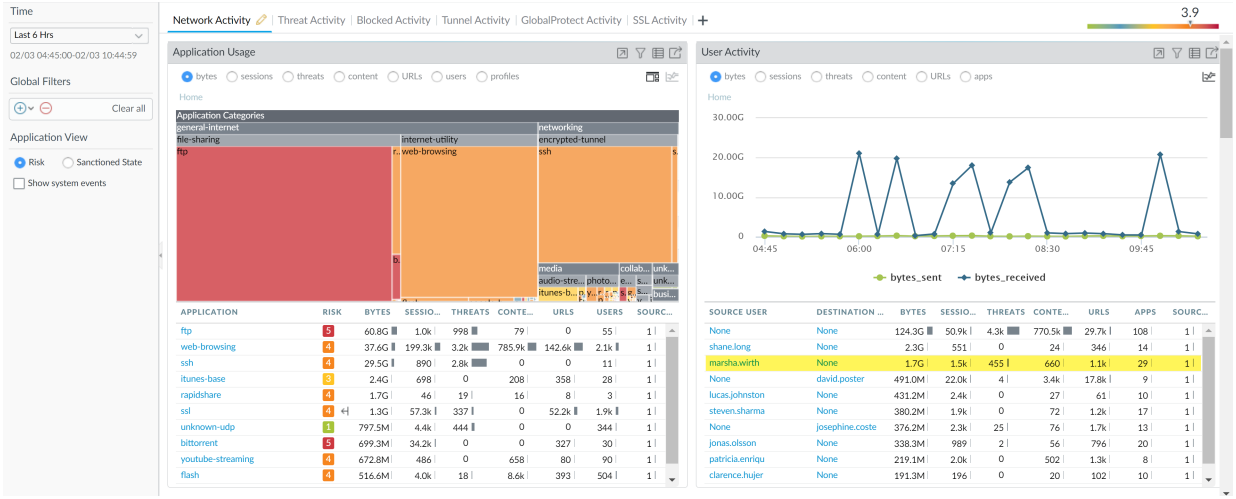
© 2020 Palo Alto Networks, Inc.

Caso de uso: ACC: Ruta de descubrimiento de información

El ACC tiene una variedad de información que puede usarse como punto de inicio para el análisis de tráfico de red. Veamos un ejemplo sobre el uso de ACC para descubrir eventos de interés. Este ejemplo ilustra cómo puede usar el ACC para asegurar que los usuarios legítimos puedan responder por sus acciones, detecten y supervisen la actividad no autorizada, así como detectar y diagnosticar hosts en riesgo y sistemas vulnerables de su red.

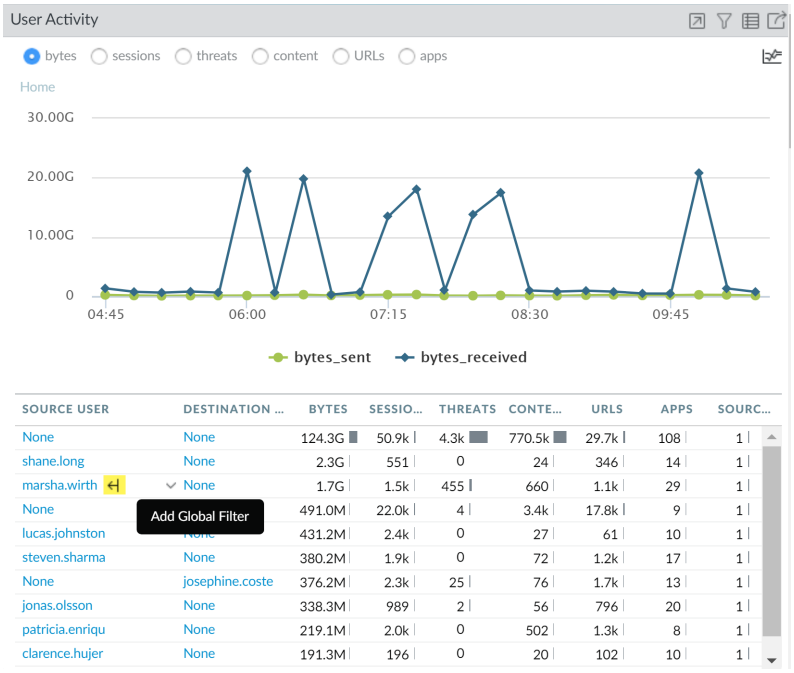
Los widgets y filtros del ACC le ofrecen la capacidad de analizar los datos y filtrar las vistas en función de los eventos de interés o preocupaciones. Puede seguir eventos que atraigan su interés, exportar directamente un PDF de una pestaña, acceder a los logs crudos sin procesar y guardar una vista personalizada de la actividad que desea monitorizar. Estas funcionalidades le permiten monitorizar la actividad y desarrollar políticas y contramedidas para fortificar su red frente a actividades malintencionadas. En esta sección, aprenderá a Interacción con el ACC widgets en distintas pestañas, desglosar con filtros widget, pivotar las vistas ACC usando filtros globales y exportar un PDF para compartir con los equipos de TI o de respuesta a incidencias.

A primera vista, verá los widgets Application Usage (Uso de aplicación) y User Activity (Actividad de usuario) en la pestaña **ACC** > **Network Activity (Actividad de red)**. El widget User Activity (Actividad de usuario) muestra que el usuario Marsha Wirth ha transferido 718 megabytes de datos durante la última hora. Este volumen es seis veces mayor que cualquier otro usuario de la red. Para ver la tendencia de las últimas horas, amplíe el valor de **Time (Tiempo)** a **Last 6 Hrs (Últimas 6 horas)** y ahora la actividad que Marsha ha tenido es de 6,5 gigabytes en más de 891 sesiones y ha activado 38 firmas de amenazas.



Como Marsha ha transferido un gran volumen de datos, aplique su nombre de usuario como un filtro global (Filtros de ACC) y pivote todas las vistas del ACC a la actividad del tráfico de Marsha.

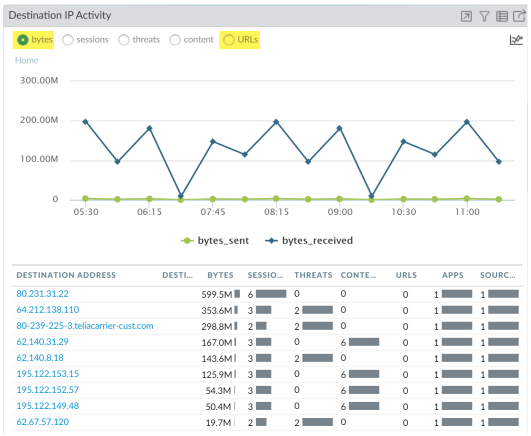
© 2020 Palo Alto Networks, Inc.



La pestaña Uso de aplicación ahora muestra que la aplicación principal que usaba Marsha era RapidShare, un sitio de alojamiento de archivos con base en Suiza que pertenece a la categoría de URL de intercambio de archivos. Para una investigación más detallada, añada RapidShare como filtro global y vea la actividad de Marsha en el contexto de RapidShare.

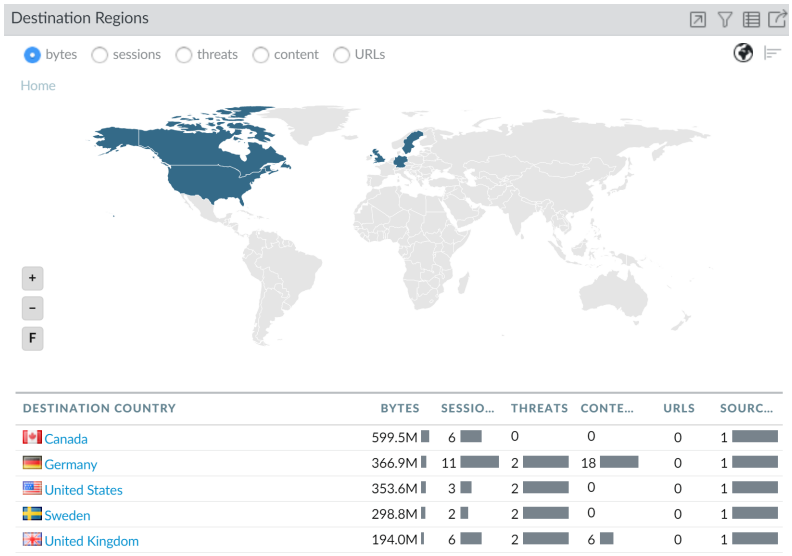
Considere si desea aprobar RapidShare para que lo use la compañía. ¿Debería permitir las cargas a este sitio y necesita una política de QoS para limitar el ancho de banda?

Para ver con qué direcciones IP se ha comunicado Marsha, seleccione el widget **Destination IP Activity (Actividad de IP de destino)** y visualice los datos por bytes y por URL.



Para saber con qué países se ha comunicado Marsha, ordene por **sessions (sesiones)** en el widget **Destination Regions (Regiones de destino)**.

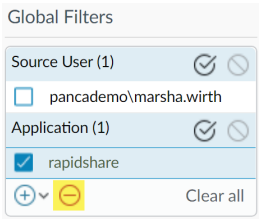
© 2020 Palo Alto Networks, Inc.



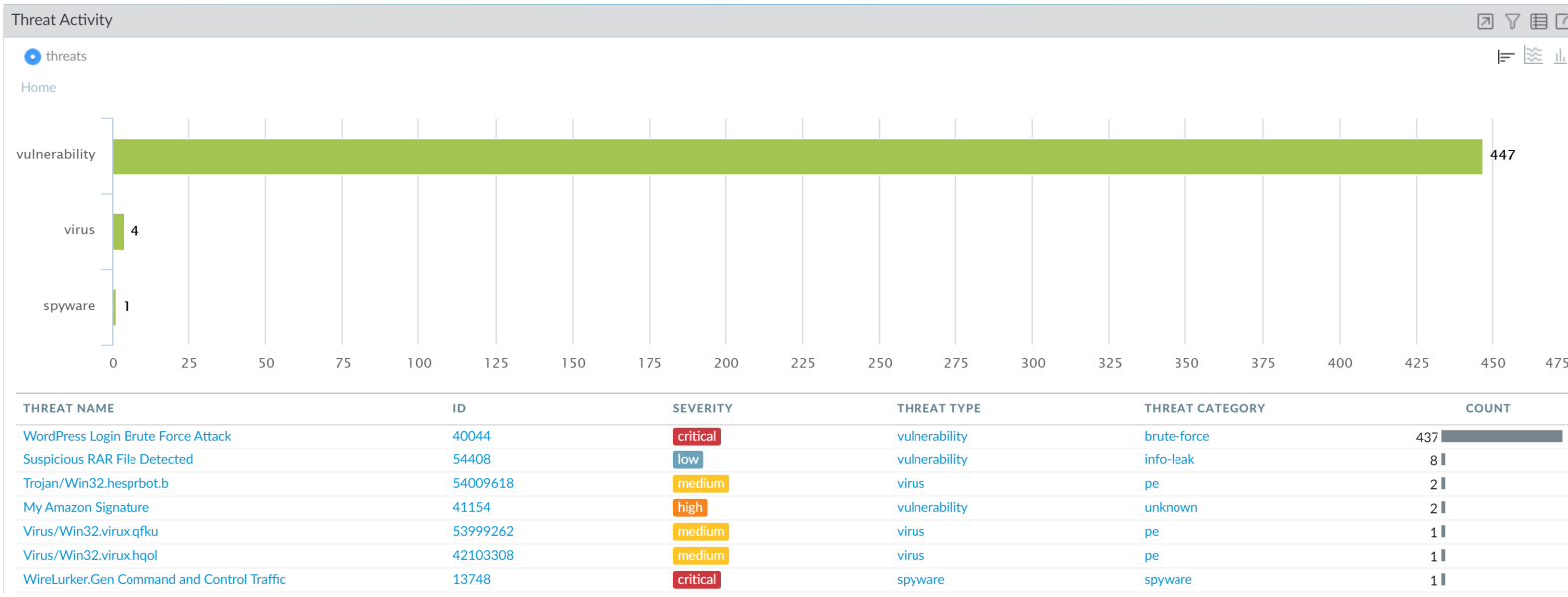
DESTINATION COUNTRY	BYTES	SESSIO...	THREATS	CONTE...	URLS	SOURC...
Canada	599.5M	6	0	0	0	1
Germany	366.9M	11	2	18	0	1
United States	353.6M	3	2	0	0	1
Sweden	298.8M	2	2	0	0	1
United Kingdom	194.0M	6	2	6	0	1

A partir de estos datos, puede confirmar que Marsha, una usuaria de su red, ha establecido sesiones establecidas en Corea y Estados Unidos, y que ha registrado 19 amenazas en sus sesiones dentro de la Unión Europea.

Para ver la actividad de Marsha desde una perspectiva de amenazas, quite el filtro global de RapidShare.



En el widget **Threat Activity (Actividad de amenazas)** de la pestaña **Threat Activity (Actividad de amenazas)**, vea las amenazas. El widget muestra que su actividad ha activado 26 vulnerabilidades en la categoría de amenazas de desbordamiento, DoS y ejecución de código. Varias de estas vulnerabilidades son de gravedad crítica.



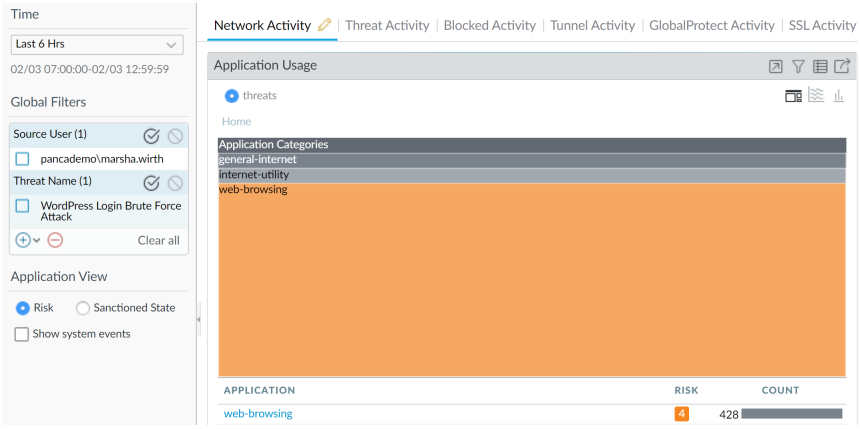
THREAT NAME	ID	SEVERITY	THREAT TYPE	THREAT CATEGORY	COUNT
WordPress Login Brute Force Attack	40044	critical	vulnerability	brute-force	437
Suspicious RAR File Detected	54408	low	vulnerability	info-leak	8
Trojan/Win32.hesprbot.b	54009618	medium	virus	pe	2
My Amazon Signature	41154	high	vulnerability	unknown	2
Virus/Win32.virux.qfku	53999262	medium	virus	pe	1
Virus/Win32.virux.hqol	42103308	medium	virus	pe	1
WireLurker.Gen Command and Control Traffic	13748	critical	spyware	spyware	1

© 2020 Palo Alto Networks, Inc.

Para desglosar cada vulnerabilidad, haga clic en el gráfico y restrinja el ámbito de su investigación. Cada clic aplica automáticamente un filtro local en el widget.



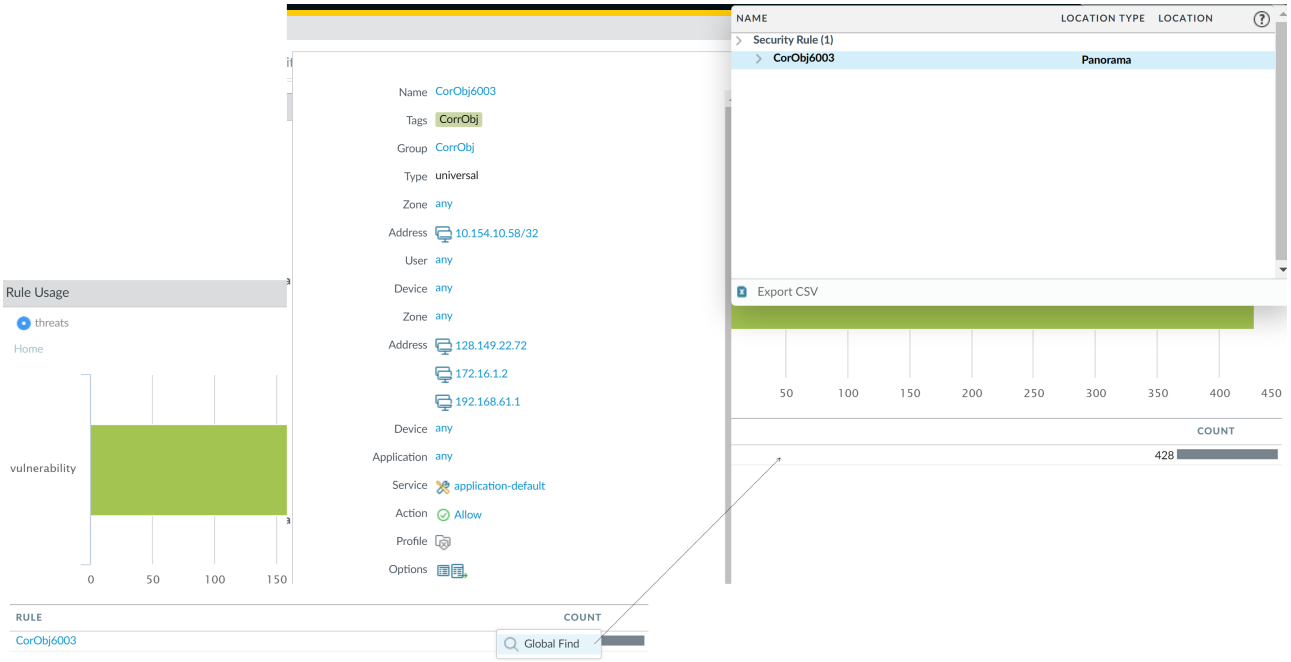
Para investigar cada amenaza por nombre, puede crear un filtro global para indicar **Microsoft Works File Converter Field Length Remote Code Execution Vulnerability (Vulnerabilidad de ejecución de código remoto de longitud de campo de conversor de archivo Microsoft Works)**. A continuación, vea el widget **User Activity widget (widget Actividad del usuario)** en la pestaña **Network Activity (Actividad de red)**. Esta pestaña se filtra automáticamente para mostrar la actividad de amenazas de Marsha (observe los filtros globales en la captura de pantalla).



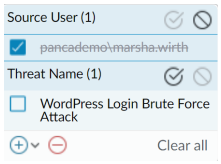
Observe que esta vulnerabilidad de ejecución de código de Microsoft se activó por correo electrónico, mediante la aplicación imap. Ahora puede establecer que Marsha tiene vulnerabilidades de IE y de archivos adjuntos al correo electrónico, y quizás su ordenador necesita parches. Ahora puede desplazarse al widget **Blocked Threats (Amenazas bloqueadas)** en la pestaña **Blocked Activity (Actividad bloqueada)** para comprobar cómo se bloquean muchas de estas vulnerabilidades.

O puede comprobar el widget **Rule Usage (Uso de reglas)** en la pestaña **Network Activity (Actividad de red)** para descubrir cuántas vulnerabilidades ingresaron en su red y qué regla de seguridad admitió este tráfico, y navegar directamente hasta la regla de seguridad usando la función **Global Find (Búsqueda global)**.

© 2020 Palo Alto Networks, Inc.

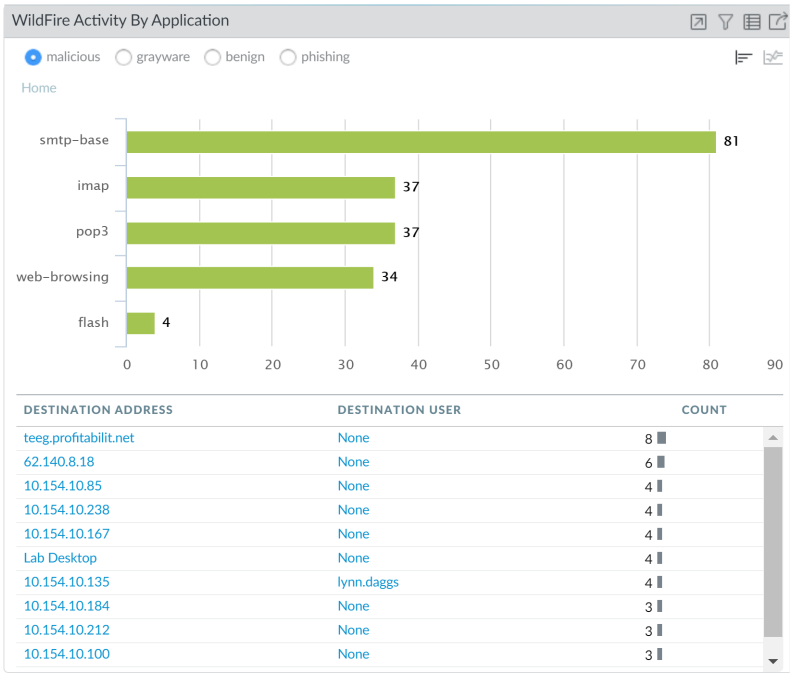


Después, averigüe por qué imap usó un puerto 43206 no estándar en lugar del puerto 143, que es el puerto predeterminado para la aplicación. Considere modificar la regla de políticas de seguridad para permitir que las aplicaciones usen únicamente el puerto predeterminado para la aplicación o evalúe si este puerto debe ser una excepción para su red.

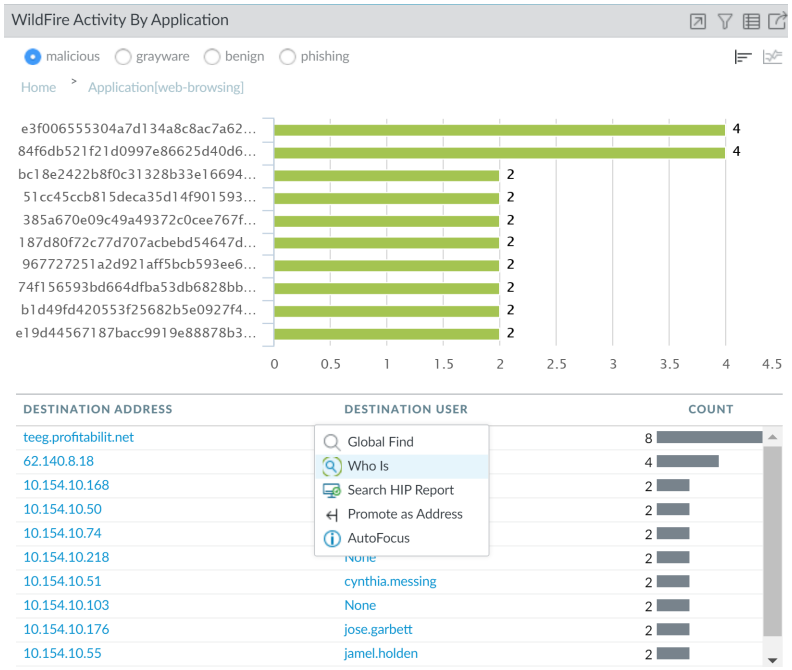


Para revisar si se registraron amenazas a través de imap, consulte la actividad de Marsha en el widget **WildFire Activity by Application (Actividad de WildFire por aplicación)** en la pestaña **Threat Activity (Actividad de amenazas)**. Puede confirmar que Marsha no realizó una actividad dañina, pero para verificar que ningún otro usuario se puso en riesgo por la aplicación imap, niegue a Marsha como filtro global y busque otros usuarios que activaron amenazas por imap.

© 2020 Palo Alto Networks, Inc.



Haga clic en la barra de imap en el gráfico y desglose las amenazas entrantes asociadas con la aplicación. Para saber con quién está registrada una dirección IP, pase el ratón sobre la dirección IP atacante y seleccione el enlace **Who Is** en el menú desplegable.



Como el recuento de sesiones desde esta dirección IP es alto, seleccione los widgets **Blocked Content (Contenido bloqueado)** y **Blocked Threats (Amenazas bloqueadas)** en la pestaña **Blocked Activity (Actividad bloqueada)** para los eventos relacionados con esta dirección IP. La pestaña **Blocked Activity (Actividad bloqueada)** le permite validar si sus reglas de políticas son efectivas a la hora de bloquear contenido o amenazas cuando un host de su red está en riesgo.

Use la funcionalidad **Export PDF (Exportar PDF)** en el ACC para exportar la vista actual (crear una instantánea de los datos) y enviarla a un equipo de respuesta a incidencias. Para ver los logs de amenazas directamente desde el widget, también puede hacer clic en el icono para ir a los logs; la consulta se genera

© 2020 Palo Alto Networks, Inc.

automáticamente y solo los logs relevantes se muestran en pantalla (por ejemplo en **Monitor [Supervisar]** > **Logs (Logs)** > **Threat Logs [Logs de amenazas]**).



Ahora ha usado el ACC para revisar las tendencias/datos de red para averiguar qué aplicaciones o usuarios están generando más tráfico, y como muchas aplicaciones son responsables de las amenazas que se detectan en la red. Así, se ha podido identificar qué aplicaciones o usuarios generaron el tráfico, determinar si la aplicación estaba en el puerto predeterminado y qué reglas de políticas permitieron que el tráfico entrara en la red, así como determinar si la amenaza se está propagando lateralmente en la red. También se identificó las direcciones IP de destino, las geoubicaciones con las que los hosts de la red se están comunicando. Use las conclusiones de su investigación para crear políticas orientadas a objetivos que puedan proteger a los usuarios y a su red.

© 2020 Palo Alto Networks, Inc.

Uso de los informes de App Scope

Los informes de Appscope proporcionan herramientas de visibilidad y análisis para detectar los comportamientos problemáticos, lo que permite comprender los cambios en el uso de las aplicaciones y la actividad del usuario, y los usuarios y las aplicaciones que consumen la mayor parte del ancho de banda de la red, e identificar las amenazas en la red.

Con los informes de Appscope, puede comprobar rápidamente si algún comportamiento es inusual o inesperado. Cada informe proporciona una ventana dinámica y personalizable por el usuario en la red; al pasar el ratón por encima y hacer clic en las líneas y barras de los gráficos, se abre información detallada acerca de la aplicación específica, categoría de la aplicación, usuario u origen del ACC. Los gráficos de App Scope en **Monitor (Supervisar)App Scope** le ofrecen la posibilidad de realizar las siguientes tareas:

- Alternar entre los atributos de la leyenda para ver solamente los detalles del gráfico que desea revisar. La posibilidad de incluir o excluir datos del gráfico permite cambiar la escala y revisar los detalles más detenidamente.
- Hacer clic en un atributo del gráfico de barras y ver los detalles de las sesiones relacionadas en el ACC. Haga clic en un nombre de aplicación, una categoría de aplicación, un nombre de amenaza, una categoría de amenaza, una dirección IP de origen o una dirección IP de destino en cualquier gráfico de barras para filtrar el atributo y ver las sesiones relacionadas en el ACC.
- Exportar un gráfico o un mapa a PDF o como una imagen. Para garantizar la portabilidad y la visualización fuera de línea, puede exportar los gráficos y mapas como PDF o imágenes PNG.

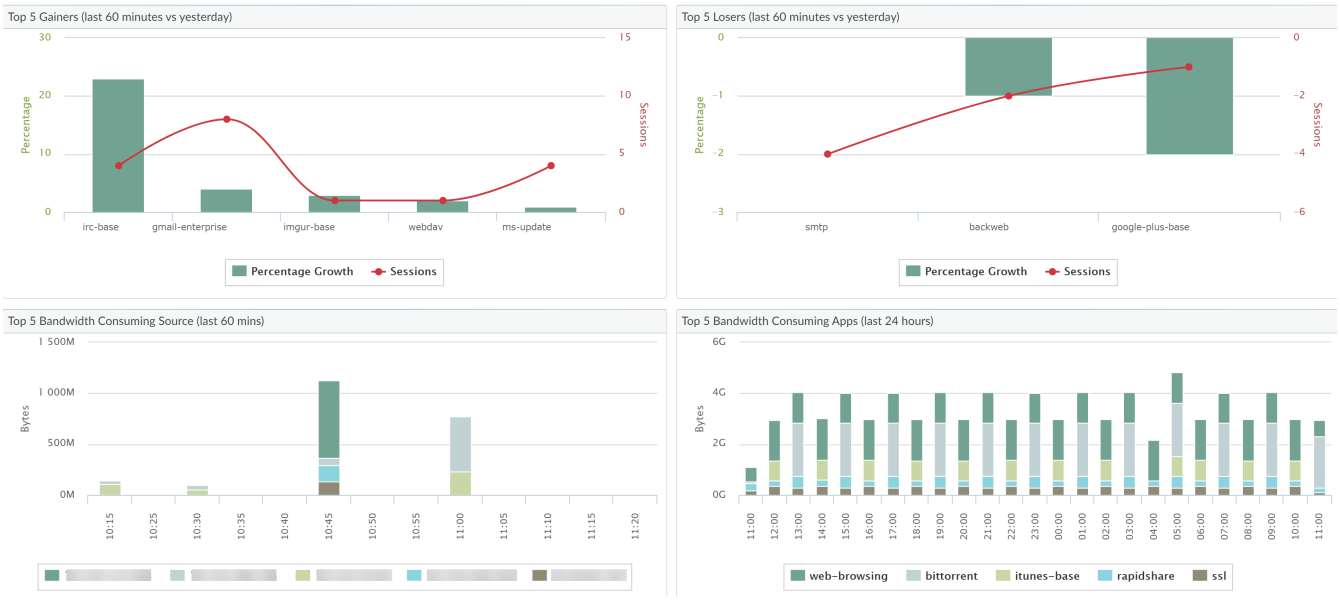
Los siguientes informes de Appscope están disponibles:

- Informe de resumen
- Informe del supervisor de cambios
- Informe del supervisor de amenazas
- Informe del mapa de amenazas
- Informe del supervisor de red
- Informe del mapa de tráfico

Informe de resumen

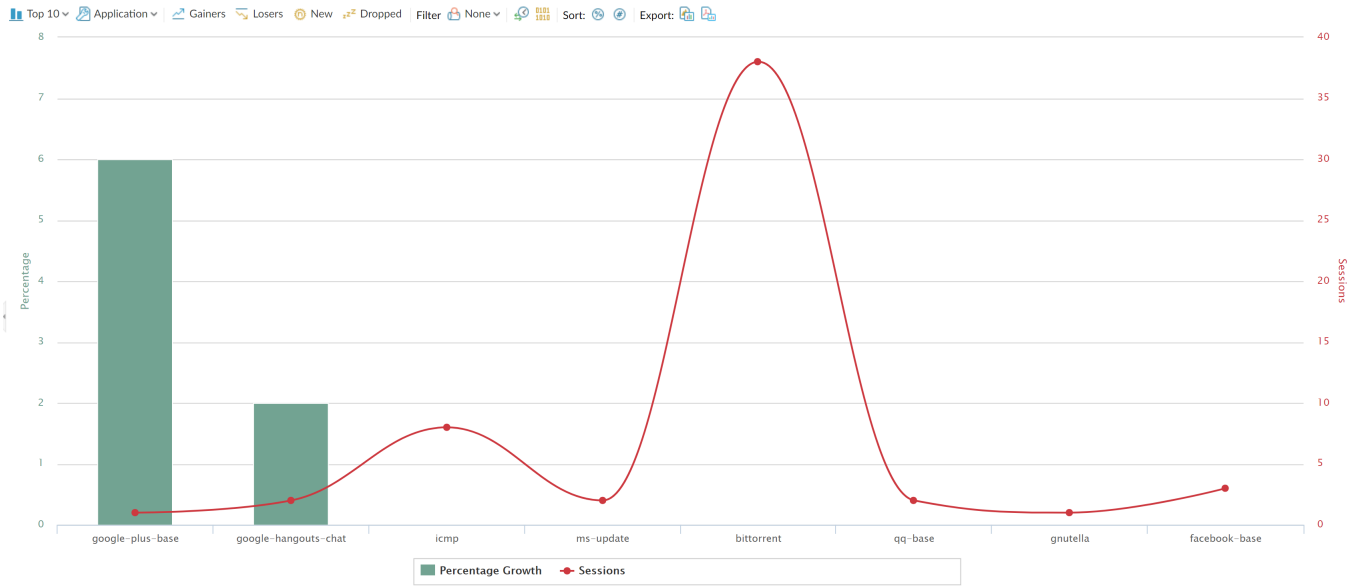
El informe de resumen de App Scope (**Monitor [Supervisar]** > **App Scope** > **Summary [Resumen]**) muestra gráficos de las cinco principales aplicaciones ganadoras, perdedoras y que consumen ancho de banda, categorías de aplicación, usuarios y orígenes.

© 2020 Palo Alto Networks, Inc.



Informe del supervisor de cambios

El informe del supervisor de cambios de App Scope (**Monitor [Supervisar]** > **App Scope [Alcance de la aplicación]** > **Change Monitor [Supervisor de cambios]**) muestra los cambios realizados en un período de tiempo específico. Por ejemplo, el siguiente gráfico muestra las principales aplicaciones más utilizadas en la última hora en comparación con el último periodo de 24 horas. Las principales aplicaciones se determinan por el recuento de sesiones y se ordenan por porcentajes.



El informe del supervisor de cambios contiene los siguientes botones y opciones.

Botón	Description (Descripción)
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.

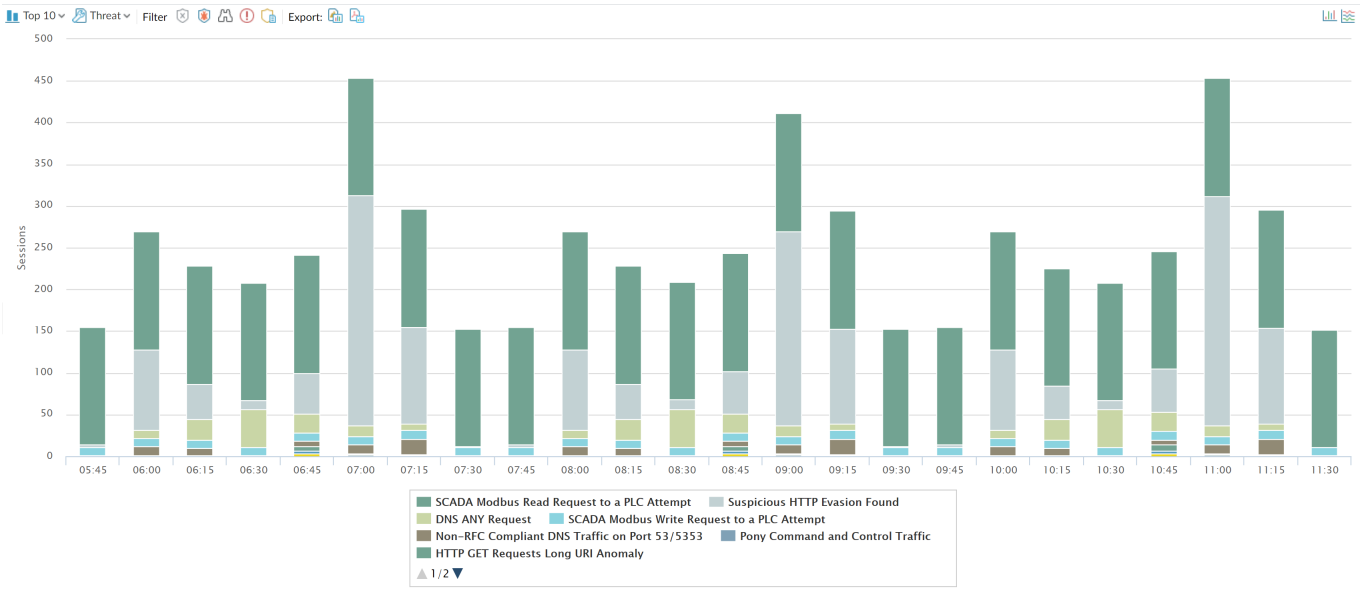
© 2020 Palo Alto Networks, Inc.

Botón	Description (Descripción)
Application (Aplicación)	Determina el tipo de elemento indicado: Aplicación, Categoría de aplicación, Origen o Destino.
Gainers (Ganadores)	Muestra mediciones de elementos que han ascendido durante el periodo de medición.
Losers (Perdedores)	Muestra mediciones de elementos que han descendido durante el periodo de medición.
New	Muestra mediciones de elementos que se han agregado durante el periodo de medición.
Descartado	Muestra mediciones de elementos que se han suspendido durante el periodo de medición.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el elemento seleccionado. None (Ninguno) muestra todas las entradas.
	Determina si mostrar información de sesión o byte.
Ordenar	Determina si ordenar entradas por porcentajes o incremento bruto.
Exportar	Exporta el gráfico como imagen .png o PDF.
Comparar	Especifica el periodo durante el que se realizaron las mediciones de cambio.

Informe del supervisor de amenazas

El informe del supervisor de amenazas de App Scope (**Monitor [Supervisor]** > **App Scope** > **Threat Monitor [Supervisor de amenazas]**) muestra un recuento de las principales amenazas durante el período de tiempo seleccionado. Por ejemplo, la siguiente ilustración muestra los 10 principales tipos de amenaza en las últimas 6 horas.

© 2020 Palo Alto Networks, Inc.



Cada tipo de amenaza está indicado con colores como se indica en la leyenda debajo del gráfico. El informe del supervisor de amenazas contiene los siguientes botones y opciones.

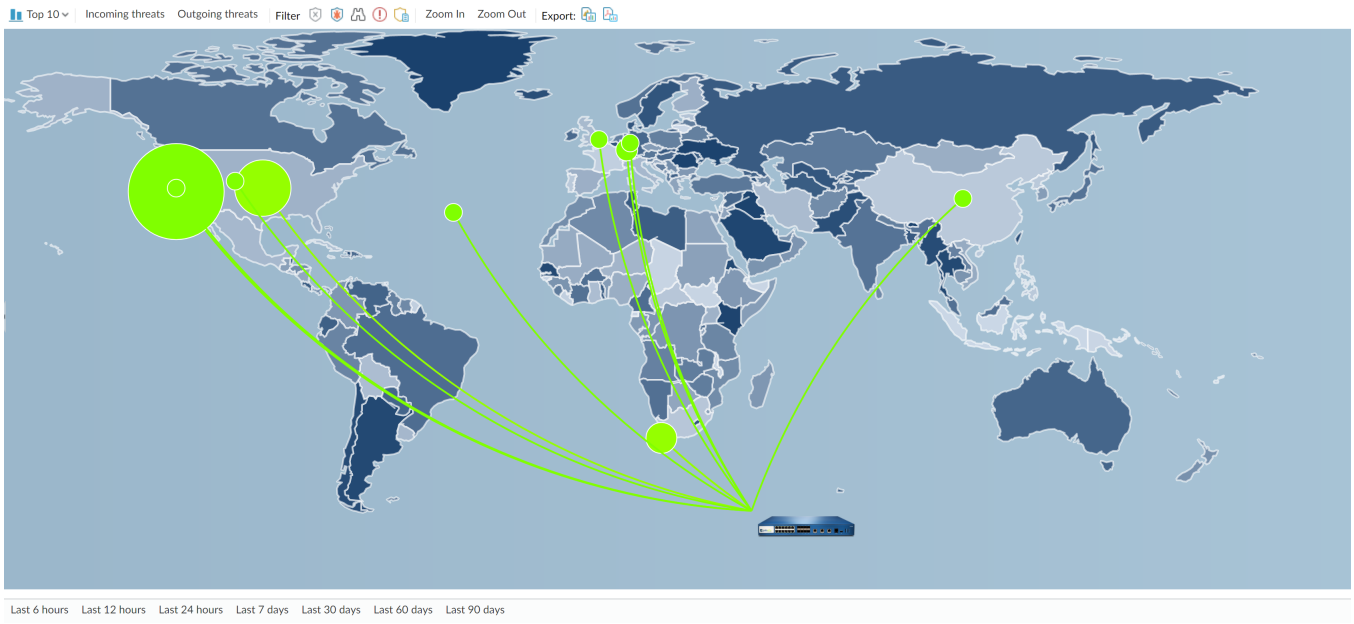
Botón	Description (Descripción)
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Threats (Amenazas)	Determina el tipo de elemento medido: Amenaza, Categoría de amenaza, Origen o Destino.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el tipo de elemento seleccionado.
	Determina si la información se presenta en un gráfico de columna apilado o un gráfico de área apilado.
Exportar	Exporta el gráfico como imagen .png o PDF.
	Especifica el periodo durante el que se realizaron las mediciones.

Informe del mapa de amenazas

El informe de mapa de amenazas de App Scope (**Monitor [Supervisar]** > **App Scope** > **Threat Map [Mapa de amenazas]**) muestra una vista geográfica de amenazas, que incluye la gravedad. Cada tipo de amenaza está indicado con colores como se indica en la leyenda debajo del gráfico.

El cortafuegos usa la geolocalización para crear mapas de amenazas. El cortafuegos se encuentra en la parte inferior de la pantalla del mapa de amenazas si no ha especificado las coordenadas de geolocalización (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]**, en la sección General Settings [Configuración general]) en el cortafuegos.

© 2020 Palo Alto Networks, Inc.



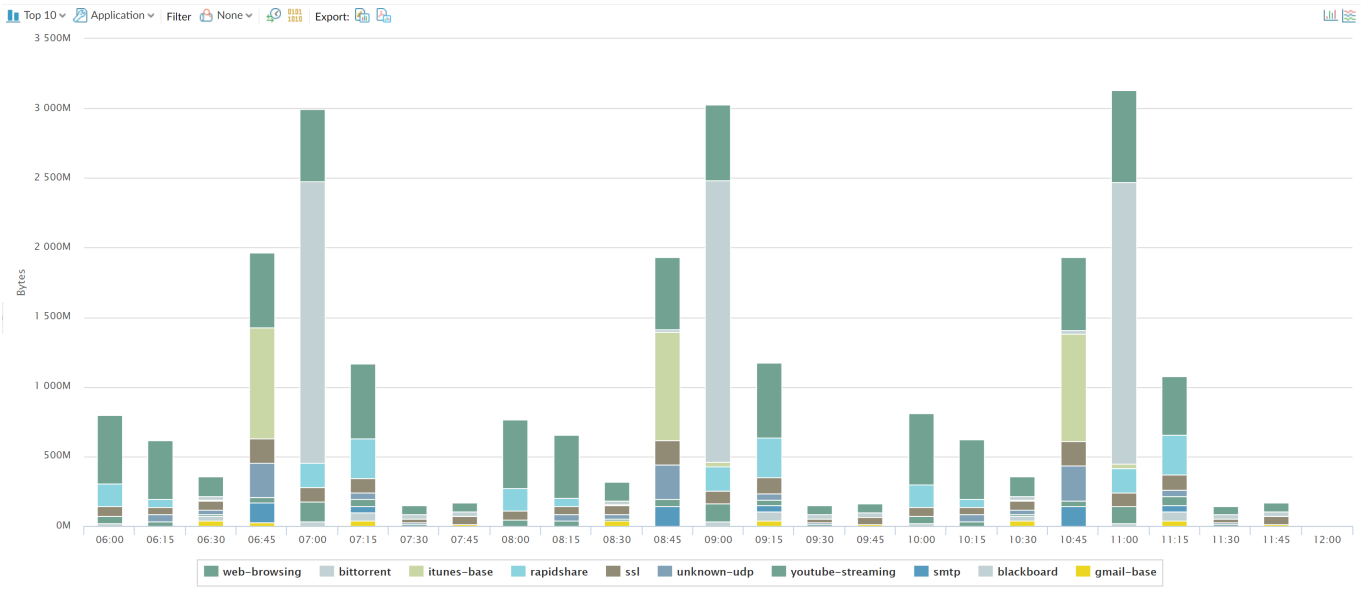
El informe del mapa de amenazas contiene los siguientes botones y opciones.

Botón	Description (Descripción)
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Amenazas entrantes	Muestra las amenazas entrantes.
Outdoing threats	Muestra las amenazas salientes.
Filtro	Aplica un filtro para mostrar únicamente el tipo de elemento seleccionado.
Acercar y alejar	Acerque y aleje el mapa.
Exportar	Exporta el gráfico como imagen .png o PDF.
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Indica el periodo durante el que se realizaron las mediciones.

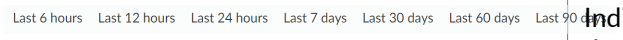
Informe del supervisor de red

El informe de supervisor de red de App Scope (**Monitor [Supervisar]** > **App Scope** > **Network Monitor [Supervisor de red]**) muestra el ancho de banda dedicado a diferentes funciones de red durante el período de tiempo especificado. Cada función de red está indicada con colores como se indica en la leyenda debajo del gráfico. Por ejemplo, la imagen siguiente muestra el ancho de banda de aplicación en los 7 últimos días basándose en la información de sesión.

© 2020 Palo Alto Networks, Inc.



El informe del supervisor de red contiene los siguientes botones y opciones.

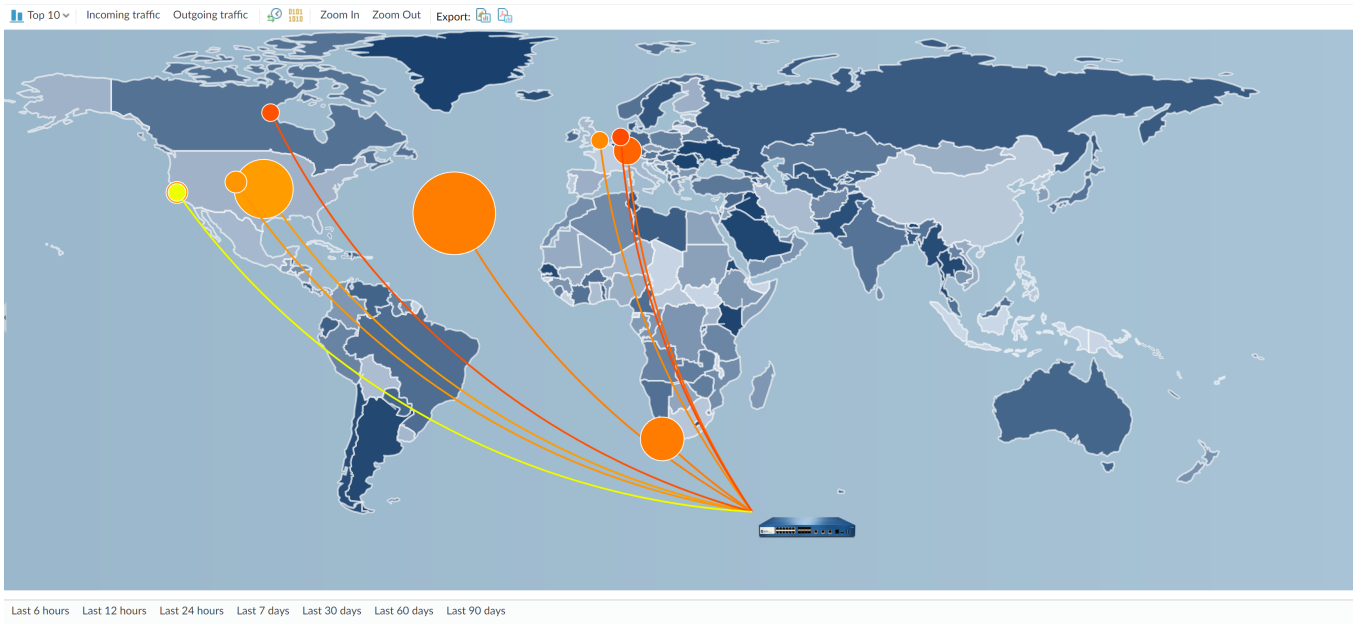
Botón	Description (Descripción)
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Application (Aplicación)	Determina el tipo de elemento indicado: Aplicación, Categoría de aplicación, Origen o Destino.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el elemento seleccionado. **None (Ninguno)** muestra todas las entradas.
	Determina si mostrar información de sesión o byte.
Exportar	Exporta el gráfico como imagen .png o PDF.
	Determina si la información se presenta en un gráfico de columna apilado o un gráfico de área apilado.
	Indica el periodo durante el que se realizaron las mediciones de cambio.

Informe del mapa de tráfico

El informe de mapa de tráfico de App Scope (**Monitor [Supervisar]** > **App Scope** > **Traffic Map [Mapa de tráfico]**) muestra una vista geográfica de los flujos de tráfico según las sesiones o los flujos.

El cortafuegos usa la geolocalización para crear mapas de tráfico. El cortafuegos se encuentra en la parte inferior de la pantalla del mapa de tráfico si no ha especificado las coordenadas de geolocalización (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** sección General Settings [Configuración general]) en el cortafuegos.

© 2020 Palo Alto Networks, Inc.



Cada tipo de tráfico está indicado con colores como se indica en la leyenda debajo del gráfico. El informe del mapa de tráfico contiene los siguientes botones y opciones.

Botones	Description (Descripción)
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Amenazas entrantes	Muestra las amenazas entrantes.
Amenazas salientes	Muestra las amenazas salientes.
	Determina si mostrar información de sesión o byte.
Acercar y alejar	Acerque y aleje el mapa.
Exportar	Exporta el gráfico como imagen .png o PDF.
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Indica el periodo durante el que se realizaron las mediciones de cambio.

© 2020 Palo Alto Networks, Inc.

Use el motor de correlación automatizada.

El motor de correlación automatizado se encuentra en una herramienta de análisis que usa los logs en el cortafuegos para detectar los eventos útiles en su red. El motor correlaciona una serie de eventos de amenazas relacionado que, cuando se combina, indica un host que puede estar comprometido en su red u otra conclusión de mayor nivel. Señala áreas de riesgo, como hosts en riesgo en la red, le permite evaluar el riesgo y desarrollar acciones para evitar la explotación de los recursos de red. El motor de correlación automatizado usa *objetos de correlación* para analizar los logs en busca de patrones cuando se produce una coincidencia, y genera un *evento correlacionado*.

Los siguientes modelos admiten el motor de correlación automatizado:

- *Panorama: dispositivos M-Series y dispositivos virtuales.*
- *Cortafuegos PA-7000 Series*
- *Cortafuegos PA-5200 Series*
- *Cortafuegos PA-3200 Series*

- Conceptos del motor de correlación automatizada
- Visualización de los objetos de correlación
- Interpretación de eventos correlacionados
- Uso del widget de los hosts en riesgo en el ACC

Conceptos del motor de correlación automatizada

El motor de correlación automatizado usa *objetos de correlación* para analizar los logs en busca de patrones cuando se produce una coincidencia, y genera un *evento correlacionado*.

- Objeto de correlación
- Eventos correlacionados

Objeto de correlación

Un objeto de correlación es un archivo de definición que especifica patrones para la búsqueda de coincidencias, orígenes de datos que se usarán para las búsquedas y el periodo durante el que buscarán dichos patrones. Un patrón es una estructura booleana de condiciones que consulta los siguientes orígenes de datos (o logs) en el cortafuegos: estadísticas de aplicación, tráfico, resumen de tráfico, resumen de amenazas, amenazas, filtrado de datos y filtrado de URL. Cada patrón tiene una puntuación de gravedad, y un umbral para el número de veces que el patrón debe ocurrir en un límite de tiempo definido para indicar una actividad malintencionada. Cuando se produce una coincidencia con un patrón, se registra un evento de correlación.

Un objeto de correlación puede conectar eventos de red aislados y buscar patrones que indiquen un evento más significativo. Estos objetos identifican patrones de tráfico sospechosos y anomalías de red, incluida la actividad IP sospechosa, actividad de comando y control conocida, explotaciones de vulnerabilidad conocidas o actividad de botnet que, cuando se correlaciona, indica que hay una alta probabilidad de que un host de la red esté en riesgo. Los objetos de correlación se han definido y desarrollado por el equipo de investigación de amenazas de Palo Alto Networks y se han distribuido con las actualizaciones dinámicas semanales al cortafuegos y a Panorama. Para obtener nuevos objetos de correlación, el cortafuegos debe tener una licencia de Threat Prevention. Panorama requiere una licencia de compatibilidad para obtener las actualizaciones.

Los patrones definidos en un objeto de correlación pueden ser estáticos y dinámicos. Los objetos correlacionados que incluyen los patrones observados en WildFire son dinámicos y pueden correlacionar patrones de malware detectados por WildFire con la actividad de comando y control iniciada por el host al

© 2020 Palo Alto Networks, Inc.

que estaba dirigido el malware de su red o la actividad detectada por un extremo protegido por capturas en Panorama. Por ejemplo, cuando un host envía un archivo a la nube de WildFire y el veredicto es que es malintencionado, el objeto de correlación busca otros hosts o clientes en la red que muestren el mismo comportamiento visto en la nube. Si la muestra de malware ha realizado una consulta DNS y navegado hasta un dominio de malware, el objeto de correlación analizará los logs en busca de un evento similar. Cuando la actividad de un host coincide con el análisis de la nube, se registra un evento correlacionado de alta gravedad.

Eventos correlacionados

Un evento correlacionado se registra cuando los patrones y umbrales definidos en un objeto de correlación coincide con los patrones de tráfico de su red. Para Interpretación de eventos correlacionados y la visualización de una pantalla gráfica de los eventos, consulte Uso del widget de los hosts en riesgo en el ACC.

Visualización de los objetos de correlación

Puede ver los objetos de correlación disponibles actualmente en el cortafuegos.

STEP 1 | Seleccione **Monitor (Supervisar)** > **Automated Correlation Engine (Motor de correlación automatizada)** > **Correlation Objects (Objetos de correlación)**. Todos los objetos de la lista están habilitados de manera predeterminada.

TITLE	CATEGORY	STATE	DESCRIPTION
Multiple User from One Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects multiple account abuse from a possibly compromised endpoint
WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
WildFire and Traps ESM Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware.
Single Account and Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects activity from a possibly compromised user account from a single endpoint
Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Single Account 1 FA Multiple Endpoints Credential Timeouts	credential-theft-abuse	active	This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Single Account and Endpoint MFA Credential Timeout	credential-theft-abuse	active	This correlation object detects timedout MFA authentication attempts from a single endpoint using single account
Multiple Endpoint MFA Credential Timeout Abuse	credential-theft-abuse	active	This correlation object detects timed out second factor authentications from multiple endpoints using a single user account
Multiple Endpoint MFA Credential Abuse	credential-theft-abuse	active	This correlation object detects activity from multiple endpoints using a single user account
Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
Single Account 1 FA Credential Abuse	credential-theft-abuse	active	This correlation object detects timed out first factor authentications from an endpoint using a single user account

STEP 2 | Visualice los detalles de cada objeto de correlación. Cada objeto ofrece la siguiente información:

- **Name (Nombre)** y **Title (Título)**: el nombre y el título indican el tipo de actividad que detecta el objeto de correlación. La columna Nombre está oculta a la vista de manera predeterminada. Para ver la definición del objeto, muestre la columna y haga clic en el enlace del nombre.
- **ID**: un número único que identifica el objeto de correlación; esta columna también está oculta de manera predeterminada. Los ID están en la serie 6000.
- **Category (Categoría)**: una clasificación del tipo de amenaza o daño que supone para la red, el usuario o el host. Por ahora, todos los objetos identifican los hosts comprometidos en la red.
- **State (Estado)**: indica si el objeto de correlación está habilitado (activo) o deshabilitado (inactivo). Todos los objetos de la lista están habilitados de manera predeterminada, por lo tanto están activos. Como estos objetos se han basado en los datos de inteligencia de amenazas y los ha definido el equipo de investigación de amenazas de Palo Alto Networks, mantenga los objetos activos para poder monitorizar y detectar una actividad malintencionada en su red.
- **Description (Descripción)**: especifica las condiciones de coincidencia que el cortafuegos o Panorama utilizará para analizar los logs. Describe la secuencia de condiciones que se comparan para identificar

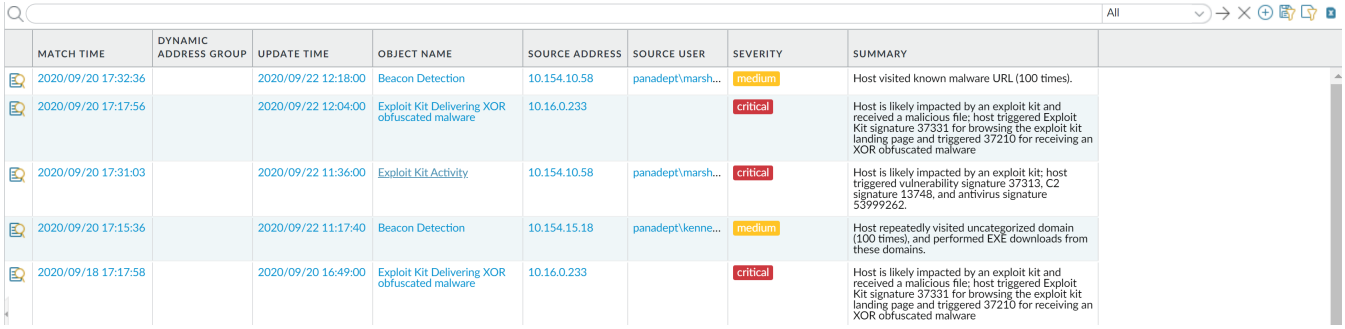
© 2020 Palo Alto Networks, Inc.

la aceleración o progresión de la actividad malintencionada o el comportamiento sospechoso del host. Por ejemplo, el objeto **Compromise Lifecycle (Alterar ciclo de vida)** detecta un host implicado en un ciclo de vida de ataques completo en una progresión de tres pasos que comienza con una actividad de análisis o sondeo, continúa con el aprovechamiento de la vulnerabilidades y concluye con el contacto con la red con un dominio malintencionado conocido.

Para obtener más información, consulte Conceptos del motor de correlación automatizada y Use el motor de correlación automatizada..

Interpretación de eventos correlacionados

Puede visualizar y analizar los logs generados para cada evento correlacionado en la pestaña **Monitor (Supervisar)** > **Automated Correlation Engine (Motor de correlación automatizada)** > **Correlated Events (Eventos correlacionados)**



MATCH TIME	DYNAMIC ADDRESS GROUP	UPDATE TIME	OBJECT NAME	SOURCE ADDRESS	SOURCE USER	SEVERITY	SUMMARY
2020/09/20 17:32:36		2020/09/22 12:18:00	Beacon Detection	10.154.10.58	panadept\marsh...	medium	Host visited known malware URL (100 times).
2020/09/20 17:17:56		2020/09/22 12:04:00	Exploit Kit Delivering XOR obfuscated malware	10.16.0.233		critical	Host is likely impacted by an exploit kit and received a malicious file; host triggered Exploit Kit signature 37331 for browsing the exploit kit landing page and triggered 37210 for receiving an XOR obfuscated malware
2020/09/20 17:31:03		2020/09/22 11:36:00	Exploit Kit Activity	10.154.10.58	panadept\marsh...	critical	Host is likely impacted by an exploit kit; host triggered vulnerability signature 37313, C2 signature 13748, and antivirus signature 53999262.
2020/09/20 17:15:36		2020/09/22 11:17:40	Beacon Detection	10.154.15.18	panadept\kenne...	medium	Host repeatedly visited uncategorized domain (100 times), and performed EXE downloads from these domains.
2020/09/18 17:17:58		2020/09/20 16:49:00	Exploit Kit Delivering XOR obfuscated malware	10.16.0.233		critical	Host is likely impacted by an exploit kit and received a malicious file; host triggered Exploit Kit signature 37331 for browsing the exploit kit landing page and triggered 37210 for receiving an XOR obfuscated malware

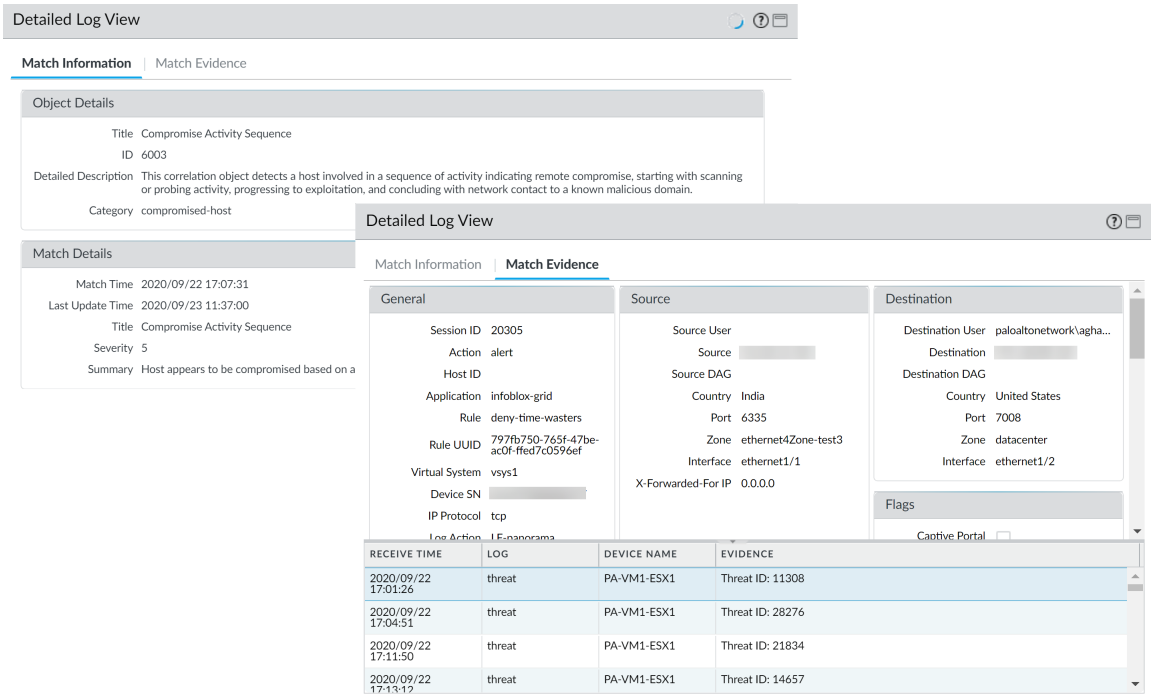
Eventos correlacionados incluye los siguientes detalles:

Campo	Description (Descripción)
Hora de coincidencias	La hora a la que el objeto de correlación activó una coincidencia.
Hora de actualización	La hora en la que evento se actualizó por última vez con evidencia sobre la coincidencia. Cuando el cortafuegos recopila pruebas sobre el patrón o secuencia de eventos definidos en un objeto de correlación, la marca de tiempo del log de evento correlacionado se actualiza.
Nombre de objeto	El nombre del objeto de correlación que activó la coincidencia.
Dirección de origen	La dirección IP del usuario/dispositivo de su red desde la que se originó el tráfico.
Source User (Usuario de origen)	La información del usuario y grupo de usuarios del servidor de directorios, si User-ID está habilitado.
Gravedad *Para configurar el cortafuegos o Panorama para enviar*	La gravedad indica la urgencia y el impacto de la coincidencia. El nivel de gravedad indica la extensión del daño o el patrón de progresión y la frecuencia de la incidencia. Dado que los objetos de correlación se centran en la detección de amenazas, los eventos correlacionados suelen relacionarse con la identificación de hosts en riesgo en la red y el nivel de gravedad tiene las siguientes implicaciones: • **Critical**: confirma que se ha comprometido la seguridad de un host basándose en eventos correlacionados que indican un patrón en aumento. Por ejemplo, se registra un evento crítico cuando un host

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
alertas usando un correo electrónico, SNMP o mensajes syslog para un nivel de gravedad deseado, consulte Uso de servicios externos para la monitorización.	que ha recibido un archivo considerado malintencionado por WildFire muestra la misma actividad de comando y control observada en ese archivo malintencionado dentro del espacio aislado de WildFire. • **High**: indica que hay una probabilidad muy alta de que un host vea comprometida su seguridad en función de una correlación entre varios eventos de amenaza, como el malware detectado en cualquier punto de la red que coincida con la actividad de comando y control generada por un host concreto. • **Medium**: indica que hay cierta probabilidad de que un host vea comprometida su seguridad en función de la detección de uno o varios eventos sospechosos, como las visitas repetidas a URL consideradas malintencionadas, lo que sugiere la existencia de una actividad de comando y control planeada. • **Low**: indica la posibilidad de que un host vea comprometida su seguridad en función de la detección de uno o varios eventos sospechosos, como el ingreso en una URL considerada malintencionada o un dominio DNS dinámico. • **Informational**: detecta un evento que podría resultar útil en conjunto para identificar una actividad sospechosa, pero un evento por separado no necesariamente es significativo.
Resumen	Una descripción que resume las pruebas recopiladas en el evento correlacionado.

Haga clic en el icono para consultar la vista detallada de log, que incluye todas las pruebas de una coincidencia:

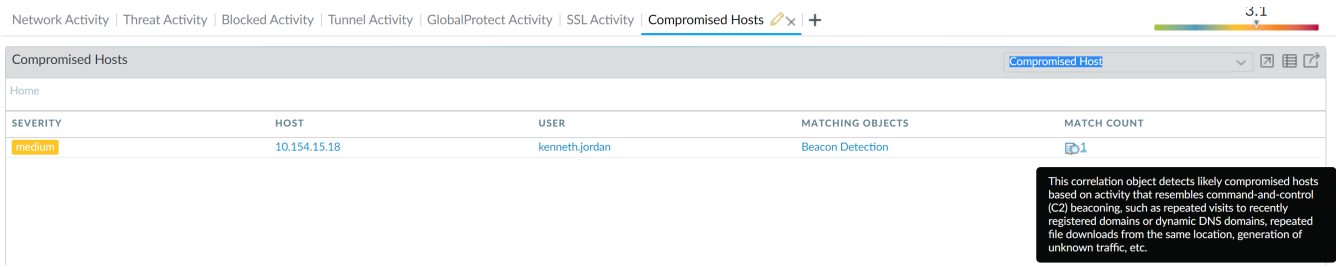


© 2020 Palo Alto Networks, Inc.

Pestaña	Description (Descripción)
Información de coincidencias	Detalles de objeto: Presenta la información sobre el Objeto de correlación que activó la coincidencia.
	Detalles de coincidencia: Un resumen de los detalles de coincidencia que incluye la hora de la coincidencia, la última hora de actualización de la prueba de coincidencia, la gravedad del evento y un resumen de eventos.
Evidencia de coincidencias	Presenta todas las pruebas que corroboran el evento correlacionado. Enumera la información detallada en las pruebas recopiladas de cada sesión.

Uso del widget de los hosts en riesgo en el ACC

El widget de hosts en riesgo en **ACC** > **Threat Activity (Actividad de amenazas)** acumula los Eventos correlacionados y los ordena por gravedad. Muestra el usuario/dirección IP de origen que activó el evento, el objeto de correlación que se compara y el número de veces que se hizo coincidir el objeto. Use el enlace de recuento de coincidencias para cambiar a los detalles de pruebas de coincidencias.



Si desea más información, consulte Use el motor de correlación automatizada. y Uso del Centro de control de aplicaciones.

© 2020 Palo Alto Networks, Inc.

Realización de capturas de paquetes

Todos los cortafuegos de Palo Alto Networks le permiten tomar capturas de paquetes (pcap) del tráfico que atraviesa la interfaz de gestión y las interfaces de red del cortafuegos. Cuando se toman capturas de paquetes en el plano de datos, puede tener que usar la Deshabilitación de descarga de hardware para garantizar que el cortafuegos capture todo el tráfico.

La captura de paquetes puede hacer un uso muy intensivo de la CPU y puede degradar el rendimiento del cortafuegos. Utilice esta función únicamente cuando sea necesario y asegúrese de desactivarla cuando haya recopilado los paquetes necesarios.

- Tipos de captura de paquetes
- Deshabilitación de descarga de hardware
- Captura de paquetes personalizada
- Captura de paquetes de amenazas
- Tome una captura de paquetes de aplicaciones
- Captura de paquetes en la interfaz de gestión

Tipos de captura de paquetes

Puede habilitar distintos tipos de capturas de paquetes en función de lo que deba hacer:

- **Captura de paquetes personalizada**: el cortafuegos captura paquetes para todo el tráfico o el tráfico basado en los filtros que defina. Por ejemplo, puede configurar el cortafuegos para que solamente capture paquetes destinados o procedentes de una dirección IP o un puerto de origen y destino específicos. Entonces, puede usar las capturas de paquetes para solucionar los problemas relacionados con la red o para reunir los atributos de aplicación, lo que le permitirá escribir firmas de aplicaciones personalizadas o solicitar una firma de aplicación de Palo Alto Networks. Consulte Captura de paquetes personalizada.
- **Captura de paquetes de amenazas**: El cortafuegos captura paquetes cuando detecta un virus, spyware o una vulnerabilidad. Puede habilitar esta función en los perfiles de seguridad Antivirus, Antispyware y Protección de vulnerabilidades. Aparecerá un enlace para ver o exportar las capturas de paquetes en la segunda columna del log de amenazas. Estas capturas de paquetes le ofrecen el contexto de una amenaza para ayudarle a determinar si un ataque ha tenido éxito o para obtener más información sobre los métodos utilizados por un atacante. También puede enviar este tipo de pcap a Palo Alto Networks para volver a analizar una amenaza si cree que ha arrojado un falso positivo o un falso negativo. Consulte Captura de paquetes de amenazas.
- **Captura de paquetes de aplicación**: El cortafuegos captura paquetes en función de la aplicación y filtros específicos que defina. Aparecerá un enlace para ver o exportar las capturas de paquetes en la segunda columna de los logs de tráfico para el tráfico que coincide con la regla de captura de paquetes. Consulte Tome una captura de paquetes de aplicaciones.
- **Captura de paquetes de la interfaz de gestión**: el cortafuegos captura paquetes en la interfaz de gestión (MGT). Las capturas de paquetes resultan útiles para solucionar los problemas de servicios que atraviesan la interfaz, como la autenticación de gestión de cortafuegos en Servicios de autenticación externos, las actualizaciones de software y contenido, el reenvío de logs, la comunicación con servidores SNMP y las solicitudes de autenticación para GlobalProtect y el portal de autenticación. Consulte Captura de paquetes en la interfaz de gestión.
- **Captura de paquetes de eventos de GTP**: el cortafuegos captura un evento único del protocolo de túnel del servicio general de paquetes vía radio (general packet radio service [GPRS] tunneling protocol, GTP), como GTP en GTP, duplicación de direcciones IP de los usuarios finales y mensajes GTP anómalos, para facilitar la solución de problemas de GTP a los operadores de redes móviles. Habilite la captura de paquetes en un perfil de protección de red móvil.

© 2020 Palo Alto Networks, Inc.

Deshabilitación de descarga de hardware

Las capturas de paquetes en el tráfico que pasa a través de los puertos de datos de la red en un cortafuegos Palo Alto Networks se realizan en la CPU del plano de datos. Para capturar el tráfico que pasa a través de la interfaz de gestión, debe consultar Cómo tomar una captura de paquetes en la interfaz de gestión, en cuyo caso, la captura de paquetes se realiza en el plano de gestión.

Cuando una captura de paquete se realiza en el plano de datos, el filtro de captura de paquetes se utiliza de manera diferente durante la etapa de entrada, en comparación con las etapas de captura de cortafuegos, descarte y salida. La etapa de entrada utiliza el filtro de captura de paquetes para copiar los paquetes individuales que coinciden con el filtro al archivo de captura. Los paquetes que fallan las comprobaciones de análisis de paquetes se descartan antes de que se realice la captura. Las etapas de cortafuegos, descarte y salida utilizan el mismo filtro de captura de paquetes para marcar todas las sesiones nuevas que coinciden con el filtro. Debido a que cada sesión, según se registra en las tablas de la sesión, identifica las conexiones de cliente a servidor y de servidor a cliente, el tráfico, en cualquier dirección, que coincida con la sesión marcada se copiará en los archivos de la etapa de cortafuegos y de la etapa de transmisión. De igual modo, el tráfico descartado (etapa posterior a la recepción) en cualquier dirección que coincide con una sesión marcada se copiará en el archivo de captura de la etapa de descarte.

En los modelos de cortafuegos que incluyen un procesador de red, el tráfico que coincide con ciertos criterios predeterminados por Palo Alto Networks pueden descargarse para que los gestione el procesador de red. Este tráfico descargado no alcanzará la CPU del plano de datos y, por lo tanto, no se capturará. Para capturar tráfico descargado, debe utilizar la CLI para apagar la función de descarga de hardware.

Los tipos comúnes de tráfico que puede descargarse incluyen el tráfico SSL y SSH no descifrado (los cuales al estar cifrados no se pueden examinar eficientemente más que durante la configuración inicial de sesiones SSL/SSH), los protocolos de red (como OSPF, BGP, RIP) y el tráfico que coincide con una política de anulación de aplicaciones. Algunos tipos de tráfico nunca se descargarán, como ARP, todo el tráfico no IP, IPSec y las sesiones VPN. Los paquetes individuales SYN, FIN y RST, incluso cuando el tráfico de la sesión se descargó, nunca se descargarán y siempre pasarán a través de la CPU del plano de datos cuando se los reconozca como tales en el procesador de la red.

La descarga de hardware es compatible con los siguientes cortafuegos: Cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series.

Si se deshabilita la descarga de hardware, es posible que el uso de la CPU del plano de datos aumente. Si el uso de la CPI del plano de datos ya es alto, puede querer programar una ventana de mantenimiento antes de deshabilitar la descarga de hardware.

STEP 1 | Deshabilitar la descarga de hardware ejecutando el siguiente comando de la CLI:

```
admin@PA-7050>set session offload no
```

STEP 2 | Cuando el cortafuegos capture el tráfico requerido, habilite la descarga de hardware ejecutando el siguiente comando de la CLI:

```
admin@PA-7050>set session offload yes
```

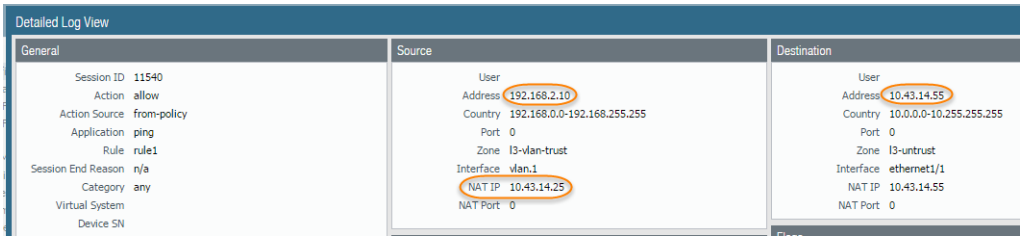

© 2020 Palo Alto Networks, Inc.

Captura de paquetes personalizada

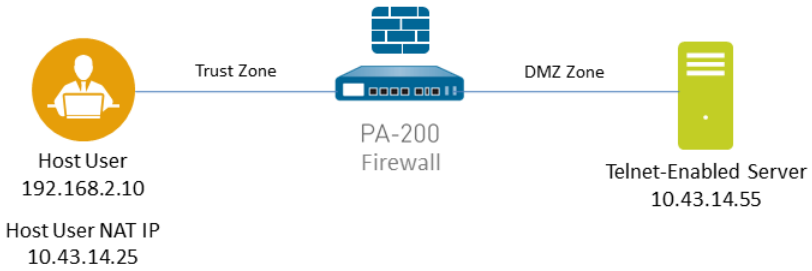
Las capturas de paquetes personalizadas le permiten definir el tráfico que capturará el cortafuegos. Para asegurarse de capturar todo el tráfico, puede tener que usar la Deshabilitación de descarga de hardware.

STEP 1 | Antes de iniciar una captura de paquetes, identifique los atributos del tráfico que desea capturar.

Por ejemplo, para determinar la dirección IP de origen, la dirección IP de NAT de origen y la dirección IP de destino para el tráfico entre dos sistemas, realice un ping desde el sistema de origen hasta el sistema de destino. Cuando el ping se haya completado, vaya a **Monitor (Supervisar)** > **Traffic (Tráfico)** y ubique el log de tráfico para los dos sistemas. Haga clic en el icono **Detailed Log View** ubicado en la primera columna del log y anote la dirección de origen, la IP NAT de origen y la dirección de destino.



El siguiente ejemplo muestra cómo usar una captura de paquete para solucionar los problemas de una conectividad Telnet desde un usuario en la zona de confianza a un servidor en la zona DMZ.



STEP 2 | Defina los filtros de captura de paquetes para que el cortafuegos solo capture el tráfico en el que está interesado.

© 2020 Palo Alto Networks, Inc.

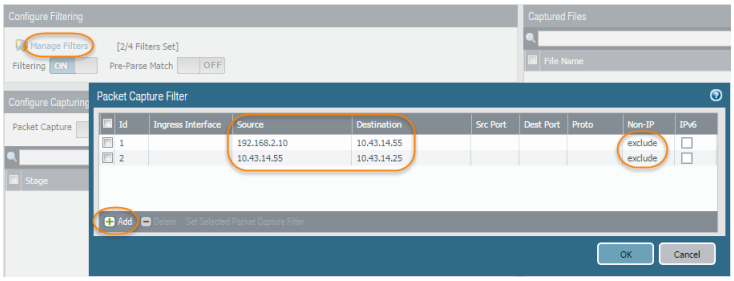
El uso de filtros le facilitará la búsqueda de la información que necesita en la captura de paquete y reducirá la potencia de procesamiento requerida para que el cortafuegos realice la captura de paquetes. Para capturar todo el tráfico, no defina filtros y deje la opción de filtro desactivada.

Por ejemplo, si ha configurado NAT en el cortafuegos, deberá aplicar dos filtros. El primero filtra según la dirección IP de origen preNAT a la dirección IP de destino, y el segundo filtra el tráfico de un servidor de destino a la dirección IP NAT de origen.

1. Seleccione **Monitor (Supervisar)** > **Packet Capture (Captura de paquetes)**.
2. Haga clic en **Clear All Settings** en la parte inferior de la ventana para borrar cualquier ajuste de captura existente.
3. Haga clic en **Manage Filters** y después en **Add**.
4. Seleccione **Id** 1 y en el campo **Source (Origen)**, escriba la dirección IP de origen en la que está interesado y en el campo **Destination (Destino)** escriba una dirección IP de destino.

   Por ejemplo, escriba la dirección IP de origen `192.168.2.10` y la dirección IP de destino `10.43.14.55`. Para filtrar aún más la captura, defina **Non-IP** como **exclude** para excluir el tráfico no IP, tal como el tráfico de difusión.
5. Seleccione **Add (Añadir)** para añadir el segundo filtro y seleccione **Id** 2.

   Por ejemplo, en el campo **Source**, escriba `10.43.14.55` y en el campo **Destination** escriba `10.43.14.25`. En el menú desplegable **Non-IP**, seleccione **exclude**.



6. Haga clic en **OK (Aceptar)**.

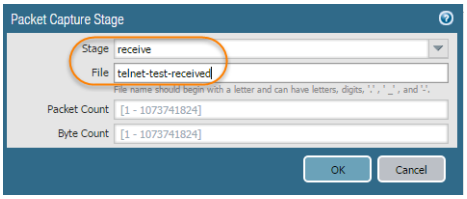
STEP 3 | Defina **Filtering** como **On**.

STEP 4 | Especifique la etapa del tráfico que activa la captura de paquetes y el nombre de archivo que se va a usar para almacenar el contenido capturado. Si desea una definición de cada etapa, haga clic en el icono **Help (Ayuda)** en la página de captura de paquetes.

Por ejemplo, para configurar todas las etapas de capturas de paquetes y definir un nombre de archivo para cada etapa, realice el siguiente procedimiento:

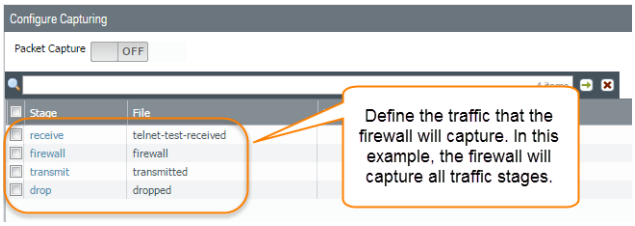
1. Seleccione **Add** para añadir una **Stage** a la configuración de captura de paquetes y defina un nombre de archivo en **File** para la captura de paquetes resultante.

   Por ejemplo, seleccione **receive (recibir)** como **Stage (Etapa)** y defina el nombre de archivo en **File (Archivo)** como telnet-test-received.



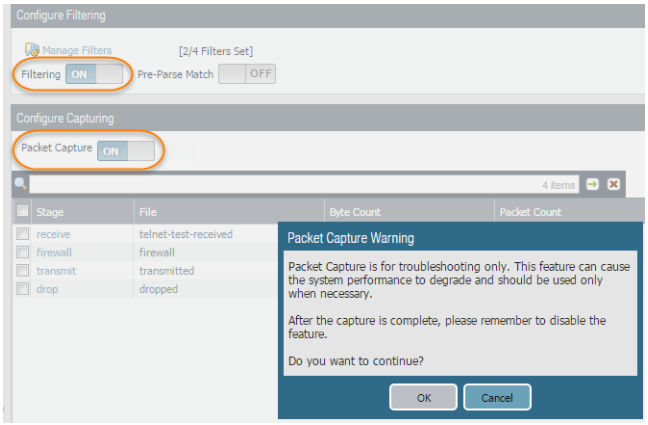
2. Seleccione nuevamente **Add (Añadir)** y luego añada cada **Stage (Etapa)** que desee capturar (**receive [recibir]**, **firewall [cortafuegos]**, **transmit [transmitir]** y **drop [descartar]**) y defina un nombre de archivo único en **File (Archivo)** para cada etapa.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Defina **Packet Capture (Captura de paquete)** como **ON (Activada)**.

El cortafuegos o dispositivo le advierte que el rendimiento del sistema puede reducirse; acepte la advertencia haciendo clic en **OK (Aceptar)**. Si define filtros, la captura de paquetes debe afectar poco en el rendimiento, aunque siempre debe definir como **Off** la captura de paquetes después de que el cortafuegos capture los datos que desea analizar.

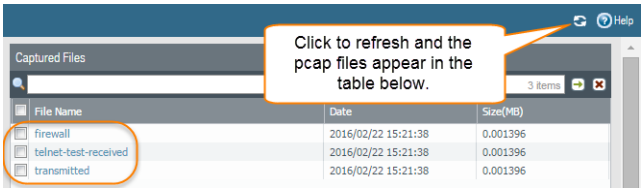


STEP 6 | Genera tráfico que coincide con los filtros que haya definido.

Para este ejemplo, genere el tráfico a partir del sistema de origen en el servidor con Telnet ejecutando el siguiente comando desde el sistema de origen (192.168.2.10):

```
telnet 10.43.14.55
```

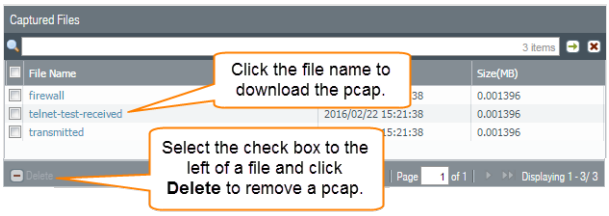
STEP 7 | Defina la captura de paquetes como **OFF** y haga clic en el icono actualizar para ver los archivos de captura de paquetes.



Observe que, en este caso, no se han perdido paquetes, de modo que el cortafuegos no ha creado un archivo para la etapa de colocación.

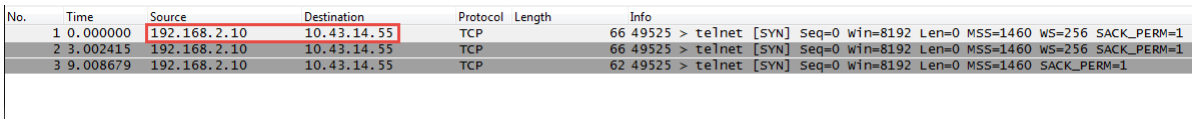
STEP 8 | Descargue las capturas de paquetes haciendo clic en el nombre de archivo de la columna Nombre de archivo.

© 2020 Palo Alto Networks, Inc.



STEP 9 | Visualice los archivos de captura de paquetes con un analizador de paquetes de red.

En este ejemplo, la captura de paquete .pcap recibida muestra una sesión de Telnet fallida desde el sistema de origen en 192.168.2.10 al servidor con Telnet en 10.43.14.55. El sistema de origen envió la solicitud de Telnet al servidor, pero este no respondió. En este ejemplo, puede que el servidor no tenga Telnet habilitado, por lo que debe consultar el servidor.



STEP 10 | Habilite el servicio Telnet en el servidor de destino (10.43.14.55) y active la captura de paquetes para tomar una nueva captura de paquetes.

STEP 11 | Genera tráfico que activará la captura de paquetes.

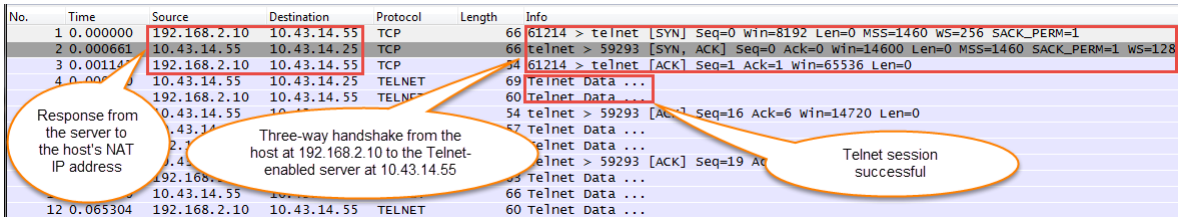
Ejecute de nuevo la sesión Telnet desde el sistema de origen al servidor con Telnet habilitado.

```
telnet 10.43.14.55
```

STEP 12 | Descargue y abra el archivo .pcap recibido y visualícelo usando un analizador de paquetes de red.

La siguiente captura de paquetes ahora muestra una sesión de Telnet fallida desde el usuario host en 192.168.2.10 al servidor con Telnet en 10.43.14.55.

También verá la dirección NAT 10.43.14.25. Cuando el servidor responda, lo hará a la dirección NAT. Puede ver que la sesión tiene éxito como se indica en el protocolo de tres direcciones entre el host y el servidor y entonces verá los datos de Telnet.



Captura de paquetes de amenazas

Para configurar al cortafuegos para que capture paquetes (pcap) cuando detecte una amenaza, habilite la opción de captura de paquetes en los perfiles de seguridad de antivirus, antispyware y protección de vulnerabilidad.

STEP 1 | Habilite la opción de captura de paquetes en el perfil de seguridad.

© 2020 Palo Alto Networks, Inc.

Algunos perfiles de seguridad le permiten definir una captura de paquete único o una captura extendida. Si selecciona la captura extendida, defina la longitud de la captura. Esto permitirá que el cortafuegos capture más paquetes para ofrecer el contexto adicional relacionado con la amenaza.

Si se permite la acción para una amenaza determinada, el cortafuegos no activa un log de amenazas y no captura paquetes. Si la acción es de alerta, puede configurar la captura de paquetes en un paquete único o una captura extendida. Todas las acciones de bloqueo (acciones de descarte, bloqueo y reinicio) capturan un solo paquete. El paquete de contenido del dispositivo determina la acción predeterminada.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** y habilite la opción de captura de paquetes para los perfiles admitidos como se indica a continuación:
   - **Antivirus**: seleccione un perfil antivirus personalizado y, en la pestaña **Antivirus**, seleccione la casilla de verificación **Packet Capture (Captura de paquetes)**.
   - **Antispyware**: seleccione un perfil antispyware personalizado, haga clic en la pestaña **DNS Signatures (Firmas DNS)** y, en la lista desplegable **Packet Capture (Captura de paquete)**, seleccione **single-packet (paquete único)** o **extended-capture (captura extendida)**.
   - **Vulnerability Protection**: seleccione un perfil de protección de vulnerabilidades personalizado y, en la pestaña **Rules**, haga clic en **Add** para añadir una nueva regla o seleccione una regla existente. Defina **Packet Capture** como **single-packet** o **extended-capture**.

   Si el perfil cuenta con excepciones de firmas definidas, haga clic en la pestaña Exceptions (Excepciones) y en la columna Packet Capture (Captura de paquetes) de una firma, seleccione single-packet (paquete único) o extended-capture (captura extendida).
2. (Opcional) Si seleccionó **extended-capture (captura extendida)** para cualquiera de los perfiles, defina la longitud de la captura de paquetes extendida.
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** y edite la configuración de Content-ID.
   2. En la sección **Extended Packet Capture Length (packets)**, especifique el número de paquetes que capturará el cortafuegos (el intervalo es 1-50; el valor por defecto es 5).
   3. Haga clic en **OK (Aceptar)**.

STEP 2 | Añada el perfil de seguridad (con la captura de paquetes habilitada) a una regla de la política de seguridad.

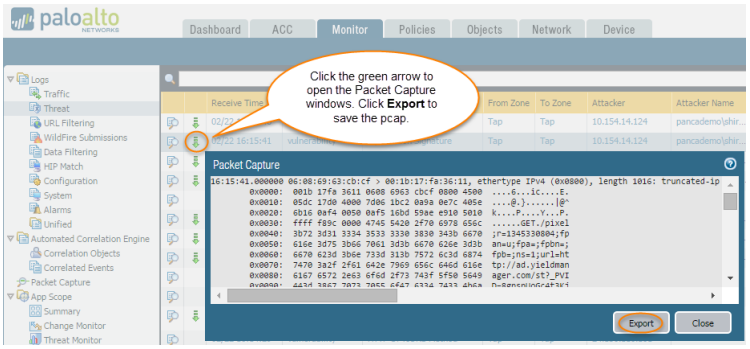
1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla.
2. Seleccione la pestaña **Actions (Acciones)**.
3. En la sección Profile Settings (Configuración de perfil), seleccione un perfil que tenga habilitada la captura de paquetes.

   Por ejemplo, haga clic en el menú desplegable **Antivirus** y seleccione un perfil que tenga habilitada la captura de paquetes.

STEP 3 | Vea/exporte la captura de paquetes de los logs de amenazas.

1. Select **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**.
2. En la entrada de log en la que está interesado, haga clic en el icono de captura de paquetes verde en la segunda columna. Vea la captura de paquetes directamente o seleccione **Export** para exportarla a su sistema.

© 2020 Palo Alto Networks, Inc.



Tome una captura de paquetes de aplicaciones

Los siguientes temas describen dos formas de configurar el cortafuegos para tomar capturas de paquetes de aplicaciones:

- Captura de paquetes de aplicaciones desconocidas
- Captura de paquetes de aplicaciones personalizada

Captura de paquetes de aplicaciones desconocidas

Los cortafuegos de Palo Alto Networks generan automáticamente una captura de paquetes de las sesiones que contienen una aplicación que el cortafuegos no puede identificar. Normalmente, las únicas aplicaciones clasificadas como tráfico desconocido (tcp, udp o tcp no sincronizado) son aplicaciones disponibles comercialmente que todavía no tienen firmas App-ID, son aplicaciones internas o personalizadas de su red o posibles amenazas. Puede usar esas capturas de paquetes para reunir más contexto relacionado con la aplicación desconocida o usar la información para analizar el tráfico en busca de posibles amenazas. También puede realizar una Gestión de aplicaciones personalizadas o desconocidas controlándolas mediante una política de seguridad o escribiendo una firma de aplicación personalizada y, después, creando una regla de seguridad basada en la firma personalizada. Si la aplicación es una aplicación comercial, puede enviar la captura de paquetes a Palo Alto Networks para que se cree una firma App-ID.

STEP 1 | Verifique que la captura de paquetes de aplicaciones desconocidas está activada (esta opción está habilitada de forma predeterminada).

1. Para ver la configuración de la captura de aplicaciones desconocidas, ejecute el siguiente comando de la CLI:

```
admin@PA-220>show running application setting | match "Unknown capture"
```

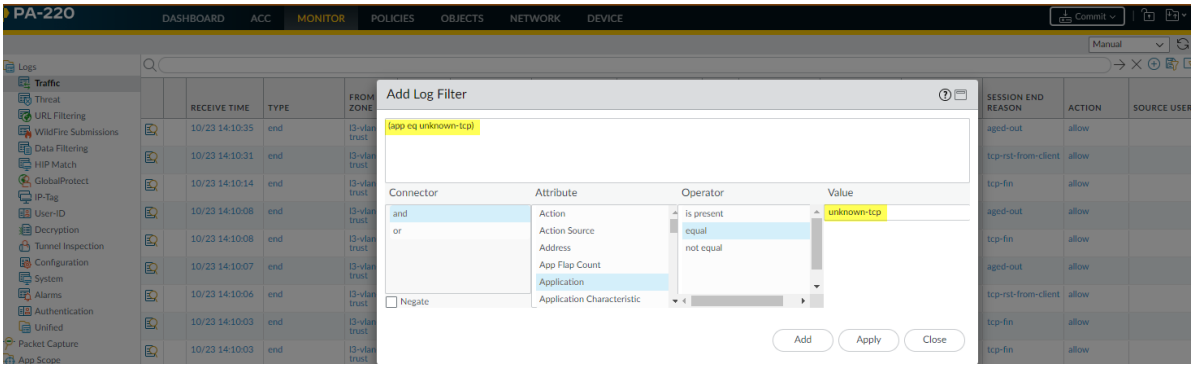
2. Si la opción del ajuste de captura desconocida está deshabilitada, habilítela:

```
admin@PA-220>set application dump-unknown yes
```

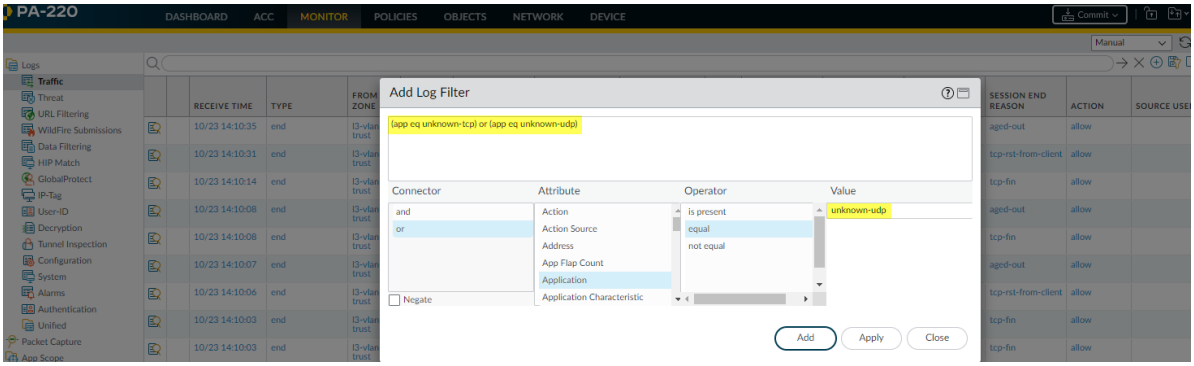
STEP 2 | Filtre log los de tráfico para localizar las aplicaciones TCP y UDP desconocidas.

1. Select **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.
2. Haga clic en **Add Filter (Añadir filtro)**, cree la parte TCP desconocida del filtro (**Connector [Conector]** = "and", **Attribute [Atributo]** = "Application", **Operator [Operador]** = "equal" y especifique "unknown-tcp" como **valor**). A continuación, haga clic en **Add (Añadir)** para agregar la consulta al filtro.

© 2020 Palo Alto Networks, Inc.



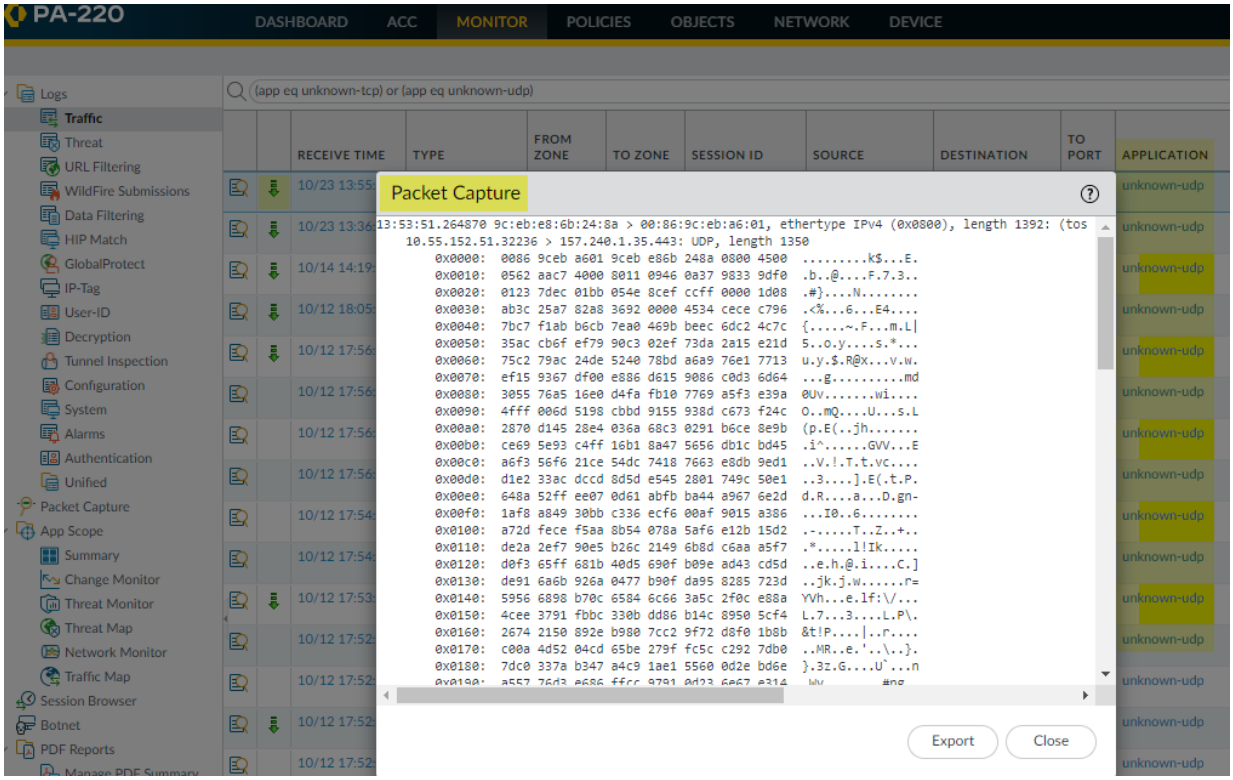
3. Cree la parte UDP desconocida del filtro (**Connector [Conector]** = "or", **Attribute [Atributo]** = "Application", **Operator [Operador]** = "equal", y especifique "unknown-udp" como **valor**). A continuación, haga clic en **Add (Añadir)** para agregar la consulta al filtro.



4. Haga clic en **Apply (Aplicar)** para colocar el filtro en el campo de consulta de la pantalla de log.

STEP 3 | Haga clic en la flecha **Apply Filter (Aplicar filtro)** junto al campo de consulta para ejecutar el filtro. A continuación, haga clic en el icono de captura de paquetes para ver la captura de paquetes o **exportarla** a su sistema.

© 2020 Palo Alto Networks, Inc.



Captura de paquetes de aplicaciones personalizada

Puede configurar un cortafuegos de Palo Alto Networks para que realice una captura de paquetes según un nombre de aplicación y los filtros que defina. A continuación, puede utilizar la captura de paquetes para solucionar los problemas de control de la aplicación. Cuando configure una captura de paquetes de aplicación, debe usar el nombre de aplicación definido en la base de datos App-ID. Puede ver una lista de todas las aplicaciones App-ID utilizando Applipedia o desde la interfaz web del cortafuegos en **Objects (Objetos)** > **Applications (Aplicaciones)**.

STEP 1 | Use una aplicación de emulador de terminal, como PuTTY, para iniciar una sesión SSH en el cortafuegos.

STEP 2 | Active la captura de paquetes de aplicaciones y defina filtros.

```
admin@PA-220>set application dump on application <application-name>
 regla<rule-name>
```

Por ejemplo, para capturar paquetes para la aplicación con base de LinkedIn que coincide con la regla de seguridad llamada Social Networking Apps (Aplicaciones de redes sociales), ejecute el siguiente comando de la CLI:

```
admin@PA-220>set application dump on application linkedin-base rule "Social
 Networking Apps"
```

También puede aplicar otros filtros, como direcciones IP de origen o destino.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Vea el resultado de la captura de paquetes para asegurarse de que se apliquen los filtros correctos. La salida se muestra después de habilitar la captura de paquetes.

El siguiente resultado confirma que el filtrado de captura de aplicaciones ahora se basa en la aplicación de LinkedIn para el tráfico que coincide con la regla de aplicaciones de redes sociales.

```
Application setting:
Application cache             : yes
Supernode                     : yes
Heuristics                    : yes
Cache Threshold               : 16
Bypass when exceeds queue limit: no
Traceroute appid              : yes
Traceroute TTL threshold      : 30
Use cache for appid           : no
Use simple appsigs for ident  : yes
Use AppID cache on SSL/SNI    : no
Unknown capture               : on
Max. unknown sessions         : 5000
Current unknown sessions      : 7
Application capture           : on
Max. application sessions     : 5000
Current application sessions  : 0
Application filter setting:
    Rule                      : Social Networking Apps
    From                      : any
    To                        : any
    Source                    : any
    Destination               : any
    Protocol                  : any
    Source Port               : any
    Dest. Port                : any
    Application               : linkedin-base

Current APPID Signature
   Memory Usage               : 16768  KB (Actual 16440  KB)
      TCP 1 C2S               : regex 11898  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4234   states
      UDP 1 S2C               : regex 1605   states

Alternate APPID Signature
   Memory Usage               : 16768  KB (Actual 16425  KB)
      TCP 1 C2S               : regex 11878  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4233   states
      UDP 1 S2C               : regex 1604   states
```

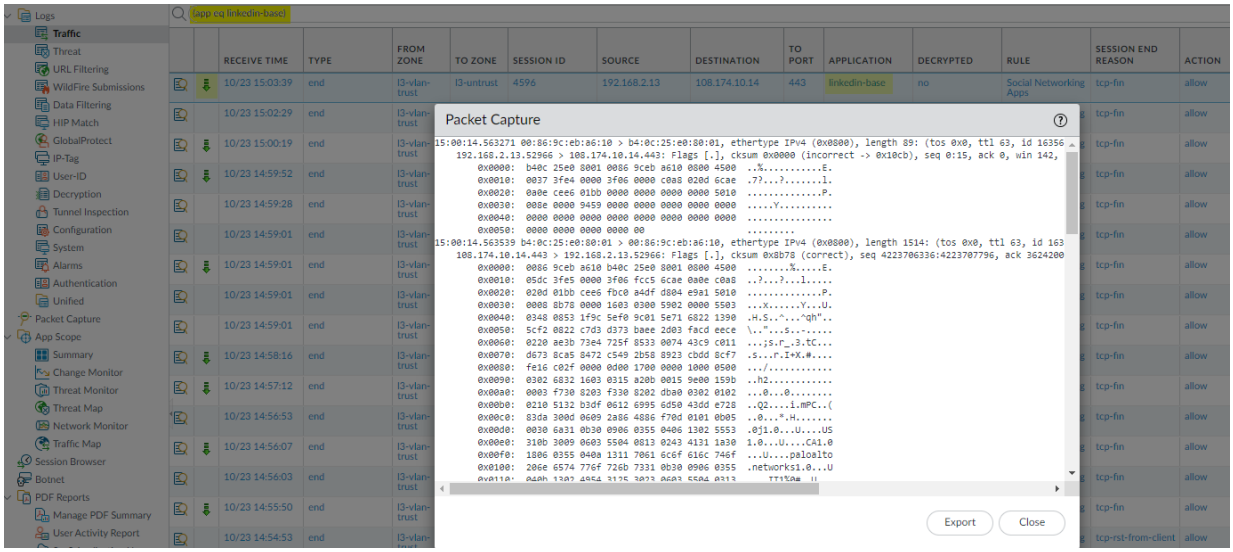
STEP 4 | Acceda a linkedin.com desde un navegador web y realice algunas tareas de LinkedIn para generar tráfico de LinkedIn. A continuación, ejecute el siguiente comando de la CLI para desactivar la captura de paquetes de aplicaciones:

```
admin@PA-220>set application dump off
```

STEP 5 | Vea/exporte la captura de paquetes.

1. Inicie sesión en la interfaz web del cortafuegos y seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.
2. En la entrada de log en la que está interesado, haga clic en el icono de captura de paquetes verde .
3. Vea la captura de paquetes directamente o seleccione **Export** para exportar esa captura a su sistema. La siguiente captura de pantalla muestra una captura de paquete basado en LinkedIn.

© 2020 Palo Alto Networks, Inc.



Captura de paquetes en la interfaz de gestión

El comando de la CLI **tcpdump** le permite capturar paquetes que atraviesen la interfaz de gestión (MGT) en un cortafuegos de Palo Alto Networks.

*Cada plataforma tiene un número predeterminado de bytes que captura **tcpdump**. Los cortafuegos PA-220 capturan 68 bytes de datos de cada paquete, y cualquier byte de más queda truncado. Los cortafuegos PA-7000 Series y VM-Series capturan 96 bytes de datos de cada paquete. Para definir el número de paquetes que capturará **tcpdump**, use la opción **snaplen** (longitud de instantánea) (intervalo 0-65535). Si define **snaplen** como 0, el cortafuegos usará la longitud máxima necesaria para capturar paquetes completos.*

STEP 1 | Use una aplicación de emulador de terminal, como PuTTY, para iniciar una sesión SSH en el cortafuegos.

STEP 2 | Para iniciar una captura de paquetes en la interfaz MGT, ejecute el comando siguiente:

```
admin@PA-220>tcpdump filter "<filter-option> <IP-address>" snaplen length
```

Por ejemplo, para capturar el tráfico que se genera cuando un administrador se autentica en el cortafuegos usando RADIUS, filtre según la dirección IP de destino del servidor RADIUS (10.5.104.99 en este ejemplo):

```
admin@PA-220>tcpdump filter "dst 10.5.104.99" snaplen 0
```

También puede filtrar por src (dirección IP de origen), host y red, y puede excluir contenido. Por ejemplo, para filtrar en una subred y excluir todo el tráfico SCP, SFTP y SSH traffic (que usa el puerto 22), ejecute el siguiente comando:

```
admin@PA-220>tcpdump filter "net 10.5.104.0/24 and not port 22" snaplen 0
```

*Cada vez que **tcpdump** realice una captura de paquete, almacenará el contenido en un archivo llamado mgmt.pcap. Este archivo se sobrescribe cada vez que ejecute **tcpdump**.*

© 2020 Palo Alto Networks, Inc.

STEP 3 | Cuando el tráfico en el que está interesado haya atravesado la interfaz MGT, pulse Ctrl + C para detener la captura.

STEP 4 | Consulte la captura de paquetes ejecutando el siguiente comando:

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

El siguiente resultado muestra la captura de paquete del puerto MTG (10.5.104.98) al servidor RADIUS (10.5.104.99):

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access
 Request (1), id: 0x00 length: 89
 09:55:29.144354 arp reply 10.5.104.98 is-at 00:25:90:23:94:98 (oui
 Unknown)
 09:55:29.379290 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access
 Request (1), id: 0x00 length: 70
 09:55:34.379262 arp who-has 10.5.104.99 tell 10.5.104.98
```

STEP 5 | (Opcional) Exporte la captura de paquetes del cortafuegos usando SCP (o TFTP). Por ejemplo, para exportar la captura de paquetes con SCP, ejecute el siguiente comando:

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to <username@host:path>
```

Por ejemplo, para exportar el pcap a un servidor con SCP en 10.5.5.20 a una carpeta temporal llamada temp-SCP, ejecute el siguiente comando de la CLI:

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to admin@10.5.5.20:c:/temp-
SCP
```

Introduzca el nombre de usuario y la contraseña de la cuenta en el servidor SCP para habilitar al cortafuegos para que copie la captura de paquetes en la carpeta c:\temp-SCP con el SCP habilitado.

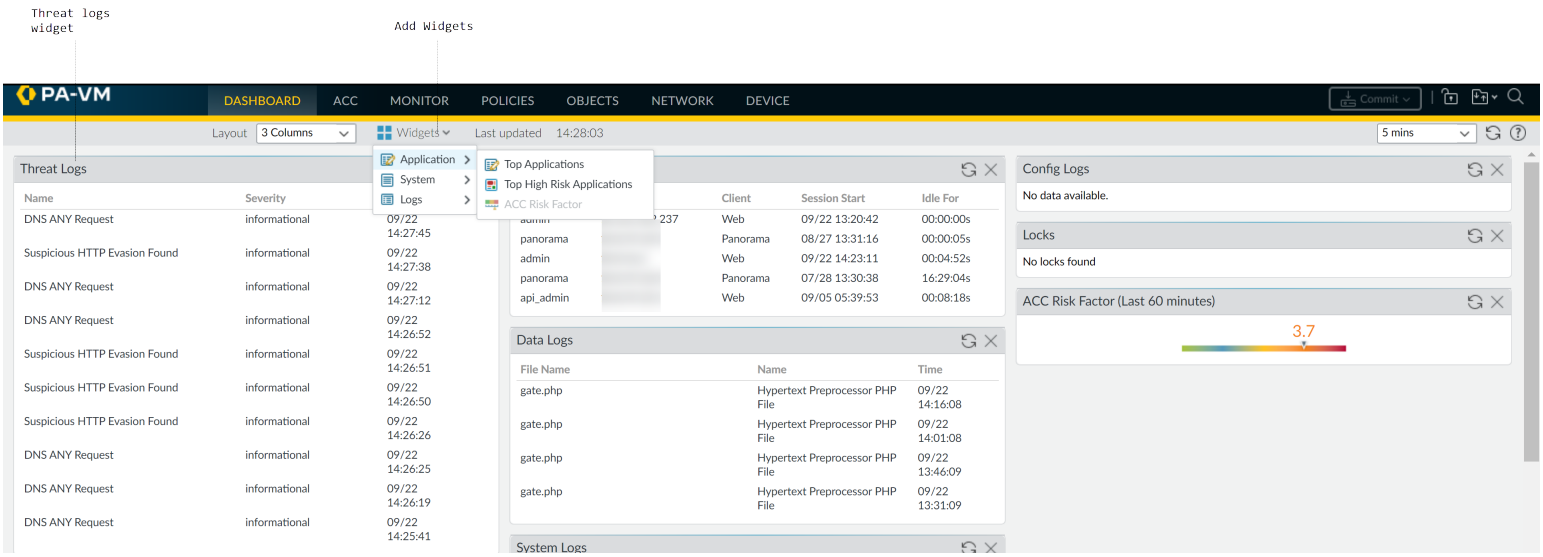
STEP 6 | Ahora puede visualizar los archivos de captura de paquetes con un analizador de paquetes de red como Wireshark.

© 2020 Palo Alto Networks, Inc.

Supervisión de aplicaciones y amenazas

Todos los cortafuegos de nueva generación de Palo Alto Networks están equipados con la tecnología App-ID, la cual permite identificar las aplicaciones que cruzan su red con independencia del protocolo, el cifrado o la táctica de evasión. De este modo, puede optar por Uso del Centro de control de aplicaciones para supervisar las aplicaciones. ACC resume gráficamente los datos de una variedad de bases de datos de logs para resaltar las aplicaciones que cruzan su red, quién las usa y su posible impacto en la seguridad. ACC se actualiza de forma dinámica de acuerdo con la clasificación de tráfico continua que App-ID realiza; si una aplicación cambia de puerto o comportamiento, App-ID continúa observando el tráfico, mostrando los resultados en ACC. La visibilidad adicional de categorías de URL, amenazas y datos ofrece una perspectiva completa e integral de la actividad de la red. Con ACC, puede obtener información rápidamente acerca del tráfico que cruza su red y traducir la información a una política de seguridad con más información.

También puede optar por Uso del panel para supervisar la red.



Infraestructura de red de entrega de contenido para comprobar si los eventos registrados en logs en el cortafuegos conllevan un riesgo de seguridad. El resumen de inteligencia de AutoFocus muestra la prevalencia de propiedades, actividades o comportamientos asociados con los logs de su red y a escala global, además del veredicto de WildFire y las etiquetas de AutoFocus vinculadas a ellos. Con una suscripción activa a AutoFocus, puede utilizar esta información para crear alertas de AutoFocus personalizadas que rastrean amenazas específicas en su red.

© 2020 Palo Alto Networks, Inc.

Visualización y gestión de logs

Un log es un archivo con marca de tiempo generado automáticamente que proporciona un código de seguimiento para los eventos del sistema en el cortafuegos o eventos de tráfico de red que el cortafuegos supervisa. Las entradas de log contienen *artefactos*, que son las propiedades, actividades o comportamientos asociados con el evento registrado en el log, tales como el tipo de aplicación o la dirección IP de un atacante. Cada tipo de log registra información para un tipo de evento separado. Por ejemplo, el cortafuegos genera un log de amenazas para registrar el tráfico que coincide con una firma de spyware, vulnerabilidad o virus, o un ataque DoS que coincide con los umbrales configurados para un análisis de puerto o actividad de barrido del host en el cortafuegos.

- Tipos de logs y niveles de gravedad
- Visualización de logs
- Filtrar logs
- Exportación de logs
- Configuración de cuotas de almacenamiento y periodos de vencimiento de logs
- Programación de exportaciones de logs a un servidor SCP o FTP

Tipos de logs y niveles de gravedad

Puede ver los siguientes tipos de log en las páginas **Monitor (Supervisar)** > **Logs**.

- Logs de tráfico
- Logs de amenazas
- Registros de filtrado de URL
- Logs de envíos de WildFire
- Logs Filtrado de datos
- Logs de correlación
- Logs de inspección de túnel
- Logs de configuración
- Logs del sistema
- Log de coincidencias HIP
- Logs de GlobalProtect
- Logs de asignación de etiquetas a IP
- Logs de User-ID
- Logs de descifrado
- Logs de alarmas
- Logs de autenticación
- Logs unificados

Logs de tráfico

Los logs de tráfico muestran una entrada para el inicio y el final de cada sesión. Todas las entradas incluyen la siguiente información: fecha y hora, las zonas de origen y destino, los grupos de direcciones dinámicas de origen y destino, las direcciones y los puertos, el nombre de la aplicación, la regla de seguridad aplicada al flujo de tráfico, la acción de la regla (permitir, denegar o descartar), la interfaz de entrada y salida, el número de bytes y la razón para finalizar la sesión.

Un grupo de direcciones dinámicas solo aparece en un log si la regla que coincide con el tráfico incluye un grupo de direcciones dinámicas. Si una dirección IP aparece en más de un

© 2020 Palo Alto Networks, Inc.

grupo de direcciones dinámicas, el cortafuegos muestra hasta cinco grupos de direcciones dinámicas en los logs junto con la dirección IP de origen.

La columna Type indica si la entrada es para el inicio o el final de la sesión. La columna Action indica si el cortafuegos permitió, denegó o descartó la sesión. El descarte indica que la regla de seguridad que ha bloqueado el tráfico ha especificado una aplicación cualquiera, mientras que la denegación indica que la regla ha identificado una aplicación específica. Si el cortafuegos descarta el tráfico antes de identificar la aplicación, como cuando una regla descarta todo el tráfico para un servicio específico, la columna Application muestra not-applicable.

Haga clic en junto a una entrada para ver detalles adicionales acerca de la sesión, como si una entrada ICMP agrega varias sesiones entre el mismo origen y destino (en cuyo caso el valor de la columna Count [Recuento] será superior a uno).

Cuando el log de descifrado introducido en PAN-OS 10.0 está deshabilitado, el cortafuegos envía logs HTTP/2 como logs de tráfico. Sin embargo, cuando los logs de descifrado están habilitados, el cortafuegos envía logs HTTP/2 como logs de inspección de túnel (cuando los logs de descifrado están deshabilitados, los logs de HTTP/2 se envían como logs de tráfico), por lo que debe verificar los logs de inspección de túnel en lugar de los logs de tráfico para eventos HTTP/2.

Logs de amenazas

Los logs de amenazas muestran entradas cuando el tráfico coincide con uno de los perfiles de seguridad adjuntos a una regla de seguridad en el cortafuegos. Cada entrada incluye la siguiente información: fecha y hora; tipo de amenaza (como virus o spyware); descripción de la amenaza o URL (columna Name [Nombre]);, zonas de origen y destino, direcciones, grupos de direcciones dinámicas de origen y puertos; nombre de la aplicación; acción de la alarma (como permitir o bloquear); y nivel de gravedad.

Un grupo de direcciones dinámicas solo aparece en un log si la regla que coincide con el tráfico incluye un grupo de direcciones dinámicas. Si una dirección IP aparece en más de un grupo de direcciones dinámicas, el cortafuegos muestra hasta cinco grupos de direcciones dinámicas en los logs junto con la dirección IP de origen.

Para ver más detalles de las entradas de log de amenazas individuales:

- Haga clic en junto a una entrada para ver detalles como si la entrada agrega varias amenazas del mismo tipo entre el mismo origen y destino (en cuyo caso el valor de la columna Count (Recuento) será superior a uno).
- Si configuró el cortafuegos para tomar capturas de paquetes, haga clic en junto a una entrada para acceder a los paquetes capturados.

La siguiente tabla resume los niveles de gravedad de las amenazas:

Gravedad	Description (Descripción)
Crítico	Amenazas graves, como aquellas que afectan a las instalaciones predeterminadas de software ampliamente implementado, que comprometen profundamente los servidores y dejan el código de explotación al alcance de los atacantes. El atacante no suele necesitar ningún tipo de credenciales de autenticación o conocimientos acerca de las víctimas y el objetivo no necesita ser manipulado para que realice ninguna función especial.
high (alta)	Amenazas que tienen la habilidad de convertirse en críticas pero que tienen factores atenuantes; por ejemplo, pueden ser difíciles de explotar, no conceder privilegios elevados o no tener un gran grupo de víctimas.

© 2020 Palo Alto Networks, Inc.

Gravedad	Description (Descripción)
	Las entradas de log de envíos de WildFire con un veredicto malicioso y una acción configurada en permitir se registran como amenazas de nivel alto.
Intermedia	Amenazas menores en las que se minimiza el impacto, como ataques DoS que no comprometen al objetivo o explotaciones que requieren que el atacante esté en la misma LAN que la víctima, afectan solo a configuraciones no estándar o aplicaciones oscuras u ofrecen acceso muy limitado. • Las entradas del log de amenazas con un veredicto malicioso y una acción de bloqueo o alerta, según la gravedad de la firma de WildFire existente, se registran como gravedad media.
low (baja)	Amenazas con nivel de advertencia que tienen muy poco impacto en la infraestructura de la organización. Suelen requerir acceso local o físico al sistema y con frecuencia suelen ocasionar problemas en la privacidad de las víctimas, problemas de DoS y fugas de información. • Las coincidencias de perfiles de filtrado de datos se registran como bajas. • Las entradas de log de envíos de WildFire con un veredicto grayware y cualquier acción registrada como amenaza de nivel bajo.
Informativo	Eventos sospechosos que no suponen una amenaza inmediata, pero que se registran para indicar que podría haber problemas más serios. • Las entradas de logs de filtrado de URL se registran como informativas. • Las entradas de log de envíos de WildFire con un veredicto benigno y cualquier acción registrada como informativa. • Las entradas de log de envíos de WildFire con cualquier veredicto y una acción configurada en bloquear y reenviar se registran como informativas. • Las entradas de log con cualquier veredicto y una acción configurada en bloquear se registran como informativas.

Registros de filtrado de URL

Los logs de Filtrado de URLs muestran entradas para el tráfico que coincide con el perfil de filtrado de URL vinculado a una regla de la política de seguridad. Por ejemplo, el cortafuegos genera un log si una regla bloquea el acceso a sitios web y categorías de sitios web específicos o si configuró una regla para generar una alerta cuando un usuario accede a un sitio web.

Logs de envíos de WildFire

El cortafuegos reenvía ejemplos (enlaces de archivos y de correo electrónico) a la nube de WildFire para su análisis en función de la configuración de los perfiles del análisis de WildFire (**Objects [Objetos]** > **Security Profiles [Perfiles de seguridad]** > **WildFire Analysis [Análisis de WildFire]**). El cortafuegos genera entradas de log de envíos de WildFire para cada muestra que reenvía después de que WildFire complete el análisis estático y dinámico de la muestra. Las entradas de log de envíos de WildFire incluyen la acción del cortafuegos para el ejemplo (permitir o bloquear), el veredicto de WildFire para el ejemplo enviado y el nivel de seguridad de la muestra.

La siguiente tabla resume los veredictos de WildFire:

© 2020 Palo Alto Networks, Inc.

Verdict	Description (Descripción)
benigno	Indica que la entrada recibió un veredicto de benigno tras el análisis de WildFire. Los archivos clasificados como benignos son seguros y no exhiben un comportamiento malintencionado.
Grayware	Indica que la entrada recibió un veredicto de grayware del análisis de WildFire. Los archivos clasificados como grayware no suponen una amenaza de seguridad directa, pero pueden mostrar un comportamiento agresivo de algún tipo. Grayware puede incluir adware, spyware y objetos de ayuda del explorador (BHO).
Phishing	Indica que WildFire le asignó un veredicto de análisis de phishing a un enlace. Un veredicto de phishing indica que el sitio hacia el que el enlace dirige a los usuarios mostró actividad de phishing de credenciales.
malicioso	Indica que la entrada recibió un veredicto malintencionado tras el análisis de WildFire. Las muestras clasificadas como malintencionadas pueden suponer una amenaza para la seguridad. El malware puede incluir virus, gusanos, troyanos, herramientas de acceso remoto (RAT), rootkits y botnets. Para las muestras que se identifican como malware, la nube de WildFire genera y distribuye una firma para evitar futuras exposiciones.

Logs Filtrado de datos

Los logs de filtrado de datos muestran entradas sobre las reglas de seguridad que ayudan a evitar que la información confidencial, como números de tarjetas de crédito, salga de la zona protegida por el cortafuegos. Consulte Data Filtering para obtener información sobre cómo definir perfiles de filtrado de datos.

Este tipo de log también muestra información de perfiles de bloqueo de archivos. Por ejemplo, si una regla bloquea los archivos .exe, el log muestra los archivos bloqueados.

Logs de correlación

El cortafuegos registra un evento correlacionado cuando los patrones y umbrales definidos en un Objeto de correlación coinciden con los patrones de tráfico de su red. Para Interpretación de eventos correlacionados y la visualización de una pantalla gráfica de los eventos, consulte Uso del widget de los hosts en riesgo en el ACC.

La siguiente tabla resume los niveles de gravedad de los logs de correlación:

Gravedad	Description (Descripción)
Crítico	Confirma que un host se ha visto en peligro basándose en eventos correlacionados que indican un patrón de progresión. Por ejemplo, se registra un evento crítico cuando un host que ha recibido un archivo considerado malintencionado por WildFire muestra la misma actividad de comando y control observada en ese archivo malintencionado dentro del espacio aislado de WildFire.
high (alta)	Indica que hay una probabilidad muy alta de que un host vea comprometida su seguridad basándose en una correlación entre varios eventos de amenaza, como el software malicioso detectado en cualquier punto de la red que coincida con la actividad de comando y control generada por un host concreto.

© 2020 Palo Alto Networks, Inc.

Gravedad	Description (Descripción)
Intermedia	Indica que hay una probabilidad de que un host vea comprometida su seguridad basándose en la detección de uno o varios eventos sospechosos, como las visitas repetidas a URL consideradas malintencionadas que sugiere la existencia de una actividad de comando y control generada por una secuencia de comandos.
low (baja)	Indica la posibilidad de que un host vea comprometida su seguridad basándose en la detección de uno o varios eventos sospechosos, como una visita a una URL considerada malintencionada o un dominio DNS dinámico.
Informativo	Detecta un evento que podría resultar útil en conjunto para identificar una actividad sospechosa; un evento por separado no tiene por qué ser significativo en sí.

Logs de inspección de túnel

Los logs de inspección de túnel son logs de tráfico para las sesiones de túnel; muestran entradas de sesiones de túnel no cifradas. Para evitar contarlas dos veces, el cortafuegos guarda solo los flujos internos en logs de tráfico y envía sesiones de túnel a los logs de inspección de túnel. Las entradas de log de inspección de túnel incluyen Receive Time (Hora de recepción) (fecha y hora de recepción del log), ID de túnel, etiqueta de supervisión, ID de sesión, regla de seguridad aplicada a la sesión de túnel, cantidad de bytes en la sesión, ID de sesión principal (ID de sesión para la sesión de túnel), dirección de origen, usuario de origen y zona de origen, dirección de destino, usuario de destino y zona de destino.

Cuando los logs de descifrado introducidos en PAN-OS 10.0 están habilitados, el cortafuegos envía logs HTTP/2 como logs de inspección de túnel (cuando los logs de descifrado están deshabilitados, los logs de HTTP/2 se envían como logs de tráfico), por lo que debe verificar los logs de inspección de túnel en lugar de los logs de tráfico para eventos HTTP/2. En este caso, también debe habilitar la inspección del contenido del túnel *para obtener el App-ID para el tráfico HTTP/2.*

Haga clic en la vista detallada de log para ver los detalles de una entrada, como el protocolo de túnel que se utiliza y la marca que indica si el contenido del túnel se inspeccionó o no. Solo una sesión con una sesión principal contará con una marca Tunnel Inspected (Túnel inspeccionado), lo que indica que la sesión se encuentra en un túnel en un túnel (dos niveles de encapsulación). El primer encabezado exterior de un túnel no contará con la marca Tunnel Inspected (Túnel inspeccionado).

Logs de configuración

Los logs de configuración muestran entradas de todos los cambios en la configuración del cortafuegos. Cada entrada incluye la fecha y hora, el nombre de usuario del administrador, la dirección IP desde la cual se realizó el cambio, el tipo de cliente (Web, CLI o Panorama), el tipo de comando ejecutado, el estado del comando (si se ejecutó correctamente o falló), la ruta de configuración y los valores anteriores y posteriores al cambio.

Logs del sistema

Los logs del sistema muestran entradas para cada evento del sistema en el cortafuegos. Cada entrada incluye la fecha y hora y la gravedad y descripción del evento. La siguiente tabla resume los niveles de gravedad de los logs de sistema. Para ver una lista parcial de mensajes de log de sistema y sus niveles de gravedad correspondientes, consulte Eventos de logs del sistema.

© 2020 Palo Alto Networks, Inc.

Gravedad	Description (Descripción)
Crítico	Fallos de hardware, lo que incluye la conmutación por error de alta disponibilidad (high availability,HA) y los fallos de enlaces.
high (alta)	Problemas graves, incluidas las interrupciones en las conexiones con dispositivos externos, como servidores LDAP y RADIUS.
Intermedia	Notificaciones de nivel medio, como actualizaciones de paquetes de antivirus.
low (baja)	Notificaciones de menor gravedad, como cambios de contraseña de usuario.
Informativo	Inicios de sesión/cierres de sesión, cambio de nombre o contraseña de administrador, cualquier cambio de configuración y el resto de eventos no cubiertos por los otros niveles de gravedad.

Log de coincidencias HIP

La coincidencia de perfil de información de host (Host Information Profile, HIP) de GlobalProtect le permite recoger información sobre el estado de seguridad de los dispositivos de destino que acceden a su red (tal como si tienen el cifrado de disco habilitado). El cortafuegos puede permitir o denegar el acceso a un host específico en función del cumplimiento con las reglas de seguridad basadas en el HIP que define. Los logs de coincidencia del HIP muestran los flujos de tráfico que coinciden con el objeto HIP o el perfil HIP que configuró para las reglas.

Logs de GlobalProtect

Los logs de GlobalProtect muestran los siguientes logs relacionados con GlobalProtect:

- Logs del sistema de GlobalProtect.

  Los logs de eventos de autenticación de GlobalProtect se conservan en **Monitor (Supervisar)** > **Logs** > **System (Sistema)**; sin embargo, la columna **Auth Method (Método de autenticación)** de los logs de GlobalProtect muestra el método de autenticación utilizado para los inicios de sesión.
- Eventos de satélite/LSVPN.
- Logs de puerta de enlace y portal de GlobalProtect.
- Logs de VPN sin cliente.

Logs de asignación de etiquetas a IP

En los logs de asignación de etiquetas a IP se muestra cómo y cuándo se registra una dirección IP de origen en el cortafuegos o se cancela su registro, junto con la etiqueta que aplica el cortafuegos a la dirección. Además, en cada entrada del log figuran el tiempo de espera (si se ha configurado) y el origen de la información sobre la asignación de la etiqueta a la dirección IP, como la máquina virtual del agente de User-ID y el etiquetado automático. Para obtener más información, consulte Registro de direcciones IP y etiquetas dinámicamente.

Logs de User-ID

User-ID muestra información sobre las asignaciones de direcciones IP a nombres de usuario y Marcas de tiempo de la autenticación, como los orígenes de la información de asignación y los períodos de tiempo cuando los usuarios se autenticaron. Puede utilizar esta información para ayudar a solucionar problemas de User-ID y de autenticación. Por ejemplo, si el cortafuegos está aplicando la regla de política incorrecta

© 2020 Palo Alto Networks, Inc.

a un usuario, puede ver los logs para verificar si ese usuario está asignado a la dirección IP correcta y si las asociaciones de grupo son correctas.

Logs de descifrado

Los logs de descifrado muestran las entradas para los enlaces TLS fallidos de forma predeterminada y pueden mostrar las entradas para los protocolos de enlace TLS correctos si los habilita en la política de descifrado. Si habilita las entradas para un protocolo de enlace correcto, asegúrese de tener los recursos del sistema (espacio de logs) para los logs.

Los logs de descifrado incluyen una gran cantidad de información para ayudarlo a Solución de problemas y supervisión del descifrado y, a continuación, resolver problemas. Hay 62 columnas de diferentes tipos de información que puede habilitar en los logs y, además, puede seleccionar cualquier log individual (, la lupa) y ver los detalles en una sola vista de detalles. Puede ver el certificado, el conjunto de cifrado y la información de error, como: nombre común del sujeto, nombre común del emisor, nombre común de la raíz, estado de la raíz, tipo y tamaño de la clave del certificado, fecha de inicio y finalización del certificado, número de serie del certificado, huella digital del certificado, versión TLS , algoritmo de intercambio de claves, algoritmo de cifrado, curva EC negociada, algoritmo de autenticación, SNI, tipo de proxy, información de errores (cifrado, HSM, recurso, reanudación, protocolo, función, certificado y versión) e índices de error (códigos que puede buscar para obtener más información sobre errores).

Logs de alarmas

Una alarma es un mensaje generado por el cortafuegos que indica que el número de eventos de un tipo determinado (por ejemplo, fallos de cifrado y descifrado) superó el límite configurado para ese tipo de evento. Para habilitar las alarmas y configurar los límites de las alarmas, seleccione **Device (Dispositivo)** > **Log Settings (Configuración de logs)** y edite la configuración de las alarmas.

Cuando genera una alarma, el cortafuegos crea un log de alarma y abre el diálogo System Alarms (Alarmas del sistema) para mostrar la alarma. Tras cerrar el diálogo haciendo clic en **Close**, puede volver a abrirlo en cualquier momento haciendo clic en **Alarms** ( ) al final de la interfaz web. Para evitar que el cortafuegos abra automáticamente el cuadro de diálogo de una alarma en particular, seleccione la alarma en la lista Unacknowledged Alarms y haga clic en **Acknowledge** para aceptar la alarma.

Logs de autenticación

Los logs de autenticación muestran información sobre los eventos de autenticación que ocurren cuando los usuarios finales tratan de acceder a los recursos de la red cuyo acceso se controla con las reglas de la Política de autenticación. Puede utilizar esta información para solucionar problemas de acceso y ajustar su política de autenticación según sea necesario. En combinación con objetos de correlación, también puede utilizar los logs de autenticación para identificar actividades sospechosas en su red, por ejemplo, ataques de fuerza bruta.

También puede configurar las reglas de autenticación para los eventos de tiempo de espera de logs. Estos tiempos de espera de autenticación de logs se relacionan con el periodo de tiempo que un usuario necesita para autenticarse solo una vez en un recurso, pero puede acceder a él varias veces. Conocer los tiempos de espera le permite decidir mejor si debe ajustarlos y cómo hacerlo (para obtener los detalles, consulte Marcas de tiempo de la autenticación).

Los logs del sistema registran eventos de autenticación relacionados con GlobalProtect y el acceso de los administradores a la interfaz web.

Logs unificados

Los logs unificados son entradas de logs de tráfico, amenazas, filtrado de URL, envíos de WildFire y filtrado de datos en una sola pantalla. La vista de logs unificados le permite investigar y filtrar las entradas más recientes de diferentes tipos de logs en un lugar, en vez de buscar en cada tipo de log por separado. Haga

© 2020 Palo Alto Networks, Inc.

clic en Effective Queries ( ) en el área de filtros para seleccionar qué tipos de logs mostrarán entradas en la vista de logs unificados.

La vista de logs unificados muestra solo las entradas de los logs de los que tiene permiso para ver. Por ejemplo un administrador que no dispone permisos para ver los logs de envíos a WildFire, no verá esas entradas al visualizar los logs unificados. Tipos de funciones administrativas define estos permisos.

Cuando realiza la Configuración de búsqueda remota en AutoFocus para realizar una búsqueda específica en el cortafuegos, los resultados de la búsqueda se muestran en la vista de logs unificados.

Visualización de logs

Puede ver los diferentes tipos de logs en el cortafuegos en forma de tabla. El cortafuegos almacena localmente todos los archivos de log y genera automáticamente logs de configuración y sistema por defecto. Para obtener más información sobre las reglas de seguridad que desencadenan la creación de entradas para los demás tipos de logs, consulte Tipos de logs y niveles de gravedad.

Para configurar el cortafuegos para el reenvío de logs como mensajes de syslog, notificaciones por correo electrónico o trampas del protocolo simple de administración de redes (Simple Network Management Protocol, SNMP), aplique el Uso de servicios externos para la monitorización.

STEP 1 | Seleccione un tipo de log para visualizar.

1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
2. Seleccione un tipo de log de la lista.

El cortafuegos muestra solo los logs que tiene permiso para ver. Por ejemplo, si su cuenta administrativa no tiene permiso para ver los logs de envíos de WildFire, el cortafuegos no muestra ese tipo de log cuando accede a las páginas de logs. Tipos de funciones administrativas definen los permisos.

STEP 2 | **(Opcional)** Personalice la visualización de la columna de logs.

1. Haga clic en la flecha a la derecha de cualquier encabezado de columna y seleccione **Columns**.
2. Seleccione las columnas para mostrar las listas. El log se actualiza automáticamente para coincidir con sus selecciones.

STEP 3 | Vea los detalles adicionales sobre las entradas del log.

- Haga clic en el catalejo ( ) para ver una entrada de log específica. La vista detallada de logs tiene más información sobre el origen y destino de la sesión, además de una lista de sesiones relacionadas con la entrada del log.
- (Solo para logs de amenazas) Haga clic en junto a una entrada para acceder a las capturas de paquetes locales de la amenaza. Para habilitar capturas de paquetes locales, consulte Realización de capturas de paquetes.
- (Solo tráfico, amenaza, filtrado de URL, envíos de WildFire, filtrado de datos y logs unificados) Vea los datos de amenazas de AutoFocus para acceder a una entrada del log.

  1. Habilitación de la inteligencia contra amenazas AutoFocus.

     Habilite AutoFocus en Panorama para ver los datos de amenazas de AutoFocus de todas las entradas de log de Panorama, incluso los de cortafuegos que no están conectados a AutoFocus o que ejecutan PAN-OS 7.0 y versiones anteriores (Panorama > Setup [Configuración] > Management [Gestión] > AutoFocus).
  2. Coloque el cursor sobre una dirección IP, una URL, un agente de usuario, un nombre de amenaza (subtipo: solo virus y wildfire), un nombre de archivo o un hash SHA-256.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en el menú desplegable (⌄) y seleccione **AutoFocus**.
4. Infraestructura de red de entrega de contenido.

Pasos siguientes:

- Filtrar logs.
- Exportación de logs.
- Configuración de cuotas de almacenamiento y periodos de vencimiento de logs.

Filtrar logs

Cada log tiene un área de filtrado que le permite configurar criterios para mostrar las entradas del log. La capacidad de filtrar logs resulta útil para centrarse en los eventos de su cortafuegos que poseen propiedades o atributos particulares. Filtre los logs según los artefactos que estén asociados con entradas de log individuales.

Por ejemplo, si aplica un filtro por UUID de regla, le resulta más fácil localizar la regla concreta que busca, aunque existan otras con nombres parecidos. Si el conjunto incluye numerosas reglas, el filtro por UUID detecta la regla que le interesa y le ahorra buscarla por varias páginas de resultados.

STEP 1 | (Solo para logs unificados) Seleccione los tipos de logs que se incluirán en la vista de logs unificados.

1. Haga clic en Effective Queries (Consultas efectivas) ( ).
2. Seleccione uno o más tipos de logs en la lista (**traffic [tráfico]**, **threat [amenaza]**, **url**, **data [datos]** y **wildfire**).
3. Haga clic en **OK (Aceptar)**. Los logs unificados se actualizan para mostrar solo las entradas de los tipos de logs que seleccionó.

STEP 2 | Añada un filtro al campo de filtros.

Si el valor del artefacto coincide con el operador (tal como has o in), coloque el valor entre comillas para evitar un error de sintaxis. Por ejemplo, si filtra por país de destino y usa IN como valor para especificar INDIA, introduzca el filtro como `( dstloc eq "IN" )`.

- Haga clic en uno o más artefactos (como el tipo de aplicación asociado con el tráfico y la dirección IP de un atacante) en una entrada de log. Por ejemplo, haga clic en **10.0.0.25** para Source y en **web-browsing** para Application en una entrada de log para mostrar solo las entradas que contienen ambos artefactos en el log (búsqueda con AND).
- Para especificar los artefactos que se añadirán al campo de filtros, haga clic en Add Filter (Añadir filtro) ( ).
- Para añadir un filtro guardado previamente, haga clic en Load Filter (Cargar filtro) ( ).

STEP 3 | Aplique el filtro al log.

Haga clic en Apply Filter (Aplicar filtro) ( ). El log se actualizará para mostrar solo las entradas de log que coinciden con el filtro actual.

STEP 4 | (Opcional) Guarde los filtros de uso frecuente.

1. Haga clic en Save Filter (Guardar filtro) ( ).
2. Introduzca un nombre para el filtro en **Name**.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en **OK (Aceptar)**. Puede ver los filtros guardados al hacer clic en Load Filter ( ).

Pasos siguientes:

- Visualización de logs.
- Exportación de logs.

Exportación de logs

Puede exportar el contenido de un tipo de log a un informe con formato de valores separados por coma (comma-separated value, CSV). Por defecto, el informe contiene hasta 2000 filas de entradas de logs.

STEP 1 | Especifique el número de filas para mostrar en el informe.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de creación de logs y creación de informes.
2. Haga clic en la pestaña **Log Export and Reporting**.
3. Modifique el número de **Max Rows in CSV Export (Cantidad máxima de filas en exportación de CSV)** (hasta 1 048 576 filas).
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Descargue el log.

1. Haga clic en Export to CSV ( ). Aparece una barra de progreso que muestra el estado de la descarga.
2. Cuando se haya completado la descarga, haga clic en **Download file** para guardar una copia del log en su carpeta local. Para obtener descripciones de los encabezados de columna en un log descargado, consulte Descripciones de los campos de Syslog.

Siguientes pasos...

Programación de exportaciones de logs a un servidor SCP o FTP.

Configuración de cuotas de almacenamiento y periodos de vencimiento de logs

El cortafuegos elimina automáticamente los logs que superan el periodo especificado. Cuando el cortafuegos alcanza la cuota de almacenamiento de un tipo de log, automáticamente elimina los logs más antiguos de ese tipo para conseguir espacio, aunque no haya definido un periodo de caducidad.

Si desea eliminar manualmente los logs, seleccione Device (Dispositivo) > Log Settings (Configuración de log) y, en la sección Manage Logs (Gestionar logs), haga clic en los enlaces para borrar los logs por tipo.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de registro e informes.

STEP 2 | Seleccione **Log Storage (Almacenamiento de logs)** e introduzca una **Quota (Cuota) (%)** para cada tipo de log. Al cambiar un valor del porcentaje, el cuadro de diálogo se actualiza para mostrar el valor absoluto correspondiente (columna de cuota GB/MB).

STEP 3 | Introduzca **Max Days (Máx. de días)** (período de vencimiento) para cada tipo de log (el intervalo es de 1 a 2000). Los campos están en blanco por defecto, lo que significa que los logs nunca vencen.

© 2020 Palo Alto Networks, Inc.

El cortafuegos sincroniza los periodos de vencimiento en pares de alta disponibilidad (HA). Como solo el peer de alta disponibilidad (HA) activo genera logs, el peer pasivo no tiene logs que eliminar a no ser que se produzca una conmutación por error y comience a generar logs.

STEP 4 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Programación de exportaciones de logs a un servidor SCP o FTP

Puede programar exportaciones de logs de envío de WildFire, tráfico, amenazas, filtrado URL, filtrado de datos y coincidencias HIP a un servidor de copias seguras (SCP) o un servidor de protocolo de transferencia de archivos (FTP). Realice esta tarea para cada tipo de log que desee exportar.

Puede usar comandos de copia segura (SCP) de la CLI para exportar la base de datos de logs completa a un servidor SCP e importarlo a otro cortafuegos. Como la base de datos de logs es demasiado grande para que sea práctico importarla o exportarla en las siguientes plataformas, estas no admiten esas opciones: Los cortafuegos serie PA-7000 (todas las versiones de PAN-OS), el dispositivo virtual de Panorama que se ejecuta en Panorama 6.0 o versiones posteriores y los dispositivos serie M de Panorama (todas las versiones de Panorama).

STEP 1 | Seleccione **Device (Dispositivo)** > **Scheduled Log Export (Exportación de logs programada)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un **nombre** para la exportación de logs programada y **habilítela**.

STEP 3 | Seleccione el **Tipo de log** que se debe exportar.

STEP 4 | Seleccione la **hora de inicio de exportación programada** diaria. Las opciones se muestran en incrementos de 15 minutos en un reloj de 24 horas (00:00 - 23:59).

STEP 5 | Seleccione el **Protocol (Protocolo)** para exportar los logs: **SCP** (seguro) o **FTP**.

STEP 6 | Introduzca el **Nombre de host** o la dirección IP del servidor.

STEP 7 | Introduzca el número de **Puerto**. De manera predeterminada, FTP usa el puerto 21 y SCP usa el puerto 22.

STEP 8 | Introduzca la **Path (Ruta)** o directorio donde se guardarán los logs almacenados.

STEP 9 | Introduzca el **Username** y, si es necesario, la **Password** (y **Confirm Password**) para acceder al servidor.

STEP 10 | **(**Solo FTP**)** Seleccione **Enable FTP Passive Mode (Habilitar modo pasivo de FTP)** si desea utilizar el modo pasivo de FTP, en el que el cortafuegos inicia una conexión de datos con el servidor FTP. De manera predeterminada, el cortafuegos utiliza el modo activo FTP en el que el servidor FTP inicia una conexión de datos con el cortafuegos. Seleccione el modo según lo que admite su servidor FTP y sus requisitos de red.

© 2020 Palo Alto Networks, Inc.

STEP 11 | (Solo SCP) Haga clic en **Test SCP server connection (Probar la conexión de servidor SCP)**. Antes de establecer una conexión, el cortafuegos debe aceptar la clave del host para el servidor SCP.



Si utiliza una plantilla Panorama para configurar la programación de exportación de logs, debe realizar este paso después de asignar la configuración de plantilla a los cortafuegos. Tras asignar la plantilla, inicie sesión en cada cortafuegos, abra la programación de exportación de logs y haga clic en Test SCP server connection (Probar la conexión del servidor SCP).

STEP 12 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Supervisión de la lista de bloqueo

Existen dos maneras de provocar que el cortafuegos ubique una dirección IP en la lista de bloqueo:

- Configure un perfil de protección frente a vulnerabilidades con una regla que bloquee las conexiones IP y aplique el perfil a la política de seguridad, que se aplica a una zona.
- Configure una regla de la política de protección contra DoS con la acción Protect (Proteger) y un perfil de protección contra DoS clasificado, que especifique una tasa máxima de conexiones por segundo permitidas. Cuando los paquetes entrantes coinciden con la política de la protección contra DoS y superan la tasa máxima, y si especificó una duración de bloqueo y una regla de la política clasificada que permite incluir la dirección IP de origen, el cortafuegos agrega la dirección IP de origen ilícita a la lista de bloqueo.

En los casos que se describen anteriormente, el cortafuegos automáticamente bloquea el tráfico en el hardware antes de que esos paquetes utilicen los recursos de la CPU o el búfer de paquetes. Si el tráfico de ataques supera la capacidad de bloqueo del hardware, el cortafuegos utiliza los mecanismos de bloqueo de IP del software para bloquear el tráfico.

El cortafuegos crea automáticamente una entrada en la lista de bloqueo de hardware basada en su perfil de protección frente a vulnerabilidades o regla de la política de protección contra DoS; la dirección de origen de la regla es la dirección IP de origen en la lista de bloqueo de hardware.

Las entradas en la lista de bloqueo indican en la columna Type (Tipo) si fueron bloqueadas por hardware (hw) o software (sw). En la parte inferior de la pantalla, se muestra lo siguiente:

- Recuento de **Total Blocked IPs (IP totales bloqueadas)** en relación con el número de direcciones IP bloqueadas que admite el cortafuegos.
- Porcentaje de la lista de bloqueo que ha utilizado el cortafuegos.

Para ver detalles sobre una dirección en la lista de bloqueo, pase el ratón sobre una dirección IP de origen y haga clic en la flecha hacia abajo. Haga clic en el enlace Who Is, que muestra la función Network Solutions Who Is (Who Is de las soluciones de red), que proporciona información sobre la dirección.

Para obtener información sobre la configuración de un perfil de protección contra vulnerabilidades, consulte Personalización de la acción y las condiciones de activación para una firma de fuerza bruta. Para obtener más información sobre la lista de bloqueo y los perfiles de protección contra DoS, consulte Protección DoS contra inundaciones de nuevas sesiones.

© 2020 Palo Alto Networks, Inc.

Visualización y gestión de informes

Las funciones de generación de informes del cortafuegos le permiten comprobar el estado de su red, validar sus políticas y concentrar sus esfuerzos en mantener la seguridad de la red para que sus usuarios estén protegidos y sean productivos.

- Tipos de informes
- Visualización de informes
- Configuración del período de vencimiento y de ejecución para los informes
- Deshabilitación de informes predefinidos
- Informes personalizados
- Generación de informes personalizados
- Generación de informes de Botnet
- Generación de informes de uso de la aplicación SaaS
- Gestión de informes de resumen en PDF
- Generación de informes de actividad del usuario/grupo
- Gestión de grupos de informes
- Programación de informes para entrega de correos electrónicos
- Gestión de la capacidad de almacenamiento de informes

Tipos de informes

El cortafuegos incluye informes predefinidos que puede utilizar tal cual o bien puede crear informes personalizados que satisfagan sus necesidades por lo que respecta a datos específicos y tareas útiles o combinar informes predefinidos y personalizados para compilar la información que necesita. El cortafuegos proporciona los siguientes tipos de informes:

- **Informes predefinidos**: le permiten ver un resumen rápido del tráfico de su red. Hay disponible un conjunto de informes predefinidos divididos en cuatro categorías: Aplicaciones, Tráfico, Amenaza y Filtrado de URL. Consulte Visualización de informes.
- **Informes de actividad de usuario o grupo**: le permiten programar o crear un informe a petición sobre el uso de la aplicación y la actividad de URL para un usuario específico o para un grupo de usuarios. El informe incluye las categorías de URL y un cálculo del tiempo de exploración estimado para usuarios individuales. Consulte Generación de informes de actividad del usuario/grupo.
- **Informes personalizados**: Cree y programe informes personalizados que muestren exactamente la información que desee ver, filtrando según las condiciones y las columnas que deben incluirse. También puede incluir generadores de consultas para un desglose más específico de los datos de informe. Consulte Generación de informes personalizados.
- **Informes de resumen en PDF**: Agregue hasta 18 informes/gráficos predefinidos o personalizados de las categorías Amenaza, Aplicación, Tendencia, Tráfico y Filtrado de URL a un documento PDF. Consulte Gestión de informes de resumen en PDF.
- **Informes de Botnet**: le permiten utilizar mecanismos basados en el comportamiento para identificar posibles hosts infectados por Botnet en la red. Consulte Generación de informes de Botnet.
- **Grupos de informes**: combine informes personalizados y predefinidos en grupos de informes y compile un único PDF que se enviará por correo electrónico a uno o más destinatarios. Consulte Gestión de grupos de informes.

Los informes se pueden generar según se necesiten, con una planificación recurrente, y se puede programar su envío diario por correo electrónico.

© 2020 Palo Alto Networks, Inc.

Visualización de informes

El cortafuegos proporciona una variedad de más de 40 informes predefinidos que se generan cada día. Estos informes se pueden visualizar directamente en el cortafuegos. Puede ver estos informes directamente en el cortafuegos. Además, puede visualizar informes personalizados e informes de resumen.

Se asignan aproximadamente 200 MB de almacenamiento para guardar informes en el cortafuegos. Este límite solo se puede cambiar para los cortafuegos PA-7000 Series y PA-5200 Series. En los demás modelos, puede permitir que el cortafuegos elimine informes una vez que hayan vencido; consulte Configuración del período de vencimiento y de ejecución para los informes. Tenga en cuenta que cuando el cortafuegos alcance su límite de almacenamiento, automáticamente elimina informes anteriores para conseguir espacio, incluso si no define un periodo de caducidad. Otra forma de conservar recursos del sistema en el cortafuegos es con la Deshabilitación de informes predefinidos. Si desea conservar los informes a largo plazo, puede exportarlos (como se describe a continuación) o programar su entrega (como se describe en Programación de informes para entrega de correos electrónicos).

A diferencia de los otros informes, no puede guardar informes Actividad de grupo/usuario en el cortafuegos. Debe usar la Generación de informes de actividad del usuario/grupo *bajo demanda o programarlos para una entrega por correo electrónico.*

STEP 1 | (Solo en cortafuegos VM-50, VM-50 Lite y PA-200) Habilite la generación de informes predefinidos.

De forma predeterminada, los informes predefinidos están deshabilitados en los cortafuegos VM-50, VM-50 Lite y PA-200 para ahorrar recursos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite**Logging and Reporting (Logs e informes)**.
2. Seleccione **Pre-Defined Reports (Informes predefinidos)** y habilite (marque) **Pre-Defined Reports (Informes predefinidos)**.
3. Marque (habilite) los informes predefinidos que desee generar y haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.
5. Acceda a la CLI del cortafuegos para habilitar informes predefinidos.

   Este paso es necesario para los informes locales predefinidos y los informes predefinidos enviados desde un servidor de gestión Panorama™.

```
admin> debug predefined-default enable
```

STEP 2 | Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.

Los informes se agrupan en secciones (tipos) en el lado derecho de la página: **Custom Reports (Informes personalizados)**, **Application Reports (Informes de aplicación)**, **Traffic Reports (Informes de tráfico)**, **Threats Reports (Informes de amenazas)**, **URL Filtering Reports (Informes de filtrado de URL)** e **PDF Summary Reports (Informes de resumen en PDF)**.

STEP 3 | Seleccione un informe para visualizarlo. Luego, la página de informes muestra el informe del día anterior.

Para ver informes de otros días, seleccione una fecha en el calendario en la parte inferior derecha de la página y seleccione un informe. Si selecciona un informe en otra sección, la selección de la fecha se restablece a la fecha actual.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Para visualizar un informe fuera de línea, puede exportar el informe en los formatos PDF, CSV o XML. Haga clic en **Export to PDF (Exportar a PDF)**, **Export to CSV (Exportar a CSV)** o **Export to XML (Exportar a XML)** en la parte inferior de la página, y luego imprima o guarde.

Configuración del período de vencimiento y de ejecución para los informes

El período de vencimiento y el período de ejecución forman parte de la configuración global y se aplican a todos los Tipos de informes. Tras realizar nuevos informes, el cortafuegos elimina automáticamente los informes que superen el período de vencimiento.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, edite la configuración de creación de logs e informes, y seleccione la pestaña **Log Export and Reporting (Exportación e informes de logs)**.

STEP 2 | Establezca el **Report Runtime (Período de ejecución del informe)** en una hora en una programación de 24 horas (valor predeterminado: 02:00; rango: 00:00 [medianoche] a 23:00).

STEP 3 | Introduzca el **Report Expiration Period (Período de vencimiento del informe)** en días (valor predeterminado: no posee vencimiento; rango: 1 a 2000).

No puede cambiar el almacenamiento que asigna el cortafuegos para guardar informes: se ha predefinido a aproximadamente 200 MB. Cuando el cortafuegos alcanza su almacenamiento máximo, automáticamente elimina informes anteriores para conseguir espacio, incluso si no define un Report Expiration Period.

STEP 4 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Deshabilitación de informes predefinidos

El cortafuegos incluye aproximadamente 40 informes predefinidos que se generan automáticamente cada día. Si no utiliza algunos o todos estos informes predefinidos, podrá deshabilitar los informes seleccionados y conservar recursos del sistema en el cortafuegos.

Asegúrese de que ningún grupo de informes o Informe de resumen en pdf incluye los informes predefinidos que va a deshabilitar. De lo contrario, el cortafuegos mostrará el informe de resumen PDF o un grupo de informes sin ningún dato.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de registro e informes.

STEP 2 | Seleccione la pestaña **Pre-Defined Reports (Informes predefinidos)** y elimine la selección de la casilla de verificación para cada informe que desee deshabilitar. Para deshabilitar todos los informes predefinidos, haga clic en **Deselect All (Anular todas las selecciones)**.

STEP 3 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Informes personalizados

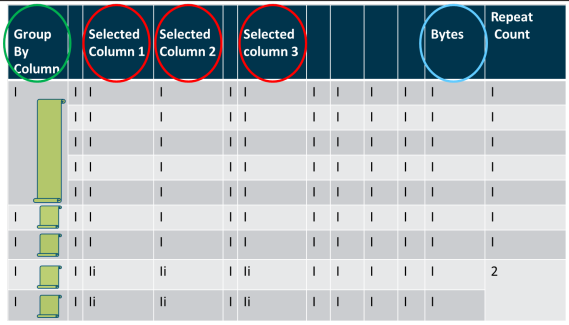
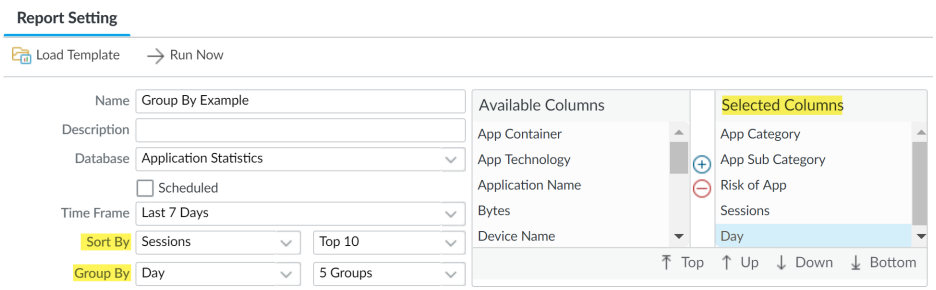
Para crear informes personalizados que tengan una finalidad concreta, ha de tener en cuenta los atributos o datos esenciales que se deben obtener y analizar (como amenazas), así como el método óptimo para categorizar la información, por ejemplo, agruparla por UUID de regla para ver qué regla se aplica a cada

© 2020 Palo Alto Networks, Inc.

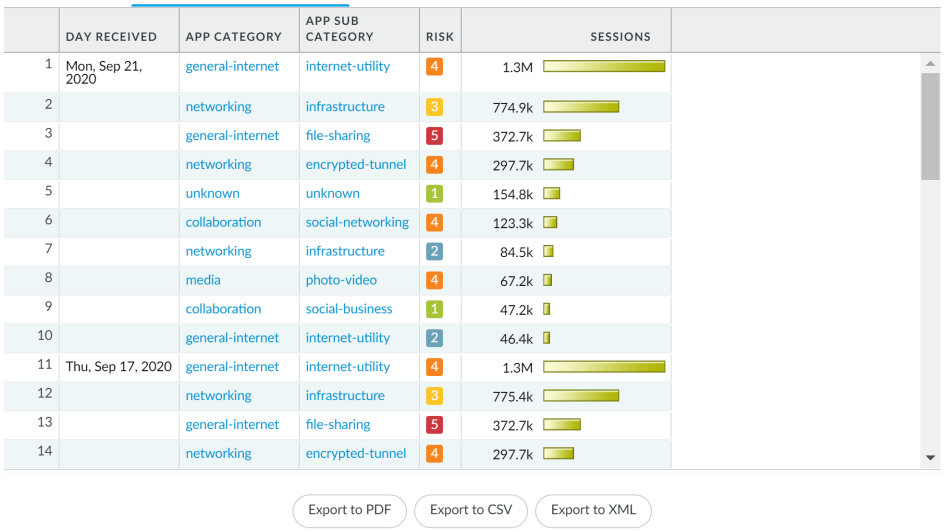
tipo de amenaza. Esta consideración le guiará a la hora de realizar las siguientes selecciones en un informe personalizado:

Selección	Description (Descripción)
Base de datos	Puede basar el informe en uno de los siguientes tipos de bases de datos: • **Summary databases (Bases de datos de resumen)**: hay disponibles para los logs de estadísticas de aplicaciones, tráfico, amenazas, filtrado de URL e inspección de túneles. El cortafuegos agrega los logs detallados en intervalos de 15 minutos. Para habilitar un tiempo de respuesta más rápido al generar informes, el cortafuegos condensa los datos: las sesiones duplicadas se agrupan e incrementan con un contador repetido y ciertos atributos (columnas) se excluyen del resumen. • **Detailed logs (Logs detallados)**: en estas bases de datos se detallan los logs y se enumeran todos los atributos (columnas) de cada entrada de log.  *Los informes basados en logs detallados tardan mucho más en ejecutarse y no se recomiendan a menos que sea absolutamente necesario.*
Atributos	Columnas que quiere utilizar como criterios de coincidencia. Los atributos son las columnas disponibles para su selección en un informe. Desde la lista de **Columnas disponibles**, puede añadir los criterios de selección para datos coincidentes y para agregar la información detallada (**Columnas seleccionadas**).
Ordenar por/Agrupar por	Los criterios **Ordenar por** y **Agrupar por** le permiten organizar/segmentar los datos del informe; los atributos de ordenación y agrupación disponibles varían basándose en el origen de datos seleccionado. La opción Sort By (Ordenar por) especifica el atributo que se utiliza para la agregación. Si no selecciona un atributo según el cual ordenar, el informe devolverá el primer número N de resultados sin ninguna agregación. La opción Agrupar por le permite seleccionar un atributo y utilizarlo como ancla para agrupar datos; a continuación, todos los datos del informe se presentarán en un conjunto de 5, 10, 25 o 50 grupos principales. Por ejemplo, si selecciona Hora para Agrupar por y desea disponer de los 25 grupos principales durante un periodo de 24 horas, los resultados del informe se generan cada hora durante un periodo de 24 horas. La primera columna del informe será la hora y el siguiente conjunto de columnas será el resto de las columnas del informe seleccionadas.
	El siguiente ejemplo muestra el modo en que los criterios **Columnas seleccionadas** y **Ordenar por**/**Agrupar por** trabajan en conjunto al generar informes:

© 2020 Palo Alto Networks, Inc.

Selección	Description (Descripción)
	 Las columnas dentro de un círculo rojo (arriba) muestran las columnas seleccionadas, que son los atributos que deben coincidir para generar el informe. Se analiza cada entrada de log del origen de datos y se establecen las coincidencias con estas columnas. Si varias sesiones tienen los mismos valores para las columnas seleccionadas, las sesiones se agregarán y se incrementará el recuento de repeticiones (o sesiones). La columna dentro de un círculo azul indica el orden de clasificación seleccionado. Cuando se especifica el orden de clasificación (**Ordenar por**), los datos se ordenan (y agregan) según el atributo seleccionado. La columna dentro de un círculo verde indica la selección de **Agrupar por**, que sirve de ancla para el informe. La columna **Group By (Agrupar por)** se utiliza como criterio de coincidencia para filtrar los N grupos principales. A continuación, para cada uno de los N grupos principales, el informe enumera los valores del resto de las columnas seleccionadas.
	Por ejemplo, si un informe tiene las siguientes selecciones:  El resultado será el siguiente:

© 2020 Palo Alto Networks, Inc.

Selección	Description (Descripción)
	Report Setting | **Group By Example (100%)** ×  El informe está anclado por **Day (Día)** y se ordena por **Sessions (Sesiones)**. Enumera los 5 días (**5 grupos**) con el máximo de tráfico en el período de tiempo de **Últimos 7 días**. Los datos se enumeran según las **5 principales** sesiones de cada día para las columnas seleccionadas: **Categoría de aplicación**, **Subcategoría de aplicación** y **Riesgo**.
Time Frame (Período de tiempo)	Intervalo de fechas para el que quiere analizar datos. Puede definir un intervalo personalizado o seleccionar un periodo que vaya desde los últimos 15 minutos hasta los últimos 30 días. Los informes se pueden ejecutar a petición o se pueden programar para su ejecución cada día o cada semana.
Generador de consultas	El generador de consultas le permite definir consultas específicas para ajustar aún más los atributos seleccionados. Le permite ver solamente lo que desee en su informe utilizando los operadores **y** y **o** y un criterio de coincidencia y, a continuación, incluir o excluir datos que coincidan o nieguen la consulta del informe. Las consultas le permiten generar una intercalación de información más centrada en un informe.

Generación de informes personalizados

Puede configurar informes personalizados que el cortafuegos genera inmediatamente (a petición) o según una planificación (cada noche). Para comprender las selecciones disponibles para crear un informe personalizado determinado, consulte informes personalizados.

Una vez que el cortafuegos genera un informe personalizado programado, existe el riesgo de invalidar los resultados anteriores de ese informe si modifica su configuración para cambiar los resultados futuros. Si desea modificar la configuración de un informe programado, se recomienda crear un informe nuevo.

STEP 1 | Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.

STEP 2 | Haga clic en **Add** y, a continuación, introduzca un nombre para el informe en **Name**.

© 2020 Palo Alto Networks, Inc.

Para basar un informe en una plantilla predefinida, haga clic en Cargar plantilla y seleccione la plantilla. A continuación, podrá editar la plantilla y guardarla como un informe personalizado.

STEP 3 | Seleccione la **Database** que debe utilizarse para el informe.

Cada vez que cree un informe personalizado, se creará un informe de vista de log automáticamente. Este informe muestra los logs que se utilizaron para crear el informe personalizado. El informe de vista de log utiliza el mismo nombre que el informe personalizado, pero añade la frase (Vista de log) al nombre del informe.

Al crear un grupo de informes, puede incluir el informe Vista de log con el informe personalizado. Para obtener más información, consulte Gestión de grupos de informes.

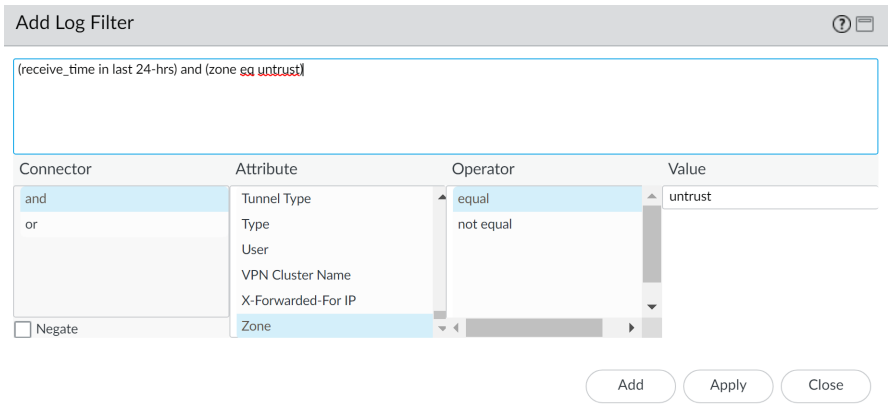
STEP 4 | Seleccione la casilla de verificación **Programado** para ejecutar el informe cada noche. A continuación, el informe estará disponible para su visualización en la columna **Reports (Informes)** del lateral.

STEP 5 | Defina los criterios de filtrado. Seleccione el **Time Frame (Período de tiempo)**, el orden **Sort By (Ordenar por)** y la preferencia **Group By (Agrupar por)**, y seleccione las columnas que deben mostrarse en el informe.

STEP 6 | (Opcional) Seleccione los atributos de **Query Builder (Generador de consultas)** si desea limitar aún más los criterios de selección. Para crear una consulta de informe, especifique lo siguiente y haga clic en **Add (Añadir)**. Repita las veces que sean necesarias para crear la consulta completa.

- **Connector (Conector)**: seleccione el conector (y/o) para preceder la expresión que está agregando.
- **Negar**: Seleccione la casilla de verificación para interpretar la consulta como una negativa. Si, por ejemplo, decide hacer coincidir las entradas de las últimas 24 horas o se originan en la zona no fiable, la opción de negación produce una coincidencia en las entradas que no se hayan producido en las últimas 24 horas o no pertenezcan a la zona no fiable.
- **Attribute (Atributo)**: seleccione un elemento de datos. Las opciones disponibles dependen de la elección de la base de datos.
- **Operator (Operador)**: seleccione el criterio para determinar si se aplica el atributo (como =). Las opciones disponibles dependen de la elección de la base de datos.
- **Value (Valor)**: Especifique el valor del atributo para coincidir.

Por ejemplo, la siguiente figura (basada en la base de datos `Traffic Log`) muestra una consulta que coincide si se ha recibido la entrada de log de tráfico de la zona no fiable en las últimas 24 horas.



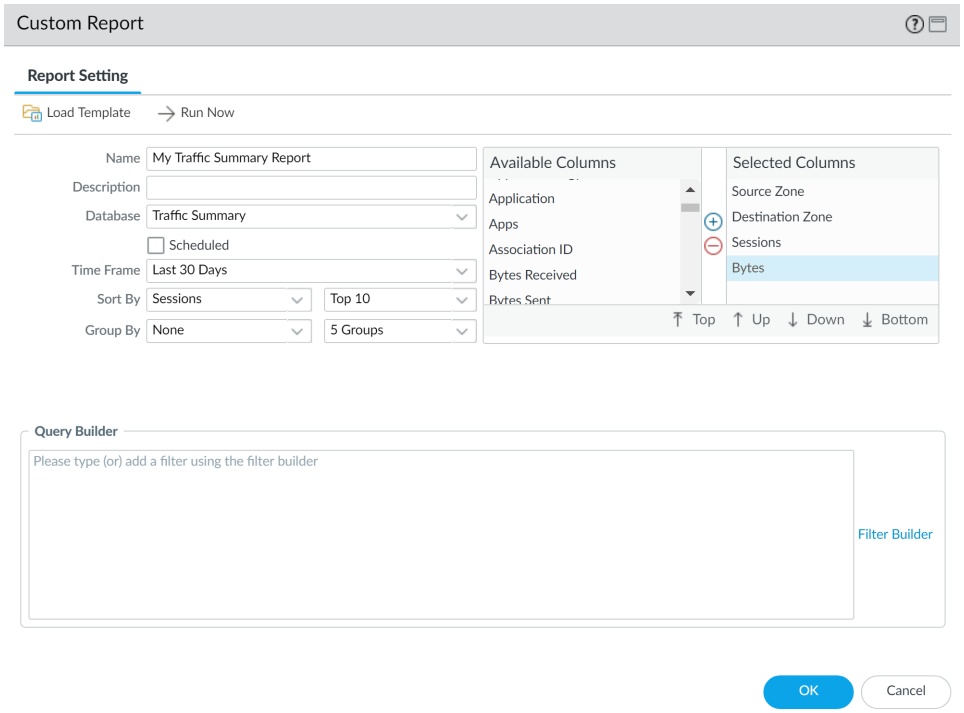
© 2020 Palo Alto Networks, Inc.

STEP 7 | Para comprobar los ajustes de informes, seleccione **Run now (Ejecutar ahora)**. Modifique los ajustes según sea necesario para cambiar la información que se muestra en el informe.

STEP 8 | Haga clic en **OK (Aceptar)** para guardar el informe personalizado.

Ejemplos de informes personalizados

Si desea configurar un informe sencillo en el que utiliza la base de datos de resumen de tráfico de los últimos 30 días y ordena los datos por las 10 sesiones principales y dichas sesiones se agrupan en 5 grupos por día de la semana. Debería configurar el informe personalizado para que tuviera un aspecto parecido a este:



Y el resultado en PDF del informe debería tener un aspecto parecido a este:

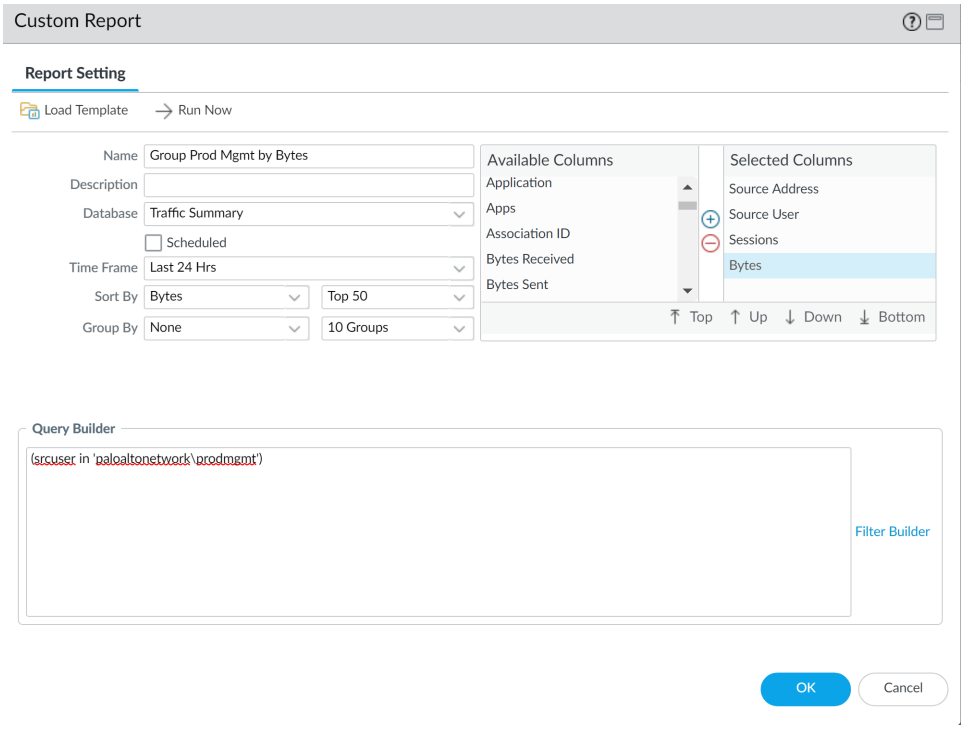
My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

Source Zone	Destination Zone	App Category	Application	Sessions	Bytes
Tap	Tap	general-internet	web-browsing	74.54 M	2.47 T
Tap	Tap	networking	dns	52.03 M	28.93 G
Tap	Tap	networking	ssl	18.01 M	678.13 G
Tap	Tap	general-internet	bittorrent	9.80 M	1.62 T
Tap	Tap	general-internet	google-base	4.48 M	168.99 G
Tap	Tap	unknown	insufficient-data	4.45 M	31.30 G
Tap	Tap	collaboration	facebook-base	4.09 M	99.14 G
Tap	Tap	networking	ntp	4.07 M	3.29 G
Tap	Tap	collaboration	blackboard	2.84 M	186 G
Tap	Tap	collaboration	smtp	1.92 M	172.57 G
Tap	Tap	networking	icmp	1.36 M	320.49 M
Tap	Tap	general-internet	gnutella	1.17 M	17.84 G
Tap	Tap	collaboration	myspace-base	1.10 M	35.22 G
Tap	Tap	general-internet	ping	1.06 M	86.21 M
Tap	Tap	general-internet	flash	1.01 M	168.14 G

© 2020 Palo Alto Networks, Inc.

Ahora, si quiere utilizar el generador de consultas para generar un informe personalizado que represente a los principales consumidores de los recursos de red dentro de un grupo de usuarios, debería configurar el informe para que tuviera un aspecto parecido a este:



El informe debería mostrar a los principales usuarios del grupo de usuarios de gestión de productos ordenados por bytes.

Generación de informes de Botnet

El informe de Botnet le permite utilizar mecanismos heurísticos y basados en el comportamiento para identificar posibles hosts infectados por Botnet en la red. Para evaluar la actividad de botnet y los hosts infectados, el cortafuegos relaciona los datos de actividad de red en los logs de amenazas, URL y filtrado de datos con la lista de URL de malware de PAN-DB, proveedores de DNS dinámico conocidos y dominios registrados en los últimos 30 días. Puede configurar el informe para identificar hosts que visitaron esos sitios, así como hosts que se comunicaron con los servidores de Internet Relay Chat (IRC) o que usaron aplicaciones desconocidas. El malware a menudo usa DNS dinámicas para evitar el bloqueo de IP, mientras que los servidores IRC a menudo usan bot para funciones automatizadas.

El cortafuegos requiere licencias de Threat Prevention y Filtrado de URL para usar el informe de botnet. Puede Use el motor de correlación automatizada. *para supervisar actividades malintencionadas según indicadores adicionales a los que usa el informe de botnet. Sin embargo, el informe de botnet es la única herramienta que usa dominios registrados recientemente como un indicador.*

- Configuración de un informe de botnet
- Interpretación de los resultados del informe de botnet

© 2020 Palo Alto Networks, Inc.

Configuración de un informe de botnet

Puede programar un informe de botnet o ejecutarlo según demanda. El cortafuegos genera informes de botnet programados cada 24 horas porque la detección basada en comportamiento requiere que se correlacione tráfico en múltiples logs a lo largo de ese intervalo de tiempo.

STEP 1 | Defina los tipos de tráfico que indican una posible actividad de botnet.

1. Seleccione **Monitor (Supervisar)** > **Botnet** y haga clic en **Configuration (Configuración)** a la derecha de la página.
2. Habilite con **Enable (Habilitar)** y defina el conteo con **Count (Recuento)** para cada tipo de Tráfico HTTP que desea que incluya el informe.

   Los valores de **Count** representan el número mínimo de eventos de cada tipo de tráfico que deben producirse para que el informe enumere el host asociado con una puntuación de confianza más alta (mayor probabilidad de infección de botnet). Si el número de eventos es inferior al **Count**, el informe mostrará una puntuación de confianza inferior o (para ciertos tipos de tráfico) no se mostrará una entrada para el host. Por ejemplo, si define el **Count (Recuento)** en tres para **Malware URL visit (Visita URL de malware)**, los hosts que ingresen en tres o más URL de malware conocidos tendrán mayores puntuaciones que los hosts que ingresen en menos de tres. Para obtener más información, consulte Interpretación de los resultados del informe de botnet.
3. Defina los umbrales que determinan si el informe incluirá hosts asociados con el tráfico que incluya aplicaciones TCP o UDP desconocidas.
4. Seleccione la casilla de verificación **IRC** para incluir tráfico que relacionado con servidores IRC.
5. Haga clic en **OK (Aceptar)** para guardar la configuración del informe.

STEP 2 | Programe el informe o ejecútelo según demanda.

1. Haga clic en **Report Setting** en la parte derecha de la página.
2. Seleccione un intervalo de tiempo para el informe en la lista desplegable **Test Run Time Frame (Marco de tiempo de ejecución de prueba)**.
3. Indique en **No. of Rows (Número de filas)** el número de filas que desee incluir en el informe.
4. (Opcional) Utilice la opción **Add (Añadir)** para añadir entradas en Query Builder (Generador de consultas) con el fin de filtrar el informe por atributos como direcciones IP de origen o destino, usuarios o zonas.

   Por ejemplo, si conoce por adelantado que el tráfico iniciado desde la dirección IP 10.3.3.15 no contiene una actividad de botnet potencial, añada `not (addr.src in 10.0.1.35)` como consulta para excluir ese host desde los resultados del informe. Para obtener más información, consulte Interpretación de los resultados del informe de botnet.
5. Seleccione **Scheduled** para ejecutar el informe diariamente o haga clic en **Run Now** para ejecutar el informe inmediatamente.
6. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Interpretación de los resultados del informe de botnet

El informe de botnet muestra una línea para cada host que está asociado con el tráfico que haya definido como sospechoso cuando configuró el informe. Para cada host, el informe muestra una puntuación de confianza de 1 a 5 para indicar la probabilidad de infección de botnet, donde 5 indica la probabilidad de infección más alta. Las puntuaciones corresponden a los niveles de gravedad de las amenazas: 1 es informativa, 2 es baja, 3 es media, 4 es alta y 5 es crítica. El cortafuegos basa las puntuaciones en:

- **Tipo de tráfico**: ciertos tipos de tráfico HTTP tienen más probabilidad de implicar actividad de botnet. Por ejemplo, el informe asigna una mayor confianza a los hosts que visitan URL de malware conocido que a los hosts que navegan a dominios de IP en lugar de URL, asumiendo que ha definido que ambas actividades son sospechosas.

© 2020 Palo Alto Networks, Inc.

- **Cantidad de eventos**: los hosts que están asociados a un número mayor de eventos sospechosos tendrán mayores puntuaciones de confianza en función de los umbrales (valores de **Count [Recuento]**) que usted define cuando realiza la Configuración de un informe de botnet.
- **Descargas ejecutables**: el informe asigna una mayor confianza a los hosts que descargan archivos ejecutables. Los archivos ejecutables son parte de muchas infecciones y, si se combinan otros tipos de tráfico sospechoso, puede ayudarle a priorizar sus investigaciones de hosts comprometidos.

Cuando revisa los resultados del informe, puede detectar que los orígenes que usa el cortafuegos para evaluar la actividad del botnet (por ejemplo, la lista de URL de malware en PAN-DB) tiene carencias. También puede averiguar que estos orígenes identifican el tráfico que considere seguro. Para compensar en ambos casos, puede agregar filtros de consulta cuando realiza una Configuración de un informe de botnet.

Generación de informes de uso de la aplicación SaaS

El informe en PDF de la utilización de la aplicación de SaaS es un informe de dos partes que le permite explorar la actividad de la aplicación de SaaS por riesgo y estado de aprobación. Una aplicación aprobada es una aplicación que aprueba formalmente para que se utilice en su red. Una aplicación SaaS es una aplicación que tiene la característica SaaS=yes en la página de detalles de las aplicaciones en **Objects (Objetos)** > **Applications (Aplicaciones)**; todas las demás aplicaciones se consideran como no SaaS. Para indicar que ha aprobado una aplicación SaaS o no SaaS, debe etiquetarla con la etiqueta predefinida denominada Sanctioned (Aprobado). El cortafuegos y Panorama consideran cualquier aplicación sin esta etiqueta predefinida como no aprobada para usar en la red.

- La primera parte del informe presenta los hallazgos de clave para las aplicaciones de SaaS en su red durante el período del informe con una comparación de las aplicaciones aprobadas y no aprobadas. Además, enumera las principales aplicaciones en función del estado de aprobación por uso, cumplimiento y transferencias de datos. Para ayudarle a identificar y explorar el alcance de la utilización de aplicaciones de alto riesgo, la sección de aplicaciones con características riesgosas del informe enumera las aplicaciones de SaaS con las siguientes características de host desfavorables: certificaciones alcanzadas, brechas de seguridad pasadas, compatibilidad con restricciones basadas en IP, viabilidad financiera y términos de servicio. También puede ver una comparación de aplicaciones SaaS aprobadas frente a no aprobadas según el número total de aplicaciones utilizadas en su red, el ancho de banda consumido por estas aplicaciones, la cantidad de usuarios que utilizan estas aplicaciones, los principales grupos de usuarios que utilizan la mayor cantidad de aplicaciones SaaS, y los principales grupos de usuarios que transfieren el mayor volumen de datos a través de aplicaciones SaaS aprobadas y no aprobadas. La primera parte del informe también resalta las principales subcategorías de aplicaciones SaaS enumeradas en orden según la cantidad máxima de aplicaciones usadas, la cantidad de usuarios y la cantidad de datos (bytes) transferidos en cada subcategoría de aplicación.
- La segunda parte del informe se concentra en la información de navegación detallada para aplicaciones SaaS y no SaaS para cada subcategoría de aplicación enumerada en la primera parte del informe. Para cada aplicación en una subcategoría, también incluye información sobre los principales usuarios que transfirieron datos, los principales tipos de archivos boqueados o con alertas, y las principales amenazas para cada aplicación. Además, esta sección del informe cuenta las muestras para cada aplicación que el cortafuegos envió para el análisis de WildFire y la cantidad de muestras que se clasificaron como benignas y malintencionadas.

Use la información de este informe para consolidar la lista de aplicaciones SaaS aprobadas y críticas de la empresa, y para aplicar las políticas para controlar las aplicaciones no aprobadas y riesgosas que representan un riesgo innecesario para la propagación del malware y la pérdida de datos.

El informe predefinido de uso de aplicaciones SaaS aún se puede ver a diario (consulte Visualización de informes). En él se enumeran las cien aplicaciones SaaS principales (es decir, las que tengan la característica SaaS=yes) que se ejecutan en la red en un

© 2020 Palo Alto Networks, Inc.

día concreto. Este informe no ofrece visibilidad de las aplicaciones que diseñó como se sancionaron; en cambio, ofrece visibilidad de todas las aplicaciones de SaaS en uso en su red.

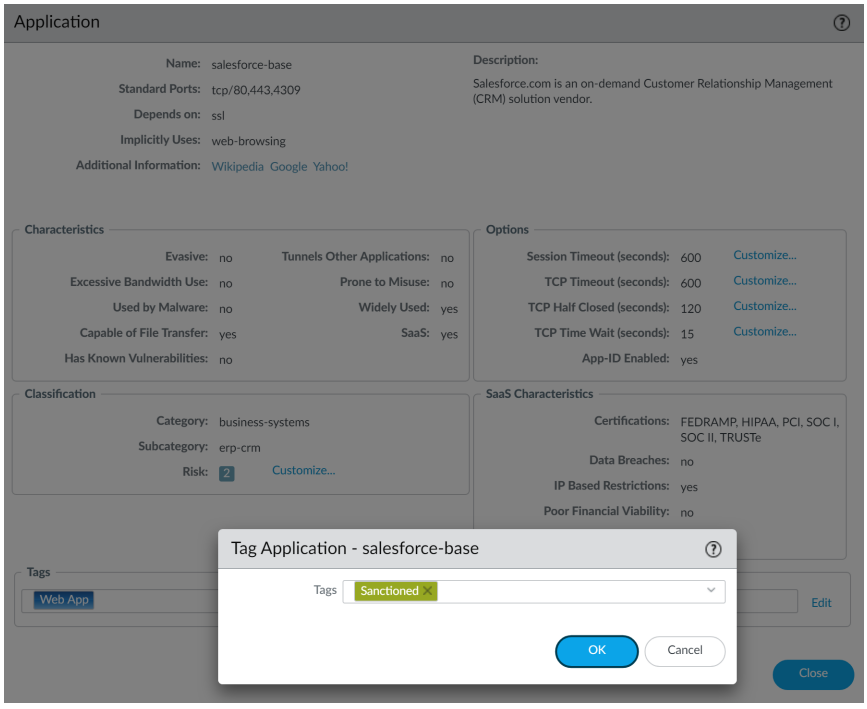
STEP 1 | Etiquete las aplicaciones que aprueba para su uso en la red como Sanctioned.

Para generar un informe correcto e informativo, debe etiquetar las aplicaciones aprobadas de manera consistente en los contrafuegos con múltiples sistemas virtuales y en los cortafuegos que pertenecen a un grupo de dispositivos en Panorama. Si la misma aplicación está etiquetada como aprobada en un sistema virtual y como no aprobada en otro, o en Panorama, si una aplicación no está aprobada en un grupo de dispositivos primarios pero está etiquetada como aprobada en un grupo de dispositivos secundarios (o viceversa), el informe de uso de la aplicación SaaS informará la aplicación como parcialmente aprobada y mostrará resultados superpuestos.

Ejemplo: Si Box es sancionada en vsys1 y Google Drive es sancionada en vsys2, los usuarios de Google Drive en vsys1 se contarán como usuarios de una aplicación SaaS no sancionada y los usuarios de Box en vsys2 se contarán como usuarios de una aplicación SaaS no sancionada. El resultado principal en el informe destacará que un total de dos aplicaciones SaaS únicas se detectan en la red con dos aplicaciones sancionadas y dos aplicaciones no sancionadas.

1. Seleccione **Objects (Objetos)** > **Applications (Aplicaciones)**.
2. Haga clic en el nombre de la aplicación en **Name** para editar una aplicación y seleccione **Edit** en la sección Tag.
3. Seleccione **Sanctioned** en la lista desplegable **Tags**.

   Debe utilizar una etiqueta **Sanctioned (Sancionada)** predefinida (Sanctioned). Si usa cualquier otra etiqueta para indicar que aprobó la aplicación, el cortafuegos no reconocerá la etiqueta y el informe será impreciso.



4. Haga clic en **OK** y **Close** para salir de todos los cuadros de diálogo abiertos.

STEP 2 | Configure el informe de uso de aplicación SaaS.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **SaaS Application Usage (Uso de aplicación SaaS)**.
2. Haga clic en **Add**, introduzca un nombre en **Name** y seleccione un **Time Period** para el informe (el valor por defecto es **Last 7 Days**).

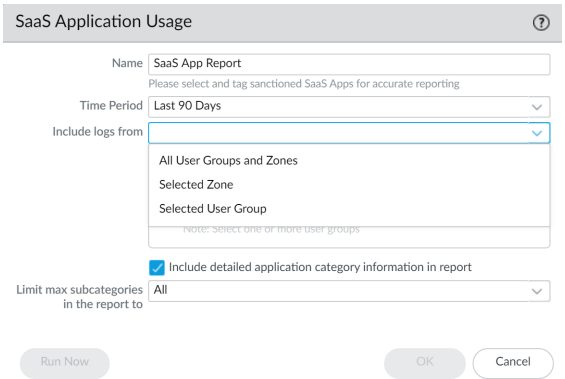
   Por defecto, el informe incluye información detallada sobre las principales subcategorías de aplicación SaaS y no SaaS, lo cual puede hacer que el informe sea grande en cuanto a páginas y tamaño de archivo. Desmarque la casilla de verificación Include detailed application category information in report (Incluir información de categoría de aplicación detallada en el informe) si desea reducir el tamaño de archivo y limitar el recuento de páginas a 10.
3. Seleccione si desea la opción de informe **Include logs from (Incluir logs de)**:

   En PAN-OS 10.0.2 y versiones posteriores, los informes generados a partir de logs en Cortex Data Lake solo admiten logs de la zona seleccionada.

   - **All User Groups and Zones (Todos los grupos de usuarios y zonas)**: el informe incluye datos sobe todas las zonas de seguridad y grupos de usuarios disponibles en los logs.

     Si desea incluir grupos de usuarios específicos en el informe, seleccione **Include user group information in the report (Incluir información de grupo de usuarios en el informe)** y haga clic en el enlace **manage groups (gestionar grupos)** para seleccionar los grupos que desea incluir. Debe añadir entre uno y un máximo de 25 grupos de usuario, de manera que el cortafuegos o Panorama puedan filtrar los logs para los grupos de usuario seleccionados. Si selecciona los grupos para incluir, el informe agregará a todos los grupos de usuario en un solo grupo denominado Others (Otros).
   - **Selected Zone (Zona seleccionada)**: el informe filtra los datos para la zona de seguridad especificada e incluye los datos de esa zona únicamente.

     Si desea incluir grupos de usuarios específicos en el informe, seleccione **Include user group information in the report (Incluir información de grupo de usuarios en el informe)** y haga clic en el enlace **manage groups for selected zone (gestionar grupos de zona seleccionada)** para seleccionar los grupos de usuarios dentro de esta zona que desea incluir en el informe. Debe añadir entre uno y un máximo de 25 grupos de usuario, de manera que el cortafuegos o Panorama puedan filtrar los logs para los grupos de usuario seleccionados dentro de la zona de seguridad. Si selecciona los grupos para incluir, el informe agregará a todos los grupos de usuario en un solo grupo denominado Others (Otros).
   - **Selected User Group (Grupo de usuarios seleccionados)**: el informe filtra los datos para el grupo de usuarios especificado únicamente e incluye la información de uso de aplicación de SaaS para el grupo de usuarios seleccionado únicamente.



4. Seleccione si desea incluir todas las subcategorías de la aplicación en el informe (opción predeterminada) o **Limit the max subcategories in the report (Limitar las subcategorías máx. en**

© 2020 Palo Alto Networks, Inc.

el informe) a las principales 10, 15, 20 o 25 categorías (la opción predeterminada es todas las subcategorías).

5. Haga clic en **Run Now (Ejecutar ahora)** para generar el informe a pedido para el periodo de los últimos 7 días y los últimos 30 días. Asegúrese de que el bloqueador de elementos emergentes esté deshabilitado en su navegador, debido a que el informe se abre en una nueva pestaña.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 3 | Programación de informes para entrega de correos electrónicos.

El informe de los últimos 90 días debe programarse para el envío por correo electrónico.

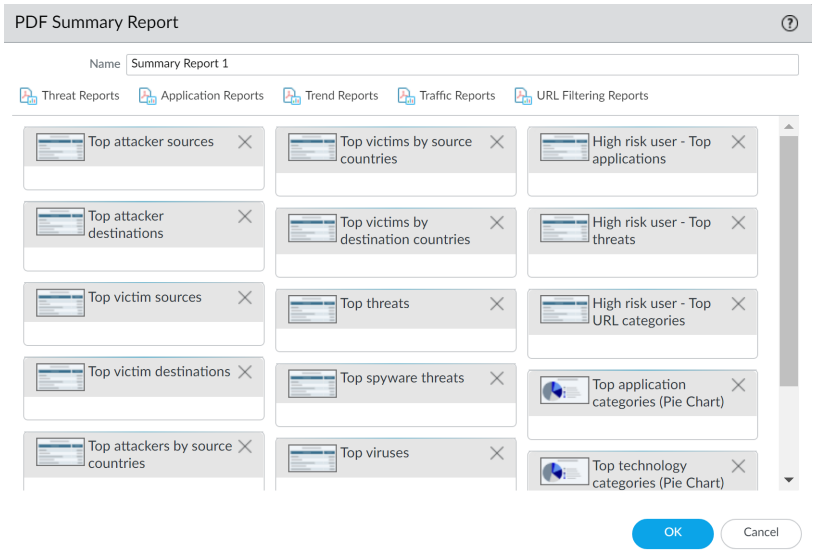
En los cortafuegos PA-220R y PA-800 Series, el informe de uso de aplicaciones SaaS no se envía como PDF adjunto al correo electrónico. En lugar de eso, el correo electrónico incluye un enlace en el que debe hacer clic para abrir el informe en un explorador web.

Gestión de informes de resumen en PDF

Los informes de resumen en PDF contienen información recopilada de informes existentes, basándose en datos de los 5 principales de cada categoría (en vez de los 50 principales). También pueden contener gráficos de tendencias que no están disponibles en otros informes.

STEP 1 | Configure un **Informe de resumen en PDF**.

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **Manage PDF Summary (Gestionar resumen en PDF)**.
2. Haga clic en **Add** y, a continuación, introduzca un nombre para el informe en **Name**.
3. Utilice la lista desplegable para cada grupo de informes y seleccione uno o varios de los elementos para diseñar el informe de resumen en PDF. Puede incluir un máximo de 18 elementos de informe.



Si se selecciona Top Threats (Amenazas principales) aparece `top-attacks` *en la columna Predefined Widgets (Widgets predefinidos) en el Informe de resumen en PDF.*

- Para eliminar un elemento del informe, haga clic en el icono **x** o cancele la selección del menú desplegable para el grupo de informes adecuado.
- Para reorganizar los informes, arrastre y coloque los iconos de elemento en otra área del informe.

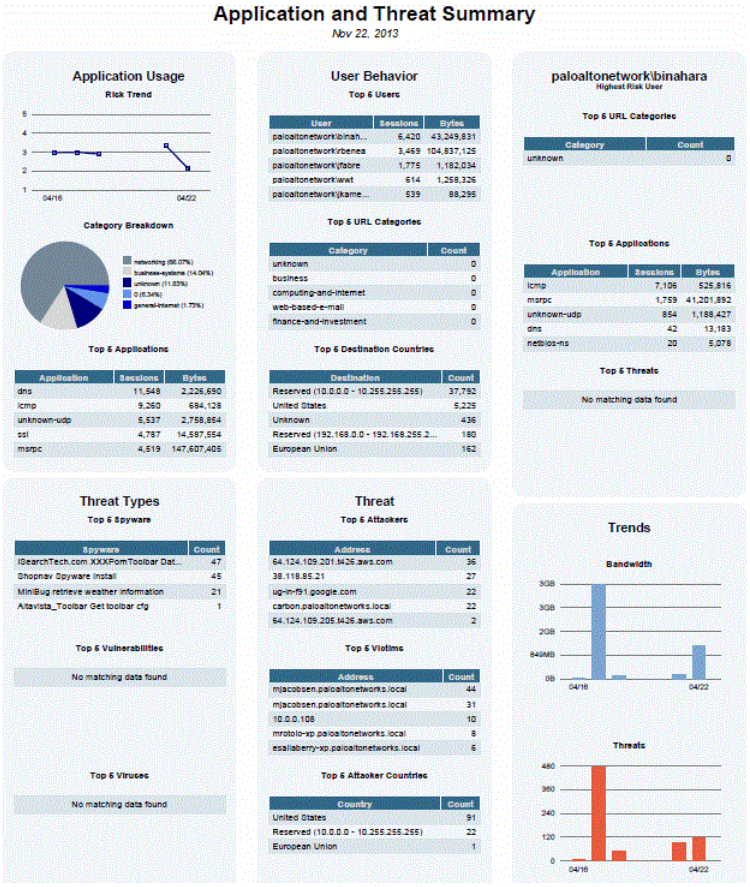
4. Haga clic en **ACEPTAR** para guardar el informe.

© 2020 Palo Alto Networks, Inc.

5. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 2 | Vea el informe.

Para descargar y ver el informe de resumen en PDF, consulte Visualización de informes.



Las siguientes secciones de resumen hacen referencia a los elementos del Informe de resumen en PDF que se detallan a continuación:

- ***Top 5 Attacks (Cinco ataques principales)**: hace referencia al elemento Top threats (Amenazas principales).*
- ***Top 5 Threats (Cinco amenazas principales)**: hace referencia al elemento High risk user - Top threats (Usuario de riesgo alto: amenazas principales).*
- *Top Threats report (Informe sobre amenazas principales): hace referencia a la lista completa de amenazas del elemento Top threats (Amenazas principales).*

Generación de informes de actividad del usuario/grupo

Los informes de actividad de grupo/usuario resumen la actividad web de usuarios individuales o grupos de usuarios. Ambos informes incluyen la misma información, excepto **Browsing Summary by URL Category** y **Browse time calculations**, que se incluyen en informes de actividad del usuario únicamente.

Debe configurar User-ID en el cortafuegos para acceder a lista de usuarios/grupos de usuarios.

STEP 1 | Configurar los tiempos de exploración y número de logs para informes de actividad de grupo/usuario.

© 2020 Palo Alto Networks, Inc.

Solo es obligatorio si desea cambiar los valores predeterminados.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, edite la configuración de creación de logs e informes, y seleccione la pestaña **Log Export and Reporting (Exportación e informes de logs)**.
2. En **Max Rows in User Activity Report (Filas máximas en informe de actividad de usuario)**: introduzca el número máximo de filas que se admite para los informes de actividad detallada del usuario (intervalo: 1-1048576; valor por defecto: 5000). Escriba el número de logs que analiza el informe.
3. Introduzca el **Average Browse Time** en segundos que estima que los usuarios deberían tardar en explorar una página web (intervalo: 0-300 segundos; por defecto: 60). Cualquier solicitud realizada después de que haya transcurrido el tiempo medio de exploración se considerará una nueva actividad de exploración. El cálculo usa Registro solo de las páginas que visita un usuario (iniciado en los logs de filtrado de URL) como base e ignorará las páginas web nuevas que se carguen entre el momento de la primera solicitud (hora de inicio) y el tiempo medio de exploración. Por ejemplo, si define que el **Average Browse Time** es de 2 minutos y un usuario abre una página web y visualiza dicha página durante 5 minutos, el tiempo de exploración de dicha página seguirá siendo de 2 minutos. Esto es así porque no hay forma de determinar durante cuánto tiempo un usuario visualiza una página concreta. El cálculo del tiempo medio de exploración ignorará los sitios categorizados como anuncios web y redes de entrega de contenido.
4. En **Page Load Threshold**, introduzca el tiempo previsto en segundos que tardan los elementos de una página en cargarse en la página (el valor por defecto es 20). Cualquier solicitud que se produzca entre la primera carga de la página y el umbral de carga de página se considerará que son elementos de la página. Cualquier solicitud que se produzca fuera del umbral de carga de página se considerará que es el usuario haciendo clic en un enlace de la página.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 2 | Genere el informe de actividad de grupo/usuario.

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **User Activity Report (Informe de actividad del usuario)**.
2. Haga clic en **Add** y, a continuación, introduzca un nombre para el informe en **Name**.
3. Cree el informe:
   - Informe de actividad del usuario: seleccione **User (Usuario)** e introduzca el nombre de usuario en **Username (Nombre de usuario)** o la dirección IP en **IP address (Dirección IP)** (IPv4 o IPv6) del usuario.
   - Informe de actividad de grupo: seleccione **Group** y elija el **Group Name** del grupo de usuarios.
4. Seleccione el **Time Period** del informe.
5. (Opcional) Seleccione la casilla de verificación **Include Detailed Browsing (Incluir exploración detallada)** (de manera predeterminada, no está seleccionada) para incluir logs de URL detallados en el informe.

   La información de navegación detallada puede incluir un gran volumen de logs (miles de logs) para el usuario o grupo de usuarios seleccionado y puede hacer que el informe sea muy extenso.
6. Para ejecutar el informe a petición, haga clic en **Run Now (Ejecutar ahora)**.
7. Para guardar la configuración del informe, haga clic en **OK**. No puede guardar la salida de los informes de actividad de grupo/usuario. Puede programar la entrega por correo electrónico del informe; consulte la Programación de informes para entrega de correos electrónicos.

Gestión de grupos de informes

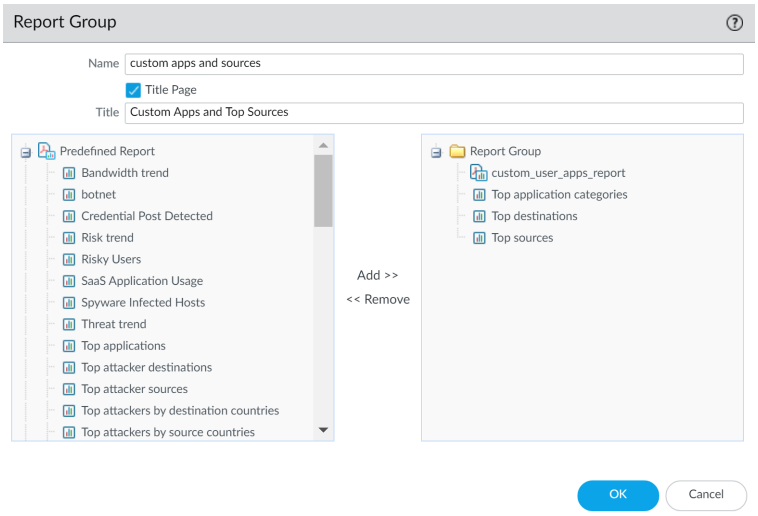
Los grupos de informes le permiten crear conjuntos de informes que el sistema puede recopilar y enviar como un informe agregado en PDF único con una página de título opcional y todos los informes constituyentes incluidos.

© 2020 Palo Alto Networks, Inc.

Configure grupos de informes.

Debe configurar un **Grupo de informes** para enviar informes por correo electrónico.

1. Cree un perfil de servidor de correo electrónico.
2. Defina el **Grupo de informes**. Un grupo de informes puede compilar informes predefinidos, informes de resumen en PDF, informes personalizados e informes Vista de log en un único PDF.
   1. Seleccione **Monitor (Supervisar)** > **Report Group (Grupo de informes)**.
   2. Haga clic en **Add** e introduzca un nombre para el grupo de informes en **Name**.
   3. (Opcional) Seleccione la **Title Page (Título de página)** y añada un **Title (Título)** para el PDF creado.
   4. Seleccione informes de la columna izquierda y haga clic en **Add** para mover cada informe al grupo de informes en la derecha.



   El informe **Log View (Ver log)** es un tipo de informe que se crea automáticamente cada vez que crea un informe personalizado y utiliza el mismo nombre que el informe personalizado. Este informe mostrará los logs que se han utilizado para crear el contenido del informe personalizado.

   Para incluir los datos de vista de log al crear un grupo de informes, añada su informe personalizado a la lista **Custom Reports (Informes personalizados)** y, a continuación, para añadir el informe Vista de log, seleccione el nombre del informe coincidente en la lista **Log View (Vista de log)**. El informe incluirá los datos del informe personalizado y los datos de log que se han utilizado para crear el informe personalizado.
5. Haga clic en **OK (Aceptar)** para guardar los ajustes.
6. Para utilizar el grupo de informes, consulte Programación de informes para entrega de correos electrónicos.

Programación de informes para entrega de correos electrónicos

Los informes se pueden programar para una entrega diaria o semanal en un día especificado. Los informes programados comienzan a ejecutarse a las 2:00 AM y la entrega de correo electrónico comienza después de que se hayan generado todos los informes programados.

STEP 1 | Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **Email Scheduler (Programador de correo electrónico)** y haga clic en **Add (Añadir)**.

STEP 2 | Introduzca un nombre en **Name** para identificar la programación.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Seleccione el **Grupo de informes** para la entrega de correos electrónicos. Para configurar un grupo de informes, consulte Gestión de grupos de informes.

STEP 4 | En **Email Profile (Perfil de correo electrónico)**, seleccione un perfil de servidor de correo electrónico que se utilizará para entregar los informes o haga clic en el enlace **Email Profile (Perfil de correo electrónico)** para llevar a cabo la Creación de un perfil de correo electrónico.

STEP 5 | Seleccione la frecuencia con la que generar y enviar el informe en **Periodicidad**.

STEP 6 | El campo **Override Email Addresses** le permite enviar este informe exclusivamente a los destinatarios especificados. Cuando añade destinatarios al campo, el cortafuegos no envía el informe a los destinatarios configurados en el perfil de servidor de correo electrónico. Utilice esta opción para las ocasiones en las que el informe vaya dirigido a una persona distinta de los administradores o destinatarios definidos en el perfil de servidor de correo electrónico.

STEP 7 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Gestión de la capacidad de almacenamiento de informes

Los cortafuegos contienen de manera predeterminada 200 MB de almacenamiento dedicado para guardar los informes que generan. En algunos casos, sobre todo en los cortafuegos PA-7000 Series y PA-5200 Series, es posible que deba aumentar el espacio de almacenamiento para poder generar más informes.

STEP 1 | Acceda a la CLI del cortafuegos.

STEP 2 | Confirme cuál es la capacidad actual del cortafuegos para almacenar informes:

El resultado del comando muestra el tamaño del almacenamiento para informes en bytes. A efectos de este procedimiento, el cortafuegos tiene la capacidad predeterminada de 200 MB.

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```

STEP 3 | Verifique si hay almacenamiento suficiente en el cortafuegos para ampliar la capacidad asignada a guardar los informes:

```
admin> show system disk-space
```

```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```

STEP 4 | Incremente la capacidad de almacenamiento de informes como resulte oportuno:

Por ejemplo, se va a aumentar el tamaño del almacenamiento a 1 GB.

```
admin> request report-storage-size set size <0-4>
```


© 2020 Palo Alto Networks, Inc.

```
admin@ISP-CONDOR-B(active)> request report-storage-size set size 1

cfg.report-storage-size-gb: 1
```

STEP 5 | Verifique que se ha aumentado la capacidad a la cantidad configurada en el paso anterior:

```
admin> request report-storage-size show
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

1073741824
```


© 2020 Palo Alto Networks, Inc.

Visualización de la utilización de las reglas de la política

Vea el número de veces que una regla de seguridad, NAT, QoS, reenvío basado en políticas (Policy-Based Forwarding, PBF), descifrado, inspección de túnel, cancelación de aplicación, autenticación o protección DoS coincide con el tráfico para ayudar a que sus políticas de cortafuegos permanezcan actualizadas debido a que su entorno y seguridad deben cambiar. Para evitar que los atacantes aprovechen las posibilidades de acceso aprovisionado en exceso (como cuando retira un servidor o ya no necesita acceso temporal a un servicio), utilice los datos del recuento de resultados de las reglas de las políticas para identificar y eliminar las que no se utilizan.

Los datos de utilización de las reglas de políticas permiten validar las incorporaciones de reglas y los cambios en las reglas, así como supervisar el período durante el que se aplica una regla. Por ejemplo, cuando migra las reglas basadas en un puerto a reglas basadas en una aplicación, crea una regla basada en una aplicación sobre una regla basada en un puerto y comprueba el tráfico que coincide con la regla basada en un puerto. Después de la migración, los datos del recuento de resultados permiten determinar si la regla basada en un puerto se puede eliminar con seguridad confirmando si el tráfico no coincide con ella, sino con la regla basada en una aplicación. El recuento de resultados de la regla de políticas le ayuda a determinar si una regla es eficaz en la ejecución del acceso.

Puede restablecer los datos del recuento de resultados de la regla de la política para validar una regla existente o medir la utilización de una regla en un período de tiempo especificado. Los datos del recuento de resultados de las reglas de políticas no se almacenan en el cortafuegos ni en Panorama, por lo que los datos dejan de estar disponibles si se restablece (borra) el recuento de resultados.

Después de filtrar su base de reglas de políticas, los administradores pueden tomar medidas para eliminar, deshabilitar, habilitar y etiquetar reglas de políticas directamente desde el optimizador de políticas. Por ejemplo, puede filtrar las reglas no utilizadas y, a continuación, etiquetarlas para su revisión con el fin de determinar si pueden eliminarse de forma segura o mantenerse en la base de reglas. Si se permite que los administradores actúen directamente desde el optimizador de políticas, se reducirá la sobrecarga de gestión necesaria, lo que contribuirá a simplificar la administración del ciclo de vida de las reglas y garantizar que sus cortafuegos no estén sobreaprovisionados.

Como los datos del recuento de resultados de las reglas no se sincronizan entre los cortafuegos de las implementaciones de alta disponibilidad (High Availability, HA), debe iniciar sesión en cada uno de ellos para ver sus respectivos datos o bien usar Panorama para ver la información sobre los peers de los cortafuegos de HA.

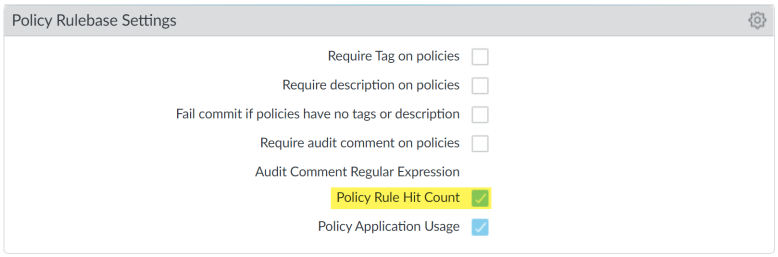
Los datos de uso de las reglas de políticas también resultan útiles cuando emplea Optimización de las reglas de la política de seguridad *para determinar las reglas que migrar o limpiar en primer lugar.*

STEP 1 | Inicio de la interfaz web.

STEP 2 | Verifique que **Policy Rule Hit Count (Recuento de resultados de reglas de políticas)** está marcada.

1. Diríjase a Policy Rulebase Settings (Configuración de base de reglas de políticas) (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**).
2. Verifique que **Policy Rule Hit Count (Recuento de resultados de reglas de políticas)** está marcada.

© 2020 Palo Alto Networks, Inc.



STEP 3 | Seleccione **Policies (Políticas)**.

STEP 4 | Vea la utilización de cada regla de la política:

- **Hit Count (Recuento de resultados)**: el número de veces que el tráfico coincide con el criterio que definió en la regla de la política. Persiste tras el reinicio, el reinicio del plano de datos y las actualizaciones, a menos que restablezca o cambie el nombre de la regla manualmente.
- **Last Hit (Último resultado)**: la marca de tiempo más reciente correspondiente a cuando el tráfico coincidió con la regla.
- **First Hit (Primer resultado)**: la primera instancia de coincidencia entre el tráfico y la regla.
- **Modified (Fecha de modificación)**: fecha y hora de la última modificación de la regla de la política.
- **Modified (Fecha de creación)**: fecha y hora de creación de la regla de la política.

Si la regla se creó cuando Panorama ejecutaba PAN-OS 8.1 y estaba marcada la opción Policy Rule Hit Count (Recuento de resultados de reglas de políticas), se usa la fecha y la hora de First Hit (Primer resultado) en Created (Fecha de creación) al actualizar a PAN-OS 9.0. Si la regla se creó cuando se utilizaba PAN-OS 8.1, pero dicha opción no estaba marcada, o si la regla se creó cuando Panorama ejecutaba PAN-OS 8.0 o una versión anterior, se usa en Created (Fecha de creación) la fecha y la hora cuando se haya actualizado Panorama a PAN-OS 9.0.

		Source			Rule Usage				
NAME	T...	Z...	A...	U...	HIT COUNT	LAST HIT	FIRST HIT	MODIFIED	CREATED
Video	n...	a...	a...	a...	2424328	2020-09-22 11:33:00	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Video Streaming	n...	a...	a...	a...	14337228	2020-09-22 16:26:58	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
cavenger	n...	a...	a...	a...	321760616	2020-09-22 16:27:10	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Web Traffic	n...	a...	a...	a...	1509584361	2020-09-22 16:27:10	2019-07-30 10:12:02	2020-07-27 13:27:16	2019-07-30 09:50
iperf	n...	a...	a...	a...	5	2019-10-15 14:54:31	2019-10-11 13:08:28	2020-07-27 13:27:16	2019-07-30 09:50

STEP 5 | En el cuadro de diálogo Policy Optimizer (Optimizador de políticas), consulte el filtro **Rule Usage (Uso de reglas)**.

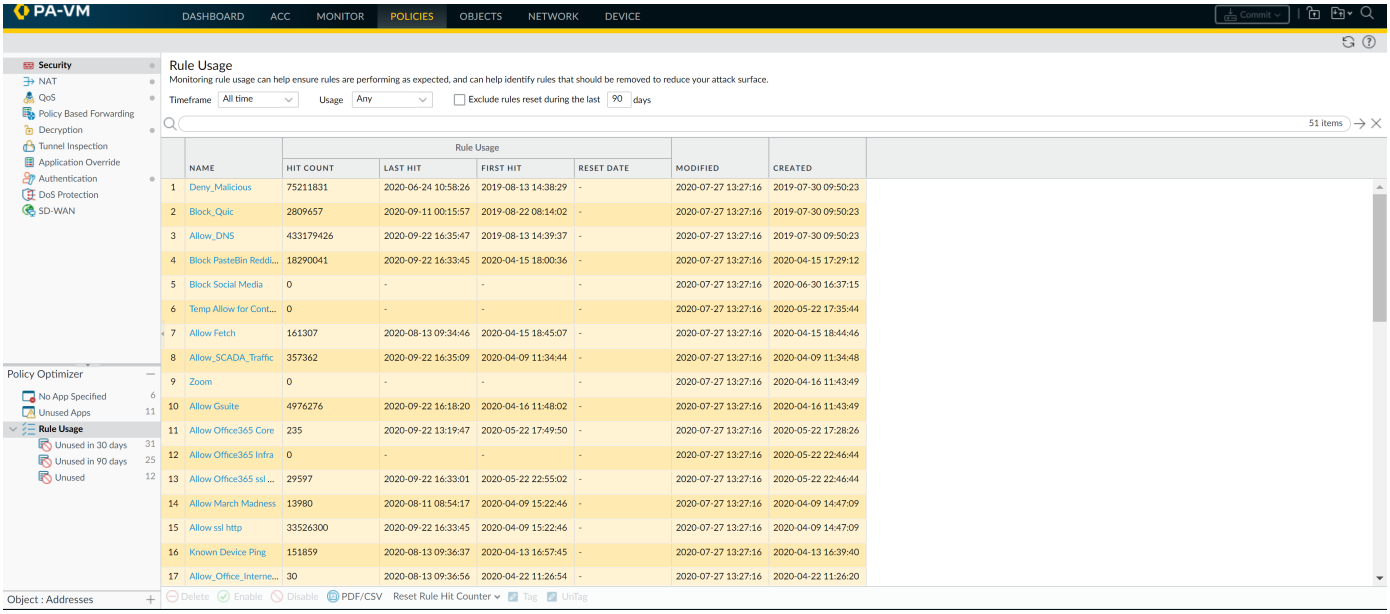
STEP 6 | Filtre las reglas de la base seleccionada.

Use el filtro de uso de las reglas para evaluar su utilización en el período especificado. Por ejemplo, filtre la base de reglas seleccionada por las reglas no utilizadas en los 30 últimos días. También puede evaluar la utilización de las reglas con otros atributos de reglas, como las fechas de creación y de modificación, que le permiten filtrar por el conjunto de reglas correcto que revisar. Estos datos resultan útiles para gestionar la vigencia de las reglas y para determinar si se deben eliminar a fin de reducir la superficie de ataque de la red.

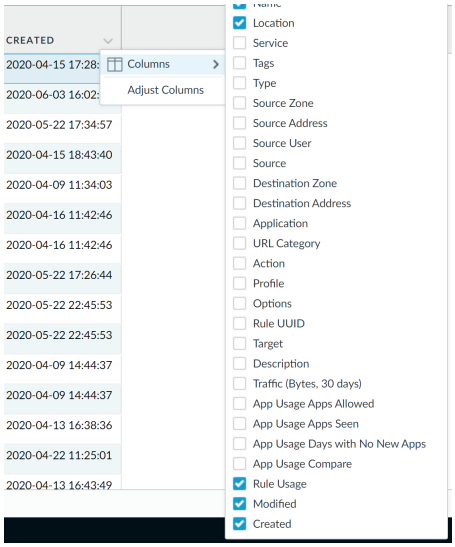
1. Seleccione el **intervalo** por el que dese filtrar o especifique el intervalo **Custom (Personalizado)**.
2. Seleccione la regla **Usage (Uso)** en la que aplicar el filtro.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Si ha restablecido los datos de uso de reglas para cualquier regla, active **Exclude rules reset during the last** *<number of days>* **days (Excluir restablecimiento de reglas durante los últimos <número de días> días)** y decida cuándo excluir una regla en función del número de días que especifique desde que se restableció la regla. En los resultados filtrados se incluyen solo las reglas restablecidas antes del número de días especificado.

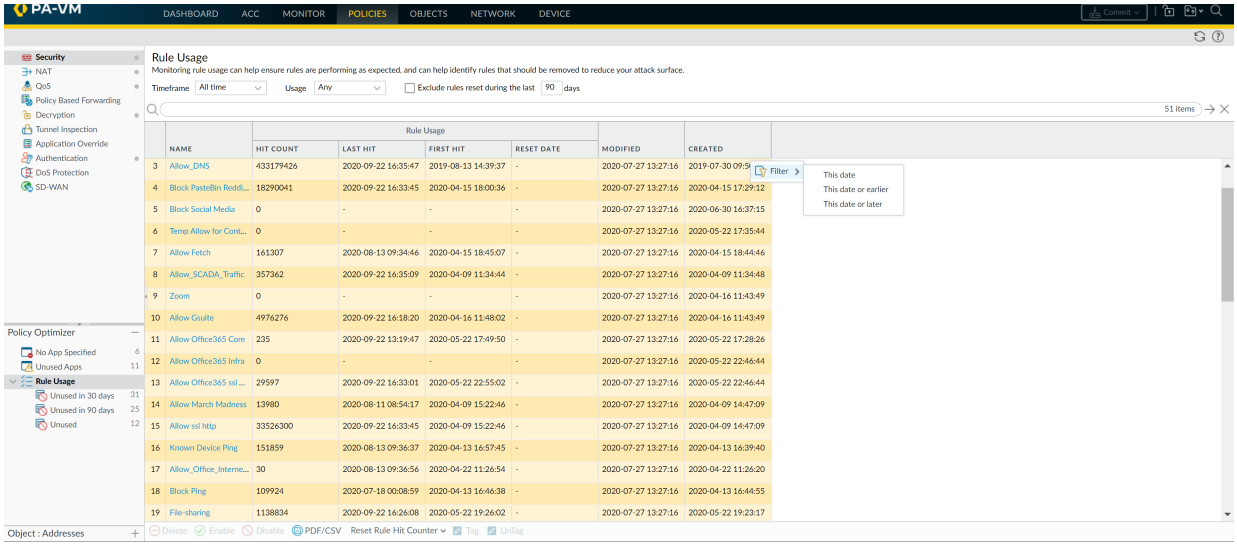


4. (Opcional) Especifique filtros de búsqueda basados en datos de reglas.
    1. Coloque el cursor sobre el encabezado de la columna y **Columns (Columnas)**.
    2. Añada cualquier columna adicional que quiera que aparezca o que desee usar para el filtro.



3. Coloque el cursor sobre los datos de columna que desee filtrar en **Filter (Filtro)**. Si los datos contienen fechas, seleccione la opción de filtro adecuada: **This date (Esta fecha)**, **This date or earlier (Esta fecha o una anterior)** o **This date or later (Esta fecha o una posterior)**.
4. **Aplique el filtro** (→).

© 2020 Palo Alto Networks, Inc.



STEP 7 | Actúe sobre una o más reglas de políticas no utilizadas.

1. Seleccione una o más reglas de políticas no utilizadas.
2. Lleve a cabo una de las siguientes acciones:
   - **Delete (Eliminar)**: permite eliminar una o más reglas de políticas seleccionadas.
   - **Enable (Habilitar)**: permite activar una o más reglas de políticas seleccionadas cuando están deshabilitadas.
   - **Disable (Deshabilitar)**: permite desactivar una o más reglas de políticas seleccionadas.
   - **Tag (Etiquetar)**: permite aplicar una o más etiquetas de grupo a una o más reglas de políticas seleccionadas. Para etiquetar la regla de políticas, la etiqueta de grupo ya debe existir.
   - **Untag (Desetiquetar)**: permite eliminar una o más etiquetas de grupo de una o más reglas de políticas seleccionadas.
3. **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Uso de servicios externos para la monitorización

El uso de un servicio externo para monitorizar el cortafuegos le permite recibir alertas de eventos importantes, archivar información monitorizada de sistema con almacenamiento dedicado a largo plazo e integrarse con herramientas de monitorización de seguridad de terceros. Los siguientes son escenarios comunes para el uso de servicios externos:

- Para una notificación inmediata de amenazas o eventos de sistema importantes, puede utilizar la Supervisión de estadísticas con SNMP, el Reenvío de capturas a un administrador SNMP o la Configuración de alertas de correo electrónico.
- Para enviar una solicitud de API basada en HTTP directamente a un servicio externo que expone una API para automatizar un flujo de trabajo o una acción. Puede, por ejemplo, reenviar logs que coinciden con los criterios definidos para crear un ticket de incidencia en Service Now en lugar de confiar en un sistema externo para convertir mensajes de syslog o capturas de SNMP en una solicitud HTTP. Puede modificar la URL, el encabezado HTTP, los parámetros y la carga en la solicitud HTTP para desencadenar una acción en función de los atributos en un log del cortafuegos. Consulte Reenvío de logs a un destino HTTP(S).
- Para el almacenamiento de logs a largo plazo y la supervisión de cortafuegos centralizados, puede utilizar la Configuración de supervisión de syslog para enviar los datos de logs a un servidor Syslog. Esto permite la integración con herramientas externas de supervisación de seguridad, como Splunk! o ArcSight.
- Si desea supervisar las estadísticas en el tráfico IP que atraviesa las interfaces de cortafuegos, puede realizar la Configuración de exportaciones de NetFlow para ver las estadísticas en un recopilador de NetFlow.

Puede realizar la Configuración de reenvío de logs desde el cortafuegos directamente a los servicios externos o desde el cortafuegos a Panorama y después configurar Panorama para reenviar los logs a los servidores. Consulte las Opciones de reenvío de logs para los factores a tener en cuenta a la hora de decidir dónde enviar los logs.



No puede agregar registros de NetFlow en Panorama; debe enviarlos directamente desde los cortafuegos al recopilador de NetFlow.

© 2020 Palo Alto Networks, Inc.

Configuración de reenvío de logs

En un entorno en el que utiliza varios cortafuegos para controlar y analizar el tráfico de red, cualquier cortafuegos puede mostrar logs e informes solo para el tráfico que supervisa. Debido a que el inicio de sesión en varios cortafuegos puede hacer de la supervisión una tarea engorrosa, puede lograr una visibilidad global de la actividad de la red de manera más eficiente al reenviar los logs de todos los cortafuegos a Panorama o los servicios externos. Si utiliza servicios externos para supervisión, el cortafuegos convierte automáticamente los logs en el formato necesario: mensajes syslog, capturas SNMP, notificaciones de correo electrónico o como una carga HTTP para enviar los detalles de log a un servidor HTTP. En los casos en que algunos equipos de su organización puedan lograr mayor eficiencia al supervisar solo los logs que son relevantes para sus operaciones, puede crear filtros de reenvío basados en cualquier atributo de logs (tal como un tipo de amenaza o usuario de origen). Por ejemplo, un analista de operaciones de seguridad que investiga ataques de malware puede estar interesado únicamente en logs de amenazas con el atributo de tipo configurado en wildfire-virus.

Puede reenviar logs desde los cortafuegos directamente a servicios externos o desde los cortafuegos a Panorama y después configurar Panorama para reenviar los logs a los servidores. Consulte las Opciones de reenvío de logs para los factores a tener en cuenta a la hora de decidir dónde enviar los logs.

Puede usar comandos de copia segura (SCP) de la CLI para exportar la base de datos de logs completa a un servidor SCP e importarlo a otro cortafuegos. Como la base de datos de logs es demasiado grande para que sea práctico importarla o exportarla en el cortafuegos PA-7000 Series, esta no admite esas opciones. También puede usar la interfaz web en todas las plataformas para Visualización y gestión de informes, pero solo según tipo de logs, no según toda la base de datos de logs.

STEP 1 | Configure un perfil de servidor para cada servicio externo que recibirá información de logs.

Puede usar perfiles diferentes para enviar conjuntos de logs diferentes, filtrados por atributos de log, a un servidor diferente. Para aumentar la disponibilidad, defina múltiples servidores en un único perfil.

Configure uno o más de los siguientes perfiles de servidor:

- (Obligatorio para SMTP sobre TLS) Si aún no lo ha hecho, cree un perfil de certificado para el servidor de correo electrónico.
- 2 Para habilitar al gestor SNMP (servidor de capturas) para que interprete las capturas de cortafuegos, debe cargar los MIB admitidas de Palo Alto Networks en el gestor SNMP y, si fuera necesario, compilarlos. Si desea información detallada, consulte la documentación de software de gestión de SNMP.
- Si el servidor syslog requiere autenticación de cliente, también debe 5.
- Configure un perfil de servidor HTTP (consulte Reenvío de logs a un destino de HTTP/S).

STEP 2 | Cree un perfil de reenvío de logs.

El perfil define los destinos para tráfico, amenaza, envío de WildFire, filtro de URL, filtro de datos, túnel y logs de autenticación.

1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)** y luego **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil.

© 2020 Palo Alto Networks, Inc.

Si desea que el cortafuegos asigne automáticamente el perfil a nuevas reglas y zonas de seguridad, escriba **`predeterminado`**. Si no desea un perfil por defecto o desea cancelar un perfil por defecto existente, introduzca un nombre en **Name**, que lo ayudará a identificar el perfil cuando lo asigne a reglas y zonas de seguridad.



*Si no existen perfiles de reenvío de logs llamados **`default`**, la selección del perfil se define como None por defecto en nuevas reglas de seguridad (campo Log Forwarding) y nuevas zonas de seguridad (campo Log Setting), aunque usted puede cambiar la selección.*

3. Seleccione **Add (Añadir)** para añadir uno o más *perfiles de la lista de coincidencias*.

   Los perfiles especifican los filtros de la consulta de log, los destinos de reenvío y las acciones automáticas, así como el etiquetado. Para cada perfil de lista de coincidencia:

   1. Introduzca un **Name (Nombre)** para identificar el perfil.
   2. Seleccione el **Log Type (Tipo de log)**.
   3. En la lista desplegable **Filter (Filtro)**, seleccione **Filter Builder (Generador de filtro)**. Especifique lo siguiente y luego seleccione **Add (Añadir)** para añadir cada consulta:
      - Lógica de **Connector (Conector)** (y/o)
      - **Attribute (Atributo)** de log
      - **Operator (Operador)** para definir lógica de inclusión o exclusión
      - **Value (Valor)** de atributo para coincidencia de la consulta
   4. Seleccione **Panorama** si desea reenviar logs a los recopiladores de logs o al servidor de gestión Panorama.
   5. Para cada tipo de servicio externo que utilice para supervisar (SNMP, correo electrónico, syslog y HTTP), seleccione **Add (Añadir)** para añadir uno o más perfiles de servidor.
4. (Opcional, solo GlobalProtect) Si está utilizando un perfil de reenvío de logs en una política de seguridad para poner en cuarentena automáticamente un dispositivo mediante GlobalProtect, seleccione **Quarantine (Cuarentena)** en el área **Built-in Actions (Acciones integradas)**.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de reenvío de logs.

STEP 3 | Asigne el perfil de reenvío de logs a las reglas de política y zonas de red.

Las reglas de seguridad, autenticación y protección DoS admiten el reenvío de logs. En este ejemplo, se asigna el perfil a una regla de seguridad.

Realice los siguientes pasos por cada regla que desee que active el reenvío de logs:

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y modifique la regla.
2. Seleccione **Actions (Acciones)** y seleccione el perfil de **Log Forwarding (Reenvío de logs)** que creó.
3. Configure el **Profile Type (Tipo de perfil)**, en **Profiles (Perfiles)** o **Group (Grupo)**, y luego seleccione los perfiles de seguridad o **Group Profile (Perfil de grupo)** requeridos para activar la generación y el reenvío de logs para lo siguiente:
   - Logs de amenazas: El tráfico debe coincidir con cualquier perfil de seguridad asignado a una regla.
   - Logs de envío de WildFire: el tráfico debe coincidir con un perfil de análisis de WildFire asignado a la regla.
4. Para los logs de tráfico, seleccione **Log At Session Start (Log al iniciar sesión)** o **Log At Session End (Log al finalizar sesión)**.
5. Haga clic en **OK (Aceptar)** para guardar la regla.

STEP 4 | Configure los destinos para los logs de sistema, configuración, correlación, GlobalProtect, coincidencias de HIP y User-ID.

© 2020 Palo Alto Networks, Inc.

Panorama genera logs de correlación basados en los logs de cortafuegos que recibe, en lugar de agrupar logs de correlación de los cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de log)**.
2. Para cada tipo de log que el cortafuegos reenviará, consulte el paso Añadir uno o más perfiles de lista de coincidencia.

STEP 5 | (Solo cortafuegos PA-7000 Series) Configure una interfaz de tarjeta de log para realizar el reenvío de logs.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en **Add Interface (Añadir interfaz)**.
2. Seleccione la **Slot** y el **Interface Name**.
3. Cambie el **Interface Type (Tipo de interfaz)** a **Log Card (Tarjeta de log)**.
4. Introduzca la **IP Address (Dirección IP)**, **Default Gateway (Puerta de enlace predeterminada)** y (para IPv4 únicamente) la **Netmask (Máscara de red)**.
5. Seleccione **Advanced (Avanzado)** y especifique **Link Speed (Velocidad del enlace)**, **Link Duplex (Dúplex de enlace)** y **Link State (Estado de enlace)**.

   Estos campos están configurados por defecto en auto, que especifica que el cortafuegos determina automáticamente los valores según la conexión. Sin embargo, el valor mínimo recomendado de Link Speed para cualquier conexión es de 1000 (Mbps).
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 6 | Compile y compruebe sus cambios.

1. **Commit (Confirmar)** los cambios.
2. Compruebe que los destinos de log que configuró reciben logs de cortafuegos:
   - Panorama: si el cortafuegos reenvía los logs a un dispositivo virtual Panorama en modo Panorama o a un dispositivo serie M, debe configurar un grupo de recopiladores antes de que Panorama reciba los logs. Después puede verificar el reenvío de logs.
   - Servidor de correo electrónico: Compruebe que los destinatarios especificados reciben logs como notificaciones de correo electrónico.
   - Servidor de syslog: consulte la documentación de su servidor syslog para comprobar que recibe logs como mensajes de syslog.
   - SNMP manager (Gestor SNMP)Active el gestor SNMP para explorar MIB y objetos para verificar que esté recibiendo logs como Traps SNMP.
   - HTTP server (Servidor HTTP): Reenvío de logs a un destino de HTTP/S.

© 2020 Palo Alto Networks, Inc.

Configuración de alertas de correo electrónico

Puede configurar alertas de correo electrónico para los logs de sistema, configuración, coincidencias HIP, correlación, amenazas, envío de WildFire y tráfico. Puede usar perfiles separados para enviar notificaciones de correo electrónico para cada tipo de log a un servidor diferente. Para aumentar la disponibilidad, defina múltiples servidores (hasta cuatro) en un único perfil.



Como práctica recomendada, configure la seguridad de la capa de transporte (TLS) para requerir que el cortafuegos se autentique con el servidor de correo electrónico antes de que el cortafuegos transmita el correo electrónico al servidor. Esto ayuda a prevenir la actividad maliciosa, como la retransmisión del Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol), que se puede usar para enviar spam o malware, y la suplantación de correo electrónico, que se puede usar para ataques de phishing.

STEP 1 | (Obligatorio para SMTP sobre TLS) Si aún no lo ha hecho, cree un perfil de certificado para el servidor de correo electrónico.

STEP 2 | Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Email (Correo electrónico)**.

STEP 3 | **Añada** un perfil de servidor de correo electrónico y especifique un **nombre**.

STEP 4 | Desde la ventana de solo lectura que aparece, **añada** el servidor de correo electrónico y especifique un **nombre**.

STEP 5 | Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la **Location (Ubicación)** (vsys o **Shared [Compartido]**) en la que el perfil está disponible.

STEP 6 | (Opcional) Especifique un **nombre para mostrar de correo electrónico** para especificar el nombre que se mostrará en el campo de remitente del correo electrónico.

STEP 7 | Especifique la dirección de correo electrónico **desde** la cual el cortafuegos envía correos electrónicos.

STEP 8 | Especifique la dirección de correo electrónico **a** la cual el cortafuegos envía correos electrónicos.

STEP 9 | (Opcional): si desea enviar correos electrónicos a una segunda cuenta, introduzca la dirección del **destinatario adicional**. Solo puede añadir un destinatario adicional. Para varios destinatarios, añada la dirección de correo electrónico de una lista de distribución.

STEP 10 | Especifique la dirección IP o el nombre de host de la **puerta de enlace de correo electrónico** que se usará para enviar los mensajes de correo electrónico.

STEP 11 | Seleccione el **tipo** de protocolo que se utilizará para conectarse al servidor de correo electrónico:

- **Unauthenticated SMTP (SMTP no autenticado)**: utilice SMTP para conectarse al servidor de correo electrónico sin autenticación. El **puerto** predeterminado es 25, pero opcionalmente puede especificar un puerto diferente. Este protocolo no proporciona la misma seguridad que SMTP sobre TLS, pero si selecciona este protocolo, omita el siguiente paso.

© 2020 Palo Alto Networks, Inc.

- **SMTP over TLS (SMTP sobre TLS)**: (Recomendado) Use TLS para requerir autenticación para conectarse al servidor de correo electrónico. Continúe con el siguiente paso para configurar la autenticación TLS.

STEP 12 | (Solo en SMTP sobre TLS) Configure el cortafuegos para usar la autenticación TLS para conectarse al servidor de correo electrónico.

1. (Opcional) Especifique el **puerto** que se utilizará para conectarse al servidor de correo electrónico (el valor predeterminado es 587).
2. **TLS Version (Versión de TLS)**: especifique la versión de TLS (**1.1** o **1.2**).

   Palo Alto Networks recomienda encarecidamente utilizar la última versión de TLS.
3. Seleccione el **método de autenticación** para el cortafuegos y el servidor de correo electrónico:
   - **Auto (Automático)**: permite que el cortafuegos y el servidor de correo electrónico determinen el método de autenticación.
   - **Login (Iniciar sesión)**: use la codificación Base64 para el nombre de usuario y la contraseña y transmítalos por separado.
   - **Plain (Sin formato)**: use la codificación Base64 para el nombre de usuario y la contraseña y transmítalos juntos.
4. Seleccione un **perfil de certificado** para autenticarse con el servidor de correo electrónico.
5. Especifique el **nombre de usuario** y la **contraseña** de la cuenta que envía correos electrónicos y, a continuación, **confirme la contraseña**.
6. (Opcional) Para confirmar que el cortafuegos puede autenticarse con éxito con el servidor de correo electrónico, puede **probar la conexión**.

STEP 13 | Haga clic en **OK (Aceptar)** para guardar el perfil de servidor de correo electrónico.

STEP 14 | (Opcional) Seleccione la pestaña **Custom Log Format** y personalice el formato de los mensajes de correo electrónico. Si desea más información sobre cómo crear formatos personalizados para los distintos tipos de log, consulte Guía de configuración de formato de eventos comunes.

STEP 15 | Configure las alertas de correo electrónico para logs de envíos de WildFire, tráfico y amenaza.

1. Consulte Creación de un perfil de reenvío de logs.
   1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**, haga clic en **Add (Añadir)** e ingrese un nombre en **Name (Nombre)** para identificar el perfil.
   2. Para cada tipo de log y nivel de gravedad o veredicto de WildFire, seleccione el perfil de servidor de correo electrónico y haga clic en **OK**.
2. Consulte Asignación del perfil de reenvío de logs a las reglas de política y zonas de red.

STEP 16 | Configure las alertas de correo electrónico de los logs de sistema, configuración, coincidencias HIP y correlación.

1. Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de log)**.
2. Para cada log de sistema y correlación, haga clic en cada nivel de gravedad, seleccione el perfil de servidor de **Email (Correo electrónico)** y haga clic en **OK (Aceptar)**.
3. Para cada log de configuración y coincidencia HIP, edite la sección, seleccione el perfil de servidor de **Email** y haga clic en **OK**.
4. Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Uso de syslog para la monitorización

Syslog es un mecanismo de transporte de logs estándar que permite añadir datos de logs desde distintos dispositivos de red (tales como enrutadores, cortafuegos o impresoras) de diferentes proveedores a un repositorio central para su archivo y análisis, así como para elaborar informes. Los cortafuegos de Palo Alto Networks pueden reenviar todos los tipos de log que generan a un servidor Syslog externo. Puede usar TCP o TLS (solo TLSv1.2) para un reenvío fiable y seguro de logs, o UDP para un reenvío no seguro.

- Configuración de la monitorización de syslog
- Descripciones de los campos de syslog

Configuración de la monitorización de syslog

Para usar Syslog para la monitorización de un cortafuegos de Palo Alto Networks, cree un perfil de servidor Syslog y asígnelo a los ajustes de log para cada tipo de log. Opcionalmente, puede configurar el formato de encabezado usado en los mensajes syslog y habilitar la autenticación de cliente para syslog en TLSv1.2.

STEP 1 | Configure un perfil de servidor Syslog.



Puede usar perfiles diferentes para enviar syslogs para cada tipo de log a un servidor diferente. Para aumentar la disponibilidad, defina múltiples servidores (hasta cuatro) en un único perfil.

1. Seleccione**Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Syslog**.
2. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para el perfil.
3. Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la **Location (Ubicación)** (vsys o **Shared [Compartido]**) en la que el perfil está disponible.
4. Para cada servidor syslog, haga clic en **Add (Añadir)** e introduzca la información que necesita el cortafuegos para conectarse con él:
   - **Name (Nombre)**: nombre exclusivo para el perfil de servidor.
   - **Syslog Server**: dirección IP o nombre de dominio completo (fully qualified domain name, FQDN) del servidor Syslog.

     Si utiliza transporte UDP y configura un FQDN que no puede resolver el cortafuegos, este emplea la resolución existente de dirección IP para el FQDN como dirección del servidor de syslog.
   - **Transporte**: seleccione **TCP**, **UDP** o **SSL** (TLS) como el protocolo de comunicación con el servidor syslog. En el caso de **SSL**, el cortafuegos admite TLSv1.2 únicamente.
   - **Port (Puerto)**: número de puerto por el que se enviarán mensajes de syslog (el valor por defecto es UDP en el puerto 514); debe usar el mismo número de puerto en el cortafuegos y en el servidor syslog.
   - **Format**: seleccione el formato de mensaje de Syslog que se debe utilizar: **BSD** (valor predeterminado) o **IETF**. Normalmente, el formato **BSD** se realiza mediante UDP y el formato **IETF** mediante TCP o SSL/TLS.
   - **Facility**: seleccione un valor de syslog estándar (por defecto es **LOG_USER**) para calcular el campo de prioridad (PRI) en la implementación del servidor syslog. Seleccione el valor que asigna cómo usa el campo PRI para gestionar sus mensajes de syslog.
5. (**Opcional**) Para personalizar el formato de los mensajes de syslog que envía el cortafuegos, seleccione la pestaña **Custom Log Format**. Si desea más información sobre cómo crear formatos personalizados para los distintos tipos de log, consulte Guía de configuración de formato de eventos comunes.

© 2020 Palo Alto Networks, Inc.

6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Configure el reenvío de syslog para logs de envíos de WildFire, tráfico y amenaza.

1. Configure el cortafuegos para reenviar logs. Para obtener más información, consulte el paso Creación de perfil de reenvío de logs.
   1. Seleccione **Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**, haga clic en **Add (Añadir)** e ingrese un nombre en **Name (Nombre)** para identificar el perfil.
   2. Para cada tipo de log y nivel de gravedad o veredicto de WildFire, seleccione el perfil de servidor de **Syslog** y haga clic en **OK**.
2. Asigne el perfil de reenvío de logs a una política de seguridad para activar la generación y el reenvío de logs. Para obtener más información, consulte el paso Asignación del perfil de reenvío de logs a las reglas de política y zonas de red.
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de políticas.
   2. Seleccione la pestaña **Actions (Acciones)** y elija el **perfil de reenvío de logs** que creó.
   3. En el menú desplegable **Profile Type (Tipo de perfil)**, seleccione **Profiles (Perfiles)** o **Groups (Grupos)** y, a continuación, elija los perfiles de seguridad o **perfiles de grupo** requeridos para activar la generación y el reenvío de logs.
   4. Para los logs de tráfico, active una de las casillas de verificación **Log at Session Start (Log al iniciar sesión)** y **Log At Session End (Log al finalizar sesión)** y haga clic en **OK (Aceptar)**.

   Para obtener información detallada sobre cómo configurar un perfil de reenvío de logs y asignar el perfil a una regla de políticas, consulte Configuración de reenvío de logs.

STEP 3 | Configure el reenvío de syslog de logs de sistema, configuración, coincidencias HIP y correlación.

1. Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de log)**.
2. Para cada log de sistema y correlación, haga clic en cada nivel de gravedad, seleccione el perfil de servidor **Syslog** y haga clic en **OK**.
3. Para cada log de configuración, coincidencia HIP y correlación, edite la sección, seleccione el perfil de servidor **Syslog** y haga clic en **OK**.

STEP 4 | (**Opcional**) Configure el formato de encabezado de los mensajes de syslog.

Los datos de log incluyen el identificador único del cortafuegos que generó el log. La selección del formato de encabezado proporciona más flexibilidad para filtrar y crear informes sobre los datos de log para algunos servidores de información de seguridad y gestión de eventos (SIEM).

Se trata de una configuración global y se aplica a todos los perfiles de servidores syslog configurados en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de registro e informes.
2. Seleccione la pestaña **Log Export and Reporting (Exportación de log y creación de informes)** y seleccione el Formato de NOMBRE DE HOST de syslog:
   - **FQDN** (valor por defecto): concatena el nombre de host y el nombre de dominio definidos en el cortafuegos de envío.
   - **hostname**: utiliza el nombre de host definido en el cortafuegos de envío.
   - **ipv4-address**: utiliza la dirección IPv4 de la interfaz del cortafuegos utilizada para enviar logs. De manera predeterminada, esta es la interfaz MGT.
   - **ipv6-address**: utiliza la dirección IPv6 de la interfaz del cortafuegos utilizada para enviar logs. De manera predeterminada, esta es la interfaz MGT.
   - **none**: deja el campo de nombre de host sin configurar en el cortafuegos. No hay ningún identificador para el cortafuegos que envía los logs.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | Cree un certificado para asegurar la comunicación de syslog en TLSv1.2.

Requerido solo si el servidor syslog usa la autenticación de cliente. El servidor syslog utiliza el certificado para verificar que el cortafuegos está autorizado para comunicarse con el servidor syslog.

Asegúrese de que se cumplen las siguientes condiciones:

- La clave privada debe estar disponible en el cortafuegos de envío; las claves no pueden almacenarse en un módulo de seguridad de hardware (Hardware Security Module, HSM).
- El sujeto y el emisor del certificado no deben ser idénticos.
- El servidor syslog y el cortafuegos de envío deben tener certificados firmados por la misma entidad de certificación (certificate authority, CA) de confianza. También puede generar un certificado autofirmado en el cortafuegos, exportar el certificado desde el cortafuegos e importarlo en el servidor syslog.
- La conexión a un servidor Syslog en TLS se valida con el Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) o con las Listas de revocación de certificados (Certificate Revocation Lists, CRL) siempre que cada certificado en la cadena de confianza especifique una o ambas de estas extensiones. Sin embargo, no puede omitir fallos OCSP o CRL, por lo que debe garantizar que la cadena de certificados sea válida y que pueda verificar cada certificado con OCSP o CRL.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)** y haga clic en **Generate (Generar)**.
2. Introduzca un **Name (Nombre)** para el certificado.
3. En el campo **Common Name**, introduzca la dirección IP del cortafuegos que enviará logs al servidor syslog.
4. En **Signed by (Firmado por)**, seleccione la CA de confianza o la CA autofirmada en las que el servidor syslog y el cortafuegos de envío confían.

   El certificado no puede ser una **Certificate Authority** o una **External Authority** (solicitud de firma de certificados [certificate signing request, CSR]).
5. Haga clic en **Generate (Generar)**. El cortafuegos genera el certificado y el par de claves.
6. Haga clic en el nombre del certificado para editarlo, seleccione la casilla de verificación **Certificate for Secure Syslog** y haga clic en **OK**.

STEP 6 | Compile sus cambios y revise los logs del servidor syslog.

1. Haga clic en **Commit (Confirmar)**.
2. Para revisar los logs, consulte la documentación de su software de gestión de syslog. También puede revisar las descripciones del campo de Syslog.

Descripciones de los campos de syslog

Los siguientes temas enumeran los campos estándar de cada tipo de log que los cortafuegos de Palo Alto Networks pueden reenviar a un servidor externo, así como los niveles de gravedad, formatos personalizados y secuencias de escape. Para facilitar el análisis, la coma es el delimitador; cada campo es una cadena de valores separados por comas (CSV). La etiqueta FUTURE_USE se aplica a los campos que los cortafuegos no implementan actualmente.



Los logs de envío de WildFire son un subtipo de logs de amenazas y utilizan el mismo formato que syslog.

- Campos del log de tráfico
- Campos del log de amenazas

© 2020 Palo Alto Networks, Inc.

- Campos de logs de coincidencias de HIP
- Campos de los logs de asignación de etiquetas a IP
- Campos de log de User-ID
- Campos de logs de descifrado
- Campos del log de inspección de túnel
- Campos de logs de SCTP
- Configuración de campos de logs
- Campos de logs de autenticación
- Campos de logs del sistema
- Campos de log de eventos correlacionados
- Campos del log de GTP
- Formato de logs/eventos personalizados
- Secuencias de escape

Campos del log de tráfico

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes, Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE_USE, Sequence Number, Action Flags, Source Country, Destination Country, FUTURE_USE, Packets Sent, Packets Received, Session End Reason, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Action Source, Source VM UUID, Destination VM UUID, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, SCTP Association ID, SCTP Chunks, SCTP Chunks Sent, SCTP Chunks Received, Rule UUID, HTTP/2 Connection, Link Change Count, Policy ID, Link Switches, SD-WAN Cluster, SD-WAN Device Type, SD-WAN Cluster Type, SD-WAN Site, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination Mac Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Host ID, Serial Number, Source Dynamic Address Group, Destination Dynamic Address Group, Session Owner, High Resolution Timestamp, A Slice Service Type, A Slice Differentiator

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es TRAFFIC.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log Tráfico; los valores son Iniciar, Finalizar, Colocar y Denegar. • Start (Iniciar): sesión iniciada. • Finalizar: sesión finalizada.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• Drop (Descartar): sesión descartada antes de identificar la aplicación; no hay ninguna regla que permita la sesión. • Deny (Denegar): sesión descartada después de identificar la aplicación; hay una regla para bloquear o no hay ninguna regla que permita la sesión.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de origen de la sesión original.
Destination Address (Dirección de destino) (dst)	Dirección IP de destino de la sesión original.
NAT Source IP (IP de NAT de origen) (natsrc)	Si se ejecuta un NAT de origen, es el NAT de dirección IP de origen posterior.
NAT Destination IP (IP de NAT de destino) (natdst)	Si se ejecuta un NAT de destino, es el NAT de dirección IP de destino posterior.
Rule Name (Rule) (Nombre de regla [Regla])	Nombre de la regla con la que ha coincidido la sesión.
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició la sesión.
Destination User (Usuario de destino) (dstuser)	Nombre del usuario para el que iba destinada la sesión.
Application (Aplicación) (app)	Aplicación asociada a la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de la sesión.
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	Perfil de reenvío de logs aplicado a la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Session ID (ID de sesión) (sessionid)	Identificador numérico interno aplicado a cada sesión.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
NAT Source Port (Puerto de origen de NAT) (natsport)	NAT de puerto de origen posterior.
NAT Destination Port (Puerto de destino de NAT) (natdport)	NAT de puerto de destino posterior.
Flags (Marcas) (flags)	Campo de 32 bits que proporciona información detallada sobre la sesión; este campo puede descodificarse añadiendo los valores con Y y con el valor registrado: • 0x80000000: la sesión tiene una captura de paquetes (PCAP) • 0x40000000: la opción está habilitada para permitir que un cliente use varias rutas para conectarse a un host de destino. • 0x20000000: se envió el archivo a WildFire para un veredicto. • 0x10000000: se detectó el envío de una credencial empresarial por parte de un usuario final. • 0x08000000: el origen del flujo está en la lista de permitidos y no está sujeta a protección de reconocimiento. • 0x02000000: sesión IPv6 • 0x01000000: se descifró la sesión SSL (proxy SSL). • 0x00800000: se denegó la sesión a través del filtrado de URL. • 0x00400000: la sesión ha realizado una traducción NAT. • 0x00200000: la información de usuario de la sesión se ha capturado mediante el portal de autenticación. • 0x00100000: el tráfico de la aplicación está en un puerto de destino no estándar. • 0x00080000: el valor X-Forwarded-For de un proxy está en el campo Usuario de origen. • 0x00040000: el log corresponde a una transacción en una sesión de proxy HTTP (Transacción proxy). • 0x00020000: el flujo de cliente a servidor está sujeto al reenvío basado en la política. • 0x00010000: el flujo de servidor a cliente está sujeto al reenvío basado en la política. • 0x00008000: la sesión es un acceso a la página de contenedor (Container Page). • 0x00002000: la sesión tiene una coincidencia temporal en una regla para la gestión de las dependencias de las aplicaciones implícitas. Disponible en PAN-OS 5.0.0 y posterior.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• 0x00000800: se utilizó el retorno simétrico para reenviar tráfico para esta sesión. • 0x00000400: el tráfico descifrado se envía en texto sin cifrar mediante un puerto de reflejo. • 0x00000100: se está inspeccionando la carga útil del túnel externo.
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son: • allow (permitir): la política permitió la sesión. • deny (denegar): la política denegó la sesión. • drop (descartar): la sesión se descartó de manera silenciosa. • drop ICMP (descartar ICMP): la sesión se descartó de manera silenciosa con un mensaje de ICMP inalcanzable al host o aplicación. • reset both (restablecer ambos): la sesión se ha terminado y un restablecimiento de TCP se envía a ambos lados de la conexión. • reset client (restablecer cliente): la sesión se ha terminado y un restablecimiento de TCP se envía al cliente. • reset server (restablecer servidor): la sesión se ha terminado y un restablecimiento de TCP se envía al servidor.
Bytes (bytes)	Número total de bytes (transmitidos y recibidos) de la sesión.
Bytes Sent (Bytes enviados) (bytes_sent)	Número de bytes en la dirección cliente a servidor de la sesión.
Bytes Received (Bytes recibidos) (bytes_received)	Número de bytes en la dirección servidor a cliente de la sesión.
Packets (Paquetes) (packets)	Número total de paquetes (transmitidos y recibidos) de la sesión.
Start Time (start) (Fecha de inicio [start])	Hora de inicio de sesión.
Elapsed Time (Tiempo transcurrido) (elapsed)	Tiempo transcurrido en la sesión.
Category (Categoría) (category)	Categoría de URL asociada a la sesión (si es aplicable).
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Source Country (País de origen) (srcloc)	País de origen o región interna para direcciones privadas; la longitud máxima es de 32 bytes.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Destination Country (País de destino) (dstloc)	País de destino o región interna para direcciones privadas. La longitud máxima es de 32 bytes.
Paquetes enviados (pkts_sent)	Números de paquetes de cliente a servidor de la sesión.
Paquetes recibidos (pkts_received)	Números de paquetes de servidor a cliente de la sesión.
Razón del fin de sesión (session_end_reason)	Razón por la que ha finalizado una sesión. Si la finalización ha tenido varias causas, este campo solo muestra la más importante. Los valores de la posible razón de finalización de la sesión son los siguientes en orden de prioridad (el primero es el más importante): • threat: el cortafuegos ha detectado una amenaza asociada a una acción de restablecimiento, borrado o bloqueo (dirección IP). • policy-deny: La sesión ha hecho coincidir una regla de seguridad con una acción de denegación o borrado. • decrypt-cert-validation: la sesión finalizó debido a que usted configuró el cortafuegos para que bloquee el cifrado de proxy de reenvío SSL o la inspección de entrada SSL cuando la sesión utilice la autenticación de cliente o un certificado de servidor con cualquiera de las siguientes condiciones: vencido, emisor no fiable, estado desconocido o tiempo de espera de verificación de estado agotado. Este motivo de fin de la sesión también se muestra cuando el certificado del servidor produce un alerta de error irrecuperable de tipo bad_certificate, unsupported_certificate, certificate_revoked, access_denied o no_certificate_RESERVED (solo SSL v. 3). • decrypt-unsupport-param: la sesión finalizó porque usted configuró el cortafuegos para que bloquee el descifrado de proxy de reenvío SSL o la inspección de entrada SSL cuando la sesión utiliza una versión de protocolo, cifra o algoritmo SSH no compatible. Este motivo de fin de la sesión se muestra cuando la sesión produce una alerta de error irrecuperable de tipo unsupported_extension, unexpected_message o handshake_failure. • Decrypt-error: la sesión finalizó porque usted configuró el cortafuegos para que bloquee el descifrado de proxy de reenvío SSL o la inspección de entrada SSL cuando los recursos del cortafuegos o el módulo de seguridad de (hardware security module, HSM) no estaban disponibles. Este motivo de fin de la sesión también se muestra cuando usted configura el cortafuegos para que bloquee el tráfico SSL con errores de SSH que produjo una alerta de error irrecuperable que no sea ninguna de las enumeradas para los motivos de finalización decrypt-cert-validation y decrypt-unsupport-param. • tcp-rst-from-client: el cliente ha enviado un restablecimiento de TCP al servidor. • tcp-rst-from-server: el servidor ha enviado un restablecimiento de TCP al cliente. • resources-unavailable: la sesión se ha cancelado debido a una limitación de recursos del sistema. Por ejemplo, la sesión podría

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	haber superado el número de paquetes que no funcionan permitidos por flujo o por la cola de paquetes que no funcionan globales. • tcp-fin: ambos hosts de la conexión enviaron un mensaje FIN de TCP para cerrar la sesión.

	• tcp-reuse: se reutiliza una sesión y el cortafuegos cierra la sesión anterior.
	• decoder: el decodificador detecta una nueva conexión en el protocolo (como HTTP-Proxy) y finaliza la conexión anterior.
	• aged-out: la sesión ha caducado.
	• unknown: este valor se aplica en las siguientes situaciones:
	  • Terminaciones de sesiones a las que no se aplican los motivos anteriores (por ejemplo, un comando `clear session all`).
	  • Para logs generados en una versión de PAN-OS que no admite el campo de razón de finalización de sesión (versiones posteriores a PAN-OS 6.1), el valor será **unknown** (desconocido) después de una actualización de la versión actual de PAN-OS o después de que los logs se carguen en el cortafuegos.
	  • En Panorama, los logs recibidos de los cortafuegos para los que la versión de PAN-OS no admite razones de finalización de sesión tendrán un valor **unknown**.
	• n/a: Este valor se aplica cuando el tipo de log de tráfico no es **end**.

Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Origen de acción (action_source)	Especifica si la acción desarrollada para permitir o bloquear una aplicación se definió en la aplicación o en la política. Las acciones

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	pueden: permitir, denegar, descartar, restablecer servidor, restablecer cliente o restablecer ambos para la sesión.
Source VM UUID (UUID de máquina virtual de origen) (src_uuid)	Indica el identificador único universal de origen para un equipo virtual invitado en el entorno NSX VMware.
Destination VM UUID (UUID de máquina virtual de destino) (dst_uuid)	Indica el identificador único universal de destino para un equipo virtual invitado en el entorno NSX VMware.
Tunnel ID/IMSI (ID o IMSI de túnel) (tunnelid/imsi)	La Identidad internacional de abonado móvil (International Mobile Subscriber Identity, IMSI) es un número único que se asigna a cada suscriptor móvil en el sistema GSM/UMTS/EPS. La IMSI incluirá digitos decimales (0 a 9) únicamente y el número máximo de digitos es de 15.
Monitor Tag/IMEI (Etiqueta o IMEI de supervisión) (monitortag/imei)	La Identidad internacional de equipo móvil (International Mobile Equipment Identity, IMEI) es un número único de 15 o 16 dígitos asignado a cada equipo de estación móvil.
Parent Session ID (ID de sesión principal) (parent_session_id)	ID de la sesión en la cual se tuneliza esta sesión. Se aplica al túnel interno (si hay dos niveles de tunelización) o al contenido interno (si hay un nivel de tunelización) únicamente.
Hora de inicio principal (parent_start_time)	Año/mes/día horas:minutos:segundos desde que comenzó la sesión de túnel principal.
Tunnel Type (Tipo de túnel) (tunnel)	Tipo de túnel, tal como GRE o IPSec.
SCTP Association ID (ID de asociación de SCTP) (assoc_id)	Número que identifica todas las conexiones para una asociación entre dos endpoints de SCTP.
SCTP Chunks (Fragmentos de SCTP) (chunks)	Suma de los fragmentos de SCTP enviados y recibidos de una asociación.
SCTP Chunks Sent (Fragmentos de SCTP enviados) (chunks_sent)	Número de fragmentos de SCTP enviados de una asociación.
SCTP Chunks Received (Fragmentos de SCTP recibidos) (chunks_received)	Número de fragmentos de SCTP recibidos de una asociación.
Rule UUID (Regla UUID) (rule_uuid)	UUID que identifica la regla de forma permanente.
HTTP/2 Connection (Conexión HTTP/2) [http2_connection]	Identificador del uso de una conexión HTTP/2 para el tráfico; aparece uno de estos valores: • Parent session ID (ID de sesión principal): conexión HTTP/2

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• 0: sesión SSL
Link Change Count (Número de cambios de enlace) (link_change_count)	Número de flaps de enlace que se produjeron en la sesión.
Policy ID (ID de política) (policy_id)	Nombre de la política de SD-WAN.
Link Switches (Cambios de enlace) (link_switches)	Contiene hasta cuatro entradas de flaps de enlace, y cada entrada contiene el nombre del enlace, la etiqueta de enlace, el tipo de enlace, la interfaz física, la marca de tiempo, los bytes leídos, los bytes escritos, el estado del enlace y la causa del flap.
SD-WAN Cluster (Clúster de SD-WAN) (sdwan_cluster)	Nombre del clúster de SD-WAN.
SD-WAN Device Type (Tipo de dispositivo de SD-WAN) (sdwan_device_type)	Tipo de dispositivo (`central` o `sucursal`).
SD-WAN Cluster Type (Tipo de clúster de SD-WAN) (sdwan_cluster_type)	Tipo de clúster (`malla` o `concentrador y radio`).
SW-WAN Site (Sitio de SW-WAN) [sdwan_site]	Nombre del sitio de SD-WAN.
Dynamic User Group Name (Nombre de grupo de usuarios dinámicos) (dynusergroup_name)	Nombre del grupo de usuarios dinámicos que contiene el usuario que inició la sesión.
XFF Address (Dirección XFF) [xff_ip]	La dirección IP del usuario que solicitó la página web o la dirección IP del penúltimo dispositivo que atravesó la solicitud. Si la solicitud pasa por uno o más proxies, equilibradores de carga u otros dispositivos de subida, el cortafuegos muestra la dirección IP del dispositivo más reciente
Source Device Category (Categoría de dispositivo de origen) [src_category]	La categoría del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Profile (Perfil de dispositivo de origen) [src_profile]	El perfil de dispositivo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Model (Modelo de dispositivo de origen) [src_model]	El modelo del dispositivo que Device-ID identifica como el origen del tráfico.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Source Device Vendor (Proveedor del dispositivo de origen) [src_vendor]	El proveedor del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Family (Familia del SO del dispositivo de origen) [src_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Version (Versión del SO del dispositivo de origen) [src_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Hostname (Nombre de host de origen) [src_host]	El nombre de host del dispositivo que Device-ID identifica como el origen del tráfico.
Source MAC Address (Dirección MAC de origen) [src_mac]	La dirección MAC del dispositivo que Device-ID identifica como origen del tráfico.
Destination Device Category (Categoría de dispositivo de destino) [dst_category]	La categoría del dispositivo que Device-ID identifica como destino del tráfico.
Destination Device Profile (Perfil de dispositivo de destino) [dst_profile]	El perfil de dispositivo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Model (Modelo de dispositivo de destino) [dst_model]	El modelo del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Vendor (Proveedor de dispositivos de destino) [dst_vendor]	El proveedor del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Family (Familia de SO del dispositivo de destino) [dst_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Version (Versión de SO del dispositivo de destino) [dst_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como destino del tráfico.
Destination Hostname (Nombre de host de destino) [dst_host]	El nombre de host del dispositivo que Device-ID identifica como el destino del tráfico.
Destination MAC Address (Dirección MAC de destino) [dst_mac]	La dirección MAC del dispositivo que Device-ID identifica como destino del tráfico.
Container ID (ID de contenedor) [container_id]	El ID de contenedor del pod PAN-NGFW en el nodo de Kubernetes donde se implementa el POD de la aplicación.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
POD Namespace (Espacio de nombres del POD) [pod_namespace]	El espacio de nombres del POD de la aplicación que se está protegiendo.
POD Name (Nombre del POD) [pod_name]	El POD de la aplicación está protegido.
Source External Dynamic List (Lista dinámica externa de origen) [src_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de origen del tráfico.
Destination External Dynamic List (Lista dinámica externa de destino) [dst_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de destino del tráfico.
Host ID (hostid)	Identificador único que GlobalProtect asigna para identificar el host.
User Device Serial Number (Número de serie del dispositivo del usuario) (serialnumber)	Número de serie de la máquina o dispositivo del usuario.
Source Dynamic Address Group (Grupo de direcciones dinámicas de origen) [src_dag]	Grupo de direcciones dinámicas de origen de sesión original.
Destination Dynamic Address Group (Grupo de direcciones dinámicas de destino) [dst_dag]	Grupo de direcciones dinámicas de origen de destino original.
Session Owner (Propietario de sesión) [session_owner]	El propietario original de la sesión de peer de alta disponibilidad HA (High Availability) en un clúster de HA desde el que se sincronizaron los datos de la tabla de sesión en la conmutación por error de HA.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los*

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo `1969-12-31T16:00:00.000-8:00` independientemente de cuándo se recibió el log.
A Slice Service Type (Tipo de servicio de segmento A) [nsdsai_sst]	El tipo de servicio de segmento A del ID de segmento de red.
A Slice Differentiator (Diferenciador de segmentos A) [nsdsai_sd]	El diferenciador de segmentos A del ID de segmento de red.

Campos del log de amenazas

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, URL/Filename, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Content Type, PCAP_ID, File Digest, Cloud, URL Index, User Agent, File Type, X-Forwarded-For, Referer, Sender, Subject, Recipient, Report ID, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, Source VM UUID, Destination VM UUID, HTTP Method, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, Threat Category, Content Version, FUTURE_USE, SCTP Association ID, Payload Protocol ID, HTTP Headers, URL Category List, Rule UUID, HTTP/2 Connection, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source MAC Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination MAC Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Host ID, Serial Number, Domain EDL, Source Dynamic Address Group, Destination Dynamic Address Group, Session Owner, Partial Hash, High Resolution Timestamp, Reason, Justification, A Slice Service Type

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Serial #) (Número de serie [n.° de serie])	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es THREAT.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de amenaza. Los valores incluyen lo siguiente: • Datodata — Patrón de datos que coinciden con un perfil de filtrado de datos. • file (archivo): tipo de archivo que coincide con un perfil de bloqueo de archivos. • flood (congestión): congestión detectada mediante un perfil de protección de zona. • packet (paquete): protección de ataque basada en paquetes desencadenada por un perfil de protección de zona. • scan (análisis): análisis detectado mediante un perfil de protección de zona. • spyware: spyware detectado mediante un perfil de antispyware. • url: log de filtrado de URL. • virus: virus detectado mediante un perfil de antivirus. • vulnerability (vulnerabilidad): exploit de vulnerabilidad detectado mediante un perfil de protección de vulnerabilidad. • wildfire: veredicto de WildFire generado cuando el cortafuegos envía un archivo a WildFire según un perfil de análisis de WildFire y se registra un veredicto (malintencionado, grayware o benigno, según lo que esté registrando) en el log de envíos de WildFire. • wildfire-virus: virus detectado mediante un perfil de antivirus.
Generate Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source address (Dirección de origen) (src)	Dirección IP de origen de la sesión original.
Destination address (Dirección de destino) (dst)	Dirección IP de destino de la sesión original.
NAT Source IP (IP de NAT de origen) (natsrc)	Si se ejecuta un NAT de origen, es el NAT de dirección IP de origen posterior.
NAT Destination IP (IP de NAT de destino) (natdst)	Si se ejecuta un NAT de destino, es el NAT de dirección IP de destino posterior.
Rule Name (Rule) (Nombre de regla [Regla])	Nombre de la regla con la que ha coincidido la sesión.
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició la sesión.
Destination User (Usuario de destino) (dstuser)	Nombre del usuario para el que iba destinada la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Application (Aplicación) (app)	Aplicación asociada a la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de la sesión.
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	Perfil de reenvío de logs aplicado a la sesión.
Session ID (ID de sesión) (sessionid)	Identificador numérico interno aplicado a cada sesión.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con la mismo IP de origen, IP de destino, aplicación y tipo de contenido/amenaza observado en 5 segundos.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
NAT Source Port (Puerto de origen de NAT) (natsport)	NAT de puerto de origen posterior.
NAT Destination Port (Puerto de destino de NAT) (natdport)	NAT de puerto de destino posterior.
Flags (Marcas) (flags)	Campo de 32 bits que proporciona información detallada sobre la sesión; este campo puede descodificarse añadiendo los valores con Y y con el valor registrado: • 0x80000000: la sesión tiene una captura de paquetes (PCAP) • 0x40000000: la opción está habilitada para permitir que un cliente use varias rutas para conectarse a un host de destino. • 0x20000000: se envió el archivo a WildFire para un veredicto. • 0x10000000: se detectó el envío de una credencial empresarial por parte de un usuario final.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• 0x08000000: el origen del flujo está en la lista de permitidos y no está sujeta a protección de reconocimiento. • 0x02000000: sesión IPv6 • 0x01000000: se descifró la sesión SSL (proxy SSL). • 0x00800000: se denegó la sesión a través del filtrado de URL. • 0x00400000: la sesión ha realizado una traducción NAT. • 0x00200000: la información de usuario de la sesión se ha capturado mediante el portal de autenticación. • 0x00100000: el tráfico de la aplicación está en un puerto de destino no estándar. • 0x00080000: el valor X-Forwarded-For de un proxy está en el campo Usuario de origen. • 0x00040000: el log corresponde a una transacción en una sesión de proxy HTTP (Transacción proxy). • 0x00020000: el flujo de cliente a servidor está sujeto al reenvío basado en la política. • 0x00010000: el flujo de servidor a cliente está sujeto al reenvío basado en la política. • 0x00008000: la sesión es un acceso a la página de contenedor (Container Page). • 0x00002000: la sesión tiene una coincidencia temporal en una regla para la gestión de las dependencias de las aplicaciones implícitas. Disponible en PAN-OS 5.0.0 y posterior. • 0x00000800: se utilizó el retorno simétrico para reenviar tráfico para esta sesión. • 0x00000400: el tráfico descifrado se envía en texto sin cifrar mediante un puerto de reflejo. • 0x00000010: se está inspeccionando la carga útil del túnel externo.
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son Alerta, Permitir, Denegar, Descartar, Descartar todos los paquetes, Restablecer cliente, Restablecer servidor, Restablecer ambos y Bloquear URL. • alert (alerta): amenaza o URL detectada pero no bloqueada. • allow (permitir): alerta de detección de inundación. • deny (denegar): el mecanismo de detección de inundación está activado, y el tráfico se deniega en función de la configuración. • drop (descartar): se detecta una amenaza y se descarta la sesión asociada. • reset-client (restablecer cliente): se detecta una amenaza y se envía un TCP RST al cliente. • reset-server (restablecer servidor): se detecta una amenaza y se envía un TCP RST al servidor. • reset-both (restablecer ambos): se detecta una amenaza y se envía un TCP RST tanto al cliente como al servidor.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• block-url (bloquear URL): la solicitud de URL se bloqueó porque coincidía con una categoría de URL que se había establecido como bloqueada. • block-ip (bloquear IP): se detecta una amenaza y la IP de cliente se bloquea. • random-drop (descarte aleatorio): se detectó la inundación y el paquete se descartó de forma aleatoria. • sinkhole: sinkhole de DNS activado • syncookie-sent (cookie de sincronización enviada): alerta de cookie de sincronización • block-continue (bloquear y continuar) (subtipo de URL únicamente): una solicitud de HTTP se bloquea y se redirige a una página de continuación con un botón para que procediera la confirmación. • continue (continuar) (subtipo de URL únicamente): respuesta a una página de continuación de URL de bloquear y continuar que indica que se permitió que una solicitud de bloquear y continuar procediera. • block-override (bloquear y anular) (subtipo de URL únicamente): una solicitud de HTTP se bloquea y se redirige a una página de anulación de administrador que requiere un código de aprobación del administrador del cortafuegos para continuar. • override-lockout (anular y bloquear) (subtipo de URL únicamente): demasiados intentos fallidos de códigos de aprobación de anulación de administrador desde la IP de origen. La IP ahora se bloquea desde la página de redirección de bloquear y anular. • override (anular) (subtipo de URL únicamente): respuesta a una página de bloquear y anular donde se ofrece un código de aprobación correcto y se permite la solicitud. • block (bloquear) (WildFire únicamente): el cortafuegos bloqueó el archivo y se cargó a WildFire.
URL/Filename (URL o nombre de archivo) (misc)	Campo de longitud variable. Los nombres de archivo pueden tener 63 caracteres como máximo y las URL, 1023. URI real cuando el subtipo es url. Nombre de archivo o tipo de archivo cuando el subtipo es Archivo. Nombre de archivo cuando el subtipo es Virus. Nombre de archivo cuando el subtipo es wildfire-virus. Nombre de archivo cuando el subtipo es wildfire. URL o nombre de archivo cuando el subtipo es vulnerability (si procede). URL cuando la Threat Category (Categoría de amenaza) es `domain-edl`
Threat/Content Name (Nombre de amenaza o contenido) (threatid)	Identificador de Palo Alto Networks para amenazas conocidas y personalizadas. Es una cadena de descripción seguida de un identificador numérico de 64 bits entre paréntesis para algunos subtipos: • 8000 - 8099: detección de exploración. • 8500 - 8599: detección de inundación. • 9999: log de filtrado de URL. • 10000 - 19999: detección de llamada a casa de spyware.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• 20000 - 29999: detección de descarga de spyware. • 30000 - 44999: detección de exploits de vulnerabilidades. • 52000 - 52999: detección de tipo de archivo. • 60000 - 69999: detección de filtrado de datos. Si se completa el campo Domain EDL (EDL de dominio), este campo se completa con el mismo valor. *Los intervalos de ID de amenaza para la detección de virus, la fuente de firmas de WildFire y las firmas C2 de DNS utilizados en versiones anteriores se han sustituido por ID únicos globales y permanentes. Consulte los nombres de campos Threat/Content Type (Tipo de amenaza o contenido) (subtype) y Threat Category (Categoría de amenaza) (thr_category) para crear informes actualizados, filtrar los logs de amenazas y la actividad de ACC.*
Category (Categoría) (category)	Para el subtipo URL, es la categoría de URL; para el subtipo WildFire, es el veredicto del archivo y es “malintencionado”, “phishing”, “grayware” o “beningno”; para otros subtipos, el valor es “Cualquiera”.
Severity (Gravedad) (severity)	Gravedad asociada a la amenaza; los valores son informational (informativo), low (bajo), medium (medio), high (alto) y critical (crítico).
Direction (Dirección) (direction)	Indica la dirección del ataque: Cliente a servidor o servidor a cliente. • 0: la dirección de la amenaza es cliente a servidor. • 1: la dirección de la amenaza es servidor a cliente.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente. Cada tipo de log tiene un espacio de número exclusivo.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Source Country (País de origen) (srcloc)	País de origen o región interna para direcciones privadas. La longitud máxima es de 32 bytes.
Destination Country (País de destino) (dstloc)	País de destino o región interna para direcciones privadas. La longitud máxima es de 32 bytes.
Tipo de contenido (contenttype)	Únicamente es aplicable cuando el subtipo es URL. Tipo de contenido de los datos de respuesta HTTP. La longitud máxima es de 32 bytes.
ID de captura de paquetes (pcap_id)	ID de captura de paquetes (pcap) es un elemento integral no firmado de 64 bits que indica un ID para correlacionar archivos de captura de paquetes de amenaza con capturas de paquetes ampliadas tomadas como parte de dicho flujo. Todos los logs de amenazas contendrán un pcap_id cuyo valor

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	es 0 (ninguna captura de paquetes asociada) o un ID que haga referencia al archivo de captura de paquetes ampliado.
Resumen de archivo (filedigest)	Solamente para el subtipo WildFire; el resto de tipos no utiliza este campo. La cadena filedigest muestra el hash binario del archivo enviado para ser analizado por el servicio WildFire.
Nube (cloud)	Solamente para el subtipo WildFire; el resto de los tipos no utilizan este campo. La cadena cloud muestra el FQDN del dispositivo WildFire (privado) o la nube de WildFire (pública) desde donde se cargó el archivo para su análisis.
Índice de URL (url_idx)	Se usa en el filtrado URL y los subtipos WildFire. Cuando una aplicación usa conexiones persistentes TCP para mantener una conexión abierta durante un periodo de tiempo, todas las entradas del log para esa sesión tienen un ID de sesión único. En esos caso, cuando tenga un log de amenazas único (e ID de sesión) que incluya múltiples entradas URL, la url_idx es un contador que le permite correlacionar el orden de cada entrada del log en la sesión única. Por ejemplo, para conocer la URL de un archivo que el cortafuegos ha reenviado a WildFire para analizarlo, encuentre el ID de sesión y el url_idx del log de envíos de WildFire y busque el mismo ID de sesión y url_idx en sus logs de filtrado de URL. La entrada del log que coincida con el ID de sesión y url_idx contendrá la URL del archivo que se reenvió a WildFire.
Agente de usuario (user_agent)	Solamente para el subtipo Filtrado de URL; el resto de los tipos no utilizan este campo. El campo Agente de usuario especifica el explorador web que utiliza el usuario para acceder a la URL (por ejemplo, Internet Explorer). Esta información se envía en la solicitud de HTTP al servidor.
Tipo de archivo (filetype)	Solamente para el subtipo WildFire; el resto de los tipos no utilizan este campo. Especifica el tipo de archivo que el cortafuegos ha reenviado para el análisis de WildFire.
X-Forwarded-For (xff)	Solamente para el subtipo Filtrado de URL; el resto de los tipos no utilizan este campo. El campo X-Forwarded-For del encabezado HTTP contiene la dirección IP del usuario que ha solicitado la página web. Permite identificar la dirección IP del usuario, lo que es especialmente útil si tiene un servidor proxy en su red que reemplaza la dirección IP del usuario por su propia dirección en el campo de dirección IP de origen del encabezado del paquete.
Sitio de referencia (referer)	Solamente para el subtipo Filtrado de URL; el resto de los tipos no utilizan este campo.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	El campo Sitio de referencia del encabezado HTTP contiene la dirección URL de la página web que enlaza al usuario a otra página web. Es el origen que redirige (remite) al usuario a la página web solicitada.
Remitente (sender)	Especifica el nombre del remitente de un correo electrónico.
Asunto (subject)	Especifica el asunto de un correo electrónico.
Destinatario (recipient)	Especifica el nombre del destinatario de un correo electrónico.
ID de informe (reportid)	Solamente para el subtipo WildFire; el resto de los tipos no utilizan este campo. Identifica la solicitud de análisis en la nube de WildFire o el dispositivo WildFire.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Source VM UUID (UUID de máquina virtual de origen) (src_uuid)	Indica el identificador único universal de origen para un equipo virtual invitado en el entorno NSX VMware.
Destination VM UUID (UUID de máquina virtual de destino) (dst_uuid)	Indica el identificador único universal de destino para un equipo virtual invitado en el entorno NSX VMware.
HTTP Method (Método HTTP) (http_method)	Solo en logs de filtrado URL. Describe el método HTTP utilizado en la solicitud web. Solo se registran los siguientes métodos: Conectar, Eliminar, Obtener, Encabezado, Opciones, Publicar, Colocar.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Tunnel ID/IMSI (ID o IMSI de túnel) (tunneli_d/imsi)	La Identidad internacional de abonado móvil (International Mobile Subscriber Identity, IMSI) es un número único que se asigna a cada suscriptor móvil en el sistema GSM/UMTS/EPS. La IMSI incluirá digitos decimales (0 a 9) únicamente y el número máximo de digitos es de 15.
Monitor Tag/IMEI (Etiqueta o IMEI de supervisión) (monitortag/imei)	La Identidad internacional de equipo móvil (International Mobile Equipment Identity, IMEI) es un número único de 15 o 16 dígitos asignado a cada equipo de estación móvil.
Parent Session ID (ID de sesión principal) (parent_session_id)	ID de la sesión en la cual se tuneliza esta sesión. Se aplica al túnel interno (si hay dos niveles de tunelización) o al contenido interno (si hay un nivel de tunelización) únicamente.
Parent Session Start Time (Fecha de inicio de sesión principal) (parent_start_time)	Año/mes/día horas:minutos:segundos desde que comenzó la sesión de túnel principal.
Tunnel Type (Tipo de túnel) (tunnel)	Tipo de túnel, tal como GRE o IPSec.
Categoría de amenaza (thr_category)	Describe las categorías de amenaza utilizadas para clasificar diferentes tipos de firmas de amenaza. Si un dominio external dynamic list (lista dinámica externa) generó el log, `domain-edl (edl de dominio)` completa este campo.
Versión de contenido (contentver)	Versión de aplicaciones y amenazas en su cortafuegos cuando se generó el log.
SCTP Association ID (ID de asociación de SCTP) (assoc_id)	Número que identifica todas las conexiones para una asociación entre dos endpoints de SCTP.
Payload Protocol ID (ID de protocolo de carga) (ppid)	ID del protocolo para la carga útil en la porción de datos del fragmento de datos.
HTTP Headers (http_headers)	Indica el encabezado de HTTP insertado en las entradas de log de URL en el cortafuegos.
URL Category List (Lista de categorías de URL) [url_category_list]	Lista de las categorías de URL Filtering que emplea el cortafuegos para aplicar la política.
Rule UUID (Regla UUID) (rule_uuid)	UUID que identifica la regla de forma permanente.
HTTP/2 Connection (Conexión HTTP/2) [http2_connection]	Identificador del uso de una conexión HTTP/2 para el tráfico; aparece uno de estos valores:

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• TCP connection session ID (ID de sesión de conexión TCP): la sesión es HTTP/2. • 0: la sesión no es HTTP/2.
Dynamic User Group Name (Nombre de grupo de usuarios dinámicos) (dynusergroup_name)	El nombre del grupo de usuarios dinámicos que contiene el usuario que inició la sesión.
XFF Address (Dirección XFF) [xff_ip]	La dirección IP del usuario que solicitó la página web o la dirección IP del penúltimo dispositivo que atravesó la solicitud. Si la solicitud pasa por uno o más proxies, equilibradores de carga u otros dispositivos de subida, el cortafuegos muestra la dirección IP del dispositivo más reciente
Source Device Category (Categoría de dispositivo de origen) [src_category]	La categoría del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Profile (Perfil de dispositivo de origen) [src_profile]	El perfil de dispositivo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Model (Modelo de dispositivo de origen) [src_model]	El modelo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Vendor (Proveedor del dispositivo de origen) [src_vendor]	El proveedor del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Family (Familia del SO del dispositivo de origen) [src_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Version (Versión del SO del dispositivo de origen) [src_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Hostname (Nombre de host de origen) [src_host]	El nombre de host del dispositivo que Device-ID identifica como el origen del tráfico.
Source MAC Address (Dirección MAC de origen) [src_mac]	La dirección MAC del dispositivo que Device-ID identifica como origen del tráfico.
Destination Device Category (Categoría de dispositivo de destino) [dst_category]	La categoría del dispositivo que Device-ID identifica como destino del tráfico.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Destination Device Profile (Perfil de dispositivo de destino) [dst_profile]	El perfil de dispositivo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Model (Modelo de dispositivo de destino) [dst_model]	El modelo del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Vendor (Proveedor de dispositivos de destino) [dst_vendor]	El proveedor del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Family (Familia de SO del dispositivo de destino) [dst_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Version (Versión de SO del dispositivo de destino) [dst_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como destino del tráfico.
Destination Hostname (Nombre de host de destino) [dst_host]	El nombre de host del dispositivo que Device-ID identifica como el destino del tráfico.
Destination MAC Address (Dirección MAC de destino) [dst_mac]	La dirección MAC del dispositivo que Device-ID identifica como destino del tráfico.
Container ID (ID de contenedor) [container_id]	El ID de contenedor del pod PAN-NGFW en el nodo de Kubernetes donde se implementa el POD de la aplicación.
POD Namespace (Espacio de nombres del POD) [pod_namespace]	El espacio de nombres del POD de la aplicación que se está protegiendo.
POD Name (Nombre del POD) [pod_name]	El POD de la aplicación está protegido.
Source External Dynamic List (Lista dinámica externa de origen) [src_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de origen del tráfico.
Destination External Dynamic List (Lista dinámica externa de destino) [dst_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de destino del tráfico.
Host ID (hostid)	Identificador único que GlobalProtect asigna para identificar el host.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
User Device Serial Number (Número de serie del dispositivo del usuario) (serialnumber)	Número de serie de la máquina o dispositivo del usuario.
Domain EDL (Dominio EDL) [domain_edl]	El nombre de la lista dinámica externa que contiene el nombre de dominio del tráfico.
Source Dynamic Address Group (Grupo de direcciones dinámicas de origen) [src_dag]	Grupo de direcciones dinámicas de origen de sesión original.
Destination Dynamic Address Group (Grupo de direcciones dinámicas de destino) [dst_dag]	Grupo de direcciones dinámicas de origen de destino original.
Partial Hash (Hash parcial) [partial_hash]	Hash parcial de aprendizaje automático.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo `1969-12-31T16:00:00:000-8:00` independientemente de cuándo se recibió el log.*
Reason (Motivo) (reason)	Motivo de la acción de filtrado de datos.
Justification (Justificación) [justification]	Justificación de la acción de filtrado de datos.
A Slice Service Type (Tipo de servicio de segmento A) [nsdsai_sst]	El tipo de servicio de segmento A del ID de segmento de red.

© 2020 Palo Alto Networks, Inc.

Campos de logs de coincidencias de HIP

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source User, Virtual System, Machine Name, Operating System, Source Address, HIP, Repeat Count, HIP Type, FUTURE_USE, FUTURE_USE, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, IPv6 Source Address, Host ID, User Device Serial Number, Device MAC Address, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es HIP-MATCH.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de coincidencias HIP; no utilizado.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log de coincidencias HIP.
Nombre de la máquina (machinename)	Nombre de la máquina del usuario.
Sistema operativo (SO)	Sistema operativo instalado en la máquina o el dispositivo del usuario (o en el sistema cliente).
Source Address (Dirección de origen) (src)	Dirección IP del usuario de origen.
HIP (matchname)	Nombre del perfil u objeto HIP.
Repeat Count (Número de	Número de veces que ha coincidido el perfil HIP.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
repeticiones) (repeatcnt)	
Tipo HIP (matchtype)	Especifica si el campo HIP representa un objeto HIP o un perfil HIP.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Virtual System ID (ID de sistema virtual) (vsys_id)	Un identificador único de un sistema virtual en un cortafuegos de Palo Alto Networks.
IPv6 System Address (Dirección de sistema IPv6) (srcipv6)	Dirección IPv6 de la máquina o dispositivo del usuario.
Host ID (hostid)	Identificador único que GlobalProtect asigna para identificar el host.
User Device Serial Number (Número de serie del dispositivo del usuario) (serialnumber)	Número de serie de la máquina o dispositivo del usuario.
Device MAC Address (Dirección MAC del dispositivo) [mac]	La dirección MAC de la máquina o dispositivo del usuario.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo* `1969-12-31T16:00:00.000-8:00` *independientemente de cuándo se recibió el log.*

Campos de logs de GlobalProtect

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Virtual System, Event ID, Stage, Authentication Method, Tunnel Type, Source User, Source Region, Machine Name, Public IP, Public IPv6, Private IP, Private IPv6, Host ID, Serial Number, Client Version, Client OS, Client OS Version, Repeat Count, Reason, Error, Description, Status, Location, Login Duration, Connect Method, Error Code, Portal, Sequence Number, Action Flags, High Res Timestamp, Selection Type, Response Time, Priority, Attempted Gateways, Gateway

Nombre de campo	Description (Descripción)
Receive Time (receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial # (N.° de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es GLOBALPROTECT.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de amenaza. Los valores incluyen lo siguiente: • Datodata — Patrón de datos que coinciden con un perfil de filtrado de datos. • file (archivo): tipo de archivo que coincide con un perfil de bloqueo de archivos. • flood (congestión): congestión detectada mediante un perfil de protección de zona.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• packet (paquete): protección de ataque basada en paquetes desencadenada por un perfil de protección de zona. • scan (análisis): análisis detectado mediante un perfil de protección de zona. • spyware: spyware detectado mediante un perfil de antispyware. • url: log de filtrado de URL. • virus: virus detectado mediante un perfil de antivirus. • vulnerability (vulnerabilidad): exploit de vulnerabilidad detectado mediante un perfil de protección de vulnerabilidad. • wildfire: veredicto de WildFire generado cuando el cortafuegos envía un archivo a WildFire según un perfil de análisis de WildFire y se registra un veredicto (malintencionado, grayware o benigno, según lo que esté registrando) en el log de envíos de WildFire. • wildfire-virus: virus detectado mediante un perfil de antivirus.
Generated Time (Hora de generación) (time_generated)	Hora a la que se generó el log en el plano de datos.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Event ID (ID de evento) (eventid)	Cadena que muestra el nombre del evento.
Stage (Etapa) (stage)	Cadena que muestra la etapa de la conexión (por ejemplo, `before-login (antes de inicio de sesión)`, `login (inicio de sesión)` o `tunnel (túnel)`).
Authentication Method (Método de autenticación) (auth_method)	Cadena que muestra el tipo de autenticación, como `LDAP`, `RADIUS` o `SAML`.
Tunnel Type (Tipo de túnel) (tunnel_type)	Tipo de túnel (SSLVPN o IPSec).
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició la sesión.
Source Region (Región de origen) (srcregion)	Región del usuario que inició la sesión.
Nombre de la máquina (machinename)	Nombre de la máquina del usuario.
Public IP (IP pública) (public_ip)	Dirección IP pública del usuario que inició la sesión.
Public IPv6 (IPv6 pública) (public_ipv6)	Dirección IPv6 pública del usuario que inició la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Private IP (IP privada) (private_ip)	Dirección IP privada del usuario que inició la sesión.
Private IPv6 (IPv6 privada) (private_ipv6)	Dirección IPv6 privada del usuario que inició la sesión.
Host ID (hostid)	El ID único que GlobalProtect asigna para identificar el host.
Serial Number (Número de serie) (serialnumber)	Número de serie de la máquina o dispositivo del usuario.
Client Version (Versión de cliente) (client_ver)	Versión de la aplicación de GlobalProtect del cliente.
Client OS (SO de cliente) (client_os)	Tipo de SO del dispositivo cliente (por ejemplo, Windows o Linux).
Client OS Version (Versión de SO de cliente) (client_os_ver)	Versión de SO del dispositivo cliente.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con la misma dirección IP de origen, dirección IP de destino, aplicación y subtipo que GlobalProtect ha detectado en los últimos cinco segundos.
Reason (Motivo) (reason)	Cadena que muestra el motivo de la cuarentena.
Error (error)	Cadena que muestra el error que se ha producido en cualquier evento.
Description (Descripción) (opaque)	Información adicional de cualquier evento ocurrido.
Status (Estado) (status)	Estado (correcto o erróneo) del evento.
Location (Ubicación) (location)	Cadena que muestra la ubicación definida por el administrador de la puerta de enlace o portal de GlobalProtect.
Login Duration (Duración de inicio de sesión) (login_duration)	El tiempo, en segundos, que el usuario está conectado a la puerta de enlace de GlobalProtect desde que inicia sesión hasta que cierra la sesión.
Connect Method (Método de conexión) (connect_method)	Cadena que muestra la forma en la que la aplicación de GlobalProtect se conecta a la puerta de enlace (por ejemplo `on-demand (a petición)` o `user-logon (inicio de sesión del usuario)`.
Error Code (Código de error) (error_code)	Número entero asociado al error que se ha producido.
Portal (portal)	Nombre de la puerta de enlace o portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Gateway Selection Method (Método de selección de puerta de enlace) [selection_type]	El método de conexión que se selecciona para conectarse a la puerta de enlace. • Manual: la puerta de enlace a la que desea que la aplicación GlobalProtect se conecte manualmente. • Preferred (Preferido): la puerta de enlace preferida a la que desea que se conecte la aplicación de GlobalProtect. • Auto (Automático): se conecta automáticamente a la puerta de enlace **mejor disponible** según la prioridad asignada a la puerta de enlace y el tiempo de respuesta.
SSL Response Time (Tiempo de respuesta SSL) [response_time]	El tiempo de respuesta SSL de la puerta de enlace seleccionada que se mide en milisegundos en el endpoint durante la configuración del túnel.
Gateway Priority (Prioridad de puerta de enlace) [priority]	El orden de prioridad de la puerta de enlace que se basa en el más alto (1), alto (2), medio (3), bajo (4) o más bajo (5) al que se puede conectar la aplicación de GlobalProtect.
Attempted Gateways (Puertas de enlace intentadas) [attempted_gateways]	Los campos que se recopilan para cada intento de conexión de puerta de enlace con el nombre de la puerta de enlace, el tiempo de respuesta SSL y la prioridad (consulte Prioridad de la puerta de enlace en una configuración de varias puertas de enlace. Cada entrada de campo está separada por comas como `g82-gateway,12,3`. Cada entrada de la puerta de enlace está separada por punto y coma, como `g83-gateway,10,2;g84-gateway,-1,1`.
Gateway Name (Nombre de la puerta de enlace) [gateway]	El nombre de la puerta de enlace que se especifica en la configuración del portal.

Campos de los logs de asignación de etiquetas a IP

Formato: FUTURE_USE , Receive Time, Serial, Type, Threat/Content Type, FUTURE_USE, Generate Time, Virtual System, Source IP, Tag Name , Event ID, Repeat Count , Timeout, Data Source Name, Data Source Type, Data Source Subtype, Sequence Number, Action Flags, DG Hierarchy Level 1 , DG Hierarchy Level 2, DG Hierarchy Level 3, DG Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o	Hora a la que se recibió el log en el plano de gestión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
cef-formatted-receive_time)	
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es IPTAG.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de coincidencias HIP; no utilizado.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log de coincidencias HIP.
Source IP (IP de origen) (src)	Dirección IP del usuario de origen.
Tag Name (Nombre de etiqueta) (tag_name)	Etiqueta asignada a la dirección IP de origen.
Event ID (ID de evento) (event_id)	Cadena que muestra el nombre del evento.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Timeout (Tiempo de espera) (timeout)	Cantidad de tiempo antes de que venza la asignación de etiquetas a dirección IP correspondiente a la dirección IP de origen.
Data Source Name (Nombre de origen de datos) (datasourcename)	Nombre del origen del que se recopila la información de asignación.
Data Source Type (Tipo de origen de datos) (datasource_type)	Origen desde el cual se recopila la información de asignación.
Data Source Subtype (Subtipo de origen de datos) (datasource_subtype)	Mecanismo utilizado para identificar las asignaciones de direcciones IP a nombres de usuario dentro del origen de los datos.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente. Cada tipo de log tiene un espacio de número exclusivo.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos, excepto el grupo de dispositivos compartidos (nivel 0), que no está incluido en esta estructura. Si los valores de log son 12, 34, 45, y 0 significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Virtual System ID (ID de sistema virtual) (vsys_id)	Un identificador único de un sistema virtual en un cortafuegos de Palo Alto Networks.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo*

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	1969-12-31T16:00:00:000-8:00 independientemente de cuándo se recibió el log.

Campos de log de User-ID

Formato: FUTURE_USER, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Virtual System, Source IP, User, Data Source Name, Event ID, Repeat Count, Time Out Threshold, Source Port, Destination Port, Data Source, Data Source Type, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, Factor Type, Factor Completion Time, Factor Number, FUTURE_USE, FUTURE_USE, User Group Flags, User by Source, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es USERID.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de User-ID; los valores son login, logout, register-tag y unregister-tag. • login: usuario que ha iniciado la sesión. • logout: usuario que ha cerrado la sesión. • register-tag: indica la etiqueta o etiquetas registradas para el usuario. • unregister-tag: indica que hay una etiqueta o varias no registradas para el usuario.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log Configuración.
Source IP (IP de origen) (ip)	Dirección IP de origen de la sesión original.
User (Usuario) (user)	Identifica el usuario final.
Data Source Name (Nombre de origen de datos) (datasourcename)	Origen de User-ID que envía la asignación de (puerto) ID a usuarios.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Event ID (ID de evento) (eventid)	Cadena que muestra el nombre del evento.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Umbral de tiempo de espera (timeout)	Tiempo de espera tras el cual se borran las asignaciones de IP a usuarios.
Source Port (beginport)	Puerto de origen utilizado por la sesión.
Destination Port (endport)	Puerto de destino utilizado por la sesión.
Data Source (Origen de datos) (datasource)	Origen desde el cual se recopila la información de asignación.
Data Source Type (Tipo de origen de datos) (datasourcetype)	Mecanismo utilizado para identificar las asignaciones de direcciones IP a usuarios dentro del origen de los datos.
Número de secuencia (seqno)	Número de serie del cortafuegos que generó el log.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Virtual System ID (ID de sistema virtual) (vsys_id)	Un identificador único de un sistema virtual en un cortafuegos de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Factor Type (Tipo de factor) (factortype)	Proveedor que se utiliza para autenticar un usuario cuando se cuenta con autenticación multifactor.
Factor Completion Time (Fecha de finalización de factor) (factorcompletiontime)	Hora de finalización de la autenticación.
Factor Number (Número de factor) (factorno)	Indica el uso de la autenticación primaria (1) o los factores adicionales (2, 3).
User Group Flags (Marcas de grupo de usuarios) (ugflags)	Indicador de si se ha encontrado el grupo de usuarios durante la asignación de grupos de usuarios. Se admiten estos valores: • User Group Found (Grupo de usuarios encontrado): indica si se ha podido asignar el usuario a un grupo. • Duplicate User (Usuario duplicado): indica si se han encontrado usuarios duplicados en un grupo de usuarios. Muestra `N/A (N/D)` si no se encuentra ningún grupo de usuarios.
User by Source (Usuario por origen) (userbysource)	Indica el nombre de usuario recibido del origen por medio de la asignación de dirección IP a nombre de usuario.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm)  *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo* `1969-12-31T16:00:00:000-8:00` *independientemente de cuándo se recibió el log.*

Campos de logs de descifrado

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, Config Version, Generate Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, Time Logged, Session ID, Repeat Count, Source Port, Destination Port,

© 2020 Palo Alto Networks, Inc.

NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, Tunnel, FUTURE_USE, FUTURE_USE, Source VM UUID, Destination VM UUID, UUID for rule, Stage for Client to Firewall, Stage for Firewall to Server, TLS Version, Key Exchange Algorithm, Encryption Algorithm, Hash Algorithm, Policy Name, Elliptic Curve, Error Index, Root Status, Chain Status, Proxy Type, Certificate Serial Number, Fingerprint, Certificate Start Date, Certificate End Date, Certificate Version, Certificate Size, Common Name Length, Issuer Common Name Length, Root Common Name Length, SNI Length, Certificate Flags, Subject Common Name, Issuer Subject Common Name, Root Subject Common Name, Server Name Indication, Error, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Source Dynamic Address Group, Destination Dynamic Address Group, High Res Timestamp, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination Mac Address, Sequence Number, Action Flags

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es DECRYPTION.
Threat/Content Type (Tipo de amenaza/contenido) [subtype]	No se utiliza en el log de descifrado.
Config Version (Versión de configuración) [config_ver]	La versión del software.
Generated Time (Hora de generación) (time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de origen de la sesión original.
Destination Address (Dirección de destino) (dst)	Dirección IP de destino de la sesión original.
NAT Source IP (IP de NAT de origen) (natsrc)	Si se ejecuta un NAT de origen, es el NAT de dirección IP de origen posterior.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
NAT Destination IP (IP de NAT de destino) (natdst)	Si se ejecuta un NAT de destino, es el NAT de dirección IP de destino posterior.
Rule (Regla) [rule]	Regla de la política de seguridad que controla el tráfico de la sesión.
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició la sesión.
Destination User (Usuario de destino) (dstuser)	Nombre del usuario para el que iba destinada la sesión.
Application (Aplicación) (app)	Aplicación asociada a la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de la sesión.
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	El perfil de reenvío de logs aplicado a la sesión.
Time Logged (Tiempo registrado) [time_received]	La hora en que se recibió el log.
Session ID (ID de sesión) (sessionid)	Identificador numérico interno aplicado a cada sesión.
Repeat Count (Número de repeticiones) (repeatcnt)	El número de sesiones con la mismo IP de origen, IP de destino, aplicación y tipo de contenido/amenaza observado en 5 segundos.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
NAT Source Port (Puerto de origen de NAT) (natsport)	NAT de puerto de origen posterior.
NAT Destination Port (Puerto de destino de NAT) (natdport)	NAT de puerto de destino posterior.
Flags (Marcas) (flags)	Campo de 32 bits que proporciona información detallada sobre la sesión; este campo puede descodificarse añadiendo los valores con Y y con el valor registrado: • 0x80000000: la sesión tiene una captura de paquetes (PCAP) • 0x40000000: la opción está habilitada para permitir que un cliente use varias rutas para conectarse a un host de destino. • 0x20000000: se envió el archivo a WildFire para un veredicto. • 0x10000000: se detectó el envío de una credencial empresarial por parte de un usuario final. • 0x08000000: el origen del flujo está en la lista de permitidos y no está sujeta a protección de reconocimiento. • 0x02000000: sesión IPv6 • 0x01000000: se descifró la sesión SSL (proxy SSL). • 0x00800000: se denegó la sesión a través del filtrado de URL. • 0x00400000: la sesión ha realizado una traducción NAT. • 0x00200000: la información de usuario de la sesión se ha capturado mediante el portal de autenticación. • 0x00100000: el tráfico de la aplicación está en un puerto de destino no estándar. • 0x00080000: el valor X-Forwarded-For de un proxy está en el campo Usuario de origen. • 0x00040000: el log corresponde a una transacción en una sesión de proxy HTTP (Transacción proxy). • 0x00020000: el flujo de cliente a servidor está sujeto al reenvío basado en la política. • 0x00010000: el flujo de servidor a cliente está sujeto al reenvío basado en la política. • 0x00008000: la sesión es un acceso a la página de contenedor (Container Page). • 0x00002000: la sesión tiene una coincidencia temporal en una regla para la gestión de las dependencias de las aplicaciones implícitas. Disponible en PAN-OS 5.0.0 y posterior. • 0x00000800: se utilizó el retorno simétrico para reenviar tráfico para esta sesión. • 0x00000400: el tráfico descifrado se envía en texto sin cifrar mediante un puerto de reflejo. • 0x00000100: se está inspeccionando la carga útil del túnel externo.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son: • allow (permitir): la política permitió la sesión. • deny (denegar): la política denegó la sesión. • drop (descartar): la sesión se descartó de manera silenciosa. • drop ICMP (descartar ICMP): la sesión se descartó de manera silenciosa con un mensaje de ICMP inalcanzable al host o aplicación. • reset both (restablecer ambos): la sesión se ha terminado y un restablecimiento de TCP se envía a ambos lados de la conexión. • reset client (restablecer cliente): la sesión se ha terminado y un restablecimiento de TCP se envía al cliente. • reset server (restablecer servidor): la sesión se ha terminado y un restablecimiento de TCP se envía al servidor.
Tunnel (Túnel) [tunnel]	Tipo de túnel.
Source VM UUID (UUID de máquina virtual de origen) (src_uuid)	El identificador único universal de origen para un equipo virtual invitado en el entorno NSX VMware.
Destination VM UUID (UUID de máquina virtual de destino) (dst_uuid)	El identificador único universal de destino para un equipo virtual invitado en el entorno NSX VMware.
UUID for rule (UUID de regla) (rule_uuid)	UUID que identifica la regla de forma permanente.
Stage for Client to Firewall (Etapa del cliente al cortafuegos) [hs_stage_c2f]	La etapa del protocolo de enlace TLS del cliente al cortafuegos, por ejemplo, saludo del cliente, saludo del servidor, certificado, intercambio de claves cliente/servidor, etc.
Stage for Firewall to Server (Etapa del cortafuegos al servidor) [hs_stage_f2s]	La etapa del protocolo de enlace TLS del cortafuegos al servidor.
TLS Version (Versión de TLS) [tls_version]	La versión del protocolo TLS utilizada para la sesión.
Key Exchange Algorithm (Algoritmo de intercambio de claves) [tls_keyxchg]	El algoritmo de intercambio de claves utilizado para la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Encryption Algorithm (Algoritmo de cifrado) [tls_enc]	El algoritmo utilizado para cifrar los datos de la sesión, como AES-128-CBC, AES-256-GCM, etc.
Hash Algorithm (Algoritmo hash) [tls_auth]	El algoritmo de autenticación utilizado para la sesión, por ejemplo, SHA, SHA256, SHA384, etc.
Policy Name (Nombre de la política) [policy_name]	El nombre de la política de descifrado asociada con la sesión.
Elliptic Curve (Curva elíptica) [ec_curve]	La curva de criptografía elíptica que el cliente y el servidor negocian y utilizan para las conexiones que utilizan conjuntos de cifrado ECDHE.
Error Index (Índice de errores) [err_index]	El tipo de error que se ha producido: cifrado, recurso, reanudación, versión, protocolo, certificado, función o HSM.
Root Status (Estado raíz) [root_status]	El estado del certificado raíz, por ejemplo, fiable, no fiable o no inspeccionado.
Chain Status (Estado de la cadena) [chain_status]	Si la cadena es fiable. Los valores son: • Uninspected (No inspeccionado) • Untrusted (No fiable) • Trusted (Fiable) • Incomplete
Proxy Type (Tipo de proxy) [proxy_type]	El tipo de proxy de descifrado, como Forward for Forward Proxy (Reenvío para proxy de reenvío), Inbound for Inbound Inspection (Entrada para inspección entrante), No Decrypt for undecrypted traffic (Sin descifrado para tráfico no descifrado), Decryption Broker (Agente de descifrado), GlobalProtect, etc.
Certificate Serial Number (Número de serie del certificado) [cert_serial]	El identificador único del certificado (generado por el emisor del certificado).
Certificate Fingerprint (Certificado de huella digital) [fingerprint]	Un hash del certificado en formato binario x509.
Certificate Start Date (Fecha de inicio del certificado) [notbefore]	La hora en que el certificado pasó a ser válido (el certificado no es válido antes de esta hora).
Certificate End Date (Fecha de finalización del certificado) [notafter]	La hora en la que caduca el certificado (el certificado deja de ser válido después de esta hora).

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Certificate Version (Versión del certificado) [cert_ver]	La versión del certificado (V1, V2 o V3).
Certificate Size (Tamaño del certificado) [cert_size]	El tamaño de la clave del certificado.
Common Name Length (Longitud del nombre común) [cn_len]	La longitud del nombre común del sujeto.
Issuer Common Name Length (Longitud del nombre común del emisor) [issuer_len]	La longitud del nombre común del emisor.
Root Common Name Length (Longitud del nombre común de raíz) [rootcn_len]	La longitud del nombre común raíz.
SNI Length (Longitud SNI) [sni_len]	La longitud de la indicación del nombre del servidor (nombre de host).
Certificate Flags (Marcas del certificado) [cert_flags]	Las marcas del certificado pueden devolver siete valores: • Session is resumed (La sesión se reanuda) [b_resume_session] • Certificate (subject) common name is truncated (El nombre común del certificado [asunto] está truncado) [b_cert_cn_truncated] • Issuer common name is truncated (El nombre común del emisor está truncado) [b_issuer_cn_truncated] • Root common name is truncated (El nombre común de la raíz está truncado) [b_root_cn_truncated] • Server Name Indication (SNI) is truncated (La indicación del nombre del servidor (SNI) está truncada) [b_sni_truncated] • Certificate type, RSA or ECDSA (Tipo de certificado, RSA o ECDSA) [b_cert_type] • Unused (Sin usar) [padding3]
Subject Common Name (Nombre común del sujeto) [cn]	El nombre de dominio (el nombre del servidor que protege el certificado).
Issuer Common Name (Nombre común del emisor) [issuer_cn]	El nombre de la organización que verificó el contenido del certificado.
Root Common Name (Nombre común de raíz) [root_cn]	El nombre de la entidad de certificación raíz.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Server Name Indication (Indicación del nombre del servidor) [sni]	El nombre de host del servidor con el que el cliente está intentando contactar. El uso de SNI permite a un servidor alojar varios sitios web y presentar varios certificados en la misma dirección IP y puerto TCP porque cada sitio web tiene una SNI única.
Error (error)	Una cadena que muestra el error que ocurrió en el evento.
Container ID (ID de contenedor) [container_id]	Una cadena alfanumérica única que identifica el contenedor si el cortafuegos se ejecuta en un contenedor en la nube.
POD Namespace (Espacio de nombres del POD) [pod_namespace]	El nombre del espacio de nombres del pod de Kubernetes.
POD Name (Nombre del POD) [pod_name]	El nombre del pod de Kubernetes.
Source External Dynamic List (Lista dinámica externa de origen) [src_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de origen del tráfico.
Destination External Dynamic List (Lista dinámica externa de destino) [dst_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de destino del tráfico.
Source Dynamic Address Group (Grupo de direcciones dinámicas de origen) [src_dag]	El grupo de direcciones dinámicas que Device-ID identifica como la fuente del tráfico.
Destination Dynamic Address Group (Grupo de direcciones dinámicas de destino) [dst_dag]	El grupo de direcciones dinámicas que Device-ID identifica como destino del tráfico.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60)

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo* `1969-12-31T16:00:00:000-8:00` *independientemente de cuándo se recibió el log.*
Source Device Category (Categoría de dispositivo de origen) [src_category]	La categoría del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Profile (Perfil de dispositivo de origen) [src_profile]	El perfil de dispositivo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Model (Modelo de dispositivo de origen) [src_model]	El modelo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Vendor (Proveedor del dispositivo de origen) [src_vendor]	El proveedor del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Family (Familia del SO del dispositivo de origen) [src_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Version (Versión del SO del dispositivo de origen) [src_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Hostname (Nombre de host de origen) [src_host]	El nombre de host del dispositivo que Device-ID identifica como el origen del tráfico.
Source MAC Address (Dirección MAC de origen) [src_mac]	La dirección MAC del dispositivo que Device-ID identifica como origen del tráfico.
Destination Device Category (Categoría de dispositivo de destino) [dst_category]	La categoría del dispositivo que Device-ID identifica como destino del tráfico.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Destination Device Profile (Perfil de dispositivo de destino) [dst_profile]	El perfil de dispositivo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Model (Modelo de dispositivo de destino) [dst_model]	El modelo del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device Vendor (Proveedor de dispositivos de destino) [dst_vendor]	El proveedor del dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Family (Familia de SO del dispositivo de destino) [dst_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el destino del tráfico.
Destination Device OS Version (Versión de SO del dispositivo de destino) [dst_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como destino del tráfico.
Destination Hostname (Nombre de host de destino) [dst_host]	El nombre de host del dispositivo que Device-ID identifica como el destino del tráfico.
Destination MAC Address (Dirección MAC de destino) [dst_mac]	La dirección MAC del dispositivo que Device-ID identifica como destino del tráfico.
Número de secuencia (seqno)	Un identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.

Campos del log de inspección de túnel

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Severity, Sequence Number, Action Flags, Source Location, Destination Location, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel, Bytes, Bytes Sent, Bytes Received, Packets, Packets Sent, Packets Received, Maximum Encapsulation, Unknown Protocol, Strict Check, Tunnel

© 2020 Palo Alto Networks, Inc.

Fragment, Sessions Created, Sessions Closed, Session End Reason, Action Source, Start Time, Elapsed Time, Tunnel Inspection Rule, Remote User IP, Remote User ID, Rule UUID, PCAP ID, Dynamic User Group, Source External Dynamic List, Destination External Dynamic List, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Mes, día y hora en que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Tipo de log en relación con la sesión: START o END.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log Tráfico; los valores son Iniciar, Finalizar, Colocar y Denegar. • Start (Iniciar): sesión iniciada. • Finalizar: sesión finalizada. • Drop (Descartar): sesión descartada antes de identificar la aplicación; no hay ninguna regla que permita la sesión. • Deny (Denegar): sesión descartada después de identificar la aplicación; hay una regla para bloquear o no hay ninguna regla que permita la sesión.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de origen de los paquetes de la sesión.
Destination Address (Dirección de destino) (dst)	Dirección IP de destino de los paquetes de la sesión.
NAT Source IP (IP de NAT de origen) (natsrc)	Si se ejecuta un NAT de origen, es el NAT de dirección IP de origen posterior.
NAT Destination IP (IP de NAT de destino) (natdst)	Si se ejecuta un NAT de destino, es el NAT de dirección IP de destino posterior.
Rule Name (Rule) (Nombre de regla [Regla])	Nombre de la regla de política de seguridad en vigencia en la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Source User (Usuario de origen) (srcuser)	ID de usuario de origen de los paquetes de la sesión.
Destination User (Usuario de destino) (dstuser)	ID de usuario de origen de los paquetes de la sesión.
Application (Aplicación) (app)	Protocolo de tunelización utilizado en la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de los paquetes de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de los paquetes de la sesión.
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	Perfil de reenvío de logs aplicado a la sesión.
Session ID (ID de sesión) (sessionid)	ID de la sesión que se está registrando.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
NAT Source Port (Puerto de origen de NAT) (natsport)	NAT de puerto de origen posterior.
NAT Destination Port (Puerto de destino de NAT) (natdport)	NAT de puerto de destino posterior.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Flags (Marcas) (flags)	Campo de 32 bits que proporciona información detallada sobre la sesión; este campo puede descodificarse añadiendo los valores con Y y con el valor registrado: • 0x80000000: la sesión tiene una captura de paquetes (PCAP). • 0x02000000: sesión IPv6. • 0x01000000: la sesión SSL se ha descifrado (proxy SSL). • 0x00800000: la sesión se ha denegado a través del filtrado de URL. • 0x00400000: la sesión ha realizado una traducción NAT (NAT). • 0x00200000: la información de usuario de la sesión se ha capturado mediante el portal de autenticación. • 0x00080000: el valor X-Forwarded-For de un proxy está en el campo Usuario de origen. • 0x00040000: el log corresponde a una transacción en una sesión de proxy HTTP (Transacción proxy). • 0x00008000: la sesión es un acceso a la página de contenedor (Container Page). • 0x00002000: la sesión tiene una coincidencia temporal en una regla para la gestión de las dependencias de las aplicaciones implícitas. Disponible en PAN-OS 5.0.0 y posterior. • 0x00000800: se utilizó el retorno simétrico para reenviar tráfico para esta sesión.
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son: • Permitir: la política permitió la sesión. • Deny (Denegar): la política denegó la sesión. • Drop (Descartar): la sesión se descartó de manera silenciosa. • Drop ICMP (Descartar ICMP): la sesión se descartó de manera silenciosa con un mensaje de ICMP inalcanzable al host o aplicación. • Restablecer ambos: La sesión se ha terminado y un restablecimiento de TCP se envía a ambos lados de la conexión. • Restablecer cliente: La sesión se ha terminado y un restablecimiento de TCP se envía al cliente. • Restablecer servidor: La sesión se ha terminado y un restablecimiento de TCP se envía al servidor.
Severity (Gravedad) (severity)	Gravedad asociada al evento; los valores son Informativo, Bajo, Medio, Alto y Crítico.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único. Este campo no es compatible con los cortafuegos PA-7000 Series.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Source Location (Ubicación de origen) (srcloc)	País de origen o región interna para direcciones privadas; la longitud máxima es de 32 bytes.
Destination Location (Ubicación de destino) (dstloc)	País de destino o región interna para direcciones privadas. La longitud máxima es de 32 bytes.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Tunnel ID (ID de túnel) (tunnelid)	ID del túnel que se está inspeccionando o ID de identidad de suscriptor móvil internacional (International Mobile Subscriber Identity, IMSI) del usuario móvil.
Monitor Tag (Etiqueta de supervisión) (monitortag)	Nombre de supervisor que configuró para la regla de política de inspección de túnel o el ID de identidad de equipo móvil internacional (International Mobile Equipment Identity, IMEI) del dispositivo móvil.
Parent Session ID (ID de sesión principal) (parent_session_id)	ID de la sesión en la cual se tuneliza esta sesión. Se aplica al túnel interno (si hay dos niveles de tunelización) o al contenido interno (si hay un nivel de tunelización) únicamente.
Hora de inicio principal (parent_start_time)	Año/mes/día horas:minutos:segundos desde que comenzó la sesión de túnel principal.
Tunnel Type (Tipo de túnel) (tunnel)	Tipo de túnel, tal como GRE o IPSec.
Bytes (bytes)	Cantidad de bytes de la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Bytes Sent (Bytes enviados) (bytes_sent)	Número de bytes en la dirección cliente a servidor de la sesión.
Bytes Received (Bytes recibidos) (bytes_received)	Número de bytes en la dirección servidor a cliente de la sesión.
Packets (Paquetes) (packets)	Número total de paquetes (transmitidos y recibidos) de la sesión.
Paquetes enviados (pkts_sent)	Números de paquetes de cliente a servidor de la sesión.
Paquetes recibidos (pkts_received)	Números de paquetes de servidor a cliente de la sesión.
Encapsulación máxima (max_encap)	Cantidad de paquetes que el cortafuegos descartó debido a que el paquete excedía la cantidad máxima de niveles de encapsulación configurados en la regla de política de inspección de túnel (descartar paquete si se excede el nivel máximo de inspección de túnel).
Protocolo desconocido (unknown_proto)	Cantidad de paquetes que el cortafuegos descartó debido a que contiene un protocolo desconocido, según se habilitó en la regla de política de inspección de túnel (descartar paquete si hay un protocolo desconocido dentro del túnel).
Comprobación estricta (strict_check)	Cantidad de paquetes que el cortafuegos descartó debido a que el encabezado del protocolo del túnel en el paquete no cumplió con el RFC para el protocolo del túnel, según se habilitó en la regla de política de inspección de túnel (**Drop packet if tunnel protocol fails strict header check [Descartar paquete si el protocolo del túnel no supera la comprobación de encabezado estricto]**).
Fragmento de túnel (tunnel_fragment)	Cantidad de paquetes que el cortafuegos descartó debido a errores de fragmentación.
Sesiones creadas (sessions_created)	Cantidad de sesiones internas creadas.
Sesiones cerradas (sessions_closed)	Cantidad de sesiones completas/cerradas que se crearon.
Razón del fin de sesión (session_end_reason)	Razón por la que ha finalizado una sesión. Si la finalización ha tenido varias causas, este campo solo muestra la más importante. Los valores de la posible razón de finalización de la sesión son los siguientes en orden de prioridad (el primero es el más importante): • threat: el cortafuegos ha detectado una amenaza asociada a una acción de restablecimiento, borrado o bloqueo (dirección IP). • policy-deny: La sesión ha hecho coincidir una regla de seguridad con una acción de denegación o borrado. • decrypt-cert-validation: la sesión finalizó debido a que usted configuró el cortafuegos para que bloquee el cifrado de proxy de reenvío SSL o

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)

	la inspección de entrada SSL cuando la sesión utilice la autenticación de cliente o un certificado de servidor con cualquiera de las siguientes condiciones: vencido, emisor no fiable, estado desconocido o tiempo de espera de verificación de estado agotado. Este motivo de fin de la sesión también se muestra cuando el certificado del servidor produce un alerta de error irrecuperable de tipo bad_certificate, unsupported_certificate, certificate_revoked, access_denied o no_certificate_RESERVED (SSLv3 únicamente).
	• decrypt-unsupport-param: la sesión finalizó porque usted configuró el cortafuegos para que bloquee el descifrado de proxy de reenvío SSL o la inspección de entrada SSL cuando la sesión utiliza una versión de protocolo, cifra o algoritmo SSH no compatible. Este motivo de fin de la sesión se muestra cuando la sesión produce una alerta de error irrecuperable de tipo unsupported_extension, unexpected_message o handshake_failure.
	• Decrypt-error: la sesión finalizó porque usted configuró el cortafuegos para que bloquee el descifrado de proxy de reenvío SSL o la inspección de entrada SSL cuando los recursos del cortafuegos o el módulo de seguridad de (hardware security module, HSM) no estaban disponibles. Este motivo de fin de la sesión también se muestra cuando usted configura el cortafuegos para que bloquee el tráfico SSL con errores de SSH que produjo una alerta de error irrecuperable que no sea ninguna de las enumeradas para los motivos de finalización decrypt-cert-validation y decrypt-unsupport-param.
	• tcp-rst-from-client: el cliente ha enviado un restablecimiento de TCP al servidor.
	• tcp-rst-from-server: el servidor ha enviado un restablecimiento de TCP al cliente.
	• resources-unavailable: la sesión se ha cancelado debido a una limitación de recursos del sistema. Por ejemplo, la sesión podría haber superado el número de paquetes que no funcionan permitidos por flujo o por la cola de paquetes que no funcionan globales.
	• tcp-fin: uno o varios hosts de la conexión han enviado un mensaje FIN de TCP para cerrar la sesión.
	• tcp-reuse: se reutiliza una sesión y el cortafuegos cierra la sesión anterior.
	• decoder: el decodificador detecta una nueva conexión en el protocolo (como HTTP-Proxy) y finaliza la conexión anterior.
	• aged-out: la sesión ha caducado.
	• unknown: este valor se aplica en las siguientes situaciones:
	  • Terminaciones de sesiones a las que no se aplican los motivos anteriores (por ejemplo, un comando `clear session all`).
	  • Para logs generados en una versión de PAN-OS que no admite el campo de razón de finalización de sesión (versiones posteriores a PAN-OS 6.1), el valor será `unknown` (desconocido) después de una actualización de la versión actual de PAN-OS o después de que los logs se carguen en el cortafuegos.
	  • En Panorama, los logs recibidos de los cortafuegos para los que la versión de PAN-OS no admite razones de finalización de sesión tendrán un valor `unknown`.
	• n/a: Este valor se aplica cuando el tipo de log de tráfico no es **end**.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Origen de acción (action_source)	Especifica si la acción desarrollada para permitir o bloquear una aplicación se definió en la aplicación o en la política. Las acciones pueden: permitir, denegar, descartar, restablecer servidor, restablecer cliente o restablecer ambos para la sesión.
Start Time (start) (Fecha de inicio [start])	Año/mes/día horas:minutos:segundos desde que comenzó la sesión.
Elapsed Time (Tiempo transcurrido) (elapsed)	Tiempo transcurrido en la sesión.
Tunnel Inspection Rule (tunnel_insp_rule)	Nombre de la regla de inspección del túnel que coincide con el tráfico del túnel de texto no cifrado.
Remote User IP (IP de usuario remoto) (remote_user_ip)	Dirección IPv4 o IPv6 de un usuario remoto.
Remote User ID (ID de usuario remoto) (remote_user_id)	Identidad IMSI de un usuario remoto y, si está disponible, una identidad IMEI o una identidad MSISDN.
Security Rule UUID (Regla UUID de seguridad) (rule_uuid)	UUID que identifica la regla de forma permanente.
ID de captura de paquetes (pcap_id)	Identificador único de captura de paquetes que define la ubicación del archivo pcap en el cortafuegos.
Dynamic User Group Name (Nombre de grupo de usuarios dinámicos) (dynusergroup_name)	El nombre del grupo de usuarios dinámicos que contiene el usuario que inició la sesión.
Source External Dynamic List (Lista dinámica externa de origen) [src_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de origen del tráfico.
Destination External Dynamic List (Lista dinámica externa de destino) [dst_edl]	El nombre de la lista dinámica externa que contiene la dirección IP de destino del tráfico.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31)

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	• **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo* `1969-12-31T16:00:00.000-8:00` *independientemente de cuándo se recibió el log.*

Campos de logs de SCTP

Formato: FUTURE_USE, Receive Time, Serial Number, Type, FUTURE_USE, FUTURE_USE, Generated Time, Source Address, Destination Address, FUTURE_USE, FUTURE_USE, Rule Name, FUTURE_USE, FUTURE_USE, FUTURE_USE, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, IP Protocol, Action, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Sequence Number, FUTURE_USE, SCTP Association ID, Payload Protocol ID, Severity, SCTP Chunk Type, FUTURE_USE, SCTP Verification Tag 1, SCTP Verification Tag 2, SCTP Cause Code, Diameter App ID, Diameter Command Code, Diameter AVP Code, SCTP Stream ID, SCTP Association End Reason, Op Code, SCCP Calling Party SSN, SCCP Calling Party Global Title, SCTP Filter, SCTP Chunks, SCTP Chunks Sent, SCTP Chunks Received, Packets, Packets Sent, Packets Received, UUID for rule, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es SCTP.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de origen de la sesión original.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Destination Address (Dirección de destino) (dst)	Dirección IP de destino de la sesión original.
Rule Name (Rule) (Nombre de regla [Regla])	Nombre de la regla de política de seguridad en vigencia en la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de la sesión.
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	Perfil de reenvío de logs aplicado a la sesión.
Session ID (ID de sesión) (sessionid)	Identificador numérico interno aplicado a cada sesión.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son: • allow (permitir): la política permitió la sesión. • deny (denegar): la política denegó la sesión.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
SCTP Association ID (ID de asociación de SCTP) (assoc_id)	Un identificador lógico interno numérico de 56 bits que se aplica a cada asociación de SCTP.
Payload Protocol ID (ID de protocolo de carga) (ppid)	Identifica el ID de protocolo de carga (Payload Protocol ID, PPID) en el fragmento de datos que activó este evento. La autoridad de asignación de números de Internet (Internet Assigned Numbers Authority, IANA) asigna el PPID.
Severity (Gravedad) (severity)	Gravedad asociada al evento; los valores son Informativo, Bajo, Medio, Alto y Crítico.
SCTP Chunk Type (Tipo de fragmento de SCTP) (sctp_chunk_type)	Describe el tipo de información en un fragmento, como datos o de control.
SCTP Event Type (Tipo de evento de SCTP) (sctp_event_type)	Define el evento activado por fragmento o paquete de SCTP cuando el perfil de protección de SCTP se aplica al tráfico de SCTP. También lo activa el inicio o el final de una asociación de SCTP.
SCTP Verification Tag 1 (Verificación de SCTP de etiqueta 1) (verif_tag_1)	La utiliza el endpoint1, que inicia la asociación para verificar si el paquete de SCTP que recibió pertenece a la asociación de SCTP actual y para validar el endpoint2.
SCTP Verification Tag 2 (Verificación de SCTP de etiqueta 2) (verif_tag_2)	La utiliza el endpoint2 para verificar si el paquete de SCTP que recibió pertenece a la asociación de SCTP actual y para validar el endpoint1.
SCTP Cause Code (Código de causa de SCTP) (sctp_cause_code)	Lo envía un endpoint para especificar el motivo de una condición de error a otro endpoint de la misma asociación de SCTP.
Diameter App ID (ID de aplicación de diámetro) (diam_app_id)	La aplicación de diámetro en el fragmento de datos que activó el evento. La autoridad de asignación de números de Internet (Internet Assigned Numbers Authority, IANA) asigna el ID de aplicación de diámetro.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Diameter Command Code (Código de comando de diámetro) (diam_cmd_code)	El código de comando de diámetro en el fragmento de datos que activó el evento. La autoridad de asignación de números de Internet (Internet Assigned Numbers Authority, IANA) asigna el código de comando del diámetro.
Diameter AVP Code (Código de AVP de diámetro) (diam_avp_code)	El código de AVP del diámetro en el fragmento de datos que activó el evento.
SCTP Stream ID (ID de flujo de SCTP) (stream_id)	ID del flujo que transporta el fragmento de datos que activó el evento.
SCTP Association End Reason (Motivo de fin de asociación de SCTP) (assoc_end_reason)	Motivo por el que finalizó una asociación. Si la finalización tuvo varios motivos, se muestra el de prioridad más alta. Los posibles motivos de la finalización de la sesión en prioridad descendente son los siguientes: • shutdown-from-endpoint (mayor prioridad): el endpoint envía `SHUTDOWN` • abort-from-endpoint: el endpoint envía `ABORT` • unknown (menor prioridad): la asociación ha caducado, o el motivo de la finalización de la asociación no se incluye en los motivos anteriores (por ejemplo, un comando clear session all [borrar todas las sesiones]).
Op Code (Código de operación) (op_code)	Identifica el código de operación de los protocolos SS7 de capa de aplicación, como MAP o CAP, en el fragmento de datos que activó el evento.
SCCP Calling Party SSN (SSN de emisor de llamada de SCCP) (sccp_calling_ssn)	El número de subsistema (subsystem number, SSN) del emisor de la llamada del dispositivo de control de la conexión de señalización (Signaling Connection Control Part, SCCP) en el fragmento de datos que activó el evento.
SCCP Calling Party Global Title (Título global de emisor de llamada de SCCP) (sccp_calling_gt)	El título global (Global Title, GT) del emisor de la llamada del dispositivo de control de la conexión de señalización (Signaling Connection Control Part, SCCP) en el fragmento de datos que activó el evento.
SCTP Filter (sctp_filter)	Nombre del filtro con el que coincidió el fragmento de SCTP.
SCTP Chunks (Fragmentos de SCTP) (chunks)	Número total de fragmentos (transmitidos y recibidos) de la asociación.
SCTP Chunks Sent (Fragmentos de SCTP enviados) (chunks_sent)	Número de fragmentos endpoint1-to-endpoint2 (que inicia la asociación) para la asociación.
SCTP Chunks Received (Fragmentos de SCTP recibidos) (chunks_received)	Número de fragmentos endpoint2-to-endpoint1 (que inicia la asociación) para la asociación.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Packets (Paquetes) (packets)	Número total de paquetes (transmitidos y recibidos) de la sesión.
Paquetes enviados (pkts_sent)	Números de paquetes de cliente a servidor de la sesión.
Paquetes recibidos (pkts_received)	Números de paquetes de servidor a cliente de la sesión.
UUID for rule (UUID de regla) (rule_uuid)	UUID que identifica la regla de forma permanente.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo `1969-12-31T16:00:00:000-8:00` independientemente de cuándo se recibió el log.*

Campos de logs de autenticación

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Virtual System, Source IP, User, Normalize User, Object, Authentication Policy, Repeat Count, Authentication ID, Vendor, Log Action, Server Profile, Description, Client Type, Event Type, Factor Number, Sequence Number, Action Flags, Device Group Hierarchy 1, Device Group Hierarchy 2, Device Group Hierarchy 3, Device Group Hierarchy 4, Virtual System Name, Device Name, Virtual System ID, Authentication Protocol, UUID for rule, High Resolution Timestamp, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o	Hora a la que se recibió el log en el plano de gestión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
cef-formatted-receive_time)	
Serial Number (Número de serie) (serial)	Número de serie del dispositivo que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es AUTHENTICATION.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log de sistema; hace referencia al demonio de sistema que genera el log. Los valores son crypto (criptográfico), dhcp, dnsproxy (proxy DNS), dos, general (general), global-protect (GlobalProtect), ha (alta disponibilidad), hw (hardware), nat (NAT), ntpd (demonio NTP), pbf (PBF), port (puerto), pppoe (PPPoE), ras (RAS), routing (enrutamiento), satd, sslmgr (gestor SSL), sslvpn (VPN SSL), userid (ID de usuario), url-filtering (filtrado de URL) y vpn (VPN).
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source IP (IP de origen) (ip)	Dirección IP de origen de la sesión original.
User (Usuario) (user)	Usuario final que se autentica.
Normalize User (Usuario normalizado) (normalize_user)	Versión normalizada del nombre de usuario que se autentica (como la anexión de un nombre de dominio al nombre de usuario).
Object (Objeto) (object)	Nombre del objeto asociado al evento del sistema.
Authentication Policy (Política de autenticación) (authpolicy)	Política que se invoca para la autenticación antes de permitir el acceso al recurso protegido.
Repeat Count (Número de repeticiones) (repeatcnt)	Número de sesiones con el mismo IP de origen, IP de destino, aplicación y subtipo observados en 5 segundos.
Authentication ID (ID de autenticación) (authid)	ID único que se brinda para la autenticación primaria y la autenticación (multifactor) adicional.
Vendor (Proveedor) (vendor)	El proveedor que brinda la autenticación de factor adicional.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Log Action (Acción con logs) (logset)	Log Action (Acción con logs) (logset)
Server Profile (serverprofile)	Servidor de autenticación que se utiliza para realizar la autenticación.
Description (desc)	Información de autenticación adicional.
Client Type (Tipo de cliente) (clienttype)	Tipo de cliente que se utiliza para completar la autenticación (como el portal de autenticación).
Event Type (Tipo de evento) (event)	Resultado del intento de autenticación.
Factor Number (Número de factor) (factorno)	Indica el uso de la autenticación primaria (1) o los factores adicionales (2, 3).
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente. Cada tipo de log tiene un espacio de número exclusivo.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Virtual System ID (ID de sistema virtual) (vsys_id)	Un identificador único de un sistema virtual en un cortafuegos de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Authentication Protocol (authproto)	Indica el protocolo de autenticación que utiliza el servidor. Por ejemplo, PEAP con GTC.
UUID for rule (UUID de regla) (rule_uuid)	UUID que identifica la regla de forma permanente.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res _timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo* `1969-12-31T16:00:00.000-8:00` *independientemente de cuándo se recibió el log.*
Source Device Category (Categoría de dispositivo de origen) [src_category]	La categoría del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Profile (Perfil de dispositivo de origen) [src_profile]	El perfil de dispositivo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Model (Modelo de dispositivo de origen) [src_model]	El modelo del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device Vendor (Proveedor del dispositivo de origen) [src_vendor]	El proveedor del dispositivo que Device-ID identifica como el origen del tráfico.
Source Device OS Family (Familia del SO del dispositivo de origen) [src_osfamily]	El tipo de sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Source Device OS Version (Versión del SO del dispositivo de origen) [src_osversion]	La versión del sistema operativo para el dispositivo que Device-ID identifica como el origen del tráfico.
Source Hostname (Nombre de host de origen) [src_host]	El nombre de host del dispositivo que Device-ID identifica como el origen del tráfico.
Source MAC Address (Dirección MAC de origen) [src_mac]	La dirección MAC del dispositivo que Device-ID identifica como origen del tráfico.

Configuración de campos de logs

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Host, Virtual System, Command, Admin, Client, Result, Configuration Path, Before Change Detail, After Change Detail, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Device Group, Audit Comment

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del dispositivo que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es CONFIG.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log Configuración; no utilizado.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Host (host)	Nombre de host o dirección IP de la máquina cliente.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log de configuración.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Comando (cmd)	Comando ejecutado por el administrador; los valores son añadir, duplicar, compilar, eliminar, editar, mover, renombrar y establecer.
Administrador (admin)	Nombre de usuario del administrador que realiza la configuración.
Cliente (client)	Cliente utilizado por el administrador; los valores son Web y CLI.
Resultado (result)	Resultado de la acción de configuración; los valores son Enviada, Correctamente, Fallo y No autorizado.
Ruta de configuración (path)	Ruta del comando de configuración emitido; puede tener una longitud de hasta 512 bytes.
Detalle antes del cambio (before_change_detail)	Este campo solo se incluye en los logs personalizados y no tiene el formato predeterminado. Contiene la xpath completa antes del cambio de configuración.
Detalle después del cambio (after_change_detail)	Este campo solo se incluye en los logs personalizados y no tiene el formato predeterminado. Contiene la xpath completa después del cambio de configuración.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente; cada tipo de log tiene un espacio de número exclusivo.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Device Group (Grupo de dispositivos) [dg_id]	El grupo de dispositivos al que pertenece el cortafuegos si lo gestiona un servidor de gestión Panorama™.
Audit Comment (Comentario de auditoría) [comment]	El comentario de auditoría especificado en un cambio de configuración de regla de políticas.

Campos de logs del sistema

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Content/Threat Type, FUTURE_USE, Generated Time, Virtual System, Event ID, Object, FUTURE_USE, FUTURE_USE, Module, Severity, Description, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, FUTURE_USE, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es SYSTEM.
Content/Threat Type (Tipo de contenido o amenaza) (subtype)	Subtipo del log de sistema; hace referencia al demonio de sistema que genera el log. Los valores son crypto (criptográfico), dhcp, dnsproxy (proxy DNS), dos, general (general), global-protect (GlobalProtect), ha (alta disponibilidad), hw (hardware), nat (NAT), ntpd (demonio NTP), pbf (PBF), port (puerto), pppoe (PPPoE), ras (RAS), routing (enrutamiento), satd, sslmgr (gestor SSL), sslvpn (VPN SSL), userid (ID de usuario), url-filtering (filtrado de URL) y vpn (VPN).
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log Configuración.
Event ID (ID de evento) (eventid)	Cadena que muestra el nombre del evento.
Object (Objeto) (object)	Nombre del objeto asociado al evento del sistema.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Módulo (module)	Este campo únicamente es válido cuando el valor del campo Subtipo es General. Proporciona información adicional acerca del subsistema que genera el log; los valores son General, Management (Gestión), Auth (Autenticación), HA, Upgrade (Actualizar) y Chassis (Bastidor).
Severity (Gravedad) (severity)	Gravedad asociada al evento; los valores son Informativo, Bajo, Medio, Alto y Crítico.
Description (Descripción) (opaque)	Descripción detallada del evento, hasta un máximo de 512 bytes.
Número de secuencia (seqno)	Identificador de entrada de log de 64 bits que aumenta secuencialmente, cada tipo de log tiene un espacio de número único.
Marcas de acción (actionflags)	Campo de bits que indica si el log se ha reenviado a Panorama.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm)

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
	La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo `1969-12-31T16:00:00.000-8:00` *independientemente de cuándo se recibió el log.*

Campos de log de eventos correlacionados

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Content/Threat Type, FUTURE_USE, Generated Time, Source Address. Source User, Virtual System, Category, Severity, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, Object Name, Object ID, Evidence

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del dispositivo que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es CORRELATION.
Content/Threat Type (Tipo de contenido o amenaza) (subtype)	Subtipo del log de sistema; hace referencia al demonio de sistema que genera el log. Los valores son crypto (criptográfico), dhcp, dnsproxy (proxy DNS), dos, general (general), global-protect (GlobalProtect), ha (alta disponibilidad), hw (hardware), nat (NAT), ntpd (demonio NTP), pbf (PBF), port (puerto), pppoe (PPPoE), ras (RAS), routing (enrutamiento), satd, sslmgr (gestor SSL), sslvpn (VPN SSL), userid (ID de usuario), url-filtering (filtrado de URL) y vpn (VPN).
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de usuario que inició el evento.
Source User (Usuario de origen) (srcuser)	Nombre del usuario que inició el evento.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado al log Configuración.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Category (Categoría) (category)	Resumen del tipo de amenaza o riesgo para la red, usuario o host.
Severity (Gravedad) (severity)	Gravedad asociada al evento; los valores son Informativo, Bajo, Medio, Alto y Crítico.
Jerarquía de grupos de dispositivos (dg_hier_level_1 a dg_hier_level_4)	Secuencia de números de identificación que indica la ubicación del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o sistema virtual) que genera el log incluye el número de identificación de cada antecesor en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartidos (nivel 0) no se incluye en esta estructura. Si los valores de log son 12, 34, 45, 0, significa que el log lo generó un cortafuegos (o sistema virtual) que pertenece al grupo de dispositivos 45, y que sus antecesores son 34 y 12. Para ver los nombres de grupos de dispositivos que corresponden con el valor 12, 34 o 45, use uno de los siguientes métodos: Consulta de la API: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
Nombre de sistema virtual (vsys_name)	El nombre del sistema virtual asociado con la sesión; solo válido en los cortafuegos habilitados para múltiples sistemas virtuales.
Nombre del dispositivo (device_name)	El nombre de host del cortafuegos en el que se inició sesión.
Virtual System ID (ID de sistema virtual) (vsys_id)	Un identificador único de un sistema virtual en un cortafuegos de Palo Alto Networks.
Nombre de objeto (objectname)	Nombre del objeto de correlación con el que se produjo la coincidencia.
Object ID (ID de objeto) (object_id)	Nombre del objeto asociado al evento del sistema.
Evidence (Evidencia) (evidence)	Una afirmación de resumen que indica las veces que el host halló coincidencias con las condiciones definidas en el objeto de correlación. Por ejemplo, el host ingresó en la URI de malware conocida (19 veces).

Campos del log de GTP

Formato: FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, FUTURE_USE, FUTURE_USE, Rule Name, FUTURE_USE, FUTURE_USE, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, FUTURE_USE, Source Port, Destination Port, FUTURE_USE, FUTURE_USE, FUTURE_USE, Protocol, Action, GTP Event Type, MSISDN, Access Point Name, Radio Access Technology, GTP Message Type, End User IP Address, Tunnel Endpoint Identifier1, Tunnel Endpoint Identifier2, GTP Interface, GTP Cause, Severity, Serving Country MCC,

© 2020 Palo Alto Networks, Inc.

Serving Network MNC, Area Code, Cell ID, GTP Event Code, FUTURE_USE, FUTURE_USE, Source Location, Destination Location, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, Tunnel ID/IMSI, Monitor Tag/IMEI, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, Start Time, Elapsed Time, Tunnel Inspection Rule, Remote User IP, Remote User ID, UUID for rule, PCAP ID, High Resolution Timestamp

Nombre de campo	Description (Descripción)
Receive Time (Hora de recepción) (receive_time o cef-formatted-receive_time)	Mes, día y hora a la que se recibió el log en el plano de gestión.
Serial Number (Número de serie) (serial)	Número de serie del cortafuegos que generó el log.
Tipo (type)	Especifica el tipo de log; el valor es GTP.
Threat/Content Type (Tipo de amenaza o contenido) (subtype)	Subtipo del log Tráfico; los valores son Iniciar, Finalizar, Colocar y Denegar. • Start (Iniciar): sesión iniciada. • Finalizar: sesión finalizada. • Drop (Descartar): sesión descartada antes de identificar la aplicación; no hay ninguna regla que permita la sesión. • Deny (Denegar): sesión descartada después de identificar la aplicación; hay una regla para bloquear o no hay ninguna regla que permita la sesión.
Generated Time (Hora de generación) (time_generated o cef-formatted-time_generated)	Hora a la que se generó el log en el plano de datos.
Source Address (Dirección de origen) (src)	Dirección IP de origen de los paquetes de la sesión.
Destination Address (Dirección de destino) (dst)	Dirección IP de destino de los paquetes de la sesión.
Rule Name (Rule) (Nombre de regla [Regla])	Nombre de la regla de política de seguridad en vigencia en la sesión.
Application (Aplicación) (app)	Protocolo de tunelización utilizado en la sesión.
Virtual System (Sistema virtual) (vsys)	Sistema virtual asociado a la sesión.
Source Zone (Zona de origen) (from)	Zona de origen de los paquetes de la sesión.
Destination Zone (Zona de destino) (to)	Zona de destino de los paquetes de la sesión.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Inbound Interface (Interfaz entrante) (inbound_if)	Interfaz de la que se obtuvo la sesión.
Outbound Interface (Interfaz saliente) (outbound_if)	Interfaz de destino de la sesión.
Log Action (Acción con logs) (logset)	Perfil de reenvío de logs aplicado a la sesión.
Session ID (ID de sesión) (sessionid)	ID de la sesión que se está registrando.
Source Port (Puerto de origen) (sport)	Puerto de origen utilizado por la sesión.
Destination Port (Puerto de destino) (dport)	Puerto de destino utilizado por la sesión.
IP Protocol (Protocolo IP) (proto)	Protocolo IP asociado a la sesión.
Action (Acción) (action)	Acción realizada para la sesión; los valores son: • allow (permitir): la política permitió la sesión. • deny (denegar): la política denegó la sesión.
Tipo de evento de GTP (event_type)	Define los eventos activados con un mensaje de GTP cuando se aplican las comprobaciones en el perfil de protección de GTP en el tráfico de GTP. También es activado por el inicio o final de una sesión GTP.
MSISDN (msisdn)	Identidad de servicio asociada con el suscriptor móvil compuesto por un código de país, código de destino nacional y suscriptor. Consta de dígitos decimales (0-9) únicamente con un máximo de 15 dígitos.
Nombre de punto de acceso (apn)	Referencia a una puerta de enlace de datos de red de datos de paquete (PGW)/nodo de soporte GPRS de puerta de enlace en una red móvil. Compuesto por un identificador de red APN obligatorio y un identificador de operador APN opcional.
Tecnología de acceso por radio (rat)	Tipo de tecnología utilizada para el acceso por radio. Por ejemplo, EUTRAN, WLAN, Virtual, HSPA Evolution, GAN y GERAN.
Tipo de mensaje de GTP (msg_type)	Indica el tipo de mensaje GTP.
Dirección IP final (end_ip_adr)	Dirección IP de un suscriptor móvil asignado por un PGW/GGSN.
Identificador1 de extremo de túnel (teid1)	Identifica el túnel GTP en el nodo de red. TEID1 es el primer TEID en el mensaje GTP.
Identificador2 de extremo de túnel (teid2)	Identifica el túnel GTP en el nodo de red. TEID2 es el segundo TEID en el mensaje GTP.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Interfaz GTP (gtp_interface)	Interfaz 3GPP de la cual se recibe un mensaje GTP.
Causa de GTP (cause_code)	El valor de causa de GTP en las respuestas de logs que contienen un elemento de información que proporciona información sobre la aceptación o el rechazo de las solicitudes GTP por un nodo de red.
Severity (Gravedad) (severity)	Gravedad asociada al evento; los valores son Informativo, Bajo, Medio, Alto y Crítico.
MCC de red de servicio (mcc)	Código de país móvil del operador de red central que brinda servicio.
MNC de red de servicio (mnc)	Código de red móvil del operador de red central que brinda servicio.
Area Code (area_code)	Área dentro de una red pública de comunicaciones móviles (Public Land Mobile Network, PLMN).
ID celular (cell_id)	Estación de base dentro de un código de área.
Código de evento de GTP (event_code)	Código de evento que describe el evento GTP.
Source Location (Ubicación de origen) (srcloc)	País de origen o región interna para direcciones privadas; la longitud máxima es de 32 bytes.
Destination Location (Ubicación de destino) (dstloc)	País de destino o región interna para direcciones privadas; la longitud máxima es de 32 bytes.
Tunnel ID/IMSI (ID o IMSI de túnel) (imsi)	La Identidad internacional de abonado móvil (International Mobile Subscriber Identity, IMSI) es un número único que se asigna a cada suscriptor móvil en el sistema GSM/UMTS/EPS. La IMSI incluirá digitos decimales (0 a 9) únicamente y el número máximo de digitos es de 15.
Monitor Tag/IMEI (Etiqueta o IMEI de supervisión) (imei)	La Identidad internacional de equipo móvil (International Mobile Equipment Identity, IMEI) es un número único de 15 o 16 dígitos asignado a cada equipo de estación móvil.
Start Time (start) (Fecha de inicio [start])	Hora de inicio de sesión.
Elapsed Time (Tiempo transcurrido) (elapsed)	Tiempo transcurrido en la sesión.
Tunnel Inspection Rule (Regla de inspección de túneles) (tunnel_insp_rule)	Nombre de la regla de inspección de túneles que coincide con el tráfico del túnel de texto sin cifrar.
Remote User IP (IP de usuario remoto) (remote_user_ip)	Dirección IPv4 o IPv6 que utiliza un usuario remoto.

© 2020 Palo Alto Networks, Inc.

Nombre de campo	Description (Descripción)
Remote User ID (ID de usuario remoto) (remote_user_id)	Identidad IMSI de un usuario remoto y, si está disponible, una identidad IMEI o una identidad MSISDN.
UUID for rule (UUID de regla) (rule_uuid)	Identificador único universal de la regla.
ID de captura de paquetes (pcap_id)	Identificador único de captura de paquetes que sirve para buscar el archivo pcap guardado en el cortafuegos.
High Resolution Timestamp (Marca de tiempo de alta resolución) [high_res_timestamp]	Hora en milisegundos a la que se recibió el log en el plano de gestión. El formato de este nuevo campo es YYYY-MM-DDThh:ss:sssTZD: • **YYYY (AAAA)**: año, cuatro dígitos • **MM**: mes, dos dígitos • **DD**: día del mes, dos dígitos (de 01 a 31) • **T (M)**: indicador de inicio de marca de tiempo • **hh**: hora (dos dígitos) mediante la hora de tipo 24 horas (de 00 a 23) • **mm**: minuto, dos dígitos (de 00 a 59) • **ss**: segundo, dos dígitos (de 00 a 60) • **sss**: uno o más dígitos para milisegundos • **TZD (DZN)**: designador de zona horaria (+hh:mm o -hh:mm) *La marca de tiempo de alta resolución es compatible con los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 10.0 y versiones posteriores. Los logs recibidos de los cortafuegos gestionados que ejecutan PAN-OS 9.1 y versiones anteriores muestran una marca de tiempo `1969-12-31T16:00:00:000-8:00` independientemente de cuándo se recibió el log.*

Gravedad de Syslog

La gravedad de Syslog se establece basándose en el tipo de log y el contenido.

Tipo/gravedad de log	Gravedad de Syslog
Tráfico	info
Configurar	info
Amenaza/Sistema: Informativo	info
Amenaza/Sistema: Bajo	Aviso
Amenaza/Sistema: Medio	Warning (Advertencia)

© 2020 Palo Alto Networks, Inc.

Tipo/gravedad de log	Gravedad de Syslog
Amenaza/Sistema: Alto	Warning (Advertencia)
Amenaza/Sistema: Crítico	Crítico

Formato de logs/eventos personalizados

Para facilitar la integración con sistemas de análisis de logs externos, el cortafuegos le permite personalizar el formato de logs; también le permite añadir pares de atributos personalizados *Clave: Pares de atributo* Valor. El formato de los mensajes personalizados puede configurarse en **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Syslog** > **Syslog Server Profile (Perfil de servidor Syslog)** > **Custom Log Format (Formato de log personalizado)**.

Para lograr un formato de log que cumpla con el formato de eventos comunes (CEF) de ArcSight, consulte CEF Configuration Guide (en inglés).

Secuencias de escape

Cualquier campo que contenga una coma o comillas dobles aparecerá entre comillas dobles. Además, si aparecen comillas dobles dentro de un campo, se definirán como carácter de escape anteponiéndoles otras comillas dobles. Para mantener la compatibilidad con versiones anteriores, el campo Varios del log de amenaza siempre aparecerá entre comillas dobles.

© 2020 Palo Alto Networks, Inc.

Monitorización de SNMP y capturas

Los siguientes temas describen cómo los cortafuegos, Panorama y los dispositivos WF-500 de Palo Alto Networks implementan SNMP, y los procedimientos para configurar la supervisión de SNMP y la entrega de capturas.

- Compatibilidad de SNMP
- Active el gestor SNMP para explorar MIB y objetos
- Habilitación de servicios SNMP para elementos de red asegurados por el cortafuegos
- Monitorización de estadísticas mediante SNMP
- Reenvío de capturas a un administrador SNMP
- MIB admitidas

Compatibilidad de SNMP

Puede utilizar el administrador del SNMP para supervisar las alertas activadas por eventos y las estadísticas operativas del cortafuegos, Panorama o el dispositivo WF-500 y para el tráfico que procesan. Las estadísticas y capturas pueden ayudarle a identificar las limitaciones de recursos, cambios o fallos de sistemas, y ataques de malware. Puede configurar alertas mediante el reenvío de datos de log como capturas y permitir el envío de estadísticas en respuesta a mensajes GET (solicitudes) desde su administrador SNMP. Cada captura y estadística tiene un identificador de objeto (OID). Los OID relacionados se organizan jerárquicamente dentro de las bases de información de gestión (MIB) que cargue en el gestor SNMP para habilitar la monitorización.

Cuando un evento desencadena la generación de capturas SNMP (por ejemplo, cuando una interfaz deja de funcionar), el cortafuegos, el dispositivo virtual Panorama, el dispositivo serie M y el dispositivo WF-500 responden mediante la actualización del objeto SNMP correspondiente (por ejemplo, las interfaces MIB) en lugar de esperar la actualización periódica de todos los objetos que se produce cada diez segundos. Esto garantiza que su administrador SNMP muestre la información más reciente al sondear un objeto para confirmar un evento.

El cortafuegos, Panorama y el dispositivo WF-500 admiten SNMP versión 2c y versión 3. Decida cuál usar en función de la versión que otros dispositivos de su red admiten y sus requisitos de seguridad de red. SNMP versión 3 es más seguro y permite un control de acceso más pormenorizado para las estadísticas del sistema que el SNMP versión 2c. La siguiente tabla resume las funciones de seguridad de cada versión. Podrá seleccionar la versión y configurar las funciones de seguridad cuando realice la Supervisión de estadísticas con SNMP y el Reenvío de capturas a un administrador SNMP.

Versión deSNMP	Autenticación	Privacidad del mensaje	Integridad delmensa	Granularidad de acceso a MIB
SNMPv2c	cadena de comunidad	No (cleartext)	No	Acceso a la comunidad SNMP a todas las MIB del dispositivo.
SNMPv3	EngineID, nombre de usuario y contraseña de autenticación (hash SHA para la contraseña)	Contraseña de privacidad para cifrado AES 128 de mensajes SNMP	yes (sí)	Acceso del usuario en función de las vistas que incluyen o excluyen los OID específicos

© 2020 Palo Alto Networks, Inc.

La Implementación de SNMP ilustra una implementación en la cual los cortafuegos reenvían capturas a un administrador SNMP a la vez que reenvían logs a los recopiladores de log. Alternativamente, puede configurar los recopiladores de logs para reenviar las capturas de cortafuegos al gestor SNMP. Para obtener información detallada sobre estas implementaciones, consulte Opciones de reenvío de logs en la creación centralizada de logs e informes. En todas las implementaciones, el administrador SNMP obtiene estadísticas directamente desde el cortafuegos Panorama o el dispositivo WF-500. En este ejemplo, un único administrador SNMP recopila tanto capturas como estadísticas, aunque puede usar administradores distintas para esas funciones si se adapta mejor a su red.

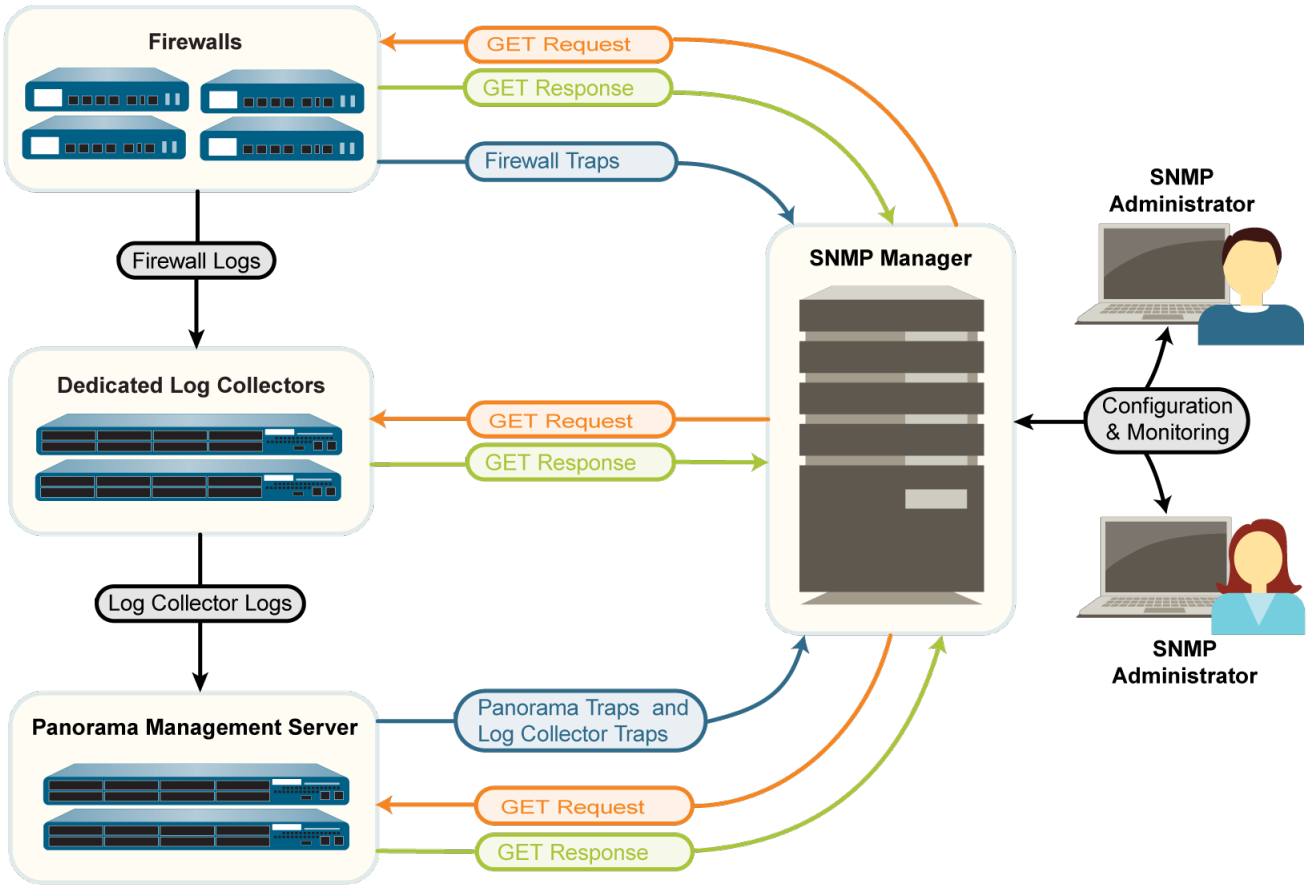


Figure 2: Implementación SNMP

Active el gestor SNMP para explorar MIB y objetos

Para usar SNMP para supervisar cortafuegos, Panorama o dispositivos WF-500 de Palo Alto Networks, primero debe cargar las MIB admitidas en su administrador SNMP y determinar qué identificadores de objeto (object identifiers, OID) corresponden a las estadísticas y capturas del sistema que desea supervisar. Los siguientes temas ofrecen una descripción de cómo encontrar OID y MIB en un administrador SNMP. Para conocer los pasos específicos para realizar esas tareas, consulte su software de gestión SNMP.

- Identificación de una MIB que contiene un OID conocido
- Recorrido por un MIB
- Identificación de OID de estadísticas o capturas de un sistema

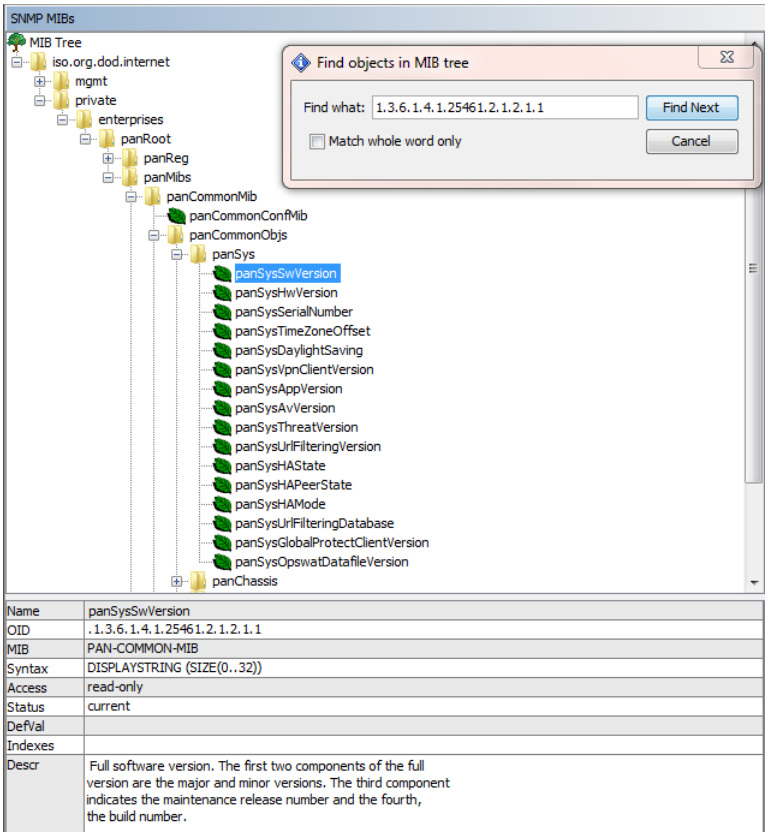
Identificación de una MIB que contiene un OID conocido

Si ya conoce el OID para el objeto SNMP concreto (estadísticas o capturas) y desea conocer los OID de objetos similares para que pueda supervisarlos, puede explorar la MIB que contiene el OID conocido.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Cargue todas las MIB admitidas en su gestor SNMP.

STEP 2 | Busque todo el árbol MIB para el OID conocido. El resultado de la búsqueda muestra la ruta de MIB para el OID, así como la información sobre el OID (por ejemplo, el nombre, estado y descripción). Luego puede seleccionar otros OID en la misma MIB para ver la información sobre ellos.

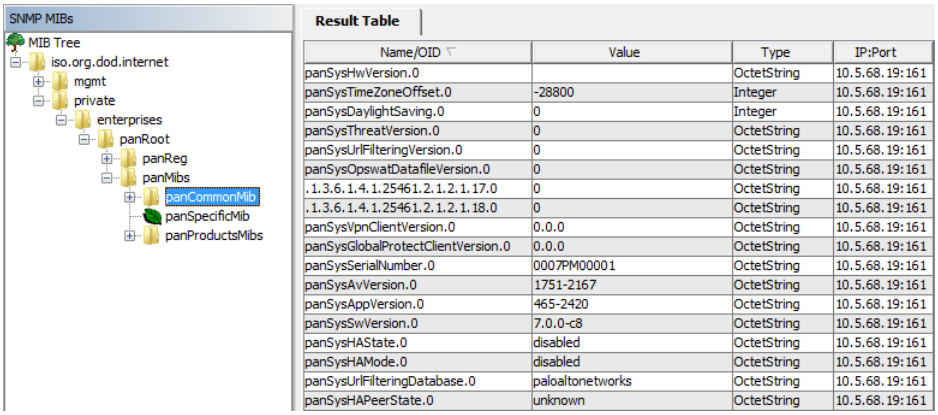


STEP 3 | (Opcional) Realice Recorrido por un MIB para mostrar todos sus objetos.

Recorrido por un MIB

Si desea ver qué objetos SNMP (estadísticas y capturas del sistema) están disponibles para su supervisión, puede que resulte útil mostrar todos los objetos de una MIB concreta. Para ello, cargue las MIB admitidas en su gestor SNMP y realice un *recorrido* por la MIB que desee. Para enumerar las capturas que los cortafuegos, Panorama o dispositivos WF-500 de Palo Alto Networks admiten, recorra la MIB de panCommonEventEventsV2. En el siguiente ejemplo, al recorrer PAN-COMMON-MIB.my se muestra la siguiente lista de OID y sus valores para ciertas estadísticas:

© 2020 Palo Alto Networks, Inc.



Name/OID	Value	Type	IP:Port
panSysHwVersion.0		OctetString	10.5.68.19:161
panSysTimeZoneOffset.0	-28800	Integer	10.5.68.19:161
panSysDaylightSaving.0	0	Integer	10.5.68.19:161
panSysThreatVersion.0	0	OctetString	10.5.68.19:161
panSysUrlFilteringVersion.0	0	OctetString	10.5.68.19:161
panSysOpswatDatafileVersion.0	0	OctetString	10.5.68.19:161
.1.3.6.1.4.1.25461.2.1.2.1.17.0	0	OctetString	10.5.68.19:161
.1.3.6.1.4.1.25461.2.1.2.1.18.0	0	OctetString	10.5.68.19:161
panSysVpnClientVersion.0	0.0.0	OctetString	10.5.68.19:161
panSysGlobalProtectClientVersion.0	0.0.0	OctetString	10.5.68.19:161
panSysSerialNumber.0	0007PM00001	OctetString	10.5.68.19:161
panSysAvVersion.0	1751-2167	OctetString	10.5.68.19:161
panSysAppVersion.0	465-2420	OctetString	10.5.68.19:161
panSysSwVersion.0	7.0.0-c8	OctetString	10.5.68.19:161
panSysHAState.0	disabled	OctetString	10.5.68.19:161
panSysHAMode.0	disabled	OctetString	10.5.68.19:161
panSysUrlFilteringDatabase.0	paloaltonetworks	OctetString	10.5.68.19:161
panSysHAPeerState.0	unknown	OctetString	10.5.68.19:161

Identificación de OID de estadísticas o capturas de un sistema

Para usar un administrador SNMP para supervisar cortafuegos, Panorama o dispositivos WF-500 de Palo Alto Networks, debe conocer los OID de las estadísticas y capturas del sistema que desea supervisar.

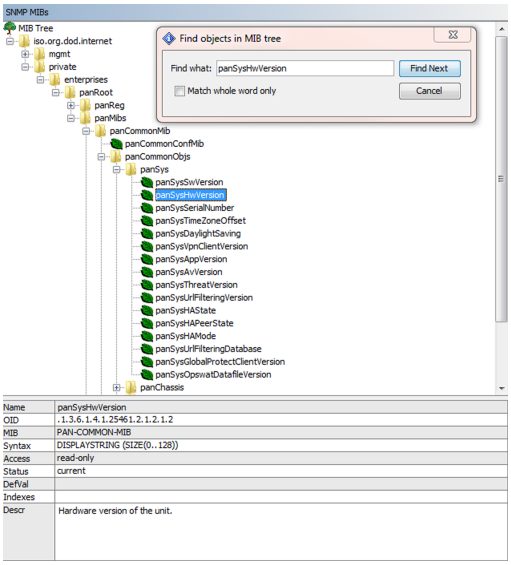
STEP 1 | Revise las MIB compatibles para determinar cuál contiene el tipo de estadística que desea. Por ejemplo, PAN-COMMON-MIB.my contiene información de versión de hardware. La MIB panCommonEventEventsV2 contiene todas las capturas que admiten los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks.

STEP 2 | Abra la MIB en un editor de texto y realice una búsqueda de palabras clave. Por ejemplo, el uso de una **versión de hardware** como cadena de búsqueda en PAN-COMMON-MIB identifica el objeto panSysHwVersion:

```
panSysHwVersion OBJECT-TYPE
 SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Hardware version of the unit."
 ::= {panSys 2}
```

STEP 3 | En una explorador de MIB, busque el árbol de MIB para que el nombre de objeto identificado muestre su OID. Por ejemplo, el objeto panSysHwVersion tiene un OID de 1.3.6.1.4.1.25461.2.1.2.1.2.

© 2020 Palo Alto Networks, Inc.



Habilitación de servicios SNMP para elementos de red asegurados por el cortafuegos

Si va a usar el protocolo simple de administración de redes (SNMP) para monitorizar o gestionar elementos de la red (por ejemplo, conmutadores y enrutadores) que están dentro de las zonas de seguridad de los cortafuegos de Palo Alto Networks, deberá crear una regla de seguridad que permita los servicios SNMP para esos elementos.

No necesita una regla de seguridad para habilitar la supervisión de SNMP de cortafuegos, Panorama o dispositivos WF-500 de Palo Alto Networks. Para obtener más información, consulte Monitorización de estadísticas mediante SNMP.

STEP 1 | Cree un grupo de aplicaciones.

1. Seleccione **Objects (Objetos)** > **Application Group (Grupo de aplicaciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre en **Name** para identificar el grupo de aplicaciones.
3. Haga clic en **Add**, introduzca **snmp** y seleccione **snmp** y **snmp-trap** en el menú desplegable.
4. Haga clic en **OK (Aceptar)** para guardar el grupo de aplicaciones.

STEP 2 | Cree una regla de seguridad para permitir los dispositivos SNMP.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un nombre en **Name** para la regla.
3. En las pestañas **Source (Origen)** y **Destination (Destino)**, haga clic en **Add (Añadir)** e introduzca una zona de origen en **Source Zone (Zona de origen)** y una zona de destino en **Destination Zone (Zona de destino)** para el tráfico.
4. En la pestaña **Applications (Aplicaciones)**, haga clic en **Add (Añadir)**, introduzca el nombre del grupo de aplicaciones que acaba de crear y selecciónelo en el menú desplegable.
5. En la pestaña **Actions**, compruebe que **Action** esté configurada en **Allow** y haga clic en **OK** y después en **Commit**.

© 2020 Palo Alto Networks, Inc.

Monitorización de estadísticas mediante SNMP

Las estadísticas que recoge un administrador de protocolo simple de administración de redes (Simple Network Management Protocol, SNMP) de los cortafuegos de Palo Alto Networks pueden ayudar a medir el estado de su red (dispositivos y conexiones), identificar las limitaciones de los recursos y supervisar el tráfico o procesar las cargas. Estas estadísticas incluyen información como los estados de la interfaz (activa o caída), las sesiones de usuarios activas, las sesiones simultáneas, el uso de sesiones, la temperatura y el tiempo de funcionamiento del sistema.

No puede configurar un administrador SNMP para que controle los cortafuegos de Palo Alto Networks (mediante mensajes SET), solo para recopilar estadísticas de ellos (mediante mensajes GET). Si desea información detallada sobre cómo se implementa el SNMP en los cortafuegos de Palo Alto Networks, consulte Asistencia de SNMP*.*

STEP 1 | Puede configurar un administrador SNMP para recibir estadísticas de los cortafuegos.

Los siguientes pasos ofrecen una descripción de las tareas que realiza en el administrador SNMP. Para ver los pasos específicos, consulte la documentación de su gestor SNMP.

1. Para habilitar el gestor SNMP para que interprete las estadísticas del cortafuegos, cargue los MIB compatibles para cortafuegos de Palo Alto Networks y, si es necesario, realice una compilación de ellos.
2. Para cada cortafuegos que vaya a supervisar el administrador SNMP, defina los ajustes de conexión (dirección IP y puerto) y los ajustes de autenticación (cadena de comunidad SNMP 2c o ID de motor/nombre de usuario/contraseña de SNMP 3) para el cortafuegos.

   Los cortafuegos de Palo Alto Networks usan el puerto 161.

   El administrador SNMP puede usar la misma conexión o una diferente, y los mismos ajustes de autenticación o diferentes para múltiples cortafuegos. Los ajustes deben coincidir con los que usted definió al configurar el SNMP en el cortafuegos (consulte el paso 3). Por ejemplo, si usa SNMPv2c, la cadena de comunidad que define al configurar el cortafuegos debe coincidir con la cadena de comunidad que defina en el administrador SNMP de ese cortafuegos.
3. Determine los identificadores de objeto (OID) de las estadísticas que desea monitorizar. Por ejemplo, para monitorizar el porcentaje de utilización de la sesión de un cortafuegos, un explorador MIB muestra que esta estadística corresponde con el OID 1.3.6.1.4.1.25461.2.1.2.3.1.0 en PAN-COMMON-MIB.my. Para obtener más detalles, consulte Cómo usar un gestor SNMP para explorar MIB y objetos.
4. Configure el gestor SNMP para monitorizar los OID deseados.

STEP 2 | Habilite el tráfico de SNMP en una interfaz de cortafuegos.

Esta es la interfaz que recibirá las solicitudes de estadísticas desde el gestor SNMP.

PAN-OS no sincroniza los ajustes de interfaz de gestión (MGT) para cortafuegos en una configuración de alta disponibilidad (high availability, HA). Debe configurar la interfaz para cada par de HA.

Realice este paso en la interfaz web del cortafuegos.

- Para habilitar el tráfico SNMP en la interfaz MGT, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Interfaces**, modifique la interfaz **Management (Gestión)**, seleccione **SNMP** y luego haga clic en **OK (Aceptar)** y **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

- Para habilitar el tráfico SNMP en cualquier otra interfaz, cree un perfil de gestión de interfaz para los servicios SNMP y asigne el perfil a la interfaz que recibirá las solicitudes SNMP. El tipo de interfaz debe ser Ethernet de capa 3.

STEP 3 | Configure el cortafuegos para responder a las solicitudes de estadísticas desde un administrador SNMP.

PAN-OS no sincroniza los ajustes de respuesta SNMP para cortafuegos en una configuración de alta disponibilidad (high availability, HA). Debe configurar esos ajustes para cada par de HA.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y, en la sección Miscellaneous (Varios), haga clic en **SNMP Setup (Configuración de SNMP)**.
2. Seleccione la **Version** de SNMP y configure los valores de autenticación del siguiente modo. Para obtener más detalles, consulte a la asistencia de SNMP.
   - **V2c**: introduzca la **SNMP Community String**, que identifica a una comunidad de administradores SNMP y dispositivos supervisados, además de servir como contraseña para autenticar a los miembros de la comunidad entre sí.

     Se recomienda no usar la cadena de comunidad ***`pública`*** *predeterminada; es bien conocida, y por ello no es segura.*
   - **V3**: cree al menos un grupo de vistas SNMP y un usuario. Las cuentas y vistas de usuario proporcionan autenticación, privacidad y control de acceso cuando los cortafuegos reenvían capturas y los administradores SNMP obtienen estadísticas de cortafuegos.
     - Vistas: cada vista es un Identificador de objeto (object identifier, OID) emparejado y una máscara binaria: el OID especifica un MIB y la máscara (en formato hexadecimal) especifica qué objetos son accesibles dentro (incluir coincidencias) o fuera (excluir coincidencias) del MIB. Haga clic en **Add (Añadir)** en la primera lista e introduzca un **Name (Nombre)** para el grupo de vistas. En cada vista del grupo, haga clic en **Add (Añadir)** y configure los campos **Name (Nombre)**, **OID (Identificador de objeto)**, **Option (Opción)** coincidente (**include [incluir]** o **exclude [excluir]**) y **Mask (Máscara)** de la vista.
     - Haga clic en **Add (Añadir)** en la segunda lista, introduzca un nombre de usuario en **Users (Usuarios)**, seleccione el grupo **View (Ver)** en la lista desplegable, escriba la contraseña de autenticación (**Auth Password**) que se usa para autenticar al administrador SNMP y escriba la contraseña de privacidad (**Priv Password**) que se usa para cifrar los mensajes SNMP al administrador SNMP.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 4 | Supervise las estadísticas del cortafuegos en un gestor SNMP.

Consulte la documentación de su gestor SNMP para obtener más detalles.

Cuando supervise las estadísticas relacionadas a las interfaces del cortafuegos, debe comparar los índices de interfaz del gestor SNMP con los nombres de interfaz de la interfaz web del cortafuegos. Si desea información detallada, consulte Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow.

Reenvío de capturas a un administrador SNMP

Las capturas del protocolo simple de administración de redes (Simple Network Management Protocol, SNMP) pueden alertarle sobre eventos del sistema (fallos o cambios del hardware o software de los cortafuegos de Palo Alto Networks) o sobre amenazas (tráfico que coincide con una regla de seguridad del cortafuegos) que requieren atención inmediata.

© 2020 Palo Alto Networks, Inc.

Para ver la lista de capturas que los dispositivos de Palo Alto Networks admiten, use su administrador SNMP para acceder a la MIB panCommonEventEventsV2. Para obtener más detalles, consulte Cómo usar un gestor SNMP para explorar MIB y objetos.

Para obtener información detallada sobre cómo los cortafuegos de Palo Alto Networks implementan el SNMP, consulte SNMP Support (Asistencia de SNMP).

STEP 1 | Habilite el gestor SNMP para que interprete las capturas que recibe.

Cargue los MIB compatibles para los cortafuegos de Palo Alto Networks y, si es necesario, confírmelos. Para ver los pasos específicos, consulte la documentación de su gestor SNMP.

STEP 2 | Configure un perfil de servidor trap SNMP.

El perfil define la forma en que el cortafuegos accede a los administradores SNMP (servidores de capturas). Puede definir hasta cuatro gestores de SNMP para cada perfil.

Otra opción es configurar distintos perfiles de servidor de capturas de SNMP para diferentes tipos de logs, niveles de gravedad y veredictos de WildFire.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SNMP Trap (Trampa SNMP)**.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para el perfil.
4. Si el cortafuegos tiene más de un sistema virtual (vsys), seleccione la **Location (Ubicación)** (vsys o **Shared [Compartido]**) en la que el perfil está disponible.
5. Seleccione la **Version** de SNMP y configure los valores de autenticación del siguiente modo. Para obtener más detalles, consulte a la asistencia de SNMP.
   - **V2c**: en cada servidor, haga clic en **Add (Añadir)** y escriba el nombre del servidor en **Name (Nombre)**, la dirección IP (**SNMP Manager [Gestor SNMP]**) y la **Community String (Cadena de comunidad)**. La cadena de comunidad que identifica a una comunidad de administradores SNMP y dispositivos monitorizados, además de servir como contraseña para autenticar a los miembros de la comunidad entre sí.

     Se recomienda no usar la cadena de comunidad ***`pública`*** *predeterminada; es bien conocida, y por ello no es segura.*
   - **V3**: para cada servidor, haga clic en **Add** y escriba el nombre del servidor en **Name**, dirección IP (**SNMP Manager**), cuenta de usuario SNMP en **User** (que debe coincidir con un nombre de usuario definido en el administrador SNMP), el **EngineID** usado para identificar de forma única el cortafuegos (puede dejar el campo en blanco para usar el número de serie del cortafuegos), la contraseña de autenticación (**Auth Password**) usada para autenticar el servidor y la contraseña de privacidad (**Priv Password**) usada para cifrar los mensajes SNMP al servidor.
6. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 3 | Configure el reenvío de logs.

1. Configure los destinos de las capturas de WildFire, tráfico y amenaza:
   1. Cree un perfil de reenvío de logs. Para cada tipo de log y nivel de gravedad o veredicto de WildFire, seleccione el perfil del servidor de la **captura de SNMP**.
   2. Asigne el perfil de reenvío de logs a las reglas de política y zonas de red. Las reglas y las zonas activarán el reenvío y la generación de capturas.

© 2020 Palo Alto Networks, Inc.

2. Configure los destinos de los logs de sistema, configuración, ID de usuario, coincidencias HIP y correlación. Para cada tipo de log (captura) y nivel de gravedad, seleccione el perfil del servidor de **captura de SNMP**.
3. Haga clic en **Commit (Confirmar)**.

STEP 4 | Supervise las capturas de un gestor SNMP.

Consulte la documentación de su gestor SNMP.

Cuando supervise las estadísticas relacionadas con las interfaces del cortafuegos, debe comparar los índices de interfaz del gestor SNMP con los nombres de interfaz de la interfaz web del cortafuegos. Si desea información detallada, consulte Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow.

MIB admitidas

La tabla siguiente muestra las bases de información de gestión (management information bases, MIB) del Protocolo simple de administración de redes (Simple Network Management Protocol, SNMP) que admiten los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks. Debe cargar esas MIB en su administrador SNMP para monitorizar los objetos (estadísticas y capturas del sistema) que se han definido en las MIB. Para obtener más detalles, consulte Cómo usar un gestor SNMP para explorar MIB y objetos.

Tipo de MIB	MIB admitidas
Estándar: El Grupo de Trabajo de Ingeniería de Internet (IETF) mantiene la mayoría de MIB estándar. Puede descargar las MIB desde el sitio web de IETF. *Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks no admiten todos los objetos (OID) de todas esas MIB. Consulte los enlaces de MIB admitidas para obtener una descripción general de los OID admitidos.*	MIB-II IF-MIB HOST-RESOURCES-MIB ENTITY-MIB ENTITY-SENSOR-MIB ENTITY-STATE-MIB IEEE 802.3 LAG MIB LLDP-V2-MIB.my BFD-STD-MIB
Empresa: puede descargar las MIB de empresa desde el portal de Documentación técnica de Palo Alto Networks.	PAN-COMMON-MIB.my PAN-GLOBAL-REG-MIB.my PAN-GLOBAL-TC-MIB.my

© 2020 Palo Alto Networks, Inc.

Tipo de MIB	MIB admitidas
	PAN-LC-MIB.my PAN-PRODUCT-MIB.my PAN-ENTITY-EXT-MIB.my PAN-TRAPS.my

MIB-II

MIB-II proporciona identificadores de objetos (OID) para protocolos de gestión de red en redes basadas en TCP/IP. Use esta MIB para supervisar información general sobre sistemas e interfaces. Por ejemplo, puede analizar tendencias de uso de ancho de banda ancha por tipo de interfaz (objeto ifType) para determinar si el cortafuegos necesita más interfaces de ese tipo para acomodar los picos de volumen del tráfico.

Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks solo admiten los siguientes grupos de objetos:

Grupo de objetos	Description (Descripción)
system	Ofrece información de sistema, como el modelo de hardware, tiempo de funcionamiento del sistema, FQDN y ubicación física.
interfaces	Ofrece estadísticas para interfaces físicas y lógicas como tipo, ancho de banda actual (velocidad), estado operativo (por ejemplo, activo o inactivo) y paquetes descartados. La interfaz lógica admite, entre otros, túneles VPN, grupos de agregación, subinterfaces de capa 2, subinterfaces de capa 3, interfaces de loopback e interfaces VLAN.

RFC 1213 define esta MIB.

IF-MIB

IF-MIB admite más tipos de interfaz (física y lógica) y contadores más grandes (64K) de los definidos en MIB-II. Use esta MIB para estadísticas de interfaz más allá de las que proporciona MIB-II. Por ejemplo, para monitorizar el ancho de banda actual de interfaces de alta velocidad (mayor que 2,2 Gps) como las interfaces 10G de los cortafuegos PA-5200 Series, debe comprobar el objeto ifHighSpeed de IF-MIB en lugar del objeto ifSpeed de MIB-II. Las estadísticas IF-MIB pueden ser útiles para evaluar la capacidad de su red.

Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks solo admiten la ifXTable en IF-MIB, lo que ofrece información de interfaz, como el número de paquetes de multidifusión y difusión que se transmiten y reciben, si la interfaz está en modo promiscuo o si tiene un conector físico.

RFC 2863 define esta MIB.

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB ofrece información sobre los recursos del ordenador host. Use esta MIB para supervisar las estadísticas de uso de memoria y CPU. Por ejemplo, si consulta la carga actual de la CPU (objeto hrProcessorLoad) puede solucionar problemas de rendimiento del cortafuegos.

Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks admiten partes de los siguientes grupos de objetos:

© 2020 Palo Alto Networks, Inc.

Grupo de objetos	Description (Descripción)
hrDevice	Ofrece información como la carga de la CPU, la capacidad de almacenamiento y el tamaño de la partición. Los OID de hrProcessorLoad ofrecen una media de los núcleos que procesan paquetes. Para los cortafuegos PA-7000 y PA-5200 Series, que tienen varios planos de datos (DP, Dataplanes), puede supervisar la utilización del procesador del plano de datos individual. Configure alertas cuando la utilización alcance un umbral específico para cada procesador DP para evitar problemas de disponibilidad del servicio.
hrSystem	Ofrece información como el tiempo de funcionamiento del sistema, el número de sesiones de usuario y de procesos actuales.
hrStorage	Ofrece información como la cantidad de almacenamiento usada.

RFC 2790 define esta MIB.

ENTITY-MIB

ENTITY-MIB ofrece OID para múltiples componentes físicos y lógicos. Use esta MIB para determinar qué componentes físicos se cargan en un sistema (por ejemplo, sensores de temperatura y de los ventiladores) y ver información relacionada como los modelos y números de serie. También puede utilizar los números de índice para que estos componentes determinen su estado operativo en ENTITY-SENSOR-MIB y ENTITY-STATE-MIB.

Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks solo admiten partes del grupo entPhysicalTable:

Object (Objeto)	Description (Descripción)
entPhysicalIndex	Nombre de espacio único que incluye ranuras y unidades de disco.
entPhysicalDescr	La descripción del componente.
entPhysicalVendorType	El sysObjectID (consulte PAN-PRODUCT-MIB.my) cuando está disponible (objetos de bastidor y módulo).
entPhysicalContainedIn	El valor de entPhysicalIndex para el componente que contiene este componente.
entPhysicalClass	Bastidor (3), contenedor (5) para una ranura, suministro de alimentación (6), ventilador (7), sensor (8) para cada temperatura u otros aspectos ambientales y módulo (9) para cada tarjeta de línea.
entPhysicalParentRelPos	La posición relativa de este componente *secundario* está entre sus componentes *iguales*. Los componentes hermanos se definen como componentes entPhysicalEntry que comparten los mismos valores de instancia de cada uno de los objetos entPhysicalContainedIn y entPhysicalClass.

© 2020 Palo Alto Networks, Inc.

Object (Objeto)	Description (Descripción)
entPhysicalName	Solo es compatible si la interfaz de gestión (MGT) permite dar nombre a la tarjeta de línea.
entPhysicalHardwareRev	La revisión de hardware específica del proveedor del componente.
entPhysicalFirwareRev	La revisión de firmware específica del proveedor del componente.
entPhysicalSoftwareRev	La revisión de software específica del proveedor del componente.
entPhysicalSerialNum	El número de serie específico del proveedor del componente.
entPhysicalMfgName	El número del fabricante del componente.
entPhysicalMfgDate	La fecha en la que se fabricó el componente.
entPhysicalModelName	El número de modelo del disco.
entPhysicalAlias	Un alias del gestor de red especificado para el componente.
entPhysicalAssetID	Un identificador de monitorización del activo asignado por el usuario que el gestor de red especificó para el componente.
entPhysicalIsFRU	Indica si el componente es una unidad reemplazable en la instalación (FRU).
entPhysicalUris	El número de identificador del equipo de lenguaje común (CLEI) del componente (por ejemplo, URN:CLEI:CNME120ARA).

RFC 4133 define esta MIB.

ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB añade compatibilidad con los sensores físicos de equipos de red más allá de lo que define la ENTITY-MIB. Use esta MIB junto con ENTITY-MIB para supervisar el estado operativo de los componentes físicos de un sistema (por ejemplo, los sensores de temperatura y de los ventiladores). Por ejemplo, para solucionar problemas que pueden derivar de las condiciones ambientales, puede asignar los índices de entidad desde la ENTITY-MIB (objeto entPhysicalDescr) para valores de estado operativo (objeto entPhysSensorOperStatus) en la ENTITY-SENSOR-MIB. En el siguiente ejemplo, todos los sensores de temperatura y ventiladores de un cortafuegos PA-3020 están funcionando:

Name/OID	Value
entPhysicalDescr.1	PA-3020
entPhysicalDescr.2	Fan #1 RPM
entPhysicalDescr.3	Fan #2 RPM
entPhysicalDescr.4	Fan #3 RPM
entPhysicalDescr.5	Fan #4 RPM
entPhysicalDescr.6	Temperature @ Ocelot
entPhysicalDescr.7	Temperature @ Switch
entPhysicalDescr.8	Temperature @ Cavium
entPhysicalDescr.9	Temperature @ Intel PHY
entPhysicalDescr.10	Temperature @ Switch Core
entPhysicalDescr.11	Temperature @ Cavium Core
entPhySensorOperStatus.2	ok (1)
entPhySensorOperStatus.3	ok (1)
entPhySensorOperStatus.4	ok (1)
entPhySensorOperStatus.5	ok (1)
entPhySensorOperStatus.6	ok (1)
entPhySensorOperStatus.7	ok (1)
entPhySensorOperStatus.8	ok (1)
entPhySensorOperStatus.9	ok (1)
entPhySensorOperStatus.10	ok (1)
entPhySensorOperStatus.11	ok (1)

© 2020 Palo Alto Networks, Inc.

El mismo OID puede referirse a diferentes sensores en una plataforma diferente. Use la ENTITY-MIB para la plataforma de destino para que la plataforma de destino compare el valor con la descripción.

Los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks solo admiten partes del grupo entPhySensorTable. Las partes admitidas varían según la plataforma e incluyen solo los sensores térmicos (temperatura en Celsius) y de los ventiladores (RPM).

RFC 3433 define la ENTITY-SENSOR-MIB.

ENTITY-STATE-MIB

ENTITY-STATE-MIB ofrece información sobre el estado de los componentes físicos más allá de lo que define la ENTITY-MIB, incluido el estado administrativo y operativo de componentes en las plataformas basadas en bastidor. Use esta MIB junto con ENTITY-MIB para monitorizar el estado operativo de los componentes físicos de un cortafuegos PA-7000 Series (por ejemplo, tarjetas de línea, bandejas de ventilador y fuentes de alimentación). Por ejemplo, para solucionar problemas de reenvío de logs de logs de amenazas, puede asignar los índices de (LPC) de tarjeta de procesamiento de logs desde la ENTITY-MIB (objeto entPhysicalDescr) a los valores de estado operativo (objeto entStateOper) en la ENTITY-SENSOR-MIB. Los valores de estado operativo usan números para indicar el estado: 1 para desconocido, 2 para deshabilitado, 3 para habilitado y 4 para pruebas. El cortafuegos de la serie PA-7000 es el único cortafuegos de Palo Alto Networks que admite esta MIB.

RFC 4268 defina la ENTITY-STATE-MIB.

IEEE 802.3 LAG MIB

Use la MIB IEEE 802.3 LAG para monitorizar el estado de grupos agregados que tengan habilitado el protocolo de control de adición de enlaces (ECMP). Cuando el cortafuegos registra eventos LACP, también genera capturas que son útiles para la resolución de problemas. Por ejemplo, las capturas pueden indicarle si las interrupciones de tráfico entre el cortafuegos y un peer LACP desde la conectividad perdida o desde una velocidad de interfaz no comparada y valores duplicados.

PAN-OS implementa las siguientes tablas SNMP para LACP.

El objeto dot3adTablesLastChanged indica la hora del cambio más reciente en dot3adAggTable, dot3adAggPortListTable y dot3adAggPortTable.

Tabla	Description (Descripción)
Tabla de configuración de agregador (dot3adAggTable)	Esta tabla contiene información sobre cada grupo de agregación que se asocia con un cortafuegos. Cada grupo de agregación tiene una entrada. Algunos objetos de tabla tienen restricciones, que describe el objeto dot3adAggIndex. Este índice es el identificador único que el sistema local asigna al grupo de agregación. Identifica una instancia de grupo de agregación entre los objetos gestionados subordinados del objeto contenido. El identificador es de solo lectura. *La MIB ifTable (una lista de entradas de interfaz) no admite interfaces lógicas y por ello no tiene una entrada para el grupo de agregación.*

© 2020 Palo Alto Networks, Inc.

Tabla	Description (Descripción)
Tabla de lista de puerto de agregación (dot3adAggPortListTable)	Esta tabla enumera los puertos asociados con cada grupo de agregación en un cortafuegos. Cada grupo de agregación tiene una entrada. El atributo dot3adAggPortListPorts enumera el conjunto completo de puertos asociados con un grupo de agregación. Cada bit definido en la lista representa un miembro de puerto. Para las plataformas no basados en bastidor, este es un valor de 64 bits. Para plataformas de bastidor, el valor es una matriz de ocho entradas de 64 bits.
Tabla de puerto de agregación (dot3adAggPortTable)	Esta tabla contiene información de configuración LACP sobre cada puerto asociado con un grupo de agregación en un cortafuegos. Cada puerto tiene una entrada. La tabla no tiene entradas para puertos que no están asociados con un grupo de agregación.
Tabla de estadística de LACP (dot3adAggPortStatsTable)	Esta tabla contiene información de agregación de enlaces sobre cada puerto asociado con un grupo de agregación en un cortafuegos. Cada puerto tiene una fila. La tabla no tiene entradas para puertos que no están asociados con un grupo de agregación.

La MIB IEEE 802.3 LAG incluye las siguientes capturas relacionadas con LACP:

Nombre de captura	Description (Descripción)
panLACPLostConnectivityTrap	El peer perdió conectividad con el cortafuegos.
panLACPUnresponsiveTrap	El peer no responde al cortafuegos.
panLACPNegoFailTrap	La negociación LACP con el peer ha fallado.
panLACPSpeedDuplexTrap	Los ajustes dúplex y la velocidad de enlace en el cortafuegos y el peer no coinciden.
panLACPLinkDownTrap	Una interfaz del grupo de agregación se ha desactivado.
panLACPLacpDownTrap	Una interfaz se retiró del grupo de agregación.
panLACPLacpUpTrap	Una interfaz se añadió al grupo de agregación.

Para las definiciones de MIB, consulte la MIB IEEE 802.3 LAG.

LLDP-V2-MIB.my

Use el LLDP-V2-MIB para supervisar los eventos de protocolo de detección de nivel de enlace (LLDP). Por ejemplo, puede consultar el objeto lldpV2StatsRxPortFramesDiscardedTotal para ver el número de tramas LLDP que se descartaron por cualquier razón. El cortafuegos de Palo Alto Networks usa LLDP para descubrir dispositivos vecinos y sus funcionalidades. LLDP facilita la solución de problemas, especialmente para las implementaciones de Virtual Wire donde las utilidades de ping o tracerout no detecta el cortafuegos.

Los cortafuegos de Palo Alto Networks admiten todos los objetos LLDP-V2-MIB excepto:

© 2020 Palo Alto Networks, Inc.

- Los siguientes objetos lldpV2Statistics:
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- The following lldpV2RemoteSystemsData objects:
  - La tabla lldpV2RemOrgDefInfoTable
  - En la tabla lldpV2RemTable: lldpV2RemTimeMark

RFC 4957 define esta MIB.

BFD-STD-MIB

Use la MIB de detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) para supervisar y recibir alertas de fallos para la ruta bidireccional entre dos motores de reenvío, tal como interfaces, enlaces de datos o los motores en sí. Por ejemplo, puede comprobar el objeto bfdSessState para ver el estado de una sesión BFD entre motores de reenvío. En la implementación de Palo Alto Networks, uno de los motores de reenvío es una interfaz en el cortafuegos y el otro es un peer BFD adyacente configurado.

RFC 7331 define esta MIB.

PAN-COMMON-MIB.my

Utilice PAN-COMMON-MIB para supervisar la siguiente información para los cortafuegos, Panorama y dispositivos WF-500 de Palo Alto Networks:

Grupo de objetos	Description (Descripción)
panSys	Contiene objetos como versiones de software/hardware de sistema, versiones de contenido dinámico, número de serie, estado/modo de HA y contadores globales. Los contadores globales incluyen los relacionados con la denegación de servicio (DoS), fragmentación de IP, estado de TCP y paquetes descartados. El seguimiento de estos contadores le permite supervisar las irregularidades de tráfico que derivan de los ataques DoS, fallos de conexión o sistema, o limitaciones de recursos. PAN-COMMON-MIB admite contadores globales para cortafuegos pero no para Panorama.
panChassis	Tipo de bastidor y modo de dispositivo M-Series (recopilador de logs o Panorama).
panSession	Información de utilización de sesión. Por ejemplo, el número total de sesiones activas en el cortafuegos o un sistema virtual específico.
panMgmt	Estado de la conexión desde el cortafuegos al servidor de gestión de Panorama.
panGlobalProtect	Uso del gateway GlobalProtect como un porcentaje, máximo de túneles permitidos y número de túneles activos.
panLogCollector	Estadísticas de creación de logs de cada recopilador de logs, que incluyen la tasa de creación de logs, las cuotas de logs, el uso del disco, los períodos

© 2020 Palo Alto Networks, Inc.

Grupo de objetos	Description (Descripción)
	de conservación, la redundancia de los logs (habilitado o deshabilitado), el estado de reenvío de los cortafuegos a los recopiladores de logs, el estado de reenvío de los recopiladores de logs a los servicios externos, y el estado de las conexiones entre el cortafuegos y el recopilador de logs.
panDeviceLogging	Estadísticas de creación de logs de cada cortafuegos, que incluyen la tasa de creación de logs, el uso del disco, los períodos de conservación, el estado de reenvío de los cortafuegos individuales a Panorama y servidores externos, y el estado de las conexiones entre el cortafuegos y el recopilador de logs.

PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my contiene definiciones de OID global de máximo nivel para varios subárboles de módulo MIB de empresa de Palo Alto Networks. Esta MIB no contiene objetos para que los supervise; solo es necesaria para que hagan referencia a ella otras MIB.

PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my define convenciones (por ejemplo, la longitud de caracteres y caracteres admitidos) para los valores de texto de objetos en módulos MIB de empresa de Palo Alto Networks. Todos los productos de Palo Alto Networks sigue estas convenciones. Esta MIB no contiene objetos para que los supervise; solo es necesaria para que hagan referencia a ella otras MIB.

PAN-LC-MIB.my

PAN-LC-MIB.my contiene definiciones de objetos gestionados que implementan los recopiladores de logs (dispositivos M-Series en un modo de recopilador de logs). Use esta MIB para monitorizar la tasa de logging, la duración de almacenamiento de base de datos de logs (en días) y uso de disco (en MB) de cada disco lógico (hasta cuatro) en un recopilador de logs. Por ejemplo, puede usar esta información para determinar si debe añadir más recopiladores de logs o reenviar logs a un servidor externo (por ejemplo, un servidor de syslog) para el archivado.

PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my define OID de sysObjectID para todos los productos de Palo Alto Networks. Esta MIB no contiene objetos para que los supervise; solo es necesaria para que hagan referencia a ella otras MIB.

PAN-ENTITY-EXT-MIB.my

Use PAN-ENTITY-EXT-MIB.my en conjunto con ENTITY-MIB para supervisar el uso de la alimentación para componentes físicos de un cortafuegos dela serie PA-7000 (por ejemplo, bandejas de ventilador y fuentes de alimentación), que es el único cortafuegos de Palo Alto Networks que admite esta MIB. Por ejemplo, para solucionar problemas de reenvío de logs, puede querer comprobar el uso de alimentación de las tarjetas de procesamiento de logs (LPC): puede asignar los índices LPC desde ENTITY-MIB (objeto entPhysicalDescr) a valores en PAN-ENTITY-EXT-MIB (objeto panEntryFRUModelPowerUsed).

PAN-TRAPS.my

Use PAN-TRAPS.my para ver una lista completa de todas las capturas generadas e información sobre ellas (por ejemplo, una descripción). Para acceder a una lista de trampas que admiten los cortafuegos, Panorama y los dispositivos WF-500 de Palo Alto Networks, consulte el objeto PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2**.

© 2020 Palo Alto Networks, Inc.

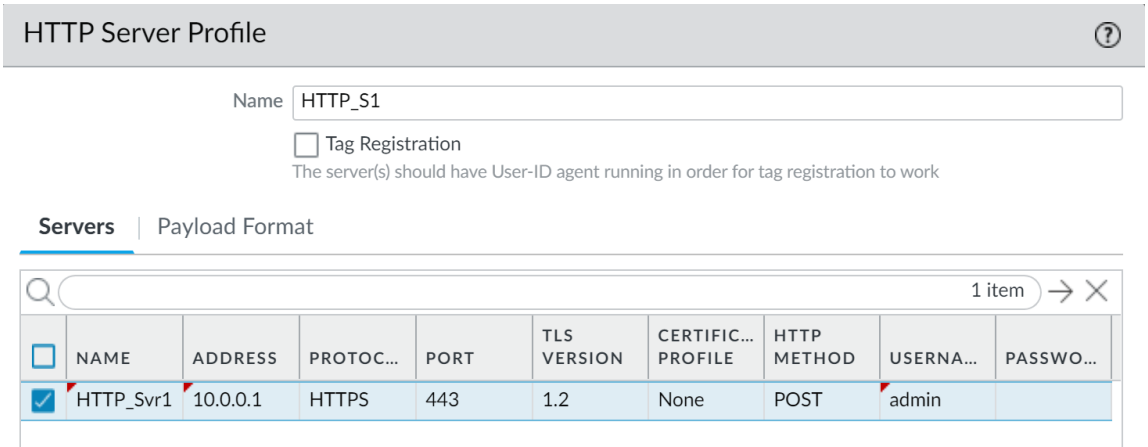
Reenvío de logs a un destino de HTTP/S

El cortafuegos y Panorama™ pueden enviar logs a un servidor HTTP/S. Puede optar por reenviar todos los logs o reenviar logs específicos para activar una acción en un servicio externo basado en HTTP cuando se produce un evento. Cuando reenvíe logs a un servidor HTTP, configure el cortafuegos para que envíe una solicitud API basada en HTTP directamente a un servicio externo a fin de activar una acción basada en los atributos en un log de cortafuegos. Puede configurar el cortafuegos para que funcione con cualquier servicio basado en HTTP que exponga una API y modificar la URL, el encabezado HTTP, los parámetros y la carga útil en la solicitud HTTP para satisfacer sus necesidades de integración.

STEP 1 | Cree un perfil de servidor HTTP para enviar logs a un destino HTTP/S.

El perfil de servidor HTTP le permite especificar de qué manera acceder al servidor y definir el formato en el cual enviar logs al destino HTTP/S. De manera predeterminada, el cortafuegos utiliza el puerto de gestión para enviar estos logs. Sin embargo, puede asignar una interfaz de origen y una dirección IP diferente en **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de ruta de servicio)**.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **HTTP** y, luego, **añada** un nuevo perfil.
2. Especifique un **nombre** para el perfil de servidor y seleccione la **ubicación**. El perfil puede ser **Shared (Compartido)**entre todos los sistemas virtuales o aplicado a un sistema virtual específico.
3. **Añada** los detalles de cada servidor. Cada perfil puede tener un máximo de cuatro servidores.
4. Introduzca un **Name (Nombre)** y una **Address (Dirección)** IP.
5. Seleccione el **protocolo** (**HTTP** o **HTTPS**). El **puerto** predeterminado es 80 o 443, respectivamente, pero puede modificar el número de puerto para que coincida con el puerto en el que escucha su servidor HTTP.
6. Seleccione la **versión de TLS** admitida en el servidor: **1.0**, **1.1** o **1.2** (predeterminada).
7. En **Certificate Profile (Perfil de certificados)**, seleccione el certificado que se debe usar para la conexión TLS al servidor.
8. Seleccione el **método HTTP** que admite el servicio externo: **`DELETE`**,**`GET`**, **`POST`** (predeterminado) o **`PUT`**.
9. (Opcional) Especifique el **nombre de usuario** y **contraseña** para autenticar el servidor, si fuera necesario.
10. (Opcional) Seleccione **Test Server Connection (Comprobar la conexión del servidor)** para verificar la conectividad de red entre el cortafuegos y el servidor HTTP/S.

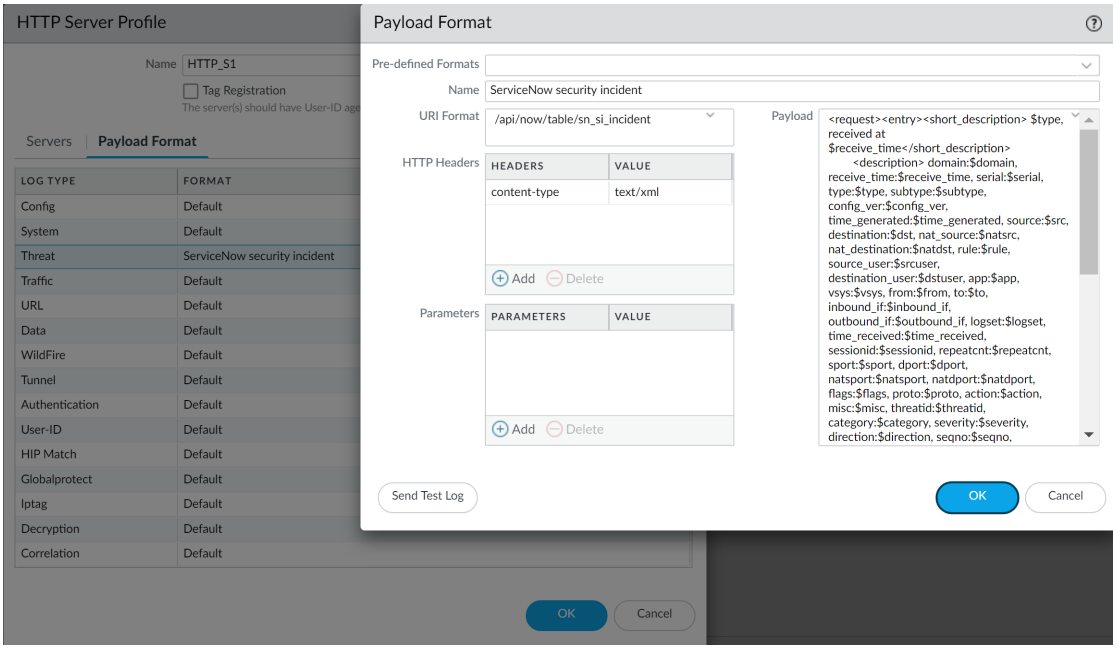


STEP 2 | Seleccione el **Payload Format (Formato de carga útil)** para la solicitud HTTP.

© 2020 Palo Alto Networks, Inc.

1. Seleccione el enlace de **Log Type (Tipo de Log)** para cada tipo de log para el cual desee definir el formato de solicitud HTTP.
2. Seleccione**Pre-defined Formats (Formatos predefinidos)** (disponibles a través de actualizaciones de contenido) o cree un formato personalizado.

   Si crea un formato personalizado, **URI** es el endpoint del recurso en el servicio HTTP. El cortafuegos agrega el URI a la dirección IP que definió anteriormente para construir la URL para la solicitud HTTP. Asegúrese de que el formato de URL y de carga útil coincida con la sintaxis que su proveedor externo requiere. Puede utilizar cualquier atributo admitido en el tipo de log seleccionado dentro de los pares de encabezado, parámetro y valor de HTTP, y la carga útil de la solicitud.

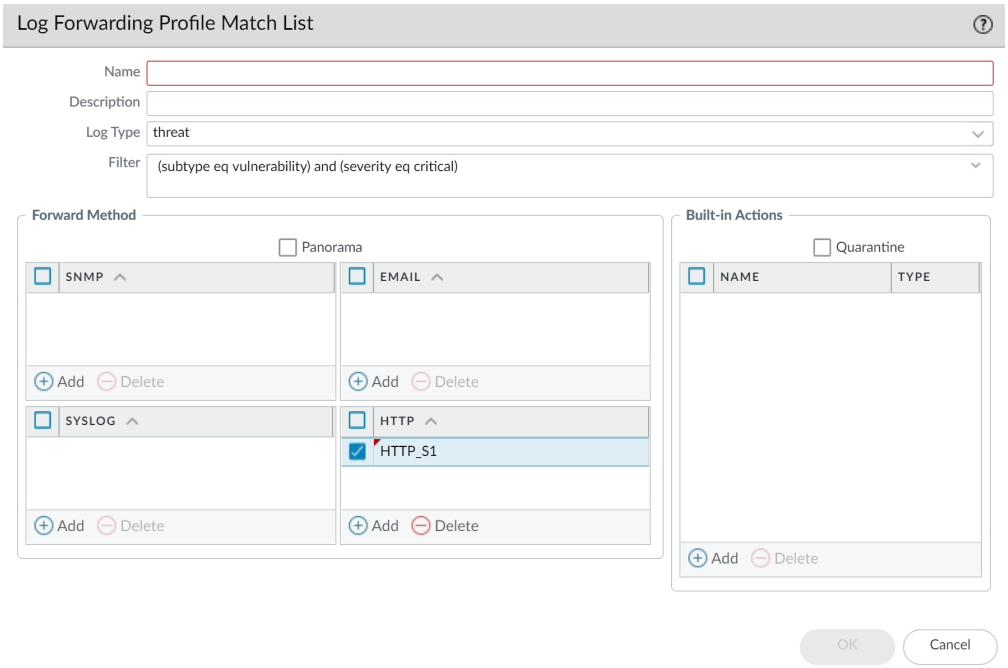


3. Seleccione **Send Test Log (Enviar log de prueba)** para verificar que el servidor HTTP reciba la solicitud. Cuando envía de manera interactiva un log de prueba, el cortafuegos utiliza el formato tal como está y no reemplaza la variable por un valor de un log del cortafuegos. Si su servidor HTTP envía una respuesta 404, proporcione valores para los parámetros, a fin de que el servidor pueda procesar la solicitud correctamente.

STEP 3 | Defina los criterios de coincidencia para determinar cuándo el cortafuegos enviará logs al servidor HTTP, y adjunte el perfil de servidor HTTP que vaya a usar.

1. Seleccione los tipos de logs para los cuales desea activar un flujo de trabajo:
   - Añada un perfil de reenvío de logs (**Objects (Objetos)** > **Log Forwarding (Reeenvío de logs)**) para los logs que pertenecen a la actividad de usuario (por ejemplo, logs de Traffic (Tráfico), Threat (Amenaza) o Authentication (Autenticación)).
   - Seleccione **Device (Dispositivo)** > **Log Settings (Configuración de logs)** para los logs que pertenecen a eventos del sistema, tales como logs de configuración o sistema.
2. Seleccione el tipo de log y utilice el nuevo **Filter Builder (Generador de filtro)** para definir los criterios de coincidencia.
3. Seleccione **Add (Añadir)** para añadir un perfil de servidor HTTP para enviar logs a un destino HTTP.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Monitorización de NetFlow

NetFlow es un protocolo estándar del sector que el cortafuegos puede utilizar para exportar estadísticas sobre el tráfico IP en sus interfaces. El cortafuegos exporta las estadísticas como campos de NetFlow a un recopilador NetFlow. El recopilador NetFlow es un servidor que utiliza para analizar el tráfico de la red con fines de seguridad, administración, contabilidad y solución de problemas. Todos los cortafuegos de Palo Alto Networks son compatibles con NetFlow Versión 9. Los cortafuegos solo son compatibles con NetFlow unidireccional, pero no bidireccional. Los cortafuegos realizan el procesamiento NetFlow en todos los paquetes IP en las interfaces y no admiten NetFlow muestreado. Puede exportar registros de NetFlow para las interfaces de capa 3, capa 2, cable virtual, tap, VLAN, loopback y túnel. Para las subinterfaces Ethernet de agregación, puede exportar registros para las subinterfaces individuales por las que fluyen los datos dentro del grupo. Para identificar las interfaces del cortafuegos en un recopilador NetFlow, consulte Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow. Los cortafuegos admiten Plantillas de NetFlow estándar y empresariales (específicas de PAN-OS), que los recopiladores NetFlow utilizan para descifrar los campos NetFlow.

- Configuración de exportaciones de NetFlow
- Plantillas de NetFlow

Configuración de exportaciones de NetFlow

Para utilizar un recopilador NetFlow con el fin de analizar el tráfico de red en las interfaces de cortafuegos, realice los siguientes pasos para configurar las exportaciones de registros de NetFlow.

STEP 1 | Cree un perfil de servidor NetFlow.

El perfil define los recopiladores NetFlow que recibirán los registros exportados y especifica los parámetros de exportación.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **NetFlow** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para identificar el perfil.
3. Especifique la velocidad a la que el cortafuegos actualiza las plantillas de NetFlow en **Minutes (Minutos)** (el valor predeterminado es 30) y **Packets (Paquetes)** (registros exportados: el valor predeterminado es 20), de acuerdo con los requisitos de su recopilador de NetFlow. El cortafuegos actualiza las plantillas después de haber superado cualquiera de los umbrales.
4. Especifique el **Active Timeout (Tiempo de espera activo)**, que es la frecuencia en minutos con la que el cortafuegos exporta registros (el valor predeterminado es 5).
5. Seleccione **PAN-OS Field Types (Tipos de campos de PAN-OS)** si desea que el cortafuegos exporte los campos App-ID y User-ID.
6. **Add (Añada)** cada recopilador NetFlow (como máximo, dos por perfil) que recibirá los registros. Para cada recopilador, especifique la siguiente información:
   - **Name (Nombre)** para identificar el recopilador.
   - Nombre de host o dirección IP del **NetFlow Server (Servidor NetFlow)**.
   - **Port (Puerto)** de acceso (el valor predeterminado es 2055).
7. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 2 | Asigne el perfil del servidor NetFlow a las interfaces del cortafuegos que transfieren el tráfico que desea analizar.

En este ejemplo, asigne el perfil a una interfaz de Ethernet existente.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en el nombre de la interfaz para editarlo.

© 2020 Palo Alto Networks, Inc.

Puede exportar registros de NetFlow para las interfaces de capa 3, capa 2, cable virtual, tap, VLAN, loopback y túnel. Para agregar interfaces Ethernet, puede exportar registros para el grupo agregado, pero no para las interfaces individuales dentro del grupo.

2. Seleccione el perfil de servidor NetFlow (**NetFlow Profile [Perfil NetFlow]**) que configuró y haga clic en **OK (Aceptar)**.

STEP 3 | **(Necesario para los cortafuegos serie PA-7000 y PA-5200)** Configure una ruta de servicio que el cortafuegos utilizará para enviar registros de NetFlow.

No puede utilizar una interfaz de gestión (MGT) para enviar registros de NetFlow desde los cortafuegos serie PA-7000 y PA-5200. En el caso de los otros modelos de cortafuegos, una ruta de servicio es opcional. En todos los cortafuegos, el interfaz que envía registros de NetFlow no debe ser el mismo que el interfaz para el que el cortafuegos recopila los registros.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
2. **(Cortafuegos con múltiples sistemas virtuales)** Seleccione una de las siguientes opciones:
   - **Global:** seleccione esta opción si la ruta de servicio se aplica a todos los sistemas virtuales del cortafuegos.
   - **Sistemas virtuales:** seleccione esta opción si la ruta de servicio se aplica a un sistema virtual específico. Establezca la **Location (Ubicación)** del sistema virtual.
3. Seleccione **Service Route Configuration (Configuración de ruta de servicios)** y personalícela.
4. Seleccione el protocolo (**IPv4** o **IPv6**) que utiliza la interfaz. Puede configurar la ruta de servicio de ambos protocolos si es necesario.
5. Haga clic en **NetFlow** en la columna Service (Servicio).
6. Seleccione la **Source Interface (Interfaz de origen)**.

   Any (Todos), Use default (Utilizar predeterminado) y MGT (Gestión) no son opciones de interfaz válidas para enviar registros de NetFlow desde cortafuegos serie PA-7000 o PA-5200.
7. Seleccione una **Source Address (Dirección de origen)** (dirección IP).
8. Haga clic en **OK (Aceptar)** dos veces para guardar los cambios.

STEP 4 | **Commit (Confirmar)** los cambios.

STEP 5 | Supervise el tráfico del cortafuegos en un recopilador de NetFlow.

Consulte la documentación de su recopilador de NetFlow.

Cuando supervise las estadísticas, debe comparar los índices de interfaz en el recopilador de NetFlow con los nombres de interfaz en la interfaz web del cortafuegos. Si desea información detallada, consulte Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow.

Para solucionar los problemas de entrega de NetFlow, utilice el comando operativo de la CLI **`debug log-receiver netflow statistics`**.

Plantillas de NetFlow

Los recopiladores de NetFlow usan plantillas para descifrar los campos que exporta el cortafuegos. El cortafuegos selecciona una plantilla según el tipo de datos exportados: tráfico IPv4 o IPv6, con o sin NAT y con campos estándar o específicos de empresa (específicos de PAN-OS). El cortafuegos actualiza periódicamente las plantillas para reevaluar cuál se usa (en caso de que el tipo de datos exportados cambie) y aplicar los cambios a los campos en la plantilla seleccionada. Cuando configura exportaciones de NetFlow,

© 2020 Palo Alto Networks, Inc.

configure la tasa de actualización en función de un intervalo y una serie de registros exportados de acuerdo con los requisitos de su recopilador de NetFlow. El cortafuegos actualiza las plantillas después de haber superado cualquiera de los umbrales.

El cortafuegos de Palo Alto Networks admite las siguientes plantillas de NetFlow:

Plantilla	ID
IPv4 estándar	256
IPv4 Enterprise	257
IPv6 estándar	258
IPv6 empresarial	259
IPv4 con NAT Standard	260
IPv4 con NAT Enterprise	261
IPv6 con NAT estándar	262
IPv6 con NAT Enterprise	263

En la siguiente tabla se incluyen los campos de NetFlow que el cortafuegos puede enviar junto con las plantillas que los definen:

Valor	Campo	Description (Descripción)	Plantillas
1	IN_BYTES	Contador de entrada con una longitud de N * 8 bits para el número de bytes asociado a un flujo IP. De forma predeterminada, N es 4.	Todas las plantillas
2	IN_PKTS	Contador de entrada con una longitud de N * 8 bits para el número de paquetes asociado a un flujo IP. De forma predeterminada, N es 4.	Todas las plantillas
4	PROTOCOL	Byte de protocolo IP.	Todas las plantillas
5	TOS	Ajuste de tipo de byte de servicio al entrar la interfaz de entrada.	Todas las plantillas
6	TCP_FLAGS	Total de marcas de TCP de este flujo.	Todas las plantillas
7	L4_SRC_PORT	Número de puerto de origen de TCP/UDP (por ejemplo FTP, Telnet o equivalente).	Todas las plantillas
8	IPV4_SRC_ADDR	Dirección de origen IPv4.	IPv4 estándar IPv4 Enterprise

© 2020 Palo Alto Networks, Inc.

Valor	Campo	Description (Descripción)	Plantillas
			IPv4 con NAT estándar IPv4 con NAT Enterprise
10	INPUT_SNMP	Índice de interfaz de entrada. La longitud del valor es de 2 bytes de forma predeterminada, pero es posible utilizar valores superiores. Para obtener detalles acerca de la manera en que los cortafuegos de Palo Alto Networks generan índices de interfaz, consulte Identificadores de interfaz de cortafuegos en gestores SNMP y recopiladores de NetFlow.	Todas las plantillas
11	L4_DST_PORT	Número de puerto de destino de TCP/UDP (por ejemplo FTP, Telnet o equivalente).	Todas las plantillas
12	IPV4_DST_ADDR	Dirección de destino IPv4.	IPv4 estándar IPv4 Enterprise IPv4 con NAT estándar IPv4 con NAT Enterprise
14	OUTPUT_SNMP	Índice de interfaz de salida. La longitud del valor es de 2 bytes de forma predeterminada, pero es posible utilizar valores superiores. Para obtener detalles acerca de la manera en que los cortafuegos de Palo Alto Networks generan índices de interfaz, consulte Identificadores de interfaz de cortafuegos en gestores SNMP y recopiladores de NetFlow.	Todas las plantillas
21	LAST_SWITCHED	Tiempo de actividad del sistema en milisegundos en el momento de conmutar el último paquete de este flujo.	Todas las plantillas
22	FIRST_SWITCHED	Tiempo de actividad del sistema en milisegundos en el momento de conmutar el primer paquete de este flujo.	Todas las plantillas
27	IPV6_SRC_ADDR	Dirección de origen IPv6.	IPv6 estándar IPv6 empresarial

© 2020 Palo Alto Networks, Inc.

Valor	Campo	Description (Descripción)	Plantillas
			IPv6 con NAT estándar IPv6 con NAT empresarial
28	IPV6_DST_ADDR	Dirección IPv6 de destino.	IPv6 estándar IPv6 empresarial IPv6 con NAT estándar IPv6 con NAT empresarial
32	ICMP_TYPE	Tipo de paquete del protocolo de mensajes de control de Internet (ICMP). Esto se indica como: Tipo de ICMP * 256 + código de ICMP	Todas las plantillas
61	DIRECTION	Dirección de flujo: • 0 = entrada • 1 = salida	Todas las plantillas
148	flowId	Identificador de flujo único en un dominio de observación. Puede usar este elemento de información para diferenciar los distintos flujos si las claves de flujo, como las direcciones IP y los números de puertos, no se indican o se indican en registros independientes. El flowID corresponde al campo de ID de sesión en los logs de tráfico y amenaza.	Todas las plantillas
233	firewallEvent	Indica un evento del cortafuegos: • 0 = Ignorar (no válido): no se utiliza. • 1 = Flujo creado: el registro de datos de NetFlow corresponde a un nuevo flujo. • 2 = Flujo eliminado: el registro de datos de NetFlow corresponde al final de un flujo. • 3 = Flow denegado: el registro de datos de NetFlow indica un flujo que la política del cortafuegos negó. • 4 = Alerta de flujo: no se utiliza. • 5 = Actualización de flujo: el registro de datos de NetFlow	Todas las plantillas

© 2020 Palo Alto Networks, Inc.

Valor	Campo	Description (Descripción)	Plantillas
		se envía para un flujo *de larga duración*, que es un flujo que dura más que el periodo de **Active Timeout (Tiempo de espera activo)** configurado en el perfil de servidor de NetFlow .	
225	postNATSourceIPv4Address	La definición de este elemento de información es idéntica a la de sourceIPv4Address, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción de la dirección de red después de que el paquete atravesara la interfaz.	IPv4 con NAT estándar IPv4 con NAT Enterprise
226	postNATDestinationIPv4Address	La definición de este elemento de información es idéntica a la de destinationIPv4Address, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción de la dirección de red después de que el paquete atravesara la interfaz.	IPv4 con NAT estándar IPv4 con NAT Enterprise
227	postNAPTSourceTransportPort	La definición de este elemento de información es idéntica a la de sourceTransportPort, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción del puerto de la dirección de red después de que el paquete atravesara la interfaz.	IPv4 con NAT estándar IPv4 con NAT Enterprise
228	postNAPTDestinationTransportPort	La definición de este elemento de información es idéntica a la de destinationTransportPort, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción del puerto de la dirección de red después de que el paquete atravesara la interfaz.	IPv4 con NAT estándar IPv4 con NAT Enterprise
281	postNATSourceIPv6Address	La definición de este elemento de información es idéntica a la definición de elemento de información sourceIPv6Address, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción de la dirección de red NAT64 después de que el paquete atravesara la interfaz. Consulte RFC 2460 para la definición del campo de	IPv6 con NAT estándar IPv6 con NAT empresarial

© 2020 Palo Alto Networks, Inc.

Valor	Campo	Description (Descripción)	Plantillas
		dirección de origen del encabezado de IPv6. Consulte RFC 6146 para la especificación de NAT64.	
282	postNATDestinationIPv6Address	La definición de este elemento de información es idéntica a la definición de elemento de información destinationIPv6Address, a excepción de que indica un valor modificado que el cortafuegos produjo durante la traducción de la dirección de red NAT64 después de que el paquete atravesara la interfaz. Consulte RFC 2460 para la definición del campo de dirección de destino del encabezado de IPv6. Consulte RFC 6146 para la especificación de NAT64.	IPv6 con NAT estándar IPv6 con NAT empresarial
346	privateEnterpriseNumber	Este es un número de empresa privado único que identifica a Palo Alto Networks: 25461.	IPv4 Enterprise IPv4 con NAT Enterprise IPv6 empresarial IPv6 con NAT empresarial
56701	App-ID	Nombre de una aplicación identificada por App-ID. El nombre puede tener hasta 32 bytes.	IPv4 Enterprise IPv4 con NAT Enterprise IPv6 empresarial IPv6 con NAT empresarial
56702	User-ID	Nombre de usuario identificado por User-ID. El nombre puede tener hasta 64 bytes.	IPv4 Enterprise IPv4 con NAT Enterprise IPv6 empresarial IPv6 con NAT empresarial

© 2020 Palo Alto Networks, Inc.

Identificadores de interfaz de cortafuegos en los gestores SNMP y recopiladores de NetFlow

Si utiliza un recopilador NetFlow (consulte Supervisión de NetFlow) o un gestor SNMP (consulte Supervisión de SNMP y capturas) para supervisar el cortafuegos de Palo Alto Networks, un índice de interfaz (objeto ifindex de SNMP) identifica la interfaz del cortafuegos que transporta un flujo concreto (consulte Índices de interfaz en un gestor SNMP). En contraste, el interfaz web del cortafuegos usa nombres de interfaz como identificadores (por ejemplo, ethernet1/1), sin índices. Para comprender qué características de las que puede ver en un recopilador de NetFlow o gestor SNMP se aplican a qué interfaz de cortafuegos, debe ser capaz de relacionar los índices de interfaz con nombres de interfaz.

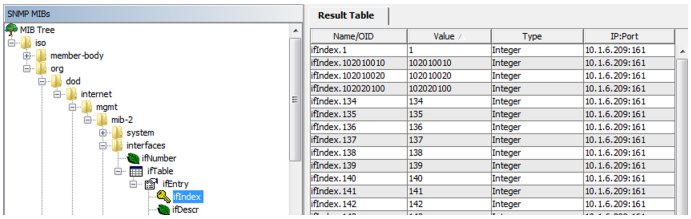


Figure 3: Índices de interfaz en un gestor SNMP

Debe hacer coincidir los índices con nombres comprendiendo las fórmulas que usa el cortafuegos para calcular los índices. Las fórmulas varían por plataforma y tipo de interfaz: física o lógica.

Los índices de interfaces físicas están comprendidos en un intervalo de 1-9999, el cual calcula el cortafuegos del modo siguiente:

Plataforma de cortafuegos	Cálculo	Ejemplo de índice de interfaz
VM-SERIES	Número de puertos de gestión + desplazamiento de puerto físico • **Número de puertos de gestión**: es una constante de 1. • **Desplazamiento de puerto físico**: es el número del puerto físico.	Cortafuegos VM-100, Eth1/4 = 1 (número de puertos de gestión) + 4 (puerto físico) = **5**
PA-220, PA-220R, PA-800 Series	Número de puertos de gestión + desplazamiento de puerto físico • **Número de puertos de gestión**: es una constante de 5. • **Desplazamiento de puerto físico**: es el número del puerto físico.	Cortafuegos de PA-5200 Series, Eth1/4 = 5 (número de puertos de gestión) + 4 (puerto físico) = **9**
PA-3200 Series y PA-5200 Series	Número de puertos de gestión + desplazamiento de puerto físico • **Número de puertos de gestión**: es una constante de 4. • **Desplazamiento de puerto físico**: es el número del puerto físico.	Cortafuegos de PA-5200 Series, Eth1/4 = 4 (número de puertos de gestión) + 4 (puerto físico) = **8**

© 2020 Palo Alto Networks, Inc.

Plataforma de cortafuegos	Cálculo	Ejemplo de índice de interfaz
PA-7000 Series	(Máx. de puertos * ranura) + desplazamiento de puerto físico + número de puertos de gestión • **Número máximo de puertos**: es una constante de 64. • **Ranura**: es el número de ranura del bastidor de la tarjeta de interfaz de red. • **Desplazamiento de puerto físico**: es el número del puerto físico. • **Número de puertos de gestión**: es una constante de 5.	Cortafuegos de PA-7000 Series, Eth3/9 = (64 [máx. de puertos] * 3 [ranura]) + 9 (puerto físico) + 5 (número de puertos de gestión) = **206**

Los índices de interfaces lógicas para todas las plataformas son números de nueve dígitos que el cortafuegos calcula del modo siguiente:

Tipo de interfaz	Intervalo	Dígito 9	Dígitos 7-8	5-6 dígitos	1-4 dígitos	Ejemplo de índice de interfaz
Subinterfaz de la capa 3	101010001-199999999	Tipo: 1	Ranura de interfaz: 1-9 (01-09)	Puerto de interfaz: 1-9 (01-09)	Subinterfaz: sufijo 1-9999 (0001-9999)	Eth1/5.22 = 100000000 (tipo) + 100000 (ranura) + 50000 (puerto) + 22 (sufijo) = **101050022**
Subinterfaz de la capa 2	101010001-199999999	Tipo: 1	Ranura de interfaz: 1-9 (01-09)	Puerto de interfaz: 1-9 (01-09)	Subinterfaz: sufijo 1-9999 (0001-9999)	Eth2/3.6 = 100000000 (tipo) + 200000 (ranura) + 30000 (puerto) + 6 (sufijo) = **102030006**
Subinterfaz Vwire	101010001-199999999	Tipo: 1	Ranura de interfaz: 1-9 (01-09)	Puerto de interfaz: 1-9 (01-09)	Subinterfaz: sufijo 1-9999 (0001-9999)	Eth4/2.312 = 100000000 (tipo) + 400000 (ranura) + 20000 (puerto) + 312 (sufijo) = **104020312**
VLAN	200000001-200009999	Tipo: 2	00	00	Sufijo de VLAN: 1-9999 (0001-9999)	VLAN.55 = 200000000 (tipo) + 55 (sufijo) = **200000055**
Bucle invertido	300000001-300009999	Tipo: 3	00	00	Sufijo de loopback: 1-9999 (0001-9999)	Loopback.55 = 300000000 (tipo) + 55 (sufijo) = **300000055**

© 2020 Palo Alto Networks, Inc.

Tipo de interfaz	Intervalo	Dígito 9	Dígitos 7-8	5-6 dígitos	1-4 dígitos	Ejemplo de índice de interfaz
Túnel	400000001-400009999	Tipo: 4	00	00	Sufijo de túnel: 1-9999 (0001-9999)	Tunnel.55 = 400000000 (tipo) + 55 (sufijo) = **400000055**
Grupo de agregados	500010001-500089999	Tipo: 5	00	Sufijo AE: 1-8 (01-08)	Subinterfaz: sufijo 1-9999 (0001-9999)	AE5.99 = 500000000 (tipo) + 50000 (sufijo AE) + 99 (sufijo) = **500050099**

© 2020 Palo Alto Networks, Inc.

Supervisión de transceptores

Puede supervisar el estado de los transceptores en su solución o dispositivo físico para facilitar la instalación y la resolución de problemas. Los diagnósticos que se pueden ver son la corriente de polarización transmitida, la potencia transmitida, la potencia recibida, la temperatura del transceptor y el voltaje de la fuente de alimentación. Consulte la información que figura a continuación para obtener una lista de dispositivos que admiten la supervisión del transceptor.

- PA-800 Series
- Serie PA-3200
- PA-5200 Series
- PA-7000 Series

Utilice la interfaz de línea de comandos para ejecutar la supervisión del transceptor. Consulte la siguiente tabla para ver todos los comandos de la CLI disponibles.



Si ejecuta comandos en un transceptor incompatible, la CLI devolverá "n/a" para cualquier información de diagnóstico que no pueda leer.

CLI	Definición
`show transceiver <interface name>`	Vea un resumen del transceptor especificado con valores para cada diagnóstico. Ejemplo: `admin@PA-7080> show transceiver ethernet11/25` La CLI devolverá los valores de temperatura, tensión, corriente, potencia Tx y potencia Rx.
`show transceiver-detail <interface name>`	Reciba especificaciones más detalladas sobre el transceptor, incluida la información del proveedor y la longitud de los enlaces. La CLI también proporcionará información de diagnóstico más detallada.
`show transceiver all`	Vea una lista de todos los transceptores activos, así como un resumen de cada uno de sus diagnósticos.
`show transceiver-detail all`	Obtenga detalles completos sobre cada transceptor en el dispositivo.

User-ID

En contraposición a una dirección IP, la identidad de un usuario es un componente fundamental de una infraestructura de seguridad eficaz. Saber quién usa cada una de las aplicaciones de su red y quién puede haber transmitido una amenaza o está transfiriendo archivos puede reforzar las políticas de seguridad y reducir los tiempos de respuesta en caso de un incidente. User-ID, una función estándar del cortafuegos de Palo Alto Networks, le permite aprovechar la información sobre usuarios almacenada en una gran variedad de repositorios. Los siguientes temas proporcionan más información detallada sobre User-ID y su configuración:

- Descripción general de User-ID
- Conceptos de User-ID
- Habilitación de User-ID
- Asignación de usuarios a grupos
- Asignación de direcciones IP a usuarios
- Habilitación de política basada en usuarios y grupos
- Habilitación de política para usuarios con múltiples cuentas
- Verificación de la configuración de User-ID
- Implementación de User-ID en una red a gran escala

© 2020 Palo Alto Networks, Inc.

Descripción general de User-ID

User-ID™ le permite identificar a todos los usuarios en su red utilizando una variedad de técnicas para garantizar que pueda identificar los usuarios en todas las ubicaciones con una variedad de métodos de acceso y sistemas operativos, como Microsoft Windows, Apple iOS, Mac OS, Android y Linux®/UNIX. Conocer sus usuarios en lugar de solo conocer sus direcciones IP le permite lo siguiente:

- **Visibilidad**: la visibilidad mejorada del uso de las aplicaciones basada en los usuarios le ofrece información más pertinente sobre la actividad de la red. La importancia de User-ID se vuelve evidente cuando observa una aplicación extraña o desconocida en su red. Por medio del ACC o el visor de logs, su equipo de seguridad puede determinar cuál es la aplicación, quién es el usuario, el consumo de ancho de banda y de sesión, el origen y el destino del tráfico de la aplicación y cualquier amenaza asociada.
- **Control de políticas:** la conexión de la información del usuario con las reglas de la política de seguridad permite una habilitación segura de las aplicaciones que atraviesan la red y garantiza que solo los usuarios con una necesidad empresarial de una aplicación puedan acceder. Por ejemplo, algunas aplicaciones, tales como las aplicaciones SaaS que habilitan el acceso a los servicios de Recursos Humanos (tales como Workday o Service Now) deben estar disponibles para todos los usuarios conocidos de la red. Sin embargo, para las aplicaciones más delicadas puede reducir la superficie de ataque al garantizar que solo los usuarios que las necesitan tengan acceso a ellas. Por ejemplo, si bien el personal de asistencia técnica de TI puede necesitar legítimamente el acceso a aplicaciones de escritorio remoto, la mayoría de sus usuarios no lo necesitan.
- **Creación de logs, creación de informes, análisis de datos:** si se produce un incidente de seguridad, el análisis de datos y la generación de informes basados en la información del usuario, en lugar de solo las direcciones IP, brindan una imagen más completa del problema. Por ejemplo, puede utilizar la actividad de grupo/usuario predefinida para ver un resumen de las actividades web de usuarios individuales o grupos de usuarios, o el informe de uso de aplicaciones SaaS para ver los usuarios que transfieren más datos mediante aplicaciones SaaS no sancionadas.

Para aplicar las políticas basadas en usuarios y grupos, el cortafuegos debe poder asignar las direcciones IP de los paquetes que recibe a nombres de usuarios. User-ID proporciona numerosos mecanismos para recopilar esta información de Asignación de usuario. Por ejemplo, el agente de User-ID supervisa los logs de servidor para eventos de inicio de sesión y escucha mensajes de syslog de servicios de autenticación. Para identificar asignaciones de direcciones IP que el agente no asignó, puede configurar Política de autenticación para que redirija las solicitudes HTTP a un inicio de sesión de portal de autenticación Puede adaptar los mecanismos de asignación de usuarios a su entorno e incluso utilizar diferentes mecanismos en diferentes sitios para garantizar que permite a todos los usuario acceder de manera segura a las aplicaciones en todas las ubicaciones, todo el tiempo.

© 2020 Palo Alto Networks, Inc.

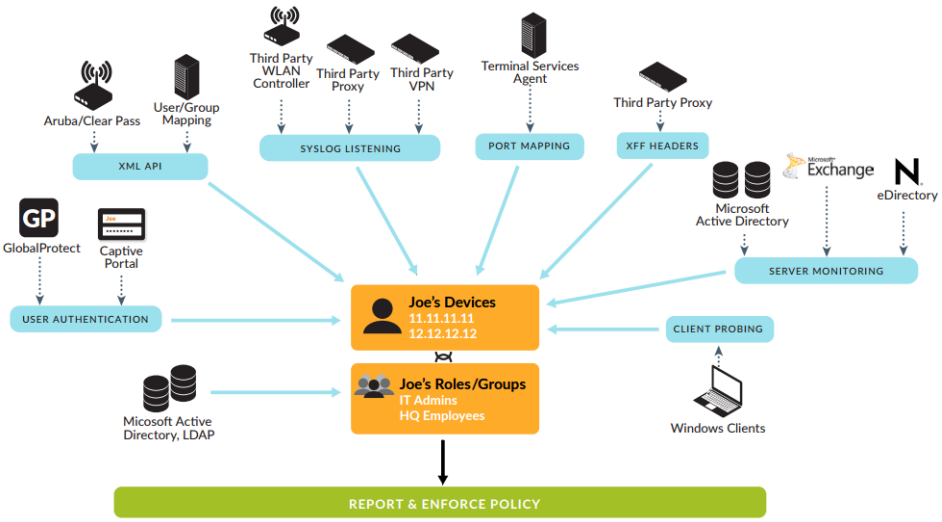


Figure 4: User-ID

Para habilitar las políticas basadas en usuarios y grupos, el cortafuegos debe tener una lista de todos los usuarios disponibles y su pertenencia a los grupos, de modo que pueda seleccionar grupos al definir las reglas de su política. El cortafuegos recopila información de Asignación de grupos conectándose directamente con el servidor de su directorio LDAP o utilizando integración de la API de XML con el servidor de su directorio.

Consulte Conceptos de User-ID si desea información sobre cómo funciona User-ID y Habilitación de User-ID si desea instrucciones sobre la configuración de User-ID.

User-ID no funciona en entornos en los que las direcciones IP de los usuarios están sujetas a la traducción NAT antes de que el cortafuegos asigne las direcciones IP a nombres de usuarios.

© 2020 Palo Alto Networks, Inc.

Conceptos de User-ID

- Asignación de grupos
- Asignación de usuario

Asignación de grupos

Para definir las reglas de políticas basadas en usuarios o grupos, primero cree un perfil de servidor LDAP que defina la forma en que el cortafuegos se conecta a su servidor de directorio y se autentica. El cortafuegos admite una variedad de servidores de directorio, incluidos Microsoft Active Directory (AD), Novell eDirectory y Sun ONE Directory Server. El perfil de servidor también define cómo el cortafuegos busca el directorio para recuperar la lista de grupos y la lista de miembros correspondiente. Si utiliza un servidor de directorio que no es compatible con el cortafuegos de forma nativa, puede integrar la función de asignación de grupos utilizando la API de XML. Luego, puede crear una configuración de asignación de grupos para realizar la Asignación de usuarios a grupos y la Habilitación de política basada en usuarios y grupos.

La definición de reglas de políticas que se basen en la pertenencia a grupos en lugar de en usuarios individuales simplifica la administración porque no tiene que actualizar las reglas siempre que se agregan nuevos usuarios a un grupo. Cuando configure una asignación de grupo, puede limitar qué grupos estarán disponibles en las reglas de políticas. Puede especificar grupos que ya existen en su servicio de directorios o especificar grupos personalizados basados en filtros LDAP. Puede tardar si define grupos personalizados que si crea nuevos grupos o cambia los existentes en un servidor LDAP, y la definición no requiere la intervención de un administrador LDAP. User-ID asigna todos los usuarios de directorio LDAP que hacen coincidir el filtro con el grupo personalizado. Por ejemplo, puede querer una política de seguridad que permita a los contratistas del departamento de marketing acceder a los sitios de redes sociales. Si no existe ningún grupo de Active Directory para ese departamento, puede configurar un filtro LDAP que coincida con los usuarios cuyo atributo de LDAP Departamento está definido como Marketing. Las consultas e informes de log que se basan en grupos de usuarios incluirán grupos personalizados.

Asignación de usuario

Conocer los nombres de usuario y de grupos representa solo un paso. El cortafuegos también debe saber qué direcciones IP asignar a qué usuarios para que puedan implementarse las reglas de seguridad de forma apropiada. Descripción general de User-ID muestra los diferentes métodos que se utilizan para identificar usuarios y grupos en su red y presenta el modo en que la asignación de usuarios y la asignación de grupos trabajan en conjunto para habilitar la visibilidad y la aplicación de la seguridad basada en usuarios y grupos. Los temas siguientes describen los diferentes métodos de asignación de usuarios:

- Monitorización de servidor
- Asignación de puertos
- Syslog
- Encabezados XFF
- Inserción del encabezado de nombre de usuario
- Política de autenticación y portal de autenticación
- GlobalProtect
- XML API
- Sondeo de cliente

Monitorización de servidor

Mediante la supervisión de servidores, un agente de User-ID (bien un agente basado en Windows que se ejecuta en un servidor de dominios de su red, bien el agente de User-ID integrado en PAN-OS que

© 2020 Palo Alto Networks, Inc.

se ejecuta en el cortafuegos) controla los logs de eventos de seguridad en busca de eventos de inicio de sesión en los Microsoft Exchange Server, los controladores de dominios o los servidores Novell eDirectory especificados. Por ejemplo, en un entorno AD, puede configurar el agente de User-ID para que supervise los logs de seguridad en busca de renovaciones o concesiones de tickets de Kerberos, acceso al servidor Exchange (si está configurado) y conexiones de servicio de impresión y archivo. Para que estos eventos se registren en el log de seguridad, el dominio AD debe configurarse para registrar eventos de inicio de sesión de cuenta correctos. Además, dado que los usuarios pueden iniciar sesión en cualquiera de los servidores del dominio, debe configurar la supervisión de servidor para todos los servidores con el fin de capturar todos los eventos de inicio de sesión de usuarios. Para obtener más información, consulte Configuración de la asignación de usuarios mediante el agente de User-ID de Windows o Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.

Asignación de puertos

En entornos con sistemas multiusuario (como entornos de Microsoft Terminal Server o Citrix), muchos usuarios comparten la misma dirección IP. En este caso, el proceso de asignación de usuario a dirección IP requiere el conocimiento del puerto de origen de cada cliente. Para realizar este tipo de asignación, debe instalar el agente de servidor de terminal de Palo Alto Networks en el propio servidor de terminal Windows/Citrix para que sirva de intermediario en la asignación de puertos de origen a los diversos procesos de usuario. Para los servidores de terminal que no admiten el agente de servidor de terminal, como los servidores de terminal de Linux, puede utilizar XML API para enviar información de asignación de usuarios de eventos de inicio de sesión y cierre de sesión a User-ID. Consulte Configuración de la asignación de usuarios para usuarios del servidor de terminal para obtener información detallada sobre la configuración.

Encabezados XFF

Si tiene un servidor proxy implementado entre los usuarios en su red y el cortafuegos, el cortafuegos puede ver la dirección IP del servidor proxy como la dirección IP de origen en el tráfico HTTP/HTTPS que el proxy reenvía en lugar de la dirección IP del cliente que ha solicitado el contenido. En muchos casos, el servidor proxy añade un encabezado X-Forwarded-For (XFF) a los paquetes de tráfico, que incluye la dirección IPv4 o IPv6 real del cliente que solicitó el contenido desde o hacia el que se origina la solicitud. En esos casos, puede configurar el cortafuegos para extraer la dirección IP del usuario final de XFF, de modo que User-ID pueda asignar la dirección IP al nombre de usuario. Esto le permite implementar el Uso de los valores XFF en las políticas y en la creación de logs de usuarios de origen, de modo que pueda aplicar la política basada en el usuario para permitir el acceso de manera segura a las aplicaciones basadas en la web a sus usuarios detrás de un servidor proxy.

Inserción del encabezado de nombre de usuario

Cuando configure un dispositivo de cumplimiento secundario con el cortafuegos de Palo Alto Networks para aplicar la política basada en el usuario, es posible que el dispositivo secundario no tenga la asignación de dirección IP a nombre de usuario del cortafuegos. La transmisión de la identidad del usuario a dispositivos posteriores puede requerir la implementación de dispositivos adicionales, como proxies, o puede afectar negativamente a la experiencia del usuario (por ejemplo, que los usuarios tengan que iniciar sesión varias veces). Puede añadir dinámicamente el dominio y el nombre de usuario al encabezado HTTP del tráfico saliente del usuario y permitir que cualquier dispositivo secundario que use con el cortafuegos de Palo Alto Networks reciba la información del usuario y aplique la política basada en el usuario. La inclusión de la identidad del usuario mediante la inserción del nombre de usuario y el dominio en los encabezados de tráfico permite la aplicación de la política basada en el usuario sin que afecte negativamente a la experiencia del usuario o a la implementación de infraestructura adicional.

Política de autenticación y portal de autenticación

En algunos casos, el agente de User-ID no puede asignar una dirección IP a un nombre de usuario usando la supervisión del servidor u otros métodos (por ejemplo, si el usuario no ha iniciado sesión o si utiliza

© 2020 Palo Alto Networks, Inc.

un sistema operativo como Linux, que no es compatible con sus servidores de dominio). En otros casos, es posible que desee que los usuarios se autentiquen cuando acceden a aplicaciones confidenciales independientemente de los métodos que el agente de User-ID utiliza para realizar la asignación de usuarios. En todos estos casos, puede realizar la configuración de la política de autenticación y la asignación de direcciones IP a nombres de usuario utilizando el portal de autenticación. Todo el tráfico web (HTTP o HTTPS) que corresponda a una regla de política de autenticación le pide al usuario que se autentique con el portal de autenticación. Puede utilizar los siguientes métodos de autenticación del portal de autenticación:

- Desafío del explorador: utilice la autenticación de inicio de sesión único de Kerberos si desea reducir la cantidad de mensajes de inicio de sesión a los que deben responder los usuarios.
- Formulario web: utilice autenticación de multifactor; la autenticación de inicio de sesión único de SAML; la autenticación de Kerberos, TACACS+, RADIUS o LDAP; o la autenticación local.
- Autenticación de certificados de cliente.

Syslog

Es posible que su entorno cuente con servicios de red existentes que autentican usuarios. Entre estos servicios se incluyen controladores inalámbricos, dispositivos 802.1x, servidores Open Directory de Apple, servidores proxy y otros mecanismos de control de acceso a la red (NAC). Puede configurar estos servicios para enviar mensajes de syslog con información sobre los eventos de inicio de sesión y cierre de sesión, y configurar el agente de User-ID para analizar estos mensajes. El agente de User-ID analiza en busca de eventos de inicio de sesión para asignar direcciones IP a nombres de usuario y analiza en busca de eventos de cierre de sesión para eliminar las asignaciones desactualizadas. La eliminación de asignaciones desactualizadas es útil en entornos donde las asignaciones de direcciones IP cambian con frecuencia.

El agente de User-ID integrado en PAN-OS y el agente de User-ID basado en Windows utilizan los perfiles de análisis de syslog para analizar los mensajes de syslog. En entornos donde los servicios envían los mensajes en diferentes formatos, puede crear un perfil personalizado para cada formato y asociar varios perfiles con cada remitente de syslog. Si utiliza el agente de User-ID integrado en PAN-OS, también puede utilizar los perfiles de análisis de syslog predefinidos que ofrece Palo Alto Networks con las actualizaciones de contenido de las aplicaciones.

Los mensajes de syslog deben cumplir los siguientes criterios para que un agente de User-ID los analice:

- Cada mensaje debe ser una cadena de texto de una sola línea. Los delimitadores permitidos de los saltos de línea son una nueva línea (**\n**) o un retorno de carro más una nueva línea (**\r\n**).
- El tamaño máximo permitido de un mensaje de syslog individual es de 8000 bytes.
- Los mensajes de syslog que se envían por UDP deben estar incluidos en un único paquete; los mensajes enviados a través de SSL pueden repartirse entre varios paquetes. Un único paquete puede contener varios mensajes de syslog.

Consulte Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios para obtener información detallada sobre la configuración.

© 2020 Palo Alto Networks, Inc.

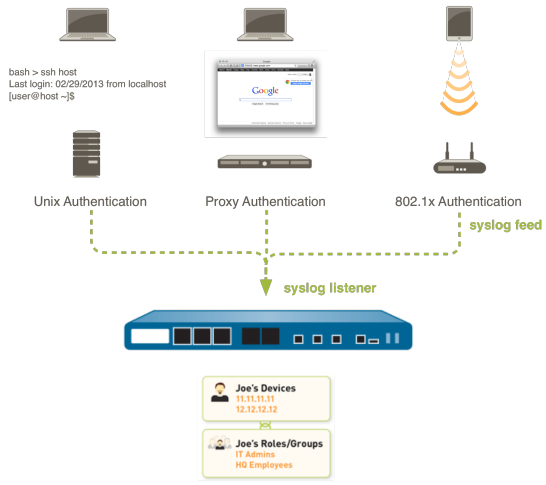


Figure 5: Integración de User-ID con Syslog

GlobalProtect

En el caso de usuarios móviles o con itinerancia, el endpoint GlobalProtect proporciona la información de asignación de usuarios directamente al cortafuegos. En este caso, cada usuario de GlobalProtect tiene una aplicación ejecutándose en el endpoint que requiere que el usuario introduzca credenciales de inicio de sesión para un acceso mediante VPN al cortafuegos. A continuación, esta información de inicio de sesión se añade a la tabla de asignaciones de usuarios de User-ID del cortafuegos para lograr visibilidad y la aplicación de políticas de seguridad basadas en usuarios. Dado que los usuarios de GlobalProtect deben autenticarse para poder acceder a la red, la asignación de direcciones IP a nombres de usuarios se conoce de manera explícita. Esta es la mejor solución en entornos confidenciales en los que deba estar seguro de quién es un usuario para permitirle el acceso a una aplicación o un servicio. Para obtener más información sobre cómo configurar GlobalProtect, consulte la GlobalProtect Administrator's Guide (Guía del administrador de GlobalProtect).

XML API

El portal de autenticación y otros métodos de asignación de usuarios estándar posiblemente no funcionen para ciertos tipos de acceso de usuarios. Por ejemplo, los métodos estándar no pueden añadir asignaciones de usuarios que se conectan desde una solución VPN de terceros o usuarios que se conectan a una red inalámbrica habilitada para 802.1x. Para estos casos, puede utilizar la API de XML de PAN-OS con el fin de capturar eventos de inicio de sesión y enviarlos al agente de User-ID integrado en PAN-OS. Consulte Envío de asignaciones de usuarios a User-ID mediante la API XML para obtener información detallada.

Sondeo de cliente

En un entorno de Microsoft Windows, puede configurar el agente de User-ID para probar sistemas de cliente con el Instrumental de administración de Windows (Windows Management Instrumentation, WMI) o sondeos de NetBIOS en intervalos regulares para verificar que la asignación de usuario existente siga siendo válida o para obtener el nombre de usuario para una dirección IP que todavía no se haya asignado.

El sondeo de NetBIOS solo es compatible en el caso del agente de User-ID basado en Windows; no es compatible en el caso del agente de User-ID integrado en PAN-OS.

El sondeo de clientes se diseñó para las redes heredadas, en las que la mayoría de los usuarios utilizan estaciones de trabajo en Windows en la red interna, pero no es ideal para las redes actuales más modernas que son compatibles con una base de usuarios móviles o con itinerancia en diversos dispositivos y sistemas

© 2020 Palo Alto Networks, Inc.

operativos. Además, el sondeo de clientes puede generar una gran cantidad de tráfico de red (basado en el número total de direcciones IP asignadas) y puede implicar una amenaza de seguridad cuando se configura incorrectamente. Por lo tanto, el sondeo de clientes ya no es un método recomendado para la asignación de usuarios. En su lugar, recoja información de asignación de usuarios de fuentes más aisladas y fiables, como controladores de dominio, y mediante integraciones con Syslog o XML API, que le permiten capturar con seguridad la información de asignación de usuarios desde cualquier tipo de dispositivo o sistema operativo. Si tiene aplicaciones confidenciales que requieren que conozca exactamente quién es cada usuario, configure Política de autenticación y portal de autenticación con el fin de garantizar que solo permita el acceso a los usuarios autorizados.

Dado que el sondeo del cliente confía en datos que se informan en el extremo, no es un método que se recomiende para obtener información de User-ID en una red de alta seguridad. Si utiliza un agente de User-ID para analizar los logs de eventos de seguridad del AD, los mensajes de syslog, o la API de XML para obtener las asignaciones de User-ID, Palo Alto Networks recomienda deshabilitar el sondeo del cliente.

Si elige el sondeo del cliente, no lo habilite en interfaces externas no fiables, dado que podría provocar que el agente envíe las sondas del cliente con información confidencial, como el nombre de usuario, el nombre de dominio y hash de contraseña de la cuenta de servicio del agente de User-ID, fuera de su red. Es muy posible que un atacante utilice esta información para penetrar la red y obtener acceso avanzado.

Si decide habilitar el sondeo en las zonas fiables, el agente sondeará cada dirección IP aprendida de forma periódica (cada 20 minutos, según los ajustes predeterminados, pero esto puede configurarse) para verificar que la sesión iniciada sea del mismo usuario. Además, cuando el cortafuegos encuentra una dirección IP para la cual no hay asignación de usuarios, enviará la dirección al agente para un sondeo inmediato.

Para obtener más información, consulte Configuración de la asignación de usuarios mediante el agente de User-ID de Windows o Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.

© 2020 Palo Alto Networks, Inc.

Habilitación de User-ID

En contraposición a una dirección IP, la identidad de un usuario es un componente fundamental de una infraestructura de seguridad eficaz. Saber quién usa cada una de las aplicaciones de su red y quién puede haber transmitido una amenaza o está transfiriendo archivos puede reforzar la política de seguridad y reducir los tiempos de respuesta en caso de un incidente. User-ID le permite aprovechar la información de usuario almacenada en una amplia variedad de repositorios para mayor visibilidad, control de política basada en el usuario y en el grupo, y un mejor registro, presentación de informes e informática forense.

STEP 1 | Habilite User-ID en las zonas de origen que contengan los usuarios que enviarán solicitudes que requieran controles de acceso basados en usuarios.

Habilite User-ID solo en zonas de confianza. Si habilita User-ID y el sondeo de clientes en una zona no fiable externa (como Internet), las sondas podrían enviarse fuera de su red protegida, y derivar en divulgación de información del nombre de cuenta de servicio del agente de User-ID, nombre de dominio y hash de contraseña cifrado, lo que podría permitir a un atacante obtener acceso no autorizado a recursos protegidos.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y haga clic en el **nombre** de la zona.
2. Seleccione **Enable User Identification (Habilitar identificación de usuario)** y haga clic en **OK (Aceptar)**.

STEP 2 | Creación de una cuenta de servicio exclusiva para el agente de User-ID.

Como práctica recomendada, cree una cuenta de servicio con el conjunto mínimo de permisos necesarios para respaldar las opciones de User-ID que usted permite para reducir la superficie de ataque en caso de que una cuenta de servicio se vea afectada.

Esto es necesario si usted planea usar el agente de User-ID basado en Windows o el agente de User-ID integrado en PAN-OS para supervisar los controladores de dominio, los servidores de Microsoft Exchange o los clientes de Windows para los eventos de inicio y cierre de sesión.

STEP 3 | Asignación de usuarios a grupos.

Esto permite que el cortafuegos se conecte con su directorio LDAP y recupere información de asignación de grupos para que usted pueda seleccionar nombres de usuario y nombres de grupo al crear la política.

STEP 4 | Asignación de direcciones IP a usuarios.

Como práctica recomendada, no habilite el sondeo de clientes como método de asignación de usuarios en redes de alta seguridad. El sondeo de clientes puede generar una gran cantidad de tráfico de red y puede representar una amenaza de seguridad cuando no se configura correctamente.

La manera de hacerlo depende de dónde se encuentran los usuarios y qué tipos de sistemas utilizan, y qué sistemas de su red están recopilando eventos de inicio y cierre de sesión para los usuarios. Debe configurar uno o más agentes de User-ID para habilitar la asignación de usuarios:

- Configuración de la asignación de usuarios mediante el agente de ID de usuario de Windows.
- Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.
- Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios.
- Configuración de la asignación de usuarios para usuarios del servidor de terminal.

© 2020 Palo Alto Networks, Inc.

- Envío de asignaciones de usuarios a User-ID mediante la API XML.
- Inserción de nombre de usuario en encabezados HTTP.

STEP 5 | Especifique las redes que se deben incluir en la asignación de usuarios y excluir de esta.



Como práctica recomendada, siempre especifique qué redes incluir y excluir de User-ID. Esto le permite asegurarse de que solo se sondeen sus activos fiables y de que no se creen asignaciones de usuario indeseables de manera imprevista.

La manera en la que especifica las redes que incluye y excluye depende de si utiliza el agente de User-ID basado en Windows o el agente de User-ID integrado en PAN-OS.

STEP 6 | Configure la Política de autenticación y el portal de autenticación.

El cortafuegos utiliza el portal de autenticación para autenticar a los usuarios finales cuando solicitan servicios, aplicaciones o categorías de URL que coinciden con reglas de la política de autenticación. En función de la información recopilada durante la autenticación, el cortafuegos crea nuevas asignaciones de usuario o actualiza asignaciones existentes. La información de asignación recopilada durante la autenticación cancela la información recopilada a través de otros métodos de User-ID.

1. Configuración del portal de autenticación.
2. Configuración de la política de autenticación

STEP 7 | Habilite el cumplimiento de la política basada en usuarios y grupos.



Cree reglas basadas en grupos en lugar de usuarios siempre que sea posible. Esto evita que tenga que actualizar continuamente sus políticas (lo que requiere una confirmación) cada vez que cambie su base de usuarios.

Después de configurar User-ID, podrá seleccionar un nombre de usuario o grupo al definir el origen o el destino de una regla de seguridad:

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** para añadir una nueva regla o haga clic en un nombre de regla existente para modificarlo.
2. Seleccione **User (Usuario)** y especifique qué usuarios y grupos deben coincidir en la regla de una de las siguientes formas:
   - Si desea seleccionar usuarios o grupos específicos como criterios de coincidencia, haga clic en el botón **Add (Añadir)** en la sección Source User (Usuario de origen) para mostrar una lista de usuarios y grupos detectados por la función de asignación de grupos del cortafuegos. Seleccione los usuarios o grupos que deben añadirse a la regla.
   - Si desea que la política coincida con cualquier usuario que se haya autenticado correctamente o no, y no necesita conocer el nombre específico del usuario o grupo, seleccione **known-user** o **unknown** en la lista desplegable que se encuentra por encima de la lista Source User.
3. Configure el resto de la regla según sea adecuado y, a continuación, haga clic en **OK**. Si desea información detallada sobre otros campos de la política de seguridad, consulte Configuración de una política de seguridad básica.

STEP 8 | Cree las reglas de política de seguridad para habilitar de manera segura User-ID en sus zonas fiables y evitar que el tráfico de User-ID salga de la red.

Respete la Práctica recomendada de política de seguridad de puerta de enlace de internet para asegurare de que la aplicación User-ID (`paloalto-userid-agent`) solo esté permitida en las zonas en las que sus agentes (tanto agentes de Windows como agentes integrados en PAN-OS) supervisen los servicios y distribuyan las asignaciones a los cortafuegos. Específicamente:

© 2020 Palo Alto Networks, Inc.

- Permita la aplicación `paloalto-userid-agent` entre las zonas donde residen sus agentes y las zonas donde residen los servidores supervisados (o incluso mejor, entre los sistemas específicos que alojan al agente y a los servidores supervisados).
- Permita la aplicación `paloalto-userid-agent` entre los agentes y los cortafuegos que necesitan las asignaciones de usuario, y entre los cortafuegos que están redistribuyendo asignaciones de usuario y los cortafuegos a los cuales están redistribuyendo la información.
- Deniegue la aplicación `paloalto-userid-agent` a las zonas externas, tal como su zona de Internet.

STEP 9 | Configure el cortafuegos para que obtenga direcciones IP de encabezados X-Forwarded-For (XFF).

Cuando el cortafuegos esté entre Internet y un servidor proxy, las direcciones IP de los paquetes que el cortafuegos ve son para el servidor proxy y no para los usuarios. Para habilitar la visibilidad de las direcciones IP, configure el cortafuegos para que utilice los encabezados XFF para la asignación de usuario. Con esta opción habilitada, el cortafuegos coteja las direcciones IP con los nombres de usuario mencionados en la política, para habilitar el control y la visibilidad para los usuarios y grupos asociados. Si desea información detallada, consulte Identificación de usuarios conectados a través de un servidor proxy.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** y edite la configuración de X-Forwarded-For Headers.
2. Seleccione **X-Forwarded-For Header in User-ID (Usar X reenviado para encabezado en ID de usuario)**.

   Al seleccionar la casilla Strip-X-Forwarded-For Header (Quitar X reenviado para encabezado) no se deshabilita el uso de encabezados XFF para atribución de usuarios en reglas de políticas; el cortafuegos solamente pone a cero el valor de XFF tras usarlo para la atribución de usuarios.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 10 | Si usa una configuración de alta disponibilidad (High Availability, HA), habilite la sincronización.

Se recomienda activar siempre la opción Enable Config Sync (Habilitar sincronización de configuración) para una configuración de HA con el fin de garantizar que las asignaciones de grupos y las asignaciones de usuarios estén sincronizadas entre el cortafuegos activo y el pasivo.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General** y edite la sección Setup (Configuración).
2. Seleccione **Enable HA (Habilitar HA)**.
3. Seleccione **Enable Config Sync**.
4. Introduzca la **Peer HA1 IP Address (Dirección IP de HA del peer)**, que es la dirección IP del enlace de control HA1 del cortafuegos del peer.
5. (Opcional) Introduzca una **Backup Peer HA1 IP Address (Dirección IP de HA1 de backup)**, que es la dirección IP del enlace de control de rcopia de seguridad del cortafuegos del peer.
6. Haga clic en **OK (Aceptar)**.

STEP 11 | Confirme los cambios.

Seleccione **Commit (Confirmar)** para confirmar los cambios a fin de activarlos.

STEP 12 | Verificación de la configuración de User-ID.

© 2020 Palo Alto Networks, Inc.

Después de configurar la asignación de usuarios y la asignación de grupos, verifique que la configuración funcione correctamente y que habilitar y supervisar de manera segura el acceso de los usuarios y grupos a sus aplicaciones y servicios.

© 2020 Palo Alto Networks, Inc.

Asignación de usuarios a grupos

La definición de reglas de políticas que se basen en la pertenencia a grupos de usuarios en lugar de en usuarios individuales simplifica la administración porque usted no tiene que actualizar las reglas siempre que cambia a pertenencia al grupo. El número de grupos de usuarios distintos a los que cada cortafuegos o instancia de Panorama puede hacer referencia en todas las políticas varía según el modelo. Si desea más información, consulte la matriz de compatibilidad.

Utilice el siguiente procedimiento para permitir que el cortafuegos se conecte con su directorio LDAP y recupere información de asignación de grupos. Luego puede Habilitar el cumplimiento de la política basada en usuarios y grupos..



Lo siguiente son prácticas recomendadas para la asignación de grupos en un entorno de Active Directory (AD):

- *Si tiene un único dominio, solamente necesita una configuración de asignación de grupos con un perfil de servidor LDAP que conecte el cortafuegos con el controlador de dominio utilizando la mejor conectividad. Puede añadir hasta cuatro controladores de dominio al perfil de servidor LDAP para redundancia. Tenga en cuenta que no puede aumentar la redundancia más allá de los cuatro controladores de dominio para un mismo dominio mediante la adición de varias configuraciones de asignación de grupo para ese dominio.*
- *Si tiene varios dominios y/o varios bosques, debe crear una configuración de asignación de grupo con un perfil de servidor LDAP que conecte el cortafuegos a un servidor de dominio en cada dominio/bosque. Tome las medidas oportunas para garantizar que los nombres se usuarios son exclusivos en los distintos bosques.*
- *Si tiene grupos universales, cree un perfil de servidor LDAP para conectarse al dominio raíz del servidor de catálogo global en el puerto 3268 o 3269 para SSL y, después, cree otro perfil de servidor LDAP para conectarse a los controladores de dominio raíz en el puerto 389. Esto ayuda a garantizar que la información de usuarios y grupos esté disponible para todos los dominios y subdominios.*
- *Antes de utilizar la asignación de grupos, configure un Primary Username (Nombre de usuario principal) para las políticas de seguridad basadas en el usuario, dado que este atributo identificará a los usuarios en la configuración de la política, los logs y los informes.*

STEP 1 | Añada un perfil de servidor LDAP.

El perfil define cómo el cortafuegos conecta con los servidores de directorio desde los que recopila la información de asignación de grupo.



Si crea varias configuraciones de asignación de grupo que utilizan el mismo nombre distinguido (DN, Distinguished Name) base o servidor LDAP, las configuraciones de asignación de grupo no pueden contener grupos superpuestos (por ejemplo, la lista Incude (Incluir) para una configuración de asignación de grupo no puede contener un grupo que también esté en una configuración de asignación de grupo diferente).

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **LDAP** y luego **Add (Añadir)** para añadir un perfil de servidor.
2. Introduzca un **Profile Name (Nombre de perfil)** para identificar el perfil de servidor.
3. Seleccione **Add (Añadir)** para añadir los servidores LDAP. Puede añadir hasta cuatro servidores al mismo perfil, pero deben tener el mismo **Type**. Para cada servidor, ingrese un nombre en **Name** (para

© 2020 Palo Alto Networks, Inc.

identificar al servidor), una dirección IP del **LDAP Server (Servidor LDAP)** o FQDN, y un **Port (Puerto)** para el servidor (el valor predeterminado es 389).

4. Seleccione el **Type (Tipo)** de servidor.

   En función de su selección (tal como **active-directory**), el cortafuegos rellena automáticamente los atributos de LDAP correctos en los ajustes de asignación de grupo. Sin embargo, si ha personalizado su esquema de LDAP, puede que tenga que modificar los ajustes predeterminados.
5. En **Base DN**, seleccione el nombre distintivo (Distinguished Name, DN) de la ubicación del árbol LDAP donde desee que el cortafuegos comience su búsqueda de información de usuarios y grupos.
6. En **Bind DN (Enlazar DN)**, **Password (Contraseña)** y **Confirm Password (Confirmar contraseña)**, ingrese las credenciales de autenticación para el enlace al árbol LDAP.

   Bind DN puede ser un nombre LDAP totalmente cualificado (tal como `cn=administrador,cn=usuarios,dc=acme,dc=local`) o un nombre principal de usuario (tal como `administrator@acme.local`).
7. Ingrese el **Bind Timeout (Tiempo de espera de enlace)** y el **Search Timeout (Tiempo de espera de búsqueda)** en segundos (el valor predeterminado es 30 para ambos).
8. Haga clic en **OK (Aceptar)** para guardar el perfil de servidor.

STEP 2 | Configure los ajustes de servidor en una configuración de asignación de grupo.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Ajustes de asignación de grupo)**.
2. Seleccione **Add (Añadir)** para añadir la configuración de asignación de grupo.
3. En **Name (Nomre)** ingrese un nombre exclusivo para identificar la configuración de asignación de grupo.
4. Seleccione el **Server Profile** de LDAP que acaba de crear.
5. (Opcional) Especifique el **intervalo de actualización** (en segundos). Especifique un valor (el intervalo es de 60 a 86 400, el valor predeterminado es 3600) según la frecuencia con la que el cortafuegos debe verificar el origen LDAP para ver si hay actualizaciones en la configuración de asignación de grupos. Si el origen LDAP contiene muchos grupos, es posible que un valor demasiado bajo no proporcione suficiente tiempo para asignar todos los grupos.
6. (Opcional) Por defecto, el campo **User Domain (Dominio de usuario)** está en blanco: el cortafuegos detecta automáticamente los nombres de dominio para servidores de Active Directory (AD). Si introduce un valor, este sobrescribirá cualquier nombre de dominio que el cortafuegos recupera en el origen LDAP. Para la mayoría de las configuraciones, si necesita especificar un valor, introduzca el nombre de dominio NetBIOS (por ejemplo, **`example`**, no **`example.com`**).

   Si usa el catálogo global, si especifica un valor, se reemplaza el nombre de dominio para todos los usuarios y grupos de ese servidor, incluidos los de otros dominios.
7. (Opcional) Para filtrar los grupos que el cortafuegos rastrea para la asignación de grupos, en la sección Group Objects (Objetos del grupo), introduzca un **Search Filter (Filtro de búsqueda)** (consulta LDAP) y una **Object Class (Clase de objeto)** (definición de grupo).
8. (Opcional) Para filtrar los usuarios que el cortafuegos rastrea para la asignación de grupos, en la sección User Objects (Objetos del usuario), introduzca un **Search Filter (Filtro de búsqueda)** (consulta LDAP) y una **Object Class (Clase de objeto)** (definición de usuario).
9. Asegúrese de que la configuración de asignación de grupo esté **Enabled (Habilitada)** (opción predeterminada).

STEP 3 | (Opcional) Defina los atributos de usuario y grupo que se recopilarán para la asignación de usuario y grupo. Este paso es necesario si desea asignar los usuarios en función de atributos del directorio, en lugar de hacerlo según el dominio.

1. Si los orígenes de su ID de usuario únicamente envían el nombre de usuario y el nombre de usuario es único en la organización, seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuarios)** > **Setup (Configuración)** y haga clic en **Edit (Editar)**

© 2020 Palo Alto Networks, Inc.

para editar la sección Setup (Configuración), y haga clic en **Allow matching usernames without domains (Permitir nombres de usuario coincidentes sin dominios)** para permitir que el cortafuegos compruebe si los nombres de usuario únicos recopilados en el servidor LDAP durante la asignación de grupos coinciden con los usuarios asociados con una política y evitar sobreescribir el dominio en su perfil de origen.



Antes de habilitar esta opción, configure la asignación de grupos en el grupo de LDAP que incluye el origen de User-ID (como GlobalProtect o el portal de autenticación) que recopila las asignaciones. Tras confirmar los cambios, el origen de User-ID rellena los nombres de usuario sin dominios. Únicamente los nombres de usuario recopilados durante la asignación de usuarios pueden coincidir sin un dominio. Si los orígenes de ID de usuario envían información de usuario en varios formatos y habilita esta opción, verifique que los atributos recopilados por el cortafuegos posean un prefijo único. Para garantizar que los usuarios se identifiquen correctamente si habilita esta opción, todos los atributos de asignación de usuarios deben ser únicos. Si el nombre de usuario no es único, el cortafuegos registra un error en los logs de depuración.

2. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Group Mapping Settings (Configuración de asignación de grupos)** > **Add (Añadir)** > **User and Group Attributes (Atributos de usuarios y grupos)** > **User Attributes (Atributos de usuarios)** e introduzca en **Directory Attribute (Atributo de directorio)** el atributo que desea recopilar para la identificación del usuario. Especifique en **Primary Username (Nombre de usuario principal)** el nombre que permite identificar al usuario en el cortafuegos y representarlo en los informes y los logs; sustituye cualquier otro formato que reciba el cortafuegos del origen de User-ID.

   Cuando selecciona Server Profile (Perfil de servidor) > **Type (Tipo)**, el cortafuegos rellena automáticamente los valores de los atributos de los usuarios y los grupos. En función de la información del usuario que envían sus fuentes de ID de usuario, es posible que deba configurar los atributos correctos:

   - **User Principal Name (UPN) (Nombre principal del usuario)**: **`userPrincipalName`**
   - **NetBios Name (Nombre NetBios)**: **`sAMAccountName`**
   - **ID de correo electrónico**: Atributo de directorio para ese correo electrónico
   - **Varios formatos**: Recupere los atributos de asignación de usuarios del directorio de usuarios antes de habilitar los orígenes de su ID de usuario.

   Si no especifica ningún nombre de usuario principal, el cortafuegos emplea los siguientes valores predeterminados para cada tipo de perfil de servidor:

Atributo	Active Directory	Novell eDirectory o Sun ONE Directory Server
Primary Username (Nombre de usuario principal)	`sAMAccountName`	`uid`
E-Mail (Correo electrónico)	`mail`	`mail`
Alternate Username 1 (Nombre de usuario alternativo 1)	`userPrincipalName`	Ninguno.
Nombre de grupo	`name`	`cn`
Group Member (Miembro de grupo)	`member`	`member`

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Especifique un formato de dirección de **E-Mail (Correo electrónico)** y hasta tres formatos de **Alternate Username (nombre de usuario alternativo)**.
4. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Group Mapping Settings (Configuración de asignación de grupos)** > **Add (Añadir)** > **User and Group Attributes (Atributos de usuarios y grupos)** > **Group Attributes (Atributos de grupos)**. Especifique el nombre en **Group Name (Nombre de grupo)**, el miembro en **Group Member (Miembro de grupo)** y los formatos de direcciones en **E-Mail (Correo electrónico)**.

   Debe confirmarlo antes de que el cortafuegos recopile los atributos del directorio del servidor LDAP.

STEP 4 | Limita qué grupos estarán disponibles en las reglas de políticas.

Solo es obligatorio si desea limitar las reglas de políticas a grupos específicos. El máximo combinado para las listas **Group Include List (Lista de inclusión de grupos)** y **Custom Group (Grupo personalizado)** es de 640 entradas para cada configuración de asignación de grupo. Cada entrada debe ser un solo grupo o una lista de grupos. Por defecto, si no especifica grupos, todos los grupos están disponibles en reglas de políticas.



*Cualquier grupo personalizado que cree también estará disponible en la Lista de permitidos de perfiles de autenticación (*Configuración de una secuencia y perfil de autenticación*).*

1. Añada grupos existentes del servicio de directorio:
   1. Seleccione **Group Include List (Lista de inclusión de grupos)**.
   2. Seleccione los grupos disponibles que desea que aparezcan en las reglas de políticas y añádalos (⊞) a los grupos incluidos.
2. Si desea basar reglas de políticas en atributos de usuario que no coincidan con grupos de usuario existentes, cree grupos personalizados que se basen en filtros de LDAP:
   1. Seleccione **Custom Group (Grupo personalizado)** y **Add (Añadir)** para añadir el grupo.
   2. Introduzca un nombre de usuario en **Name** que sea único en la configuración de asignación de grupo para el cortafuegos o sistema virtual actual.

      Si el **Name (Nombre)** tiene el mismo valor que el nombre distintivo (DN) de un dominio de grupo AD existente, el cortafuegos usa el grupo personalizado en todas las referencias a ese nombre (por ejemplo, en políticas y logs).
   3. Especifique un **LDAP Filter** de hasta 2048 caracteres UTF-8 y haga clic en **OK**.

      El cortafuegos no valida los filtros LDAP, por lo que es labor suya asegurarse de que son precisos.

      Para minimizar el impacto del rendimiento en el servidor de directorio de LDAP, lo mejor es usar únicamente los atributos indizados en el filtro.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

   Debe confirmarlo antes de que los grupos personalizados estén disponibles en las políticas y los objetos.

STEP 5 | **Commit (Confirmar)** los cambios.

Debe confirmar los cambios antes de utilizar grupos personalizados en políticas y objetos, y antes de que el cortafuegos pueda recopilar los atributos del servidor LDAP.



Tras configurar el cortafuegos para recuperar información de asignación de grupos del servidor LDAP, pero antes de configurar las políticas en función de los grupos que recupera, se recomienda esperar a que el cortafuegos actualice el caché de asignación de grupos o actualizar el caché manualmente. Para verificar qué grupos puede utilizar

© 2020 Palo Alto Networks, Inc.

actualmente en las políticas, acceda a la CLI del cortafuegos y ejecute el comando ***show user group****. Para determinar cuándo el cortafuegos actualizará nuevamente la caché de asignación de grupos, ejecute el comando* ***show user group-mapping statistics*** *y compruebe* `Next Action`*. Para actualizar manualmente la caché, ejecute el comando* ***debug user-id refresh group-mapping all****.*

STEP 6 | Verifique que la asignación de usuarios y de grupos identifique a los usuarios correctamente.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping (Asignación de grupos)** > **Group Include List (Lista de inclusión de grupos)** para confirmar que el cortafuegos ha recuperado todos los grupos.
2. Para verificar que todos los atributos de usuario se capturen correctamente, utilice el siguiente comando de la CLI:

   ```
   show user user-attributes user all
   ```

   Se muestra el formato normalizado del nombre principal del usuario (UPN), el nombre de usuario principal, los atributos de correo electrónico y otros nombres de usuario alternativos configurados de todos los usuarios:

   ```
   admin@PA-VM-8.1> show user user-attributes user all
   ```

   ```
   Primary: nam\sam-user   Email: sam-user@nam.com
   ```

   ```
   Alt User Names:1) nam.com\sam-user
   ```

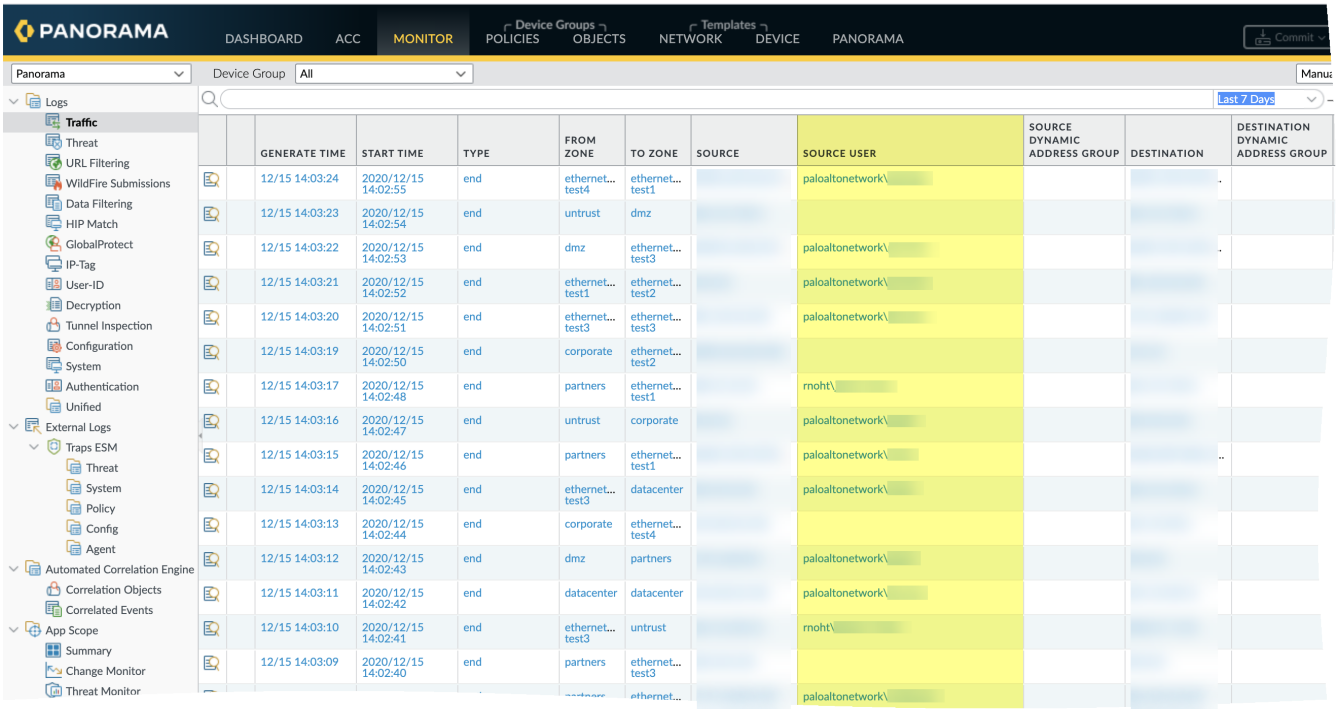
   ```
   2) nam\sam-user-upn
   ```

   ```
   3) sam-user-upn@nam.local
   ```

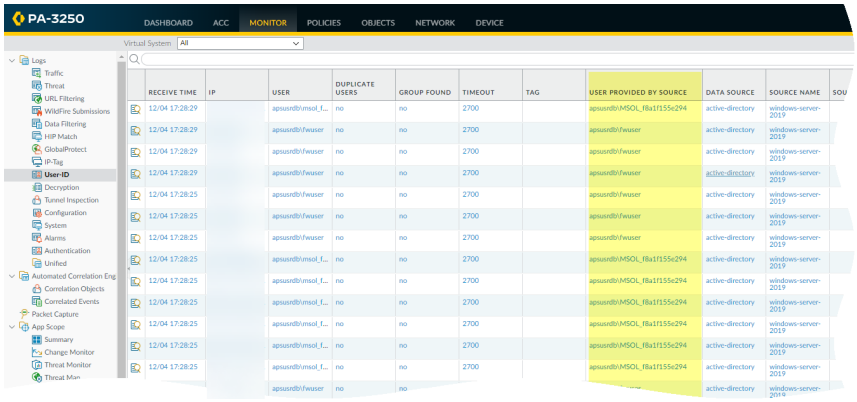
   ```
   4) sam-user@nam.com
   ```

3. Verifique que los nombres de usuario se muestren correctamente en la columna **Source User (Usuario de origen)** en **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.

© 2020 Palo Alto Networks, Inc.



4. Verifique que los usuarios se asignen a los nombres de usuario correctos en la columna **User Provided by Source (Usuario proporcionado por el origen)** en **Monitor (Supervisar)** > **Logs** > **User-ID (ID de usuario)**.



© 2020 Palo Alto Networks, Inc.

Asignación de direcciones IP a usuarios

User-ID ofrece numerosos métodos diferentes para la asignación de direcciones IP a nombres de usuarios. Antes de considerar la asignación de usuarios, tenga en cunta desde dónde inician sesión sus usuarios, los servicios a los que acceden, y las aplicaciones y datos que requieren control de acceso. Esto le proporcionará información sobre los tipos de agentes o integraciones que le permitirán identificar a sus usuarios mejor.

Cuando tenga un plan, podrá comenzar a configurar la asignación de usuarios utilizando uno o más de los siguientes métodos como sea necesario para permitir el acceso basado en los usuarios, y la visibilidad de las aplicaciones y los recursos:

- Si tiene usuarios con sistemas cliente que no hayan iniciado sesión en sus servidores de dominio (por ejemplo, usuarios que ejecuten clientes Linux que no inicien sesión en el dominio), puede realizar la Asignación de direcciones IP a nombres de usuario mediante un portal de autenticación. El uso del portal de autenticación junto con la política de autenticación también garantiza que todos los usuarios se autentiquen para acceder a sus aplicaciones y datos más delicados.
- Para asignar usuarios a medida que inician sesión en sus servidores Exchange, controladores de dominio, servidores eDirectory o clientes de Windows, debe configurar un agente de User-ID:
  - Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS
  - Configuración de la asignación de usuarios mediante el agente de User-ID de Windows
- Si tiene clientes que ejecuten sistemas multiusuario en un entorno Windows, como Microsoft Terminal Server, Citrix Metaframe Presentation Server o XenApp, Configuración del agente del servidor de terminal de Palo Alto Networks para la asignación de usuarios. En un sistema multiusuario que no se ejecuta en Windows, puede realizar la Recuperación de las asignaciones de usuario de un servidor de terminal utilizando la API de XML de PAN-OS.
- Para obtener asignaciones de usuarios a partir de servicios de red existentes que autentiquen usuarios, tales como controladores inalámbricos, dispositivos 802.1x, servidores Open Directory de Apple, servidores proxy u otros mecanismos de control de acceso a la red (Network Access Control, NAC), lleve a cabo la Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios.

  A pesar de que puede configurar el agente de Windows o el agente de User-ID integrado en PAN-OS en el cortafuegos para que escuche los mensajes syslog de autenticación de los servicios de red, dado que solo el agente integrado en PAN-OS admite el servicio de escucha mediante TLS, es la configuración recomendada.
- Para incluir el nombre de usuario y el dominio en los encabezados del tráfico saliente para que otros dispositivos de su red puedan identificar el usuario y aplicar la política basada en el usuario, puede Inserción de nombre de usuario en encabezados HTTP.
- Para compartir asignaciones, puede configurar un sistema virtual como núcleo de User-ID; consulte Asignaciones de User-ID compartidas entre sistemas virtuales.
- En el caso de otros clientes que no pueda asignar con otros métodos, puede optar por el Envío de asignaciones de usuarios a User-ID mediante la API XML.
- Una red a gran escala puede tener cientos de fuentes de información que los cortafuegos consultan para la asignación de usuarios y grupos, y puede tener numerosos cortafuegos que aplican políticas basadas en la información de asignación. Puede simplificar la administración de User-ID para dicha red al agregar la información de asignación antes de que los agentes de User-ID la recopilen. También puede reducir los recursos que usan los cortafuegos y las fuentes de información en el proceso de consulta, al configurar algunos cortafuegos para que redistribuyan la información de asignación. Para obtener información detallada, realice la Implementación de User-ID en una red a gran escala.

© 2020 Palo Alto Networks, Inc.

Creación de una cuenta de servicio exclusiva para el agente de User-ID

Si desea utilizar el agente de User-ID basado en Windows o el agente de User-ID integrado en PAN-OS para asignar usuarios a medida que inician sesión en sus servidores de Exchange, controladores de dominios, servidores de eDirectory o clientes de Windows, cree una cuenta de servicio dedicada para dicho agente en el controlador de cada uno de los dominios que deba supervisar.

El agente de User-ID asigna usuarios en función de los logs de eventos de seguridad. Para asegurarse de que el agente de User-ID pueda asignar correctamente a los usuarios, verifique que el origen de sus asignaciones genere logs para los eventos Audit Logon (Inicio de sesión de auditoría), Audit Kerberos Authentication Service (Servicio de autenticación de Kerberos de auditoría) y Audit Kerberos Service Ticket Operations (Operaciones de vales de servicio de Kerberos de auditoría). Como mínimo, el origen debe generar logs para los siguientes eventos:

- Logon Success (Inicio de sesión correcto) (4624)
- Authentication Ticket Granted (Vale de autenticación concedido) (4768)
- Service Ticket Granted (Vale de servicio concedido) (4769)
- Ticket Granted Renewed (Vale concedido renovado) (4770)

Los permisos necesarios para la cuenta de servicio dependen de los métodos y los ajustes de asignación de usuarios que planea utilizar. Por ejemplo, si está usando el agente de User-ID integrado en PAN-OS, la cuenta de servicio requiere privilegios de Server Operator (Operador de servidor) para supervisar sesiones de usuario. Si está usando el agente de User-ID basado en Windows, la cuenta de servicio no requiere privilegios de Server Operator (Operador de servidor) para supervisar sesiones de usuario. Para reducir el riesgo al que se expone la cuenta de servicio de User-ID, configúrela siempre con el conjunto mínimo de permisos que necesite el agente.

- Si desea instalar el agente basado en Windows en un servidor de Windows admitido, configure una cuenta de servicio para el agente de User-ID para Windows.
- Si desea utilizar el agente de PAN-OS en el cortafuegos, configure una cuenta de servicio para el agente de User-ID integrado en PAN-OS.

User-ID proporciona numerosos métodos para recopilar de manera segura la información de asignación de usuario. Para usar algunas funciones heredadas, diseñadas para entornos que solo necesitaban la asignación de usuarios en ordenadores con Windows conectados a la red local, hacen falta cuentas de servicio con privilegios. Si la cuenta de servicio con privilegios está en riesgo, podría dejar su red expuesta a ataques. No se recomienda usar las funciones heredadas que exigen privilegios que, en caso de verse comprometidos, suponen una amenaza, como el sondeo de clientes y la supervisión de sesiones.

Configuración de una cuenta de servicio para el agente de User-ID para Windows

Cree una cuenta de servicio de Active Directory (AD) dedicada para que el agente de User-ID para Windows acceda a los servicios y hosts que debe supervisar a fin de recopilar información sobre las asignaciones de usuarios. Debe crear una cuenta de servicio en cada dominio que el agente supervisará. Una vez habilitados los permisos necesarios en la cuenta de servicio, realice el procedimiento Configuración de la asignación de usuarios mediante el agente de User-ID de Windows.

El siguiente flujo de trabajo detalla todos los privilegios necesarios y proporciona orientación en relación con qué funciones de User-ID requieren privilegios que podrían suponer una

© 2020 Palo Alto Networks, Inc.

amenaza, de modo que usted pueda decidir cómo identificar mejor a los usuarios sin afectar su posición de seguridad en general.

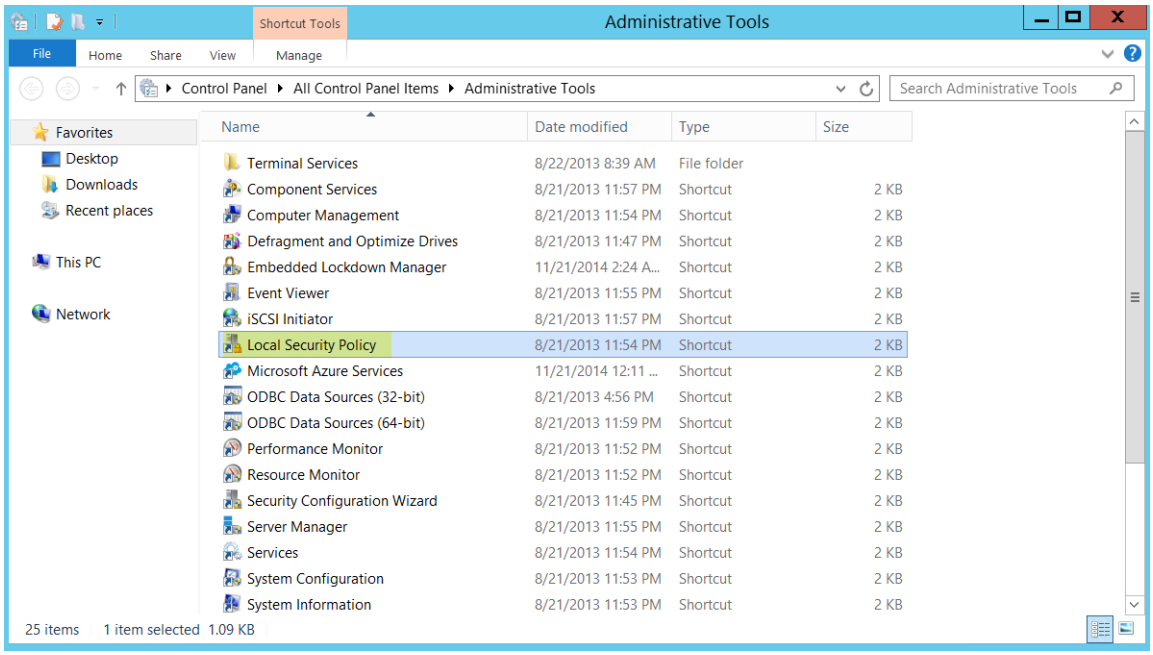
STEP 1 | Cree una cuenta de servicio de Active Directory (AD) para el agente de User-ID.

Debe crear una cuenta de servicio en cada dominio que el agente supervisará.

1. Inicie sesión en el controlador de dominio.
2. Haga clic con el botón derecho del ratón en el icono de Windows (), seleccione **Search (Buscar)** para buscar **`Active Directory Users and Computers`** e inicie la aplicación.
3. En el panel de navegación, abra el árbol de dominio, haga clic con el botón derecho en **Managed Service Accounts (Cuentas de servicio gestionadas)** y seleccione **New (Nuevo)** > **User (Usuario)**.
4. Introduzca el **First Name (Nombre)**, **Last Name (Apellido)** y **User logon name (Nombre de inicio de sesión de usuario)** del usuario y haga clic en **Next (Siguiente)**.
5. Introduzca la **Password (Contraseña)**, haga clic en **Confirm Password (Confirmar contraseña)** y luego haga clic en **Next (Siguiente)** y **Finish (Finalizar)**.

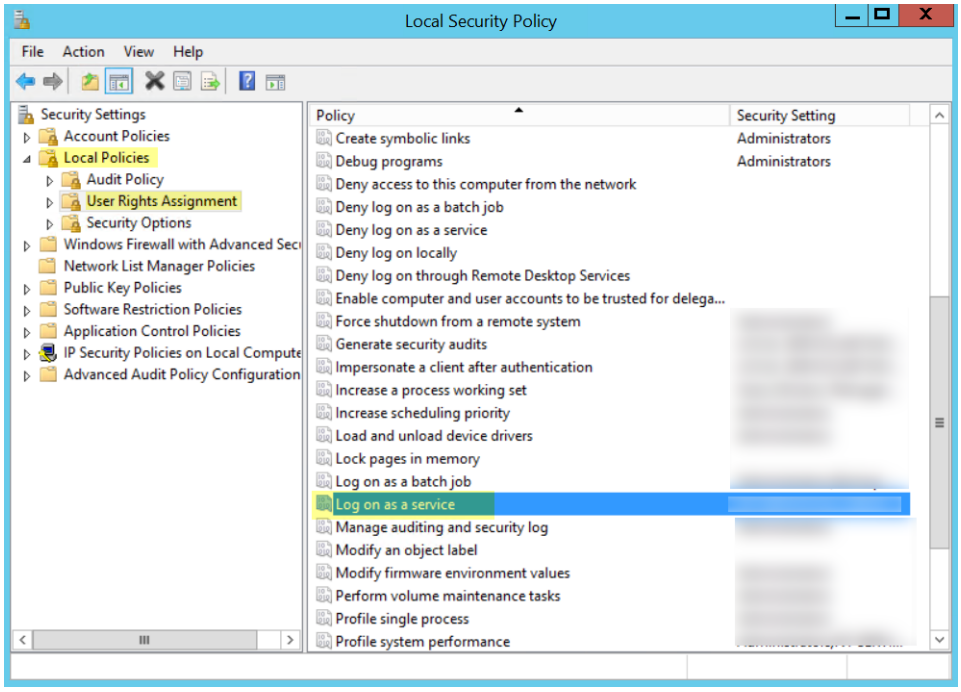
STEP 2 | Configure una política (directiva) local o de grupo para que la cuenta de servicio pueda iniciar sesión como servicio.

El permiso para iniciar sesión como un servicio solo es necesario localmente en el servidor de Windows que es el host del agente.

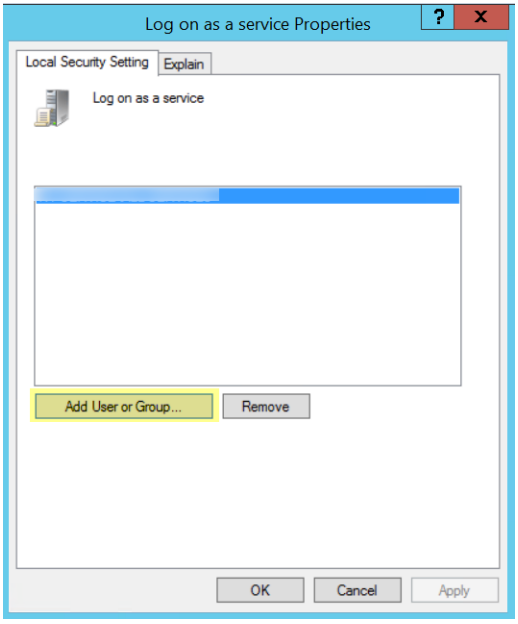
- Para asignar los permisos de forma local:
  1. Seleccione **Control Panel (Panel de control)** > **Administrative Tools (Herramientas administrativas)** > **Local Security Policy (Directiva de seguridad local)**.
  2. 

  3. Seleccione **Local Policies (Políticas locales)** > **User Rights Assignment (Asignación de derechos del usuario)** > **Log on as a service (Iniciar sesión como un servicio)**.

© 2020 Palo Alto Networks, Inc.

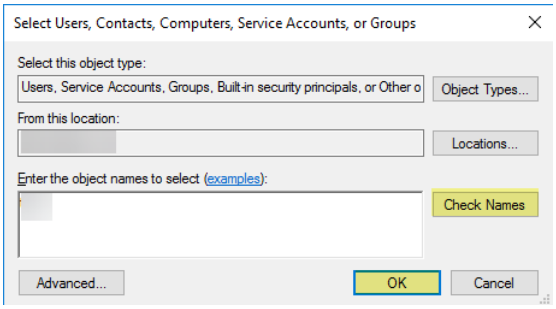


4. Seleccione **Add User or Group (Añadir usuario o grupo)** para añadir la cuenta de servicio.



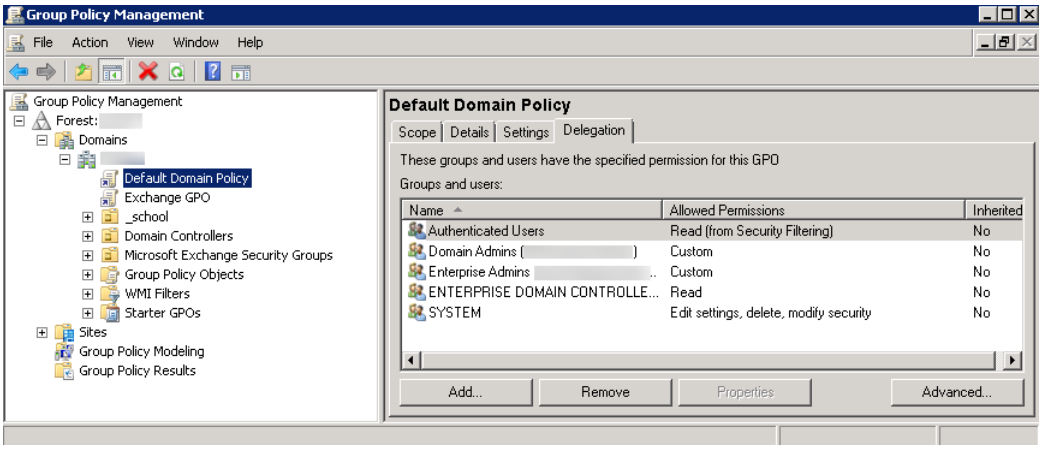
5. Introduzca el nombre de la cuenta de servicio en **Enter the object names to select (Escriba los nombres de objeto que desea seleccionar)** con el formato `dominio\nombre-usuario` y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

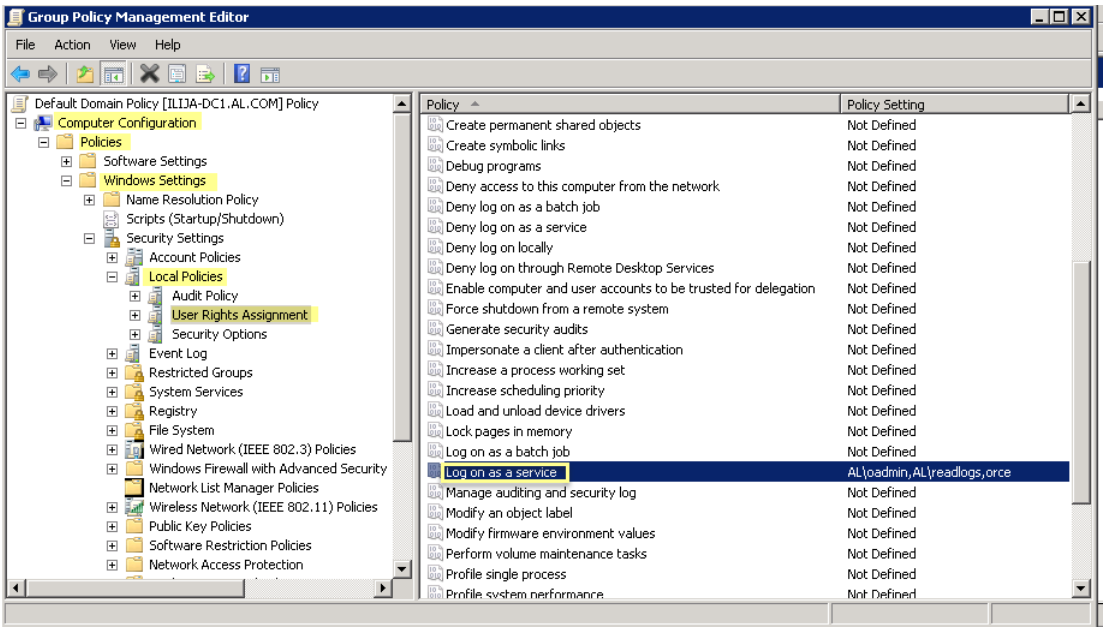


- Si pretende instalar los agentes de User-ID para Windows en varios servidores, use Group Policy Management Editor (Editor de administración de directivas de grupo) para configurar la política de grupo.

  1. Seleccione **Start (Inicio)** > **Group Policy Management (Administración de directivas de grupo)** > **<your domain>** > **Default Domain Policy (Directiva predeterminada de dominio)** > **Action (Acción)** > **Edit (Editar)** en el servidor de Windows que actúa como host del agente.



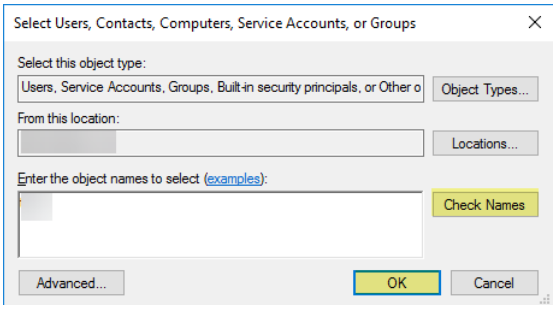
  2. Seleccione **Computer Configuration (Configuración del equipo)** > **Policies (Directivas)** > **Windows Settings (Configuración de Windows)** > **Security Settings (Configuración de seguridad)** > **Local Policies (Directivas locales)** > **User Rights Assignment (Asignación de derechos de usuario)**.



© 2020 Palo Alto Networks, Inc.

3. Haga clic con el botón derecho en **Log on as a service (Iniciar sesión como servicio)**, luego seleccione **Properties (Propiedades)**.
4. Haga clic en **Add User or Group (Agregar usuario o grupo)** para añadir el grupo integrado o el nombre de usuario de la cuenta de servicio y, luego, haga clic en **OK (Aceptar)** dos veces.

Los administradores tienen este privilegio de manera predeterminada.



STEP 3 | Si desea utilizar WMI para recopilar datos de los usuarios, asigne privilegios de DCOM a la cuenta de servicio, de modo que pueda realizar consultas de WMI en los servidores supervisados.

1. Seleccione **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **<your domain>** > **Builtin (Integrado)** > **Distributed COM Users (Usuarios COM distribuidos)**.
2. Haga clic con el botón derecho en **Properties (Propiedades)** > **Members (Miembros)** > **Add (Agregar)** e introduzca el nombre de la cuenta de servicio.

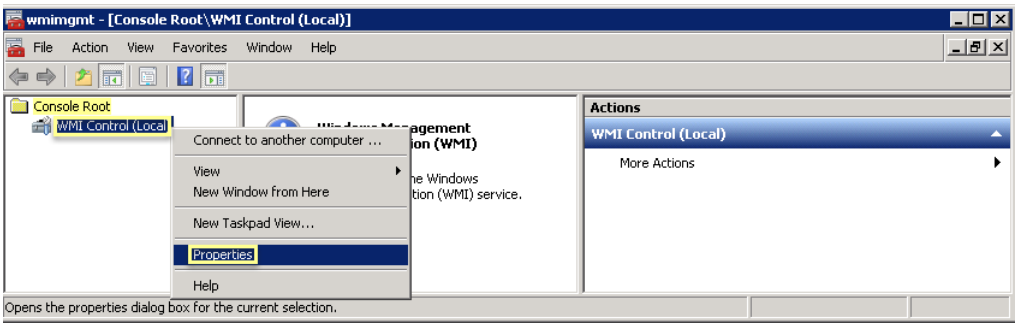
STEP 4 | Si planea utilizar el sondeo de WMI, habilite la cuenta para leer el espacio de nombres CIMV2 y asignar los permisos necesarios en los sistemas cliente que se deben sondear.

No habilite el sondeo de clientes en redes de alta seguridad. El sondeo de clientes puede generar una gran cantidad de tráfico de red y puede representar una amenaza de seguridad cuando no se configura correctamente. En su lugar, recopile información de asignación de usuarios de fuentes más aisladas y fiables, como controladores de dominio y a través de integraciones con Syslog o XML API, que tienen el beneficio adicional de permitir la captura segura de información de asignación de usuarios desde cualquier tipo de dispositivo o sistema operativo. Solo clientes de Windows.

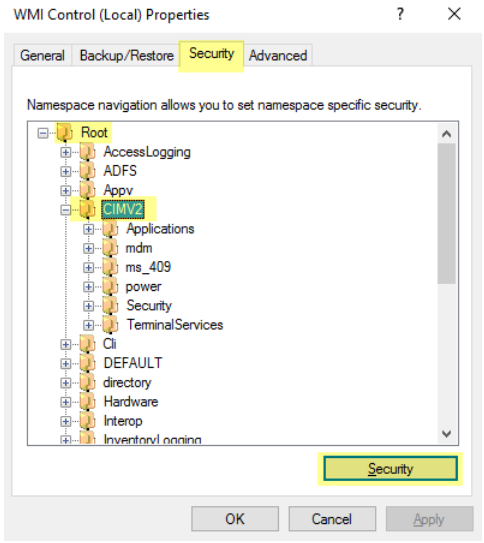
Realice esta tarea en cada sistema cliente que el agente de User-ID sondeará para la información de asignación de usuarios:

1. Haga clic con el botón derecho del ratón en el icono de Windows (), seleccione **Search (Buscar)** para buscar **`wmimgmt.msc`** e inicie la consola de gestión WMI.
2. En el árbol de la consola, haga clic con el botón derecho en **WMI Control (Control de WMI)** y seleccione **Properties (Propiedades)**.

© 2020 Palo Alto Networks, Inc.



3. Haga clic en la pestaña **Security (Seguridad)**, seleccione **Root (Raíz)** > **CIMV2** y haga clic en el botón **Security (Seguridad)**.

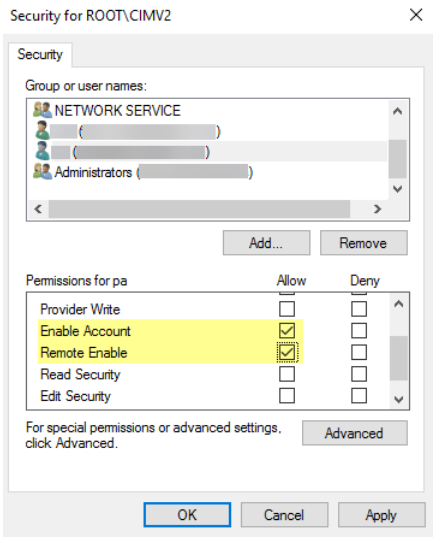


4. Seleccione **Add (Añadir)** para añadir el nombre de la cuenta de servicio que creó y luego **Check Names (Comprobar nombres)** para verificar su entrada, y haga clic en **OK (Aceptar)**.

   Es posible que deba cambiar las Locations (Ubicaciones) o hacer clic en Advanced (Avanzado) para consultar los nombres de cuenta. Consulte la ayuda del cuadro de diálogo para obtener más detalles.

5. En la sección Permissions for **<nombre-usuario>** (Permisos de [nombre-usuario]), haga clic en **Allow (Permitir)** y en los permisos **Enable Account (Habilitar cuenta)** y **Remote Enable (Llamada remota habilitada)**.

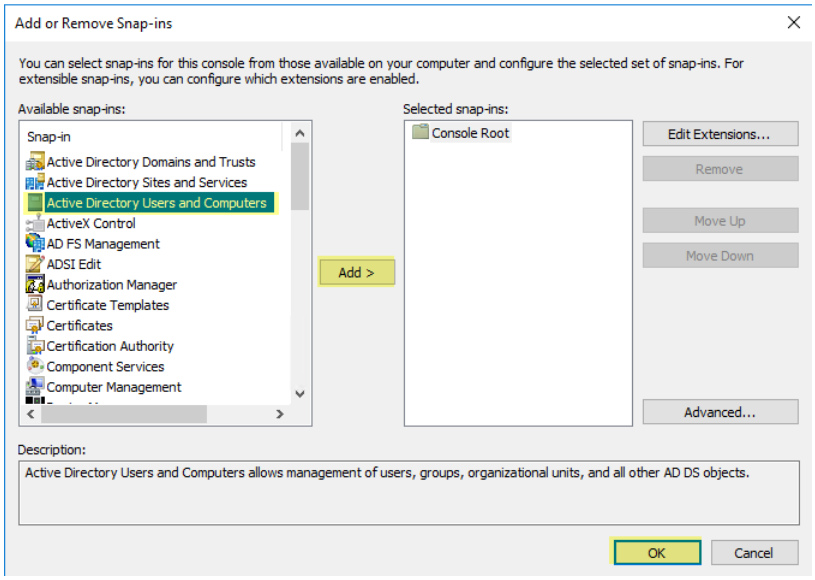
© 2020 Palo Alto Networks, Inc.



6. Haga clic en **OK** dos veces.
7. Utilice el complemento de MCC para usuarios locales y grupos (lusrmgr.msc) a fin de añadir la cuenta de servicio a los grupos locales de usuarios del modelo de objeto de componente distribuido (Distributed Component Object Model, DCOM) y usuarios de escritorio remoto en el sistema que se probará.

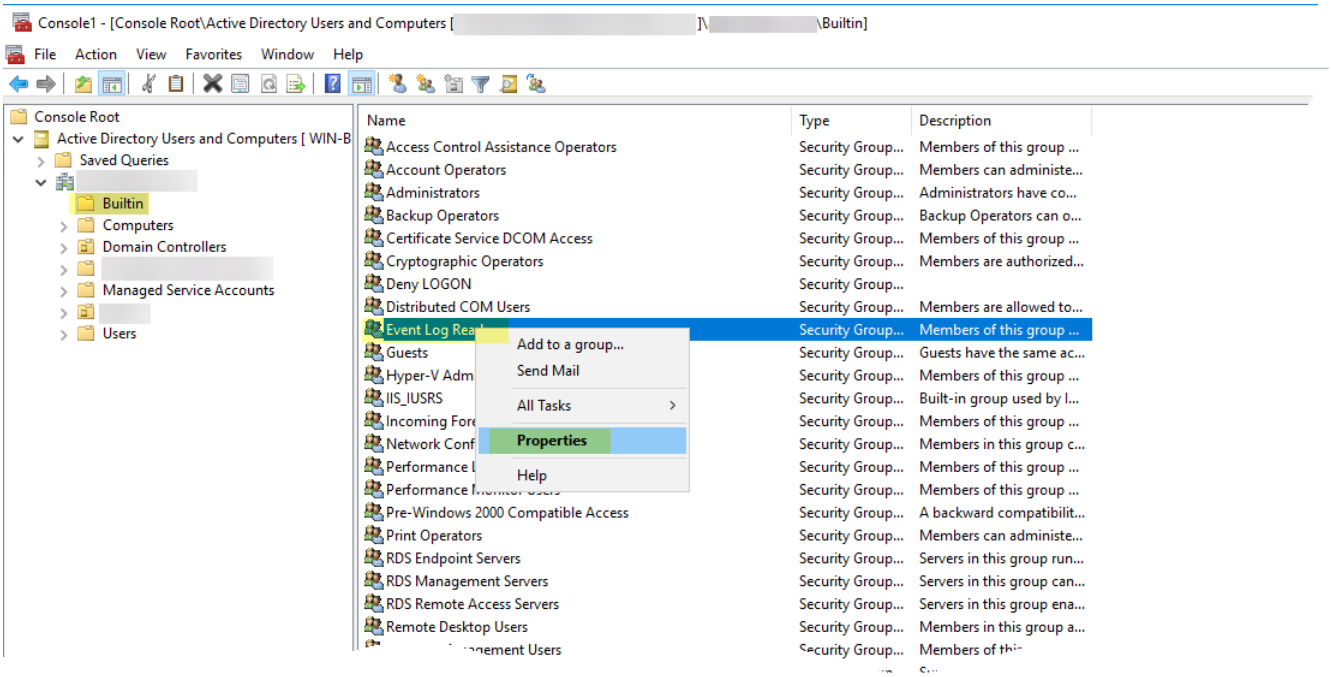
STEP 5 | Si desea usar la Monitorización de servidor para identificar a los usuarios, añada la cuenta de servicio al grupo integrado de lectores del registro de eventos para que pueda leer los eventos del log de seguridad.

1. En el controlador de dominio o servidor Exchange que contiene los logs que desea que el agente de User-ID lea, o en el servidor miembro que recibe eventos desde el reenvío de logs de Windows, seleccione **Start (Iniciar)** > **Run (Ejecutar)** y escriba **`MMC`**.
2. Seleccione **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **Add (Agregar)** y, a continuación, haga clic en **OK (Aceptar)** para ejecutar la MMC e iniciar el complemento Usuarios y equipos de Active Directory.

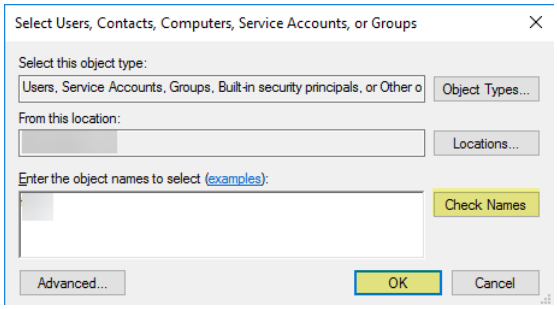


© 2020 Palo Alto Networks, Inc.

3. Desplácese hasta la carpeta Builtin (Integrado) del dominio, haga clic con el botón derecho en el grupo **Event Log Readers (Lectores del registro de eventos)** y seleccione **Properties (Propiedades)** > **Members (Miembros)**.



4. **Añada** la cuenta de servicio y, a continuación, haga clic en **Check Names (Comprobar nombres)** para validar que tiene el nombre de objeto adecuado.



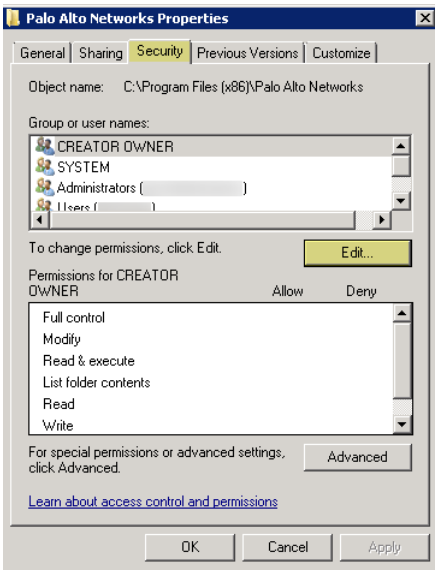
5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.
6. Confirme que en el grupo integrado Event Log Reader (Lector de logs de evento) aparece la cuenta de servicio como miembro (**Event Log Readers (Lectores de log de evento)** > **Properties (Propiedades)** > **Members (Miembros)**).

STEP 6 | Asigne los permisos de cuenta a la carpeta de instalación para permitir que la cuenta de servicio acceda a la carpeta de instalación del agente y pueda leer los logs de escritura y configuración.

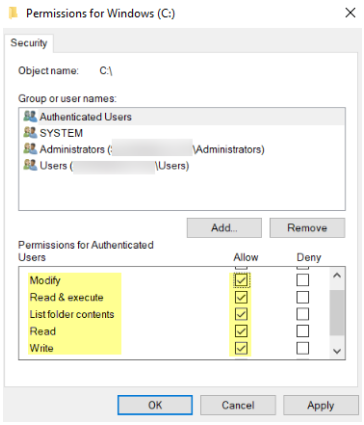
Solo debe realizar este paso si la cuenta de servicio que configuró para el agente de User-ID no es un administrador de dominio ni un administrador local en el host de servidor del agente de User-ID.

1. En Windows Explorer (Explorador de Windows), desplácese hasta **`C:\Program Files(x86)\Palo Alto Networks (C:\Archivos de programa [x86]\Palo Alto Networks)`**, haga clic con el botón derecho en la carpeta y seleccione **Properties (Propiedades)**.
2. En la pestaña **Security (Seguridad)**, haga clic en **Edit (Editar)**.

© 2020 Palo Alto Networks, Inc.



3. Haga clic en **Add (Agregar)** para añadir la cuenta de servicio del agente de User-ID y haga clic en **Allow (Permitir)** en los permisos **Modify (Modificar)**, **Read & execute (Lectura y ejecución)**, **List folder contents (Mostrar el contenido de la carpeta)**, **Read (Lectura)** y **Write (Escritura)**. A continuación, haga clic en **OK (Aceptar)** para guardar la configuración de la cuenta.

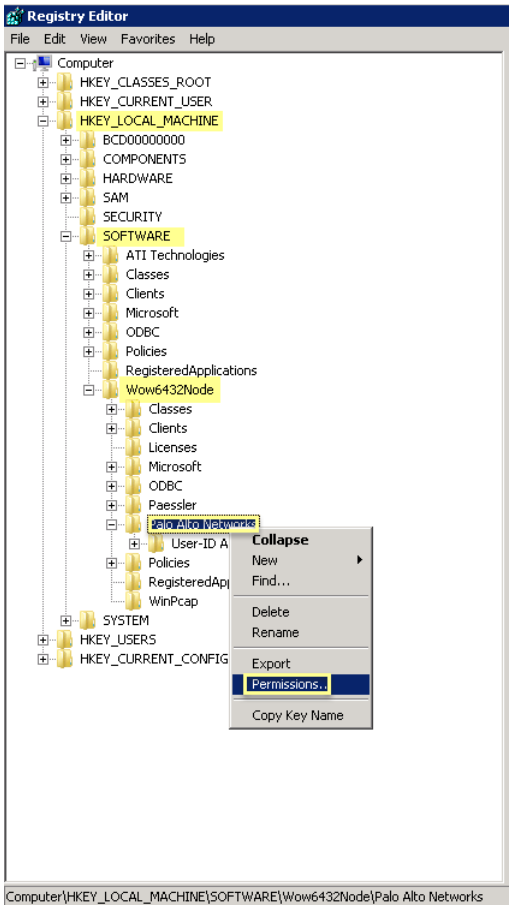


Si no desea configurar permisos individuales, haga clic en Allow (Permitir) y en el permiso Full Control (Control total).

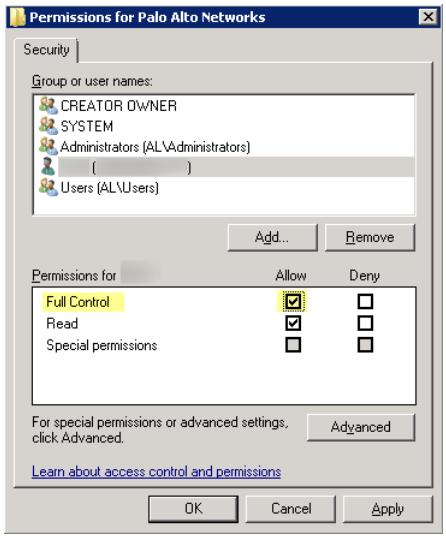
STEP 7 | Si desea que el agente pueda aplicar cambios en la configuración (por ejemplo, si selecciona otro nivel de creación de logs), conceda a la cuenta de servicio permisos en el subárbol de registro del agente de User-ID.

1. Seleccione **Start (Inicio)** > **Run (Ejecutar)**, introduzca **`regedt32`** y desplácese al subárbol Palo Alto Networks, que se encuentra en una de estas ubicaciones:
   - **Sistemas de 32 bits**: `HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`
   - **Sistemas de 64 bits**: `HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. Haga clic con el botón derecho en el nodo **Palo Alto Networks** y seleccione **Permissions (Permisos)**.

© 2020 Palo Alto Networks, Inc.



3. Asigne a la cuenta de servicio de User-ID **Full Control (Control completo)** y, a continuación, haga clic en **OK (Aceptar)** para guardar el ajuste.



STEP 8 | Deshabilite los privilegios de la cuenta de servicio que no sean imprescindibles.

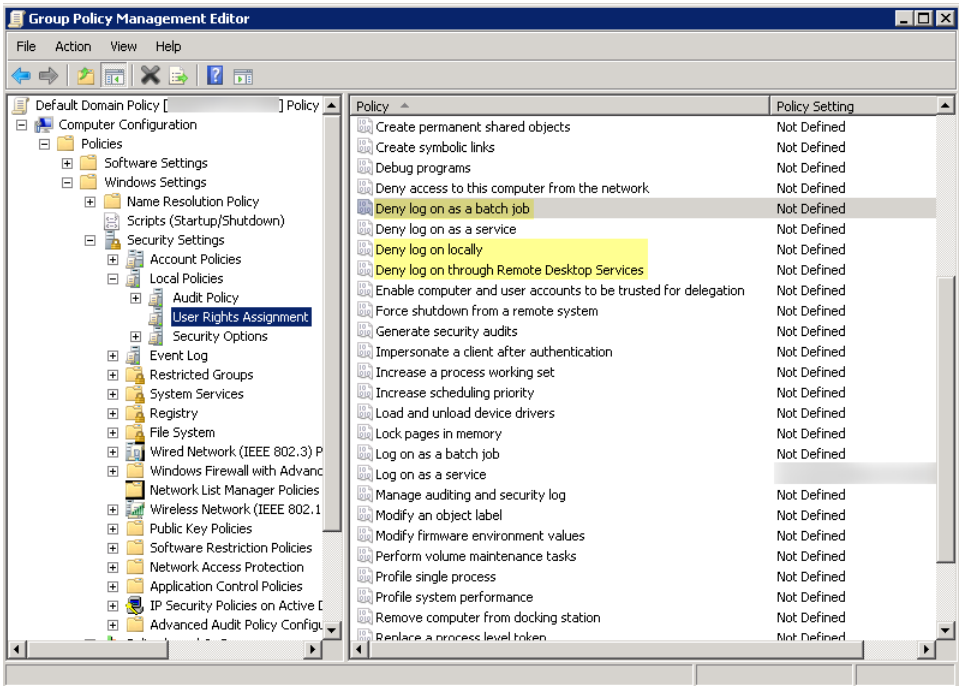
Al garantizar que la cuenta de servicio de User-ID tenga el conjunto mínimo de privilegios de cuenta, puede reducir la superficie de ataque en caso de que la cuenta sea alterada.

© 2020 Palo Alto Networks, Inc.

Para garantizar que la cuenta de User-ID tenga los mínimos privilegios necesarios, deniegue los privilegios siguientes en la cuenta.

- **Denegar el inicio de sesión interactivo para la cuenta de servicio de User-ID**: si bien la cuenta de servicio de User-ID necesita permiso para leer y analizar los logs de eventos de seguridad de Active Directory, no requiere la capacidad de inicio de sesión en los servidores o sistemas de dominio de forma interactiva. Usted puede limitar este privilegio al utilizar políticas de grupo o al utilizar una cuenta de servicio gestionado (consulte Microsoft TechNet para obtener más información).

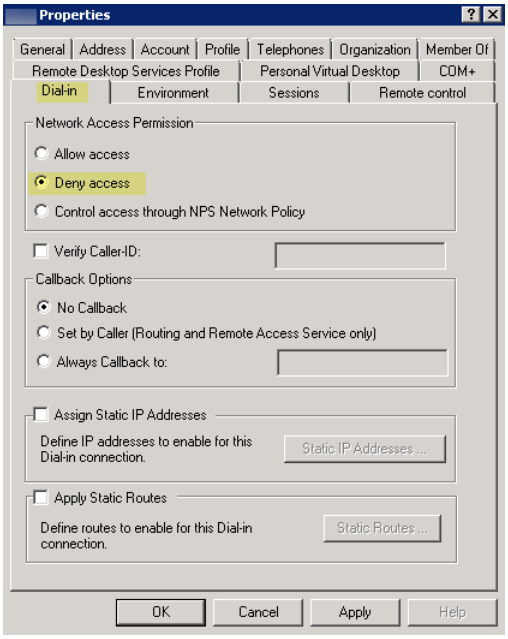
  1. Seleccione **Group Policy Management Editor (Editor de administración de directivas de grupo)** > **Default Domain Policy (Directiva predeterminada de dominio)** > **Computer Configuration (Configuración del equipo)** > **Policies (Directivas)** > **Windows Settings (Configuración de Windows)** > **Security Settings (Configuración de seguridad)** > **User Rights Assignment (Asignación de derechos de usuario)**.
  2. En **Deny log on as a batch job (Denegar el inicio de sesión como trabajo por lotes)**, **Deny log on locally (Denegar el inicio de sesión local)** y **Deny log on through Remote Desktop Services (Denegar inicio de sesión a través de Servicios de Escritorio remoto)**, haga clic con el botón derecho en **Properties (Propiedades)**.
  3. Seleccione **Define these policy settings (Definir esta configuración de directiva)** > **Add User or Group (Agregar usuario o grupo)**, añada el nombre de la cuenta de servicio y haga clic en **OK (Aceptar)**.



- **Denegar el acceso remoto para la cuenta de servicio de User-ID**: esto impide que un atacante utilice la cuenta para acceder a la red desde el exterior de la red.

  1. Seleccione **Start (Inicio)** > **Run (Ejecutar)**, introduzca `MMC` y seleccione **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **Users (Usuarios)**.
  2. Haga clic con el botón derecho en el nombre de la cuenta de servicio y seleccione **Properties (Propiedades)**.
  3. Seleccione **Dial-in (Marcado)** y, en **Network Access Permission (Permiso de acceso a redes)**, seleccione **Deny access (Denegar acceso)**.

© 2020 Palo Alto Networks, Inc.



STEP 9 | A continuación, siga el procedimiento Configuración de la asignación de usuarios mediante el agente de User-ID de Windows.

Configuración de una cuenta de servicio para el agente de User-ID integrado en PAN-OS

Cree una cuenta de servicio de Active Directory (AD) dedicada para que el agente de User-ID integrado en PAN-OS acceda a los servicios y hosts que debe supervisar a fin de recopilar información sobre las asignaciones de usuarios. Tiene que crear una cuenta de servicio en cada uno de los dominios que deba supervisar el agente. Una vez habilitados los permisos necesarios en la cuenta de servicio, realice el procedimiento Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.

El siguiente flujo de trabajo detalla todos los privilegios necesarios y proporciona orientación en relación con qué funciones de User-ID requieren privilegios que podrían suponer una amenaza, de modo que usted pueda decidir cómo identificar mejor a los usuarios sin afectar su posición de seguridad en general.

STEP 1 | Cree una cuenta de servicio de Active Directory (AD) para el agente de User-ID.

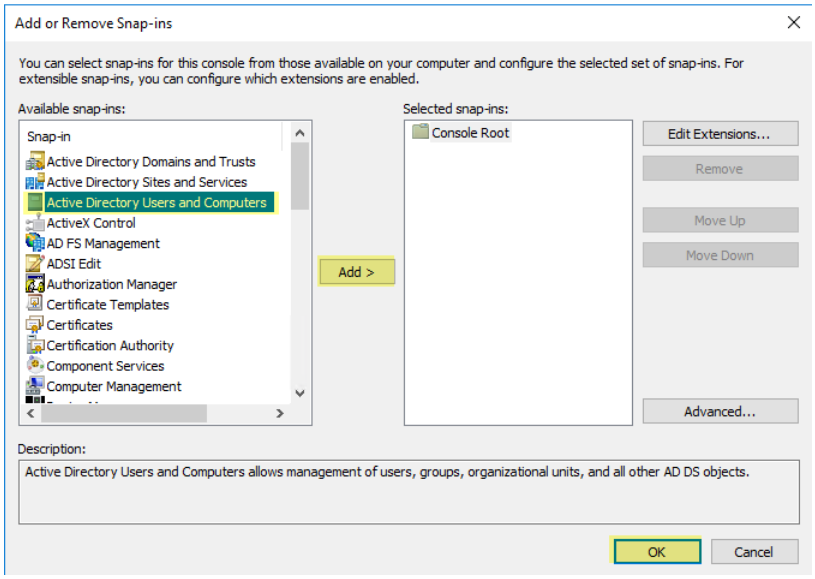
Debe crear una cuenta de servicio en cada dominio que el agente supervisará.

1. Inicie sesión en el controlador de dominio.
2. Haga clic con el botón derecho del ratón en el icono de Windows (), seleccione **Search (Buscar)** para buscar **`Active Directory Users and Computers`** e inicie la aplicación.
3. En el panel de navegación, abra el árbol de dominio, haga clic con el botón derecho en **Managed Service Accounts (Cuentas de servicio gestionadas)** y seleccione **New (Nuevo)** > **User (Usuario)**.
4. Introduzca el **First Name (Nombre)**, **Last Name (Apellido)** y **User logon name (Nombre de inicio de sesión de usuario)** del usuario y haga clic en **Next (Siguiente)**.
5. Introduzca la **Password (Contraseña)**, haga clic en **Confirm Password (Confirmar contraseña)** y luego haga clic en **Next (Siguiente)** y **Finish (Finalizar)**.

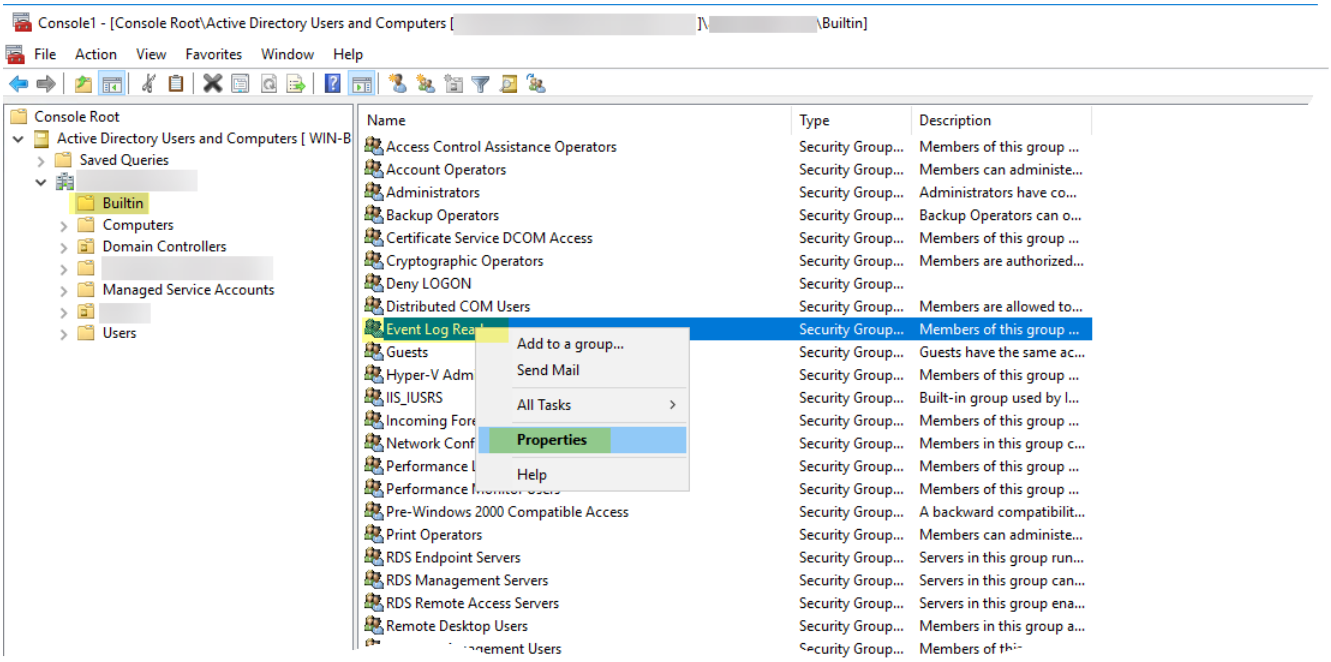
© 2020 Palo Alto Networks, Inc.

STEP 2 | Si desea usar la Monitorización de servidor para identificar a los usuarios, añada la cuenta de servicio al grupo integrado de lectores del registro de eventos para que pueda leer los eventos del log de seguridad.

1. En el controlador de dominio o servidor Exchange que contiene los logs que desea que el agente de User-ID lea, o en el servidor miembro que recibe eventos desde el reenvío de logs de Windows, seleccione **Start (Iniciar)** > **Run (Ejecutar)** y escriba `MMC`.
2. Seleccione **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **Add (Agregar)** y, a continuación, haga clic en **OK (Aceptar)** para ejecutar la MMC e iniciar el complemento Usuarios y equipos de Active Directory.

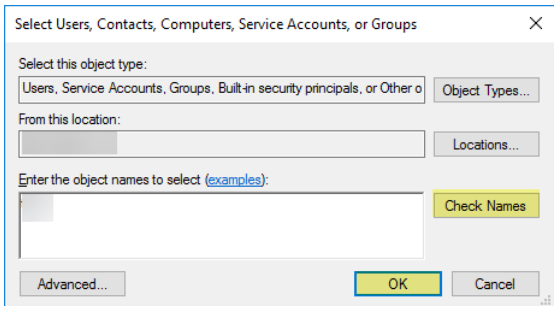


3. Desplácese hasta la carpeta Builtin (Integrado) del dominio, haga clic con el botón derecho en el grupo **Event Log Readers (Lectores del registro de eventos)** y seleccione **Properties (Propiedades)** > **Members (Miembros)**.



© 2020 Palo Alto Networks, Inc.

4. **Añada** la cuenta de servicio y, a continuación, haga clic en **Check Names (Comprobar nombres)** para validar que tiene el nombre de objeto adecuado.



5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.
6. Confirme que en el grupo integrado Event Log Reader (Lector de logs de evento) aparece la cuenta de servicio como miembro (**Event Log Readers (Lectores de log de evento)** > **Properties (Propiedades)** > **Members (Miembros)**).

STEP 3 | Si desea utilizar WMI para recopilar datos de los usuarios, asigne privilegios de DCOM a la cuenta de servicio, de modo que pueda realizar consultas de WMI en los servidores supervisados.

1. Seleccione **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **<your domain>** > **Builtin (Integrado)** > **Distributed COM Users (Usuarios COM distribuidos)**.
2. Haga clic con el botón derecho en **Properties (Propiedades)** > **Members (Miembros)** > **Add (Agregar)** e introduzca el nombre de la cuenta de servicio.

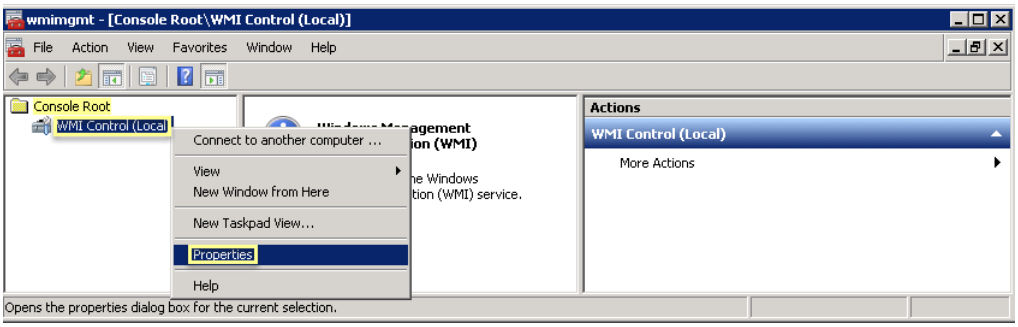
STEP 4 | Si piensa usar el sondeo de WMI, habilite la cuenta de servicio para leer el espacio de nombres CIMV2 en los controles de dominio que dese supervisar y asigne los permisos necesarios en los sistemas cliente que se deben sondear.

No habilite el sondeo de clientes en redes de alta seguridad. El sondeo de clientes puede generar una gran cantidad de tráfico de red y puede representar una amenaza de seguridad cuando no se configura correctamente. En su lugar, recopile información de asignación de usuarios de fuentes más aisladas y fiables, como controladores de dominio y a través de integraciones con Syslog o XML API, que tienen el beneficio adicional de permitir la captura segura de información de asignación de usuarios desde cualquier tipo de dispositivo o sistema operativo. Solo clientes de Windows.

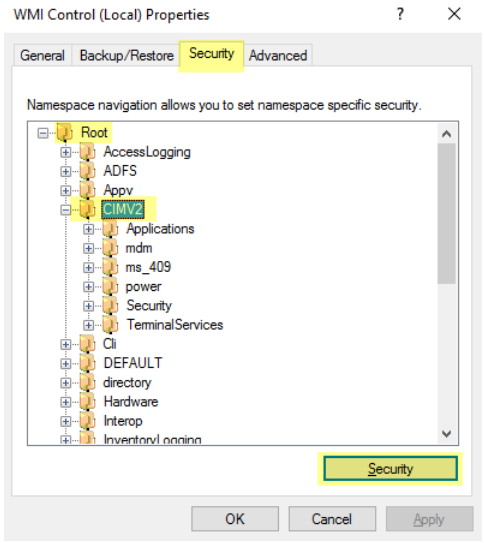
Realice esta tarea en cada sistema cliente que el agente de User-ID sondeará para la información de asignación de usuarios:

1. Haga clic con el botón derecho del ratón en el icono de Windows (), seleccione **Search (Buscar)** para buscar **`wmimgmt.msc`** e inicie la consola de gestión WMI.
2. En el árbol de la consola, haga clic con el botón derecho en **WMI Control (Control de WMI)** y seleccione **Properties (Propiedades)**.

© 2020 Palo Alto Networks, Inc.



3. Haga clic en la pestaña **Security (Seguridad)**, seleccione **Root (Raíz)** > **CIMV2** y haga clic en el botón **Security (Seguridad)**.

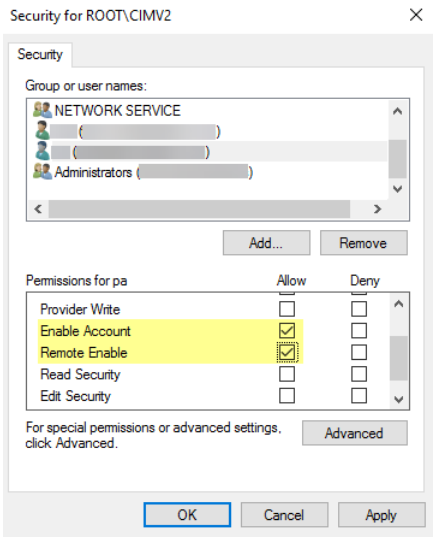


4. Seleccione **Add (Añadir)** para añadir el nombre de la cuenta de servicio que creó y luego **Check Names (Comprobar nombres)** para verificar su entrada, y haga clic en **OK (Aceptar)**.

   Es posible que deba cambiar las Locations (Ubicaciones) o hacer clic en Advanced (Avanzado) para consultar los nombres de cuenta. Consulte la ayuda del cuadro de diálogo para obtener más detalles.

5. En la sección Permissions for **<nombre-usuario>** (Permisos de [nombre-usuario]), haga clic en **Allow (Permitir)** y en los permisos **Enable Account (Habilitar cuenta)** y **Remote Enable (Llamada remota habilitada)**.

© 2020 Palo Alto Networks, Inc.



6. Haga clic en **OK** dos veces.
7. Utilice el complemento de MCC para usuarios locales y grupos (lusrmgr.msc) a fin de añadir la cuenta de servicio a los grupos locales de usuarios del modelo de objeto de componente distribuido (Distributed Component Object Model, DCOM) y usuarios de escritorio remoto en el sistema que se probará.

STEP 5 | (No recomendado) Si desea permitir que el agente supervise las sesiones de los usuarios para sondear los servidores de Windows en busca de información sobre las asignaciones de usuarios, asigne los privilegios de Server Operator (Operador de servidor) a la cuenta de servicio.

Debido a que este grupo también tiene privilegios para apagar y reiniciar servidores, asígnele la cuenta solo si la supervisión de las sesiones de usuario es muy importante.

1. Seleccione **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **<your domain>** > **Builtin (Integrado)** > **Server Operators (Operadores de servidor)**.
2. Haga clic con el botón derecho en **Properties (Propiedades)** > **Members (Miembros)** > **Add (Agregar)** y añada el nombre de la cuenta de servicio.

STEP 6 | Deshabilite los privilegios de la cuenta de servicio que no sean imprescindibles.

Al garantizar que la cuenta de servicio de User-ID tenga el conjunto mínimo de privilegios de cuenta, puede reducir la superficie de ataque en caso de que la cuenta sea alterada.

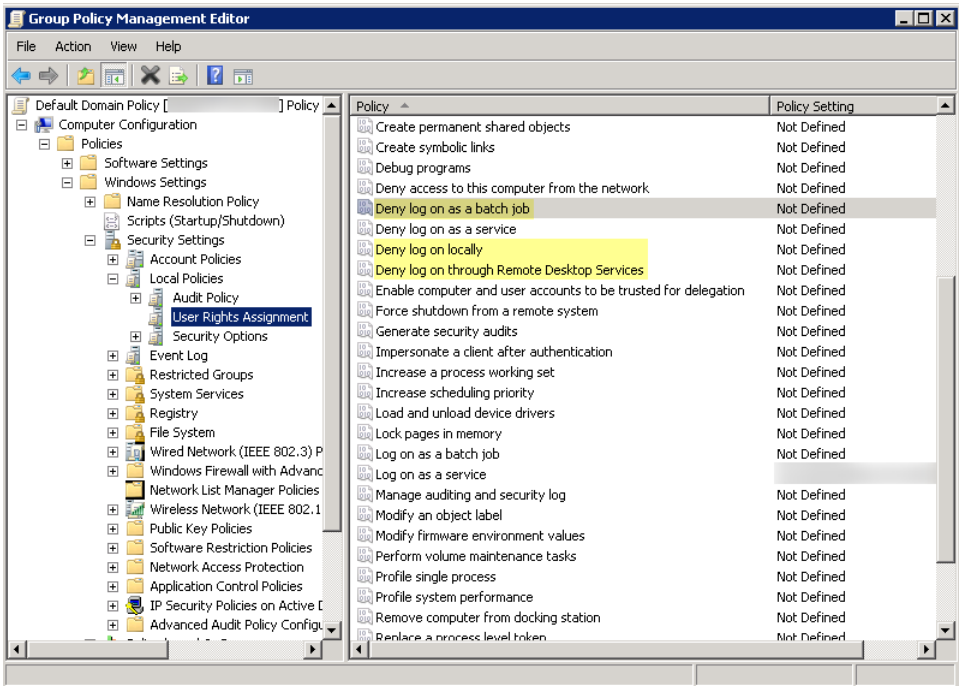
Para garantizar que la cuenta de User-ID tenga los mínimos privilegios necesarios, deniegue los siguientes privilegios en la cuenta:

- **Denegar el inicio de sesión interactivo para la cuenta de servicio de User-ID**: si bien la cuenta de servicio de User-ID necesita permiso para leer y analizar los logs de eventos de seguridad de Active Directory, no requiere la capacidad de inicio de sesión en los servidores o sistemas de dominio de forma interactiva. Usted puede limitar este privilegio al utilizar políticas de grupo o al utilizar una cuenta de servicio gestionado (consulte Microsoft TechNet para obtener más información).

  1. Seleccione **Group Policy Management Editor (Editor de administración de directivas de grupo)** > **Default Domain Policy (Directiva predeterminada de dominio)** > **Computer Configuration (Configuración del equipo)** > **Policies (Directivas)** > **Windows Settings (Configuración de Windows)** > **Security Settings (Configuración de seguridad)** > **User Rights Assignment (Asignación de derechos de usuario)**.

© 2020 Palo Alto Networks, Inc.

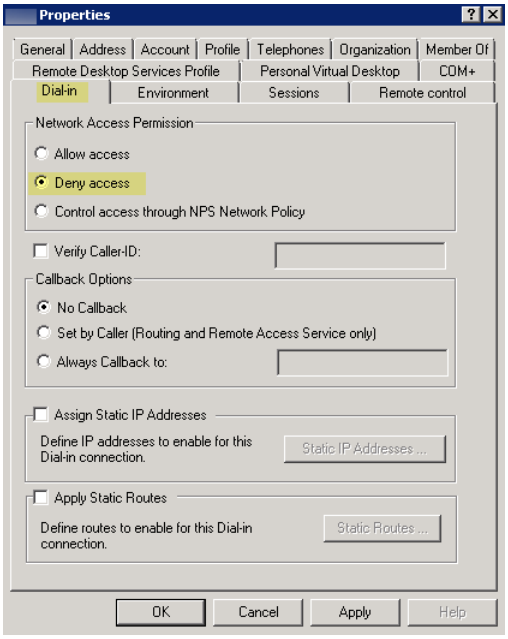
2. En **Deny log on as a batch job (Denegar el inicio de sesión como trabajo por lotes)**, **Deny log on locally (Denegar el inicio de sesión local)** y **Deny log on through Remote Desktop Services (Denegar inicio de sesión a través de Servicios de Escritorio remoto)**, haga clic con el botón derecho en **Properties (Propiedades)**. A continuación, seleccione **Define these policy settings (Definir esta configuración de directiva)** > **Add User or Group (Agregar usuario o grupo)**, añada el nombre de la cuenta de servicio y haga clic en **OK (Aceptar)**.



- **Denegar el acceso remoto para la cuenta de servicio de User-ID**: esto impide que un atacante utilice la cuenta para acceder a la red desde el exterior de la red.

  1. Seleccione **Start (Inicio)** > **Run (Ejecutar)**, introduzca **`MMC`** y seleccione **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Active Directory Users and Computers (Usuarios y equipos de Active Directory)** > **Users (Usuarios)**.
  2. Haga clic con el botón derecho en el nombre de la cuenta de servicio y seleccione **Properties (Propiedades)**.
  3. Seleccione **Dial-in (Marcado)** y, en **Network Access Permission (Permiso de acceso a redes)**, seleccione **Deny access (Denegar acceso)**.

© 2020 Palo Alto Networks, Inc.



STEP 7 | A continuación, siga el procedimiento Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.

Configuración de la asignación de usuarios mediante el agente de User-ID de Windows

En la mayoría de los casos, la gran parte de los usuarios de su red tendrán inicios de sesión en sus servicios de dominio supervisados. Para estos usuarios, el agente de User-ID de Palo Alto Networks supervisa los servidores en busca de eventos de inicio de sesión y realiza la asignación de direcciones IP a nombres de usuarios. El modo en que configure el agente de User-ID dependerá del tamaño de su entorno y la ubicación de sus servidores de dominio. La práctica recomendada es que ubique a sus agentes de User-ID cerca de los servidores que supervisarán (es decir, los servidores supervisados y el agente de User-ID de Windows no deberían estar separados por un enlace WAN). Esto se debe a que la mayor parte del tráfico para la asignación de usuarios se produce entre el agente y el servidor supervisado, y únicamente una pequeña cantidad del tráfico (la diferencia de asignaciones de usuarios desde la última actualización) se produce desde el agente al cortafuegos.

Los siguientes temas describen cómo instalar y configurar el agente de User-ID y cómo configurar el cortafuegos para que recupere información de asignación de usuarios del agente:

- Instalación del agente de User-ID basado en Windows
- Configuración del agente de User-ID de Windows para la asignación de usuarios

Instalación del agente de User-ID basado en Windows

El siguiente procedimiento muestra cómo instalar el agente de User-ID en un servidor miembro en el dominio y configurar la cuenta de servicio con los permisos obligatorios. Si está realizando una actualización, el instalador eliminará automáticamente la versión anterior; no obstante, es conveniente hacer una copia de seguridad del archivo config.xml antes de ejecutar el instalador.

Para obtener información sobre los requisitos del sistema para instalar el agente de User-ID basado en Windows y para obtener información sobre las versiones admitidas del SO del

© 2020 Palo Alto Networks, Inc.

servidor, consulte las Notas de la versión del agente de User-ID *y la* Matriz de compatibilidad de Palo Alto Networks.

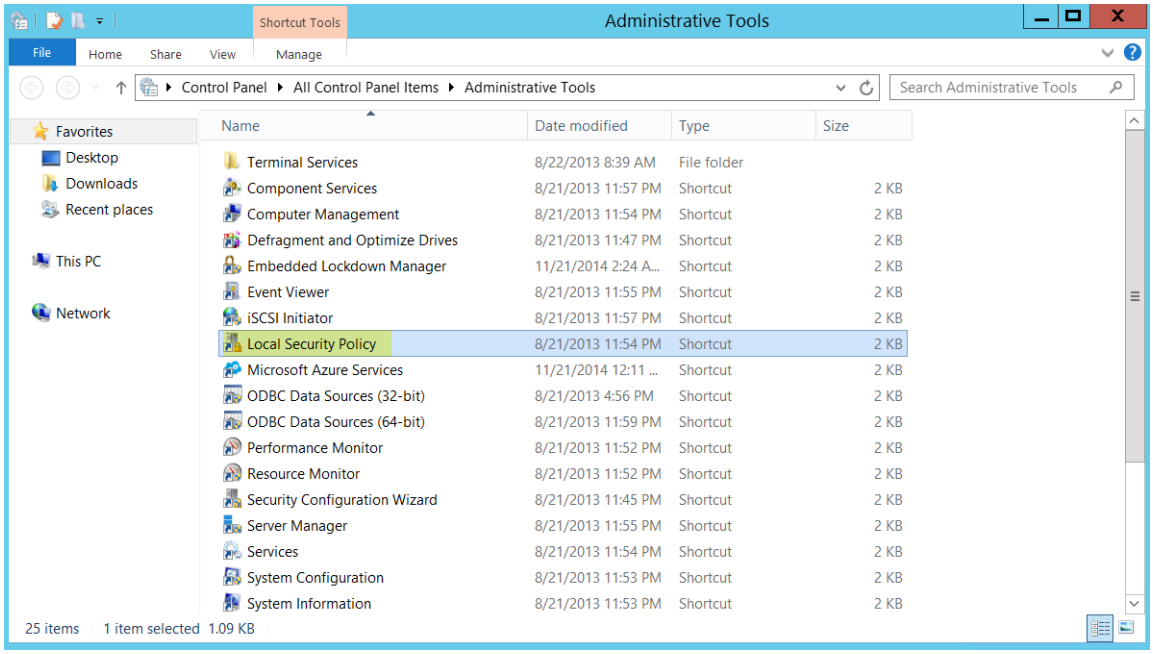
STEP 1 | Cree una cuenta de servicio de Active Directory exclusiva para que el agente de User-ID acceda a los servicios y hosts que supervisará para recopilar información de asignación de usuarios.

Cree una cuenta de servicio dedicada para el agente de User-ID y conceda los permisos necesarios para el agente de User-ID de Windows.

1. Habilite la cuenta de servicio para iniciar sesión como un servicio configurando una política local o de grupo.
    1. Para configurar la política de grupo si está instalando agentes de User-ID basados en Windows en varios servidores, seleccione **Group Policy Management (Gestión de política de grupo)** > **Default Domain Policy (Política de dominio predeterminada)** > **Computer Configuration (Configuración del ordenador)** > **Policies (Políticas)** > **Windows Settings (Configuración de Windows)** > **Security Settings (Configuración de seguridad)** > **Local Policies (Políticas locales)** > **User Rights Assignment (Asignación de derechos del usuario)** para el servidor Windows que es el host de agente.
    2. Haga clic con el botón derecho en **Log on as a service (Iniciar sesión como servicio)**, luego seleccione **Properties (Propiedades)**.
    3. Añada el nombre de usuario de la cuenta de servicio o el grupo integrado (administradores que tienen este privilegio de manera predeterminada).

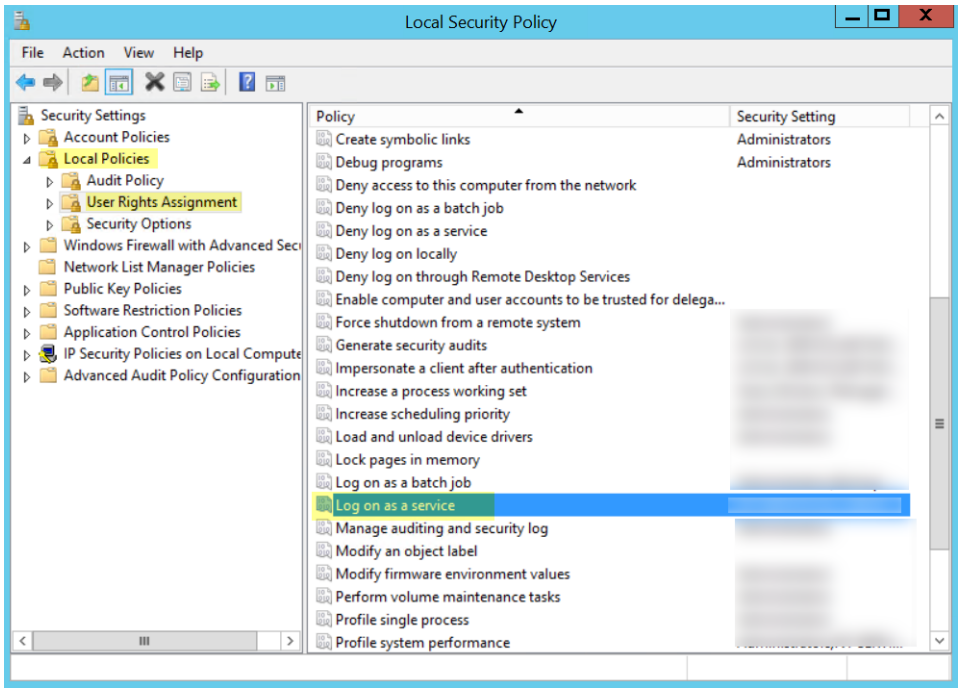
    El permiso para iniciar sesión como un servicio solo es necesario localmente en el servidor de Windows que es el host del agente. Si está usando solo un agente de User-ID, puede conceder los permisos de manera local en el host del agente mediante las siguientes instrucciones.

    1. Para asignar los permisos de manera local, seleccione **Control Panel (Panel de control)** > **Administrative Tools (Herramientas administrativas)** > **Local Security Policy (Política de seguridad local)**.

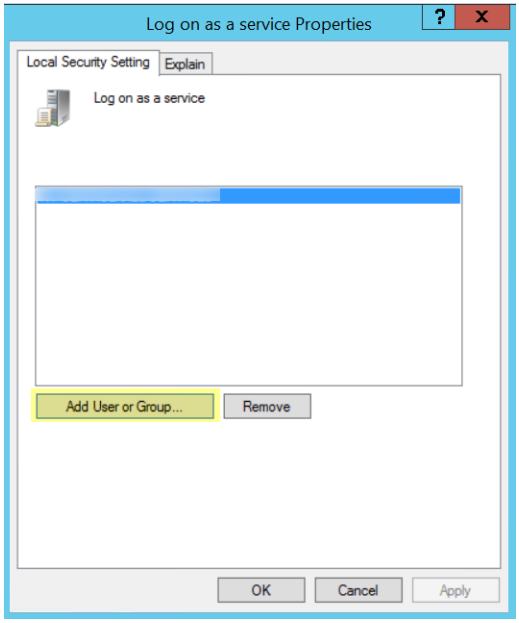


© 2020 Palo Alto Networks, Inc.

2. Seleccione **Local Policies (Políticas locales)** > **User Rights Assignment (Asignación de derechos del usuario)** > **Log on as a service (Iniciar sesión como un servicio)**.

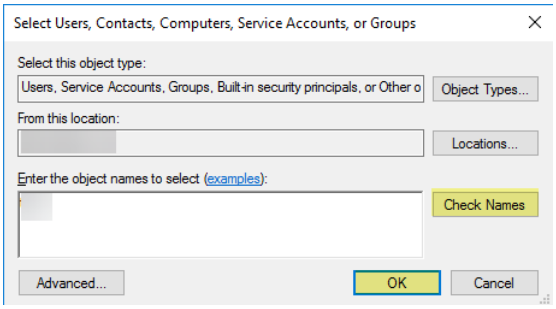


3. Seleccione **Add User or Group (Añadir usuario o grupo)** para añadir la cuenta de servicio.



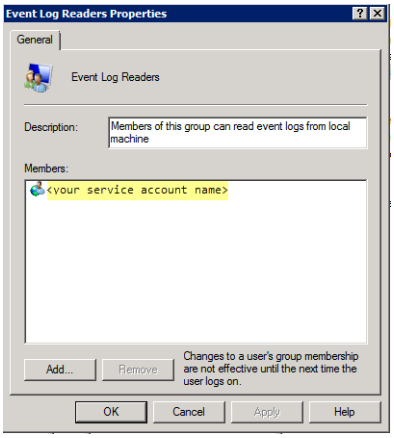
4. Introduzca el nombre de la cuenta de servicio en el formato **`domain\username`** en el campo de entrada **Enter the object names to select (Introduzca los nombres de objetos para seleccionar)** y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.



Para confirmar que el nombre de la cuenta de servicio es válido, seleccione **Check Names (Verificar nombres)**.

2. Si desea usar la supervisión del servidor para identificar usuarios, añada la cuenta de servicio al grupo integrado del lector de logs de eventos para habilitar los privilegios de lectura de los eventos del log de seguridad.
    1. En el controlador de dominio o servidor Exchange que contiene los logs que desea que el agente de User-ID lea, o en el servidor miembro que recibe eventos desde el reenvío de logs de Windows, ejecute MMC e inicie el complemento de Usuarios y equipos de Active Directory.
    2. Desplácese hasta la carpeta Builtin del dominio y, a continuación, haga clic con el botón derecho en cada grupo de **Event Log Reader (Lector de logs de evento)** y seleccione **Add to Group (Añadir al grupo)** para abrir el cuadro de diálogo de propiedades.
    3. Haga clic en **Add (Añadir)** e introduzca el nombre de la cuenta de servicio que configuró para ser utilizada por el servicio de User-ID y, a continuación, haga clic en **Check Names (Comprobar nombres)** para validar que tiene el nombre de objeto adecuado.
    4. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración.
    5. Confirme que en el grupo integrado Event Log Reader (Lector de logs de evento) aparece la cuenta de servicio como miembro.

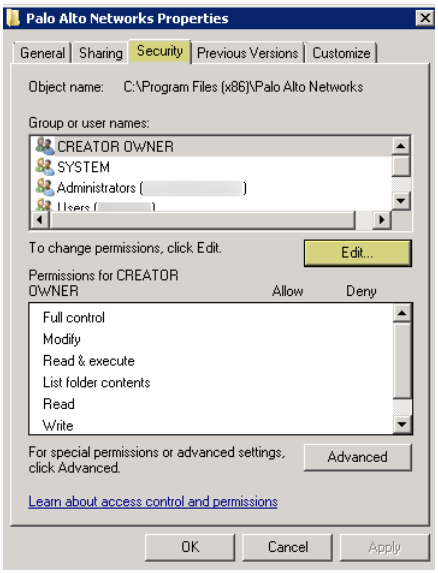


3. Asigne los permisos de cuenta a la carpeta de instalación para permitir que la cuenta de servicio acceda a la carpeta de instalación del agente y pueda leer los logs de escritura y configuración.

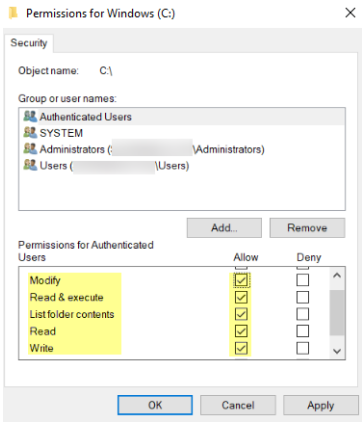
    Solo debe realizar este paso si la cuenta de servicio que configuró para el agente de User-ID no es un administrador de dominio ni un administrador local en el host de servidor del agente de User-ID.

    1. Desde el Explorador de Windows, desplácese hasta `C:\Program Files(x86)\Palo Alto Networks` para sistemas de 32 bits, haga clic con el botón derecho en la carpeta y seleccione **Properties (Propiedades)**.
    2. En la pestaña **Security (Seguridad)**, haga clic en **Edit (Editar)**.

© 2020 Palo Alto Networks, Inc.



3. Seleccione **Add (Añadir)** para añadir la cuenta de servicio del agente de User-ID y asígnele los permisos para **Modify (Modificar)**, **Read & execute (Leer y ejecutar)**, **List folder contents (Mostrar lista del contenido de carpeta)**, **Read (Leer)** y **Write (Escribir)** y, luego, haga clic en **OK (Aceptar)** para guardar la configuración de la cuenta



Si desea permitir que la cuenta de servicio acceda a las claves de registro del agente de User-ID, haga clic en Allow (Permitir) para habilitar el permiso de Full Control (Control completo).

4. Otorgue permisos a la cuenta de servicio para el subárbol de registro del agente de User-ID:
    1. Ejecute **`regedt32`** y desplácese hasta el subárbol de Palo Alto Networks en la siguiente ubicación: `HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`.
    2. Haga clic con el botón derecho en el nodo de Palo Alto Networks y seleccione **Permisos**.
    3. Asigne a la cuenta de servicio de User-ID **Full Control (Control completo)** y, a continuación, haga clic en **OK (Aceptar)** para guardar el ajuste.

STEP 2 | Decida dónde instalar los agentes de User-ID.

El agente de User-ID consulta los logs del controlador de dominio y el servidor Exchange mediante llamadas a procedimiento remoto de Microsoft (Microsoft Remote Procedure Calls, MSRPC). Durante la conexión inicial, el agente transfiere los 50 000 eventos más recientes desde el log para asignarlos a los usuarios. En las siguientes conexiones, el agente transfiere eventos con una marca de tiempo posterior a

© 2020 Palo Alto Networks, Inc.

la última comunicación con el controlador de dominios. Por lo tanto, siempre instale uno o más agentes de User-ID en cada ubicación que tenga servidores que tengan que supervisarse.

- Debe instalar el agente de User-ID en un sistema que ejecute una de las versiones de SO compatibles: consulte "Operating System (OS) Compatibility User-ID Agent" (en inglés) en la Matriz de compatibilidad. El sistema también debe cumplir con los requisitos mínimos (consulte las Notas de la versión del agente de User-ID).
- Asegúrese de que el sistema que alojará el agente de User-ID es un miembro del mismo dominio que los servidores que supervisará.
- Se recomienda instalar el agente de User-ID cerca de los servidores que supervisará (hay más tráfico entre el agente de User-ID y los servidores supervisados que entre el agente de User-ID y el cortafuegos, de modo que ubicar el agente cerca de los servidores supervisados optimiza el uso del ancho de banda).
- Para garantizar la asignación de usuarios más completa, debe supervisar los controladores de todos los dominios que procesan la autenticación de los usuarios que desea asignar. Puede que necesite instalar varios agentes de User-ID para supervisar eficazmente todos sus recursos.
- Si está usando el agente de User-ID para la detección de credenciales, debe instalarlo en el Controlador de dominio de solo lectura (read-only domain controller, RODC). La acción recomendada es implementar un agente diferente para este fin. No use el agente de User-ID que se instaló en el RODC para asignar direcciones IP a usuarios. El instalador del agente de User-ID para la detección de credenciales se llama UaCredInstall64-x.x.x.msi.

STEP 3 | Descargue el instalador de agente de User-ID.

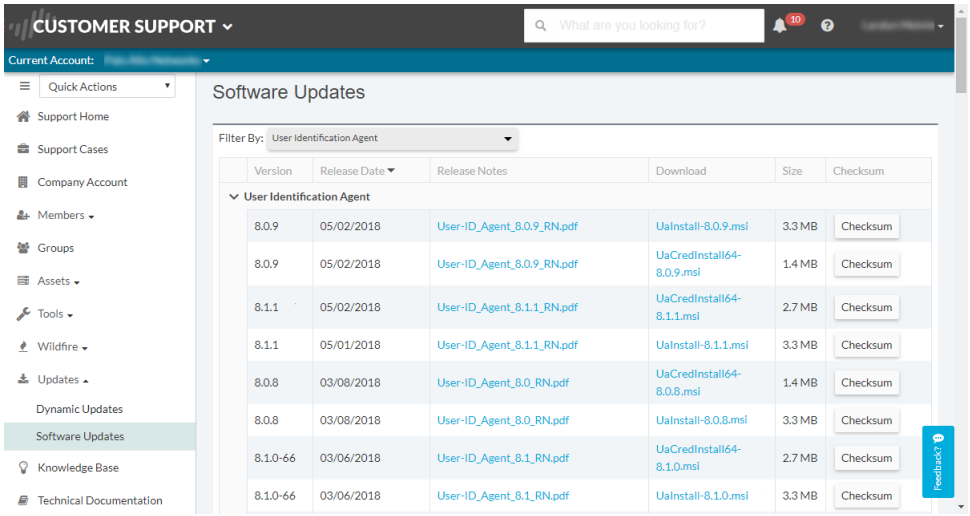


Instale la misma versión del agente de User-ID que la versión de PAN-OS que se esté ejecutando en el cortafuegos. Si no hubiera una versión de agente de User-ID que coincida con la versión de PAN-OS, instale la versión más reciente que sea más cercana a la versión de PAN-OS.

1. Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.
3. Configure **Filter By (Filtrar por)** en **User Identification Agent (Agente de identificación de usuario)** y seleccione la versión del agente de User-ID que desea instalar desde la columna Download (Descarga) correspondiente. Por ejemplo, para descargar la versión 9.0 del agente de User-ID, seleccione **UaInstall-9.0.0-0.msi**.

   Si está usando el agente de User-ID para la detección de credenciales, asegúrese de descargar el archivo `UaCredInstall64-x.x.x.msi` en lugar del archivo de instalación normal de User-ID, que se llama `UaInstall-x.x.x.msi`.
4. Guarde el archivo `UaCredInstall64-x.x.x-xx.msi` o `UaInstall-x.x.x-xx.msi` (asegúrese de seleccionar la versión adecuada según si el sistema Windows está ejecutando un SO de 32 bits o de 64 bits) en los sistemas en los que tenga la intención de instalar el agente.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Ejecute el instalador como administrador.

1. Abra el menú de **Inicio** de Windows, haga clic con el botón derecho en el programa **Símbolo del sistema** y seleccione **Ejecutar como administrador**.
2. Desde la línea de comandos, ejecute el archivo .msi que ha descargado. Por ejemplo, si guardó el archivo .msi en el escritorio, introduzca lo siguiente:

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. Siga los mensajes de configuración para instalar el agente con los ajustes predeterminados. De manera predeterminada, el agente se instala en la carpeta **`C:\Program Files(x86)\Palo Alto Networks`** para sistemas de 32 bits, pero puede hacer clic en **Browse (Examinar)** para seleccionar una ubicación diferente.
4. Cuando finalice la instalación, haga clic en **Cerrar** para cerrar la ventana de configuración.

STEP 5 | Inicie la aplicación del agente de User-ID como administrador.

Abra el menú de **Inicio** de Windows, haga clic con el botón derecho en el programa **User-ID Agent (Agente de User-ID)** y seleccione **Run as administrator (Ejecutar como administrador)**.

Debe ejecutar la aplicación del agente de User-ID como administrador para instalar la aplicación, confirmar los cambios de configuración o desinstalar la aplicación.

STEP 6 | (Opcional) Cambie la cuenta de servicio que utiliza el agente de User-ID para iniciar sesión.

De manera predeterminada, el agente utiliza la cuenta de administrador utilizada para instalar el archivo .msi. Para cambiar de una cuenta a una cuenta restringida:

1. Seleccione **User Identification (Identificación de usuarios)** > **Setup (Configuración)** y haga clic en **Edit (Editar)**.
2. Seleccione la pestaña **Authentication (Autenticación)** e introduzca el nombre de cuenta de servicio que quiera que utilice el agente de User-ID en el campo **User name for Active Directory (Nombre de usuario para Active Directory)**.
3. Introduzca la **Password (Contraseña)** para la cuenta especificada.
4. Haga clic en **Commit (Confirmar)** para confirmar los cambios en la configuración de agente de User-ID para reiniciar el servicio utilizando las credenciales de la cuenta de servicio.

© 2020 Palo Alto Networks, Inc.

STEP 7 | (Opcional) Asigne sus propios certificados para la autenticación mutua entre el agente de User-ID de Windows y el cortafuegos.

1. Obtenga su certificado para el agente de User-ID de Windows utilizando uno de los siguientes métodos. Cargue el certificado del servidor en formato de correo con privacidad mejorada (Privacy Enhanced Mail, PEM) y la clave cifrada del certificado del servidor.
   - Genere un certificado y expórtelo para cargarlo en el agente de User-ID de Windows.
   - Exporte un certificado de la autoridad de certificados (CA) de la empresa y cárguelo en el agente de User-ID de Windows.
2. Añada un certificado de servidor en el agente de User-ID de Windows.
   1. En el agente de User-ID de Windows, seleccione **Server Certificate (Certificado de servidor)** y haga clic en **Add (Añadir)**.
   2. Ingrese la ruta y el nombre del archivo de certificado que recibió de la CA o busque el archivo de certificado.
   3. Ingrese la frase de contraseña de clave privada.
   4. Haga clic en **OK (Aceptar)** y, a continuación, en **Commit (Confirmar)**.
3. Cargue un certificado en el cortafuegos para validar la identidad del agente de User-ID de Windows.
4. Configure el perfil de certificado para el dispositivo de cliente (cortafuegos o Panorama).
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificados)**.
   2. Configuración de un perfil de certificado.

      Solo puede asignar un perfil de certificado para los agentes de User-ID de Windows y los agentes de servidor de terminal (Terminal Server, TS). Por lo tanto, su perfil de certificado debe incluir todas las autoridades de certificado que emitieron certificados cargados en los agentes de TS User-ID conectados.
5. Asigne el perfil de certificado para el cortafuegos.
   1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Connection Security (Seguridad de conexión)** y haga clic en el botón edit (modificar).
   2. Seleccione el **User-ID Certificate Profile (Perfil de certificado de User-ID)** que configuró en el paso anterior.
   3. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

STEP 8 | Configuración de la detección de credenciales con el agente de ID de usuario basado en Windows.

Para usar el agente de User-ID basado en Windows para detectar envíos de credenciales y prevenir el phishing de identidades, debe instalar el servicio de credenciales de User-ID en el agente de User-ID basado en Windows. Solo puede instalar este complemento en un controlador de dominio de solo lectura (RODC).

Configuración del agente de User-ID de Windows para la asignación de usuarios

El agente de User-ID de Palo Alto Networks es un servicio de Windows que se conecta con servidores de su red (por ejemplo, servidores Active Directory, Microsoft Exchange y Novell eDirectory) y supervisa los logs en busca de eventos de inicio de sesión. El agente utiliza esta información para asignar direcciones IP a nombres de usuarios. Los cortafuegos de Palo Alto Networks se conectan con el agente de User-ID para recuperar esta información de asignación de usuarios, habilitando la visibilidad de la actividad de

© 2020 Palo Alto Networks, Inc.

los usuarios por nombre de usuario en lugar de por dirección IP. Esto también habilita la aplicación de la seguridad basada en usuarios y grupos.

Para obtener información sobre las versiones del OS del servidor admitidas por el agente de User-ID, consulte "Operating System (OS) Compatibility User-ID Agent" (en inglés) en las notas de versión de agente de User-ID*.*

STEP 1 | Defina los servidores que supervisará el agente de User-ID para recopilar información de asignación de direcciones IP a usuarios.

El agente de User-ID puede supervisar hasta 100 servidores, de los cuales hasta 50 pueden ser emisores de syslog.

Para recopilar todas las asignaciones necesarias, el agente de User-ID debe conectarse a todos los servidores en los que sus usuarios inician sesión para supervisar los archivos de log de seguridad en todos los servidores que contengan eventos de inicio de sesión.

1. Abra el menú **Inicio** de Windows y seleccione **User-ID Agent**.
2. Seleccione **User Identification (Identificación de usuarios)** > **Discovery (Detección)**.
3. En la sección **Servidores** de la pantalla, haga clic en **Añadir**.
4. Introduzca un **Nombre** y una **Dirección de servidor** para el servidor que vaya a supervisarse. La dirección de red puede ser un FQDN o una dirección IP.
5. Seleccione el **Server Type (Tipo de servidor)** (**Microsoft Active Directory**, **Microsoft Exchange**, **Novell eDirectory**, o **Emisor de syslog**) y, a continuación, haga clic en **OK (Aceptar)** para guardar la entrada del servidor. Repita este paso para este servidor que vaya a supervisarse.
6. (Opcional) Para permitir que el cortafuegos detecte automáticamente controladores de dominio en su red mediante búsquedas de DNS, haga clic en **Auto Discover**.

   La detección automática únicamente localiza los controladores de dominio del dominio local; deberá añadir manualmente los servidores Exchange, los servidores eDirectory y los emisores de Syslog.
7. (Opcional) Para ajustar la frecuencia con la que el cortafuegos sondea los servidores configurados en busca de información de asignación, seleccione **User Identification (Identificación de usuario)** > **Setup (Configuración)** y **Edit (Editar)** para modificar la sección Setup (Configuración). En la pestaña **Supervisión de servidor**, modifique el valor del campo **Frecuencia de supervisión de log de servidor (segundos)**. Aumente el valor de este campo a 5 segundos en entornos con controladores de dominio de mayor antigüedad o enlaces de alta latencia.

   Asegúrese de que el ajuste Enable Server Session Read (Habilitar lectura de sesión de servidor) no esté seleccionado. Esta configuración requiere que el agente de User-ID tenga una cuenta de Active Directory con privilegios de operador de servidor, para que pueda leer todas las sesiones de usuario. En su lugar, debe utilizar una integración de Syslog o XML API para supervisar los orígenes que capturan eventos de inicio de sesión y cierre de sesión para todos los tipos de dispositivos y sistemas operativos (en lugar de solo sistemas operativos Windows), como controladores inalámbricos y Controladores de Acceso de Red (Network Access Controllers, NAC).
8. Haga clic en **OK (Aceptar)** para guardar los ajustes.

STEP 2 | Especifique las subredes que el agente de User-ID de Windows debería incluir o excluir de User-ID.

De manera predeterminada, User-ID asigna a todos los usuarios que acceden a los servidores que usted está supervisando.

© 2020 Palo Alto Networks, Inc.

Como práctica recomendada, siempre especifique qué redes incluir y excluir de User-ID para garantizar que el agente solo se comunique con recursos internos y evitar la asignación de usuarios no autorizados. Solo debe habilitar User-ID en las subredes en las que los usuarios internos de su organización inician sesión.

1. Seleccione **User Identification (Identificación de usuarios)** > **Discovery (Detección)**.
2. Seleccione **Add (Añadir)** para añadir una entrada en la lista Incluir/Excluir e ingrese un nombre para la entrada en **Name** y el intervalo de dirección IP de la subred, como la **Network Address (Dirección de red)**.
3. Seleccione si se incluirá en la red o excluirá de la red:
   - **Include specified network (Incluir red especificada)**: seleccione esta opción si desea limitar la asignación de usuarios a los usuarios que iniciaron sesión únicamente en la subred especificada. Por ejemplo, si incluye 10.0.0.0/8, el agente asigna a los usuarios en esa subred y excluye a los demás. Si desea que el agente asigne usuarios en otras subredes, debe repetir estos pasos para añadir redes adicionales a la lista.
   - **Exclude specified network (Excluir red especificada)**: seleccione esta opción si desea que el agente excluya un subconjunto de las subredes que añadió para inclusión. Por ejemplo, si incluye 10.0.0.0/8 y excluye 10.2.50.0/22, el agente asignará a los usuarios en todas las subredes de 10.0.0.0/8 excepto 10.2.50.0/22, y excluirá todas las subredes fuera de 10.0.0.0/8.

     Observe que si añade perfiles de exclusión sin añadir ningún perfil de inclusión, el agente User-ID excluye todas las subredes, no solo las que ha añadido.
4. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Si ha configurado el agente para que se conecte a un servidor Novell eDirectory, debe especificar el modo en que el agente debería buscar el directorio.

1. Seleccione **User Identification (Identificación de usuarios)** > **Setup (Configuración)** y haga clic en **Edit (Editar)** en la sección Setup (Configuración) de la ventana.
2. Seleccione la pestaña **eDirectory** y, a continuación, cumplimente los campos siguientes:
   - **Base de búsqueda**: punto de partida o contexto raíz para las consultas del agente, por ejemplo: `dc=domain1,dc=example, dc=com`.
   - **Enlazar nombre distintivo**: cuenta que debe utilizarse para enlazarla con el directorio, por ejemplo: `cn=admin,ou=IT, dc=domain1, dc=example, dc=com`.
   - **Enlazar contraseña**: Contraseña de la cuenta de enlace. El agente guardará la contraseña cifrada en el archivo de configuración.
   - **Filtro de búsqueda**: Consulta de búsqueda para entradas de usuarios (el valor predeterminado es `objectClass=Person`).
   - **Server Domain Prefix (Prefijo del dominio de servidor)**: prefijo que identifica de manera exclusiva al usuario. Esto solamente es obligatorio si hay espacios de nombres solapados, como diferentes usuarios con el mismo nombre de dos directorios diferentes.
   - **Use SSL (Utilizar SSL)**: seleccione la casilla de verificación para utilizar SSL para el enlace de eDirectory.
   - **Comprobar certificado de servidor**: Seleccione la casilla de verificación para comprobar el certificado de servidor de eDirectory al utilizar SSL.

STEP 4 | (Opcional, no recomendado) Configure el sondeo de clientes.

No habilite el sondeo de clientes en redes de alta seguridad. El sondeo de clientes puede generar una gran cantidad de tráfico de red y puede representar una amenaza de seguridad cuando no se configura correctamente.

© 2020 Palo Alto Networks, Inc.

1. En la pestaña **Sondeo de clientes**, seleccione la casilla de verificación **Habilitar sondeo de WMI** y/o la casilla de verificación **Habilitar sondeo de NetBIOS**.
2. Asegúrese de que el cortafuegos de Windows permitirá el sondeo de clientes añadiendo una excepción de administración remota al cortafuegos de Windows para cada cliente sondeado.



Para que el sondeo de NetBIOS funcione de forma efectiva, cada PC cliente sondeado debe proporcionar un puerto 139 en el cortafuegos de Windows y debe tener los servicios de uso compartido de archivos e impresoras activados. Si bien el sondeo de clientes no es una práctica recomendada, si usted planea habilitarlo, se prefiere el sondeo de WMI antes que NetBIOS siempre que fuera posible.

STEP 5 | Guarde la configuración.

Haga clic en **OK (Aceptar)** para guardar los ajustes de configuración del agente de User-ID y, a continuación, haga clic en **Commit (Confirmar)** para reiniciar el agente de User-ID y cargar los nuevos ajustes.

STEP 6 | (Opcional) Defina el conjunto de usuarios para los que no necesite proporcionar asignaciones de dirección IP a nombre de usuario, como cuentas de kiosco.

Guarde la lista `ignore-user (usuarios-omitidos)` como documento de texto (extensión de archivo .txt) con el título `ignore_user_list (lista_usuarios_omitidos)` en la carpeta User-ID Agent (Agente de User-ID) del host del agente, es decir, el servidor de dominio donde está instalado.

Enumere las cuentas de usuario que deben ignorarse; no hay ningún límite en el número de cuentas que puede añadir a la lista. Cada nombre de cuenta de usuario debe estar en una línea separada. Por ejemplo:

```
SPAdmin
SPInstall
TFSReport
```

Puede utilizar un asterisco como carácter de comodín para hacer coincidir varios nombres de usuario, pero solo como último carácter en la entrada. Por ejemplo, `corpdomain\it-admin*` coincidiría con todos los administradores del dominio `corpdomain` , cuyos nombres de usuario comienzan con la cadena `it#admin`. También puede utilizar la lista `ignore-user` para identificar a usuarios que desee obligar a autenticarse mediante un portal de autenticación.



Después de añadir entradas en la lista de usuarios ignorados, debe parar y reiniciar la conexión con el servicio.

STEP 7 | Configure los cortafuegos para conectarlos al agente de User-ID.



El cortafuegos puede conectarse únicamente a un agente de User-ID basado en Windows que está usando el complemento de servicio de credenciales de User-ID para detectar los envíos de credenciales corporativas. Consulte Configuración de la detección de credenciales con el agente de User-ID basado en Windows *para obtener más detalles sobre cómo usar este servicio para la prevención de suplantación de identidad de credenciales.*

Realice los siguientes pasos en cada cortafuegos que quiera conectar al agente de User-ID para recibir asignaciones de usuarios:

1. Seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)** y haga clic en **Add (Añadir)**.
2. Introduzca un **nombre** para el agente.

© 2020 Palo Alto Networks, Inc.

3. **Añada un agente con Host and Port (Host y puerto)**.
4. Introduzca la dirección IP del **Host** de Windows en el que está instalado el agente de User-ID.
5. Introduzca el número de **Port** (1-65535) en el que el agente escuchará solicitudes de asignación de usuarios. Este valor debe coincidir con el valor configurado en el agente de User-ID. De manera predeterminada, el puerto se establece como 5007 en el cortafuegos y en versiones más recientes del agente de User-ID. Sin embargo, algunas versiones anteriores del agente de User-ID utilizan el puerto 2010 como valor predeterminado.
6. Seleccione **IP User Mappings (Asignaciones de usuarios IP)** como **Data type (Tipo de datos)**.
7. Asegúrese de que la configuración esté establecida en **Enabled** y, a continuación, haga clic en **OK**.
8. Haga clic en **Commit (Confirmar)** para confirmar los cambios.
9. Verifique que el estado **Connected status (Estado conectado)** aparezca activado (luz verde).

STEP 8 | Verifique que el agente de User-ID está asignando correctamente direcciones IP a nombres de usuarios y que los cortafuegos pueden conectarse con el agente.

1. Inicie el agente de User-ID y seleccione **Identificación de usuarios**.
2. Verifique que el estado del agente muestra **El agente se está ejecutando**. Si el agente no se está ejecutando, haga clic en **Iniciar**.
3. Para verificar que el agente de User-ID se puede conectar con servidores supervisados, asegúrese de que el estado de cada servidor sea **Conectado**.
4. Para verificar que los cortafuegos se pueden conectar con el agente de User-ID, asegúrese de que el estado de cada dispositivo conectado sea **Connected (Conectado)**.
5. Para verificar que el agente de User-ID está asignando direcciones IP a nombres de usuarios, seleccione **Supervisando** y asegúrese de que la tabla de asignaciones se cumplimenta. También puede seleccionar **Search (Búsqueda)** para buscar usuarios específicos o **Delete (Eliminar)** para borrar asignaciones de usuarios de la lista.

Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS

El siguiente procedimiento se describe cómo configurar el agente de User-ID™ integrado en PAN-OS® en el cortafuegos para la asignación de dirección IP a nombre de usuario. El agente de User-ID integrado realiza las mismas tareas que el agente basado en Windows a excepción del sondeo de clientes de NetBIOS (se admite el sondeo de WMI).

STEP 1 | Cree una cuenta de servicio de Active Directory para que el agente de User-ID acceda a los servicios y hosts que el cortafuegos supervisará para recopilar información de asignación de usuarios.

Creación de una cuenta de servicio exclusiva para el agente de User-ID.

STEP 2 | Defina los servidores que supervisará el cortafuegos para recopilar información de asignación de usuarios.

Dentro del máximo total de 100 servidores supervisados por cortafuegos, puede definir no más de 50 emisores de syslog para cualquier sistema virtual simple.

Para recopilar todas las asignaciones necesarias, el cortafuegos debe conectarse a todos los servidores en los que sus usuarios inician sesión para que el cortafuegos pueda supervisar los archivos de log de seguridad en todos los servidores que contengan eventos de inicio de sesión.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)**.

© 2020 Palo Alto Networks, Inc.

2. **Añada** un servidor (sección Monitorización de servidor).
3. Introduzca un nombre en **Name** para identificar el servidor.
4. Seleccione el **Tipo** de servidor.
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - **Emisor de syslog**
5. (Solo en Active Directory de Microsoft y Microsoft Exchange) Seleccione en **Transport Protocol (Protocolo de transporte)** el protocolo que desea usar para supervisar los logs de seguridad y la información de las sesiones del servidor.
   - **WMI**: el cortafuegos y los servidores supervisados se comunican por medio de Instrumental de administración de Windows (Windows Management Instrumentation, WMI).
   - **WinRM-HTTP**: el cortafuegos y los servidores supervisados emplean Kerberos para la autenticación mutua; los servidores supervisados cifran la comunicación con el cortafuegos mediante una clave de sesión de Kerberos negociada.
   - **WinRM-HTTPS**: el cortafuegos y los servidores supervisados se comunican por medio de HTTPS y emplean la autenticación básica o Kerberos para la autenticación mutua.

   Si selecciona una de las opciones de Administración remota de Windows (Windows Remote Management, WinRM), debe realizar el procedimiento Configuración de la supervisión de servidores con WinRM.
6. (Solo en Active Directory de Microsoft, Microsoft Exchange y Novell eDirectory) Introduzca en **Network Address (Dirección de red)** la dirección del servidor.

   Si utiliza WinRM con Kerberos, debe introducir un nombre de dominio completo (fully qualified domain name, FDQN). Si desea utilizar WinRM con la autenticación básica o usa WMI para supervisar el servidor, puede introducir una dirección IP o un FQDN.

   Para supervisar los servidores con WMI, especifique una dirección IP, el nombre de la cuenta de servicio (si todos los servidores supervisados se encuentran en el mismo dominio) o un FQDN. Si especifica un FQDN, emplee el nombre de inicio de sesión específico (Down-level Logon Name, DLN) con el formato (DLN)\sAMAccountName en lugar del formato FQDN\sAMAccountName. Por ejemplo, use `ejemplo\servicios.usuario`*, no* `ejemplo.es\servicios.usuario`*. Si especifica un FQDN, el cortafuegos intenta autenticarse con Kerberos, que no admite WMI.*
7. (Solo en Syslog Sender) Si selecciona **Syslog Sender** como tipo de servidor en **Type (Tipo)**, realice el procedimiento Configuración del agente de User-ID integrado en PAN-OS como receptor de syslog.
8. (Solo en Novell eDirectory) Compruebe que el perfil seleccionado en **Server Profile (Perfil de servidor)** tenga marcada la opción **Enabled (Habilitado)** y haga clic en **OK (Aceptar)**.
9. (Opcional) Configure el cortafuegos para **detectar** automáticamente los controladores de dominio en su red mediante búsquedas de DNS.

   La función de detección automática es únicamente para controladores de dominio; deberá añadir manualmente los servidores Exchange o eDirectory que desee supervisar.

STEP 3 | (Opcional) Especifique la frecuencia con la que el cortafuegos sondea los servidores de Windows en busca de información de asignación. Este es el intervalo entre el final de la última consulta y el inicio de la siguiente.

Si el controlador de dominio está procesando muchas solicitudes, el retraso entre las consultas puede superar el valor especificado.

© 2020 Palo Alto Networks, Inc.

1. **Edite** la **configuración del agente User-ID de Palo Alto Networks**.
2. Seleccione la pestaña **Server Monitor (Supervisor de servidor)** y especifique el valor **Server Log Monitor Frequency (Frecuencia de supervisión de log de servidor)** en segundos (el intervalo es de 1 a 3600; el valor predeterminado es 2). En entornos con controladores de dominio más antiguos o enlaces de alta latencia, establezca esta frecuencia en un mínimo de cinco segundos.

   Asegúrese de que la opción Enable Session (Habilitar sesión) no esté habilitada. Esta opción requiere que el agente de User-ID tenga una cuenta de Active Directory con privilegios de operador de servidor, para que pueda leer todas las sesiones de usuario. En su lugar, debe utilizar una integración de Syslog o XML API para supervisar los orígenes que capturan eventos de inicio de sesión y cierre de sesión para todos los tipos de dispositivos y sistemas operativos (en lugar de solo sistemas operativos Windows), como controladores inalámbricos y dispositivos de control de acceso de red (Network Access Controllers, NAC).
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 4 | Especifique las subredes que el agente de User-ID integrado a PAN-OS debería incluir en la asignación de usuarios o excluir de dicha asignación.

De manera predeterminada, User-ID asigna a todos los usuarios que acceden a los servidores que usted está supervisando.



Como práctica recomendada, siempre especifique qué redes incluir en User-ID y cuáles excluir de User-ID, para garantizar que el agente solo se comunique con recursos internos y evitar la asignación de usuarios no autorizados. Solo debe habilitar la asignación de usuarios en las subredes en las que los usuarios internos de su organización inician sesión.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)**.
2. **Añada** una entrada a las **redes de inclusión/exclusión** y especifique un **nombre** para la entrada. Asegúrese de que la entrada esté **habilitada**.
3. Introduzca la **Network Address (Dirección de red)** y luego seleccione si se incluirá o excluirá:
   - **Include (Incluir)**: seleccione esta opción para limitar la asignación de usuarios a los usuarios que iniciaron sesión únicamente en la subred especificada. Por ejemplo, si incluye 10.0.0.0/8, el agente asigna a los usuarios en esa subred y excluye a los demás. Si desea que el agente asigne usuarios en otras subredes, debe repetir estos pasos para añadir redes adicionales a la lista.
   - **Exclude (Excluir)**: seleccione esta opción para configurar el agente y excluir un subconjunto de las subredes que añadió para inclusión. Por ejemplo, si incluye 10.0.0.0/8 y excluye 10.2.50.0/22, el agente asignará a los usuarios en todas las subredes de 10.0.0.0/8 excepto 10.2.50.0/22, y excluirá todas las subredes fuera de 10.0.0.0/8.

     Observe que si añade perfiles de exclusión sin añadir ningún perfil de inclusión, el agente User-ID excluye todas las subredes, no solo las que ha añadido.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Establezca las credenciales de dominio de la cuenta que utilizará el cortafuegos para acceder a recursos de Windows. Esto es necesario para supervisar servidores Exchange y controladores de dominio, así como para el sondeo de WMI.

1. **Edite** la **configuración del agente User-ID de Palo Alto Networks**.
2. Seleccione la pestaña **Server Monitor Account (Cuenta de supervisión de servidores)** e introduzca en **User Name (Nombre de usuario)** y en **Password (Contraseña)** los valores correspondientes a la

© 2020 Palo Alto Networks, Inc.

cuenta de servicio que debe usar el agente de User-ID para sondear los clientes y supervisar los servidores. Introduzca el nombre de usuario con la sintaxis **`dominio/nombre-usuario`**.

3. Si utiliza WinRM para supervisar los servidores, configure el cortafuegos para autenticarse en el servidor supervisado.
   - Si desea utilizar WinRM con la autenticación básica, habilite WinRM en el servidor, configure la autenticación básica y especifique el valor de **Domain's DNS Name (Nombre DNS de dominio)** que corresponda a la cuenta de servicio.
   - Si desea utilizar WinRM con Kerberos, configure un perfil de servidor Kerberos (si aún no lo ha hecho) y, a continuación, seleccione **Kerberos Server Profile (Perfil de servidor Kerberos)**.

STEP 6 | (Opcional, no recomendado) Configure el sondeo de WMI (el agente de User-ID integrado a PAN-OS no admite el sondeo de NetBIOS).

No habilite el sondeo de WMI en redes de alta seguridad. El sondeo de clientes puede generar una gran cantidad de tráfico de red y puede representar una amenaza de seguridad cuando no se configura correctamente.

1. En la pestaña **Client Probing (Sondeo de clientes)**, haga clic en **Enable Probing (Habilitar sondeo)**.
2. (Opcional) En **Probe Interval (Intervalo de sondeo)**, defina el intervalo (en minutos) entre el final de la última solicitud de sondeo y el inicio de la siguiente.

   Si es preciso, aumente el valor para asegurarse de que el agente de User-ID tenga tiempo suficiente para sondear todas las direcciones IP obtenidas (el intervalo es de 1 a 1440; el valor predeterminado es 20).

   Si la carga de consultas es alta, el intervalo observado entre solicitudes puede superar considerablemente el intervalo que especifique.
3. Haga clic en **OK (Aceptar)**.
4. Asegúrese de que el cortafuegos de Windows permitirá el sondeo de clientes añadiendo una excepción de administración remota al cortafuegos de Windows para cada cliente sondeado.

STEP 7 | (Opcional) Defina el conjunto de cuentas de usuario que no necesitan asignaciones de direcciones IP a nombres de usuario, como las cuentas de kiosco.

Defina la lista de usuarios omitidos en el cortafuegos que actúa como agente de User-ID, no como cliente. Si la define en el cortafuegos cliente, los usuarios de la lista se siguen asignando durante la redistribución.

En la pestaña **Ignore User List (Ignorar lista de usuarios)**, **añada** cada nombre de usuario que desee excluir de la asignación de usuarios. También puede utilizar la lista ignore user (ignorar usuario) para identificar a usuarios que desee obligar a autenticarse mediante un portal de autenticación. Puede utilizar un asterisco como carácter de comodín para hacer coincidir varios nombres de usuario pero solo como último carácter en la entrada. Por ejemplo, **`corpdomain\it-admin*`** coincidiría con todos los administradores del dominio `corpdomain` , cuyos nombres de usuario comienzan con la cadena `it#admin`. Puede añadir hasta 5.000 entradas para excluir de la asignación de usuarios.

STEP 8 | Active los cambios de configuración.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 9 | Verifique la configuración.

1. Acceda a la CLI del cortafuegos.
2. Introduzca el siguiente comando operativo:

© 2020 Palo Alto Networks, Inc.

```
> show user server-monitor state all
```

3. En la pestaña **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)** en la interfaz web, verifique que el estado de cada servidor configurado para la supervisión de servidores sea `Connected (Conectado)`.

Configuración de la supervisión de servidores con WinRM

Puede configurar el agente de User-ID integrado en PAN-OS para supervisar los servidores con Administración remota de Windows (Windows Remote Management, WinRM). El uso del protocolo WinRM mejora la rapidez, la eficiencia y la seguridad cuando se supervisan eventos de los servidores para asignar eventos de los usuarios a direcciones IP. El agente de User-ID integrado en PAN-OS admite el protocolo WinRM en Windows Server 2012 Active Directory y Microsoft Exchange Server 2012 o versiones posteriores de ambos.

Hay tres formas de configurar la supervisión de los servidores con WinRM:

- Configuración de WinRM por HTTPS con autenticación básica: el cortafuegos se autentica en el servidor supervisado con el nombre de usuario y la contraseña de la cuenta de servicio del agente de User-ID, y el cortafuegos autentica el servidor supervisado mediante el perfil de certificados de User-ID.
- Configuración de WinRM por HTTP con Kerberos: el cortafuegos y los servidores supervisados emplean Kerberos para la autenticación mutua, y los servidores supervisados cifran la comunicación con el cortafuegos mediante una clave de sesión de Kerberos negociada.
- Configuración de WinRM por HTTPS con Kerberos: el cortafuegos y el servidor supervisado se comunican por medio de HTTPS y emplean Kerberos para la autenticación mutua.

Configuración de WinRM por HTTPS con autenticación básica

Si configura WinRM para que utilice HTTPS con la autenticación básica, el cortafuegos transfiere las credenciales de la cuenta de servicio por un túnel seguro que usa SSL.

STEP 1 | Configure la cuenta de servicio con privilegios de usuario de Administración remota y CIMV2 en el servidor que desea supervisar.

STEP 2 | En el servidor de Windows que pretende supervisar, obtenga la huella digital del certificado para dicho servidor que se debe utilizar con WinRM y habilite esta función.

La cuenta usada para configurar WinRM en el servidor supervisado debe tener privilegios de administrador.

1. Verifique si el certificado está instalado en el almacén de certificados del ordenador local con **Certificates (Local Computer) (Certificados [equipo local])** > **Personal** > **Certificates (Certificados)**.

   Si no ve el almacén de certificados del ordenador local, inicie Microsoft Management Console con **Start (Inicio)** > **Run (Ejecutar)** > **MMC** y añada el complemento Certificates (Certificados) con **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Certificates (Certificados)** > **Add (Agregar)** > **Computer account (Cuenta de equipo)** > **Next (Siguiente)** > **Finish (Finalizar)**.
2. Abra el certificado y seleccione **General** > **Details (Detalles)** > **Show: <All> (Mostrar: <Todos>)**.
3. Seleccione **Thumbprint (Huella)** y cópiela.
4. Para que el cortafuegos se pueda conectar al servidor de Windows mediante WinRM, introduzca el siguiente comando: **`winrm quickconfig`**.
5. Especifique **`y (s)`** para confirmar los cambios. Después, confirme que el resultado muestra `WinRM service started (Servicio WinRM iniciado)`.

© 2020 Palo Alto Networks, Inc.

Si WinRM ya está habilitado, el resultado muestra `WinRM service is already running on this machine (El servicio WinRM ya está ejecutándose en esta máquina)`. Si hacen falta cambios en la configuración, se le pide que los confirme.

6. Para verificar si WinRM se comunica por HTTPS, introduzca el comando: **`winrm enumerate winrm/config/listener`** y confirme que se muestra `Transport = HTTPS (Transporte = HTTPS)`.

   WinRM por HTTPS utiliza el puerto 5986 de manera predeterminada.
7. Desde el símbolo del sistema de Windows, ingrese el siguiente comando: **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**, donde *hostname* es el nombre de host del servidor de Windows y *Certificate Thumbprint* es el valor que copió del certificado.

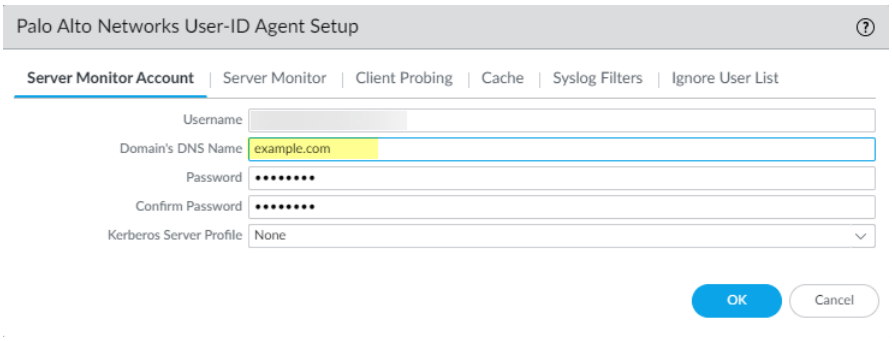
   Utilice el símbolo del sistema (no PowerShell) y elimine los espacios de la huella del certificado para que WinRM pueda validarlo.
8. En el símbolo del sistema del servidor de Windows, introduzca el comando

```
c:\> winrm set winrm/config/client/auth @{Basic="true"}
```

9. Ingrese el siguiente comando: **`winrm get winrm/config/service/Auth`** y confirme que muestra `Basic = true (Básica = sí)`.

STEP 3 | Habilite la autenticación básica entre el agente de User-ID integrado en PAN-OS y los servidores supervisados.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Server Monitor Account (Cuenta de supervisión de servidores)**.
2. Introduzca en **User Name (Nombre de usuario)**, con el formato **`dominio/nombre-usuario`**, el valor correspondiente a la cuenta de servicio que debe usar el agente de User-ID para supervisar los servidores.
3. Introduzca en **Domain's DNS Name (Nombre DNS de dominio)** el valor que corresponda a la cuenta de supervisión de servidores.



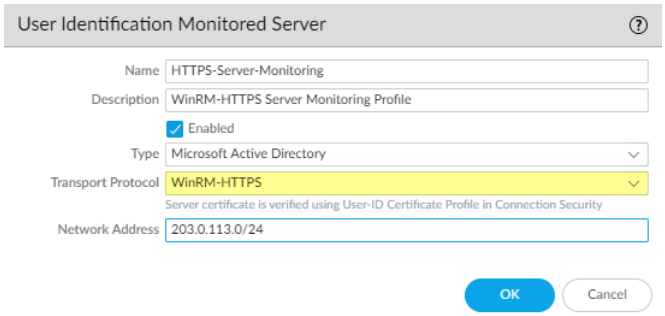
4. Introduzca la contraseña de la cuenta de servicio en **Password (Contraseña)** y en **Confirm Password (Confirmar contraseña)**.
5. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure la supervisión de los servidores en el agente de User-ID integrado en PAN-OS.

1. En **Type (Tipo)**, seleccione el tipo de servidor de Microsoft: **Microsoft Active Directory** o **Microsoft Exchange**.

© 2020 Palo Alto Networks, Inc.

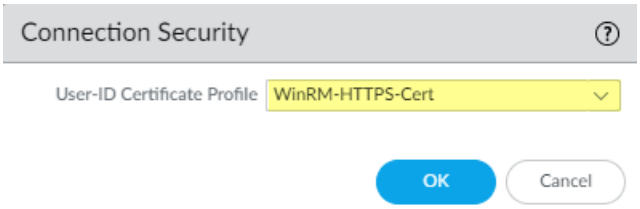
2. Seleccione **WinRM-HTTPS** en **Transport Protocol (Protocolo de transporte)** si desea utilizar Administración remota de Windows (Windows Remote Management, WinRM) por HTTPS para supervisar los logs de seguridad y la información de las sesiones del servidor.



3. Introduzca la dirección IP o el FQDN del servidor en **Network Address (Dirección de red)**.

STEP 5 | Para que el agente de User-ID integrado en PAN-OS se comunique con los servidores supervisados mediante WinRM por HTTPS, verifique que ha importado correctamente al cortafuegos el certificado raíz de los certificados de servicio que emplea el servidor de Windows para WinRM y asocie el certificado al perfil de certificados de User-ID.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Connection Security (Seguridad de conexión)**.
2. Haga clic en **Edit (Editar)**.
3. Seleccione el certificado del servidor de Windows que se debe usar en **User-ID Certificate Profile (Perfil del certificado de User-ID)**.



4. Haga clic en **OK (Aceptar)**.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Verifique que el estado de todos los servidores supervisados es Connected (Conectado) con **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)**.

Configuración de WinRM por HTTP con Kerberos

Cuando configura WinRM por HTTP con Kerberos, el cortafuegos y los servidores supervisados emplean Kerberos para la autenticación mutua; los servidores supervisados cifran la comunicación con el cortafuegos mediante una clave de sesión de Kerberos negociada.

WinRM con Kerberos admite los cifrados aes128-cts-hmac-sha1-96 y aes256-cts-hmac-sha1-96. Si el servidor que desea supervisar utiliza RC4, debe descargar la actualización de Windows y deshabilitar RC4 para Kerberos en la configuración del registro de dicho servidor.

STEP 1 | Configure la cuenta de servicio con privilegios de usuario de Administración remota y CIMV2 en el servidor que desea supervisar.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Confirme que WinRM está habilitado en el servidor de Windows supervisado.

La cuenta usada para configurar WinRM en el servidor supervisado debe tener privilegios de administrador.

1. Para que el cortafuegos se pueda conectar al servidor de Windows mediante WinRM, introduzca el siguiente comando: **`winrm quickconfig`**.
2. Especifique **`y (s)`** para confirmar los cambios. Después, confirme que el resultado muestra `WinRM service started (Servicio WinRM iniciado)`.

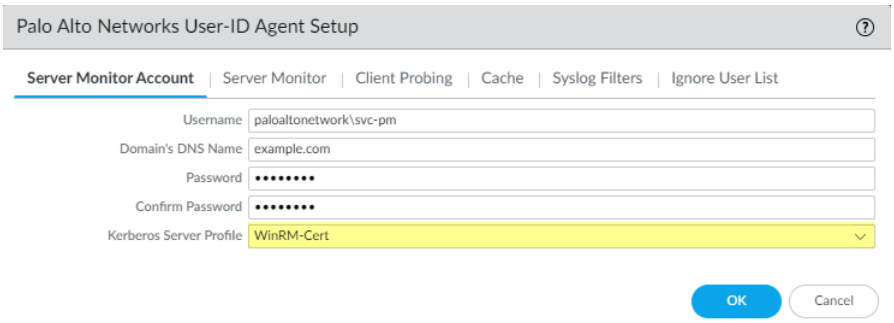
   Si WinRM ya está habilitado, el resultado muestra `WinRM service is already running on this machine (El servicio WinRM ya está ejecutándose en esta máquina)`. Si hacen falta cambios en la configuración, se le pide que los confirme.
3. Para verificar si WinRM se comunica por HTTP, introduzca el comando: **`winrm enumerate winrm/config/listener`** y confirme que se muestra `Transport = HTTP (Transporte = HTTP)`.

   WinRM por HTTP utiliza el puerto 5985 de manera predeterminada.
4. Ingrese el siguiente comando: **`winrm get winrm/config/service/Auth`** y confirme que muestra `Kerberos = true (Kerberos = sí)`.

STEP 3 | Habilite la autenticación con Kerberos del agente de User-ID integrado en PAN-OS y de los servidores supervisados.

1. Para garantizar la correcta negociación de Kerberos, configure los ajustes de fecha y hora (NTP) si no lo ha hecho durante la configuración inicial.
2. Configure un perfil de servidor Kerberos en el cortafuegos para autenticarse en el servidor a fin de supervisar los logs de seguridad y la información de las sesiones.
3. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Server Monitor Account (Cuenta de supervisión de servidores)**.
4. Introduzca en **User Name (Nombre de usuario)**, con el formato **`dominio/nombre-usuario`**, el valor correspondiente a la cuenta de servicio que debe usar el agente de User-ID para supervisar los servidores.
5. Introduzca en **Domain's DNS Name (Nombre DNS de dominio)** el valor que corresponda a la cuenta de supervisión de servidores.

   Kerberos se sirve del nombre de dominio para localizar la cuenta de servicio.
6. Introduzca la contraseña de la cuenta de servicio en **Password (Contraseña)** y en **Confirm Password (Confirmar contraseña)**.
7. Seleccione el **Kerberos Server Profile (Perfil de servidor Kerberos)** que configuró en el paso 3.2.

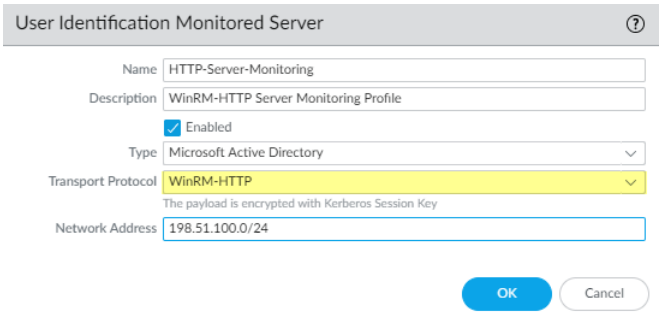


8. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure la supervisión de los servidores en el agente de User-ID integrado en PAN-OS.

© 2020 Palo Alto Networks, Inc.

1. Configure el tipo de servidor de Microsoft: **Microsoft Active Directory** o **Microsoft Exchange**.
2. Seleccione **WinRM-HTTP** en **Transport Protocol (Protocolo de transporte)** si desea utilizar WinRMpor HTTP para supervisar los logs de seguridad y la información de las sesiones del servidor.



3. Introduzca el FQDN del servidor en **Network Address (Dirección de red)**.

   Si utiliza Kerberos, la dirección de red debe ser un FDQN.

STEP 5 | **Commit (Confirmar)** los cambios.

STEP 6 | Verifique que el estado de todos los servidores supervisados es Connected (Conectado) con **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)**.

Configuración de WinRM por HTTPS con Kerberos

Cuando configura WinRM por HTTPS con Kerberos, el cortafuegos y el servidor supervisado se comunican por medio de HTTPS y emplean Kerberos para la autenticación mutua.

WinRM con Kerberos admite los cifrados aes128-cts-hmac-sha1-96 y aes256-cts-hmac-sha1-96. Si el servidor que desea supervisar utiliza RC4, debe descargar la actualización de Windows y deshabilitar RC4 para Kerberos en la configuración del registro de dicho servidor.

STEP 1 | Configure la cuenta de servicio con privilegios de usuario de Administración remota y CIMV2 en el servidor que desea supervisar.

STEP 2 | En el servidor de Windows que pretende supervisar, obtenga la huella digital del certificado para dicho servidor que se debe utilizar con WinRM y habilite esta función.

La cuenta usada para configurar WinRM en el servidor supervisado debe tener privilegios de administrador.

1. Verifique si el certificado está instalado en el almacén de certificados del ordenador local con **Certificates (Local Computer) (Certificados [equipo local])** > **Personal** > **Certificates (Certificados)**.

   Si no ve el almacén de certificados del ordenador local, inicie Microsoft Management Console con **Start (Inicio)** > **Run (Ejecutar)** > **MMC** y añada el complemento Certificates (Certificados) con **File (Archivo)** > **Add/Remove Snap-in (Agregar o quitar complemento)** > **Certificates (Certificados)** > **Add (Agregar)** > **Computer account (Cuenta de equipo)** > **Next (Siguiente)** > **Finish (Finalizar)**.
2. Abra el certificado y seleccione **General** > **Details (Detalles)** > **Show: <All> (Mostrar: <Todos>)**.
3. Seleccione **Thumbprint (Huella)** y cópiela.
4. Para que el cortafuegos se pueda conectar al servidor de Windows mediante WinRM, introduzca el siguiente comando: **`winrm quickconfig`**.

© 2020 Palo Alto Networks, Inc.

5. Especifique **`y (s)`** para confirmar los cambios. Después, confirme que el resultado muestra `WinRM service started (Servicio WinRM iniciado)`.

   Si WinRM ya está habilitado, el resultado muestra `WinRM service is already running on this machine (El servicio WinRM ya está ejecutándose en esta máquina)`. Si hacen falta cambios en la configuración, se le pide que los confirme.
6. Para verificar si WinRM se comunica por HTTPS, introduzca el comando: **`winrm enumerate winrm/config/listener`**. A continuación, confirme que el resultado sea `Transport = HTTPS`.

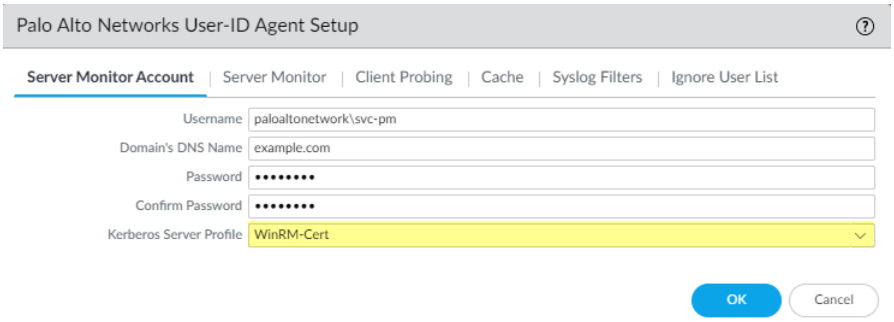
   WinRM por HTTPS utiliza el puerto 5986 de manera predeterminada.
7. Desde el símbolo del sistema de Windows, ingrese el siguiente comando: **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**, donde *hostname* es el nombre de host del servidor de Windows y *Certificate Thumbprint* es el valor que copió del certificado.

   Utilice el símbolo del sistema (no PowerShell) y elimine los espacios de la huella del certificado para que WinRM pueda validarlo.
8. Ingrese el siguiente comando: **`winrm get winrm/config/service/Auth`** y confirme que muestra `Basic = false (Básica = no)` y `Kerberos = true (Kerberos = sí)`.

STEP 3 | Habilite la autenticación con Kerberos del agente de User-ID integrado en PAN-OS y de los servidores supervisados.

1. Para garantizar la correcta negociación de Kerberos, configure los ajustes de fecha y hora (NTP) si no lo ha hecho durante la configuración inicial.
2. Configure un perfil de servidor Kerberos en el cortafuegos para autenticarse en el servidor a fin de supervisar los logs de seguridad y la información de las sesiones.
3. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Server Monitor Account (Cuenta de supervisión de servidores)**.
4. Introduzca en **User Name (Nombre de usuario)**, con el formato **`dominio/nombre-usuario`**, el valor correspondiente a la cuenta de servicio que debe usar el agente de User-ID para supervisar los servidores.
5. Introduzca en **Domain's DNS Name (Nombre DNS de dominio)** el valor que corresponda a la cuenta de supervisión de servidores.

   Kerberos se sirve del nombre de dominio para localizar la cuenta de servicio.
6. Introduzca la contraseña de la cuenta de servicio en **Password (Contraseña)** y en **Confirm Password (Confirmar contraseña)**.
7. Seleccione el perfil creado en el paso 3.2 en **Kerberos Server Profile (Perfil de servidor Kerberos)**.

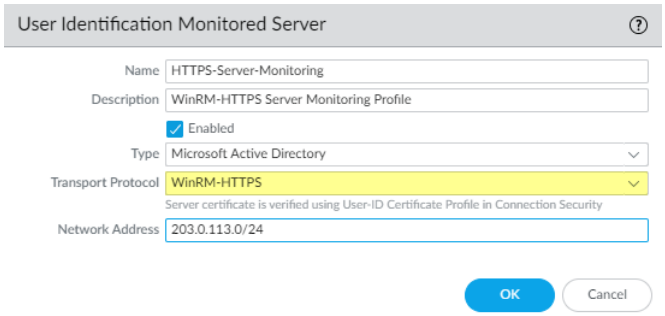


8. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure la supervisión de los servidores en el agente de User-ID integrado en PAN-OS.

© 2020 Palo Alto Networks, Inc.

1. Configure el tipo de servidor de Microsoft: **Microsoft Active Directory** o **Microsoft Exchange**.
2. Seleccione **WinRM-HTTPS** en **Transport Protocol (Protocolo de transporte)** si desea utilizar Administración remota de Windows (Windows Remote Management, WinRM) por HTTPS para supervisar los logs de seguridad y la información de las sesiones del servidor.



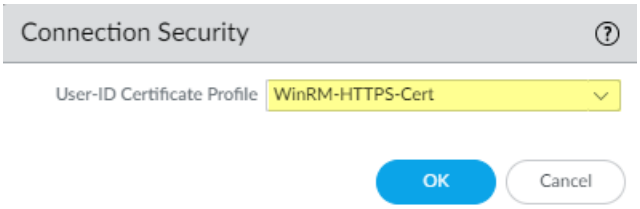
3. Introduzca el FQDN del servidor en **Network Address (Dirección de red)**.

   Si utiliza Kerberos, la dirección de red debe ser un FDQN.

STEP 5 | Para que el agente de User-ID integrado en PAN-OS se comunique con los servidores supervisados mediante WinRM por HTTPS, verifique que ha importado correctamente al cortafuegos el certificado raíz de los certificados de servicio que emplea el servidor de Windows para WinRM y asocie el certificado al perfil de certificados de User-ID.

El cortafuegos utiliza el mismo certificado para autenticarse en todos los servidores supervisados.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Connection Security (Seguridad de conexión)**.
2. Haga clic en **Edit (Editar)**.
3. Seleccione el certificado del servidor de Windows que se debe usar en **User-ID Certificate Profile (Perfil del certificado de User-ID)**.



4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

STEP 6 | Verifique que el estado de todos los servidores supervisados es Connected (Conectado) con **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)**.

Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios

Para obtener asignaciones de dirección IP a nombre de usuario de servicios de red existentes que autentican usuarios, puede configurar el agente de User-ID integrado en PAN-OS o el agente de User-ID basado en Windows para analizar mensajes de Syslog de esos servicios. Para garantizar que las asignaciones de usuarios permanezcan actualizadas, puede configurar el agente de User-ID para analizar mensajes

© 2020 Palo Alto Networks, Inc.

de Syslog para eventos de cierre de sesión, de modo que el cortafuegos elimine automáticamente las asignaciones desactualizadas.

- Configuración del agente de User-ID integrado en PAN-OS como receptor de syslog
- Configuración del agente de User-ID de Windows como receptor de Syslog

Configuración del agente de User-ID integrado en PAN-OS como receptor de syslog

Para configurar el agente de User-ID integrado en PAN-OS para crear nuevas asignaciones de usuario y eliminar asignaciones obsoletas a través del control de syslog, comience por definir los perfiles de análisis de Syslog. El agente de User-ID utiliza los perfiles para encontrar eventos de inicio y cierre de sesión en mensajes de syslog. En entornos en los que los *emisores de syslog* (los servicios de red que autentican a los usuarios) envían mensajes de syslog en diferentes formatos, configure un perfil para cada formato de syslog. Los mensajes de syslog deben cumplir ciertos criterios para que un agente de User-ID los analice (consulte Syslog). Este procedimiento utiliza ejemplos con los siguientes formatos:

- **Eventos de inicio de sesión**: `[Tue Jul 5 13:15:04 2016 CDT] Administratorauthentication success User:johndoe1 Source:192.168.3.212`
- **Eventos de cierre de sesión**: `[Tue Jul 5 13:18:05 2016CDT]User logout successful User:johndoe1 Source:192.168.3.212`

Después de configurar los perfiles de análisis de Syslog, debe especificar los emisores de syslog para que el agente de User-ID supervise.

STEP 1 | Determine si hay un perfil de análisis de Syslog predefinido para sus emisores syslog particulares.

Palo Alto Networks proporciona varios perfiles predefinidos a través de actualizaciones de contenido de aplicaciones. Los filtros predefinidos son generales para el cortafuegos, mientras que los perfiles definidos de manera personalizada solo se aplican a un sistema virtual.

Los perfiles de análisis de Syslog nuevos de una versión de contenido particular se documentan en la nota de versión correspondiente junto con la regex específica utilizada para definir el filtro.

1. Instale la última actualización de Aplicaciones o de Aplicaciones y amenazas.
    1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y **Check Now (Comprobar ahora)**.
    2. Seleccione **Download (Descargar)** y luego **Install (Instalar)** para descargar e instalar cualquier actualización.
2. Determine qué perfiles de análisis de Syslog están disponibles:
    1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)** y haga clic en **Add (Añadir)** en la sección Server Monitoring (Supervisión de servidores).
    2. Configure el **Type (Tipo)** en **Syslog Sender (Emisor de Syslog)** y haga clic en **Add (Añadir)** en la sección Filter (Filtro). Si el perfil de análisis de Syslog que necesita está disponible, omita los pasos para la definición de perfiles personalizados.

STEP 2 | Defina los perfiles de análisis de Syslog para crear y eliminar asignaciones de usuario.

Cada perfil filtra los mensajes syslog para identificar eventos de inicio de sesión (para crear asignaciones de usuario) o eventos de cierre de sesión (para eliminar asignaciones), pero ningún perfil puede hacer ambas cosas.

© 2020 Palo Alto Networks, Inc.

1. Revise los mensajes syslog que el emisor syslog genera para identificar la sintaxis de los eventos de inicio y cierre de sesión. Esto le permite identificar los patrones coincidentes al crear perfiles de análisis de Syslog.

   Al revisar mensajes syslog, determine también si incluyen el nombre de dominio. Si no lo incluyen y sus asignaciones de usuario requieren nombres de dominio, ingrese el Default Domain Name (Nombre de dominio predeterminado) al definir los emisores syslog que el agente de User-ID supervisa (en pasos posteriores de este procedimiento).
2. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)** y modifique la configuración del agente de User-ID de Palo Alto Networks.
3. Seleccione **Syslog Filters (Filtros de Syslog)** y haga clic en **Add (Añadir)** para añadir un perfil de análisis de Syslog.
4. Introduzca un nombre para identificar el **Syslog Parse Profile (Perfil de análisis de Syslog)**.
5. Seleccione el **Type (Tipo)** de análisis para encontrar eventos de inicio o cierre de sesión en los mensajes de syslog:
   - **Regex Identifier (Identificador de regex)**: expresiones regulares.
   - **Field Identifier (Identificador de campo)**: cadenas de texto.

   Los siguientes pasos describen cómo configurar estos tipos de análisis.

STEP 3 | (**Identificador de regex únicamente**) Defina los patrones de coincidencia de regex.



Si el mensaje syslog contiene un espacio o una tabulación independiente como delimitador, debe utilizar **`\s`** *para un espacio y* **`\t`** *para una tabulación.*

1. Ingrese el **Event Regex (Regex de evento)** para el tipo de evento que desea encontrar:
   - **Eventos de inicio de sesión**: en el mensaje de ejemplo, la expresión regular **`(authentication\ success){1}`** extrae la primera **`{1}`** instancia de la cadena `authenticationsuccess`.
   - **Eventos de cierre de sesión**: en el mensaje de ejemplo, la expresión regular **`(logout\ successful){1}`** extrae la primera instancia de **`{1}`** de la cadena `logoutsuccessful`.

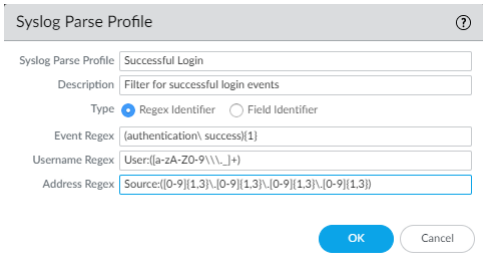
   La barra invertida (\) antes del espacio es un carácter regex de "escape" estándar que indica al motor de regex que no trate el espacio como carácter especial.
2. Ingrese el **Username Regex (Regex de nombre de usuario)** para identificar el inicio del nombre de usuario.

   En el mensaje de ejemplo, la regex **`User:([a-zA-Z0-9\\\._]+)`** coincidiría con la cadena `User:johndoe1` e identificaría `johndoe1` como el nombre de usuario.
3. Ingrese la **Address Regex (Regex de dirección)** para identificar la parte de la dirección IP de los mensajes syslog.

   En el mensaje de ejemplo, la expresión regular **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** coincide con la dirección IPv4 `Source:192.168.3.212`.

   El siguiente es un ejemplo de un perfil de análisis de Syslog que utiliza regex para identificar eventos de inicio de sesión:

© 2020 Palo Alto Networks, Inc.



4. Haga clic en **OK (Aceptar)** dos veces para guardar el perfil.

STEP 4 | (**Análisis de identificador de campo únicamente**) Defina los patrones de coincidencia de cadena.

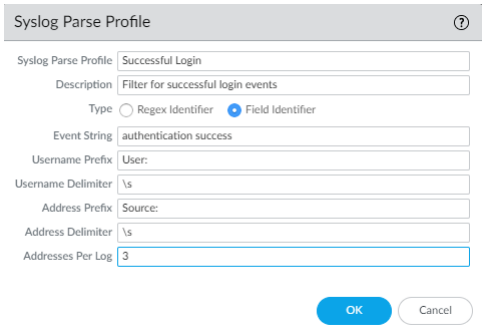
1. Ingrese una **Event String (Cadena de evento)** para identificar el tipo de eventos que desea encontrar:
   - **Eventos de inicio de sesión:** para el mensaje de ejemplo, la cadena `authentication success` identifica los eventos de inicio de sesión.
   - **Eventos de cierre de sesión**: en el mensaje de ejemplo, la cadena `logoutsuccessful` identifica los eventos de cierre de sesión.
2. Ingrese un **Username Prefix (Prefijo de nombre de usuario)** para identificar el inicio del campo de nombre de usuario en los mensaje de syslog. Este campo no admite regex como \s (para un espacio) o \t (para una pestaña).

   En los mensajes de ejemplo, `User:` identifica el inicio del campo del nombre de usuario.
3. Ingrese el **Username Delimiter (Delimitador de nombre de usuario)** que indica el final del campo del nombre de usuario en los mensaje de syslog. Utilice **`\s`** para indicar un espacio independiente (como en el mensaje de ejemplo) y **`\t`** para indicar tabulación.
4. Ingrese un **Address Prefix (Prefijo de dirección)** para identificar el inicio del campo de dirección IP en los mensaje de syslog. Este campo no admite regex como \s (para un espacio) o \t (para una pestaña).

   En los mensajes de ejemplo, `Source:` identifica el inicio del campo de dirección.
5. Ingrese el **Address Delimiter (Delimitador de dirección)** que indica el final del campo del nombre de dirección en los mensaje de syslog.

   Por ejemplo, introduzca \n para indicar que el delimitador es un salto de línea.

   El siguiente es un ejemplo de un perfil de análisis de Syslog completo que utiliza la coincidencia de cadenas para identificar eventos de inicio de sesión:



6. Haga clic en **OK (Aceptar)** dos veces para guardar el perfil.

STEP 5 | Especifique los emisores de syslog que el cortafuegos supervisa.

Dentro del máximo total de 100 servidores supervisados por cortafuegos, puede definir no más de 50 emisores de syslog para cualquier sistema virtual simple.

El cortafuegos descartará los mensajes de Syslog recibidos de emisores que no estén en esta lista.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuario)** y haga clic en **Add (Añadir)** para añadir una entrada en la lista Server Monitoring (Supervisión de servidores).
2. Ingrese un nombre en **Name** para identificar el emisor.
3. Asegúrese de que el perfil del emisor esté **Enabled (Habilitado)** (opción predeterminada).
4. Configure el **Type (Tipo)** en **Syslog Sender (Emisor de Syslog)**.
5. Especifique la **dirección de red** (dirección IP) del emisor de syslog.
6. Seleccione **SSL** (opción predeterminada) o **UDP** como el **Connection Type (Tipo de conexión)**.

   Para seleccionar el certificado TLS que el cortafuegos usa para recibir mensajes de syslog, seleccione Device (Dispositivo) > User Identification (Identificación de usuarios) > User Mapping (Asignación de usuarios) > Palo Alto Networks User-ID Agent Setup (Configuración del agente de User-ID de Palo Alto Networks). Edite la configuración y seleccione Server Monitor (Supervisor de servidor) y, a continuación, seleccione Syslog Service Profile (Perfil de servicio de syslog) que contiene el certificado TLS que desea que use el cortafuegos para recibir mensajes de syslog.

   El agente de User-ID integrado en PAN-OS acepta Syslogs únicamente a través de SSL y UDP. Sin embargo, debe tener precaución a la hora de usar UDP para recibir mensajes de syslog, ya que no es un protocolo fiable y, como tal, no hay manera de verificar que un mensaje se haya enviado desde un emisor syslog de confianza. Aunque puede restringir los mensajes de syslog a direcciones IP de origen específicas, esto no impide a los atacantes replicar la dirección IP, lo que permite la inyección de mensajes de syslog no autorizados en el cortafuegos.

   Utilice SSL siempre para escuchar los mensajes de syslog porque el tráfico está cifrado (UDP envía el tráfico en texto sin cifrar). Si debe usar UDP, asegúrese de que tanto el emisor de syslog como el cliente estén en una red dedicada y segura para evitar que los hosts no fiables envíen tráfico UDP al cortafuegos.

   Un emisor de Syslog que utilice SSL para conectarse mostrará un estado conectado cuando haya una conexión SSL activa. Los emisores de Syslog que utilicen UDP no mostrarán ningún valor para Estado.
7. Para cada formato de syslog que el emisor admita, seleccione **Add (Añadir)** para añadir un perfil de análisis de Syslog a la lista de filtros. Seleccione el **Event Type (Tipo de evento)** para cuya identificación se ha configurado cada perfil: **login (inicio de sesión)** (predeterminado) o **logout (cierre de sesión)**.
8. (Opcional) Si los mensajes de syslog no contienen información de dominio y sus asignaciones de usuario requieren nombres de dominio, ingrese un **Default Domain Name (Nombre de dominio predeterminado)** para anexar a las asignaciones.
9. Haga clic en **OK (Aceptar)** para guardar los ajustes.

STEP 6 | Habilite los servicios del receptor de syslog en la interfaz que el cortafuegos utiliza para recopilar asignaciones de usuario.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaces)** y modifique un perfil de gestión de interfaz existente o seleccione **Add (Añadir)** para añadir un nuevo perfil.
2. Seleccione **User-ID Syslog Listener-SSL** o **User-ID Syslog Listener-UDP**, o ambos, dependiendo de los protocolos que definió para los emisores de syslog en la lista de supervisión de servidores.

   Los puertos de recepción (514 para UDP y 6514 para SSL) no son configurables; están habilitados a través del servicio de gestión únicamente.
3. Haga clic en **Aceptar** para guardar el perfil de gestión de interfaz.

© 2020 Palo Alto Networks, Inc.

Incluso después de habilitar el servicio de recepción de syslog User-ID en la interfaz, esta solamente aceptará conexiones con syslog desde emisores que tengan una entrada correspondiente en la configuración de los servidores supervisados de User-ID. El cortafuegos descartará las conexiones o los mensajes de emisores que no estén en esta lista.

4. Asigne el perfil de gestión de interfaz a la interfaz que el cortafuegos utiliza para recopilar asignaciones de usuario:
   1. Seleccione **Network (Red)** > **Interfaces** y modifique la interfaz.
   2. Seleccione **Advanced (Avanzado)** > **Other info (Otra información)**, seleccione la interfaz **Management Profile (Perfil de gestión)** que acaba de agregar y haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

STEP 7 | Verifique que el cortafuegos añada y elimine asignaciones de usuario cuando los usuarios inician o cierran sesión.

Puede usar comandos CLI para ver información adicional sobre emisores syslog, mensajes syslog y asignaciones de usuario.

1. Inicie sesión en un sistema cliente para el cual un emisor syslog supervisado genere mensajes de evento de inicio y cierre de sesión.
2. Inicie sesión en la CLI del cortafuegos.
3. Verifique que el cortafuegos haya asignado el nombre de usuario de inicio de sesión a la dirección IP del cliente:

```
> show user ip-user-mapping ip <ip-address>
IP address:    192.0.2.1 (vsys1)
User:          localdomain\username
From:          SYSLOG
```

4. Cierre sesión en el sistema cliente.
5. Verifique que el cortafuegos haya eliminado la asignación de usuario:

```
> show user ip-user-mapping ip <ip-address>
No matched record
```

Configuración del agente de User-ID de Windows como receptor de Syslog

Para configurar el agente de User-ID basado en Windows para crear nuevas asignaciones de usuario y eliminar asignaciones obsoletas a través del control de syslog, comience por definir los perfiles de análisis de Syslog. El agente de User-ID utiliza los perfiles para encontrar eventos de inicio y cierre de sesión en mensajes de syslog. En entornos en los que los *emisores de syslog* (los servicios de red que autentican a los usuarios) envían mensajes de syslog en diferentes formatos, configure un perfil para cada formato de syslog. Los mensajes de syslog deben cumplir ciertos criterios para que un agente de User-ID los analice (consulte Syslog). Este procedimiento utiliza ejemplos con los siguientes formatos:

- Eventos de inicio de sesión: `[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- Eventos de cierre de sesión: `[Tue Jul 5 13:18:05 2016 CDT] User logout successful User:johndoe1 Source:192.168.3.212`

© 2020 Palo Alto Networks, Inc.

Después de configurar los perfiles de análisis de Syslog, debe especificar los emisores de syslog para que el agente de User-ID supervise.

El agente de User-ID de Windows acepta Syslogs únicamente a través de TCP y UDP. Sin embargo, debe tener precaución a la hora de usar UDP para recibir mensajes de syslog, ya que no es un protocolo fiable y, como tal, no hay manera de verificar que un mensaje se haya enviado desde un emisor syslog de confianza. Aunque puede restringir los mensajes de syslog a direcciones IP de origen específicas, esto no impide a los atacantes replicar la dirección IP, lo que permite la inyección de mensajes de syslog no autorizados en el cortafuegos. Se recomienda utilizar TCP en lugar de UDP. En ambos casos, asegúrese de que tanto el servidor syslog como el cliente de syslog estén en una VLAN dedicada y segura, para evitar que hosts no fiables envíen syslogs al agente User-ID.

STEP 1 | Implemente los agentes de User-ID basados en Windows si aún no lo ha hecho.

1. Instale el agente de User-ID basado en Windows.
2. Configure los cortafuegos para conectarlos al agente de User-ID.

STEP 2 | Defina los perfiles de análisis de Syslog para crear y eliminar asignaciones de usuario.

Cada perfil filtra los mensajes syslog para identificar eventos de inicio de sesión (para crear asignaciones de usuario) o eventos de cierre de sesión (para eliminar asignaciones), pero ningún perfil puede hacer ambas cosas.

1. Revise los mensajes syslog que el emisor syslog genera para identificar la sintaxis de los eventos de inicio y cierre de sesión. Esto le permite identificar los patrones coincidentes al crear perfiles de análisis de Syslog.

   Al revisar mensajes syslog, determine también si incluyen el nombre de dominio. Si no lo incluyen y sus asignaciones de usuario requieren nombres de dominio, ingrese el Default Domain Name (Nombre de dominio predeterminado) al definir los emisores syslog que el agente de User-ID supervisa (en pasos posteriores de este procedimiento).
2. Abra el menú **Inicio** de Windows y seleccione **User-ID Agent**.
3. Seleccione **User Identification (Identificación de usuario)** > **Setup (Configuración)** y luego **Edit (Editar)** para modificar la configuración.
4. Seleccione **Syslog**, **Enable Syslog Service (Habilitar servicio de Syslog)** y luego **Add (Añadir)** para añadir un perfil de análisis de Syslog.
5. Introduzca un **Nombre de perfil** y una **Descripción**.
6. Seleccione el **Type (Tipo)** de análisis para encontrar eventos de inicio o cierre de sesión en los mensajes de syslog:
   - **Regex**: expresiones regulares.
   - **Field (Campo)**: cadenas de texto.

   Los siguientes pasos describen cómo configurar estos tipos de análisis.

STEP 3 | (**Análisis de regex únicamente**) Defina los patrones de coincidencia de regex.

Si el mensaje syslog contiene un espacio o una tabulación independiente como delimitador, debe utilizar **`\s`** para un espacio y **`\t`** para una tabulación.

1. Ingrese el **Event Regex (Regex de evento)** para el tipo de evento que desea encontrar:
   - **Eventos de inicio de sesión:** para el mensaje de ejemplo, la regex **`(authentication\ success){1}`** extrae la primera instancia **`{1}`** de la cadena `authentication success`.

© 2020 Palo Alto Networks, Inc.

- **Eventos de cierre de sesión:** para el mensaje de ejemplo, la regex **`(logout\ successful){1}`** extrae la primera instancia **`{1}`** de la cadena `logout successful`.

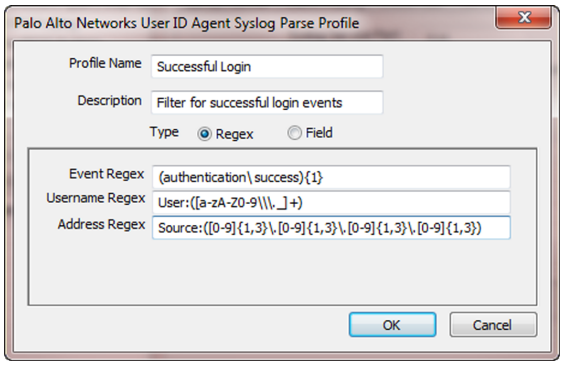
La barra invertida antes del espacio es un carácter regex de "escape" estándar que indica al motor de regex que no trate el espacio como carácter especial.

2. Ingrese el **Username Regex (Regex de nombre de usuario)** para identificar el inicio del nombre de usuario.

   En el mensaje de ejemplo, la regex **`User:([a-zA-Z0-9\\\._]+)`** coincidiría con la cadena `User:johndoe1` e identificaría `johndoe1` como el nombre de usuario.
3. Ingrese la **Address Regex (Regex de dirección)** para identificar la parte de la dirección IP de los mensajes syslog.

   En el mensaje de ejemplo, la expresión regular **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** coincide con la dirección IPv4 `Source:192.168.3.212`.

   El siguiente es un ejemplo de un perfil de análisis de Syslog que utiliza regex para identificar eventos de inicio de sesión:



4. Haga clic en **OK (Aceptar)** dos veces para guardar el perfil.

STEP 4 | (**Análisis de identificador de campo únicamente**) Defina los patrones de coincidencia de cadena.

1. Ingrese una **Event String (Cadena de evento)** para identificar el tipo de eventos que desea encontrar:
   - **Eventos de inicio de sesión:** para el mensaje de ejemplo, la cadena `authentication success` identifica los eventos de inicio de sesión.
   - **Eventos de cierre de sesión:** para el mensaje de ejemplo, la cadena `logout successful` identifica los eventos de cierre de sesión.
2. Ingrese un **Username Prefix (Prefijo de nombre de usuario)** para identificar el inicio del campo de nombre de usuario en los mensaje de syslog. Este campo no admite regex como \s (para un espacio) o \t (para una pestaña).

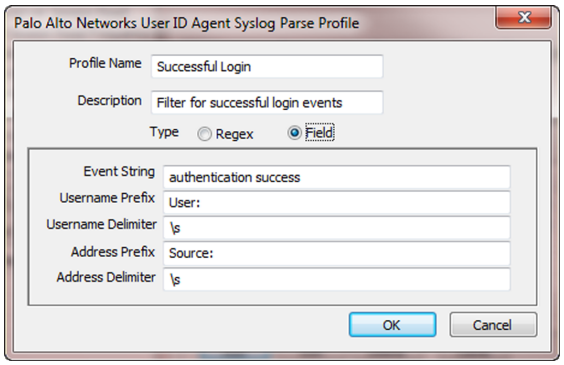
   En los mensajes de ejemplo, `User:` identifica el inicio del campo del nombre de usuario.
3. Ingrese el **Username Delimiter (Delimitador de nombre de usuario)** que indica el final del campo del nombre de usuario en los mensaje de syslog. Utilice **`\s`** para indicar un espacio independiente (como en el mensaje de ejemplo) y **`\t`** para indicar tabulación.
4. Ingrese un **Address Prefix (Prefijo de dirección)** para identificar el inicio del campo de dirección IP en los mensaje de syslog. Este campo no admite regex como \s (para un espacio) o \t (para una pestaña).

   En los mensajes de ejemplo, `Source:` identifica el inicio del campo de dirección.
5. Ingrese el **Address Delimiter (Delimitador de dirección)** que indica el final del campo del nombre de dirección en los mensaje de syslog.

   Por ejemplo, introduzca \n para indicar que el delimitador es un salto de línea.

© 2020 Palo Alto Networks, Inc.

El siguiente es un ejemplo de un perfil de análisis de Syslog completo que utiliza la coincidencia de cadenas para identificar eventos de inicio de sesión:



6. Haga clic en **OK (Aceptar)** dos veces para guardar el perfil.

STEP 5 | Especifique los emisores de syslog que el agente de User-ID supervisa.

Dentro del máximo total de 100 servidores de todos los tipos que el agente de User-ID puede supervisar, hasta 50 pueden ser emisores de syslog.

El agente de User-ID descartará los mensajes de Syslog recibidos de emisores que no estén en esta lista.

1. Seleccione **User Identification (Identificación de usuario)** > **Discovery (Detección)** y haga clic en **Add (Añadir)** para añadir una entrada en la lista de servidores.
2. Ingrese un nombre en **Name** para identificar el emisor.
3. Ingrese la **Server Address (Dirección de servidor)** del emisor de syslog (dirección IP o FQDN).
4. Configure el **Server Type (Tipo de servidor)** en **Syslog Sender (Emisor de Syslog)**.
5. (**Opcional**) Si desea anular el dominio actual en el nombre de usuario de syslog o desea que el dominio preceda al nombre de usuario si su mensaje syslog no contiene un dominio, introduzca un **Default Domain Name (Nombre de dominio predeterminado)**.
6. Para cada formato de syslog que el emisor admita, seleccione **Add (Añadir)** para añadir un perfil de análisis de Syslog a la lista de filtros. Seleccione el **Event Type (Tipo de evento)** para cuya identificación configuró cada perfil: **login (inicio de sesión)** (opción predeterminada) o **logout (cierre de sesión)**, y luego haga clic en **OK (Aceptar)**.
7. Haga clic en **OK (Aceptar)** para guardar los ajustes.
8. Seleccione **Commit (Confirmar)** para confirmar los cambios a la configuración del agente de User-ID.

STEP 6 | Verifique que el agente de User-ID añada y elimine asignaciones de usuario cuando los usuarios inician o cierran sesión.

Puede usar comandos CLI para ver información adicional sobre emisores syslog, mensajes syslog y asignaciones de usuario.

1. Inicie sesión en un sistema cliente para el cual un emisor syslog supervisado genere mensajes de evento de inicio y cierre de sesión.
2. Verifique que el agente de User-ID haya asignado el nombre de usuario de inicio de sesión a la dirección IP del cliente:
   1. En el agente de User-ID, seleccione **Monitoring (Supervisión)**.
   2. Ingrese el nombre de usuario o la dirección IP en el campo de filtro, seleccione **Search (Buscar)**, y verifique que la lista muestre la asignación.
3. Verifique que el cortafuegos reciba la asignación de usuario del agente de User-ID:
   1. Inicie sesión en la CLI del cortafuegos.

© 2020 Palo Alto Networks, Inc.

2. Ejecute el siguiente comando:

```
> show user ip-user-mapping ip <ip-address>
```

Si el cortafuegos recibió la asignación de usuario, el resultado se asemeja al siguiente:

```
IP address:    192.0.2.1 (vsys1)
User:          localdomain\username
From:          SYSLOG
```

4. Cierre sesión en el sistema cliente.
5. Verifique que el agente de User-ID haya eliminado la asignación de usuario:
   1. En el agente de User-ID, seleccione **Monitoring (Supervisión)**.
   2. Ingrese el nombre de usuario o la dirección IP en el campo de filtro, seleccione **Search (Buscar)**, y verifique que la lista no muestre la asignación.
6. Verifique que el cortafuegos haya eliminado la asignación de usuario:
   1. Acceda a la CLI del cortafuegos.
   2. Ejecute el siguiente comando:

```
> show user ip-user-mapping ip <ip-address>
```

Si el cortafuegos eliminó la asignación de usuario, el resultado se verá como el siguiente:

```
No matched record
```

Asignación de direcciones IP a nombres de usuario mediante un portal de autenticación

Cuando un usuario inicia un tráfico web (HTTP o HTTPS) que coincide con una regla de Política de autenticación, el cortafuegos solicita al usuario que se autentique con el portal de autenticación. Esto garantiza que conozca exactamente quién accede a sus aplicaciones y datos más delicados. En función de la información del usuario que se recoge durante la autenticación, el cortafuegos crea una nueva asignación de dirección IP a nombre de usuario o actualiza la asignación existente para ese usuario. Este método de asignación de usuario es útil en los entornos en donde el cortafuegos no puede obtener información sobre las asignaciones mediante otros métodos como los servidores de supervisión. Por ejemplo, puede contar con usuarios que no iniciaron sesión en sus servidores de dominio supervisados, como usuarios en clientes Linux.

- Métodos de autenticación del portal de autenticación
- Modos del portal de autenticación
- Configuración del portal de autenticación

Métodos de autenticación del portal de autenticación

El portal de autenticación utiliza los siguientes métodos para autenticar a los usuarios cuyas solicitudes web coinciden con las reglas de la Política de autenticación:

© 2020 Palo Alto Networks, Inc.

Authentication Method	Description (Descripción)
Kerberos SSO	El cortafuegos utiliza el inicio de sesión único (SSO) de Kerberos para obtener credenciales de usuario del explorador de forma transparente. Para usar este método, su red requiere una infraestructura Kerberos que incluya un centro de distribución de claves (KDC) con un servidor de autenticación y servicios de concesión de tickets. El cortafuegos no debe tener una cuenta de Kerberos. Si se produce un error en la autenticación del SSO de Kerberos, el cortafuegos retrocederá a una autenticación con formato web o certificado de cliente, en función de su política de autenticación y la configuración del portal de autenticación.
Formato web	El cortafuegos redirige solicitudes a un formato web para su autenticación. Para implementar este método, puede configurar la política de autenticación para que utilice la autenticación multifactor (MFA); la autenticación SAML, Kerberos, TACACS+, RADIUS, o la autenticación LDAP. Aunque los usuarios deben introducir manualmente sus credenciales de inicio de sesión, este método funciona con todos los exploradores y sistemas operativos.
Autenticación de certificación de cliente	El cortafuegos pide al explorador que presente un certificado de cliente válido para autenticar al usuario. Para utilizar este método debe proporcionar certificados de cliente en cada sistema de usuario e instalar el certificado de la entidad de certificación (certificate authority, CA) de confianza utilizada para emitir esos certificados en el cortafuegos.

Modos del portal de autenticación

El modo de portal de autenticación define el modo en que el cortafuegos captura solicitudes web para su autenticación:

Modo	Description (Descripción)
Transparente	El cortafuegos intercepta el tráfico del explorador mediante la regla de la política de autenticación y representa la URL de destino original, y emite un HTTP 401 para invocar la autenticación. Sin embargo, como el cortafuegos no tiene el certificado real para la URL de destino, el explorador muestra un error de certificado a los usuarios que intenten acceder a un sitio seguro. Por lo tanto, utilice este modo solo cuando sea absolutamente necesario, como en implementaciones de capa 2 o cable virtual.
Redirigir	El cortafuegos intercepta sesiones de HTTP o HTTPS desconocidas y las redirige a una interfaz de capa 3 en el cortafuegos utilizando una redirección HTTP 302 para realizar la autenticación. Este es el modo preferido porque proporciona una mejor experiencia de usuario final (sin errores de certificado). Sin embargo, requiere una configuración de capa 3 adicional. Otra ventaja del modo Redirigir es que permite el uso de cookies de sesión, que permiten que el usuario siga explorando sitios autenticados sin tener que volver a asignar cada

© 2020 Palo Alto Networks, Inc.

Modo	Description (Descripción)
	vez que venza el tiempo de espera. Esto es de especial utilidad para los usuarios que se desplazan de una dirección IP a otra (por ejemplo, de la LAN corporativa a la red inalámbrica) porque no tendrán que volver a autenticar al cambiar de dirección IP siempre que la sesión permanezca abierta. Si utiliza la autenticación del SSO de Kerberos, deberá utilizar el modo Redirigir porque el explorador únicamente proporcionará credenciales a sitios fiables. El modo Redirect (Redirigir) también es necesario si utiliza Autenticación de múltiples factores para autenticar a usuarios del portal de autenticación.

Configuración del portal de autenticación

El siguiente procedimiento muestra cómo configurar un portal de autenticación utilizando el agente de User-ID integrado en PAN-OS para redirigir solicitudes web que coincidan con una regla de Authentication Policy (Política de autenticación) a una interfaz de cortafuegos (host de redireccionamiento).

La inspección de SSL entrante no admite la redirección del portal de autenticación. Para utilizar el redireccionamiento y el descifrado del portal de autenticación, debe utilizar el proxy SSL de reenvío.

Según la sensibilidad, las aplicaciones a las que acceden los usuarios a través del portal de autenticación requieren diferentes métodos y ajustes de autenticación. Para adaptarse a todos los requisitos de autenticación, puede usar los objetos de aplicación de autenticación predeterminados y personalizados. Cada objeto se asocia a una regla de autenticación con un perfil de autenticación en un método de autenticación de portal de autenticación.

- **Objetos de aplicación de autenticación predeterminados:** utilice los objetos predeterminados si desea asociar varias reglas de autenticación al mismo perfil de autenticación global. Debe configurar este perfil de autenticación antes de configurar el portal de autenticación y, a continuación, asignarlo en los ajustes del portal de autenticación. No puede usar los objetos de cumplimiento de autenticación predeterminados para las reglas de autenticación que requieren autenticación multifactor (MFA).
- **Objetos de aplicación de autenticación personalizados:** utilice un objeto personalizado para cada regla de autenticación que requiera un perfil de autenticación que difiera del perfil global. Los objetos personalizados son obligatorios para las reglas de autenticación que requieren MFA. Para usar objetos personalizados, cree perfiles de autenticación y asígnelos a los objetos después de configurar el portal de autenticación, cuando realiza la configuración de la política de autenticación.

Tenga en cuenta que los perfiles de autenticación son necesarios solo si los usuarios se autentican a través del formulario web de un portal de autenticación o SSO de Kerberos. Como alternativa o complemento de estos métodos, el siguiente procedimiento también describe de qué manera implementar la autenticación del certificado de cliente.

Si tiene la intención de utilizar un portal de autenticación sin utilizar las otras funciones de User-ID (asignación de usuarios y grupos), no necesita configurar un agente de User-ID.

STEP 1 | Configure las interfaces que el cortafuegos usará para las solicitudes web entrantes, la autenticación de usuarios y la comunicación con servidores de directorio para asignar nombres de usuario a direcciones IP.

© 2020 Palo Alto Networks, Inc.

Cuando el cortafuegos se conecta a servidores de autenticación o agentes de User-ID, utiliza la interfaz de gestión de manera predeterminada. Se recomienda aislar la red de gestión configurando rutas de servicio para conectarse a servidores de autenticación o agentes de User-ID.

1. (Interfaz MGT únicamente) Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Interfaces**, modifique la interfaz **Management (Gestión)**, seleccione **User-ID (ID de usuario)** y haga clic en **OK (Aceptar)**.
2. (Solo interfaz no MGT) Asigne un perfil de gestión de interfaz a la interfaz de capa 3 que el cortafuegos usará para las solicitudes web entrantes o la comunicación con los servidores de directorio. Debe habilitar **Response Pages (Páginas de respuesta)** y **User ID (ID de usuario)** en el perfil de gestión de interfaz.
3. (Solo interfaces no MGT) Configure una ruta de servicio para la interfaz que usará el cortafuegos para autenticar a usuarios. Si el cortafuegos tiene más de un sistema virtual (vsys), la ruta de servicio puede ser global o específica de vsys. Los servicios deben incluir **LDAP** y, posiblemente, lo siguiente:
   - **Kerberos**, **RADIUS**, **TACACS+** o **Multi-Factor Authentication (Autenticación multifactor)**: configure una ruta de servicio para cualquier servicio de autenticación que utilice.
   - **UID Agent (Agente de UID)**: configure este servicio solo si habilita la política basada en usuarios y grupos.
4. (Modo de redireccionamiento únicamente): cree un registro de dirección DNS (A) que asigne la dirección IP de la interfaz de capa 3 al host de redireccionamiento. Si va a usar SSO de Kerberos, deberá añadir además un registro de puntero DNS (PTR) que realice la misma asignación.

Si su red no admite el acceso a los servidores de directorio desde ninguna interfaz de cortafuegos, deberá realizar la configuración de la asignación de usuarios usando el agente de ID de usuario de Windows.

STEP 2 | Asegúrese de que el sistema de nombres de dominio (DNS, Domain Name System) está configurado para resolver sus direcciones de controlador de dominio.

Para verificar que la resolución es correcta, haga ping en el FQDN del servidor. Por ejemplo:

```
admin@PA-220> ping host dc1.acme.com
```

STEP 3 | Configure los clientes para que confíen en los certificados del portal de autenticación.

Obligatorio para el modo de redireccionamiento: para redirigir usuarios de forma transparente sin mostrar errores de certificados. Utilice un certificado autofirmado o importe un certificado que haya firmado una entidad de certificación (CA) externa.

Para utilizar un certificado autofirmado, primero deberá crear un certificado de CA raíz y, a continuación, utilizarlo para firmar el certificado que usará en el portal de autenticación:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.
2. Cree un certificado CA raíz autofirmado o importe un certificado CA (consulte Importación de un certificado y clave privada).
3. Genere un certificado para usar con el portal de autenticación. Asegúrese de configurar los siguientes campos:
   - **Common Name (Nombre común)**: introduzca el nombre DNS del host de intranet para la interfaz de capa 3.
   - **Signed By**: seleccione el certificado de CA que acaba de crear o importar.
   - Atributos de certificados: haga clic en **Add (Añadir)**, en el **Type (Tipo)**, seleccione **IP** y para el **Value (Valor)**, introduzca la dirección IP de la interfaz de capa 3 a la que el cortafuegos redirigirá las solicitudes.

© 2020 Palo Alto Networks, Inc.

4. Configuración de un perfil de servicio SSL/TLS. Asigne el certificado de portal de autenticación que acaba de crear al perfil.

   Si no asigna un perfil de servicio SSL/TLS, el cortafuegos utiliza TLS 1.2 de manera predeterminada. Para utilizar una versión de TLS diferente, configure un perfil de servicio SSL/TLS con la versión de TLS que desea utilizar.

5. Configure los clientes para que confíen en el certificado:
   1. Exporte el certificado de CA que ha creado o importado.
   2. Importe el certificado como una CA raíz de confianza en todos los exploradores de cliente, ya sea configurando manualmente el explorador o añadiendo el certificado a las raíces de confianza en un objeto de directiva de grupo (GPO, Group Policy Object) de Active Directory.

STEP 4 | (Opcional) Configure la autenticación de certificado de cliente.

No necesita una secuencia o perfil de autenticación para la autenticación de certificados de cliente. Si configura tanto un perfil/secuencia de autenticación como una autenticación de certificado, los usuarios deberán autenticarse usando ambos.

1. Use un certificado de CA raíz para generar un certificado de cliente para cada usuario que se autenticará a través del portal de autenticación. La CA en este caso suele ser la CA de su empresa, no el cortafuegos.
2. Exporte el certificado de CA en el formato PEM a un sistema al que puede acceder el cortafuegos.
3. Importe el certificado CA al cortafuegos: consulte Importación de un certificado y clave privada. Después de la importación, haga clic en el certificado importado, seleccione **Trusted Root CA** y haga clic en **OK**.
4. Configuración de un perfil de certificado.
   - En el menú desplegable **Username Field**, seleccione el campo de certificado que contenga la información de la identidad del usuario.
   - En la lista **CA Certificates**, haga clic en **Add** y seleccione el certificado de CA que acaba de importar.

STEP 5 | (Opcional) Configure el portal de autenticación para el Asistente de red cautiva de Apple.

Este paso solo se requiere si usa el portal de autenticación con el Asistente de red cautiva (Captive Network Assistant, CNA) de Apple Para usar el portal de autenticación con CNA, lleve a cabo los siguientes pasos.

1. Verifique que ha especificado un FQDN para el host de redireccionamiento (no solo una dirección IP).
2. Seleccione un perfil de servicio SSL/TLS que use un certificado de firma pública para el FQDN especificado.
3. Introduzca el siguiente comando para ajustar la cantidad de solicitudes admitidas para el portal de autenticación: **`set deviceconfig setting ctd cap-portal-ask-requests <threshold-value>`**

   De manera predeterminada, el cortafuegos tiene un umbral de límite para el portal de autenticación que limita la cantidad de solicitudes a una solicitud cada dos segundos. El CNA envía varias solicitudes que pueden superar este límite, lo que puede resultar en un restablecimiento de TCP y un error del CNA. El valor de umbral recomendado es 5 (el predeterminado es uno). Este valor permitirá hasta 5 solicitudes cada dos segundos. En función de su entorno, es posible que deba configura un valor diferente. Si el valor actual no es suficiente para administrar la cantidad de solicitudes, auméntelo.

STEP 6 | Configure los ajustes del portal de autenticación.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Authentication Portal Settings (Configuración de portal de autenticación)** y modifique los ajustes.

© 2020 Palo Alto Networks, Inc.

2. **Habilite el portal de autenticación** (está habilitado de forma predeterminada).
3. Especifique el **Timer (Temporizador)**, que es el tiempo máximo en minutos que el cortafuegos retiene una asignación de dirección IP a usuario para un usuario después de que ese usuario se autentique a través del portal de autenticación (el valor predeterminado es 60; el intervalo es de 1 a 1440). Después de que el **Timer (Temporizador)** finalice, el cortafuegos elimina la asignación y las marcas de tiempo de autenticación asociadas que se utilizaron para evaluar el **tiempo de espera** en las reglas de política de autenticación.

   Al evaluar el temporizador del portal de autenticación y el valor de tiempo de espera en cada regla de política de autenticación, el cortafuegos indica al usuario que vuelva a autenticarse para el ajuste que caduque primero. Tras la nueva autenticación, el cortafuegos vuelve a establecer el recuento de tiempo del temporizador del portal de autenticación y registra las nuevas marcas de tiempo de autenticación para el usuario. Por lo tanto, para habilitar diferentes periodos de tiempo de espera para diferentes reglas de autenticación, configure el temporizador del portal de autenticación en un valor que sea igual o superior a cualquier tiempo de espera de regla.
4. Seleccione el **SSL/TLS Service Profile** que creó para redirigir las solicitudes por TLS. Consulte Configuración de un perfil de servicio SSL/TLS.
5. Seleccione el **Modo** (en este ejemplo, **Redirect**).
6. (Modo de redireccionamiento únicamente) Especifique el **Redirect Host (Host de redireccionamiento)**, que es el nombre de host de intranet (el nombre de host sin punto en su nombre) que resuelve a la dirección IP de la interfaz de capa 3 del cortafuegos a la que se redirigirán las solicitudes web.

   Si los usuarios se autentican mediante el inicio de sesión único (SSO) de Kerberos, el **Redirect Host (Host de redireccionamiento)** debe ser el mismo que el nombre de host especificado en el Kerberos keytab.
7. Seleccione el método de autenticación de retroceso que utilizar:
   - Para usar la autenticación de certificados cliente, seleccione el **Certificate Profile** que ha creado.
   - Para usar los ajustes globales para la autenticación SSO o interactiva, seleccione el **Authentication Profile (Perfil de autenticación)** que configuró.
   - Para usar los ajustes específicos de la regla de la política de autenticación para la autenticación interactiva o SSO, asigne perfiles de autenticación a los objetos de cumplimiento de autenticación cuando configure la política de autenticación.
8. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para confirmar la configuración del portal de autenticación.

STEP 7 | Pasos siguientes:

El cortafuegos no muestra el formulario web de portal de autenticación a los usuarios hasta que se configuran las reglas de la política de autenticación cuando los usuarios soliciten servicios o aplicaciones.

Configuración de la asignación de usuarios para usuarios del servidor de terminal

Los usuarios individuales del servidor de terminal parecen tener la misma dirección IP y, por lo tanto, una asignación de direcciones IP a nombres de usuarios no es suficiente para identificar a un usuario específico. Para identificar usuarios específicos en servidores de terminal basados en Windows, el agente de servidor de terminal (agente de TS) de Palo Alto Networks asignará un intervalo de puertos a cada usuario. El agente de TS notificará a cada cortafuegos conectado sobre el intervalo de puertos asignado, lo que permitirá que el cortafuegos cree una tabla de asignaciones de direcciones IP, puertos y usuarios y habilite la aplicación de políticas de seguridad basadas en usuarios y grupos. Para los servidores de terminal que no sean de

© 2020 Palo Alto Networks, Inc.

Windows, puede configurar XML API de PAN-OS para que extraiga información de asignación de usuarios. Los siguientes valores se aplican a ambos métodos:

- Intervalo de puertos predeterminado: De 1025 a 65534
- Tamaño de bloque por usuario: 200
- Número máximo de sistemas multiusuario: 2.500

Para obtener información sobre los servidores de terminal compatibles con el agente de TS y el número de agentes de TS admitido en cada modelo de cortafuegos, consulte la Matriz de compatibilidad de Palo Alto Networks y la Herramienta de comparación de productos.

Las siguientes secciones describen cómo configurar la asignación de usuarios para usuarios del servidor de terminal:

- Configuración del agente del servidor de terminal de Palo Alto Networks para la asignación de usuarios
- Recuperación de asignaciones de usuarios de un servidor de terminal mediante la API XML de PAN-OS

Configuración del agente del servidor de terminal de Palo Alto Networks para la asignación de usuarios

Utilice el siguiente procedimiento para instalar y configurar el agente de TS en el servidor de terminal. Para asignar a todos sus usuarios, debe instalar el agente de TS en todos los servidores de terminal en los que sus usuarios inicien sesión.



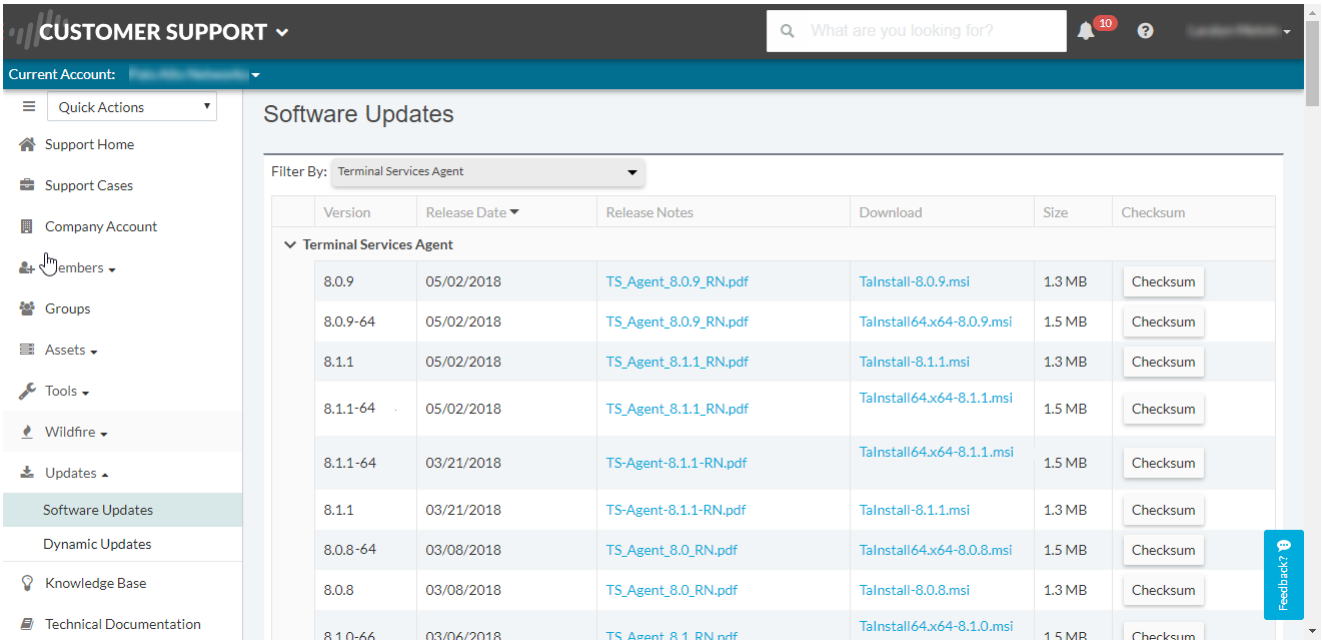
Si usa el agente de TS 7.0 o una versión posterior, deshabilite cualquier software antivirus Sophos en el host del agente de TS. De lo contrario, el software antivirus sobrescribe los puertos de origen que asigna el agente de TS.

Para obtener información sobre valores predeterminados, intervalos y otras especificaciones, consulte Configuración de la asignación de usuarios para usuarios del servidor de terminal*. Para obtener información sobre los servidores de terminal compatibles con el agente de TS y el número de agentes de TS admitido en cada modelo de cortafuegos, consulte la* Matriz de compatibilidad de Palo Alto Networks*.*

STEP 1 | Descargue el instalador de agente de TS.

1. Inicie sesión en el Portal de atención al cliente de Palo Alto Networks.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.
3. Configure **Filter By (Filtrar por)** en **Terminal Services Agent (Agente de servicios de terminal)** y seleccione la versión del agente que desea instalar desde la columna Download (Descarga) correspondiente. Por ejemplo, para descargar el agente de TS 9.0, seleccione **TaInstall-9.0.msi**.
4. Guarde el archivo `TaInstall.x64-x.x.x-xx.msi` o `TaInstall-x.x.x-xx.msi` en los sistemas en los que tenga intención de instalar el agente; asegúrese de seleccionar la versión adecuada dependiendo de si el sistema Windows utiliza un SO de 32 bits o de 64 bits.

© 2020 Palo Alto Networks, Inc.



STEP 2 | Ejecute el instalador como administrador.

1. Abra el menú de **Inicio** de Windows, haga clic con el botón derecho en el programa **Símbolo del sistema** y **Ejecutar como administrador**.
2. Desde la línea de comandos, ejecute el archivo .msi que ha descargado. Por ejemplo, si guardó el archivo `TaInstall-9.0.msi` en el escritorio, introduzca lo siguiente:

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. Siga los mensajes de configuración para instalar el agente con los ajustes predeterminados. La configuración instala el agente en `C:\ProgramFiles (x86)\Palo Alto Networks\Terminal Server Agent`.

   Para garantizar la asignación correcta de puertos, debe usar la ubicación predeterminada de la carpeta de instalación del agente de servidor de terminal predeterminada.
4. Cuando finalice la instalación, **cierre** el cuadro de diálogo de configuración.

   Si está actualizando a una versión de agente de TS con un controlador más reciente que el de la instalación existente, el asistente de instalación le solicitará reiniciar el sistema después de actualizar.

STEP 3 | Defina el intervalo de puertos para el agente de TS que debe asignarse a los usuarios finales.

Los campos Intervalo de asignación del puerto de origen del sistema y Puertos de origen reservados del sistema especifican el intervalo de puertos que se asignará a las sesiones que no sean de usuarios. Asegúrese de que los valores de estos campos no se solapen con los puertos que designó para el tráfico de usuarios. Estos valores solo pueden cambiarse editando los correspondientes ajustes de registro de Windows. El agente de TS no asigna puertos para el tráfico de red emitido por la sesión 0.

1. Abra el menú **Inicio** de Windows y seleccione **Terminal Server Agent (Agente de servidor de terminal)** para iniciar la aplicación de agente de servidor de terminal.

© 2020 Palo Alto Networks, Inc.

2. **Configure** (menú lateral) el agente.
3. Introduzca el **Source Port Allocation Range** (valor predeterminado: 20,000-39,999). Este es el intervalo completo de números de puertos que el agente de TS adjudicará para la asignación de usuarios. El intervalo de puertos que especifique no puede solaparse con el **intervalo de asignación del puerto de origen del sistema**.
4. (Opcional) Si hay puertos o intervalos de puertos en la asignación del puerto de origen que no desea que el agente de TS adjudique a sesiones de usuario, especifíquelos como **Reserved Source Ports (Puertos de origen reservados)**. Para incluir varios intervalos, utilice comas sin espacios, por ejemplo: `2000-3000, 3500, 4000-5000`).
5. Especifique el número de puertos que deben asignarse a cada usuario individual tras su inicio de sesión en el servidor de terminal (**Port Allocation Start Size Per User (Tamaño de inicio de asignación de puertos por usuario)**); el valor predeterminado es 200.
6. Especifique el **Port Allocation Maximum Size Per User (Tamaño máximo de asignación de puerto por usuario)**, que es el número máximo de puertos que el agente de servidor de terminal puede asignar a un usuario individual.
7. Especifique si desea continuar procesando el tráfico del usuario si el usuario se queda sin puertos asignados. La opción **Fail port binding when available ports are used up (Fallo en el enlace de puertos cuando se utilizan los puertos disponibles)** está habilitada de forma predeterminada e indica que la aplicación no enviará tráfico cuando se hayan utilizado todos los puertos. Para permitir que los usuarios continúen usando aplicaciones cuando se queden sin puertos, deshabilite (desactive) esta opción, pero si lo hace, es posible que este tráfico no se identifique con User-ID.
8. Si el servidor terminal deja de responder cuando intenta apagarlo, habilite la opción **Detach agent driver at shutdown (Desconectar controlador de agente al apagar)**.

STEP 4 | (Opcional) Asigne sus propios certificados para la autenticación mutua entre el agente de TS y el cortafuegos.

1. Obtenga el certificado para el agente de TS de la infraestructura de claves públicas (public key infrastructure, PKI) de su empresa o genere uno en el cortafuegos. La clave privada del certificado del servidor debe estar cifrada y el certificado debe estar cargado en formato de archivo PEM. Realice una de las siguientes tareas para cargar un certificado:
   - Genere un certificado y expórtelo.
   - Exporte un certificado de la entidad de certificación (Certificate Authority, CA) de la empresa
2. Añada un certificado de servidor en el agente de TS.
   1. En el agente de TS, seleccione **Server Certificate (Certificado de servidor)** y **añada** un nuevo certificado.
   2. Ingrese la ruta y el nombre del archivo de certificado que recibió de la CA o busque el archivo de certificado.
   3. Ingrese la contraseña de clave privada.
   4. Haga clic en **OK (Aceptar)**.
   5. **Commit (Confirmar)** los cambios.

   El agente de TS usa un certificado autofirmado en el puerto 5009 con la siguiente información:Issuer: CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=USSubject: CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=US
3. Configure y asigne el perfil de certificado para el cortafuegos.
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)** y configure un perfil de certificado.

      Solo puede asignar un perfil de certificado para los agentes de User-ID de Windows y los agentes de TS. Por lo tanto, su perfil de certificado debe incluir

© 2020 Palo Alto Networks, Inc.

todas las autoridades de certificado que emitieron certificados cargados en los agentes de TS e ID de usuario de Windows conectados.

2. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **Connection Security (Seguridad de conexión)**.
3. Edite () y seleccione el perfil de certificado que ha configurado en el paso anterior como **perfil de certificado de ID de usuario**.
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

STEP 5 | Configure el cortafuegos para conectarlo al agente de servidor de terminal.

Realice los siguientes pasos en cada cortafuegos que desee conectar al agente de servidor de terminal para recibir asignaciones de usuarios:

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Terminal Server Agents (Agentes de servidor de terminal)** y **añada** un nuevo agente de TS.
2. Introduzca un **nombre** para el agente de servidor de terminal.
3. Introduzca en **Host** el nombre de host o la dirección IP del host de Windows en el que está instalado el agente de servidor de terminal.

   El nombre de host o la dirección IP se deben resolver en una dirección IP estática. Si modifica el nombre de host existente, al confirmar los cambios, se reanuda el agente de TS para resolver el nuevo. Si el nombre de host se resuelve en varias direcciones IP, el agente de TS utiliza la primera de la lista.
4. (Opcional) En **Alternative IP Addresses (Direcciones IP alternativas)**, introduzca el nombre de host o la dirección IP de cualquier otra dirección IP que pueda actuar como origen del tráfico saliente.

   El nombre de host o la dirección IP se deben resolver en una dirección IP estática. Puede introducir hasta ocho direcciones IP o nombres de host.
5. Introduzca el número de **Port (Puerto)** en el que el agente escuchará solicitudes de asignación de usuarios. Este valor debe coincidir con el valor configurado en el agente de servidor de terminal. De manera predeterminada, el puerto se establece como 5009 en el cortafuegos y en el agente. Si lo cambia en el cortafuegos, también debe cambiar el **puerto de escucha** en el cuadro de diálogo de **configuración** del agente de servidor de terminal al mismo puerto.
6. Asegúrese de que la configuración esté **Enabled (Habilitada)** y, a continuación, haga clic en **OK (Aceptar)**.
7. **Commit (Confirmar)** los cambios.
8. Verifique que el estado **Connected (Conectado)** aparezca como conectado (luz verde).

STEP 6 | Verifique que el agente de servidor de terminal está asignando correctamente direcciones IP a nombres de usuarios y que los cortafuegos pueden conectarse con el agente.

1. Abra el menú **Inicio** de Windows y seleccione **Terminal Server Agent**.
2. Verifique que los cortafuegos puedan conectarse asegurándose de que el **Connection Status (Estado de conexión)** de cada cortafuegos de la lista de conexión sea `Connected (Conectado)`.
3. Compruebe que el agente de servidor de terminal esté asignando correctamente intervalos de puertos a nombres de usuarios (**Monitoring (Supervisión)** en el menú lateral) y asegúrese de que la tabla de asignaciones está cumplimentada.

STEP 7 | (Servidores Windows 2012 R2 únicamente) Deshabilite el modo protegido mejorado de Microsoft Internet Explorer para cada usuario que utilice ese navegador.

Esta tarea no es necesaria para otros navegadores tales como Google Chrome o Mozilla Firefox.

© 2020 Palo Alto Networks, Inc.

Para deshabilitar el modo protegido mejorado para todos los usuarios, use la política de seguridad local*.*

Siga los pasos a continuación en Windows Server:

1. Inicie Internet Explorer.
2. Seleccione **Settings (Configuración)** > **Internet options (Opciones de Internet)** > **Advanced (Avanzado)** y desplácese hasta la sección Security (Seguridad).
3. Deshabilite (quite) la opción **Enable Enhanced Protected Mode (Habilitar modo protegido mejorado)**.
4. Haga clic en **OK (Aceptar)**.

En Internet Explorer, Palo Alto Networks recomienda que no deshabilite el modo protegido, que es diferente del modo protegido mejorado.

Recuperación de asignaciones de usuarios de un servidor de terminal mediante la API XML de PAN-OS

La API XML de PAN-OS utiliza solicitudes HTTP estándar para enviar y recibir datos. Las llamadas de la API se pueden realizar directamente desde utilidades de la línea de comandos como cURL o usando cualquier secuencia de comandos o marco de aplicaciones que sea compatible con los servicios de la REST.

Para habilitar un servidor de terminal que no sea de Windows para que envíe información de asignación de usuarios directamente al cortafuegos, cree secuencias de comandos que extraigan los eventos de inicio de sesión y cierre de sesión de usuarios y utilícelas para introducirlos en el formato de solicitud de API XML de PAN-OS. A continuación defina los mecanismos para enviar solicitudes de API XML al cortafuegos utilizando cURL o wget y proporcionando la clave de API del cortafuegos para lograr comunicaciones seguras. La creación de asignaciones de usuarios desde sistemas multiusuario como servidores de terminal requiere el uso de los siguientes mensajes de la API:

- **<multiusersystem>**: Establece la configuración para un sistema multiusuario de la API XML en el cortafuegos. Este mensaje permite la definición de la dirección IP de servidor de terminal (esta será la dirección de origen para todos los usuarios de ese servidor de terminal). Además, el mensaje de configuración **<multiusersystem>** especifica el intervalo de números de puertos de origen que debe adjudicarse para la asignación de usuarios y el número de puertos que debe adjudicarse a cada usuario individual después de iniciar sesión (lo que se denomina *tamaño de bloque*). Si quiere utilizar el intervalo de asignación del puerto de origen predeterminado (1025-65534) y el tamaño de bloque (200), no necesita enviar un evento de configuración **<multiusersystem>** al cortafuegos. En vez de eso, el cortafuegos generará automáticamente la configuración del sistema multiusuario de la API XML con los ajustes predeterminados tras recibir el primer mensaje de evento de inicio de sesión de usuario.
- **<blockstart>**: se utiliza con los mensajes **<login>** y **<logout>** para indicar el número de puerto de origen de partida asignado al usuario. A continuación, el cortafuegos utiliza el tamaño de bloque para determinar el intervalo de números de puertos que debe asignarse a la dirección IP y al nombre de usuario del mensaje de inicio de sesión. Por ejemplo, si el valor de **<blockstart>** es 13200 y el tamaño de bloque configurado para el sistema multiusuario es 300, el intervalo del puerto de origen asignado al usuario es del 13200 al 13499. Cada conexión iniciada por el usuario debería utilizar un número de puerto de origen exclusivo dentro del intervalo asignado, lo que permite que el cortafuegos identifique al usuario basándose en sus asignaciones de direcciones IP, puertos y usuarios para la aplicación de reglas de políticas de seguridad basadas en usuarios y grupos. Cuando un usuario agota todos los puertos asignados, el servidor de terminal debe enviar un nuevo mensaje **<login>** que asigne un nuevo intervalo de puertos al usuario con el fin de que el cortafuegos pueda actualizar la asignación de direcciones IP, puertos y usuarios. Además, un único nombre de usuario puede tener varios bloques

© 2020 Palo Alto Networks, Inc.

de puertos asignados simultáneamente. Cuando un cortafuegos recibe un mensaje **<logout>** que incluye un parámetro **<blockstart>**, elimina la correspondiente asignación de dirección IP, puerto y usuario de su tabla de asignaciones. Cuando el cortafuegos recibe un mensaje **<logout>** con un nombre de usuario y una dirección IP, pero sin **<blockstart>**, elimina al usuario de su tabla. Y si el cortafuegos recibe un mensaje **<logout>** únicamente con una dirección IP, elimina el sistema multiusuario y todas las asignaciones asociadas al mismo.

Los archivos XML que el servidor de terminal envía al cortafuegos pueden contener varios tipos de mensajes, y estos mensajes no tienen que estar en ningún orden específico dentro del archivo. Sin embargo, al recibir un archivo XML que contenga varios tipos de mensajes, el cortafuegos los procesará en el siguiente orden: solicitudes multiusersystem en primer lugar, seguidas de inicios de sesión y cierres de sesión.

El siguiente flujo de trabajo ofrece un ejemplo de cómo utilizar la API XML de PAN-OS para enviar asignaciones de usuarios desde un servidor de terminal que no sea de Windows al cortafuegos.

STEP 1 | Genere la clave de API que se utilizará para autenticar la comunicación de la API entre el cortafuegos y el servidor de terminal. Para generar la clave, debe proporcionar credenciales de inicio de sesión para una cuenta administrativa; la API está disponible para todos los administradores (incluidos los administradores basados en funciones con privilegios de la API XML habilitados).

Todos los caracteres especiales de la contraseña deben estar codificados con URL/ porcentaje.

Desde un explorador, inicie sesión en el cortafuegos. A continuación, para generar la clave de API para el cortafuegos, abra una nueva ventana del explorador e introduzca la siguiente URL:

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

donde <Firewall-IPaddress> es la dirección IP o FQDN del cortafuegos y <username> y <password> son las credenciales para la cuenta de usuario administrativo del cortafuegos. Por ejemplo:

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

El cortafuegos responde con un mensaje que contiene la clave, por ejemplo:

```
<response status="success">
   <result>
      <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
   </result>
</response>
```

STEP 2 | (Opcional) Genere un mensaje de configuración que el servidor de terminal enviará para especificar el intervalo de puertos y el tamaño de bloque de los puertos por usuario que utiliza su agente de servidor del terminal.

Si el agente de servidor del terminal no envía un mensaje de configuración, el cortafuegos automáticamente creará una configuración de agente de servidor de terminal mediante los siguientes ajustes predeterminados tras recibir el primer mensaje de inicio de sesión:

- Intervalo de puertos predeterminado: De 1025 a 65534

© 2020 Palo Alto Networks, Inc.

- Tamaño de bloque por usuario: 200
- Número máximo de sistemas multiusuario: 1000

A continuación puede ver un mensaje de configuración de muestra:

```
<uid-message>
  <payload>
<multiusersystem>
<entry ip="10.1.1.23" startport="20000"          endport="39999"
 blocksize="100/">
</multiusersystem>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

donde `entry ip` especifica la dirección IP asignada a los usuarios del servidor de terminal, `startport` y `endport` especifican el intervalo de puertos que debe utilizarse al asignar puertos a usuarios individuales y `blocksize` especifica el número de puertos que debe asignarse a cada usuario. El tamaño de bloque máximo es 4000 y cada sistema multiusuario puede asignar un máximo de 1000 bloques.

Si define un tamaño de bloque y/o intervalo de puertos personalizado, recuerde que debe configurar los valores de modo que se asignen todos los puertos del intervalo y que no haya huecos ni puertos sin utilizar. Por ejemplo, si establece el intervalo de puertos como 1000-1499, podría establecer el tamaño de bloque como 100, pero no como 200. Esto se debe a que si lo estableciera como 200, habría puertos sin utilizar al final del intervalo.

STEP 3 | Cree una secuencia de comandos que extraiga los eventos de inicio de sesión y cree el archivo de entrada XML que debe enviarse al cortafuegos.

Asegúrese de que la secuencia de comandos aplica la asignación de intervalos de números de puertos con límites fijos y sin que los puertos se solapen. Por ejemplo, si el intervalo de puertos es 1000-1999 y el tamaño de bloque es 200, los valores aceptables de blockstart serían 1000, 1200, 1400, 1600 o 1800. Los valores de blockstart 1001, 1300 o 1850 no serían aceptables porque algunos de los números de puertos del intervalo se quedarían sin utilizar.

La carga de eventos de inicio de sesión que el servidor de terminal envía al cortafuegos puede contener varios eventos de inicio de sesión.

A continuación se muestra el formato del archivo de entrada de un evento de inicio de sesión XML de PAN-OS:

```
<uid-message>
<payload>
<login>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\jparker" ip="10.1.1.23" blockstart="20100">
<entry name="acme\ccrisp" ip="10.1.1.23" blockstart="21000">
</login>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

El cortafuegos utiliza esta información para completar su tabla de asignación de usuarios. Sobre la base de las asignaciones extraídas del ejemplo anterior, si el cortafuegos recibiera un paquete cuya dirección y

© 2020 Palo Alto Networks, Inc.

cuyo puerto de origen fueran 10.1.1.23:20101, asignaría la solicitud al usuario jparker para la aplicación de políticas.

Cada sistema multiusuario puede asignar un máximo de 1.000 bloques de puertos.

STEP 4 | Cree una secuencia de comandos que extraiga los eventos de cierre de sesión y cree el archivo de entrada XML que debe enviarse al cortafuegos.

Tras recibir un mensaje de evento `logout` con un parámetro `blockstart`, el cortafuegos elimina la correspondiente asignación de dirección IP, puerto y usuario. Si el mensaje `logout` contiene un nombre de usuario y una dirección IP, pero ningún parámetro `blockstart`, el cortafuegos eliminará todas las asignaciones del usuario. Si el mensaje `logout` solamente contiene una dirección IP, el cortafuegos eliminará el sistema multiusuario y todas las asignaciones asociadas.

A continuación se muestra el formato del archivo de entrada de un evento de cierre de sesión XML de PAN-OS:

```
<uid-message>
<payload>
<logout>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\ccrisp" ip="10.1.1.23">
<entry ip="10.2.5.4">
</logout>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

También puede borrar del cortafuegos la entrada del sistema multiusuario mediante el siguiente comando de la CLI: ***`clear xml-api multiusersystem`***

STEP 5 | Asegúrese de que las secuencias de comandos que cree incluyan un modo de aplicar dinámicamente que el intervalo de bloques de puertos asignado mediante la API XML coincida con el puerto de origen asignado al usuario en el servidor de terminal y que la asignación se elimine cuando el usuario cierre sesión o cuando cambie la asignación de puertos.

Una forma de hacerlo sería utilizar reglas de NAT netfilter para ocultar sesiones de usuarios detrás de los intervalos de puertos específicos asignados a través de la API XML basándose en el UID. Por ejemplo, para garantizar que un usuario cuyo User-ID sea jjaso se asigne a una traducción de direcciones de red de origen (SNAT) cuyo valor sea 10.1.1.23:20000-20099, la secuencia de comandos que cree debería incluir lo siguiente:

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner jjaso -p
 tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

Del mismo modo, las secuencias de comandos que cree también deben garantizar que la configuración de enrutamiento de la tabla de IP elimine dinámicamente la asignación de SNAT cuando el usuario cierre sesión o cambie la asignación de puertos:

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```

STEP 6 | Defina cómo empaquetar los archivos de entrada XML que contienen los eventos de configuración, inicio de sesión y cierre de sesión en mensajes wget o cURL para su transmisión al cortafuegos.

© 2020 Palo Alto Networks, Inc.

Para aplicar los archivos al cortafuegos mediante wget:

```
> wget --post file <filename> "https://<Firewall-
IPaddress>/api/?type=user-id&key=<key>&file-
name=<input_filename.xml>&client=wget&vsys=<VSYS_name>"
```

Por ejemplo, la sintaxis para enviar un archivo de entrada denominado login.xml al cortafuegos en 10.2.5.11 utilizando la clave k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg con wget tendría el siguiente aspecto:

```
> wget --post file login.xml "https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-
name=login.xml&client=wget&vsys=vsys1"
```

Para aplicar el archivo al cortafuegos mediante cURL:

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?
type=user-id&key=<key>&vsys=<VSYS_name>
```

Por ejemplo, la sintaxis para enviar un archivo de entrada denominado login.xml al cortafuegos en 10.2.5.11 utilizando la clave `k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg` con cURL tendría el siguiente aspecto:

```
> curl --form file@login.xml "https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1"
```

STEP 7 | Verifique que el cortafuegos esté recibiendo correctamente eventos de inicio de sesión de los servidores de terminal.

Verifique la configuración abriendo una conexión de SSH con el cortafuegos y, a continuación, ejecutando los siguientes comandos de la CLI:

Para verificar si el servidor de terminal se está conectando con el cortafuegos a través de XML:

```
admin@PA-5250> show user xml-api multiusersystem
Host            Vsys    Users   Blocks
--------------------------------------
10.5.204.43   vsys1      5         2
```

Para verificar que el cortafuegos está recibiendo asignaciones de un servidor de terminal a través de XML:

```
admin@PA-5250> show user ip-port-user-mapping all

Global max host index 1, host hash count 1

XML API Multi-user System 10.5.204.43
Vsys 1, Flag 3
Port range: 20000 - 39999
Port size: start 200; max 2000
Block count 100, port count 20000
20000-20199: acme\administrator

Total host: 1
```


© 2020 Palo Alto Networks, Inc.

Envío de asignaciones de usuarios a User-ID mediante la API XML

User-ID proporciona muchos métodos integrados para obtener información de asignación de usuarios. Sin embargo, es posible que tenga aplicaciones o dispositivos que capturan la información de usuario pero no pueden integrarse de forma nativa con User-ID. Por ejemplo, podría tener una aplicación personalizada desarrollada internamente o un dispositivo que el método de asignación de usuario no estándar admita. En estos casos, puede utilizar la API de XML de PAN-OS para crear secuencias de comando personalizadas que envíen la información al agente de User-ID integrado en PAN-OS o directamente al cortafuegos. La API XML de PAN-OS utiliza solicitudes HTTP estándar para enviar y recibir datos. Las llamadas a la API se pueden realizar directamente mediante las utilidades de línea de comandos, como cURL, o mediante cualquier marco de secuencias de comandos o aplicaciones compatible con las solicitudes POST y GET.

Para habilitar un sistema externo para que envíe información de asignación de usuarios al agente de User-ID integrado en PAN-OS, cree secuencias de comandos que extraigan los eventos de inicio de sesión y cierre de sesión de usuarios, y utilice los eventos como entrada para la solicitud de API de XML de PAN-OS. A continuación defina los mecanismos para enviar solicitudes de API XML al cortafuegos (utilizando cURL, por ejemplo) y use la clave de API del cortafuegos para una comunicación segura. Para obtener información más detallada, consulte Guía de uso de PAN-OS XML API.

© 2020 Palo Alto Networks, Inc.

Habilitación de política basada en usuarios y grupos

Tras realizar la Habilitación de User-ID, podrá configurar la política de seguridad que se aplica a usuarios y grupos específicos. Los controles de políticas en función del usuario también pueden incluir información sobre la aplicación, incluso a qué categoría o subcategoría pertenece, en qué tecnología está basada o cuáles son sus características. Puede definir las reglas de la política para habilitar aplicaciones de forma segura en función de los usuarios o grupos de usuarios, en cualquier dirección, entrante o saliente.

Ejemplos de políticas en función del usuario:

- Permitir que solamente el departamento de TI utilice herramientas como SSH, telnet y FTP en los puertos estándares.
- Permitir al grupo de servicios de asistencia y soporte utilizar Slack.
- Permitir a todos los usuarios leer Facebook, pero bloquear el uso de las aplicaciones de Facebook y limitar la publicación a los empleados del departamento de marketing.

© 2020 Palo Alto Networks, Inc.

Habilitación de política para usuarios con múltiples cuentas

Si un usuario de su organización tiene múltiples responsabilidades, ese usuario puede tener múltiples nombres de usuario (cuentas), cada uno con distintos privilegios para acceder a un conjunto de servicios específico, pero todos los nombres de usuarios comparten la misma dirección IP (el sistema cliente del usuario). Sin embargo, el agente de User-ID puede asignar cualquier dirección IP (o dirección IP e intervalo de puertos para usuarios de servidor de terminal) a un único nombre de usuario para aplicar la política, y no puede predecir qué nombre de usuario asignará el agente. Para controlar el acceso de todos los nombres de usuario de un usuario, puede aplicar ajustes a las reglas, grupos de usuarios y agente de User-ID.

Por ejemplo, supongamos que el cortafuegos tiene una regla que permite que el nombre de usuario corp_user acceda al correo electrónico y una regla que permita que el nombre de usuario admin_user acceda a un servidor MySQL. El usuario inicia sesión con cualquiera de los nombres de usuario desde la misma dirección IP de cliente. Si el agente User-ID asigna la dirección IP a corp_user, entonces, si el usuario inicia sesión como corp_user o si lo hace como admin_user, el cortafuegos identificará que el usuario es corp_user y le concederá acceso al correo electrónico, pero no al servidor MySQL. Por otro lado, si el agente User-ID asigna la dirección IP a admin_user, el cortafuegos siempre identificará al usuario como admin_user, independientemente del inicio de sesión, y le concederá acceso al servidor MySQL, pero no al correo electrónico. Los siguientes pasos describen cómo aplicar ambas reglas en este ejemplo.

STEP 1 | Configure un grupo de usuarios para cada servicio que requiera distintos privilegios de acceso.

En este ejemplo, cada grupo es para un único servicio (servidor MySQL o correo electrónico). Sin embargo, es común configurar cada grupo para un conjunto de servicios que requieran los mismos privilegios (por ejemplo, un grupo para todos los servicios de usuario básicos y otro grupo para todos los servicios administrativos).

Si su organización ya tiene grupos de usuarios que pueden acceder a los servicios que requiere el usuario, solo tiene que añadir el nombre de usuario que se use para servicios menos restringidos a esos grupos. En este ejemplo, el servidor de correo electrónico requiere un acceso menos restringido que el servidor MySQL, y corp_user es el nombre de usuario para acceder al correo electrónico. Así, usted añade corp_user a un grupo que pueda acceder al correo electrónico (corp_employees) y a un grupo que pueda acceder al servidor MySQL (network_services).

Si añadir un nombre de usuario a un grupo existente concreto puede infringir las normas de su organización, puede crear un grupo personalizado que se base en un filtro LDAP. En este ejemplo, supongamos que network_services es un grupo personalizado que configura como sigue:

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Configuración de asignación de grupo)** y seleccione **Add (Añadir)** para añadir una configuración de asignación de grupo con un nombre único en **Name (Nombre)**.
2. Seleccione un **Server Profile** LDAP y asegúrese de que la casilla de verificación **Enabled** esté habilitada.
3. Seleccione la pestaña **Custom Group (Grupo personalizado)** y seleccione **Add (Añadir)** para añadir un grupo personalizado con network_services en **Name (Nombre)**.
4. Especifique un **LDAP Filter** que coincida con un atributo LDAP de corp_user y haga clic en **OK**.
5. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.



Por último, si otros usuarios que están en el grupo de servicios menos restringidos reciben nombres de usuario adicionales que acceden a servicios más restringidos, puede añadir esos nombres de usuario al grupo para obtener más servicios

© 2020 Palo Alto Networks, Inc.

restringidos. Este escenario es más común que el inverso; un usuario con acceso a servicios más restringidos suele tener ya acceso a servicios menos restringidos.

STEP 2 | Configure las reglas que controlan el acceso del usuario en función de los grupos que acaba de configurar.

Si desea más información, consulte Habilite la instauración de la política basada en usuarios y grupos.

1. Configure una regla de seguridad que permita que el grupo corp_employees acceda al correo electrónico.
2. Configure una regla de seguridad que permita que el grupo network_services acceda al servidor MySQL.

STEP 3 | Configure la lista de ignorados del agente de User-ID.

Esto garantiza que el agente de User-ID asigne la dirección IP cliente únicamente al nombre de usuario que sea miembro de los grupos asignados a las reglas que acaba de configurar. La lista de ignorados debe contener todos los nombres de usuario de los usuarios que no son miembros de estos grupos.

En este ejemplo, añada admin_user a la lista de ignorados del agente de User-ID basado en Windows para garantizar que asigna la dirección IP del cliente a corp_user. Esto garantiza que, si el usuario inicia sesión como corp_user o admin_user, el cortafuegos identifica al usuario como corp_user y aplica ambas reglas que ha configurado porque corp_user es un miembro de los grupos a los que las reglas hacen referencia.

1. Cree un archivo `ignore_user_list.txt`.
2. Abra el archivo y añada admin_user.

   Si después añade más nombres de usuarios, cada uno debe estar en una línea separada.
3. Guarde el archivo en la carpeta de agente de User-ID en el servicio de dominio donde el agente está instalado.

Si usa el agente de User-ID integrado en PAN-OS, consulte Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS *para obtener instrucciones sobre cómo configurar la lista de ignorados.*

STEP 4 | Configure la autenticación de endpoint para los servicios restringidos.

Esto permite que el endpoint compruebe las credenciales del usuario y conserva la capacidad de permitir el acceso a los usuarios con múltiples nombres de usuario.

En este ejemplo, ha configurado una regla de cortafuegos que permite que corp_user, como miembro del grupo network_services, envíe una solicitud de servicio al servidor MySQL. Ahora debe configurar el servidor MySQL para que responda a cualquier nombre de usuario no autorizado (como corp_user) pidiendo al usuario que introduzca las credenciales de inicio de sesión de un nombre de usuario autorizado (admin_user).

Si el usuario inicia sesión en la red como admin_user, el usuario podrá acceder al servidor MySQL sin pedir las credenciales de admin_user de nuevo.

En este ejemplo, tanto corp_user como admin_user deben tener cuentas de correo electrónico, de modo que el servidor de correo electrónico no pedirá credenciales adicionales independientemente del nombre de usuario que haya introducido el usuario al iniciar sesión en la red.

El cortafuegos está ahora listo para aplicar reglas a un usuario con múltiples nombres de usuario.

© 2020 Palo Alto Networks, Inc.

Verificación de la configuración de User-ID

Después de configurar la asignación de usuarios y grupos, habilitar User-ID en su política de seguridad y configurar la política de autenticación, debe comprobar que User-ID funcione correctamente.

STEP 1 | Acceda a la CLI del cortafuegos.

STEP 2 | Verifique que la asignación de grupos funciona.

Desde la CLI, introduzca el siguiente comando operativo:

```
> show user group-mapping statistics
```

STEP 3 | Verifique que la asignación de usuarios funciona.

Si está utilizando el agente de User-ID integrado en PAN-OS, podrá verificarlo desde la CLI utilizando el siguiente comando:

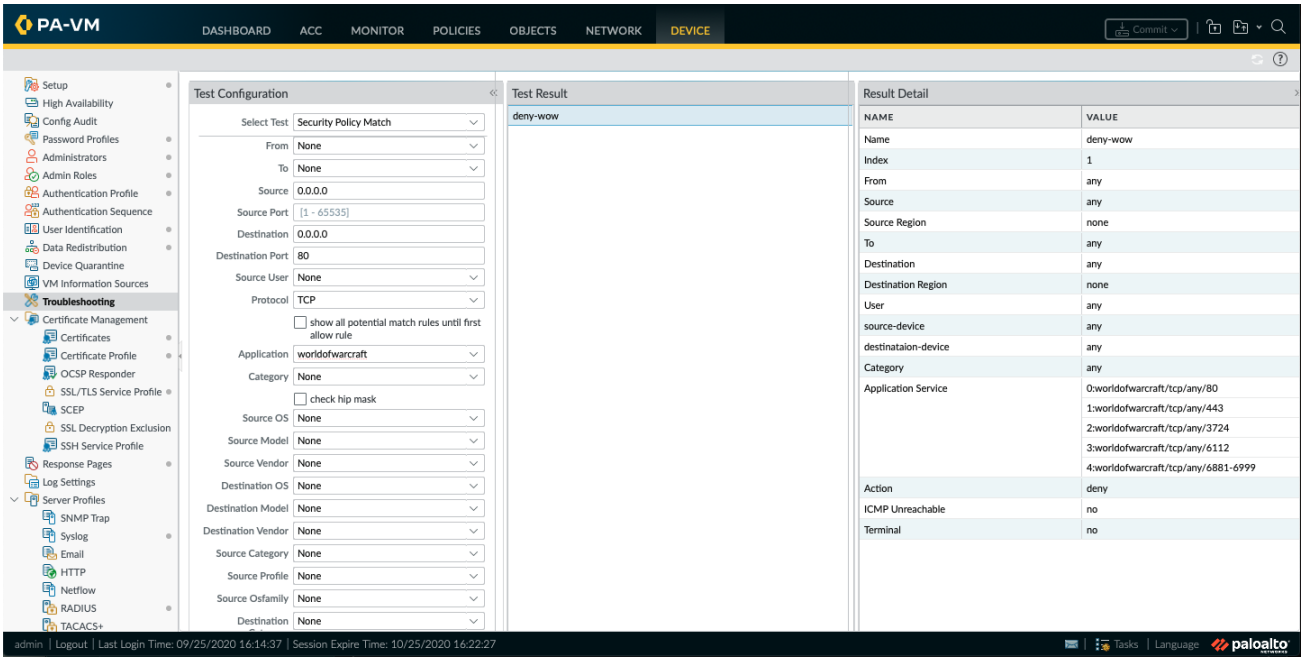
```
> show user ip-user-mapping-mp all
IP              Vsys  From  User          Timeout (sec)
------------------------------------------------------
192.168.201.1   vsys1 UIA   acme\george            210
192.168.201.11  vsys1 UIA   acme\duane             210
192.168.201.50  vsys1 UIA   acme\betsy             210
192.168.201.10  vsys1 UIA   acme\administrator     210
192.168.201.100 vsys1 AD    acme\administrator     748
Total: 5 users
*: WMI probe succeeded
```

STEP 4 | Compruebe la regla de su política de seguridad.

- Desde una máquina en la zona donde esté habilitado User-ID, intente acceder a sitios y aplicaciones para comprobar las reglas que ha definido en su política y asegúrese de que el tráfico se permite y deniega del modo esperado.
- Asimismo, puede comprobar la configuración que se está ejecutando para averiguar si la política está bien configurada. Por ejemplo, supongamos que tiene una regla que bloquea a los usuarios y les impide jugar a World of Warcraft. Podría comprobar la política del modo siguiente:

1. Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y, luego, seleccione **Security Policy Match (Coincidencia con política de seguridad)** en el menú desplegable Select Test (Seleccionar prueba).
2. Introduzca `0.0.0.0` como direcciones IP de origen y de destino. Así se ejecuta la prueba de coincidencia con la política en todas las direcciones IP de origen y de destino.
3. Introduzca el puerto de destino.
4. Introduzca el protocolo.
5. Haga clic en **Execute (Ejecutar)** para comprobar la coincidencia con la política de seguridad.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Compruebe su configuración de política de autenticación y portal de autenticación.

1. Desde la misma zona, vaya a una máquina que no sea miembro de su directorio, como un sistema Mac OS, e intente hacer ping a un sistema externo a la zona. El ping debería funcionar sin requerir autenticación.
2. Desde la misma máquina, abra un explorador y desplácese hasta un sitio web en una zona de destino que coincida con una regla de autenticación que haya definido. El formulario web del portal de autenticación debería aparecer y solicitarle las credenciales de inicio de sesión.
3. Inicie sesión utilizando las credenciales correctas y confirme que se le ha redirigido a la página solicitada.
4. También puede comprobar su política de autenticación utilizando el comando operativo **`test authentication-policy-match`** de la manera siguiente:

```
> test authentication-policy-match from corporate to internet source
 192.168.201.10 destination 8.8.8.8
Matched rule: 'authentication portal' action: web-form
```

STEP 6 | Verifique que los archivos de log muestren nombres de usuario.

Seleccione una página de logs (como **Monitor [Supervisar]** > **Logs** > **Traffic [Tráfico]**) y compruebe que la columna Source User (Usuario de origen) muestre nombres de usuario.

STEP 7 | Verifique que los informes muestren nombres de usuario.

1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
2. Seleccione un tipo de informe que incluya nombres de usuario. Por ejemplo, el informe Denied Applications, la columna Source User, deberían mostrar una lista de los usuarios que intentaron acceder a las aplicaciones.

© 2020 Palo Alto Networks, Inc.

Implementación de User-ID en una red a gran escala

Una red a gran escala puede tener cientos de fuentes de información que los cortafuegos consultan para asignar direcciones IP a nombres de usuario y asignar nombres de usuario a grupos de usuario. Puede simplificar la administración de User-ID para dicha red al agregar la información de asignación de usuario y grupo antes de que los agentes de User-ID la recopilen, con lo cual se reduce la cantidad de agentes necesarios.

Una red a gran escala también puede tener numerosos cortafuegos que usan la información de asignación para aplicar las políticas. Puede reducir los recursos que usan los cortafuegos y las fuentes de información en el proceso de consulta al configurar algunos cortafuegos para que adquieran la información de asignación a través de la redistribución en lugar de la consulta directa. La redistribución también permite que los cortafuegos apliquen políticas basadas en el usuario cuando los usuarios dependen de las fuentes locales para la autenticación (por ejemplo, servicios de directorio regional), pero necesitan acceso a servicios y aplicaciones remotos (por ejemplo, aplicaciones de centro de datos globales).

Si realiza el procedimiento Configuración de la información de autenticación, los cortafuegos deben redistribuir las Marcas de tiempo de la autenticación asociadas a las respuestas del usuario a las comprobaciones de autenticación. Los cortafuegos utilizan las marcas de tiempo para evaluar los tiempo de espera para las reglas de la política de autenticación. El tiempo de espera permite al usuario que se autentica correctamente solicitar servicios y aplicaciones posteriormente sin volver a autenticarse dentro del período de tiempo de espera. La redistribución de las marcas de tiempo le permitirá aplicar el tiempo de espera incluso si el cortafuegos que inicialmente concedió el acceso para un usuario no es el mismo cortafuegos que más tarde controla el acceso para ese usuario.

Si configura varios sistemas virtuales, puede compartir la información de asignación de direcciones IP a nombres de usuarios entre todos ellos seleccionando uno como núcleo de User-ID.

- Implementación de User-ID para numerosas fuentes de información de asignación
- Redistribución de las marcas de tiempo de autenticación y datos
- Asignaciones de User-ID compartidas entre sistemas virtuales

Implementación de User-ID para numerosas fuentes de información de asignación

Puede usar el reenvío de logs de Windows y los servidores de catálogo globales para simplificar la asignación de usuarios y grupos en una red a gran escala de controladores de dominio de Microsoft Active Directory (AD) o servidores de Exchange. Estos métodos simplifican la administración de User-ID al agregar la información de asignación antes de que los agentes de User-ID la recopilen, con lo cual se reduce la cantidad de agentes necesarios.

- Servidores de catálogo global y reenvío de logs de Windows
- Planificación de una implementación de User-ID a gran escala
- Configuración de reenvío de logs de Windows
- Configuración de User-ID para numerosas fuentes de información de asignación

Servidores de catálogo global y reenvío de logs de Windows

Como cada agente de User-ID puede supervisar hasta 100 servidores, el cortafuegos necesitará múltiples agentes de User-ID para supervisar una red con cientos de controladores de dominio de AD o servidores de Exchange. La creación y gestión de numerosos agentes de User-ID implica una considerable carga administrativa, especialmente al expandir las redes donde la monitorización de controladores de nuevos

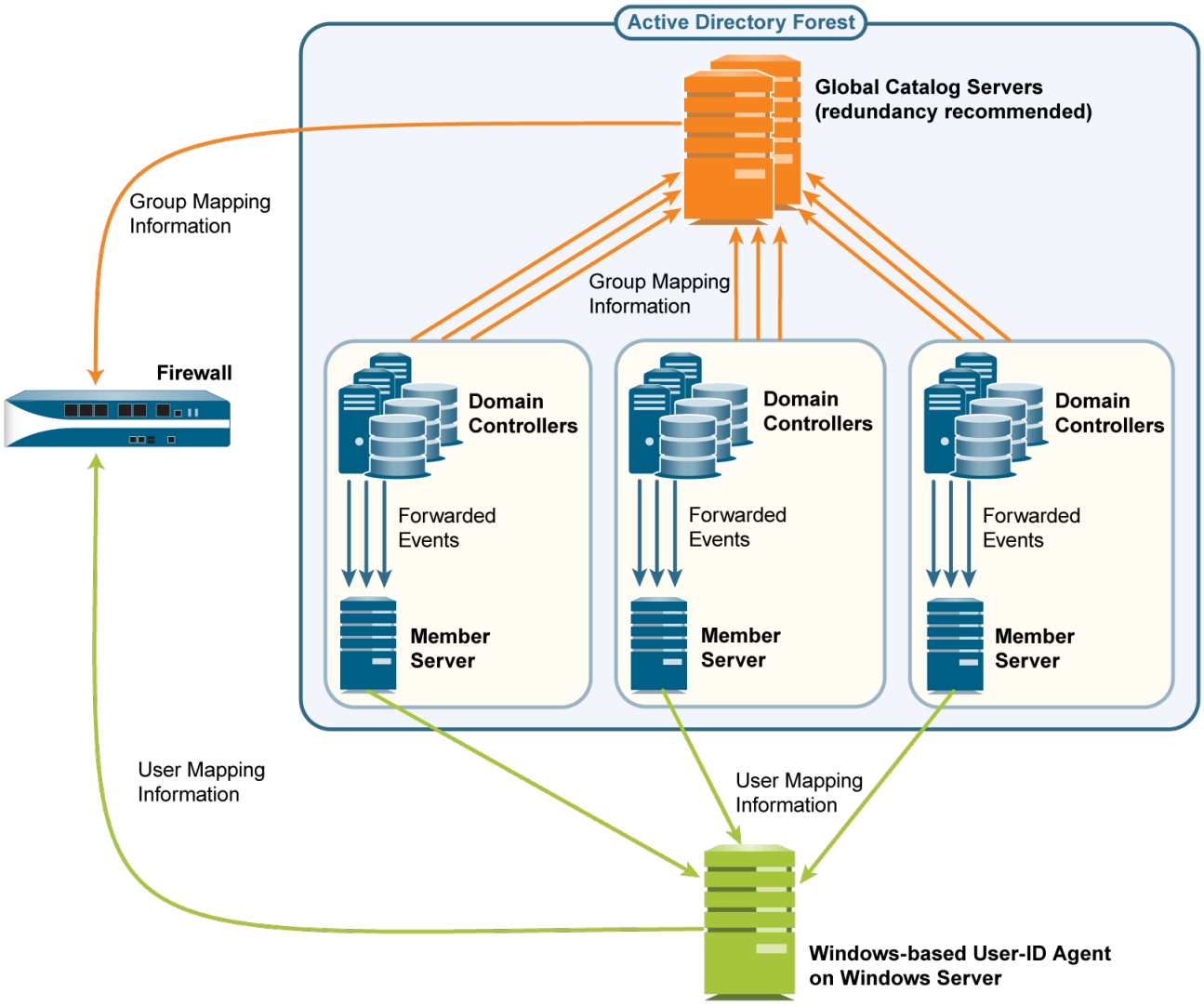
© 2020 Palo Alto Networks, Inc.

dominios resulta muy difícil. El reenvío de logs de Windows le permite minimizar la carga administrativa reduciendo el número de servidores que hay que supervisar y reduciendo por tanto el número de agentes de User-ID que hay que gestionar. Cuando configure el reenvío de logs de Windows, múltiples controladores de dominio exportan sus eventos de inicio de sesión a un único miembro de dominio desde el que el agente de User-ID recopila la información de asignación de usuario.

Puede configurar el reenvío de logs de Windows para las versiones 2012 y 2012 R2 de Windows Server. El reenvío de logs de Windows no está disponible para los servidores que no son de Microsoft.

Para recopilar la información de asignación de grupo en una red a gran escala, puede configurar el cortafuegos para que consulte a un servidor del catálogo global que recibe la información de cuenta desde los controladores de dominio.

La siguiente figura ilustra la asignación de usuarios y la asignación de grupos para una red a gran escala en la que el cortafuegos usa un agente de User-ID basado en Windows. Consulte Planificación de una implementación de User-ID a gran escala para determinar si esta implementación se adapta a su red.



© 2020 Palo Alto Networks, Inc.

Planificación de una implementación de User-ID a gran escala

Cuando decide si usar los servidores de catálogo global y de reenvío de logs de Windows para su implementación de User-ID, consulte a su administrador de sistema para determinar:

- El ancho de banda necesario para que los controladores reenvíen eventos de inicio de sesión a los servidores miembros. El ancho de banda es un múltiplo de la tasa de inicio de sesión (número de inicios de sesión por minuto) de los controladores de dominio y el tamaño de byte para cada evento de inicio de sesión.

  Los controladores de dominio no reenvían sus logs de seguridad completos; solo reenvían los eventos que el proceso de asignación de usuarios necesitan por inicio de sesión: cuatro eventos para Windows Server 2012 y MS Exchange.
- Si los siguientes elementos de red admiten el ancho de banda requerido:
  - **Domain controllers (Controladores de dominio)**: deben admitir la carga de procesamiento asociada con el reenvío de los eventos.
  - **Member Servers (Servidores miembros)**: deben admitir la carga de procesamiento asociada con la recepción de los eventos.
  - **Connections (Conexiones)**: la distribución geográfica (local o remota) de los controladores de dominio, servidores miembros y servidores del catálogo global es un factor. Por lo general, una distribución remota admite menor ancho de banda.

Configuración de reenvío de logs de Windows

Para configurar el reenvío de logs de Windows necesitará privilegios administrativos para configurar políticas de grupos en servidores de Windows. Configure el reenvío de logs de Windows en todos los *recopiladores de eventos de Windows* (los servidores miembro que recopilan eventos de inicio de sesión de los controladores de dominios). A continuación se incluye un resumen general de las tareas; consulte su documentación de Windows Server para conocer los pasos específicos.

STEP 1 | En cada recopilador de eventos de Windows, habilite la recopilación de eventos, añada los controladores de dominio con orígenes de eventos y configure la consulta de recopilación de eventos (suscripción). Los eventos que especifique en la suscripción varían según la plataforma de controlador del dominio:

- **Windows Server 2012 (incluso R2) y 2016, o MS Exchange**: los ID de evento para los eventos requeridos son 4768 (vale de autenticación concedido), 4769 (vale de servicio concedido), 4770 (vale concedido renovado) y 4624 (inicio de sesión correcto).



Para reenviar eventos lo más rápidamente posible, seleccione la opción Minimize Latency (Minimizar latencia) cuando configure la suscripción.

Los agentes de User-ID supervisan el log de seguridad, no la ubicación de los eventos reenviados predeterminados en los recopiladores de eventos de Windows. Por lo tanto, realice los siguientes pasos en cada recopilador de eventos de Windows para cambiar la ruta de creación de logs de eventos al log de seguridad.

1. Abra Event Viewer (Visor de eventos).
2. Haga clic con el botón derecho en el log **Security (Seguridad)** y seleccione **Properties (Propiedades)**.
3. Copie la **Log path (Ruta de log)** (la predeterminada es `%SystemRoot%\System32\Winevt\Logs\security.evtx`) y haga clic en **OK (Aceptar)**.
4. Haga clic con el botón derecho en la carpeta **Forwarded Events (Eventos reenviados)** y seleccione **Properties (Propiedades)**.

© 2020 Palo Alto Networks, Inc.

5. Sustituya la **Log path (Ruta de log)** (`%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx`) pegando el valor del log de **Security (Seguridad)** y, luego, haga clic en **OK (Aceptar)**.

STEP 2 | Configure una política de grupo para permitir la gestión remota de Windows (WinRM, Windows Remote Management) en los controladores de dominio.

STEP 3 | Configure una política de grupo para permitir el reenvío de eventos de Windows en los controladores de dominio.

Configuración de User-ID para numerosas fuentes de información de asignación

STEP 1 | Configure el reenvío de logs de Windows en los servidores miembros que recopilarán eventos de inicio de sesión.

Configuración de reenvío de logs de Windows. Este paso requiere privilegios administrativos para configurar políticas de grupos en servidores de Windows.

STEP 2 | Instale el agente de User-ID basado en Windows.

Instale el agente de User-ID basado en Windows en un servidor Windows que pueda acceder a los servidores miembros. Asegúrese de que el sistema que alojará el agente de User-ID es un miembro del mismo dominio que los servidores que supervisará.

STEP 3 | Configure el agente de User-ID de Windows para recopilar asignaciones de usuarios desde los servidores miembros.

1. Inicie el agente de User-ID basado en Windows.
2. Seleccione **User Identification (Identificación de usuarios)** > **Discovery (Detección)** y realice los siguientes pasos para cada servidor miembro que recibirá eventos de los controladores de dominio:
    1. En la sección Servers, haga clic en **Add** e introduzca un nombre en **Name** para identificar el servidor miembro.
    2. En el campo **Server Address**, introduzca el FQDN o dirección IP del servidor miembro.
    3. En **Server Type**, seleccione **Microsoft Active Directory**.
    4. Haga clic en **OK** para guardar la entrada del servidor.
3. Realice el resto de la configuración del agente de User-ID: consulte la Configuración del agente de User-ID basado en Windows para la asignación de usuarios.
4. Si los orígenes de User-ID proporcionan nombres de usuario en varios formatos, especifique el formato de **Primary Username (Nombre de usuario principal)** cuando realice el procedimiento Asignación de usuarios a grupos.

    El nombre de usuario principal identifica al usuario en el cortafuegos y lo representa en los informes y los logs con independencia del formato que proporcione el origen de User-ID.

STEP 4 | Configure un perfil de servidor LDAP para especificar cómo conecta el cortafuegos con los servidores de catálogo global (hasta cuatro) para obtener información de asignación del grupo.



Para mejorar la disponibilidad, use al menos dos servidores de catálogo global para asegurar la redundancia.

Puede recopilar información de asignación de grupos únicamente para grupos universales, no para grupos de dominio local (subdominios).

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **LDAP**, haga clic en **Add (Añadir)** e introduzca un nombre para el perfil en **Name (Nombre)**.
2. En la sección Servers, para cada catálogo global, haga clic en **Add** e introduzca en **Name** el nombre del servidor, la dirección IP (**LDAP Server**) y el **Port**. En el caso de una conexión con texto sin formato o seguridad de capa de transporte de inicio (Start TLS), use el **Port (Puerto)** 3268. Para una conexión de LDAP por SSL, use el **Port (Puerto)** 3269. Si la conexión va a usar TLS de inicio o LDAP en SSL, seleccione la casilla de verificación **Require SSL/TLS secured connection (Exigir conexión SSL/TLS segura)**.
3. En el campo **Base DN**, introduzca el nombre distintivo (DN) del punto en el servidor de catálogo global en el que el cortafuegos comenzará a buscar información de asignación de grupo (por ejemplo, `DC=acbdomain,DC=com`).
4. En **Type (Tipo)**, seleccione **active-directory**.

STEP 5 | Configure un perfil de servidor LDAP para especificar cómo conecta el cortafuegos con los servidores (hasta cuatro) para obtener información de asignación de dominio.

User-ID utiliza esta información para asignar nombres de dominios DNS a los nombres de dominios de NetBIOS. Esta asignación garantiza que las referencias a nombres de usuario/dominio sean coherentes en las reglas de políticas.

Para mejorar la disponibilidad, use al menos dos servidores para asegurar la redundancia.

Debe seguir los mismos pasos que con el perfil de servidor LDAP creado para los catálogos globales en el paso anterior, excepto en los siguientes campos:

- **LDAP Server**: introduzca la dirección IP del controlador de dominio que contiene la información de asignación de dominios.
- **Port**: para una conexión de texto sin formato o TLS de inicio, use el **Port** 389. Para una conexión de LDAP por SSL, use el **Port (Puerto)** 636. Si la conexión va a usar TLS de inicio o LDAP en SSL, seleccione la casilla de verificación **Require SSL/TLS secured connection (Exigir conexión SSL/TLS segura)**.
- **Base DN**: seleccione el DN del punto en el controlador de dominio donde el cortafuegos comenzará su búsqueda de información de asignación de dominio. El valor debe comenzar con la cadena: `cn=partitions,cn=configuration` (por ejemplo, `cn=partitions,cn=configuration,DC=acbdomain,DC=com`).

STEP 6 | Cree una configuración de asignación de grupos para cada perfil de servidor de LDAP que haya creado.

1. Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Ajustes de asignación de grupo)**.
2. Haga clic en **Add** e introduzca un nombre en **Name** para identificar la configuración de asignación de grupos.
3. Seleccione el **Server Profile** de LDAP y asegúrese de que la casilla de verificación **Enabled** esté seleccionada.

   Si el catálogo global y los servidores de asignación de dominios hacen referencia a más grupos de lo que exigen sus reglas de seguridad, configure la Group Include List o la lista Custom Group para limitar los grupos para los cuales User-ID realiza la asignación.
4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Inserción de nombre de usuario en encabezados HTTP

Cuando configure un dispositivo de cumplimiento secundario con el cortafuegos de Palo Alto Networks para aplicar la política basada en el usuario, es posible que el dispositivo secundario no tenga la asignación de dirección IP a nombre de usuario del cortafuegos. La transmisión de la información del usuario a dispositivos posteriores puede requerir la implementación de dispositivos adicionales, como proxies, o puede afectar negativamente a la experiencia del usuario (por ejemplo, que los usuarios tengan que iniciar sesión varias veces). Cuando se comparta la identidad del usuario en los encabezados HTTP, puede aplicar la política basada en el usuario sin que afecte negativamente a la experiencia del usuario o tener que implementar una infraestructura adicional.

Cuando configure esta función, aplique el perfil de URL a su política de seguridad y confirme los cambios, el cortafuegos realizará las siguientes acciones:

1. Completará los valores de usuario y dominio con el formato del nombre de usuario principal en la asignación de grupos para el usuario de origen.
2. Codificará esta información mediante Base64.
3. Añadirá el encabezado con codificación Base64 a la carga útil.
4. Enrutará el tráfico al dispositivo posterior.

Si desea incluir el nombre de usuario y el dominio solo cuando el usuario acceda a dominios específicos, configure una lista de dominios y el cortafuegos insertará el encabezado solo cuando un dominio de la lista coincida con el encabezado de host de la solicitud HTTP.

Para compartir información de usuario con dispositivos posteriores, primero debe habilitar User-ID y configurar la asignación de grupos.

Para incluir el nombre de usuario y el dominio en el encabezado, el cortafuegos requiere la asignación de dirección IP a nombre de usuario para el usuario. Si el usuario no está asignado, el cortafuegos inserta `unknown (desconocido)` en la codificación Base64 tanto para el dominio como para el nombre de usuario en el encabezado.

Para incluir el nombre de usuario y el dominio en los encabezados para el tráfico HTTPS, primero debe crear un perfil de descifrado para descifrar el tráfico HTTPS.

Esta función admite el tráfico de descifrado de proxy de reenvío.

STEP 1 | Cree o edite un **perfil de filtrado de URL**.

*El cortafuegos no inserta encabezados si la acción para el perfil de filtrado de URL es **`block (bloquear)`** para el dominio.*

STEP 2 | Cree o edite una entrada de inserción del encabezado HTTP mediante tipos predefinidos.

Puede definir hasta cinco encabezados para cada perfil.

STEP 3 | Seleccione **Dynamic Fields (Campos dinámicos)** como **tipo** de encabezado.

STEP 4 | **Añada** los **dominios** donde quiera insertar encabezados. Cuando el usuario acceda a un dominio de la lista, el cortafuegos insertará el encabezado especificado.

STEP 5 | **Añada** un nuevo **encabezado** o seleccione **X-Authenticated-User (Usuario con autenticación X)** para editarlo.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Seleccione un formato de **valor** del encabezado (`($domain)\($user)` o `WinNT://($domain)/($user)`) o especifique su propio formato con los tokens dinámicos `($domain)` y `($user)` (por ejemplo, `($user)@($domain)` para UserPrincipalName).



No use el mismo token dinámico (`($user)` o `($domain)`) más de una vez por valor.

Cada valor puede tener hasta 512 caracteres. El cortafuegos completa los tokens dinámicos `($user)` y `($domain)` con el nombre de usuario principal en el perfil de asignación de grupos. Por ejemplo:

- Si el nombre de usuario principal es sAMAccountName, el valor de `($user)` es sAMAccountName y el valor de `($domain)` es el nombre de dominio de NetBios.
- Si el nombre de usuario principal es UserPrincipalName, el valor de `($user)` es el nombre de cuenta de usuario (prefijo) y el valor de `($domain)` es el nombre del Sistema de nombres de dominio (Domain Name System, DNS).

STEP 7 | (Opcional) Seleccione **Log** para habilitar la creación de logs para la inserción del encabezado.

STEP 8 | Aplique el perfil de filtrado de URL a la regla de la política de seguridad para el tráfico HTTP o HTTPS.

STEP 9 | Seleccione **OK (Aceptar)** dos veces para confirmar la configuración del encabezado HTTP.

STEP 10 | **Commit (Confirmar)** los cambios.

STEP 11 | Compruebe que el cortafuegos incluya el nombre de usuario y el dominio en los encabezados HTTP.

- Utilice el comando **`show user user-ids all`** para comprobar que la asignación de grupos sea correcta.
- Use el comando **`show counter global name ctd_header_insert`** para ver la cantidad de encabezados HTTP insertados por el cortafuegos.
- Si configuró la creación de logs en el paso 7, compruebe los logs para la carga útil con codificación Base64 insertada (por ejemplo, **`corpexample\testuser`** debería aparecer en los logs como **`Y29ycGV4YW1wbGVcdGVzdHVzZXI=`**).

Redistribución de las marcas de tiempo de autenticación y datos

En una red a gran escala, en lugar de configurar todos sus cortafuegos para consultar directamente la asignación de fuentes de información, puede dinamizar el uso de recursos configurando algunos cortafuegos para recoger la asignación de información a través de la redistribución.

Si realiza la Configuración de la política de autenticación, sus cortafuegos también deben redistribuir las marcas de tiempo de autenticación que se generan cuando los usuarios se autentican para acceder a las aplicaciones y los servicios. Los cortafuegos utilizan las marcas de tiempo para evaluar los tiempo de espera para las reglas de la política de autenticación. El tiempo de espera permite al usuario que se autentica correctamente solicitar servicios y aplicaciones posteriormente sin volver a autenticarse dentro del período de tiempo de espera. La redistribución de las marcas de tiempo le permite aplicar tiempos de espera uniformes en todos los cortafuegos de su red.

Los cortafuegos comparten datos y marcas de tiempo de autenticación como parte del mismo flujo de redistribución; no debe configurar la redistribución para cada tipo de información por separado.

- Implementación del cortafuegos para la redistribución de datos
- Configuración de la redistribución de datos

© 2020 Palo Alto Networks, Inc.

Implementación del cortafuegos para la redistribución de datos

En una red a gran escala, en lugar de configurar todos sus cortafuegos para consultar directamente los orígenes de datos, puede dinamizar el uso de recursos configurando algunos cortafuegos para recopilar los orígenes de datos a través de la redistribución. La redistribución de datos también proporciona granularidad, lo que le permite redistribuir solo los tipos de información que especifique solo a los dispositivos que seleccione. También puede filtrar las asignaciones de usuarios de IP o las asignaciones de etiquetas de IP mediante subredes e intervalos para garantizar que los cortafuegos recopilen solo las asignaciones que necesitan para hacer cumplir la política.

La redistribución de datos puede ser unidireccional (el agente proporciona datos al cliente) o bidireccional, donde tanto el agente como el cliente pueden enviar y recibir datos simultáneamente.

Para redistribuir los datos, puede utilizar los siguientes tipos de arquitectura:

- **Hub and spoke architecture for a single region (Arquitectura de hubs y radios para una sola región):**

  Para redistribuir datos entre cortafuegos, utilice una arquitectura de hub y radio como práctica recomendada. En esta configuración, un servidor de seguridad central recopila los datos de orígenes como agentes de User-ID de Windows, servidores Syslog, controladores de dominio u otros servidores de seguridad. Configure los cortafuegos del cliente de redistribución para recopilar los datos del cortafuegos del hub.

  Por ejemplo, un hub (que consta de un par de VM-50 para la resistencia) podría conectarse a los orígenes de User-ID para las asignaciones de usuarios. Entonces, el hub podría redistribuir las asignaciones de usuarios cuando los cortafuegos del cliente que utilicen las asignaciones de usuarios para hacer cumplir la política se conecten al hub para recibir datos.
- **Multi-Hub and spoke architecture for multiple regions (Arquitectura de radios y hubs múltiples para varias regiones):**

  Si tiene cortafuegos implementados en varias regiones y desea distribuir los datos a los cortafuegos en todas estas regiones para hacer cumplir la política de forma coherente, independientemente de dónde inicie sesión el usuario, puede utilizar una arquitectura radial y de varios hubs para varias regiones.

  Configure primero un cortafuegos en cada región para recopilar datos de los orígenes. Este cortafuegos actúa como un hub local para la redistribución. Este cortafuegos recopila los datos de todos los orígenes en esa región para poder redistribuirlos a los cortafuegos del cliente. A continuación, configure los cortafuegos del cliente para que se conecten a los hubs de redistribución de su región y todas las demás regiones, de modo que los cortafuegos del cliente tengan todos los datos de todos los hubs.

  Como práctica recomendada, habilite la redistribución bidireccional dentro de una región si los cortafuegos necesitan enviar y recibir datos. Por ejemplo, si un cortafuegos actúa como puerta de enlace de GlobalProtect para usuarios remotos y como cortafuegos de sucursal para usuarios locales, este debe enviar las asignaciones de usuarios que recopila para los usuarios remotos al cortafuegos del hub, así como recibir las asignaciones de usuarios de los usuarios locales del cortafuegos del hub.
- **Hierarchical architecture (Arquitectura jerárquica):**

  Para redistribuir datos, también puede utilizar una arquitectura jerárquica. Por ejemplo, para redistribuir datos como la información de identificación de usuario, organice la secuencia de redistribución en capas, donde cada capa tiene uno o más cortafuegos. En la capa inferior, los agentes de User-ID integrados a PAN-OS que se ejecutan en cortafuegos y agentes de User-ID basados en Windows que se ejecutan en servidores de Windows realizan la asignación de direcciones IP a nombres de usuario. Cada capa superior tiene cortafuegos que reciben la información de asignación y marcas de tiempo de autenticación de hasta 100 puntos de redistribución en la capa inmediatamente inferior. Los cortafuegos de capas superiores agregan la información de asignación y las marcas de tiempo de todas las capas. Esta implementación ofrece la opción de configurar políticas para todos los usuarios en los cortafuegos de capa superior y políticas específicas de la región o de la función para un subconjunto de usuarios en los dominios correspondientes en los cortafuegos de capa inferior.

© 2020 Palo Alto Networks, Inc.

En este escenario, hay tres capas de cortafuegos que redistribuyen la información de asignación y las marcas de tiempo desde fuentes de información locales a oficinas regionales y luego a un centro de datos global. El cortafuegos del centro de datos que agrega toda la información la comparte con otros cortafuegos del centro de datos, de modo que todos puedan aplicar la política y generar informes para todos los usuarios en toda su red. Solo los cortafuegos de la capa inferior utilizan agentes de User-ID para consultar a los servidores del directorio.

Las fuentes de información desde las cuales consultan los agentes User-ID no cuentan para el máximo de diez *saltos* en la secuencia. Sin embargo, los agentes User-ID basados en Windows que reenvían información de asignación a los cortafuegos sí cuentan. También en este ejemplo, la capa superior posee dos saltos: el primero para agregar la información en un cortafuegos del centro de datos y el segundo para compartir la información con otros cortafuegos del centro de datos.

Configuración de la redistribución de datos

Antes de configurar la redistribución de datos, realice el siguiente procedimiento:

- ❑ Planifique la arquitectura de redistribución. Algunos factores que deben considerarse son los siguientes:
  - ¿Qué cortafuegos aplicarán políticas para todos los tipos de datos y qué cortafuegos aplicarán políticas específicas de la región o de la función para un subconjunto de datos?
  - ¿Cuántos saltos requiere la secuencia de redistribución para agregar todos los datos? El número máximo permitido de saltos para las asignaciones de usuario es 10 y el número máximo permitido de saltos para las asignaciones de dirección IP a nombre de usuario y de dirección IP a etiqueta es 1.
  - ¿Cómo puede minimizar la cantidad de cortafuegos que consultan las fuentes de información de asignación de usuarios? Mientras menor sea la cantidad de cortafuegos que consultan, menor será la carga de procesamiento en los cortafuegos y las fuentes.
- ❑ Configure los orígenes de datos a partir de los que los agentes de redistribución obtienen los datos para redistribuir a sus clientes:
  - Asignaciones de usuarios a partir de agentes de User-ID integrados en PAN-OS o agentes de User-ID basados en Windows.
  - Asignaciones de dirección IP a etiqueta para grupos de direcciones dinámicas
  - Asignaciones de nombre de usuario a etiqueta para grupos de usuarios dinámicos
  - GlobalProtect para la aplicación de políticas basadas en HIP
  - Datos para la cuarentena de dispositivos (Solo en Panorama)
- ❑ Configuración de la política de autenticación

La redistribución de datos consiste en lo siguiente:

- El agente de redistribución que proporciona información.
- El cliente de redistribución que recibe la información.

Realice los siguientes pasos en el cortafuegos en la secuencia de redistribución de datos.

STEP 1 | En un cortafuegos de cliente de redistribución, configure un cortafuegos, Panorama o un agente de User-ID de Windows como agente de redistribución de datos.

1. Seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**.
2. **Añada** un agente de redistribución y especifique un **nombre**.
3. Confirme que el agente esté **habilitado**.

STEP 2 | Añada el agente mediante su **número de serie** o su **host y puerto**.

- Para añadir un agente mediante un número de serie, seleccione el **número de serie** del cortafuegos que desee usar como agente de redistribución.

© 2020 Palo Alto Networks, Inc.

- Para añadir un agente mediante la información de puerto y host:
  1. Especifique la información del **host**.
  2. Seleccione si el host es un **proxy LDAP**.
  3. Indique el **puerto** (el valor predeterminado es 5007; el intervalo es de 1 a 65 535).
  4. (Solo en sistemas virtuales múltiples) Especifique el **nombre del recopilador** para identificar qué sistema virtual desea utilizar como agente de redistribución.
  5. (Solo en sistemas virtuales múltiples) Especifique y confirme la **clave precompartida del recopilador** para el sistema virtual que desee utilizar como agente de redistribución.

STEP 3 | Seleccione uno o más **tipo de datos** para que el agente los redistribuya.

- **IP User Mappings (Asignaciones de usuario IP)**: asignaciones de dirección IP a nombre de usuario para User-ID.
- **IP Tags (Etiquetas IP)**: asignaciones de dirección IP a etiqueta para grupos de direcciones dinámicas.
- **User Tags (Etiquetas de usuario)**: asignaciones de nombre de usuario a etiqueta para grupos de usuarios dinámicos.
- **HIP**: datos del perfil de información del host (HIP, Host Information Profile) de GlobalProtect, que incluye objetos y perfiles de HIP.
- **Quarantine List (Lista de cuarentena)**: dispositivos que GlobalProtect identifica como en cuarentena.

STEP 4 | (Solo en sistemas virtuales múltiples): configure un sistema virtual como un recopilador que puede redistribuir datos.

Omita este paso si el cortafuegos recibe, pero no redistribuye datos.

Puede redistribuir la información entre sistemas virtuales en diferentes cortafuegos o en el mismo cortafuego. En ambos casos, cada sistema virtual cuenta como un salto en la secuencia de redistribución.

1. Seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Collector Settings (Configuración del recopilador)**.
2. Edite la **configuración del agente de redistribución de datos**.
3. Introduzca el **Collector Name (Nombre del recopilador)** y la **Pre-Shared Key (Clave precompartida)** para identificar este cortafuegos o sistema virtual como agente de User-ID.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | (Opcional pero recomendado) Configure las redes que desee incluir en la redistribución de datos y las redes que desee excluir de la redistribución de datos.

Puede incluir o excluir redes y subredes al redistribuir asignaciones de dirección IP a etiqueta o asignaciones de dirección IP a nombre de usuario.

Como práctica recomendada, siempre especifique qué redes incluir y excluir para asegurarse de que el agente solo se comunique con recursos internos.

1. Seleccione **Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Include/Exclude Networks (Redes de inclusión/exclusión)**.
2. **Añada** una entrada y especifique un **nombre**.
3. Confirme que la entrada esté **habilitada**.
4. Seleccione si desea **incluir** o **excluir** la entrada.
5. Especifique la **dirección de red** para la entrada.
6. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Configure la ruta de servicio que utiliza el cortafuegos para consultar a otros cortafuegos la información de User-ID.

Omita este paso si el cortafuegos solo recibe información de asignación de usuarios de agentes de User-ID basados en Windows o directamente de las fuentes de información (como los servidores de directorio) en lugar de otros cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**.
2. (**Cortafuegos con sistemas virtuales múltiples únicamente**) Seleccione **Global** (para una ruta de servicio de todo el cortafuegos) o **Virtual Systems (Sistemas virtuales)** (para una ruta de servicio específica del sistema virtual), y realice la Configuración de la ruta de servicio.
3. Haga clic en **Service Route Configuration (Configuración de ruta de servicios)**, seleccione **Customize (Personalizar)** y seleccione **IPv4** o **IPv6** según los protocolos de su red. Configure la ruta de servicio para ambos protocolos si su red usa ambos.
4. Seleccione **UID Agent (Agente UID)** y luego seleccione la **Source Interface (Interfaz de origen)** y la **Source Address (Dirección de origen)**.
5. Haga clic en **OK (Aceptar)** dos veces para guardar la ruta de servicio.

STEP 7 | Permita que el cortafuegos responda cuando otros cortafuegos consulten los datos que redistribuir.

Omita este paso si el cortafuegos recibe, pero no redistribuye datos.

Configure un perfil de gestión de interfaz con el servicio de **User-ID** habilitado y asigne el perfil a una interfaz de cortafuegos.

STEP 8 | (Opcional, pero recomendado) Utilice un certificado personalizado de su PKI empresarial para establecer una cadena de confianza única desde el cliente de redistribución hasta el agente de redistribución.

1. En el cortafuegos del cliente de redistribución, cree un perfil del certificado SSL personalizado para utilizarlo en las conexiones salientes.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Secure Communication Settings (Configuración de comunicación segura)**.
3. **Edite** la configuración.
4. Seleccione la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
5. Seleccione el **perfil de certificado** que creó en el subpaso 1.
6. Haga clic en **OK (Aceptar)**.
7. **Personalice la comunicación** para la **redistribución de datos**.
8. **Commit (Confirmar)** los cambios.
9. Especifique el siguiente comando de la CLI para confirmar que el perfil del certificado (`SSL config`) utiliza los `certificados personalizados`: **`show redistribution agent state <nombre-agente>`** (donde *<nombre-agente>* es el nombre del agente de redistribución o agente de User-ID).

STEP 9 | (Opcional, pero recomendado) Utilice un certificado personalizado de su PKI empresarial para establecer una cadena de confianza única desde el agente de redistribución hasta el agente de cliente.

1. En el cortafuegos del agente de redistribución, cree un perfil de servicio SSL/TLS personalizado para que el cortafuegos lo utilice para las conexiones entrantes.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Secure Communication Settings (Configuración de comunicación segura)**.
3. **Edite** la configuración.

© 2020 Palo Alto Networks, Inc.

4. Seleccione la opción **Customize Secure Server Communication (Personalizar comunicación de servidor segura)**.
5. Seleccione el **perfil de servicio SSL/TLS** que creó en el paso 1.
6. Haga clic en **OK (Aceptar)**.
7. **Commit (Confirmar)** los cambios.
8. Especifique el siguiente comando de la CLI para confirmar que el perfil del certificado (`SSL config [Config. de SSL])` utilice `certificados personalizados`: **`show redistribution service status`**.

STEP 10 | Verifique que los agentes redistribuyan correctamente los datos a los clientes.

1. Vea las estadísticas del agente (**Device (Dispositivo)** > **Data Redistribution (Redistribución de datos)** > **Agents (Agentes)**) y seleccione **Status (Estado)** para ver un resumen de la actividad del agente de redistribución, como el número de asignaciones que ha recibido el cortafuegos del cliente.
2. Confirme que el estado **Connected (Conectado)** sea **yes (sí)**.
3. En el agente, acceda a la CLI y especifique el siguiente comando de la CLI para verificar el estado de la redistribución: **`show redistribution service status`**.
4. En el agente, escriba el siguiente comando de la CLI para ver los clientes de redistribución: **`show redistribution service client all`**.
5. En el cliente, especifique el siguiente comando de la CLI para verificar el estado de la redistribución: **`show redistribution service client all`**.
6. Confirme el **nombre de origen** en los logs de User-ID (**Monitor (Supervisar)** > **Logs** > **User-ID**) para verificar que el cortafuegos reciba las asignaciones a partir de los agentes de redistribución.
7. En el cliente, vea el log de etiquetas IP (**Monitor (Supervisor)** > **Logs** > **IP-Tag (Etiqueta IP)**) para confirmar que el cortafuegos del cliente recibe datos.
8. En el cliente, especifique el siguiente comando de la CLI y verifique que el origen del que el cortafuegos recibe las asignaciones sea `REDIST`: **`show user ip-user-mapping all`**.

STEP 11 | (Opcional) Para solucionar problemas de redistribución de datos, habilite la opción traceroute.

Cuando habilite la opción traceroute, el cortafuegos que recibe los datos añadirá su dirección IP al campo `<route>`, que es una lista de todas las direcciones IP del cortafuegos que han atravesado los datos. Esta opción requiere que todos los dispositivos PAN-OS en la ruta de redistribución utilicen la versión 10.0 de PAN-OS. Si un dispositivo PAN-OS en la ruta de redistribución usa PAN-OS 9.1.x o versiones anteriores, la información de traceroute termina en ese dispositivo.

1. En el agente de redistribución en el que se crea el origen, especifique el siguiente comando de la CLI: **`debug user-id test cp-login traceroute yes ip-address <dirección-ip> user <nombreusuario>`** (donde ***<dirección-ip>*** es la dirección IP de la asignación de dirección IP a nombre de usuario que desea verificar y ***<nombreusuario>*** es el nombre de usuario de la asignación de dirección IP a nombre de usuario que desea verificar.
2. En un cliente del cortafuegos en el que configuró traceroute, verifique que dicho cortafuegos redistribuya los datos. Para ello, especifique el siguiente comando de la CLI: **`show user ip-user-mapping all`**.

   El cortafuegos muestra la marca de tiempo para la creación de la asignación (`SeqNumber`) y si el usuario tiene GlobalProtect (`GP User [Usuario de GP]`).

```
admin > show user ip-user-mapping-mp ip 192.0.2.0

IP address:  192.0.2.0 (vsys1)
User:    jimdoe
From:   REDIST
Timeout:  889s
Created:  11s ago
Origin:   198.51.100.0
```


© 2020 Palo Alto Networks, Inc.

```
SeqNumber:  15895329682-67831262
GP User:  No
Local HIP:  No
Route Node 0: 198.51.100.0 (vsys1)
Route Node 1: 198.51.100.1 (vsys1)
```

Asignaciones de User-ID compartidas entre sistemas virtuales

Cuando hay varios sistemas virtuales, simplifique la configuración de los orígenes de User-ID™ definiéndolos en un solo sistema virtual, que comparte las asignaciones de direcciones IP a nombres de usuarios con los demás sistemas virtuales del cortafuegos.

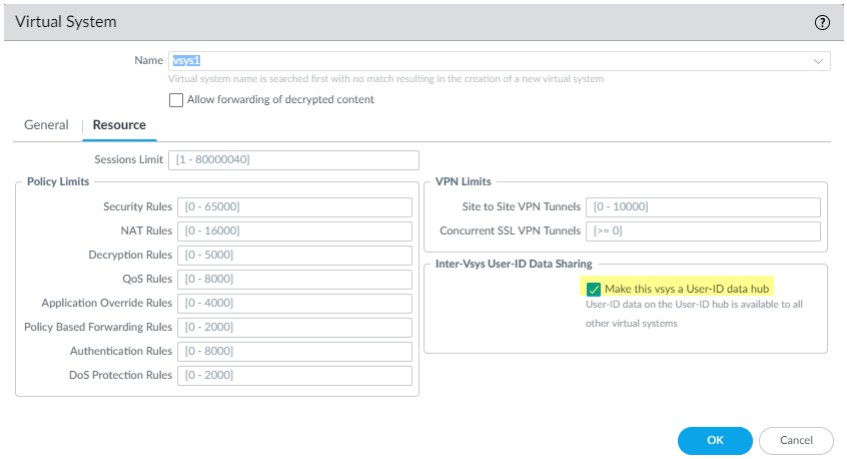
Configure un solo sistema virtual como *núcleo de User-ID* para asignar los usuarios de forma más sencilla. Así se ahorra configurar los orígenes en múltiples sistemas virtuales, en especial cuando los recursos a los que intenta acceder el usuario están dispersos por varios de ellos; en las redes universitarias, por ejemplo, los alumnos acceden a distintos departamentos con diferentes sistemas virtuales para gestionar el tráfico.

Para asignar el usuario, el cortafuegos recurre a la tabla de asignaciones disponible en el sistema virtual local y le aplica la política que le corresponde. Si el cortafuegos no encuentra ninguna asignación para un usuario concreto en el sistema virtual donde se origina su tráfico, consulta el núcleo para obtener los datos de asignación de dirección IP al nombre de ese usuario. Si encuentra la asignación tanto en el núcleo de User-ID como en el sistema virtual local, utiliza la asignación obtenida de forma local.

Tras configurar el núcleo de User-ID, cuando un sistema virtual debe identificar un usuario para aplicar la política basada en usuarios o bien mostrar el nombre de usuario en un log o informe, pero el origen no está disponible de manera local, puede recurrir a la tabla de asignaciones del núcleo de User-ID. Cuando selecciona un núcleo, el cortafuegos conserva las asignaciones en los demás sistemas virtuales, por lo que es recomendable consolidar los orígenes de User-ID en el núcleo. Sin embargo, si no desea compartir las asignaciones de algún origen concreto, puede configurar un sistema virtual separado para que realice la asignación de usuarios.

STEP 1 | Asigne el sistema virtual como núcleo de User-ID.

1. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** y, a continuación, seleccione el sistema virtual en el que haya consolidado los orígenes de User-ID.
2. En la pestaña **Resource (Recurso)**, marque **Make this vsys a User-ID data hub (Usar este vsys como núcleo de datos de User-ID)** y, a continuación, haga clic en **Yes (Sí)** para confirmar. Después, haga clic en **OK (Aceptar)**.



© 2020 Palo Alto Networks, Inc.

STEP 2 | Consolide los orígenes de User-ID y mígrelos al sistema virtual que desea emplea como núcleo de User-ID.

De esta forma, se consolida la configuración de User-ID para simplificar el funcionamiento operativo. Si configura el núcleo para que supervise los servidores y se conecte a los agentes que antes supervisaban otros sistemas virtuales, el núcleo se encarga de recopilar la información de las asignaciones de usuarios, en lugar de que los hagan los sistemas por separado. Si no desea compartir las asignaciones de algún sistema virtual concreto, configúrelas en un sistema virtual que no actúe como núcleo.

1. Elimine los orígenes que no hagan falta o estén obsoletos.
2. Identifique todas las configuraciones de los agentes integrados o basados en Windows y los orígenes que envían asignaciones de usuarios mediante la XML API y cópielas en el sistema virtual que desee utilizar como núcleo de User-ID.

   En el núcleo puede configurar cualquier origen de User-ID que esté configurado en algún sistema virtual. Sin embargo, la información sobre las asignaciones de direcciones IP y puertos a nombres de usuario de los agentes de servidores de terminal y las asignaciones de grupos no se comparten entre el núcleo de User-ID y los sistemas virtuales conectados.
3. Especifique las subredes que User-ID debe incluir en la asignación o excluir de ella.
4. Defina los usuarios oportunos en **Ignore User List (Lista de usuarios ignorados)**.
5. Elimine de todos los demás sistemas virtuales los orígenes que están en el núcleo de User-ID.

STEP 3 | Haga clic en **Commit (Confirmar)** para aceptar los cambios, habilitar el núcleo de User-ID y empezar a recopilar las asignaciones de los orígenes consolidados.

STEP 4 | Confirme que el núcleo de User-ID está asignando los usuarios.

1. Use el comando **`show user ip-user-mapping all`** para mostrar las asignaciones de direcciones IP a nombres de usuarios y los sistemas virtuales que las proporcionan.
2. Use el comando **`show user user-id-agent statistics`** para mostrar el sistema virtual que actúa como núcleo de User-ID.

App-ID

Para habilitar aplicaciones de forma segura en su red, los cortafuegos de nueva generación de Palo Alto Networks ofrecen una perspectiva tanto web como de aplicación (App-ID y filtrado de URL) frente a una amplia gama de riesgos legales, normativos, de productividad y de uso de recursos.

App-ID le permite visualizar las aplicaciones de la red, para que así pueda saber cómo funcionan y comprender las características de su comportamiento y su riesgo relativo. Este conocimiento sobre las aplicaciones le permite crear y aplicar reglas de políticas de seguridad tanto para habilitar, examinar y moldear las aplicaciones deseadas como para bloquear aquellas que no desea. Cuando defina reglas de políticas para permitir el tráfico, App-ID empezará a clasificar el tráfico sin ninguna configuración adicional.

Los App-ID nuevos y modificados se publican como parte de las actualizaciones de contenido de aplicaciones y amenazas. Siga las sugerencias de Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas para mantener actualizadas las firmas de aplicaciones y contra amenazas con eficacia.

- Descripción general de App-ID
- Reglas de políticas de App-ID mejoradas
- Inspección de App-ID y HTTP/2
- Gestión de aplicaciones personalizadas o desconocidas
- Gestión de App-ID nuevas y modificadas
- Uso de objetos de aplicación en la política
- Habilitación segura de aplicaciones en los puertos predeterminados
- Aplicaciones con compatibilidad implícita
- Optimización de las reglas de la política de seguridad
- Gateways de nivel de aplicación
- Deshabilitación de la gateway de nivel de aplicación (ALG) SIP
- Uso de encabezados de HTTP para la gestión del acceso a aplicaciones de SaaS
- Mantenimiento de los tiempos de espera personalizados de aplicaciones heredadas

© 2020 Palo Alto Networks, Inc.

Descripción general de App-ID

App-ID, un sistema de clasificación de tráfico patentado disponible únicamente en los cortafuegos de Palo Alto Networks, determina qué es la aplicación, independientemente del puerto, el protocolo, el cifrado (SSH o SSL) o cualquier otra táctica evasiva utilizada por la aplicación. Aplica múltiples mecanismos de clasificación (firmas de aplicaciones, decodificación de protocolos de aplicaciones y heurística) al flujo de tráfico de su red para identificar aplicaciones de forma precisa.

App-ID identifica las aplicaciones que pasan por su red de la siguiente forma:

- El tráfico se compara con la política para comprobar si está permitido en la red.
- A continuación, se aplican firmas al tráfico permitido para identificar la aplicación en función de sus propiedades y características de transacciones. La firma también determina si la aplicación se está utilizando en su puerto predeterminado o si está utilizando un puerto no estándar. Si la política permite el tráfico, a continuación, este se examina en busca de amenazas y se analiza en mayor profundidad para identificar la aplicación de manera más granular.
- Si App-ID determina que ya está en uso el cifrado (SSL o SSH) y que se aplica una regla de la política de descifrado, se descifra la sesión y se vuelven a aplicar las firmas de aplicaciones al flujo descifrado.
- Posteriormente, los decodificadores de protocolos conocidos se utilizan para aplicar firmas adicionales basadas en contextos para detectar otras aplicaciones que podrían estar pasando por dentro del protocolo (por ejemplo, Yahoo! Instant Messenger a través de HTTP). Los decodificadores validan si el tráfico cumple con la especificación del protocolo y ofrecen soporte para NAT transversal y la apertura de pinholes dinámicos para aplicaciones como SIP y FTP.
- Para aplicaciones que son especialmente evasivas y que no se pueden identificar mediante firmas avanzadas y análisis de protocolos, podrán utilizarse la heurística o el análisis de comportamiento para determinar la identidad de la aplicación.

Cuando se identifica la aplicación, la comprobación de la política determina cómo tratarla: por ejemplo, bloquearla o autorizarla y analizarla en busca de amenazas, inspeccionar la transferencia no autorizada de archivos y patrones de datos o moldearla utilizando QoS.

© 2020 Palo Alto Networks, Inc.

Reglas de políticas de App-ID mejoradas

Habilite de forma segura un amplio conjunto de aplicaciones con atributos comunes mediante una sola regla de políticas (por ejemplo, dé a sus usuarios acceso amplio a aplicaciones basadas en la web o habilite de forma segura todas las aplicaciones VoIP empresariales). Palo Alto Networks asume la tarea de investigar aplicaciones con atributos comunes. Después las proporciona a través de etiquetas en actualizaciones de contenido dinámico. Este procedimiento permite lo siguiente:

- Minimiza errores y ahorra tiempo.
- Le ayuda a crear políticas que se actualizan automáticamente para gestionar aplicaciones recién publicadas.
- Simplifica la transición hacia un conjunto de reglas basado en App-ID mediante el optimizador de políticas.

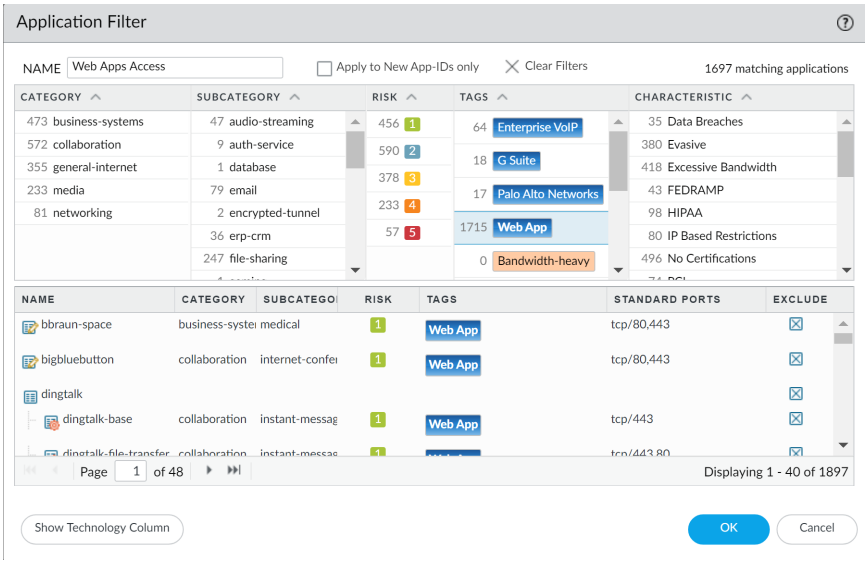
A continuación, el cortafuegos podrá usar el filtro de aplicaciones basado en etiquetas para hacer cumplir dinámicamente los App-ID nuevos y actualizados sin necesidad de revisar o actualizar las reglas de políticas cada vez que se añadan nuevas aplicaciones. Si elige excluir aplicaciones de una etiqueta específica, las nuevas actualizaciones de contenido respetarán esas exclusiones. También puede usar sus propias etiquetas para definir tipos de aplicaciones según los requisitos de su política.

- Creación de un filtro de aplicaciones mediante etiquetas
- Creación de un filtro de aplicaciones basado en etiquetas personalizadas

Creación de un filtro de aplicaciones mediante etiquetas

STEP 1 | Cree un filtro de aplicaciones con una o más etiquetas.

Si selecciona más de una etiqueta, las aplicaciones deben coincidir con ambas etiquetas para que se incluyan en el filtro.



STEP 2 | Crear una regla de la política de seguridad y **añada** el nuevo filtro de aplicaciones en la pestaña **Application (Aplicación)**.

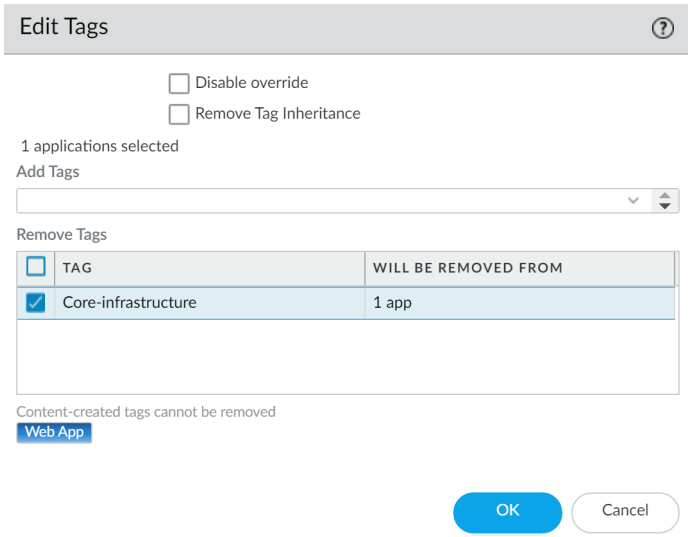
STEP 3 | **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Creación de un filtro de aplicaciones basado en etiquetas personalizadas

STEP 1 | Cree una etiqueta personalizada y aplíquela a los App-ID.

1. (Opcional) Elimine las etiquetas de la aplicación.
2. Filtre o busque aplicaciones y, a continuación, seleccione las aplicaciones específicas para eliminar etiquetas.
3. **Edite las etiquetas** y seleccione las etiquetas que quitar.

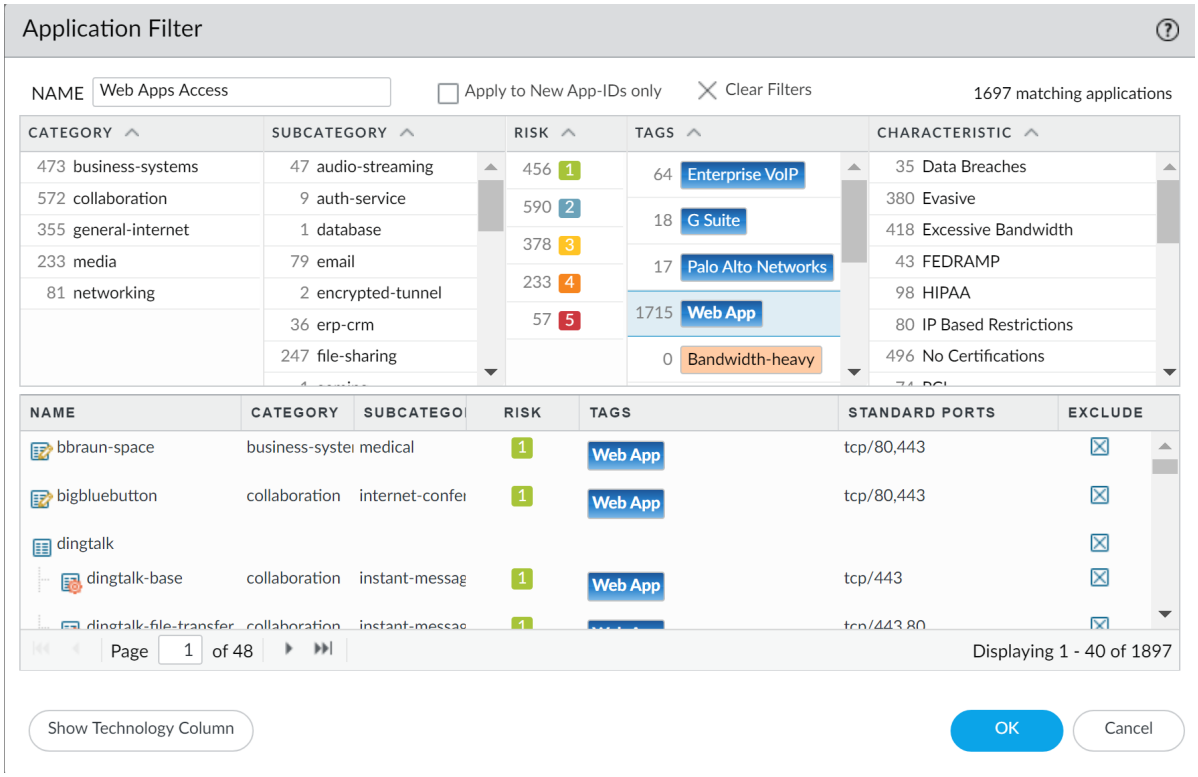


4. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree un filtro de aplicaciones con una o más etiquetas.

Si selecciona más de una etiqueta, las aplicaciones deben coincidir con ambas etiquetas para que se incluyan en el filtro.

© 2020 Palo Alto Networks, Inc.



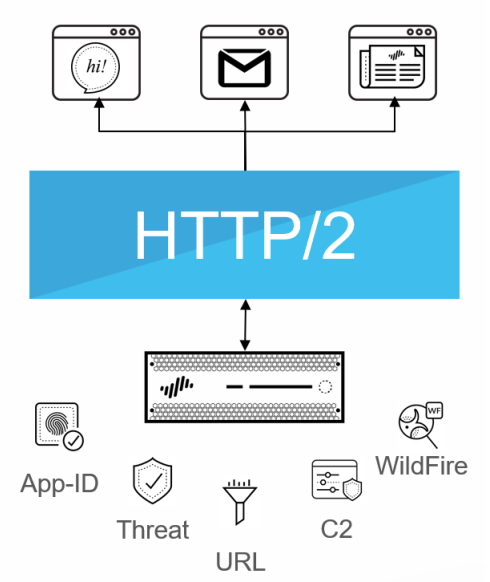
STEP 3 | Crear una regla de la política de seguridad y **añada** el nuevo filtro de aplicaciones en la pestaña **Application (Aplicación)**.

STEP 4 | **Commit (Confirmar)** los cambios.

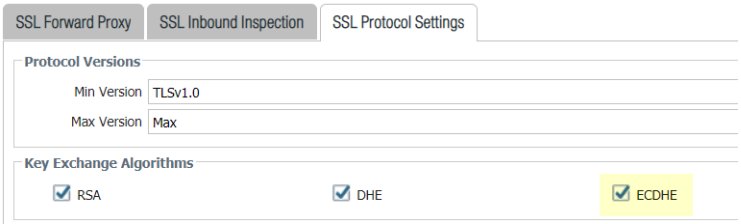
© 2020 Palo Alto Networks, Inc.

Inspección de App-ID y HTTP/2

Ya puede habilitar con seguridad las aplicaciones que se ejecutan por HTTP/2, sin tener que especificar ninguna configuración adicional en el cortafuegos. Cada vez son más los sitios web que adoptan HTTP/2, y el cortafuegos puede aplicar flujo por flujo la política de seguridad y todas las funciones de prevención y detección de amenazas. Gracias a esta visibilidad sobre el tráfico HTTP/2, no solo protege los servidores web que prestan servicios por HTTP/2, sino que también permite que sus usuarios disfruten del aumento en la rapidez y la mejora en la eficiencia de los recursos que ofrece este protocolo.



El cortafuegos procesa e inspecciona el tráfico HTTP/2 de manera predeterminada si habilita el descifrado de SSL. Para que la inspección de HTTP/2 funcione correctamente, debe habilitar el uso de ECDHE (Elliptic-Curve Diffie-Hellman) en el cortafuegos como algoritmo de intercambio de claves de las sesiones SSL. Aunque ECDHE está habilitado de forma predeterminada, puede comprobarlo seleccionando **Objects (Objetos)Decryption (Descifrado)Decryption Profile (Perfil de descifrado) SSL Decryption (Descifrado de SSL)SSL Protocol Settings (Configuración de protocolo SSL)**.



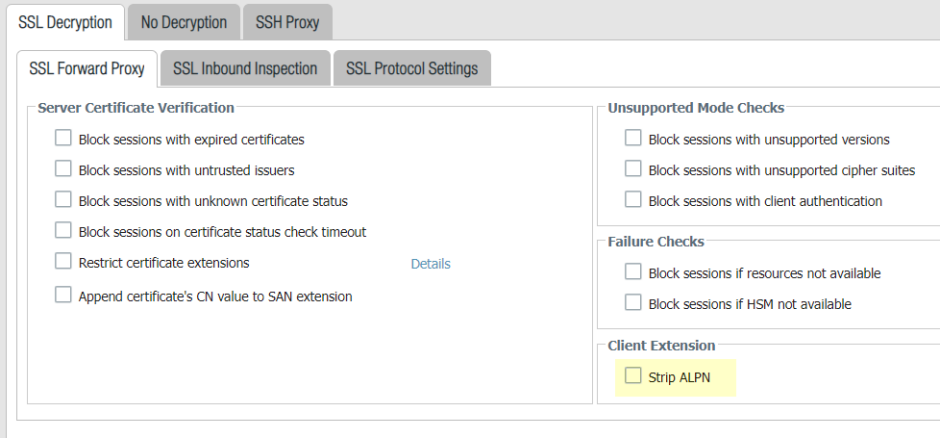
Cuando los logs de descifrado introducidos en PAN-OS 10.0 estén activados, deberá habilitar Tunnel Content Inspection (Inspección de contenido de túnel) para obtener el App-ID para el tráfico HTTP/2.

Puede deshabilitar la inspección de HTTP/2 de parte del tráfico o de todo el tráfico:

- Deshabilite la inspección de HTTP/2 de parte del tráfico.

© 2020 Palo Alto Networks, Inc.

Debe especificar que el cortafuegos elimine los valores incluidos en la extensión TLS de negociación del protocolo de la capa de aplicaciones (application-layer protocol negotiation, ALPN). ALPN se utiliza para proteger las conexiones HTTP/2; por eso, cuando no se especifica ningún valor para esta extensión de TLS, el cortafuegos cambia el tráfico HTTP/2 a la versión HTTP/1.1 o lo clasifica como tráfico TCP desconocido.



1. Seleccione **Objects (Objetos)** > **Decryption (Descifrado)** > **Decryption Profile (Perfil de descifrado)** > **SSL Decryption (Descifrado de SSL)** > **SSL Forward Proxy (Proxy SSL de reenvío)** y, a continuación, seleccione **Strip ALPN (Quitar ALPN)**.
2. Vincule el perfil de descifrado a una política de descifrado (**Policies (Políticas)** > **Decryption (Descifrado)**) para desactivar la inspección de HTTP/2 en el tráfico que coincida con dicha política.
3. **Commit (Confirmar)** los cambios.

- Deshabilite la inspección de HTTP/2 de todo el tráfico.

  Use el comando de la CLI: `set deviceconfig setting http2 enable no` y haga clic en **Commit (Confirmar)** para aceptar los cambios. El cortafuegos clasifica el tráfico HTTP/2 como tráfico TCP desconocido.

© 2020 Palo Alto Networks, Inc.

Gestión de aplicaciones personalizadas o desconocidas

Palo Alto Networks proporciona actualizaciones semanales de aplicaciones para identificar nuevas firmas App-ID. De manera predeterminada, App-ID siempre está habilitado en el cortafuegos y no necesita configurar una serie de firmas para identificar aplicaciones conocidas. Normalmente, las únicas aplicaciones clasificadas como tráfico desconocido (tcp, udp o tcp no sincronizado) en el ACC y los logs de tráfico son aplicaciones disponibles comercialmente que todavía no se han añadido a App-ID, aplicaciones internas o personalizadas de su red o posibles amenazas.

En ocasiones, el cortafuegos puede determinar que una aplicación es desconocida por los siguientes motivos:

- Datos incompletos: Se inicia el protocolo, pero no se ha enviado ningún paquete de datos antes de que se agote el tiempo de espera.
- Datos insuficientes: Se inicia el protocolo seguido por uno o más paquetes de datos; sin embargo, no se han intercambiado suficientes paquetes de datos para identificar la aplicación.

Las siguientes opciones son las disponibles para gestionar aplicaciones desconocidas:

- Cree políticas de seguridad para controlar aplicaciones desconocidas por TCP desconocido, UDP desconocido o por una combinación de zona de origen, zona de destino y direcciones IP.
- Solicite una App-ID de Palo Alto Networks: Si desea inspeccionar y controlar las aplicaciones que atraviesan su red en busca de tráfico desconocido, puede tomar una captura de paquetes. Si la captura de paquetes revela que la aplicación es una aplicación comercial, puede enviar dicha captura de paquetes a Palo Alto Networks para que desarrolle una App-ID. Si es una aplicación interna, puede crear un App-ID personalizado o definir una política de cancelación de aplicación.
- Creación de una aplicación personalizadacon una firma y adjúntela a una política de seguridad, o cree una aplicación personalizada y defina una política de cancelación de aplicación. Una aplicación personalizada le permite personalizar la definición de la aplicación interna (sus características, categoría y subcategoría, riesgo, puerto y tiempo de espera) y ejercer un control detallado de las políticas para minimizar el rango de tráfico no identificado en su red. La creación de una aplicación personalizada también le permite identificar correctamente la aplicación en el **ACC** y los logs de tráfico, y resulta de utilidad a la hora de realizar auditorías/informes de las aplicaciones de su red. En el caso de una aplicación personalizada, puede especificar una firma y un patrón que identifiquen de manera exclusiva la aplicación y usarla en una política de seguridad que permita o niegue la aplicación.

  De forma alternativa, si desea que el cortafuegos procese la aplicación personalizada utilizando el método rápido (la inspección de capa 4 en lugar de utilizar App-ID para la inspección de capa 7), puede hacer referencia al App-ID personalizado en una regla de políticas de cancelación de aplicación. Una cancelación de aplicación con una aplicación personalizada evitará que el motor de App-ID procese la sesión, lo cual es una inspección de capa 7. Por el contrario, obliga a que el cortafuegos gestione la sesión como un cortafuegos de inspección de estado normal en la capa 4, con lo que ahorra tiempo de procesamiento de la aplicación.

  Por ejemplo, si crea una aplicación personalizada que se activa en el encabezado de un host *www.misitioweb.com*, los paquetes se identifican primero como *navegación web* y, a continuación, se identifican con su aplicación personalizada (cuya aplicación principal es navegación web). Dado que la aplicación principal es navegación web, la aplicación personalizada se inspecciona como capa 7 y se examina en busca de contenido y vulnerabilidades.

  Si define una cancelación de aplicación, el cortafuegos deja de procesar en la capa 4. El nombre de la aplicación personalizada se asigna a la sesión para ayudar a identificarla en los logs y no se examina el tráfico en busca de amenazas.

© 2020 Palo Alto Networks, Inc.

Gestión de App-ID nuevas y modificadas

Las App-ID nuevas y modificadas se entregan al cortafuegos como parte de las Actualizaciones de contenido de aplicaciones y prevención de amenazas. Mientras que las App-ID nuevas y modificadas permiten al cortafuegos aplicar su política de seguridad con una precisión cada vez mayor, los cambios en la aplicación de la política de seguridad que se producen cuando se instala una versión de actualización de contenido pueden afectar la disponibilidad de la aplicación. Por este motivo, deberá considerar cómo implementar mejor las actualizaciones de contenido, de modo que pueda obtener la prevención de amenazas más reciente cuando esté disponible y ajustar la política de seguridad para aprovechar mejor las App-ID nuevas y modificadas.

Las siguientes opciones le permiten evaluar el impacto de una nueva App-ID en la aplicación de las políticas existentes, deshabilitar (y habilitar) App-ID, y actualizar a la perfección las reglas de políticas para asegurar y aplicar las aplicaciones recientemente identificadas:

- Flujo de trabajo para incorporar mejor las App-ID nuevas y modificadas
- Visualización de las ID de aplicación nuevas y modificadas en una versión de contenido
- Cómo las App-ID nuevas y modificadas afectan su política de seguridad
- Garantizar que se permitan nuevas App-ID críticas
- Supervisión de nuevos App-ID
- Deshabilitación y habilitación de App-ID

También puede aprovechar las Reglas de políticas de App-ID mejoradas que utilizan etiquetas de aplicación proporcionadas en las actualizaciones de contenido.

Flujo de trabajo para incorporar mejor las App-ID nuevas y modificadas

Consulte este flujo de trabajo principal para configurar las actualizaciones de contenido de aplicaciones y amenazas, y para incorporar mejor las App-ID nuevas y modificadas en su política de seguridad. Todo lo que necesita para implementar las actualizaciones de contenido se encuentra aquí.

STEP 1 | Alinee sus necesidades empresariales con un enfoque hacia la implementación de actualizaciones de contenido de aplicaciones y prevención de amenazas.

Descubra cómo funcionan las actualizaciones de contenido de aplicaciones y prevención de amenazas e identifique a su organización como crítica o prioridad de seguridad. Comprender cuáles son más importantes para su empresa le permitirá decidir cómo implementar mejor las actualizaciones de contenido y aplicar las prácticas recomendadas para satisfacer sus necesidades empresariales. Es posible que desee aplicar una combinación de ambos enfoques, según la implementación del cortafuegos (centro de datos o perímetro) o la ubicación de la oficina (remota o sede).

STEP 2 | Lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas y aplique las recomendaciones adecuadas según los requisitos de seguridad de la red y disponibilidad de las aplicaciones de su organización.

STEP 3 | Configure una regla de la política de seguridad para siempre permitir las App-ID nuevas que podrían afectar a toda la red, como las aplicaciones de autenticación o desarrollo de software.

La característica de la nueva App-ID coincide únicamente con las App-ID que se introducen en la versión de contenido más reciente. Cuando se utiliza en una política de seguridad, esto les brinda un mes para ajustar la política de seguridad en función de las nuevas App-ID, lo que garantiza una disponibilidad

© 2020 Palo Alto Networks, Inc.

constante para las App-ID con categoría crítica (consulte Garantizar que se permitan nuevas App-ID críticas).

STEP 4 | Configure la programación para implementar actualizaciones de contenido de aplicaciones y amenazas; esto incluye la demora de la instalación de la nueva App-ID hasta contar con el tiempo para realizar las actualizaciones necesarias en la política de seguridad (mediante el uso del **umbral de App-ID nueva**).

STEP 5 | Tras configurar la programación de la instalación de actualizaciones de contenido, se recomienda que la compruebe con regularidad y vea las App-ID nuevas y modificadas en una versión de contenido.

STEP 6 | Luego, puede ver cómo las App-ID nuevas y modificadas afectan su política de seguridad, y realizar los ajustes en la política de seguridad como sea necesario.

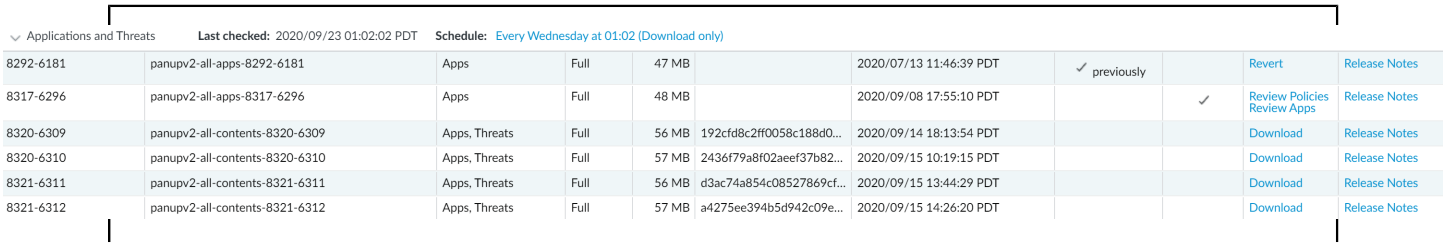
STEP 7 | Supervise las nuevas App-ID para ver la actividad de la nueva App-ID en su red, de modo que esté mejor preparado para realizar las actualizaciones más eficaces en la política de seguridad.

Visualización de las ID de aplicación nuevas y modificadas en una versión de contenido

Para las actualizaciones de contenido descargadas e instaladas, puede ver una lista de las App-ID nuevas y modificadas que incluye la actualización. Se proporcionan detalles completos de la aplicación y las actualizaciones de aplicaciones con impacto en toda la red (por ejemplo, LDAP o IKE) se marcan visiblemente como recomendadas para la revisión de la política. Para las App-ID modificadas, los detalles de la aplicación también describen cómo la cobertura se expande o es más precisa.

STEP 1 | Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y **Check Now (Comprobar ahora)** para actualizar la lista de actualizaciones de contenido disponibles.

STEP 2 | Para las versiones de contenido descargadas o instaladas actualmente, haga clic en el enlace **Review Apps (Revisar aplicaciones)** en la columna **Actions (Acciones)** para ver los detalles de las aplicaciones identificadas y modificadas recientemente en esa versión.



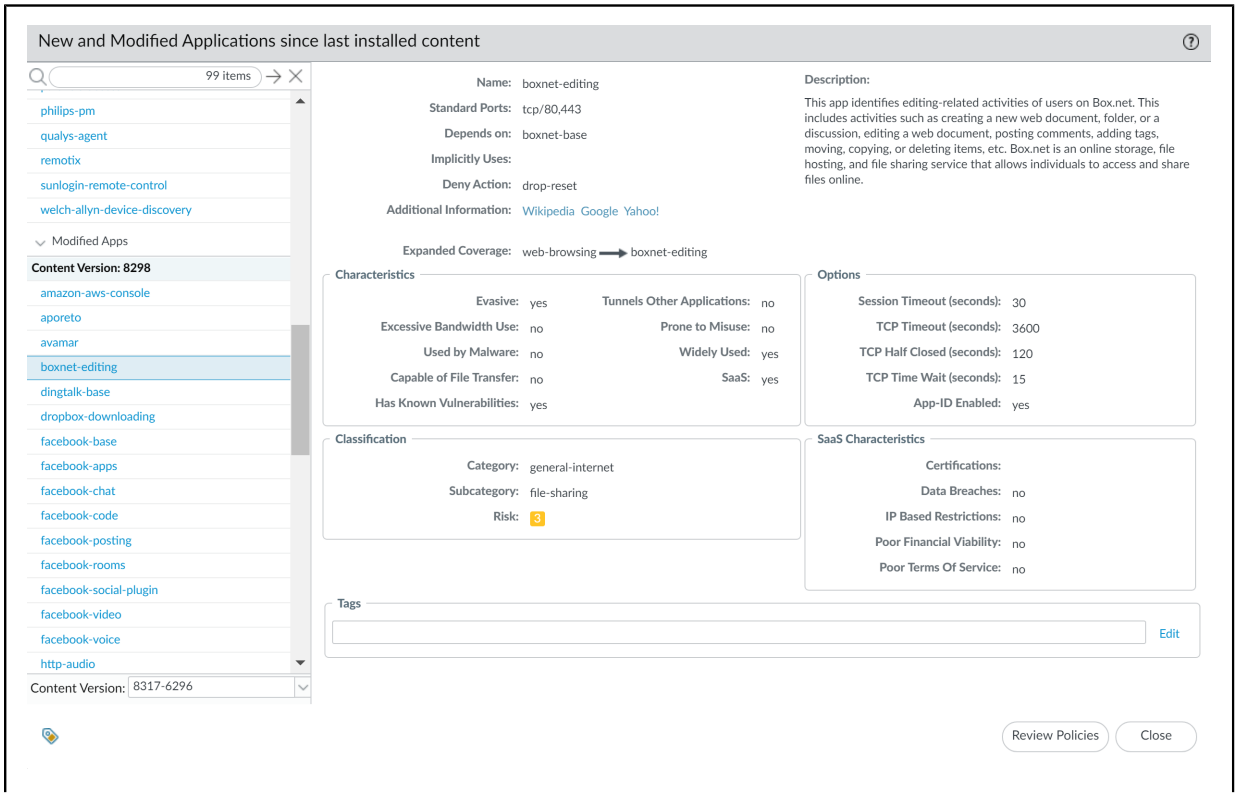
Applications and Threats **Last checked:** 2020/09/23 01:02:02 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB		2020/07/13 11:46:39 PDT	✓ previously		Revert	Release Notes
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB		2020/09/08 17:55:10 PDT		✓	Review Policies Review Apps	Release Notes
8320-6309	panupv2-all-contents-8320-6309	Apps, Threats	Full	56 MB	192cfd8c2ff0058c188d0...	2020/09/14 18:13:54 PDT			Download	Release Notes
8320-6310	panupv2-all-contents-8320-6310	Apps, Threats	Full	57 MB	2436f79a8f02aeef37b82...	2020/09/15 10:19:15 PDT			Download	Release Notes
8321-6311	panupv2-all-contents-8321-6311	Apps, Threats	Full	56 MB	d3ac74a854c08527869cf...	2020/09/15 13:44:29 PDT			Download	Release Notes
8321-6312	panupv2-all-contents-8321-6312	Apps, Threats	Full	57 MB	a4275ee394b5d942c09e...	2020/09/15 14:26:20 PDT			Download	Release Notes

STEP 3 | Revise la App-ID que introduce o modifica esta versión de contenido en comparación con la última versión de contenido.

Las App-ID nuevas y modificadas se enumeran por separado. Se proporcionan detalles completos de aplicaciones de ambas y las App-ID que Palo Alto Networks preve que afectarán a toda la red se marcan como una recomendación para que se les revise la política.

© 2020 Palo Alto Networks, Inc.



La información detallada de las App-ID nuevas que puede utilizar para evaluar un posible impacto en la aplicación de políticas incluyen:

- **Depends on**: enumera las firmas de aplicación en la que se basa este App-ID para identificar de forma única la aplicación. Si una de las firmas de aplicación enumeradas en el campo **Depends On** está deshabilitada, el App-ID que depende de ella también lo estará.
- **Previously Identified As**: enumera los App-ID que coinciden con la aplicación antes de que el nuevo App-ID se instale para identificar de forma única la aplicación.
- **App-ID Enabled (App-ID habilitada)**: todas las App-ID aparecen como habilitadas cuando se descarga una versión de contenido, a menos que opte por deshabilitar manualmente la firma de App-ID antes de instalar la actualización de contenido.

Para las App-ID modificadas, los detalles incluyen la información en: **Expanded Coverage (Cobertura expandida)**, **Remove False Positive (Eliminar falso positivo)** y los cambios en los metadatos de la aplicación. Los campos Expanded Coverage (Cobertura expandida) y Remove False Positive (Eliminar falso positivo) indican cómo cambió la cobertura de la aplicación (más completo o limitado) y un icono de reloj indica los cambios en los metadatos, donde ciertos detalles de la aplicación se actualizan.

STEP 4 | En función de sus hallazgos, haga clic en **Review Policies (Revisar políticas)** para ver cómo las App-ID nuevas y modificadas impactan en la aplicación de la política de seguridad: Cómo las App-ID nuevas y modificadas afectan su política de seguridad.

Cómo las App-ID nuevas y modificadas afectan su política de seguridad

Las App-ID recientemente clasificadas y modificadas pueden cambiar la manera en la que el cortafuegos aplica el tráfico. Realice una revisión de la política de actualización de contenido para ver cómo las App-ID nuevas y modificadas afectan su política de seguridad, y para realizar los ajustes necesarios con facilidad.

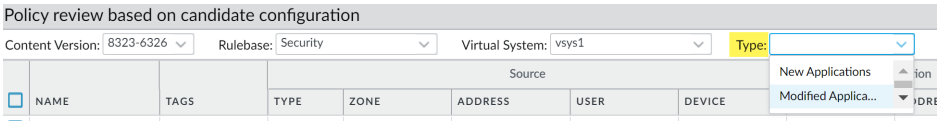
© 2020 Palo Alto Networks, Inc.

Puede realizar una revisión de la política de actualización de contenido en el contenido descargado e instalado.

STEP 1 | Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).

STEP 2 | Asegúrese de Visualizar las App-ID nuevas y modificadas en una versión de contenido para obtener más información sobre cada App-ID que introduce o modifica una versión de contenido.

STEP 3 | Para una versión de contenido descargada o instalada actualmente, haga clic en **Review Policies (Revisar políticas)** en la columna Action (Acción). El cuadro de diálogo **Policy review based on candidate configuration (Revisión de políticas basada en la configuración de candidatos)** le permite filtrar por **Content Version (Versión de contenidos)** y ver las App-ID nuevas o modificadas introducidas en una versión específica (también puede filtrar el impacto en la política de las App-ID nuevas en función de la **Rulebase [Base de reglas]** y el **Virtual System [Sistema virtual]**).



STEP 4 | Seleccione una App-ID en el menú desplegable **Application (Aplicación)** para ver las reglas de la política que implementa actualmente la aplicación. Las reglas mostradas se basan en las App-ID que coinciden con la aplicación antes de que se instale la App-ID nueva (vea los detalles de la aplicación para ver la lista de firmas de aplicaciones en **Previously Identified As [Identificado anteriormente como]** antes de la nueva App-ID).

STEP 5 | Use la información detallada que se proporciona en la revisión de la política para planificar que las actualizaciones de la regla de la política se implementen cuando la App-ID se instala, o si la versión de contenido que incluía la App-ID se encuentra instalada actualmente, los cambios que realice se implementen inmediatamente.

Puede **Add app to selected policies (Añadir aplicación a las políticas seleccionadas)** o **Remove app from selected policies (Eliminar aplicación de las políticas seleccionadas)**.

Garantizar que se permitan nuevas App-ID críticas

Las nuevas App-ID pueden causar un cambio en la aplicación de la política al tráfico que se identifica recientemente como perteneciente a una aplicación concreta. Para mitigar los impactos en la aplicación de la política de seguridad, puede utilizar la característica **New App-ID (Nueva App-ID)** en una regla de la política de seguridad, de modo que la regla siempre se aplique a las App-ID más recientes sin solicitar que se realicen cambios en la configuración cuando se instalen nuevas App-ID. La característica de la nueva App-ID siempre coincide únicamente con las App-ID nuevas en la versión de contenido más reciente. Cuando se instala una nueva versión de contenido, la característica de la nueva App-ID inicia automáticamente para coincidir únicamente con las nuevas App-ID en esa versión de contenido.

Puede optar por aplicar todos los App-ID nuevos o dirigir la regla de la política de seguridad para que aplique ciertos tipos de App-ID nuevos que puedan tener un impacto en toda la red o un impacto crítico (por ejemplo, aplicar solo aplicaciones de autenticación o desarrollo de software). Establezca la regla de la política de seguridad en **Allow (Permitir)** para garantizar que incluso si una versión de App-ID introduce una cobertura expandida o más precisa de las aplicaciones críticas, el cortafuegos las permita.

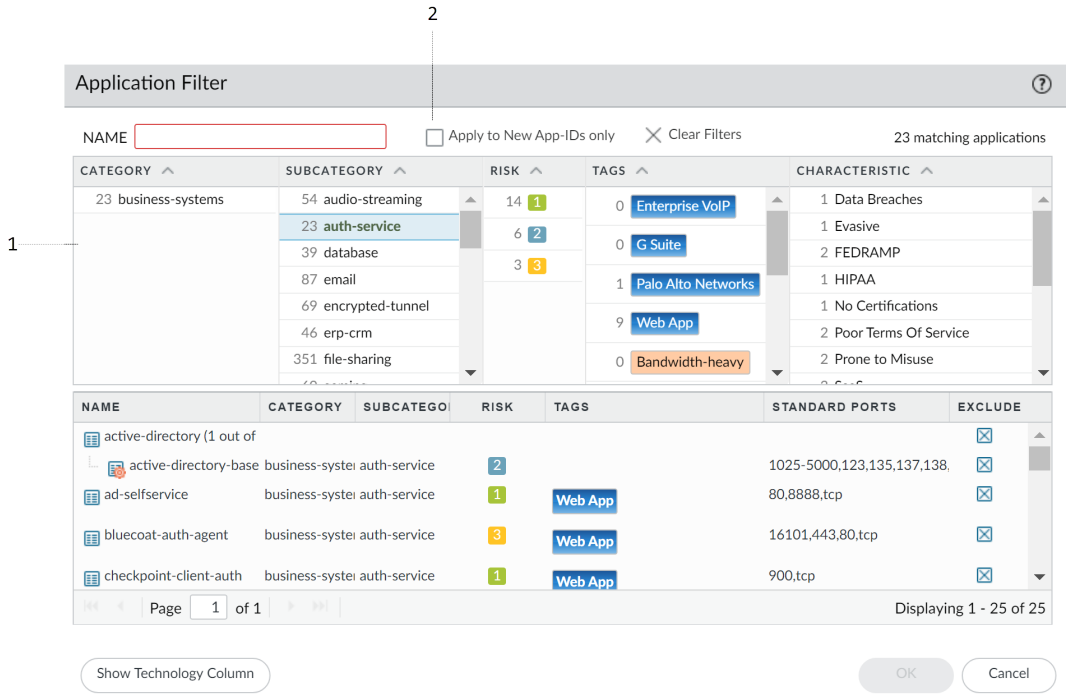
© 2020 Palo Alto Networks, Inc.

Los App-ID se liberan una vez al mes, de modo que una regla de la política que permite los App-ID más recientes le brinda un mes (o si el cortafuegos no instala actualizaciones de contenido de manera programada, hasta la próxima vez que instale manualmente el contenido) para evaluar cómo las aplicaciones recientemente clasificadas podrían afectar la aplicación de la política de seguridad y realizar los ajustes necesarios.

STEP 1 | Seleccione **Objects (Objetos)** > **Application Filters (Filtros de aplicación)** y haga clic en **Add (Añadir)** para añadir un filtro de aplicación nuevo.

STEP 2 | Defina los tipos de aplicaciones nuevas en los que desea garantizar una disponibilidad constante en función de una subcategoría o característica. Por ejemplo, seleccione la categoría "auth-service" (servicio de autenticación) para garantizar que se permitan las aplicaciones instaladas recientemente conocidas por realizar o admitir la autenticación.

STEP 3 | Solo después de filtrar los tipos de aplicaciones nuevas que desea permitir inmediatamente después de la instalación, seleccione **Apply to New App-IDs only (Aplicar a App-ID nuevos únicamente)**.



STEP 4 | Seleccione **Policies (Políticas)** > **Security (Seguridad)**, y añada o edite una regla de la política de seguridad que se configuró para que permita el tráfico coincidente.

STEP 5 | Seleccione **Application (Aplicación)** y añada el nuevo **Application Filter (Filtro de aplicación)** a la regla de la política como criterio de coincidencia.

STEP 6 | Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para guardar los cambios.

STEP 7 | Para continuar ajustando su política de seguridad para que tenga en cuenta los cambios de aplicación que introducen las nuevas App-ID:

- Supervisión de App-ID nuevos: supervise y obtenga informes de la actividad de los App-ID nuevos.

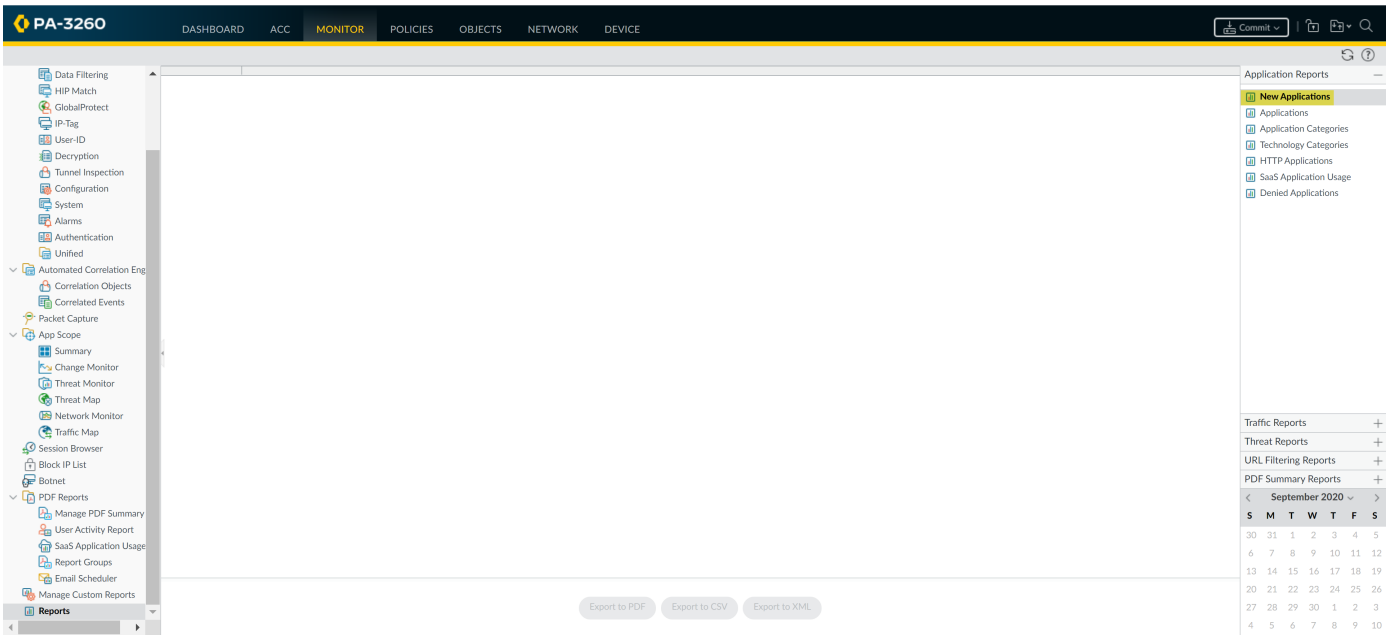
© 2020 Palo Alto Networks, Inc.

- Visualización de los App-ID nuevos y modificados en una versión de contenido: vea cómo los App-ID instalados recientemente afectan las reglas de la política de seguridad existente.

Supervisión de nuevos App-ID

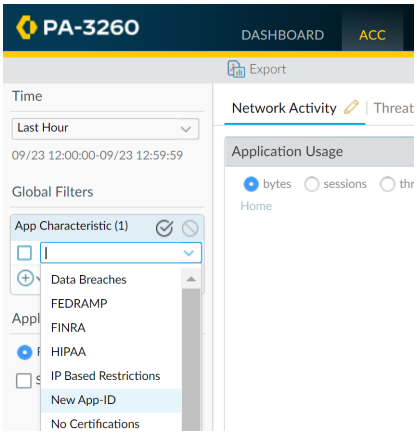
La característica **New App-ID (Nueva App-ID)** le permite supervisar nuevas aplicaciones de su red, de modo que pueda evaluar mejor las actualizaciones de la política de seguridad que desee realizar. Utilice la característica Nueva App-ID en el ACC para obtener visibilidad de las aplicaciones nuevas en su red y para generar informes que detallen la actividad de la aplicación con categoría nueva. La información que obtenga lo ayudará a tomar las decisiones correctas con respecto a cómo actualiza su política de seguridad para aplicar las App-ID con categoría nueva más recientes. Ya sea que las utilice en el ACC o para generar informes (o para Garantizar que se permitan nuevas App-ID críticas), la característica de nueva App-ID siempre coincide únicamente con la App-ID nueva en las versiones de contenido instaladas más recientes. Cuando se instala una nueva versión de contenido, la característica de la nueva App-ID inicia automáticamente para coincidir únicamente con las nuevas App-ID en esa versión de contenido.

- Genere un informe con la información detallada sobre las nuevas aplicaciones (aplicaciones introducidas únicamente en la versión de contenido más reciente).



- Utilice el ACC para supervisar las actividades nuevas de las aplicaciones: seleccione **ACC** y en **Global Filters (Filtros globales)**, seleccione **Application (Aplicaciones)** > **Application Characteristics (Características de las aplicaciones)** > **New App-ID (Nueva App-ID)**.

© 2020 Palo Alto Networks, Inc.



Deshabilitación y habilitación de App-ID

Puede deshabilitar todas las App-ID en una versión de contenido si desea aprovechar inmediatamente la prevención de amenazas más reciente y planea habilitar las App-ID en el futuro, y puede deshabilitar las App-ID de aplicaciones específicas.

Las reglas de políticas que hacen referencia a App-ID solo identifican y aplican el tráfico basado en los App-ID habilitados.

Ciertos App-ID no pueden deshabilitarse, y solo permiten el estado habilitado. Las App-ID que no se pueden deshabilitar incluyen las firmas de aplicaciones que utilizan implícitamente otras App-ID (como tcp desconocido). La deshabilitación de un App-ID base puede provocar que también se deshabiliten los App-ID que dependan de ese App-ID base. Por ejemplo, la deshabilitación de la base-facebook deshabilitaría también todas las demás App-ID de Facebook.

- Deshabilitación de todos los App-ID de una versión de contenido o de actualizaciones de contenido programadas.

  Mientras que esta opción le permite protegerse contra las amenazas y le brinda la opción de habilitar la App-ID en el futuro, Palo Alto Networks recomienda que en lugar de deshabilitar las App-ID de manera regular, configure una regla de la política de seguridad para permitir temporalmente App-ID nuevas. Esta regla siempre permitirá las App-ID nuevas únicamente en la versión de contenido más reciente. Debido a que las actualizaciones de contenido que incluyen las App-ID nuevas se publican una vez al mes, esto le brinda tiempo para evaluar las App-ID nuevas y ajustar su política de seguridad para abarcar las App-ID nuevas de ser necesario, lo que garantiza que la disponibilidad de las aplicaciones críticas no se ve afectada.

  - Para deshabilitar todas las App-ID nuevas en una versión de contenido, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Install (Instalar)** para instalar una versión de contenido de aplicación y prevención de amenazas. Cuando se le pida, seleccione **Disable new apps in content update**. Seleccione la casilla de verificación para deshabilitar las aplicaciones y continúe instalando la actualización de contenido.
  - En la página **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, seleccione **Schedule (Programación)**. Seleccione **Disable new apps in content update (Deshabilitar nuevas aplicaciones en actualización de contenido)** para las descargas e instalaciones de versiones de contenido.

- Deshabilitación de los App-ID de una o múltiples aplicaciones a la vez.

© 2020 Palo Alto Networks, Inc.

- Para deshabilitar rápidamente una o múltiples aplicaciones a la vez, haga clic en **Objects (Objetos)** > **Applications (Aplicaciones)**. Seleccione la casilla de verificación de una o más aplicaciones y haga clic en **Disable**.
- Para revisar los detalles de una única aplicación y después deshabilitar el App-ID de esa aplicación, seleccione **Objects (Objetos)** > **Applications (Aplicaciones)** y **Disable App-ID (Deshabilitar App-ID)**. Puede usar este paso para deshabilitar ambos App-ID pendientes (cuando se descarga en el cortafuegos la versión de contenido que incluye el App-ID pero no se instala) o App-ID instalados.

- Habilitación de App-ID.

  Habilite los App-ID que deshabilitó previamente seleccionando **Objects (Objetos)** > **Applications (Aplicaciones)**. Seleccione la casilla de verificación de una o más aplicaciones y haga clic en **Enable** o abra los detalles de una aplicación específica y haga clic en **Enable App-ID**.

© 2020 Palo Alto Networks, Inc.

Uso de objetos de aplicación en la política

Utilice objetos de aplicación para definir cómo su política de seguridad gestiona las aplicaciones.

- Creación de un grupo de aplicaciones
- Creación de un filtro de aplicaciones
- Creación de una aplicación personalizada
- Resolución de dependencias de aplicaciones

Creación de un grupo de aplicaciones

Un grupo de aplicaciones es un objeto que contiene aplicaciones que desea tratar de forma similar en una política. Los grupos de aplicaciones son útiles para permitir acceso a aplicaciones cuyo uso puede aprobar explícitamente dentro de su organización. La agrupación de aplicaciones sancionadas simplifica la administración de las bases de reglas. En lugar de tener que actualizar reglas individuales de la política cuando hay un cambio en las aplicaciones que admite, puede actualizar únicamente los grupos de aplicaciones afectadas.

Cuando decida cómo agrupar aplicaciones, considere cómo quiere aplicar acceso a sus aplicaciones aprobadas y cree un grupo de aplicaciones que corresponda con cada uno de sus objetivos de políticas. Por ejemplo, puede que haya algunas aplicaciones a las que solo quiere que accedan sus administradores de TI, y otras aplicaciones que quiera que estén a disposición de cualquier usuario conocido de su organización. En este caso, debe crear grupos de aplicaciones separadas para cada uno de esos objetivos de políticas. Aunque por lo general quiera permitir acceso a las aplicaciones únicamente en el puerto predeterminado, puede que quiera agrupar aplicaciones que sean una excepción y aplicar acceso a estas aplicaciones en una regla distinta.

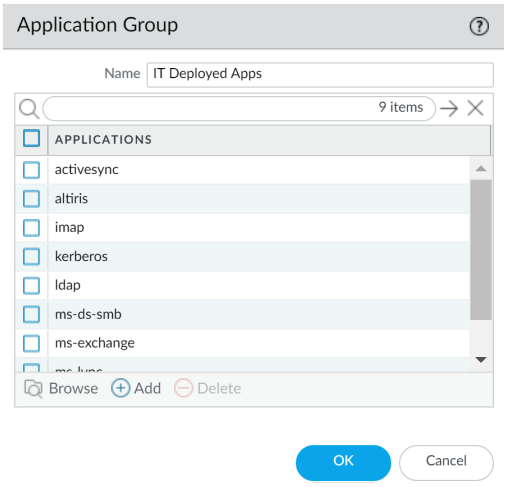
STEP 1 | Seleccione **Objects (Objetos)** > **Application Groups (Grupos de aplicaciones)**.

STEP 2 | Seleccione **Add (Añadir)** para añadir un grupo y **Name (Nombre)** para asignarle un nombre descriptivo.

STEP 3 | (Opcional) Seleccione **Shared (Compartido)** para crear el objeto en una ubicación compartida para el acceso como un objeto compartido en Panorama para el uso en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple.

STEP 4 | Seleccione **Add** para añadir las aplicaciones que desea incluir en el grupo y haga clic en **OK**.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Creación de un filtro de aplicaciones

Un filtro de aplicaciones es un objeto que agrupa dinámicamente las aplicaciones basadas en los atributos de aplicación que defina, incluidas su categoría, subcategoría, tecnología, factor de riesgo y características. Esto es útil cuando desee habilitar un acceso seguro a aplicaciones que no aprueba explícitamente, pero a la que desea que los usuarios puedan acceder. Por ejemplo, puede querer permitir que los empleados seleccionen sus propios programas de oficina (como Evernote, Google Docs o Microsoft Office 365) para uso empresarial. Para permitir de forma segura estos tipos de aplicaciones, puede crear un filtro de aplicaciones que coincida con la categoría **business-systems** y la subcategoría **office-programs**. A medida que surgen nuevos programas de oficina en aplicaciones y se crean App-ID nuevos, estas nuevas aplicaciones coincidirán automáticamente con el filtro que defina; no tendrá que realizar ningún cambio adicional en su base de reglas de políticas para habilitar de forma segura cualquier aplicación que coincida con los atributos que defina en el filtro.

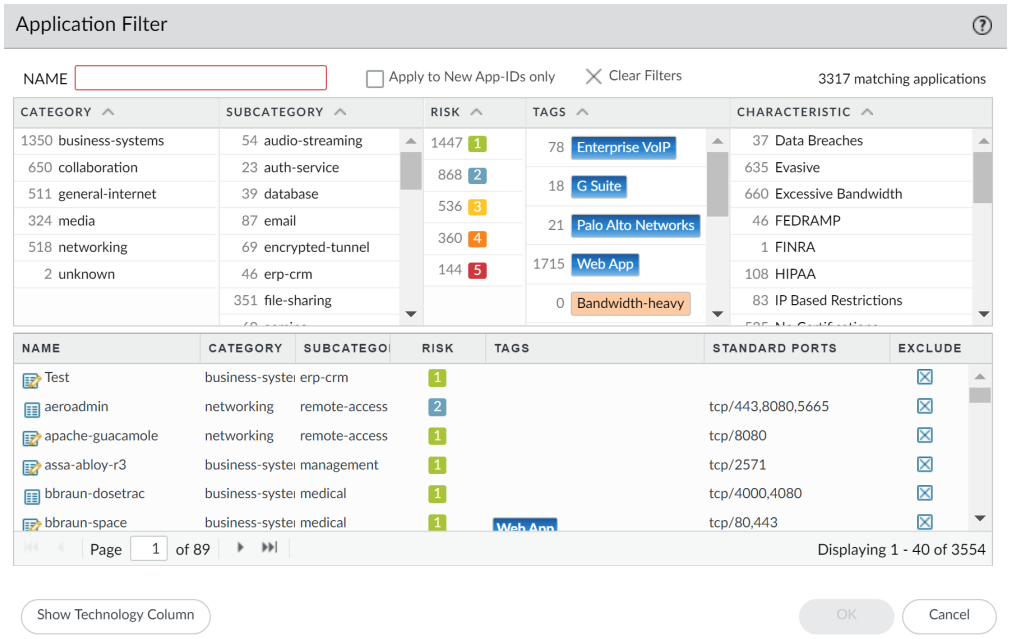
STEP 1 | Seleccione **Objects (Objetos)** > **Application Filters (FIltros de aplicación)**.

STEP 2 | Seleccione **Add** para añadir un filtro y **Name** para asignarle un nombre descriptivo.

STEP 3 | (Opcional) Seleccione **Shared (Compartido)** para crear el objeto en una ubicación compartida para el acceso como un objeto compartido en Panorama para el uso en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple.

STEP 4 | Defina el filtro seleccionando valores de atributo desde las secciones Categoría, Subcategoría, Tecnología, Riesgo y Característica. A medida que seleccione valores, observará que la lista de aplicaciones coincidentes de la parte inferior del cuadro de diálogo se reduce. Cuando ajuste los atributos de filtro para que coincidan con los tipos de aplicaciones que desee habilitar de forma segura, haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Creación de una aplicación personalizada

Para habilitar aplicaciones de forma segura, deberá clasificar todo el tráfico, en todos los puertos, en todo momento. Con App-ID, las únicas aplicaciones clasificadas normalmente como tráfico desconocido (tcp, udp o tcp no sincronizado) en el ACC y los logs de tráfico son aplicaciones disponibles comercialmente que todavía no se han añadido a App-ID, aplicaciones internas o personalizadas de su red o posibles amenazas.

Si busca tráfico desconocido de una aplicación comercial que aún no tiene un App-ID, puede enviar una solicitud para un nuevo App-ID aquí: http://researchcenter.paloaltonetworks.com/submit-an-application/.

Para garantizar que sus aplicaciones personalizadas internas no aparezcan como tráfico desconocido, cree una aplicación personalizada. Así podrá ejercer un control granular de las políticas sobre esas aplicaciones para minimizar el intervalo de tráfico no identificado de su red, reduciendo así la superficie de ataque. La creación de una aplicación personalizada también le permite identificar correctamente la aplicación del ACC y los logs de tráfico y resulta de utilidad a la hora de realizar auditorías/informes de las aplicaciones de su red.

Para crear una aplicación personalizada, debe definir los atributos de aplicaciones: sus características, categoría y subcategoría, riesgo, puerto y tiempo de espera. Además, debe definir patrones o valores que el cortafuegos pueda usar para comparar los propios flujos de tráfico (la *firma*). Por último, puede vincular la aplicación personalizada a una política de seguridad que permita o deniegue la aplicación (o añadirla a un grupo de aplicaciones o identificarla con un filtro de aplicaciones). También puede crear aplicaciones personalizadas para identificar aplicaciones efímeras según tema, como vídeo ESPN3 del mundial de fútbol o un campeonato de baloncesto.

Para recopilar los datos correctos y así crear una firma de aplicación personalizada, necesitará comprender bien las capturas de paquetes y cómo se forman los datagramas. Si la firma se crea de manera demasiado amplia, puede que incluya otro tráfico similar

© 2020 Palo Alto Networks, Inc.

de forma accidental; si se define de manera demasiado específica, el tráfico evadirá la detección si no coincide exactamente con el patrón.

Las aplicaciones personalizadas se almacenan en una base de datos separada del cortafuegos y su base de datos no se ve afectada por las actualizaciones semanales de App-ID.

Los decodificadores de protocolos de aplicación admitidos que habilitan el cortafuegos para que detecte las aplicaciones que puedan estar pasando a través de un túnel dentro del protocolo incluyen los siguientes, según la actualización de contenido 609: FTP, HTTP, IMAP, POP3, SMB y SMTP.

A continuación se muestra un ejemplo básico de cómo crear una aplicación personalizada.

STEP 1 | Reúna información sobre la aplicación que pueda usar para escribir firmas personalizadas.

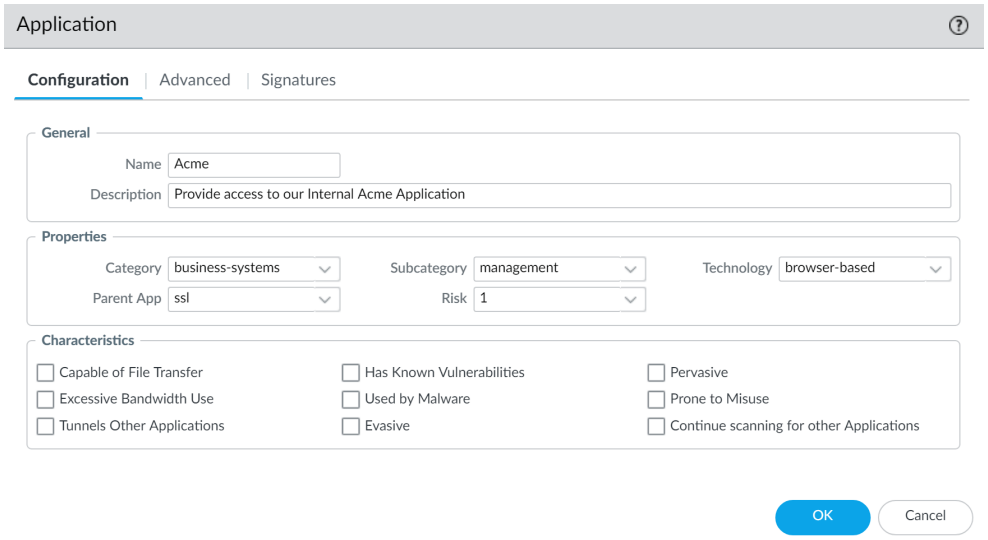
Para ello, debe conocer la aplicación y cómo controlar el acceso. Por ejemplo, puede limitar qué operaciones pueden realizar los usuarios en la aplicación (como cargar, descargar o transmitir en directo). Tal vez quiera permitir la aplicación, pero aplicando políticas de QoS.

- Capture paquetes de aplicación de modo que pueda encontrar características únicas sobre la aplicación en la que basar su firma de aplicación personalizada. Un modo de hacerlo es ejecutar un analizador de protocolos, como Wireshark, en el sistema del cliente para capturar los paquetes entre el cliente y el servidor. Realice distintas acciones en la aplicación, como la carga y descarga, para que pueda ubicar cada tipo de sesión en las capturas de paquetes resultantes (PCAP).
- Como el cortafuegos por defecto toma capturas de paquetes de todo el tráfico desconocido, si el cortafuegos se encuentra el cliente y el servidor podrá ver la captura de paquete para el tráfico desconocido directamente desde el log de tráfico.
- Use las capturas de paquete para encontrar patrones o valores en los *contextos* de paquete que puede usar para crear firmas que coincidan de forma única con el tráfico de aplicación. Por ejemplo, busque patrones de cadena en encabezados de solicitudes o respuestas HTTP, rutas URI o nombres de host. Si desea información sobre los distintos contextos de cadena que puede usar para crear firmas de aplicaciones y en los que puede buscar los valores correspondientes en el paquete, consulte Creación de firmas de amenazas personalizadas.

STEP 2 | Añada la aplicación personalizada.

1. Seleccione **Objects (Objetos)** > **Applications (Aplicaciones)** y haga clic en **Add (Añadir)**.
2. En la pestaña **Configuration (Configuración)**, escriba un nombre en **Name** y una descripción en **Description (Descripción)** para la aplicación personalizada, lo que ayudará a otros administradores a entender por qué creó la aplicación.
3. (Opcional) Seleccione **Shared (Compartido)** para crear el objeto en una ubicación compartida para el acceso como un objeto compartido en Panorama para el uso en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple.
4. Defina las Propiedades y Características de la aplicación.

© 2020 Palo Alto Networks, Inc.



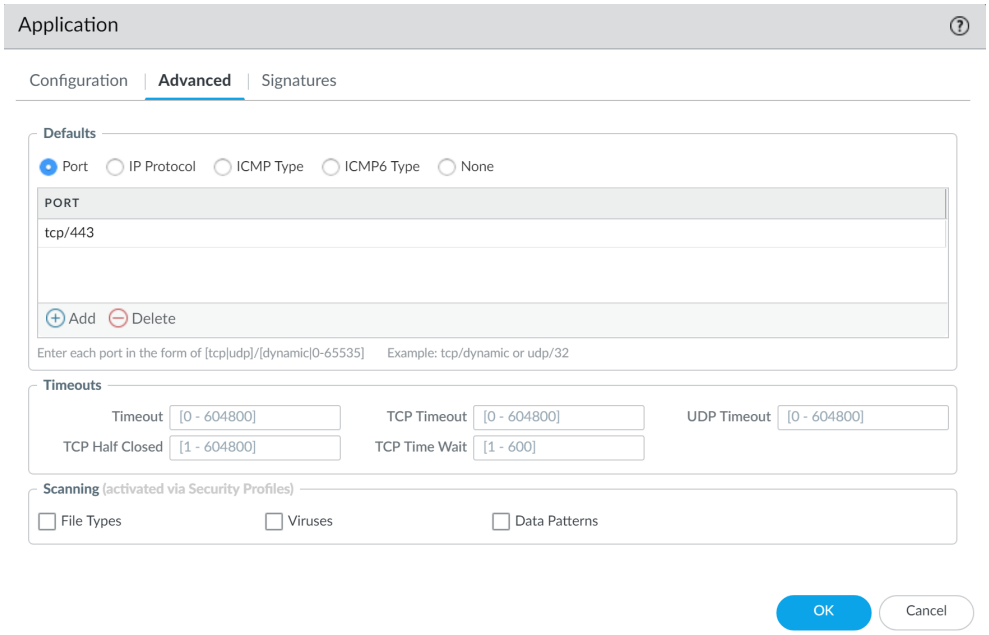
STEP 3 | Defina detalles sobre la aplicación, como el protocolo subyacente, el número de puerto en el que se ejecuta la aplicación, los valores de tiempo de espera y cualquier tipo de escaneo que puede realizar en el tráfico.

En la pestaña **Advanced**, defina los ajustes que permitirán al cortafuegos identificar el protocolo de la aplicación:

- Especifique el protocolo y los puertos predeterminados que usa la aplicación.
- Especifique los valores de tiempo de espera de sesión. Si no especifica valores de tiempo de espera, se usarán los predeterminados.
- Indique cualquier tipo de escaneo adicional que planee realizar en el tráfico de aplicación.

Por ejemplo, para crear una aplicación personalizada basada en TCP que se ejecute en SSL, pero use el puerto 4443 (en lugar del puerto predeterminado de SSL, 443), deberá especificar el número de puerto. Al añadir el número de puerto para una aplicación personalizada, puede crear reglas de políticas que usen el puerto predeterminado para la aplicación, en lugar de abrir puertos adicionales en el cortafuegos. Hacerlo mejora su estrategia de seguridad.

© 2020 Palo Alto Networks, Inc.



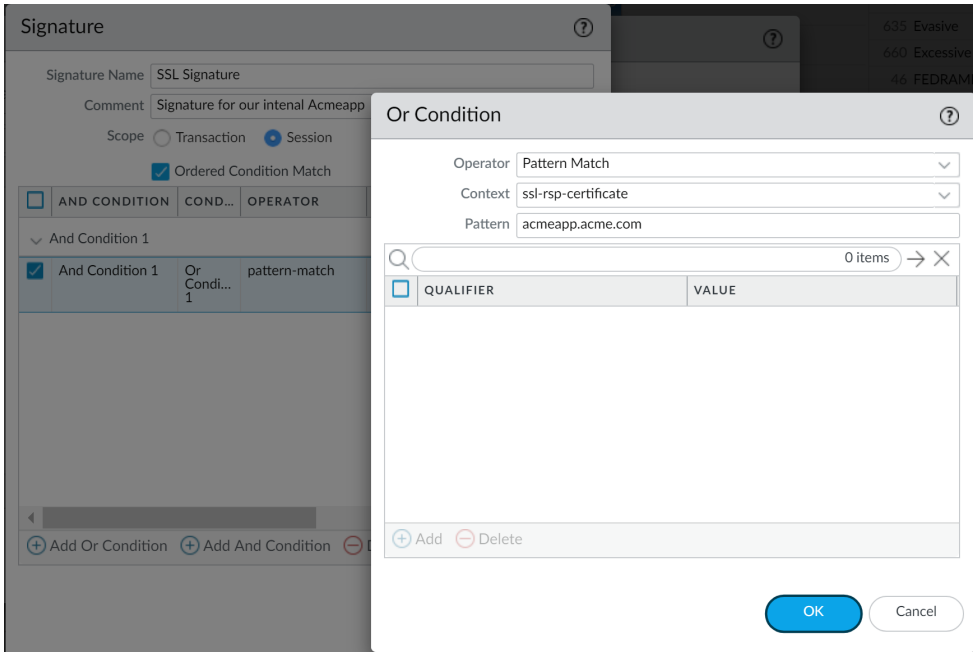
STEP 4 | Defina los criterios que utilizará el cortafuegos para comparar el tráfico con la nueva aplicación.

Usará la información que obtuvo de las capturas de paquete para especificar los valores de contexto de cadena que puede usar el cortafuegos para comparar los patrones en el tráfico de aplicación.

1. En la pestaña **Signatures (Firmas)**, haga clic en **Add (Añadir)**, defina un nombre en **Signature Name (Nombre de firma)** y, si lo desea, un comentario en **Comment (Comentario)** para ofrecer información sobre cómo desea usar esta firma.
2. Especifique el ámbito de la firma en **Scope**: **Session** si coincide con una sesión completa o **Transaction** si es una única transacción.
3. Especifique condiciones para definir firmas haciendo clic en **Add And Condition (Añadir condición Y)** o **Add Or Condition (Añadir condición O)**.
4. Seleccione un **Operator (Operador)** para definir el tipo de condiciones de comparación que usará: **Pattern Match (Coincidencia de patrón)** o **Equal To (Igual a)**.
   - Si ha seleccionado **Pattern Match (Coincidencia de patrón)**, seleccione el contexto en **Context (Contexto)** y use una expresión regular para definir el **Pattern (Patrón)** para que coincida con el contexto seleccionado. Opcionalmente, haga clic en **Add** para definir un par de calificador/valor. La lista **Qualifier (Calificador)** es específica del **Context (Contexto)** que seleccione.
   - Si ha seleccionado **Equal To (Igual a)**, seleccione el **Context (Contexto)** y use una expresión regular para definir que la opción **Position (Posición)** de los bytes del encabezado del paquete utilizada coincida con el contexto seleccionado. Seleccione **first-4bytes** o **second-4bytes**. Defina el valor hexadecimal de 4 bytes de **Mask** (por ejemplo, 0xffffff00) y **Value** (por ejemplo, 0xaabbccdd).

   Por ejemplo, si está creando una aplicación personalizada para una de sus aplicaciones internas, puede usar **ssl-rsp-certificate Context (Contexto ssl-rsp-certificado)** para definir una coincidencia de patrón para el mensaje de respuesta de certificado de una negociación SSL desde el servidor y crear un patrón en **Pattern (Patrón)** para cotejar el commonName del servidor en el mensaje como aparece aquí:

© 2020 Palo Alto Networks, Inc.



5. Repita los pasos 4.c y 4.d con cada condición que coincida.
6. Si el orden en el que el cortafuegos intenta buscar coincidencias con las definiciones de firma es importante, asegúrese de seleccionar la casilla de verificación **Ordered Condition Match (Coincidencia de condición ordenada)** y luego ordenar las condiciones para que se evalúen adecuadamente. Seleccione una condición o un grupo y haga clic en **Move Up** o **Move Down**. No puede mover condiciones de un grupo a otro.
7. Haga clic en **OK** para guardar la definición de firma.

STEP 5 | Guarde la aplicación.

1. Haga clic en **OK** para guardar la definición de aplicación personalizada.
2. Haga clic en **Commit (Confirmar)**.

STEP 6 | Valide que el tráfico coincida con la aplicación personalizada como se espera.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir una regla de la política de seguridad que permita la nueva aplicación.
2. Ejecute la aplicación desde un sistema cliente que esté entre el cortafuegos y la aplicación, y compruebe los logs de tráfico (**Monitor (Supervisar)** > **Traffic (Tráfico)**) para asegurarse de ver el tráfico que coincide con la aplicación nueva (y de que se está gestionando según su regla de políticas).

Resolución de dependencias de aplicaciones

Puede ver las dependencias de aplicaciones cuando cree una nueva regla de la política de seguridad y cuando realice confirmaciones. Cuando una política no incluye todas las dependencias de aplicación, puede acceder directamente a la regla de la política de seguridad asociada para añadir las aplicaciones necesarias.

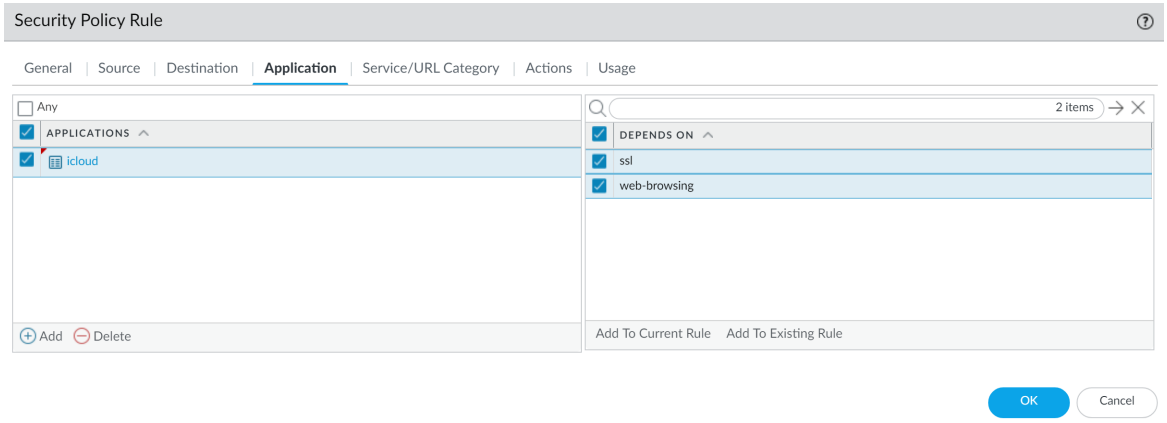
STEP 1 | Cree una regla de la política de seguridad.

STEP 2 | Especifique la aplicación que la regla permitirá o bloqueará.

1. En la pestaña **Applications (Aplicaciones)**, seleccione **Add (Añadir)** para añadir la **Application (Aplicación)** que desea habilitar de modo seguro. Puede seleccionar varias aplicaciones o utilizar grupos de aplicaciones o filtros de aplicación.

© 2020 Palo Alto Networks, Inc.

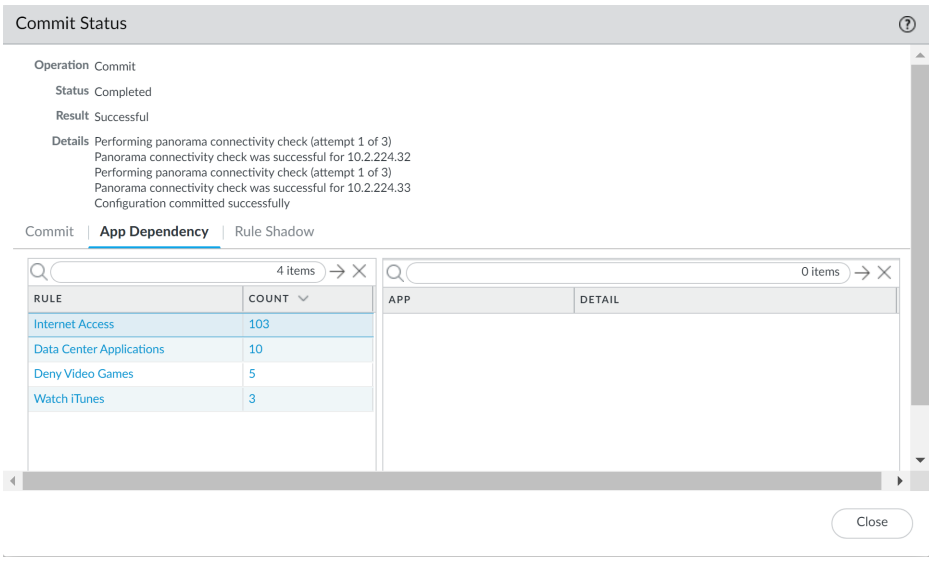
2. Vea las dependencias de las aplicaciones seleccionadas y **añádala a la regla actual** o a la **regla existente**.



3. Si se añade a una regla existente, **seleccione la regla** y haga clic en **OK (Aceptar)**.

STEP 3 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

1. Revise las advertencias de confirmación en la pestaña **App Dependency (Dependencia de aplicación)**.



2. Seleccione el **número** para ver las dependencias de aplicación no incluidas.
3. Seleccione el nombre de **regla** para abrir la política y añadir las dependencias.

Resuelva las aplicaciones dependientes. De lo contrario, seguirán generando advertencias en las confirmaciones.

4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

© 2020 Palo Alto Networks, Inc.

Habilitación segura de aplicaciones en los puertos predeterminados

Si las aplicaciones se ejecutan en puertos poco habituales, puede ser un indicio de que un atacante intenta sortear las medidas de protección tradicionales, que se implantan en los puertos. La opción application-default (valor predeterminado para la aplicación) de los cortafuegos de Palo Alto Networks ofrece un método sencillo para prevenir este tipo de elusión, así como para habilitar las aplicaciones en los puertos que más se utilizan de forma segura. Se recomienda utilizar application-default (valor predeterminado para la aplicación) en las políticas de seguridad basadas en aplicaciones, ya que reduce la sobrecarga administrativa y soluciona las brechas en la seguridad que presentan las políticas basadas en puertos:

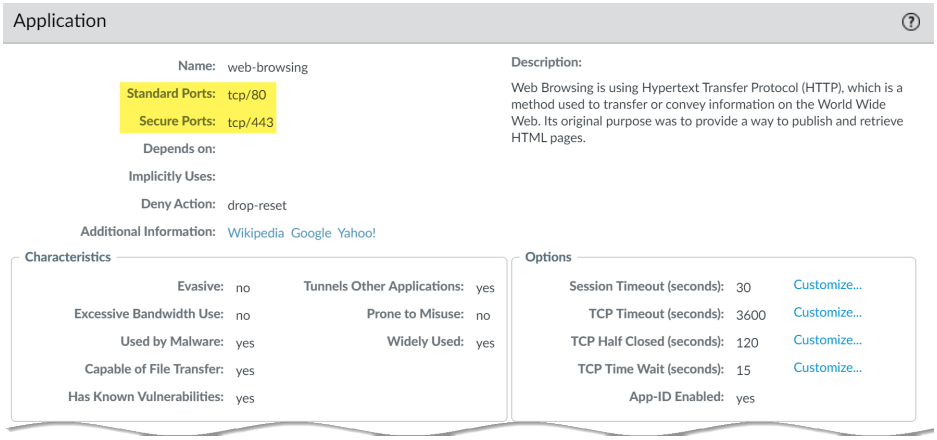
- **Reducción de la sobrecarga**: si la política de seguridad se basa en aplicaciones, puede escribir reglas sencillas que atiendan a los requisitos empresariales, en lugar de investigar y mantener asignaciones de aplicaciones a puertos. Se han definido los puertos predeterminados para todas las aplicaciones que tengan un App-ID.
- **Seguridad reforzada**: desde el punto de vista de la seguridad, siempre es recomendable habilitar las aplicaciones de modo que se ejecuten solo en sus puertos predeterminados. Con application-default (valor predeterminado para la aplicación), se asegura de que las aplicaciones vitales están disponibles, pero no ponen en peligro la seguridad si muestran un comportamiento inesperado.

  A veces, los puertos predeterminados cambian si las aplicaciones están cifradas o si emplean texto sin cifrar. La política basada en puertos exige abrir todos los puertos predeterminados que puedan usar las aplicaciones para posibilitar el cifrado. Los puertos abiertos son posibles brechas que pueden aprovechar los atacantes para eludir la política de seguridad. Con application-default (valor predeterminado para la aplicación), en cambio, se diferencia entre el tráfico de aplicaciones cifradas y el de las de texto sin cifrar. Por eso, en ambos casos, puede imponer el uso de un puerto predeterminado concreto.

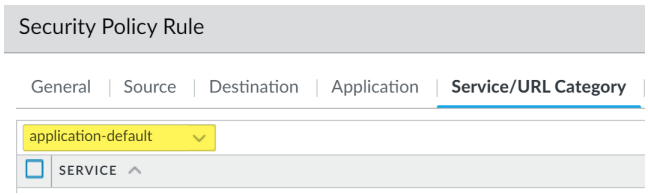
  Por ejemplo, sin application-default (valor predeterminado para la aplicación), debe abrir los puertos 80 y 443 para permitir el tráfico de navegación web —tanto cifrado como de texto sin cifrar— en ambos. Si activa application-default (valor predeterminado para la aplicación), el cortafuegos fuerza el tráfico de navegación web de texto sin cifrar solo en el puerto 80 y el tráfico por túneles de SSL solo en el puerto 443, sin concesiones.

Para ver los puertos que utiliza cada aplicación de forma predeterminada, visite Applipedia o seleccione **Objects (Objetos)** > **Applications (Aplicaciones)**. Los datos de la aplicación incluyen su puerto estándar, es decir, el puerto que se suele usar con el tráfico de texto sin cifrar. En el caso de la navegación web, los datos de SMTP, FTP, LDAP, IMAP y POP3 también incluyen el puerto seguro de la aplicación, es decir, el puerto que utiliza con el tráfico cifrado.

© 2020 Palo Alto Networks, Inc.



Seleccione **Policies (Políticas)** > **Security (Seguridad)** y añada o modifique una regla para que las aplicaciones solo puedan usar los puertos predeterminados:



Se recomienda usar application-default (valor predeterminado para la aplicación) junto con el cifrado de SSL como parte de la política de seguridad basada en aplicaciones. Además, si ya existen reglas de la política de seguridad que controlan la navegación web mediante la configuración de Service (Servicio) en service-http (servicio HTTP) y service-https (servicio HTTPS), debe actualizarlas para que usen application-default (valor predeterminado para la aplicación).

© 2020 Palo Alto Networks, Inc.

Aplicaciones con compatibilidad implícita

Cuando cree una política para permitir aplicaciones específicas, también debe asegurarse de permitir cualquier otra aplicación de la que dependa la aplicación en cuestión. En muchos casos, no tiene que permitir de manera explícita el acceso a las aplicaciones dependientes para que el tráfico fluya, ya que el cortafuegos es capaz de determinar las dependencias y permitirlas de manera implícita. Esta compatibilidad implícita también se aplica a las aplicaciones personalizadas que se basen en HTTP, SSL, MS-RPC o RTSP. Las aplicaciones para las que el cortafuegos no pueda determinar las aplicaciones dependientes a tiempo requerirán que permita de manera explícita las aplicaciones dependientes al definir sus políticas. Puede determinar las dependencias de la aplicación desde el flujo de trabajo de la política de seguridad basada en la aplicación utilizando uno de los siguientes procedimientos:

- Optimizador de políticas
- Creación de un filtro de aplicaciones mediante etiquetas
- Creación de un filtro de aplicaciones basado en etiquetas personalizadas
- Resolución de dependencias de aplicaciones

Applipedia está también disponible si fuese necesario.

La tabla siguiente enumera las aplicaciones para las que el cortafuegos tiene una compatibilidad implícita (según la actualización de contenido 595).

Application (Aplicación)	Admite implícitamente
360-safeguard-update	http
apple-update	http
apt-get	http
as2	http
avg-update	http
avira-antivir-update	http, ssl
blokus	rtmp
bugzilla	http
clubcooee	http
corba	http
cubby	http, ssl
dropbox	ssl
esignal	http
evernote	http, ssl

© 2020 Palo Alto Networks, Inc.

Application (Aplicación)	Admite implícitamente
ezhelp	http
facebook	http, ssl
chat de Facebook	jabber
complemento social de facebook	http
fastviewer	http, ssl
forticlient-update	http
good-for-enterprise	http, ssl
google-cloud-print	http, ssl, jabber
google-desktop	http
google-talk	jabber
google-update	http
gotomypc-desktop-sharing	citrix-jedi
gotomypc-file-transfer	citrix-jedi
gotomypc-printing	citrix-jedi
hipchat	http
iheartradio	ssl, http, rtmp
infront	http
instagram	http, ssl
issuu	http, ssl
java-update	http
jepptech-updates	http
kerberos	rpc
kik	http, ssl
lastpass	http, ssl
logmein	http, ssl
mcafee-update	http

© 2020 Palo Alto Networks, Inc.

Application (Aplicación)	Admite implícitamente
megaupload	http
metatrader	http
mocha-rdp	t_120
mount	rpc
ms-frs	msrpc
ms-rdp	t_120
ms-scheduler	msrpc
ms-service-controller	msrpc
nfs	rpc
oovoo	http, ssl
paloalto-updates	ssl
panos-global-protect	http
panos-web-interface	http
pastebin	http
pastebin-posting	http
pinterest	http, ssl
portmapper	rpc
prezi	http, ssl
rdp2tcp	t_120
renren-im	jabber
roboform	http, ssl
salesforce	http
stumbleupon	http
supremo	http
symantec-av-update	http
trendmicro	http

© 2020 Palo Alto Networks, Inc.

Application (Aplicación)	Admite implícitamente
trillian	http, ssl
twitter	http
whatsapp	http, ssl
xm-radio	rtsp

© 2020 Palo Alto Networks, Inc.

Optimización de las reglas de la política de seguridad

La función Policy Optimizer (Optimizador de políticas) proporciona un flujo de trabajo sencillo para migrar la base de reglas de la política de seguridad heredada a otra basada en App-ID. Esta refuerza la seguridad, ya que reduce la superficie de ataque y ofrece visibilidad sobre las aplicaciones para habilitarlas de forma segura. El optimizador identifica las reglas basadas en puertos para que pueda convertirlas en reglas permitidas basadas en aplicaciones o bien para que añada aplicaciones de una regla basada en puertos a una regla basada en aplicaciones existente sin perjudicar su disponibilidad. También identifica las reglas basadas en App-ID aprovisionadas en exceso, es decir, las configuradas con aplicaciones que no se utilizan. El optimizador resulta útil para priorizar la migración de las reglas basadas en puertos, para identificar las reglas basadas en aplicaciones que permiten aplicaciones que no utiliza y para analizar las características de uso de las reglas, como el recuento de resultados.

Al convertir las reglas basadas en puertos en otras basadas en aplicaciones, se refuerza la estrategia de seguridad porque selecciona las aplicaciones que desea permitir y deniega el permiso a todas las demás. De ese modo, elimina de la red el tráfico no deseado y potencialmente malintencionado. Si combina esta conversión con la restricción del tráfico de las aplicaciones a los puertos predeterminados (configure Service [Servicio] en **application-default** [valor predeterminado para la aplicación]), también evita que las aplicaciones evasivas se ejecuten en puertos distintos de los estándar.

Puede utilizar esta función en lo siguiente:

- Cortafuegos que ejecutan PAN-OS versión 9.0 y que tienen habilitada la función App-ID.
- Instancias de Panorama que ejecutan PAN-OS versión 9.0. Para disfrutar de las funciones de **Policy Optimizer (Optimizador de políticas)**, no tiene que actualizar los cortafuegos que gestiona Panorama. En cambio, para usar las funciones de **Rule Usage (Uso de reglas)** (Supervisión del uso de las reglas de políticas), los cortafuegos gestionados deben ejecutar PAN-OS 8.1 o una versión posterior. Además, si los cortafuegos gestionados se conectan a recopiladores de logs, estos también deben ejecutar PAN-OS versión 9.0. Los cortafuegos PA-7000 Series gestionados que tienen una tarjeta de procesamiento de logs (Log Processing Card, LPC) también pueden utilizar PAN-OS 8.1 (o una versión posterior).



Los cortafuegos PA-7000 Series admiten dos tarjetas de logs: la tarjeta de procesamiento de logs (log processing card, LPC) para cortafuegos PA-7000 Series y la tarjeta de reenvío de logs (log forwarding card, LFC) de alto rendimiento para cortafuegos PA-7000 Series. A diferencia de la LPC, la LFC carece de discos locales para almacenar los logs, por lo que reeenvía todos los logs a un sistema externo (o varios) de almacenamiento de logs, como Panorama o un servidor de syslog. Si utiliza la LFC, la información sobre el uso de las aplicaciones del optimizador no se muestra en el cortafuegos porque los logs del tráfico no se almacenan en ninguna ubicación local. Si utiliza la LFC, los logs de tráfico se almacenan localmente en el cortafuegos, por lo que la información de uso de la aplicación del optimizador de políticas aparece en el cortafuegos.

Sírvase de esta función para lo siguiente:

- **Migrar las reglas basadas en puertos a reglas basadas en aplicaciones**: en lugar de rastrear los logs del tráfico y asignar las aplicaciones a las reglas basadas en puertos manualmente, use el optimizador para identificar esas reglas y confeccionar una lista con las aplicaciones que coincidan con cada una. Así, puede seleccionar las aplicaciones a las que desea conceder permiso y habilitarlas de forma segura. Al convertir las reglas basadas en puertos heredadas en reglas permitidas basadas en aplicaciones, puede avalar el uso de las aplicaciones empresariales y bloquear las aplicaciones asociadas a actividades malintencionadas.

© 2020 Palo Alto Networks, Inc.

- **Identificar las reglas basadas en aplicaciones aprovisionadas en exceso**: si las reglas son demasiado generales, la red admite aplicaciones que no utiliza, lo cual incrementa la superficie de ataque y el riesgo de que se produzca tráfico malintencionado.



Elimine las aplicaciones que no utiliza de las reglas de la política de seguridad para reducir la superficie de ataque y mantener limpia la base de reglas. No admita en la red aplicaciones que no usa nadie.



Para migrar la configuración de un cortafuegos heredado a un dispositivo de Palo Alto Networks, consulte Prácticas recomendadas para realizar la migración a políticas basadas en aplicaciones.

No puede ordenar las reglas de la política de seguridad en **Policies (Políticas)** > **Security (Seguridad)** porque esa acción cambiaría el orden de las reglas en la base de reglas. Sin embargo, en **Polices (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)**, el optimizador de políticas proporciona opciones que no afectan al orden de las reglas y resultan útiles a la hora de priorizar las reglas que se deben convertir o limpiar en primer lugar. Puede ordenar las reglas por la cantidad de tráfico de los 30 últimos días, el número de aplicaciones detectadas en la regla, el número de días sin que hayan aparecido aplicaciones nuevas y el número de aplicaciones permitidas (en las reglas aprovisionadas en exceso).

Además, el optimizador sirve para otros fines, como validar las reglas de preproducción y solucionar problemas de las reglas existentes. Tenga en cuenta que el optimizador solo tiene en consideración el valor de **Log at Session End (Crear log al cerrar sesión)** e ignora **Log at Session Start (Crear log al iniciar sesión)** para no contar en las reglas las aplicaciones efímeras.



Debido a las limitaciones de recursos, los cortafuegos virtuales VM-50 Lite no admiten el optimizador de políticas.

- Conceptos de Policy Optimizer
- Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID
- Caso de uso de migración mediante la clonación de reglas: navegación web y tráfico SSL
- Adición de aplicaciones a reglas existentes
- Identificación de reglas de la política de seguridad con aplicaciones no utilizadas
- Alta disponibilidad para las estadísticas sobre el uso de las aplicaciones
- Habilitación o deshabilitación de Policy Optimizer

Conceptos de Policy Optimizer

Lea los siguientes temas para obtener más información sobre las prestaciones de esta función:

- Ordenación y filtrado de las reglas de la política de seguridad
- Borrado de los datos sobre el uso de las aplicaciones

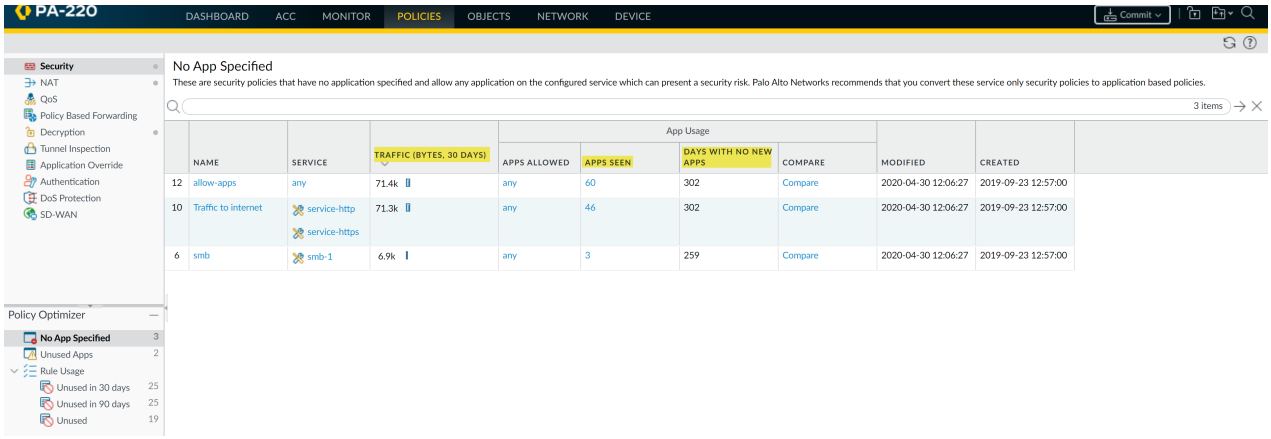
Ordenación y filtrado de las reglas de la política de seguridad

Puede filtrar las reglas de la política de seguridad para ver todas las que se basan en puertos y no tienen configuradas aplicaciones con **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)**. También puede filtrar todas las reglas que tienen configuradas aplicaciones pero no hay tráfico en todas ellas con **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **Unused Apps (Aplicaciones no usadas)**. Puede ordenar las reglas de la política filtradas por distintos tipos de estadísticas para que le resulte más fácil priorizar las reglas basadas en puertos que se deben convertir en otras basadas en aplicaciones o que se deben limpiar en primer lugar.

© 2020 Palo Alto Networks, Inc.

No puede filtrar ni ordenar las reglas en Policies (Políticas) > Security (Seguridad) porque esa acción cambiaría el orden de las reglas de la política en la base de reglas. Filtrar y ordenar Policies (Políticas) > Security (Seguridad) > Policy Optimizer (Optimizador de políticas) > No App Specified (Ninguna aplicación especificada) y Policies (Políticas) > Security (Seguridad) > Policy Optimizer (Optimizador de políticas) > Unused Apps (Aplicaciones no usadas) no cambia el orden de las reglas en la base de reglas.

Puede hacer clic en el encabezado de varias columnas para ordenar las reglas basadas en puertos (**No App Specified [Ninguna aplicación especificada]**) y las reglas con aplicaciones que no se utilizan (**Unused Apps [Aplicaciones no usadas]**) en función de las estadísticas de uso de las aplicaciones. Además, puede consultarlas para identificar y eliminar las reglas que no se utilizan a fin de reducir los riesgos para la seguridad y mantener organizada la base de reglas de la política; para ello, lea Visualización de la utilización de las reglas de la política. El seguimiento de la utilización de las reglas le permite validar con rapidez las nuevas reglas añadidas y las modificadas, así como supervisar el uso de todas en las operaciones y las tareas de solución de problemas.



- **Traffic (Bytes, 30 days) (Tráfico [bytes, 30 días])**: indica la cantidad de tráfico detectada en la regla en los 30 últimos días. Con esta franja de 30 días, las reglas que tienen más tráfico *en ese momento* se sitúan al principio de la lista de forma predeterminada; ahora bien, si la franja es más prolongada, las más antiguas ocupan los primeros puestos de la lista, ya que el total acumulado es mayor, aunque ya no detecten mucho tráfico. Haga clic para invertir el orden.
- **Apps Seen (Aplicaciones detectadas)**: se sitúan al principio las reglas que tienen más o menos aplicaciones. El cortafuegos no depura nunca los datos de las aplicaciones de forma automática.

  El cortafuegos actualiza Apps Seen (Aplicaciones detectadas) cada hora más o menos, aunque puede ser más tiempo si existen numerosas reglas o un gran volumen de tráfico de aplicaciones. Cuando añada una aplicación a una regla, espere al menos una hora antes de ejecutar los logs de tráfico para ver su información.
- **Days with No New Apps (Días sin aplicaciones nuevas)**: se sitúan al principio las reglas con las que no ha coincidido ninguna aplicación nueva durante más o menos días.
- (Solo en **Unused Apps [Aplicaciones no usadas]**) **Apps Allowed (Aplicaciones permitidas)**: se sitúan al principio las reglas que tienen más o menos aplicaciones configuradas.

En las estadísticas de uso, solo se tienen en cuenta las aplicaciones de las reglas que cumplen los siguientes criterios:

- El valor Action (Acción) de la regla debe ser **Allow (Permitir)**.
- El valor Log Settings (Configuración de logs) de la regla debe ser **Log at Session End (Crear log al cerrar sesión)**, que es el predeterminado. Se ignoran las reglas que tienen el valor **Log at Session Start (Crear log al iniciar sesión)** para que no se cuenten las aplicaciones efímeras.

© 2020 Palo Alto Networks, Inc.

- El tráfico válido debe coincidir con la regla. Por ejemplo, si la sesión termina antes de que el tráfico atraviese el cortafuegos y se identifique la aplicación, no se tiene en cuenta. Los tipos de tráfico siguientes no son válidos y, por lo tanto, no se cuentan en las estadísticas de Policy Optimizer (Optimizador de políticas):
  - Insufficient-data
  - Not-applicable
  - Non-syn-tcp
  - Incomplete

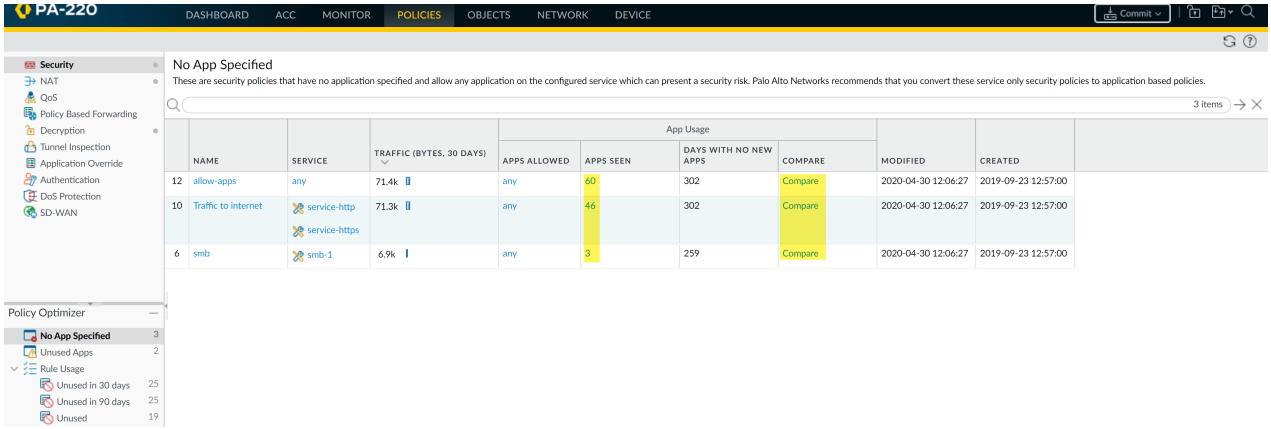
  Puede filtrar los logs del tráfico con **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** para ver el tráfico que se identifica como perteneciente a uno de esos tipos. Por ejemplo, para ver todo el tráfico identificado como incomplete (incompleto), use el filtro **`(app eq incomplete)`**.

Si no se cumplen estos criterios, la aplicación no se tiene en cuenta en estadísticas como **Apps Seen (Aplicaciones detectadas)**, no afecta a estadísticas como **Days with No New Apps (Días sin aplicaciones nuevas)**, ni aparece en las listas de aplicaciones.

El cortafuegos no realiza el seguimiento de las estadísticas de uso de las aplicaciones correspondientes a las reglas interzone-default e intrazone-default (valores predeterminados entre zonas y dentro de cada zona) de la política de seguridad.

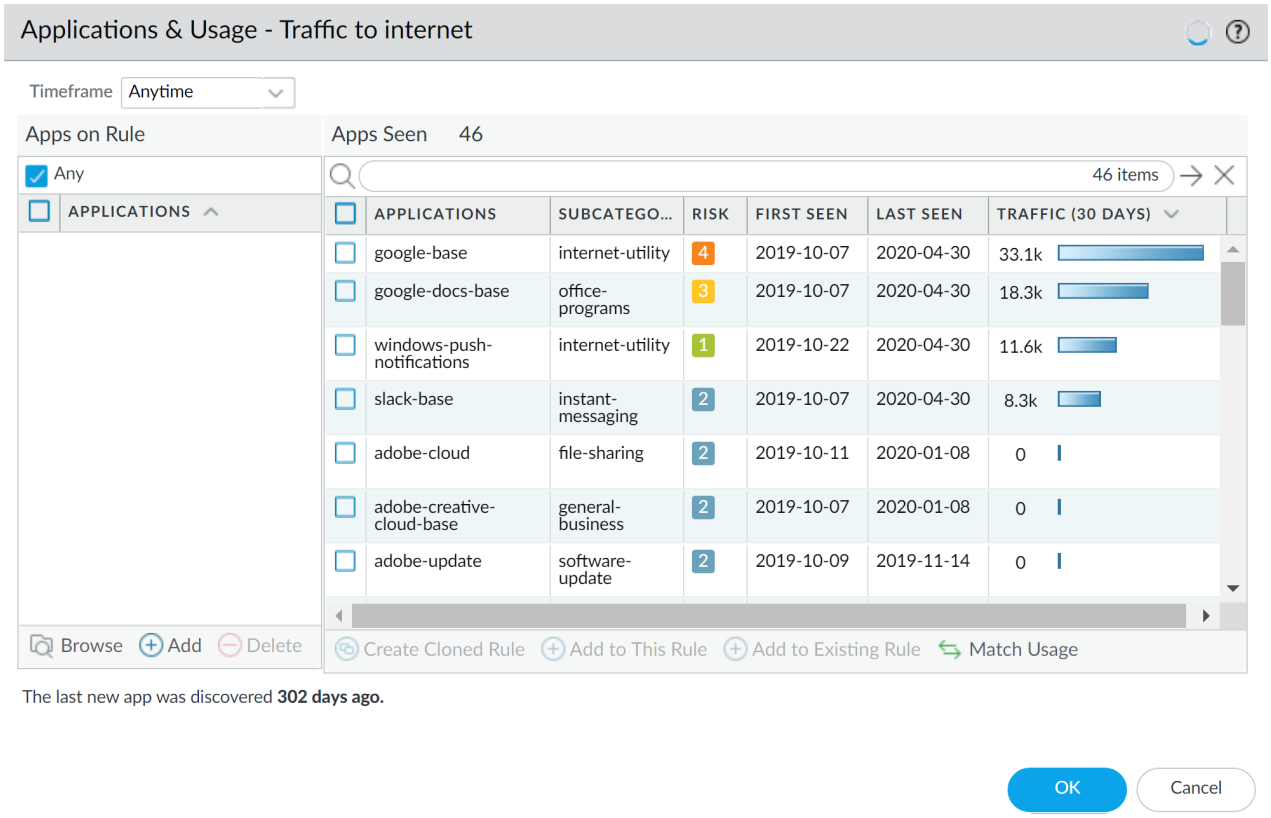
Si cambia el UUID de una regla, se restablecen sus estadísticas de uso de las aplicaciones porque, al realizar la modificación, el cortafuegos considera la regla como otra distinta, es decir, nueva.

Para ver y ordenar las aplicaciones detectadas en una regla, en la fila de esta, haga clic en **Compare (Comparar)** o bien en el número que figura en **Apps Seen (Aplicaciones detectadas)**.



En lo que respecta a las reglas que se muestran en **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)** y en **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **Unused Apps (Aplicaciones no usadas)**, al hacer clic en **Compare (Comparar)** o en el número de **Apps Seen (Aplicaciones detectadas)**, se abre **Applications & Usage (Aplicaciones y uso)**, donde puede ver y ordenar las aplicaciones detectadas en la regla oportuna. En **Applications & Usage (Aplicaciones y uso)** también puede eliminar de las reglas las aplicaciones que no se utilizan, así como realizar el procedimiento Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID.

© 2020 Palo Alto Networks, Inc.



Puede ordenar las aplicaciones detectadas en la regla por las seis estadísticas disponibles en **Apps Seen (Aplicaciones detectadas)**; tenga en cuenta que **Apps Seen (Aplicaciones detectadas)** no se actualiza en tiempo real, sino que tarda una hora o más en actualizarse en función del volumen del tráfico y del número de reglas.

- **Applications (Aplicaciones)**: nombre de las aplicaciones por orden alfabético. Si configura puertos o intervalos de puertos concretos para el servicio de una regla (el valor de Service [Servicio] no puede ser **any [cualquiera]**) y hay puertos estándar (application-default [valor predeterminado para la aplicación]) para la aplicación, pero los puertos configurados no coinciden con los puertos predeterminados para la aplicación, aparece un triángulo amarillo de advertencia junto a la aplicación.
- **Subcategory (Subcategoría)**: categoría secundaria de la aplicación por orden alfabético, que se obtiene de sus metadatos de contenido.
- **Risk (Riesgo)**: calificación de riesgo de la aplicación.
- **First Seen (Primera detección)**: primer día que se ha detectado la aplicación en la regla. La marca de tiempo solo incluye la fecha, no la hora.
- **Last Seen (Última detección)**: última día que se ha detectado la aplicación en la regla. La marca de tiempo solo incluye la fecha, no la hora.
- **Traffic (30 days) (Tráfico [30 días])**: tráfico en bytes que coincide con la regla en los 30 últimos días; es el método de ordenación predeterminado.

Para ver las estadísticas de un espacio de tiempo concreto, selecciónelo en **Timeframe (Período)**: **Anytime (Cualquiera)**, **Past 7 days (7 últimos días)**, **Past 15 days (15 últimos días)** o **Past 30 days (30 últimos días)**.

En Traffic (30 days) (Tráfico [30 días]), solo se muestran los 30 últimos días de tráfico en bytes siempre. Aunque cambie el valor de Timeframe (Período), no varía la duración de los bytes medidos en Traffic (30 days) (Tráfico [30 días]).

© 2020 Palo Alto Networks, Inc.

La visualización se ordena al hacer clic en el encabezado de una columna, y el orden se invierte al hacer clic en él de nuevo. Por ejemplo, haga clic en **Risk (Riesgo)** para ordenar las aplicaciones de menor a mayor riesgo. Vuelva a hacer clic en **Risk (Riesgo)** para ordenarlas de mayor a menor riesgo.

El cortafuegos no muestra las estadísticas en tiempo real sobre el uso de las aplicaciones en **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)**, en **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **Unused Apps (Aplicaciones no usadas)** ni en **Applications & Usage (Aplicaciones y uso)**. Por lo tanto, esta función no sustituye la ejecución de informes.

- El cortafuegos actualiza los valores de **Apps Allowed (Aplicaciones permitidas)** y de **Apps Seen (Aplicaciones detectadas)** y las aplicaciones enumeradas en **Applications & Usage (Aplicaciones y uso)** cada hora aproximadamente, no en tiempo real, aunque puede ser más tiempo si existen numerosas reglas o una gran cantidad de tráfico. Cuando añada una aplicación a una regla, espere al menos una hora antes de ejecutar los logs de tráfico para ver su información.

  El cortafuegos actualiza **Apps Seen (Aplicaciones detectadas)** cada hora más o menos, aunque puede ser más tiempo si existen numerosas reglas o un gran volumen de tráfico de aplicaciones. Cuando añada una aplicación a una regla, espere al menos una hora antes de ejecutar los logs de tráfico para ver su información.
- El cortafuegos actualiza **Days with No New Apps (Días sin aplicaciones nuevas)**, así como los valores de **First Seen (Primera detección)** y **Last Seen (Última detección)** en **Applications & Usage (Aplicaciones y uso)**, una vez al día, a medianoche según la hora del dispositivo.
- En el caso de las reglas donde se han detectado numerosas aplicaciones, se puede tardar más en procesar las estadísticas sobre el uso de las aplicaciones.
- En el caso de las bases de reglas de la política de seguridad que tengan numerosas reglas con muchas aplicaciones, se puede tardar más en procesar las estadísticas sobre el uso de las aplicaciones.
- En el caso de los cortafuegos que gestiona Panorama, solo se ven los datos sobre el uso de las aplicaciones correspondientes a las reglas que envía Panorama a los cortafuegos, no a las reglas configuradas de forma local en cortafuegos concretos.

Borrado de los datos sobre el uso de las aplicaciones

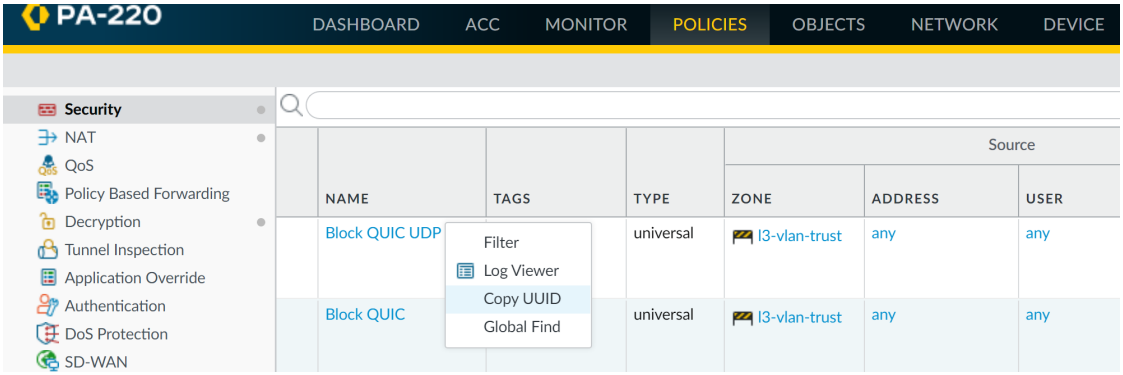
Puede usar un comando de la CLI para borrar los datos sobre el uso de las aplicaciones de reglas concretas de la política de seguridad y restablecer el valor de **Apps Seen (Aplicaciones detectadas)** junto con el de otros datos de uso.

STEP 1 | Busque el UUID de la regla de la política de seguridad cuyos datos sobre el uso de las aplicaciones desea borrar.

Hay dos formas de localizar el UUID en la IU:

- En **Policies (Políticas)** > **Security (Seguridad)**, copie el UUID de la columna **Rule UUID (UUID de regla)**.
- En **Policies (Políticas)** > **Security (Seguridad)**, seleccione **Copy UUID (Copiar UUID)** en el menú desplegable **Name (Nombre)** correspondiente a la regla.

© 2020 Palo Alto Networks, Inc.



STEP 2 | Cambie de la IU a la CLI.

Utilice el UUID obtenido en la IU para borrar los datos sobre el uso de las aplicaciones de la regla:

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <valor-uuid>
```

Pegue o escriba el UUID de la regla como valor y ejecute el comando para borrar sus datos sobre el uso de las aplicaciones.

Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID

Cuando cambia un cortafuegos antiguo por un cortafuegos de nueva generación de Palo Alto Networks, se heredan numerosas reglas basadas en puertos que permiten en ellos todas las aplicaciones. Eso aumenta la superficie de ataque, ya que cualquier aplicación puede utilizar un puerto abierto. La función Policy Optimizer (Optimizador de políticas) identifica todas las aplicaciones detectadas en las reglas basadas en puertos heredadas de la política de seguridad y proporciona un flujo de trabajo sencillo para seleccionar las aplicaciones que desea permitir en cada regla. Migre las reglas basadas en puertos a reglas basadas en aplicaciones para reducir la superficie de ataque y habilitar las aplicaciones de forma segura en la red. Sírvase del optimizador para mantener la base de reglas a medida que añade aplicaciones nuevas.

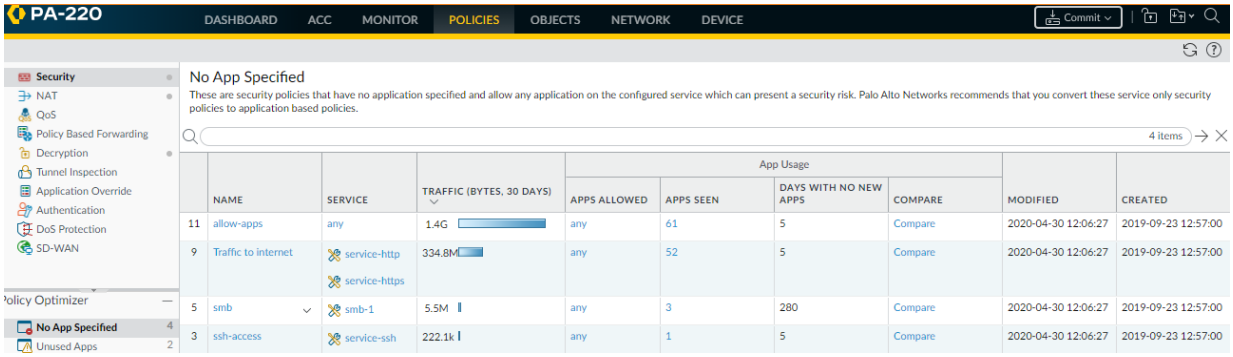
Migre unas cuantas reglas basadas en puertos a otras basadas en aplicaciones cada vez por orden de prioridad. Es más seguro realizar una conversión gradual que migrar una base de reglas grande de una sola vez; también hace que sea más fácil asegurarse de que las reglas nuevas controlan las aplicaciones necesarias. Use Policy Optimizer (Optimizador de políticas) para priorizar las reglas que se convierten en primer lugar.

Para migrar la configuración de un cortafuegos heredado a un dispositivo de Palo Alto Networks, consulte Prácticas recomendadas para realizar la migración a políticas basadas en aplicaciones.

STEP 1 | Identifique las reglas basadas en puertos.

Las reglas basadas en puertos no tienen aplicaciones configuradas (permitidas). **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)** muestra todas las reglas basadas en puertos (**Apps Allowed [Aplicaciones permitidas]** es **any [cualquiera]**).

© 2020 Palo Alto Networks, Inc.



STEP 2 | Priorice las reglas basadas en puertos que se deben convertir en primer lugar.

Policies (Políticas) > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)** permite ordenar las reglas sin alterar su orden en la base de reglas y aporta otra información útil para priorizar su conversión en función de los objetivos comerciales y la tolerancia al riesgo.

- **Traffic (Bytes, 30 days) (Tráfico [bytes, 30 días])**: haga clic para ordenar los datos por esta columna. Las reglas que tienen más tráfico *en ese momento* se sitúan al principio de la lista. Es el orden predeterminado.
- **Apps Seen (Aplicaciones detectadas)**: haga clic para ordenar los datos por esta columna. Si coinciden con una regla basada en puertos numerosas aplicaciones legítimas, es conveniente sustituirla por varias reglas basadas en aplicaciones que definan de forma estricta las aplicaciones, los usuarios, los orígenes y los destinos. Por ejemplo, si una regla basada en puertos controla el tráfico de varias aplicaciones de distintos grupos de usuarios en conjuntos de dispositivos diferentes, cree reglas independientes que emparejen las aplicaciones con los usuarios y los dispositivos legítimos para reducir la superficie de ataque y aumentar la visibilidad. Si hace clic en el número de **Apps Seen (Aplicaciones detectadas)** o en **Compare (Comparar)**, se muestran las aplicaciones que han coincidido con la regla.

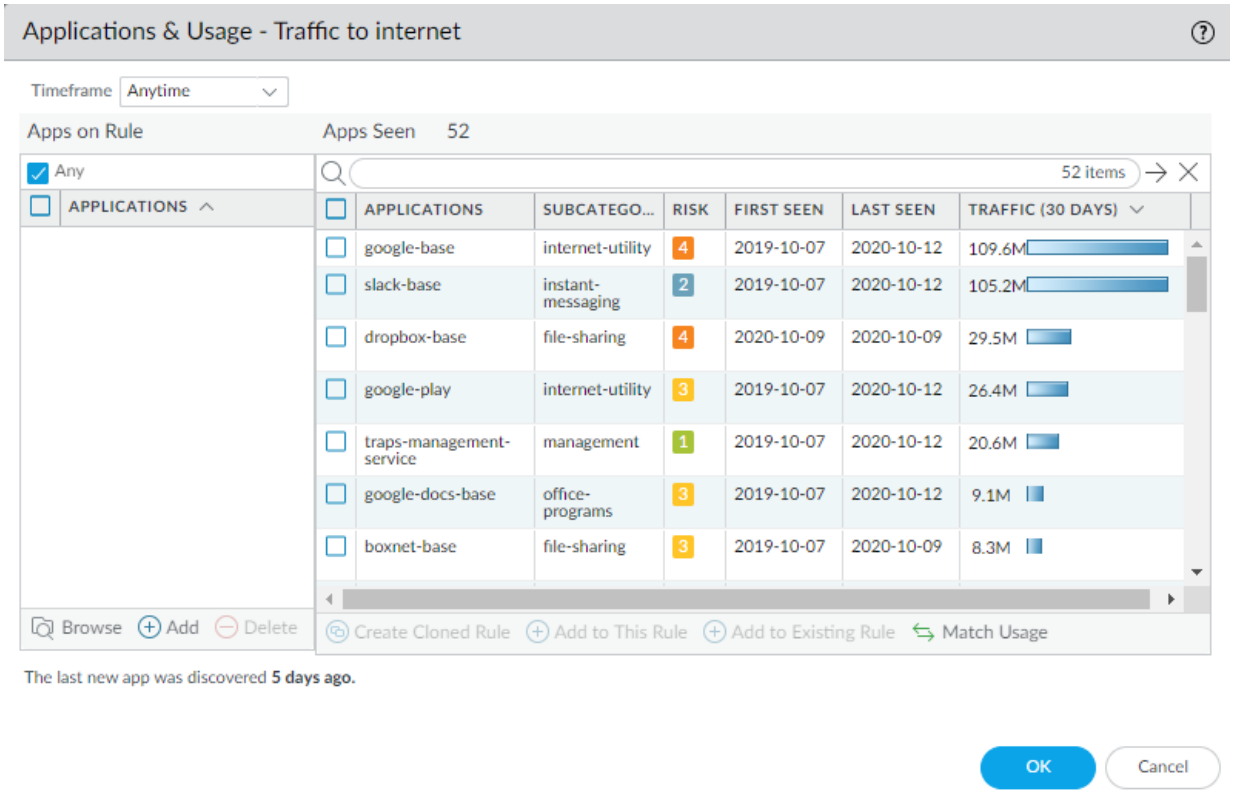
  El cortafuegos actualiza Apps Seen (Aplicaciones detectadas) cada hora más o menos, aunque puede ser más tiempo si existen numerosas reglas o un gran volumen de tráfico de aplicaciones. Cuando añada una aplicación a una regla, espere al menos una hora antes de ejecutar los logs de tráfico para ver su información.
- **Days with No New Apps (Días sin aplicaciones nuevas)**: haga clic para ordenar los datos por esta columna. Cuando se estabilizan las aplicaciones detectadas en una regla basada en puertos, puede tener más confianza en que es sólida, en que la conversión no excluirá por accidente aplicaciones legítimas y en que no coincidirá con ella ninguna aplicación más. Las datas de **Created (Fecha de creación)** y de **Modified (Fecha de modificación)** resultan útiles para evaluar la estabilidad de las reglas, ya que también suelen parecer más estables las más antiguas que no se han modificado de forma reciente.
- **Hit Count (Recuento de resultados)**: muestra las reglas que han tenido más coincidencias en el período seleccionado. Puede excluir las reglas en las que haya restablecido el contador de resultados y especificar el período de exclusión en días. Si excluye las reglas cuyos contadores se hayan restablecido recientemente, evita malas interpretaciones sobre las reglas que muestran menos resultados de los esperados porque desconocía ese hecho.

  Hit Count (Recuento de resultados) también permite ver el uso (consulte Visualización de la utilización de las reglas de la política), así como identificar y eliminar las reglas que no se utilizan a fin de reducir los riesgos para la seguridad y mantener organizada la base de reglas.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Revise el número de **Apps Seen (Aplicaciones detectadas)** en las reglas basadas en puertos, empezando por las de mayor prioridad.

En **No Apps Specified (Ninguna aplicación especificada)**, haga clic en **Compare (Comparar)** o en el número de **Apps Seen (Aplicaciones detectadas)** para abrir **Applications & Usage (Aplicaciones y uso)**. En esta pantalla, se enumeran las aplicaciones que han coincidido en la regla basada en puertos oportuna durante el intervalo especificado en **Timeframe (Período)**, con el valor de **Risk (Riesgo)** y las fechas de **First Seen (Primera detección)** y **Last Seen (Última detección)** correspondientes a cada aplicación, así como la cantidad de tráfico registrada en los 30 últimos días.



Puede consultar las **aplicaciones detectadas** en las reglas basadas en puertos en los 7, los 15 o los 30 últimos días o bien desde que están vigentes (**Anytime [Cualquiera]**). A la hora de migrar las reglas, **Anytime (Cualquiera)** ofrece la evaluación más completa de aplicaciones que han coincidido con ellas.

Puede filtrar **Apps Seen (Aplicaciones detectadas)** y buscar aplicaciones en este cuadro, pero tenga en cuenta que tarda una hora o más en actualizarse. También puede ordenar los valores de **Apps Seen (Aplicaciones detectadas)** haciendo clic en el encabezado de las columnas. Por ejemplo, si hace clic en **Traffic (30 days) (Tráfico [30 días])**, ocupan el principio de la lista las aplicaciones que tengan el tráfico más reciente o, si hace clic en **Subcategory (Subcategoría)**, las aplicaciones se organizan según su categoría secundaria.

Los datos de First Seen (Primera detección) y Last Seen (Última detección) corresponden a un día. Por eso, el día que define una regla, ambas columnas tienen la misma fecha, la cual cambia el segundo día que el cortafuegos detecte tráfico en una aplicación.

STEP 4 | Clone la regla o añádale aplicaciones para especificar cuáles desea permitir en ella.

En **Applications & Usage (Aplicaciones y uso)**, convierta una regla basada en puertos en otra basada en aplicaciones con alguno de estos métodos:

© 2020 Palo Alto Networks, Inc.

- **Clone the rule (Clonar la regla)**: conserva la regla basada en puertos original y coloca la regla basada en aplicaciones clonada directamente por encima de ella en la base de reglas.
- **Add Applications to the Rule (Añadir aplicaciones a la regla)**: sustituye la regla basada en puertos por la regla basada en aplicaciones nueva y elimina la original.

Si tiene reglas basadas en aplicaciones existentes y desea migrar aplicaciones a ellas desde reglas basadas en puertos, puede Adición de aplicaciones a reglas existentes en lugar de clonar una nueva regla o convertir la regla basada en puertos añadiéndole aplicaciones.

Algunas aplicaciones aparecen en la red a intervalos, por ejemplo, en eventos trimestrales o anuales. Es posible que esas aplicaciones no se muestren en la pantalla Applications & Usage (Aplicaciones y uso) si el historial no recoge tanto tiempo como para capturar su última actividad.

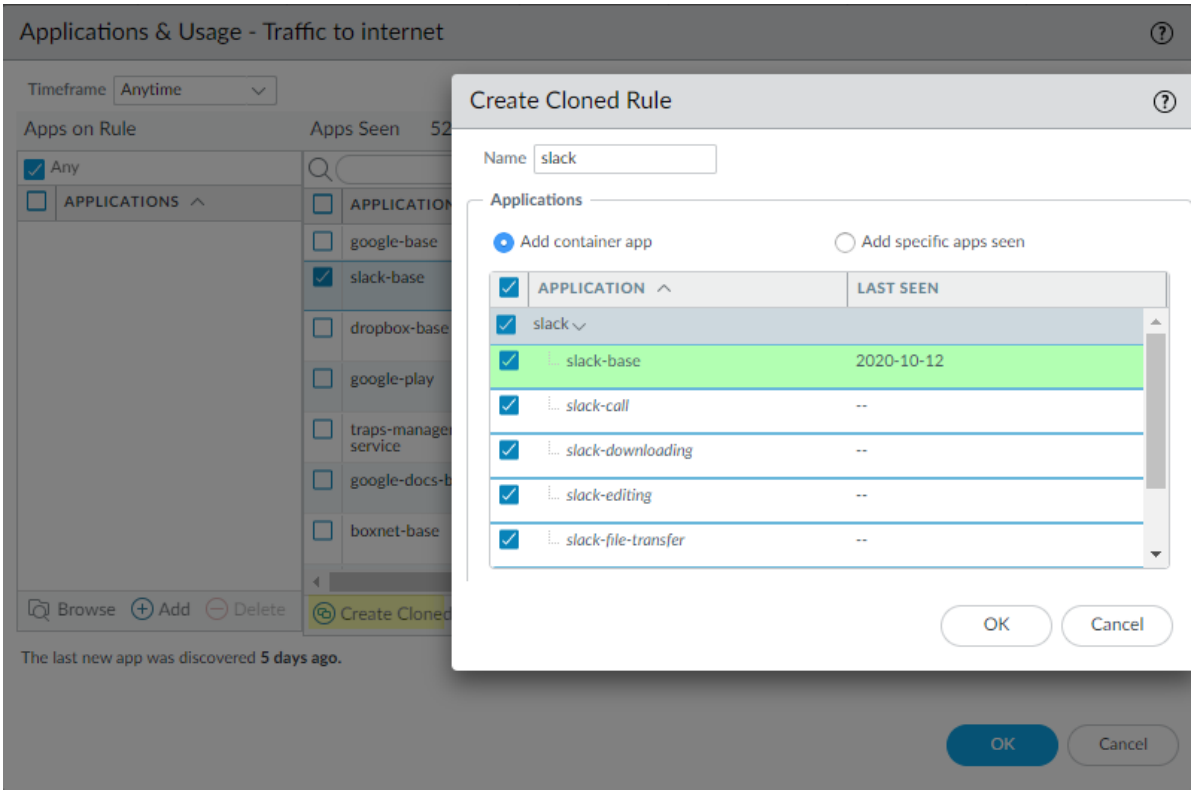
Cuando clona una regla o le añade aplicaciones, no cambia nada en la original. La configuración de la regla original permanece igual, salvo por las aplicaciones que le añada. Por ejemplo, si indica any (cualquiera) en Service (Servicio) o especifica un servicio concreto en la regla original, debe cambiar el valor a application-default (valor predeterminado para la aplicación) para restringir el uso de las aplicaciones permitidas a los puertos predeterminados en la nueva regla.

La clonación es el método más seguro para migrar las reglas, sobre todo cuando, en **Applications & Usage (Aplicaciones y uso)**, figuran bastantes aplicaciones conocidas que coinciden con ellas (consulte un ejemplo en Caso de uso de migración mediante la clonación de reglas: navegación web y tráfico SSL). Con la clonación, se conserva la regla basada en puertos original, que se coloca por debajo de la regla basada en aplicaciones clonada. De ese modo, se elimina el riesgo de que las aplicaciones dejen de estar disponibles, puesto el tráfico que no coincida con la regla clonada pasa por la regla de puertos. Cuando el tráfico de aplicaciones legítimas lleve un tiempo razonable sin coincidir con la regla basada en puertos, puede eliminarla para completar la migración.

Para **clonar** una regla basada en puertos:

1. En **Apps Seen (Aplicaciones detectadas)**, marque la casilla de verificación que hay junto a cada una de las aplicaciones que desea incluir en la regla clonada. Tenga en cuenta que **Apps Seen (Aplicaciones detectadas)** tarda una hora o más en actualizarse.
2. Haga clic en **Create Cloned Rule (Crear regla clonada)**. En el cuadro de diálogo **Create Cloned Rule (Crear regla clonada)**, indique el nombre de la regla clonada en **Name (Nombre)** (slack en este ejemplo) y, si procede, añada otras aplicaciones del mismo contenedor y las dependencias oportunas. Por ejemplo, para clonar una regla seleccionando la aplicación slack-base:

© 2020 Palo Alto Networks, Inc.



El texto resaltado en verde es la aplicación seleccionada para la clonación. La aplicación de contenedor (**slack**) aparece en la fila de color gris. Las aplicaciones en *cursiva* son aplicaciones que no se han detectado en la regla, pero pertenecen al mismo contenedor que la aplicación seleccionada. Las demás aplicaciones que se han detectado en la regla aparecen con la fuente normal. En la regla clonada se incluyen todas las aplicaciones de forma predeterminada: la opción predeterminada seleccionada es **Add container app (Añadir aplicación de contenedor)**, que añade todas las aplicaciones del contenedor. Así se evita que la regla se rompa en el futuro.

3. Si desea permitir todas las aplicaciones del contenedor, deje seleccionada la opción **Add container app (Añadir aplicación de contenedor)**. De este modo, la regla está preparada para cualquier contingencia, ya que se le añade automáticamente cualquier aplicación que se añada a la aplicación de contenedor.

   Si desea limitar el acceso de los usuarios a algunas aplicaciones del contenedor, quite la marca de su casilla. Al hacerlo, también se quita la selección de la aplicación de contenedor, de manera que, si quiere permitir otras aplicaciones en el contenedor más adelante, debe añadirlas una a una.

   Al quitar la marca de la aplicación de contenedor, también se quita de todas las aplicaciones, así que debe marcar manualmente las que desea incluir en la regla clonada.
4. Si las dependencias de la aplicación se muestran en un cuadro debajo de Applications (Aplicaciones) (no hay ninguna en este ejemplo), déjelas marcadas. Las aplicaciones que seleccionó necesitan esas dependencias de aplicaciones para ejecutarse. Las dependencias comunes incluyen **ssl** y **navegación web**.
5. Haga clic en **OK (Aceptar)** para añadir la nueva regla basadas en aplicaciones directamente por encima de la regla basada en puertos en la base de reglas.
6. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Cuando clona una regla y hace clic en **Commit (Confirmar)** para aceptar la configuración, las aplicaciones seleccionadas para la regla clonada se elimina de la lista **Apps Seen (Aplicaciones detectadas)** de la regla basada en puertos original. Por ejemplo, si una regla basada en puertos tiene 16 aplicaciones en **Apps Seen (Aplicaciones detectadas)** y selecciona 2 aplicaciones individuales y 1 aplicación dependiente para

© 2020 Palo Alto Networks, Inc.

la regla clonada, después de la clonación, la regla basada en puertos muestra 13 aplicaciones en **Apps Seen (Aplicaciones detectadas)** porque las 3 aplicaciones seleccionadas se eliminan de la regla basada en puertos (16 - 3 = 13). La regla clonada muestra las 3 aplicaciones añadidas en **Apps on Rule (Aplicaciones de regla)**.

La creación de una regla clonada con una aplicación de contenedor es algo diferente. Por ejemplo, una regla basada en puertos tiene 16 aplicaciones en **Apps Seen (Aplicaciones detectadas)** y selecciona 1 aplicación individual y 1 aplicación de contenedor para la regla clonada. La aplicación de contenedor tiene 5 aplicaciones individuales y 1 aplicación dependiente. Después de la clonación, la regla clonada muestra 7 aplicaciones en **Apps on Rule (Aplicaciones de regla)**: la aplicación individual, las 5 aplicaciones individuales de la aplicación de contenedor y la aplicación dependiente de la aplicación de contenedor. Sin embargo, la regla basada en puertos original muestra 13 aplicaciones en **Apps Seen (Aplicaciones detectadas)** porque solo se eliminan de ella la aplicación individual, la aplicación de contenedor y la aplicación dependiente de la aplicación de contenedor.

A diferencia de lo que ocurre con la clonación, si se añaden aplicaciones a una regla basada en puertos, esta se sustituye por la regla basada en aplicaciones resultante. Aunque es más fácil añadir aplicaciones a una regla que clonar esta, también entraña más riesgos porque, sin querer, puede pasar por alto aplicaciones que deben estar presentes en la regla, y la regla basada en puertos original deja de estar en la base de reglas para capturar posibles omisiones accidentales. No obstante, si añade aplicaciones a reglas basadas en puertos que se aplican solo a unas cuantas aplicaciones conocidas, se agiliza la migración a reglas basadas en aplicaciones. Por ejemplo, la única aplicación legítima de una regla basada en puertos que solo controla el tráfico al puerto TCP 22 es SSH, así que es seguro añadir aplicaciones a la regla.

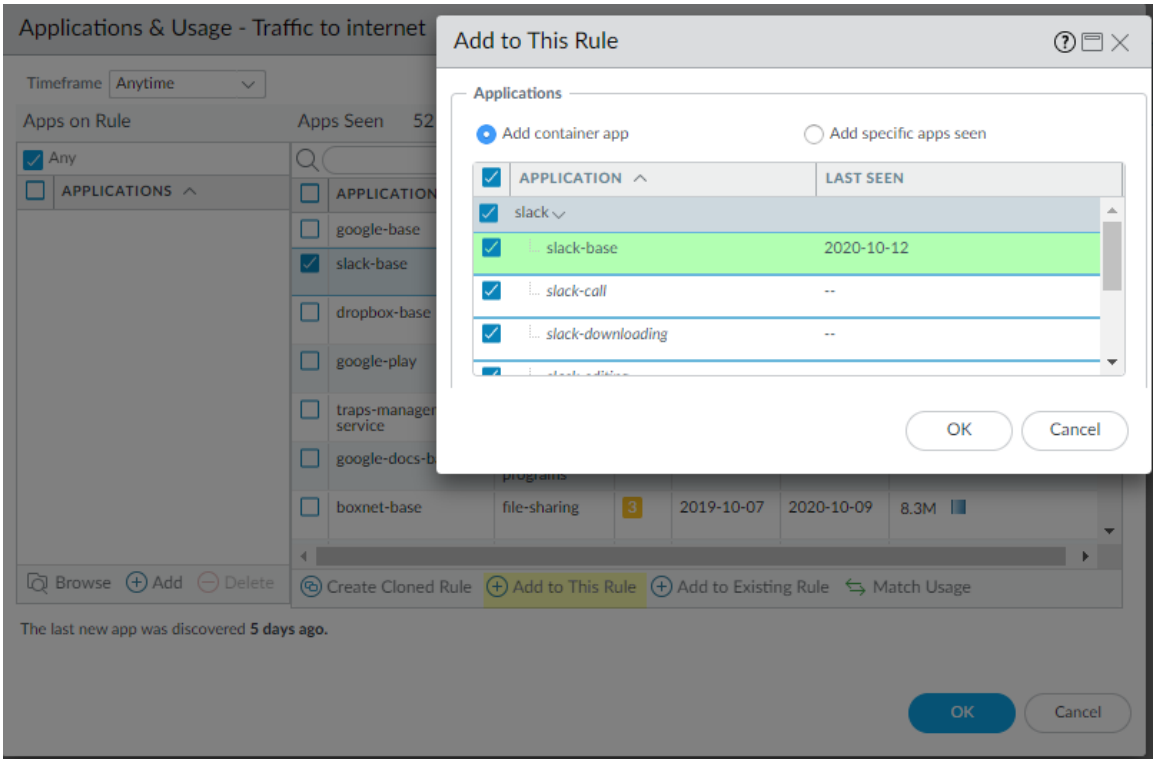


Si añade aplicaciones con la opción tradicional de la pestaña Application (Aplicación) de la regla de la política de seguridad, no cambian los valores de Apps Seen (Aplicaciones detectadas) ni de Apps on Rule (Aplicaciones de regla). Para que la información sobre el uso de las aplicaciones siga siendo precisa, cuando sustituya las reglas basadas en puertos por otras basadas en aplicaciones, añada estas con las opciones Add to This Rule (Añadir a esta regla) o Match Usage (Comprobar uso) de Apps Seen (Aplicaciones detectadas); si no, cree una regla clonada o añada aplicaciones a una regla basada en aplicaciones existentes.

Hay tres formas de sustituir reglas basadas en puertos por otras basadas en aplicaciones añadiendo aplicaciones: **Add to This Rule (Añadir a esta regla)** y **Match Usage (Comprobar uso)** en **Apps Seen (Aplicaciones detectadas)** y **Add (Añadir)** en **Apps on Rule (Aplicaciones de regla)**:

- Con **Add to This Rule (Añadir a esta regla)**, puede añadir aplicaciones de **Apps Seen (Aplicaciones detectadas)** que coinciden con la regla. Tenga en cuenta que **Apps Seen (Aplicaciones detectadas)** tarda una hora o más en actualizarse.
  1. Seleccione aplicaciones de la regla que figuran en **Apps Seen (Aplicaciones detectadas)**.
  2. Haga clic en **Add to This Rule (Añadir a esta regla)**. En el cuadro de diálogo **Add to This Rule (Añadir a esta regla)**, si procede, añada otras aplicaciones de la misma aplicación de contenedor y las dependencias oportunas. Por ejemplo, para añadir slack-base a una regla:

© 2020 Palo Alto Networks, Inc.



Al igual que en el cuadro de diálogo **Create Cloned Rule (Crear regla clonada)**, el texto resaltado en verde de **Add to This Rule (Añadir a esta regla)** es la aplicación seleccionada para añadirla a la regla. La aplicación de contenedor (**slack**) aparece en la fila de color gris. Las aplicaciones en *cursiva* son aplicaciones que no se han detectado en la regla, pero pertenecen al mismo contenedor que la aplicación seleccionada. Las demás aplicaciones que se han detectado en la regla aparecen con la fuente normal. En la regla clonada se incluyen todas las aplicaciones de forma predeterminada: la opción predeterminada seleccionada es **Add container app (Añadir aplicación de contenedor)**, que añade todas las aplicaciones del contenedor. Así se evita que la regla se rompa en el futuro.

3. Si desea permitir todas las aplicaciones del contenedor, deje seleccionada la opción **Add container app (Añadir aplicación de contenedor)**. De este modo, la regla está preparada para cualquier contingencia, ya que se le añade automáticamente cualquier aplicación que se añada a la aplicación de contenedor.

   Si desea limitar el acceso de los usuarios a algunas aplicaciones del contenedor, quite la marca de su casilla. Al hacerlo, también se quita la selección de la aplicación de contenedor, de manera que, si quiere permitir otras aplicaciones en el contenedor más adelante, debe añadirlas una a una.

   Al quitar la marca de la aplicación de contenedor, también se quita de todas las aplicaciones, así que debe marcar manualmente las que desea incluir en la regla clonada.
4. Si las dependencias de la aplicación se muestran en un cuadro debajo de Applications (Aplicaciones) (no hay ninguna en este ejemplo), déjelas marcadas. Las aplicaciones que seleccionó necesitan esas dependencias de aplicaciones para ejecutarse.
5. Haga clic en **OK (Aceptar)** para sustituir la regla basada en puertos por la nueva regla basada en aplicaciones.

Cuando rellena **Add to This Rule (Añadir a esta regla)** y hace clic en **Commit (Confirmar)** para aceptar la configuración, las aplicaciones que no ha añadido se eliminan de la lista **Apps Seen (Aplicaciones detectadas)** porque la nueva regla basada en aplicaciones ya no las permite. Por ejemplo, si una regla tiene 16 aplicaciones en **Apps Seen (Aplicaciones detectadas)** y añade 3 aplicaciones con **Add to**

© 2020 Palo Alto Networks, Inc.

This Rule (Añadir a esta regla), la nueva regla resultante solo muestra esas 3 aplicaciones añadidas en **Apps Seen (Aplicaciones detectadas)**.

El funcionamiento de **Add to This Rule (Añadir a esta regla)** con una aplicación de contenedor es algo diferente. Por ejemplo, una regla basada en puertos tiene 16 aplicaciones en **Apps Seen (Aplicaciones detectadas)** y selecciona 1 aplicación individual y 1 aplicación de contenedor para añadir a la regla nueva. La aplicación de contenedor tiene 5 aplicaciones individuales y 1 aplicación dependiente. Después de añadir las aplicaciones a la regla, la regla nueva muestra 7 aplicaciones en **Apps on Rule (Aplicaciones de regla)**: la aplicación individual, las 5 aplicaciones individuales de la aplicación de contenedor y la aplicación dependiente de la aplicación de contenedor. Sin embargo, se muestran 13 aplicaciones en **Apps Seen (Aplicaciones detectadas)** porque se eliminan de esa lista la aplicación individual, la aplicación de contenedor y la aplicación dependiente de la aplicación de contenedor.

- Añada todas las aplicaciones de la regla que figuran en **Apps Seen (Aplicaciones detectadas)** a la regla nueva de una vez con un solo clic en **Match Usage (Comprobar uso)**.

  Como las reglas basadas en puertos permiten cualquier aplicación, puede haber aplicaciones innecesarias o poco seguras en Apps Seen (Aplicaciones detectadas). Emplee Match Usage (Comprobar uso) para convertir únicamente las reglas que tengan un número reducido de aplicaciones conocidas con fines comerciales legítimos. Un buen ejemplo es el puerto TCP 22, que solo permite tráfico SSH. Si SSH es la única aplicación que se detecta en una regla basada en puertos que abre el puerto 22, no hay inconveniente en usar Match Usage (Comprobar uso).

  1. En **Apps Seen (Aplicaciones detectadas)**, haga clic en **Match Usage (Comprobar uso)**. Tenga en cuenta que **Apps Seen (Aplicaciones detectadas)** tarda una hora o más en actualizarse. Todas las aplicaciones que figuran en **Apps Seen (Aplicaciones detectadas** se copian en **Apps on Rule (Aplicaciones de regla)**.
  2. Haga clic en **OK (Aceptar)** para crear la regla basada en aplicaciones y sustituir la regla basada en puertos.
- Si sabe qué aplicaciones desea incluir en la regla, haga clic en la opción **Add (Añadir)** de **Apps on Rule (Aplicaciones de regla)** para añadirlas manualmente. No obstante, este método es equivalente al de la opción tradicional de la pestaña **Application (Aplicación)** de la regla de la política de seguridad, que no cambia los valores de **Apps Seen (Aplicaciones detectadas)** ni de **Apps on Rule (Aplicaciones de regla)**. Para que la información sobre el uso de las aplicaciones siga siendo precisa, convierta las reglas con las opciones **Add to This Rule (Añadir a esta regla)**, **Create Cloned Rule (Crear regla clonada)** o **Match Usage (Comprobar uso)** de **Apps Seen (Aplicaciones detectadas)**.

  1. En **Apps on Rule (Aplicaciones de regla)**, haga clic en **Add (Añadir)** o en **Browse (Examinar)** y seleccione las aplicaciones que se deben añadir a la regla. Es el método equivalente a añadir aplicaciones en la pestaña **Application (Aplicación)**.
  2. Haga clic en **OK (Aceptar)** para añadir las aplicaciones a la regla y sustituir la regla basada en puertos por la nueva regla basada en aplicaciones.

     Como este método es equivalente a añadir aplicaciones en la pestaña Application (Aplicación), no aparece el cuadro de diálogo para añadir dependencias de las aplicaciones.

STEP 5 | En cada una de las reglas basadas en aplicaciones, configure **Service (Servicio)** en **application-default (valor predeterminado para la aplicación)**.

Si debe permitir ciertas aplicaciones (como aplicaciones internas personalizadas) en puertos no estándar entre clientes y servidores concretos por motivos empresariales, restrinja la excepción exclusivamente a la aplicación, los orígenes y los destinos que sean indispensables. Conviene que reescriba las aplicaciones personalizadas para que utilicen el puerto predeterminado.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 7 | Supervise las reglas.

- **Reglas clonadas**: supervise la regla basada en puertos original para asegurarse de que la regla basada en aplicaciones coincide con el tráfico deseado. Si las aplicaciones que desea permitir coinciden con la regla basada en puertos, añádalas a la regla basada en aplicaciones o clone otra regla basada en aplicaciones que las incluya. Cuando solo coinciden con la regla basada en puertos aplicaciones que no desea en la red durante un tiempo razonable, significa que la regla nueva es sólida (es decir, captura todo el tráfico de aplicaciones que desea controlar), así que puede eliminar la antigua.
- **Reglas con aplicaciones añadidas**: como solo convierte reglas basadas en puertos que tienen unas pocas aplicaciones conocidas directamente a reglas basadas en aplicaciones, estas son sólidas desde el principio en la mayoría de los casos. Supervise las reglas convertidas para comprobar si coincide con ellas el tráfico esperado. Si hay menos tráfico del previsto, es posible que no permitan todas las aplicaciones necesarias. Si hay más tráfico del previsto, es posible que permitan tráfico no deseado. Solicite información a los usuarios: si no pueden acceder a aplicaciones que necesitan para su trabajo, es posible que alguna regla sea demasiado estricta.

Caso de uso de migración mediante la clonación de reglas: navegación web y tráfico SSL

Si una regla basada en puertos permite el acceso web en los puertos TCP 80 (navegación web por HTTP) y 443 (SSL por HTTPS), no ejerce ningún control sobre las aplicaciones que usan esos puertos abiertos. Hay tantas aplicaciones web que una regla general que permita el tráfico web admite miles de aplicaciones, y es probable que no desee muchas de ellas en su red.

En este caso de uso se demuestra cómo migrar una política basada en puertos que permite todas las aplicaciones web a una política basada en aplicaciones que solo permita las aplicaciones que le interesen, de modo que pueda habilitarlas de forma segura. Cuando las reglas detectan infinidad de aplicaciones, resulta más seguro clonar la regla basada en puertos original que añadirle aplicaciones porque, con este procedimiento, se sustituye la regla original. En ese caso, si olvida añadir alguna aplicación esencial, perjudica su disponibilidad. Si utiliza **Match Usage (Comprobar uso)**, que también sustituye la regla basada en puertos, permite todas las aplicaciones que detecta, lo cual es peligroso, sobre todo con el tráfico de navegación web.

Si clona la regla, se conserva la regla basada en puertos original y se coloca la regla clonada directamente por encima de ella en la base de reglas para que pueda supervisarlas. La clonación también permite dividir las reglas que detectan muchas aplicaciones diferentes (como las basadas en puertos que regulan el tráfico web) en varias reglas basadas en aplicaciones para tratar de forma distinta cada grupo de aplicaciones. En cuanto se asegure de que están permitidas todas las aplicaciones necesarias en las reglas clonadas, puede eliminar las correspondientes reglas basadas en puertos.

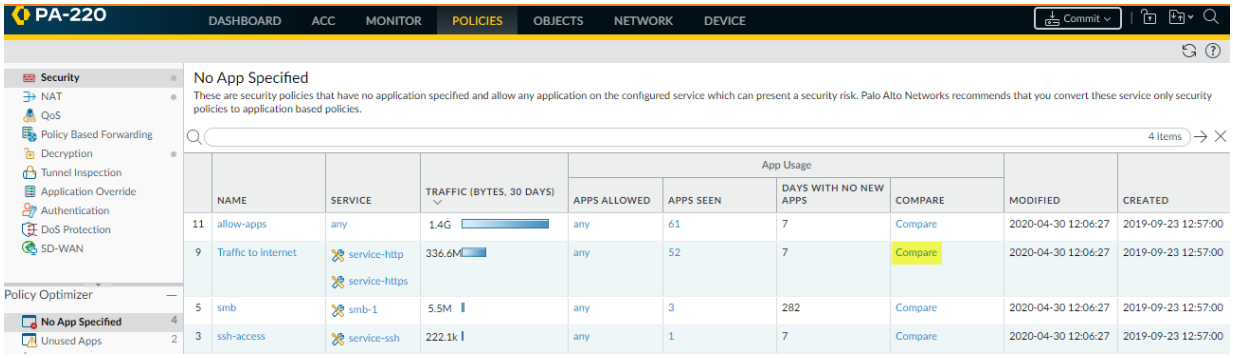
En este ejemplo se clona una regla basada en puertos para el tráfico web con el fin de crear una regla basada en aplicaciones para el tráfico de uso compartido de archivos basado en la web, que es un subconjunto del tráfico de aplicaciones detectado en la regla basada en puertos.

STEP 1 | Desplácese a **Policies (Políticas)** > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **No App Specified (Ninguna aplicación especificada)** para ver las reglas basadas en puertos.

STEP 2 | Haga clic en la opción **Compare (Comparar)** correspondiente a la regla que desea migrar.

En este ejemplo, la regla basadas en puertos que permite el acceso web se llama Traffic to internet (Tráfico a internet).

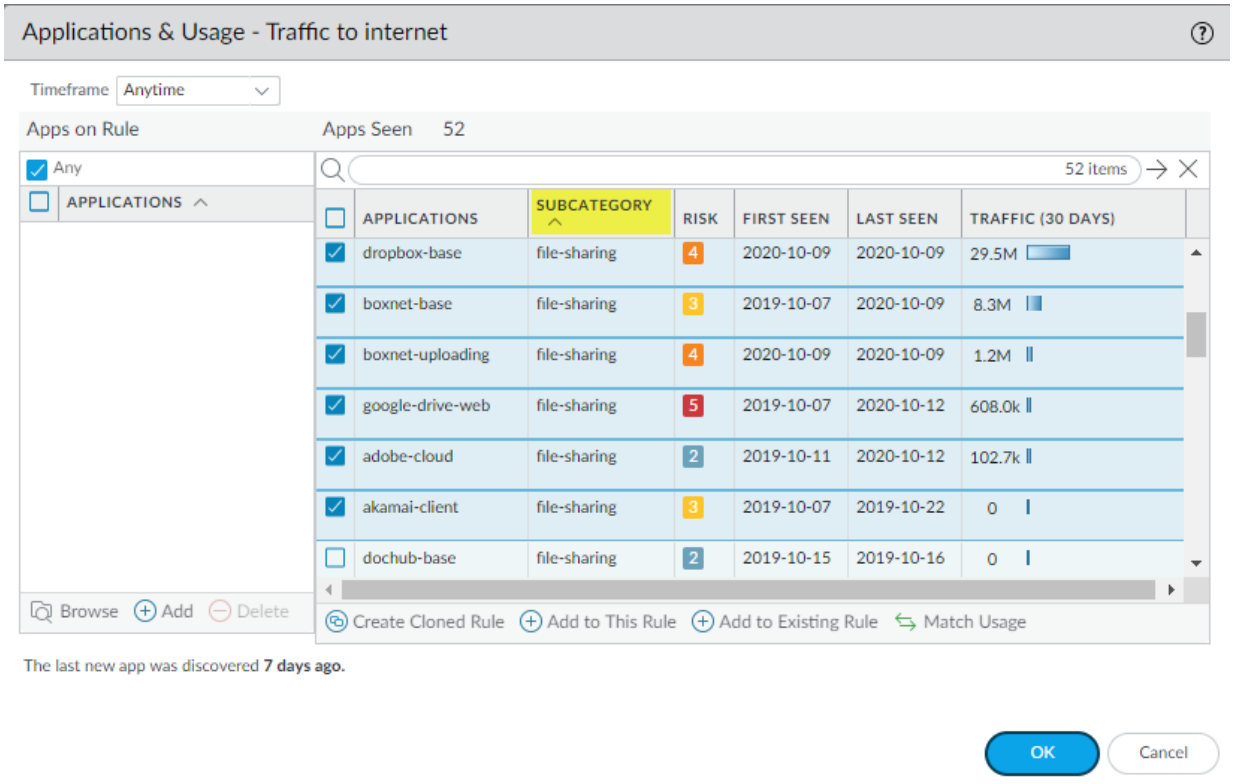
© 2020 Palo Alto Networks, Inc.



STEP 3 | Use las opciones de ordenación de **Apps Seen (Aplicaciones detectadas)** para revisar y seleccionar las aplicaciones que desea permitir.

El número de aplicaciones que aparecen en Apps Seen (Aplicaciones detectadas) se actualiza cada hora aproximadamente; si no ve tantas aplicaciones como esperaba, compruebe esta pantalla al cabo de una hora más o menos. Según la carga del cortafuegos, estos campos pueden tardar más tiempo en actualizarse.

Por ejemplo, haga clic en **Subcategory (Subcategoría)** para ordenar las aplicaciones, desplácese hasta la categoría secundaria de uso compartido de archivos y, entonces, seleccione las aplicaciones que desea permitir. También puede filtrar (buscar) aplicaciones para el uso compartido de archivos.

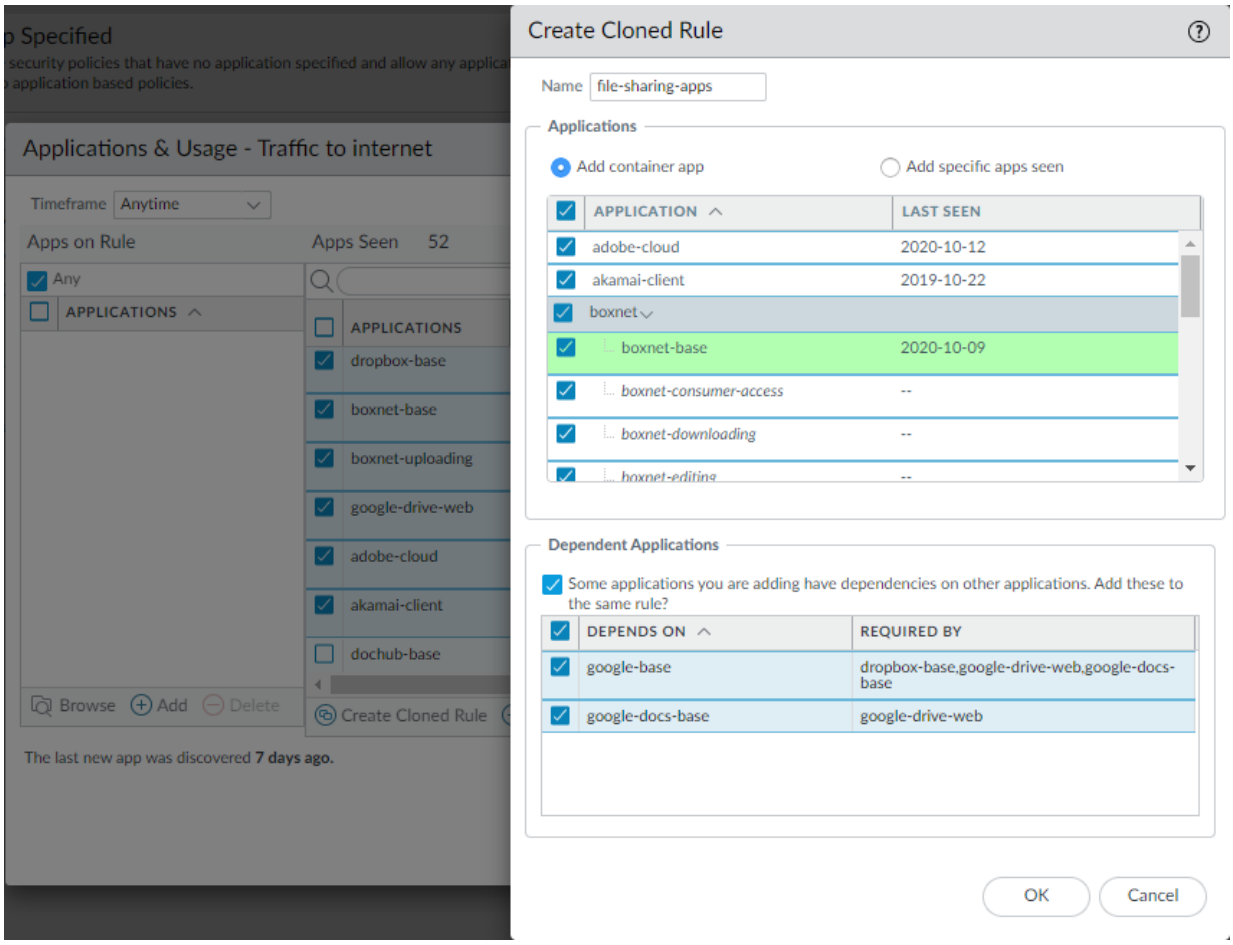


STEP 4 | Haga clic en **Create Cloned Rule (Crear regla clonada)** y **nombre** la regla clonada (aplicaciones para el uso compartido de archivos en este ejemplo).

En **Create Cloned Rule (Crear regla clonada)**, las aplicaciones seleccionadas están sombreadas en color verde, las aplicaciones de contenedor están sombreadas en color gris, las aplicaciones pertenecientes al

© 2020 Palo Alto Networks, Inc.

contenedor que no se han detectado en la regla aparecen en *cursiva* y las aplicaciones sueltas que se han detectado en la regla aparecen con la fuente de texto normal. Si se desplaza por **Application (Aplicación)**, se van mostrando todas las aplicaciones de contenedor, además de sus aplicaciones individuales.



Create Cloned Rule (Crear regla clonada) también muestra las aplicaciones dependientes para las aplicaciones seleccionadas. En este ejemplo, algunas de las aplicaciones seleccionadas requieren (**Required By [Requerido por]**) las aplicaciones google-base y google-docs-base para ejecutarse.

STEP 5 | Seleccione las aplicaciones que desea incluir en la regla clonada.

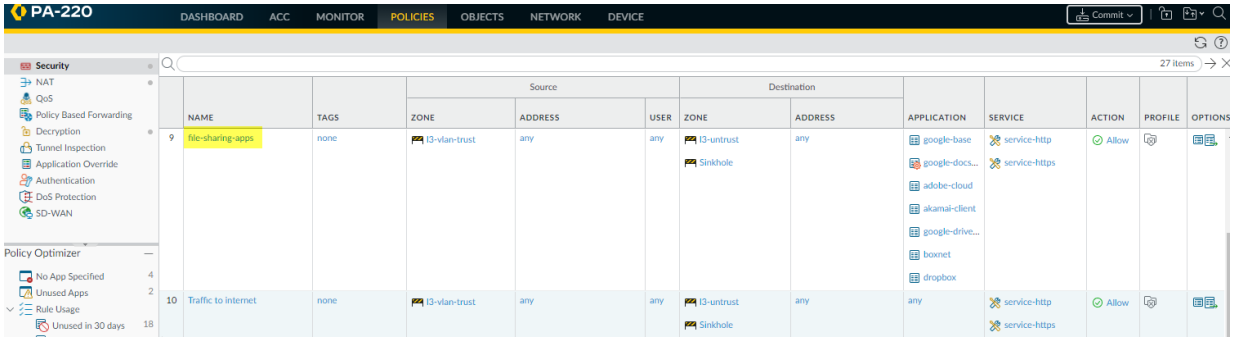
Si no quiere incluir algunas aplicaciones, quite la marca de su casilla. Al hacerlo, también se quita la marca de la aplicación de contenedor. Si no incluye la aplicación de contenedor, las aplicaciones nuevas que se añadan al contenedor no se añadirán automáticamente a la regla.

Si quita la marca de la aplicación de contenedor, también se quita de todas las aplicaciones sueltas del contenedor, por lo que debe seleccionar manualmente las aplicaciones que desea añadir.

STEP 6 | Haga clic en **OK (Aceptar)** para crean la regla clonada.

STEP 7 | En **Policies (Políticas)** > **Security (Seguridad)**, la regla clonada (file-sharing-apps [aplicaciones de uso compartido de archivos]) se inserta en la base de reglas por encima de la regla basada en puertos original (Traffic to internet [Tráfico a internet]).

© 2020 Palo Alto Networks, Inc.



STEP 8 | Haga clic en el nombre si desea editar la regla clonada, que hereda las propiedades de la regla basada en puertos original.

STEP 9 | En la pestaña **Service/URL Category (Servicio/Categoría de URL)**, elimine service-http (servicio HTTP) y service-https (servicio HTTPS) de **Service (Servicio)**.

Al hacerlo, **Service (Servicio)** cambia a **application-default (valor predeterminado para la aplicación)**: este valor impide que las aplicaciones utilicen puertos que no sean los estándar y reduce aún más la superficie de ataque.

Si debe permitir ciertas aplicaciones (como aplicaciones internas personalizadas) en puertos no estándar entre clientes y servidores concretos por motivos empresariales, restrinja la excepción exclusivamente a la aplicación, los orígenes y los destinos que sean indispensables. Conviene que reescriba las aplicaciones personalizadas para que utilicen el puerto predeterminado.

STEP 10 | En las pestañas **Source (Origen)**, **User (Usuario)** y **Destination (Destino)**, endurezca la regla para que solo se aplique a los usuarios correctos en las ubicaciones (zonas y subredes) adecuadas.

Por ejemplo, puede decidir limitar la actividad de uso compartido de archivos web solo a los grupos de usuarios que tengan motivos empresariales para compartir archivos en la web.

STEP 11 | Haga clic en **OK (Aceptar)**.

STEP 12 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 13 | Repita este procedimiento con otras categorías de aplicaciones de la regla basada en puertos para el acceso web hasta que las reglas basadas en aplicaciones solo permitan en la red las aplicaciones que le interesan.

Cuando el tráfico que desea permitir deje de pasar por la regla basada en puertos original durante el tiempo suficiente para tener la certeza de que ya no es necesaria, puede eliminarla de la base de reglas.

Adición de aplicaciones a reglas existentes

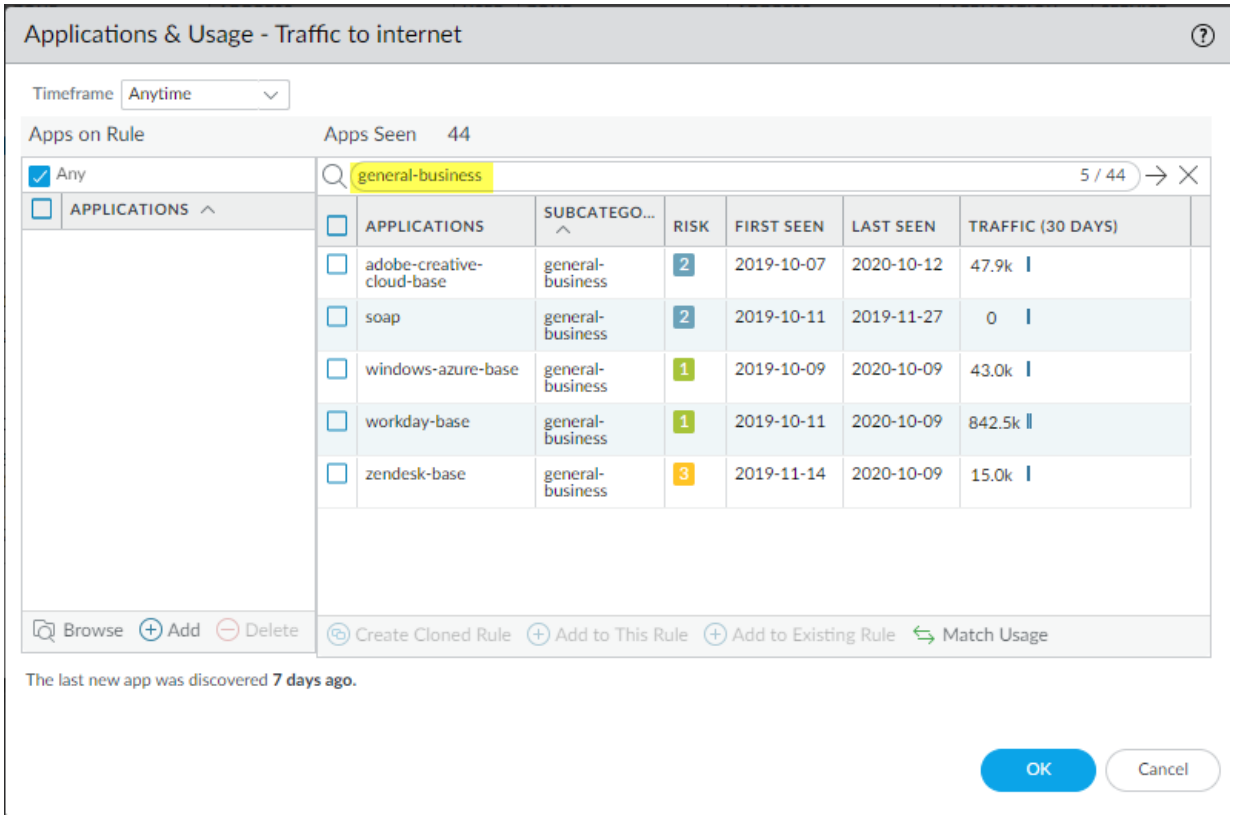
En algunas ocasiones, es conveniente añadir aplicaciones detectadas con una regla basada en puertos a una regla que ya existe. Por ejemplo, un administrador crea una regla clonada basada en aplicaciones para aplicaciones web empresariales generales a partir de una regla basada en puertos que permite el acceso a internet, esto es, una regla para los puertos 80/443. Después, el administrador se da cuenta de que la regla basada en puertos detecta más aplicaciones empresariales generales. Desea añadirlas a la regla clonada, pero sin clonar otra regla del mismo tipo porque se crearía una regla innecesaria y complicaría la base de reglas.

© 2020 Palo Alto Networks, Inc.

En este ejemplo se presupone que ya existe una regla de la política de seguridad basada en aplicaciones para controlar el tráfico empresarial general o que se clonó a partir de una regla de acceso a Internet basada en puertos, de manera similar a Caso de uso de migración mediante la clonación de reglas: navegación web y tráfico SSL. En ese ejemplo, clonamos una regla basada en aplicaciones a partir de la regla de acceso a Internet basada en puertos y cambiamos el servicio de la nueva regla al valor predeterminado de la aplicación para evitar que las aplicaciones basadas en la web usaran puertos no estándar.

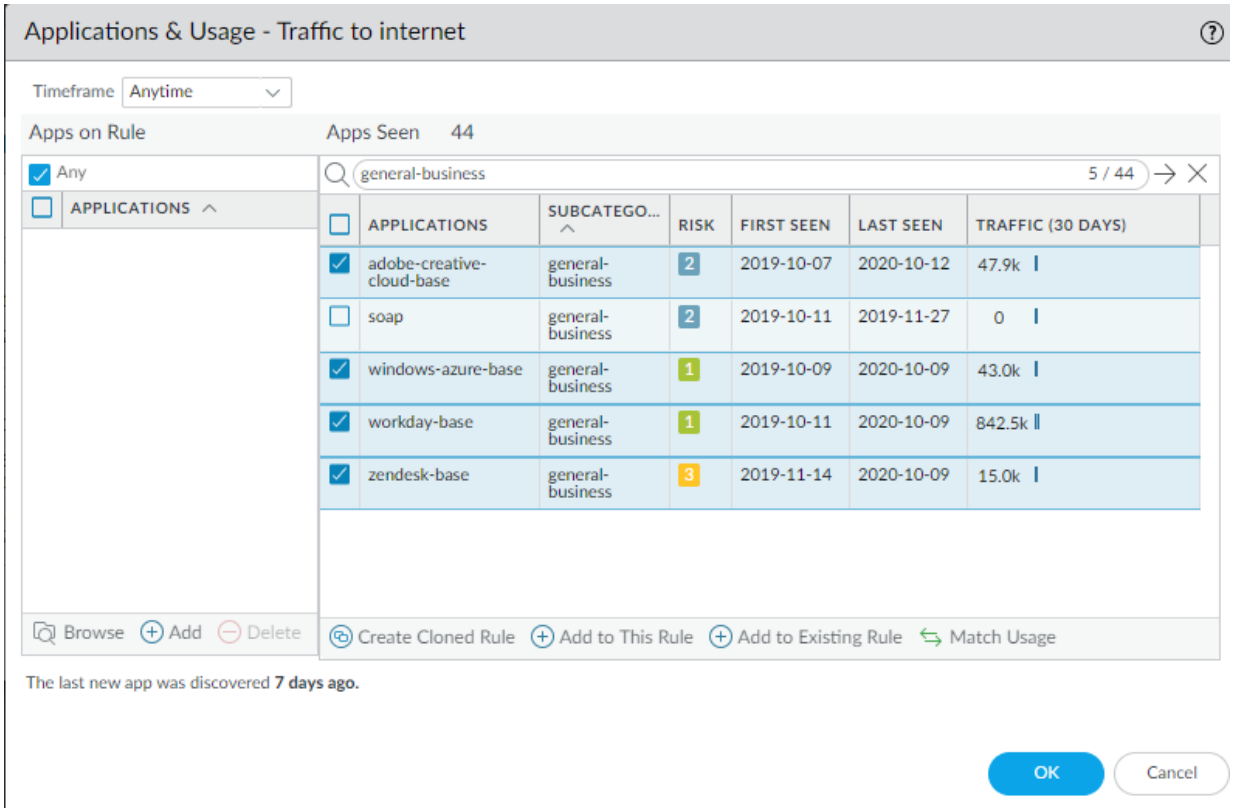
Además de añadir aplicaciones a una regla basada en aplicaciones existente, puede agregar aplicaciones a una regla basada en puertos existente. Esto convierte la regla basada en puertos en una regla basada en aplicaciones para las aplicaciones que añade a la regla. Si hace esto, diríjase a la regla y cambie el servicio al valor predeterminado de la aplicación para evitar que las aplicaciones utilicen puertos no estándar (además, el servicio configurado en la regla puede no coincidir con la aplicación).

STEP 1 | Compruebe la regla de acceso a Internet basada en puertos y asegúrese de que la regla haya visualizado aplicaciones empresariales generales y de que necesita permitir algunas de ellas para fines comerciales.



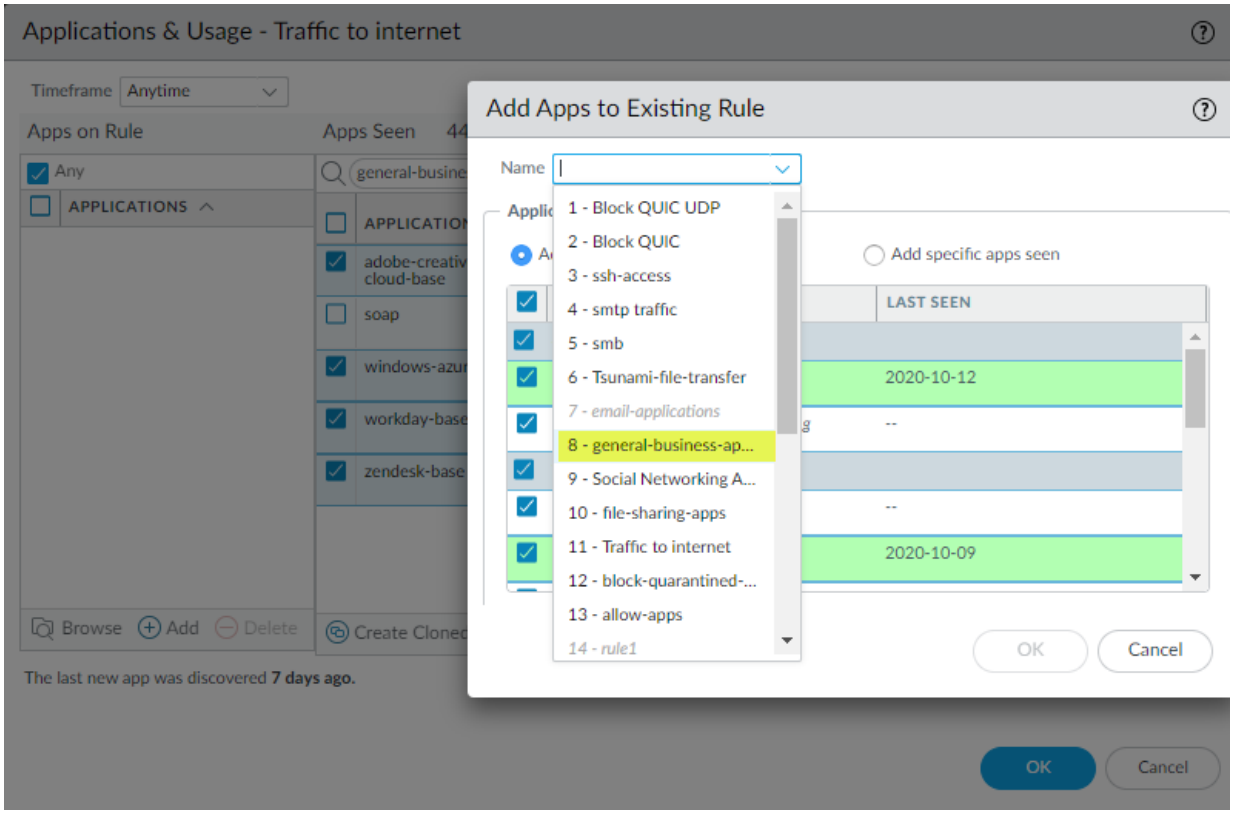
STEP 2 | Seleccione las aplicaciones empresariales generales que desee añadir a la regla existente.

© 2020 Palo Alto Networks, Inc.



STEP 3 | Haga clic en **Add to Existing Rule (Añadir a regla existente)** y seleccione en **Name (Nombre)** el nombre de la regla a la que desee añadir las aplicaciones, en este caso,**general-business-applications**.

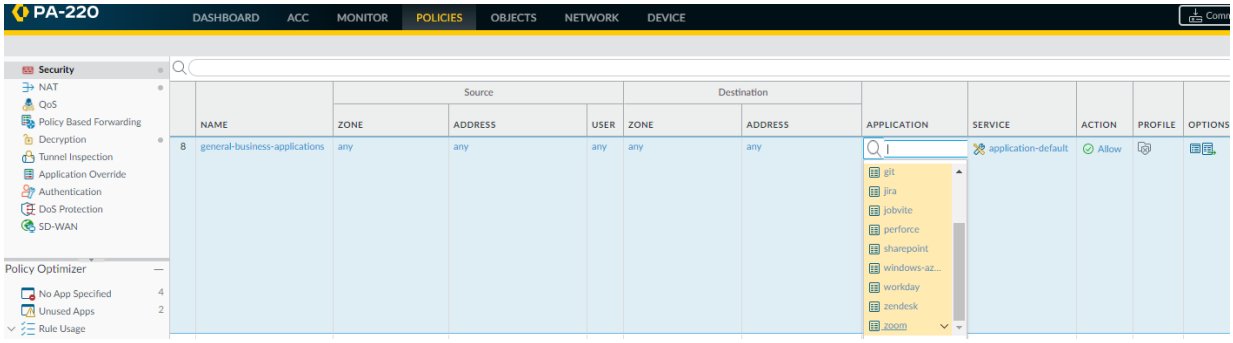
© 2020 Palo Alto Networks, Inc.



STEP 4 | Haga clic en **OK (Aceptar)** en **Add Apps to Existing Rule (Añadir aplicaciones a la regla existente)** para agregar las aplicaciones seleccionadas a la regla **general-business-applications**.

STEP 5 | Haga clic en **OK (Aceptar)** en **Applications & Usage (Aplicaciones y uso)**.

STEP 6 | Ahora, la regla actualizada controla las aplicaciones originales en la regla y las aplicaciones que acaba de añadir.



Identificación de reglas de la política de seguridad con aplicaciones no utilizadas

Si tiene reglas basadas en aplicaciones de la política de seguridad que permiten numerosas aplicaciones, puede eliminar las que no se usen (es decir, las aplicaciones que no se detectan nunca) para restringir esas reglas, de modo que solo permitan aplicaciones que de verdad aparezcan en el tráfico que coincida con la regla. La identificación de las aplicaciones no utilizadas y su eliminación de las reglas de la política de

© 2020 Palo Alto Networks, Inc.

seguridad es una práctica recomendada que refuerza la estrategia de seguridad, ya que reduce la superficie de ataque.

STEP 1 | Identifique las reglas de la política de seguridad que tienen aplicaciones que no se utilizan.

Policies (Políticas) > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **Unused Apps (Aplicaciones no utilizadas)** muestra todas las reglas basadas en aplicaciones que están configuradas con aplicaciones que no han coincidido con la regla (no se han visualizado en ella). Esto significa que estas reglas permiten aplicaciones que no puede usar en su red (o que otra regla oculta la regla, por lo que el tráfico que espera que coincida con la regla se corresponde con una regla anterior en la base de reglas).

El número de aplicaciones que aparecen en Apps Allowed (Aplicaciones permitidas) y en Apps Seen (Aplicaciones detectadas) se actualiza cada hora aproximadamente; si configura aplicaciones en una regla, pero no ve tantas en Apps Allowed (Aplicaciones permitidas) como esperaba, vuelva a comprobar la pantalla al cabo de una hora más o menos. Según la carga del cortafuegos, estos campos pueden tardar más tiempo en actualizarse.

STEP 2 | Priorice las reglas con aplicaciones que no se utilizan que se deben modificar en primer lugar.

Policies (Políticas) > **Security (Seguridad)** > **Policy Optimizer (Optimizador de políticas)** > **Unused Apps (Aplicaciones no usadas)** ofrece opciones para ordenar las reglas sin alterar su orden en la base de reglas y aporta otra información útil para priorizar que se deben limpiar en función de los objetivos comerciales y la tolerancia al riesgo.

- La diferencia entre **Apps Allowed (Aplicaciones permitidas)** —el número de aplicaciones en la lista de permitidos— y **Apps Seen (Aplicaciones detectadas)** —el número de aplicaciones permitidas que se visualizan realmente en la regla— indica cuántas de las aplicaciones configuradas en cada regla no se detectan en realidad, es decir, hasta qué punto se ha aprovisionado de más. Haga clic en **Apps Allowed (Aplicaciones permitidas)** para ordenar la lista por el número de aplicaciones permitidas en la regla o en **Apps Seen (Aplicaciones detectadas)** para ordenarla por el número de aplicaciones detectadas.
- Haga clic para ordenar los datos por la columna **Days with No New Apps (Días sin aplicaciones nuevas)**, que muestra el número de días que han transcurrido desde la última vez que la regla detectó alguna aplicación nueva. Este valor indica la solidez de la regla y la nula probabilidad de que aparezcan otras aplicaciones que no se hayan detectado ya. Cuanto mayor es el valor de **Days with No New Apps (Días sin aplicaciones nuevas)**, menos probable es que coincidan aplicaciones nuevas con la regla y más probable es que conozca todas las aplicaciones que permite.
- Las datas de **Created (Fecha de creación)** y de **Modified (Fecha de modificación)** también resultan útiles para determinar si la regla posee la solidez suficiente para inferir si detectará más adelante aplicaciones que aún no ha detectado o si ya ha detectado todas las aplicaciones esperadas. Cuanto más tiempo haya pasado desde la data de **Modified (Fecha de modificación)**, más probable es que la regla sea sólida. Si aparece el mismo valor en **Created (Fecha de creación)** y en **Modified (Fecha de modificación)**, significa que no se ha modificado la regla.
- **Hit Count (Recuento de resultados)**: muestra las reglas que han tenido más coincidencias en el período seleccionado. Puede excluir las reglas en las que haya restablecido el contador de resultados y especificar el período de exclusión en días. Si excluye las reglas cuyos contadores se hayan restablecido recientemente, evita malas interpretaciones sobre las reglas que muestran menos resultados de los esperados porque desconocía ese hecho.

También puede usar Hit Count (Recuento de resultados) para ver el uso (consulte Visualización de la utilización de las reglas de la política).

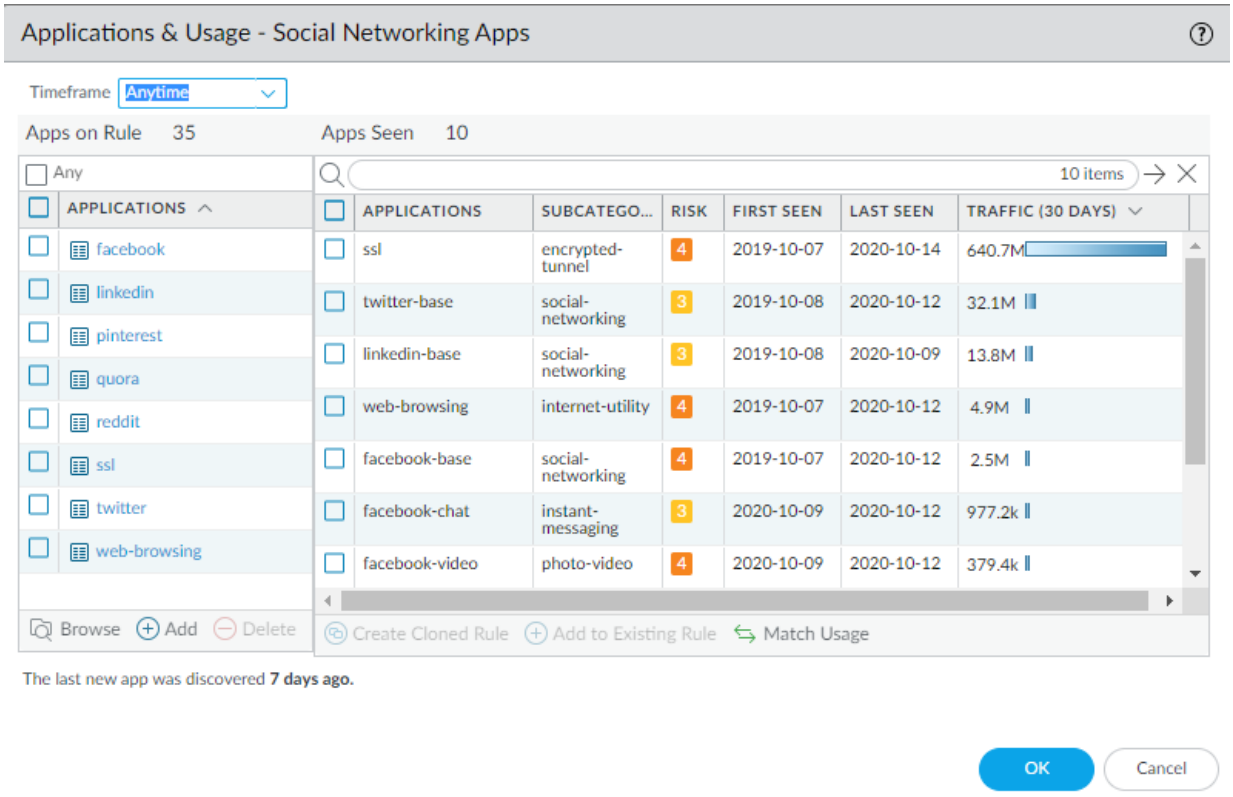
Además, puede hacer clic en **Traffic (Bytes, 30 days) (Tráfico [bytes, 30 días])** para ordenar la lista por la cantidad de tráfico que ha detectado la regla en los 30 últimos días. Use esta información para priorizar las reglas que se deben modificar en primer lugar. Por ejemplo, puede priorizar las reglas que muestren la

© 2020 Palo Alto Networks, Inc.

mayor diferencia entre **Apps Allowed (Aplicaciones permitidas)** y **Apps Seen (Aplicaciones detectadas)** y que también exhiban el valor más alto en **Days with No New Apps (Días sin aplicaciones nuevas)**, puesto que son las reglas más sólidas, con más aplicaciones no utilizadas.

STEP 3 | Revise las aplicaciones de la regla que figuran en **Apps Seen (Aplicaciones detectadas)**.

En **Unused Apps (Aplicaciones no usadas)**, haga clic en **Compare (Comparar)** o en el número de la columna **Apps Seen (Aplicaciones detectadas)** para abrir **Applications & Usage (Aplicaciones y uso)**. En este cuadro, **Apps on Rule (Aplicaciones de regla)** muestra las aplicaciones configuradas en la regla y **Apps Seen (Aplicaciones detectadas)**, las detectadas.

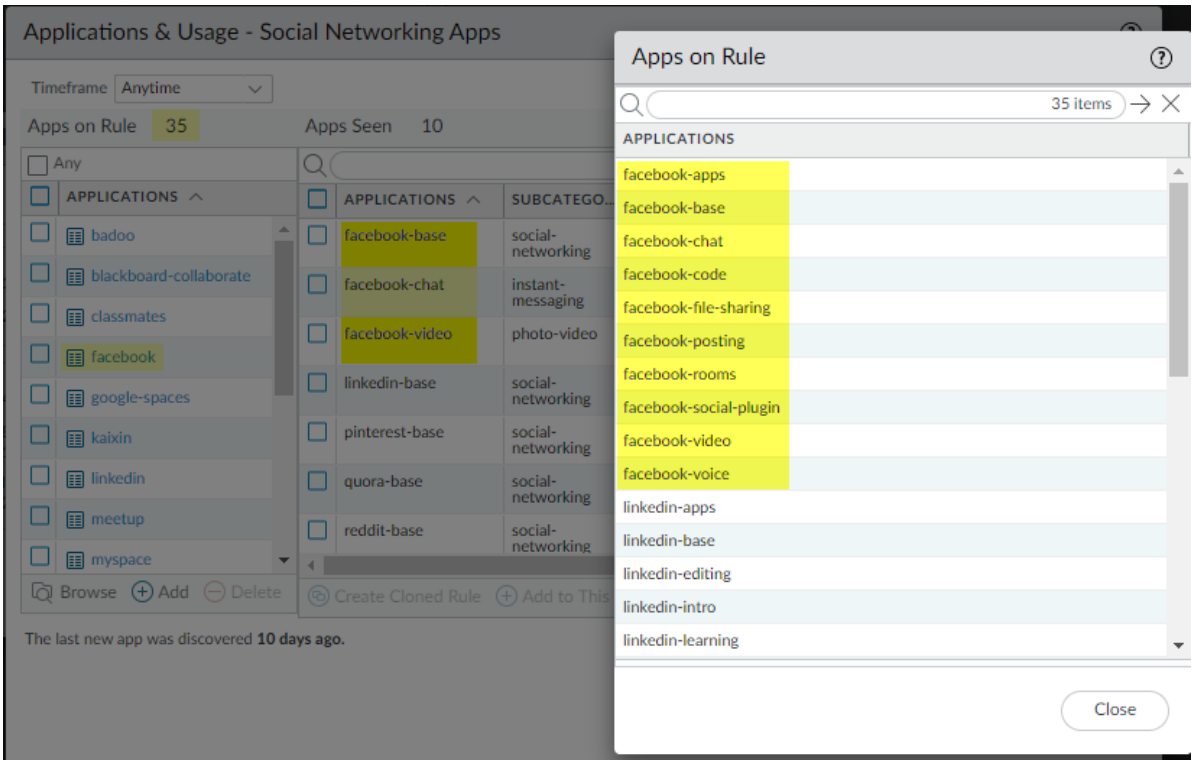


- El número que aparece junto a **Apps Seen (Aplicaciones detectadas)** (10 en este ejemplo) indica cuántas aplicaciones coincidían con la regla. Tenga en cuenta que el cortafuegos tarda al menos una hora en actualizar **Apps Seen (Aplicaciones detectadas)**.
- El número que aparece junto a **Apps on Rule (Aplicaciones de regla)** (35 en este ejemplo) indica cuántas aplicaciones hay configuradas en la regla. Para calcularlo, se cuentan las aplicaciones incluidas en una aplicación de contenedor, excepto esta. Si configura una aplicación de contenedor en la regla, esta permite todas las aplicaciones individuales que incluya. La lista **Applications (Aplicaciones)** solo muestra las aplicaciones configuradas manualmente en la regla. Así, cuando configura en una regla una aplicación de contenedor, solo aparece esta en **Applications (Aplicaciones)**, no todas las aplicaciones sueltas del contenedor, a menos que también las configure manualmente en la regla. Por este motivo, el número de aplicaciones que aparece en **Apps on Rule (Aplicaciones de regla)** puede ser distinto del número de aplicaciones que puede ver en la lista **Applications (Aplicaciones)**.
- Haga clic en el número que hay junto a **Apps on Rule (Aplicaciones de regla)** para ver todas las aplicaciones individuales en la regla.

  Esta regla de ejemplo tiene 10 **aplicaciones vistas** (aplicaciones que coinciden con la regla), pero permite 35 **aplicaciones en regla**. La aplicación de contenedor **facebook** está configurada en la regla y la regla visualiza el tráfico de las aplicaciones individuales facebook-base, facebook-chat, and facebook-video (**Apps Seen [Aplicaciones vistas]**). Cuando hace clic en el número **Apps on**

© 2020 Palo Alto Networks, Inc.

Rule (Aplicaciones en regla), el cuadro de diálogo **Apps on Rule (Aplicaciones en regla)** muestra las aplicaciones individuales permitidas, pero no la aplicación contenedora en sí.



No puede añadir ni eliminar aplicaciones en este cuadro de diálogo.

Compare las **aplicaciones vistas** en la regla con las **aplicaciones en regla**. Si no se utiliza una aplicación de la regla (no ve la aplicación o no ve aplicaciones en un contenedor permitido en **Apps Seen [Aplicaciones vistas]**), considere eliminar la aplicación de la regla para reducir la superficie de ataque. Tenga en cuenta que algunas aplicaciones solo se usan de forma periódica, por ejemplo, en eventos trimestrales o anuales, y pueden parecer prescindibles si no examine un período prolongado. **Timeframe (Período)** le permite seleccionar el intervalo de tiempo durante el que se **detectan aplicaciones** en la regla. Seleccione **Anytime (Cualquiera)** para ver todas las aplicaciones detectadas desde que está en vigor la regla. Según los valores indicados en **Created (Fecha de creación)** o **Modified (Fecha de modificación)** en el cuadro de diálogo **No App Specified (Ninguna aplicación especificada)** y el período que transcurre entre los eventos periódicos, es posible que la regla no lleve en el cortafuegos el tiempo suficiente para detectar todas las aplicaciones utilizadas a intervalos.

STEP 4 | Elimine de la regla las aplicaciones que no se utilizan.

Para eliminar manualmente aplicaciones de **Apps on Rule (Aplicaciones de regla)**, haga clic en **Delete (Eliminar)**; para añadirlas, haga clic en **Add (Añadir)**. Además, con un solo clic en **Match Usage (Comprobar uso)**, se añaden las aplicaciones de la regla que figuran en **Apps Seen (Aplicaciones detectadas)** y se eliminan las aplicaciones en las que no se haya detectado tráfico.

Para eliminar aplicaciones de la regla manualmente, seleccione las aplicaciones de **Apps on Rule (Aplicaciones de regla)** y haga clic en **Delete (Eliminar)**. Antes de hacerlo, compruebe que ninguna de ellas sea imprescindible en eventos periódicos. (También puede añadir o eliminar aplicaciones en la pestaña **Application (Aplicación)** de la regla de política de seguridad).

La opción **Match Usage (Comprobar uso)** mueve las aplicaciones de la regla que constan en **Apps Seen (Aplicaciones detectadas)** a la pantalla **Apps on Rule (Aplicaciones de regla)** y elimina todas las que no se utilizan.

© 2020 Palo Alto Networks, Inc.

Puede clonar reglas de Policies (Políticas) > Security (Seguridad) y de No App Specified (Ninguna aplicación especificada) para realizar el procedimiento Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID*. No puede clonar reglas a partir de Unused Apps (Aplicaciones no usadas).*

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 6 | Supervise las reglas actualizadas y solicite información a los usuarios para asegurarse de que permiten las aplicaciones deseadas y de que no bloquean las que se utilizan de forma periódica.

El número de Apps Allowed (Aplicaciones permitidas) y de Apps Seen (Aplicaciones detectadas) se actualiza cada hora aproximadamente. Tras eliminar todas las aplicaciones que no se utilizan de una regla, esta sigue figurando en Policies (Políticas) > Security (Seguridad) > Policy Optimzer (Optimizador de políticas) > Unused Apps (Aplicaciones no usadas) hasta que el cortafuegos actualice la pantalla. Cuando se actualiza, el número de Apps Allowed (Aplicaciones permitidas) coincide con el de Apps Seen (Aplicaciones detectadas) y la regla deja de aparecer en la pantalla Unused Apps (Aplicaciones no usadas). No obstante, según la carga del cortafuegos, estos campos pueden tardar más de una hora en actualizarse.

Alta disponibilidad para las estadísticas sobre el uso de las aplicaciones

Cuando configura dos cortafuegos en un par de alta disponibilidad (high availability, HA), las estadísticas sobre el uso se encuentran en el cortafuegos que genera los logs de tráfico de las aplicaciones. El dispositivo donde puede consultarlas también depende en parte de la configuración de HA:

- **Activo/pasivo**: el dispositivo activo genera las estadísticas sobre el uso de las aplicaciones. Si el dispositivo pasivo no detecta tráfico del usuario, las estadísticas solo se muestran en el dispositivo activo. Si el dispositivo pasivo detecta tráfico, solo muestra las estadísticas correspondientes al tráfico detectado.

  En caso de conmutación por error, las estadísticas sobre el uso de las aplicaciones se basan en exclusiva en los logs de tráfico que se generen en el nuevo dispositivo activo, es decir, el que era pasivo antes del intercambio de papeles.
- **Activo/activo**: el dispositivo que posee la sesión genera los logs de tráfico correspondientes, de modo que las estadísticas sobre el uso de las aplicaciones de dicha sesión solo están disponibles en ese dispositivo. Si un dispositivo activo posee la sesión, el otro dispositivo activo no muestra las estadísticas de esa sesión.

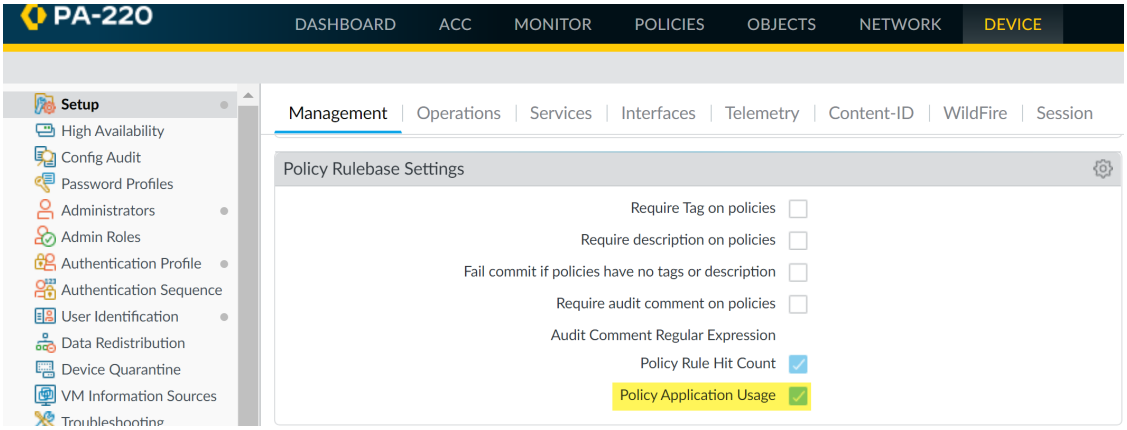
Habilitación o deshabilitación de Policy Optimizer

La función Policy Optimizer (Optimizador de políticas) está habilitada de manera predeterminada. Ofrece muchas opciones que facilitan los procedimientos Migración de reglas de la política de seguridad basadas en puertos a reglas basadas en App-ID y Identificación de reglas de la política de seguridad con aplicaciones no utilizadas, así como eliminar de las reglas las aplicaciones que no se utilizan. No obstante, puede deshabilitarla si lo desea.

STEP 1 | Desplácese hasta **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Policy Rulebase Settings (Configuración de base de reglas de políticas)**.

STEP 2 | Marque la casilla de verificación **Policy Application Usage (Uso de aplicaciones de políticas)** para habilitar la función y quite la marca para deshabilitarla.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Gateways de nivel de aplicación

El cortafuegos de Palo Alto Networks no clasifica el tráfico por puerto y protocolo; en lugar de eso, identifica la aplicación basándose en sus propiedades y características de transacciones exclusivas mediante la tecnología App-ID. Sin embargo, algunas aplicaciones requieren que el cortafuegos abra pinholes dinámicamente para establecer la conexión, determinar los parámetros de la sesión y negociar los puertos que se utilizarán para la transferencia de datos; estas aplicaciones utilizan la carga de la capa de aplicación para comunicar los puertos TCP o UDP dinámicos en los que la aplicación abre conexiones de datos. Para dichas aplicaciones, el cortafuegos sirve de gateway de nivel de aplicación (ALG) y abre un pinhole durante un tiempo limitado y para transferir exclusivamente datos o tráfico de control. El cortafuegos también realiza una reescritura NAT del payload cuando es necesario.



- *El ALG H.323 (H.225 y H.248) no es compatible con el modo de distribución al equipo selector.*
- *Cuando el cortafuegos sirve de ALG para el protocolo de inicio de sesión (SIP), de manera predeterminada realiza NAT en el payload y abre pinholes dinámicos para los puertos de medios. En algunos casos, dependiendo de las aplicaciones del SIP en uso en su entorno, los puntos de autenticación del SIP tienen inteligencia de NAT incorporada en sus clientes. En esos casos, quizás deba deshabilitar la función de ALG del SIP para evitar que el cortafuegos modifique las sesiones de saturación. Cuando la ALG SIP está deshabilitada, si App-ID determina que una sesión es de tipo SIP, no se traduce la carga y no se abren pinholes dinámicos. Consulte* Deshabilitación de la puerta de enlace de nivel de aplicación (ALG) SIP*.*



Cuando utilice NAT de IP dinámica y puerto (Dynamic IP and Port , DIPP), el descodificador ALG del cortafuegos de Palo Alto Networks necesitará una combinación de IP y puerto (dirección de envío y puerto de envío) en encabezados SIP (campos de contacto y vía) para poder traducir los encabezados mencionados y abrir sesiones de predicción basadas en ellos.

La siguiente tabla enumera los ALG IPv4, NAT, IPv6, NPTv6 y NAT64 e indica con una marca de verificación si el ALG admite cada protocolo (como el SIP).

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
SIP	✓	✓	✓	–	–
SCCP	✓	✓	✓	–	–
MGCP	✓	✓	–	–	–
FTP	✓	✓	✓	✓	–
RTSP	✓	✓	✓	✓	–
MySQL	✓	✓	–	–	–

© 2020 Palo Alto Networks, Inc.

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
Oracle/SQLNet/ TNS	✓	✓	✓	✓	—
RPC	✓	✓	—	—	—
RSH	✓	✓	—	—	—
UNIStim	✓	✓	—	—	—
H.225	✓	✓	—	—	—
H.248	✓	✓	—	—	—

© 2020 Palo Alto Networks, Inc.

Deshabilitación de la gateway de nivel de aplicación (ALG) SIP

El cortafuegos de Palo Alto Networks utiliza la gateway de nivel de aplicación (ALG) del protocolo de inicio de sesión (SIP) para abrir pinholes dinámicos en el cortafuegos donde la NAT está habilitada. Sin embargo, algunas aplicaciones (como las de VoIP) tienen inteligencia NAT incorporada en la aplicación cliente. En estos casos, la ALG del SIP del cortafuegos puede interferir en las sesiones de saturación y provocar que la aplicación cliente deje de funcionar.

Una solución a este problema es definir una política de cancelación de aplicación para SIP, pero utilizar este enfoque deshabilita la App-ID y la función de detección de amenazas. Un enfoque mejor es deshabilitar el ALG SIP, lo cual no deshabilita la App-ID ni la detección de amenazas.

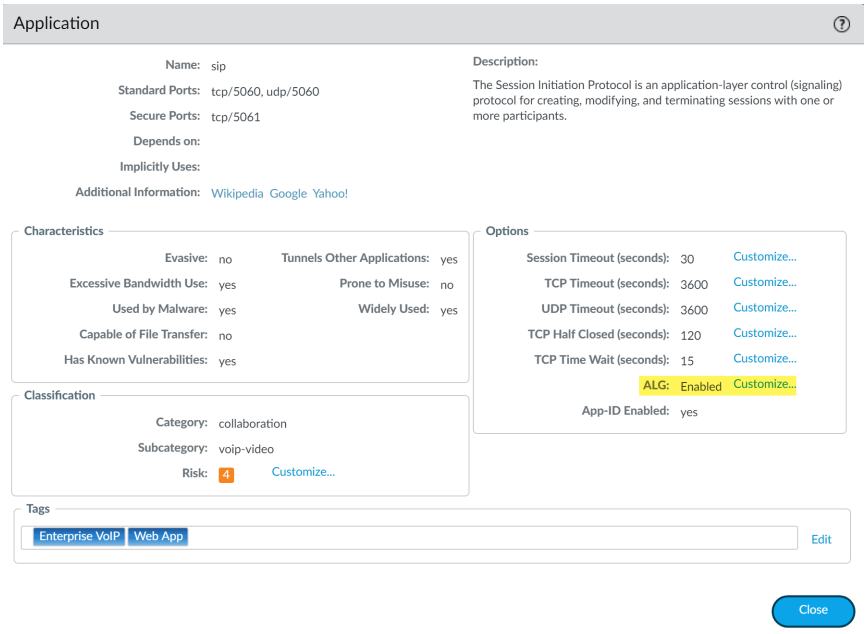
El siguiente procedimiento describe cómo deshabilitar el ALG SIP.

STEP 1 | Seleccione **Objects (Objetos)** > **Applications (Aplicaciones)**.

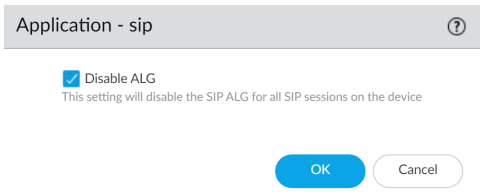
STEP 2 | Seleccione la aplicación sip.

Puede escribir **sip** en el cuadro **Search (Búsqueda)** para ayudar a encontrar la aplicación sip.

STEP 3 | Seleccione **Personalizar...** para **ALG** en la sección Opciones del cuadro de diálogo Aplicación.



STEP 4 | Seleccione la casilla de verificación **Disable ALG (Deshabilitar ALG)** del cuadro de diálogo Aplicación - sip y haga clic en **OK (Aceptar)**.



© 2020 Palo Alto Networks, Inc.

STEP 5 | Haga clic en **Close (Cerrar)** para cerrar el cuadro de diálogo Application (Aplicación) y en **Commit (Confirmar)** para guardar el cambio.

© 2020 Palo Alto Networks, Inc.

Uso de encabezados de HTTP para la gestión del acceso a aplicaciones de SaaS

El uso no aprobado de aplicaciones de SaaS puede ser una manera de que sus usuarios transmitan información confidencial fuera de su red accediendo, por lo general, a una versión personal de una aplicación. Sin embargo, si desea permitir el acceso a la versión empresarial de estas aplicaciones a personas u organizaciones, no puede bloquear toda la aplicación de SaaS.

Puede utilizar encabezados personalizados de HTTP para no permitir las cuentas personales de SaaS y permitir una cuenta empresarial específica. Varias aplicaciones de SaaS permiten o no permiten el acceso a las aplicaciones en función de la información en encabezados de HTTP específicos. Puede implementar la Creación de entradas de inserción de encabezados HTTP utilizando tipos predefinidos para gestionar el acceso a aplicaciones de SaaS populares, como Google G Suite y Microsoft Office 365. Palo Alto Networks® utiliza actualizaciones de contenido para mantener los conjuntos de reglas predefinidas específicos de estas aplicaciones, además de añadir nuevos conjuntos de reglas predefinidas.

También puede implementar la Creación de entradas de inserción de encabezado HTTP personalizadas si desea gestionar el acceso a una aplicación de SaaS (que utiliza encabezados HTTP para limitar el acceso al servicio) para la que Palo Alto Networks no proporcionó un conjunto predefinido de reglas.

Tenga en cuenta que las aplicaciones de SaaS comerciales siempre utilizan SSL, de modo que se necesita el descifrado para realizar la inserción de encabezados HTTP. Puede configurar el cortafuegos para que descifre el tráfico utilizando el descifrado de proxy SSL de reenvío si al tráfico aún no lo descifró un cortafuegos de subida.

No necesita una licencia de filtrado de URL para utilizar esta función.

Para comprender cómo utilizar los encabezados HTTP a fin de gestionar aplicaciones de SaaS, consulte los siguientes artículos:

- Comprensión de los encabezados personalizados de SaaS
- Dominios utilizados por los tipos de aplicación SaaS predefinidos
- Creación de entradas de inserción de encabezados HTTP utilizando tipos predefinidos
- Creación de entradas de inserción de encabezado HTTP personalizadas

Comprensión de los encabezados personalizados de SaaS

Antes de comenzar, asegúrese de comprender los encabezados de HTTP personalizados que utilizará con la aplicación de SaaS que gestiona. Debe comprender lo que puede lograr con estos encabezados y la información que debe especificar para lograr sus objetivos.

Tenga en cuenta que las aplicaciones de SaaS que utilizan encabezados personalizados no siempre los utilizan para controlar el acceso a los tipos de cuentas. Por ejemplo, Palo Alto Networks® proporciona asistencia predefinida para encabezados personalizados de YouTube que determina si los usuarios de la red pueden acceder a contenido restringido.

También debe leer la documentación de la aplicación de SaaS cuyo acceso desea controlar, de modo que comprenda los encabezados que debe utilizar en esta aplicación.

Se aplican los siguientes límites a la inserción del encabezado HTTP:

- *Longitud de caracteres del nombre de encabezado: 100.*
- *Longitud de caracteres del valor de encabezado: 512.*

© 2020 Palo Alto Networks, Inc.

Tenga en cuenta que algunas aplicaciones SaaS pueden definir nombres de encabezado personalizados o asignar valores a sus encabezados personalizados que excedan esos límites. Estas situaciones deberían ser poco frecuentes, pero si una aplicación SaaS excede uno o ambos de estos límites de longitud de caracteres, su cortafuegos de nueva generación no podrá gestionar correctamente el acceso a esa aplicación SaaS.

La siguiente tabla enumera los encabezados que puede utilizar en las aplicaciones de SaaS para las cuales Palo Alto Networks proporciona asistencia predefinida; cada encabezado también incluye un enlace a información más específica.

Application (Aplicación)	Cabeceras	Más información
Dropbox	`X-Dropbox-allowed-Team-Ids`	www.dropbox.com/help/business/network-control Puede permitir el acceso a las cuentas aprobadas de Dropbox empresarial. El valor de este encabezado es la ID de equipo de la cuenta empresarial, que puede obtener desde la sección de control de red de la consola de administración de Dropbox. También debe habilitar esta funcionalidad desde la misma ubicación. Si desea información detallada sobre la gestión de este encabezado, además de cómo habilitar sus clientes de Dropbox, de modo que pueda descifrar su tráfico, póngase en contacto con el representante de su cuenta de Dropbox.
Google G Suite	`X-GooGApps-Allowed-Domains`	support.google.com/a/answer/1668854?hl=en Puede permitir el acceso a cuentas de Google específicas desde su dominio. Los valores que brinda a este encabezado son sus dominios y subdominios. Para insertar correctamente los encabezados de las aplicaciones de Google, también debe realizar las siguientes acciones: 1. Crear un perfil de descifrado SSL que incluya las siguientes categorías y URL: • business-and-economy • computer-and-internet-info • content-delivery-networks • internet-communications-and-telephony • Low-Risk (Riesgo bajo) • online-storage-and-backup • search-engine • web-based-email • drive.google.com • *.google.com • *.googleusercontent.com • *.gstatic.com

© 2020 Palo Alto Networks, Inc.

Application (Aplicación)	Cabeceras	Más información
		2. Actualmente, la inserción de encabezados HTTP no es compatible con HTTP/2. Para insertar encabezados, cambie a las conexiones HTTP/2 a HTTP/1.1 mediante la función **Strip ALPN (Eliminar ALPN)** en el perfil de descifrado apropiado. Para obtener más información, consulte Inspección de App-ID y HTTP/2. 3. Cree reglas para bloquear App-ID de Quick UDP Internet Connections (QUIC, conexiones a Internet de UDP rápidas) y colóquelas en la parte superior de su política de seguridad, ya que el cortafuegos no admite la inserción de encabezados para este protocolo. Cuando lo haga, la aplicación volverá a usar HTTP/2 sobre TLS, que el cortafuegos gestiona en el paso anterior.
Microsoft Office 365	`Restrict-Access-To-Tenants` `Restrict-Access-Context`	docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions Usted proporciona a `Restrict-Access-To-Tenants` una lista de inquilinos a los que desea permitir el acceso a sus usuarios. Puede utilizar cualquier dominio registrado con un inquilino para identificar al inquilino en esta lista. Proporcione la ID de directorio que configura la restricción de inquilinos en `Restrict-Access-Context`. Su ID de directorio se encuentra en el portal de Azure. Inicie sesión como administrador, seleccione **Azure Active Directory** y seleccione **Properties (Propiedades)**.
YouTube	`YouTube-Restrict`	support.google.com/a/answer/6214622?hl=en Usted proporciona a este encabezado la información del tipo de vídeos que desea que sus usuarios puedan ver. Puede especificar un ajuste **Strict (Estricto)** o **Moderate (Moderado)**. Consulte support.google.com/a/answer/6212415 para obtener detalles sobre estas diferentes configuraciones.

Dominios utilizados por los tipos de aplicación SaaS predefinidos

Las aplicaciones de SaaS implementan HTTPS, de modo que para insertar encabezados personalizados en este tráfico, los encabezados personalizados deben cifrarse. Si utiliza el descifrado de proxy de reenvío disponible en el cortafuegos para descifrar los encabezados personalizados, debe identificar el tráfico de HTTPS específico que desea descifrar identificando los dominios asociados al tráfico. La siguiente tabla identifica los dominios relevantes de cada aplicación de SaaS para la que Palo Alto Networks® proporciona reglas predefinidas.

© 2020 Palo Alto Networks, Inc.

Application (Aplicación)	Dominios
Dropbox	`*.dropbox.com`
G Suite	`*.google.com` `gmail.com`

Microsoft Office 365	`login.microsoftonline.com`
	`login.microsoft.com`
	`login.windows.net`

YouTube	`www.youtube.com`
	`m.youtube.com`
	`youtubei.googleapis.com`
	`youtube.googleapis.com`
	`www.youtube-nocookie.com`

Creación de entradas de inserción de encabezados HTTP utilizando tipos predefinidos

STEP 1 | Si aún no existen dispositivos de subida que descifren tráfico de HTTPS, configure el Descifrado utilizando la Configuración de proxy SSL de reenvío.

Si configura el descifrado SSL para Dropbox, también debe configurar sus clientes Dropbox para que permitan el tráfico SSL. Estos procedimientos son específicos y privados de Dropbox. Para obtener estos procedimientos, póngase en contacto con los representantes de su cuenta de Dropbox.

1. Haga clic en **Add (Añadir)** para añadir una categoría de URL personalizada para la aplicación de SaaS que gestiona (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**).
2. Especifique un **Name (Nombre)** para la categoría.
3. **Añada** los dominios específicos de la aplicación SaaS que está gestionando o para los que desee insertar el nombre de usuario y el dominio en los encabezados. Consulte Dominios utilizados por los tipos de aplicación SaaS predefinidos para acceder a una lista de los dominios que utiliza para cada una de las aplicaciones de SaaS predefinidas. Consulte Inserción de nombre de usuario en encabezados HTTP para obtener más información sobre cómo configurar el cortafuegos para incluir el nombre de usuario y el dominio en los encabezados HTTP.

   Cada nombre de dominio puede tener hasta 254 caracteres y puede identificar, como máximo, 50 dominios para cada entrada. La lista de dominios admite comodines (por ejemplo, **`*.example.com`**). Le recomendamos que no anide comodines (por ejemplo, **`*.*.*`**) y no superponga dominios dentro del mismo perfil de URL.
4. Para la gestión de aplicaciones SaaS, cree una regla de políticas de descifrado y, mientras sigue ese procedimiento, configure lo siguiente:
   - En la pestaña **Service/URL Category (Categoría de URL/servicio)**, haga clic en **Add (Añadir)** para añadir la **URL Category (Categoría de URL)** que creó en el paso anterior.

© 2020 Palo Alto Networks, Inc.

- En la pestaña **Options (Opciones)**, asegúrese de establecer **Action (Acción)** en **Decrypt (Descifrar)** y **Type(Tipo)** en **SSL Forward Proxy (Proxy SSL de reenvío)**.

STEP 2 | Edite o añada un perfil de filtrado de URL.

STEP 3 | Seleccione **HTTP Header Insertion (Inserción de encabezados HTTP)** en el cuadro de diálogo **URL Filtering Profile (Perfil de filtrado de URL)**.

STEP 4 | Haga clic en **Add (Añadir)** para añadir una entrada.

1. Especifique un **nombre** (hasta 100 caracteres) para esta entrada.
2. Seleccione un **tipo** predefinido.

   Esto rellena las listas de **Domains (Dominios)** y **Headers (Encabezados)**.
3. En cada **Header (Encabezado)**, introduzca un **Value (Valor)**.
4. (Opcional) Seleccione **Log** para habilitar la creación de logs y la actividad de inserción de encabezados.

   El tráfico permitido no se registra, por lo que las inserciones de encabezado no se registran para el tráfico permitido.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | **Añada** o edite una regla de la política de seguridad (**Policies (Políticas)** > **Security (Seguridad)**) para incluir el perfil de filtrado de URL de la inserción del encabezado HTTP.

- Para la gestión de aplicaciones SaaS, permita a los usuarios acceder a la aplicación SaaS para la que está configurando esta regla de inserción de encabezado.
- Para incluir el nombre de usuario y el dominio en los encabezados HTTP, aplique el perfil de filtrado de URL a la regla de la política de seguridad para el tráfico HTTP o HTTPS.

1. Seleccione el perfil de filtrado de URL (**Actions [Acciones]** > **URL Filtering [Filtrado de URL]**) que editó o creó en el paso 2.
2. Haga clic en **OK (Aceptar)** para guardar y en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Compruebe que el cortafuegos inserte correctamente el encabezado.

- Para la gestión de aplicaciones Saas, desde un endpoint, confirme que el acceso a la aplicación SaaS funciona de la manera esperada.

  1. Intente acceder a una cuenta o a contenido que espera poder acceder. Si no puede acceder a la cuenta o al contenido de SaaS, la configuración no funciona.
  2. Intente acceder a una cuenta o a contenido que espera que esté bloqueado. Si puede acceder a la cuenta o al contenido de SaaS, la configuración no funciona.
  3. Si ambos pasos anteriores funcionan como lo espera, puede acceder a View Logs (Visualización de logs) (si configuró la creación de logs en el paso 4.4) y debería ver la actividad grabada de inserción de encabezados HTTP.

Creación de entradas de inserción de encabezado HTTP personalizadas

STEP 1 | Si aún no existen dispositivos de subida que descifren tráfico de HTTPS, configure el Descifrado utilizando la Configuración de descifrado del proxy SSL dereenvío.

1. Haga clic en **Add (Añadir)** para añadir una categoría de URL personalizada para la aplicación de SaaS que gestiona (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**).
2. Especifique un **Name (Nombre)** para la categoría.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en **Add (Añadir)** para añadir los dominios específicos de la aplicación de SaaS que gestiona.
4. Realice la Creación de una regla de política de descifrado y mientras sigue este procedimiento, configure lo siguiente:
   - En la pestaña **Service/URL Category (Categoría de URL/servicio)**, haga clic en **Add (Añadir)** para añadir la **URL Category (Categoría de URL)** que creó en el paso anterior.
   - En la pestaña **Options (Opciones)**, asegúrese de establecer **Action (Acción)** en **Decrypt (Descifrar)** y **Type(Tipo)** en **SSL Forward Proxy (Proxy SSL de reenvío)**.

STEP 2 | Edite o cree un perfil de filtrado de URL.

STEP 3 | Seleccione **HTTP Header Insertion (Inserción de encabezados HTTP)** en el cuadro de diálogo **URL Filtering Profile (Perfil de filtrado de URL)**.

STEP 4 | Haga clic en **Add (Añadir)** para añadir una entrada.

1. Especifique un **Name (Nombre)** para esta entrada.
2. Seleccione **Custom (Personalizado)** como el **Type (Tipo)**.
3. Haga clic en **Add (Añadir)** para añadir dominios en la lista de **Domains (Dominios)**.

   Puede añadir hasta 50 dominios y cada nombre de dominio puede tener hasta 256 caracteres; los comodines son compatibles (por ejemplo, *.example.com).

   La inserción de encabezados HTTP se produce cuando un dominio en esta lista coincide con el encabezado host de la solicitud de HTTP.
4. Haga clic en **Add (Añadir)** para añadir encabezados en la lista de **Headers (Encabezados)**.

   Puede añadir hasta 5 encabezados y cada encabezado puede tener hasta 100 caracteres, pero no puede contener espacios.
5. Para cada **Value (Valor)** del encabezado.
6. (Opcional) Seleccione **Log** para habilitar la creación de logs y la actividad de inserción de encabezados.
7. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | Haga clic en **Add (Añadir)** para añadir una regla de la política de seguridad o edite una existente (**Policies [Políticas]** > **Security [Seguridad]**) Política de seguridad que permite que los usuarios accedan a la aplicación de SaaS para la que configura esta regla de inserción de encabezados.

1. Seleccione el perfil de filtrado de URL (**Actions [Acciones]** > **URL Filtering [Filtrado de URL]**) que editó o creó en el paso 2.
2. Haga clic en **OK (Aceptar)** para guardar y en **Commit (Confirmar)** para confirmar los cambios.

STEP 6 | Verifique que el acceso a la aplicación de SaaS funcione como espera. En el endpoint conectado a su red:

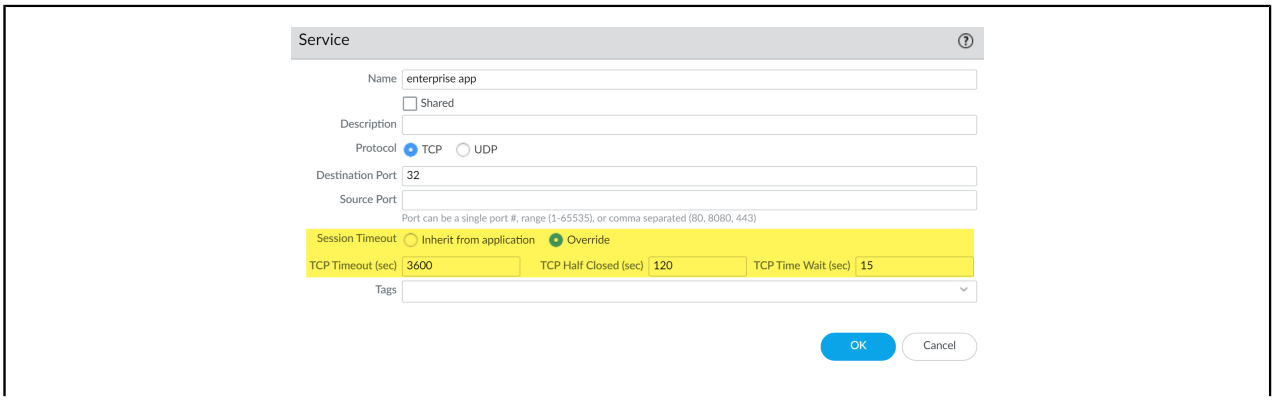
1. Intente acceder a una cuenta o a contenido que espera poder acceder. Si no puede acceder a la cuenta o al contenido de SaaS, la configuración no funciona.
2. Intente acceder a una cuenta o a contenido que espera que esté bloqueado. Si puede acceder a la cuenta o al contenido de SaaS, la configuración no funciona.
3. Si ambos pasos anteriores funcionan como lo espera, puede acceder a la Visualización de logs (si configuró la creación de logs en el paso 4.6) y debería ver la actividad grabada de inserción de encabezados HTTP.

© 2020 Palo Alto Networks, Inc.

Mantenimiento de los tiempos de espera personalizados para aplicaciones de centros de datos

Mantenga los tiempos de espera personalizados de las aplicaciones cuando pasa de una política basada en un puerto a una política basada en una aplicación. Utilice este método para mantener los tiempos de espera personalizados en lugar de anular la App-ID (perder visibilidad de la aplicación) o crear una App-ID personalizada (dedicar tiempo e investigación).

Para comenzar, configure los ajustes de tiempo de espera personalizado como parte de un objeto de servicio:



Luego, añada el objeto de servicio de una regla de la política para aplicar los tiempos de espera personalizados a la aplicación que aplica la regla.

Los siguientes pasos describen cómo aplicar los tiempos de espera personalizados a las aplicaciones; para aplicar los tiempos de espera personalizados a los grupos de usuarios, debe seguir los mismos pasos, pero asegúrese de añadir el objeto de servicio a la regla de la política de seguridad que se aplica a los usuarios a los que desea que se aplique el tiempo de espera.

STEP 1 | Seleccione **Objects (Objetos)** > **Services (Servicios)** para añadir o modificar un objeto de servicio.

También puede crear objetos de servicio cuando define los criterios de coincidencia de una regla de la política de seguridad: seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Service/URL Category (Categoría de URL/servicio)** y haga clic en **Add (Añadir)** para añadir un nuevo objeto de servicio que se aplicará al tráfico de aplicaciones que regula la regla.

STEP 2 | Seleccione el protocolo del servicio que utilizará (TCP o UDP).

STEP 3 | Introduzca el número de puerto de destino o el intervalo de números de puerto que utiliza el servicio.

STEP 4 | Defina el tiempo de espera de una sesión del servicio.

- **Inherit from application (Heredar de la aplicación)** (predeterminado): no se aplican tiempos de espera basados en el servicio; en cambio, se aplica el tiempo de espera de la aplicación.
- **Override (Anular)**: defina un tiempo de espera de sesión personalizado para el servicio.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Si elige anular el tiempo de espera de la aplicación y definir un tiempo de espera de sesión personalizado, realice las siguientes acciones:

- Introduzca un valor de **TCP Timeout (Tiempo de espera de TCP)** para establecer el tiempo máximo en los segundos que una sesión de TCP puede permanecer abierta después de que se inicia la transmisión de datos. Cuando este tiempo se agota, la sesión se cierra. El intervalo es de 1 a 604800; el valor predeterminado es 3600 segundos.
- Introduzca el valor de **TCP Half Closed (TCP semicerrado)** para establecer el tiempo máximo en los segundos que una sesión permanece en la tabla de sesiones entre la recepción del primer paquete FIN y la recepción del segundo paquete FIN o RST. Cuando el temporizador expira, la sesión se cierra. El intervalo es de 1 a 604800; el valor predeterminado es 120 segundos.
- Introduzca el valor de **TCP Wait Time (Tiempo de espera de TCP)** para establecer el tiempo máximo en los segundos que una sesión permanece en la tabla de sesiones tras la recepción del segundo paquete FIN o RST. Cuando el temporizador expira, la sesión se cierra. El intervalo es de 1 a 600; el valor predeterminado es 15 segundos.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar el objeto de servicio.

STEP 7 | Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)** para añadir una regla de la política o modificar una existente para regular el tráfico de aplicación que desea controlar.

STEP 8 | Seleccione **Service/URL Category (Categoría de URL/servicio)** y haga clic en **Add (Añadir)** para añadir el objeto de servicio que acaba de crear a la regla de la política de seguridad.

STEP 9 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

© 2020 Palo Alto Networks, Inc.

ID de dispositivo

> Descripción general de Device-ID
> Preparación para la implementación de Device-ID
> Configuración de Device-ID
> Gestión de Device-ID
> Comandos de la CLI para Device-ID

© 2020 Palo Alto Networks, Inc.

Descripción general de Device-ID

Tanto si su entorno admite o no una política de Bring Your Own Device (BYOD, traiga su propio dispositivo) como si no, es probable que ya tenga una gran cantidad de dispositivos en su red; tal vez incluso más de lo que cree. Eso, combinado con la necesidad de escalabilidad a medida que aumenta el número de usuarios y los dispositivos que los acompañan en su red, sin mencionar la creciente infraestructura de Internet de las cosas (IoT), genera un área de riesgo en constante crecimiento con muchas posibilidades de explotación por parte de usuarios malintencionados. Además, una vez que identifica estos dispositivos, ¿cómo los protege de vulnerabilidades como software operativo desactualizado? El uso de Device-ID™ en su cortafuegos o el envío de políticas desde Panorama le permiten obtener el contexto del dispositivo para eventos en su red, obtener recomendaciones de reglas de políticas para esos dispositivos, escribir políticas basadas en dispositivos y hacer cumplir la política de seguridad según las recomendaciones.

De manera similar a cómo User-ID proporciona una política basada en el usuario y App-ID ofrece una política basada en la aplicación, Device-ID brinda reglas de política que se basan en un dispositivo, independientemente de los cambios en su dirección IP o ubicación. Device-ID, que proporciona trazabilidad para dispositivos y asocia eventos de red con dispositivos específicos, permite obtener un contexto sobre cómo los eventos se relacionan con los dispositivos y escribir políticas que están asociadas con los dispositivos, en lugar de usuarios, ubicaciones o direcciones IP, que pueden cambiar con el paso del tiempo. Puede utilizar Device-ID en las políticas de seguridad, descifrado, calidad de servicio (QoS) y autenticación.

Device-ID requiere una licencia de seguridad de IoT, una licencia de Cortex Data Lake (CDL) y el certificado del dispositivo.

Si usa una versión de PAN-OS 8.1.0 a PAN-OS 9.1.x en un cortafuegos, la licencia de seguridad de IoT proporciona clasificación de dispositivos, análisis de comportamiento y análisis de amenazas para sus dispositivos. Si usa PAN-OS 10.0 o posterior, puede usar Device-ID para obtener asignaciones de dirección IP a dispositivo para ver el contexto del dispositivo para eventos de red, usar la seguridad de IoT para obtener recomendaciones de reglas de políticas para esos dispositivos y obtener visibilidad para los dispositivos en informes y la ACC.

Puede crear una política de seguridad basada en dispositivos en cualquier solución Panorama o cortafuegos que use la versión 10.0 o posterior de PAN-OS. Para hacer cumplir la política de seguridad, el dispositivo debe tener una licencia de seguridad de IoT válida.

Para identificar y clasificar dispositivos, la aplicación IoT Security (Seguridad de IoT) utiliza metadatos de logs, protocolos de red y sesiones en el cortafuegos. Esto no incluye información o datos privados o sensibles que no sean relevantes para la identificación del dispositivo. Los metadatos también forman la base del comportamiento esperado para el dispositivo, que luego establece los criterios para la recomendación de la regla de políticas que define qué tráfico y protocolos permitir para ese dispositivo.

Después de que IoT Security (Seguridad de IoT) identifique y clasifique los dispositivos en su red mediante los cortafuegos de Palo Alto Networks que ya están en su red, para que no tenga que implementar nuevos dispositivos o soluciones de terceros, Device-ID puede aprovechar esos datos para hacer coincidir los dispositivos con las reglas de políticas y proporcionar contexto de dispositivo para eventos de red. Puede rastrear instantáneamente los eventos de la red hasta los dispositivos individuales y obtener recomendaciones de reglas de políticas de seguridad para proteger esos dispositivos a través de la visibilidad que proporciona el cortafuegos o Panorama para el tráfico, las aplicaciones, los usuarios, los dispositivos y las amenazas.

Todas las plataformas de cortafuegos que son compatibles con PAN-OS 10.0 admiten Device-ID y la aplicación IoT Security (Seguridad de IoT), a excepción de la serie VM-50, VM-200, la serie CN y Prisma Access.

© 2020 Palo Alto Networks, Inc.

Existen seis niveles de clasificación (también conocidos como atributos) para dispositivos:

Atributo	Ejemplo
Category	`ATM Machine (Cajero automático)`; `3D Printer (Impresora 3D)`
Perfil	`Palo Alto Networks Device (Dispositivo de Palo Alto Networks)`
Modelo	`iPad`
Versión de OS	`iOS 9.9.3`
Familia del SO	`Android`; `iOS`
Proveedor	`ASUS`; `Philips`

Para obtener recomendaciones de reglas de políticas para dispositivos en su red, el cortafuegos observa el tráfico para generar logs de aplicaciones mejorados (EAL, Enhanced Application Logs). A continuación, el cortafuegos envía los EAL a Cortex Data Lake (CDL) para su procesamiento. La aplicación IoT Security (Seguridad de IoT) en el hub recibe logs de CDL para su análisis, proporciona asignaciones de dirección IP a dispositivo y genera las recomendaciones de reglas de políticas más recientes para sus dispositivos. Con la aplicación IoT Security (Seguridad de IoT), puede revisar estas recomendaciones de reglas de políticas y crear una política de seguridad para esos dispositivos. Después de activar las reglas de políticas en la aplicación IoT Security (Seguridad de IoT), impórtelas al cortafuegos o Panorama y confirme su política de seguridad.

El cortafuegos debe poder observar el tráfico de difusión y unidifusión DHCP en su red para identificar dispositivos. Cuanto más tráfico pueda observar el cortafuegos, más precisas serán las recomendaciones de reglas de políticas para el dispositivo y más rápidas y precisas serán las asignaciones de dirección IP a dispositivo para el dispositivo. Cuando un dispositivo envía tráfico DHCP para obtener una dirección IP, el cortafuegos observa ese tipo de solicitud, genera EAL para enviarlos a Cortex Data Lake para su procesamiento y que finalmente IoT Security (Seguridad de IoT) los analice.

Para observar el tráfico en una interfaz L2, debe configurar una VLAN para esa interfaz. El cortafuegos permite tratar la interfaz como una interfaz L3 para un relé DHCP, por lo que podrá observar el tráfico de transmisión DHCP sin que el tráfico o el rendimiento se vean afectados.

Puesto que el cortafuegos necesita detectar los dispositivos en función de su tráfico y, luego, hacer cumplir la política de seguridad para esos dispositivos, el cortafuegos actúa como un *sensor* para recopilar metadatos de los dispositivos y un *ejecutor* que hace cumplir su política de seguridad para los dispositivos. La aplicación IoT Security (Seguridad de IoT) detecta automáticamente nuevos dispositivos tan pronto como envían tráfico DHCP y puede identificar el 95 % de los dispositivos durante la primera semana.

Cada aplicación tiene una recomendación individual que puede importar al cortafuegos o Panorama como regla. Cuando importa la recomendación, el cortafuegos o Panorama crean al menos dos objetos para definir el comportamiento del dispositivo a partir de la recomendación:

- Un objeto de dispositivo de origen que identifica el dispositivo donde se origina el tráfico.
- Uno o más objetos de destino que identifican los destinos permitidos para el tráfico, que pueden ser un dispositivo, una dirección IP o un nombre de dominio completo (FQDN, Fully Qualified Domain Name).

© 2020 Palo Alto Networks, Inc.

Si alguno de los objetos del dispositivo ya existe en el cortafuegos o Panorama, el cortafuegos o Panorama actualizan el objeto del dispositivo en lugar de crear un nuevo objeto de dispositivo. Puede utilizar estos objetos de dispositivo en las políticas de seguridad, autenticación, descifrado y calidad de servicio (QoS, Quality of Service).

El cortafuegos también asocia etiquetas que identifican el dispositivo de origen y que la regla es una recomendación de regla de políticas de IoT Security (Seguridad de IoT).



No edite ni elimine las etiquetas, ya que las etiquetas asociadas con la regla son la única forma de restaurar sus asignaciones si se desincronizan.

Para una implementación y operación óptimas de Device-ID, recomendamos las siguientes prácticas:

- Implemente Device-ID en cortafuegos que estén ubicados centralmente en su red. Por ejemplo, si tiene un entorno grande, implemente Device-ID en un cortafuegos de subida del dispositivo de gestión de direcciones IP (IPAM, IP Address Management). Si tiene un entorno pequeño, implemente Device-ID en un cortafuegos que actúe como servidor DHCP.
- Durante la implementación inicial, permita que Device-ID recopile metadatos de su red durante al menos catorce días. Si los dispositivos no están activos a diario, el proceso de identificación puede tardar más.
- Escriba la política basada en dispositivos siguiendo el orden de dispositivos más críticos a menos críticos. Priorice por:
  1. Clase (primero, los dispositivos en red seguros)
  2. Dispositivos críticos (como servidores o máquinas de resonancia magnética)
  3. Dispositivos específicos del entorno (como alarmas contra incendios y lectores de credenciales)
  4. Dispositivos de IoT orientados al consumidor (como un smartwatch o un altavoz inteligente)
- Habilite Device-ID por zona solo para zonas internas.

© 2020 Palo Alto Networks, Inc.

Preparación para la implementación de Device-ID

Para preparar su red para la implementación de Device-ID, complete las siguientes tareas previas para permitir que su cortafuegos genere y envíe logs de aplicaciones mejoradas (EAL, Enhanced Application Logs) a Cortex Data Lake para que IoT Security (Seguridad de IoT) los procese y los analice para la generación de recomendaciones de reglas de políticas.

STEP 1 | Si aún no lo ha hecho, instale el certificado del dispositivo en el cortafuegos o Panorama.

STEP 2 | Active su instancia de Cortex Data Lake (CDL) y conecte el cortafuegos a la instancia.

1. Active una instancia de Cortex Data Lake.
2. Conecte el cortafuegos a Cortex Data Lake.

STEP 3 | (Solo interfaces L2) Cree una interfaz VLAN para cada interfaz L2 para que el cortafuegos pueda observar el tráfico de transmisión DHCP.

STEP 4 | (Opcional) Configure una ruta de servicio para permitir el tráfico necesario para Device-ID y IoT Security (Seguridad de IoT).

De forma predeterminada, el cortafuegos utiliza la interfaz de gestión. Para usar una interfaz diferente, complete los siguientes pasos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y, a continuación, seleccione **Service Route Configuration (Configuración de ruta de servicio)**.
2. Seleccione **Customize (Personalizar)** para personalizar una ruta de servicio.
3. Seleccione el protocolo **IPv4**.

   Device-ID e IoT Security (Seguridad de IoT) no son compatibles con IPv6.
4. Seleccione **Data Services (Servicios de datos)** en la columna Service (Servicio).
5. Seleccione una **interfaz de origen** y una **dirección de origen**.
6. Haga clic en **OK** dos veces.

STEP 5 | Utilice App-ID para permitir el tráfico necesario para Device-ID e IoT Security (Seguridad de IoT).

- Utilice el App-ID **`paloalto-iot-security`** para permitir el tráfico entre la aplicación de IoT Security (Seguridad de IoT) y el cortafuegos o Panorama.

  Este App-ID no es necesario si el cortafuegos envía tráfico desde la interfaz de gestión a través de una interfaz de datos en la misma zona que CDL e IoT Security (Seguridad de IoT), solo si el tráfico atraviesa más de una zona de seguridad.
- Utilice el App-ID **`paloalto-logging-service`** para permitir el tráfico para todos los EAL y todos los logs de sesión.
- Utilice el App-ID **`paloalto-updates`** para permitir la recuperación de actualizaciones dinámicas de seguridad de IoT y actualizaciones del diccionario de dispositivos.
- Utilice el App-ID **`paloalto-iot-security`** para permitir la recuperación de recomendaciones de reglas de políticas.

© 2020 Palo Alto Networks, Inc.



Si tiene un cortafuegos que no es de Palo Alto Networks entre el cortafuegos que usa Device-ID e Internet, verifique que el cortafuegos que no sea de Palo Alto Networks pueda acceder a iot.services-edge.paloaltonetworks.com:443.

STEP 6 | Configure el cortafuegos para observar y generar logs para el tráfico DHCP y, a continuación, reenviar los logs para su procesamiento y análisis mediante IoT Security (Seguridad de IoT).

- Si el cortafuegos actúa como servidor DHCP:
  1. Habilite los logs de aplicaciones mejorados.
  2. Cree un perfil de reenvío de logs para reenviar los logs a CDL para su procesamiento.
  3. Habilite la opción **DHCP Broadcast Session (Sesión de difusión de DHCP)** (**Device [Dispositivo]** > **Setup [Configuración]** > **Session [Sesión]** > **Session Settings [Configuración de sesión]**).
  4. Cree una regla de política de seguridad para permitir **dhcp** como el tipo de **aplicación**
- Si el cortafuegos no es un servidor DHCP, configure una interfaz como agente de retransmisión DHCP para que el cortafuegos pueda generar EAL para el tráfico DHCP que recibe de los clientes.
- Si su servidor DHCP está en el mismo segmento de red que la interfaz del cortafuegos, implemente una interfaz de cable virtual frente al servidor DHCP para asegurarse de que el cortafuegos genere EAL para todos los paquetes en el intercambio DHCP inicial con un impacto mínimo en el rendimiento.
  1. Configure una interfaz de cable virtual con las zonas correspondientes y habilite la opción **Multicast Firewalling (Cortafuegos de multidifusión)** (**Network [Red]** > **Virtual Wires [Cables virtuales]** > **Add [Añadir]**).
  2. Configure una regla para permitir el tráfico DHCP hacia el servidor DHCP y, desde él, entre las zonas de cables virtuales. La política debe permitir todo el tráfico existente que el servidor observa actualmente y utilizar el mismo perfil de reenvío de logs que el resto de sus reglas.
  3. Para permitir que los servidores DHCP verifiquen si una dirección IP está activa antes de asignarla como una concesión a una nueva solicitud, configure una regla para permitir pings desde el servidor DHCP al resto de la subred.
  4. Configure una regla para permitir el resto del tráfico hacia el servidor DHCP, y desde él, que no reenvíe logs para coincidencias de tráfico.
  5. Configure el host del servidor DHCP para usar la primera interfaz de cable virtual y el conmutador de red para usar la segunda interfaz de cable virtual. Para minimizar el cableado, puede usar una VLAN aislada en la infraestructura de conmutación en lugar de conectar el host del servidor DHCP directamente al cortafuegos.
- Si desea utilizar una interfaz de Tap para obtener visibilidad del tráfico DHCP que el cortafuegos no suele observar debido a la configuración o topología actual de la red, utilice la siguiente configuración como práctica recomendada.
  1. Configure una interfaz de Tap y la zona correspondiente.
  2. Configure una regla para que coincida con el tráfico DHCP que utiliza el mismo perfil de reenvío de logs que el resto de sus reglas.
  3. Para minimizar la carga de la sesión en el cortafuegos, configure una regla para eliminar el resto del tráfico.
  4. Conecte la interfaz de Tap al reflejo del puerto en el conmutador de red.

STEP 7 | Añada tipos de logs de sesión al perfil de reenvío de logs.

Si no existen entradas en el perfil de reenvío de logs, al seleccionar la opción **Enable enhanced application logging to Cortex Data Lake (including traffic and url logs) [Habilitar creación de logs mejorados de aplicaciones (incluidos logs de tráfico y URL)]**, se añaden todos los tipos de logs.

1. **Añada** un nuevo perfil y especifique un nombre.
2. Seleccione **traffic (tráfico)** como **Log type (Tipo de log)**.

© 2020 Palo Alto Networks, Inc.

3. Seleccione **All logs (Todos los logs)** como **Filter (Filtro)**.
4. Seleccione la opción **Cortex Data Lake**.
5. Haga clic en **OK (Aceptar)**.
6. Repita los subpasos del 1 al 5 para la **amenaza** y, si dispone de una suscripción, los tipos de logs de **wildfire**.

© 2020 Palo Alto Networks, Inc.

Configuración de Device-ID

Complete las siguientes tareas para importar las asignaciones de dirección IP a dispositivo y las recomendaciones de reglas de políticas de IoT Security (Seguridad de IoT) a su cortafuegos o Panorama.

STEP 1 | Active su licencia de IoT Security (Seguridad de IoT) en el hub.

1. Siga las instrucciones que recibió en el correo electrónico para activar su licencia de seguridad de IoT Security (Seguridad de IoT).
2. Inicialice su aplicación de IoT Security (Seguridad de IoT). Para obtener más información, consulte Introducción a IoT Security (Seguridad de IoT) y Prácticas recomendadas de IoT Security (Seguridad de IoT).
3. Aplique la licencia a los cortafuegos que desee utilizar para hacer cumplir la política de IoT Security (Seguridad de IoT).
4. Actualice su licencia en el cortafuegos o Panorama.

STEP 2 | Defina su política de IoT Security (Seguridad de IoT) en la aplicación de IoT Security (Seguridad de IoT).

1. En la aplicación de IoT Security (Seguridad de IoT), seleccione el objeto de dispositivo de origen.
2. **Cree** un nuevo conjunto de reglas de política para el objeto de dispositivo de origen.

   Para obtener más información sobre la seguridad de IoT, consulte Introducción a la seguridad de IoT.
3. **Active** las reglas de la política para confirmar sus cambios.

STEP 3 | Importe las asignaciones de dirección IP a dispositivo y las recomendaciones de reglas de política al cortafuegos o Panorama.

1. Importe la recomendación de la regla de política.
   - En el cortafuegos, seleccione **Device (Dispositivo)** > **Policy Recommendation (Recomendación de políticas)**.
   - Para Panorama, seleccione **Panorama** > **Policy Recommendation (Recomendación de políticas)** y, a continuación, envíe las reglas de política a los cortafuegos que administra Panorama.

   Después de enviar la política a los cortafuegos, debe sincronizar las reglas de política en los cortafuegos para crear la asignación de la regla de la política a la regla de la política.

   Cuando seleccione Policy Recommendation (Recomendación de políticas), el cortafuegos o Panorama se comunicará con IoT Security (Seguridad de IoT) para obtener las recomendaciones de reglas de política más recientes. Las recomendaciones de reglas de política no se almacenan en caché en el cortafuegos o Panorama.

   Debido a que IoT Security (Seguridad de IoT) crea la recomendación de la regla de políticas mediante el comportamiento de confianza para el dispositivo, la acción predeterminada para la regla es permitir.
2. Seleccione el **perfil del dispositivo de origen**.
3. Verifique que el **perfil del dispositivo de destino** y las **aplicaciones** permitidas sean correctos.
4. Seleccione **Importar reglas de políticas** para importar las reglas de políticas.
5. (Solo Panorama) Seleccione la **ubicación** del grupo de dispositivos donde desee importar las reglas de políticas.
6. Introduzca un **nombre** para las reglas de políticas.
7. (Solo en Panorama) Seleccione el **tipo de destino** (**Pre-Rulebase [Base de reglas previa]** o **Post-Rulebase [Base de reglas posterior]**).

© 2020 Palo Alto Networks, Inc.

8. Seleccione **After Rule (Después de la regla)** para definir la ubicación de la regla en la base de reglas.
   - **No Rule Selection (Sin selección de regla)**: coloca la regla en la parte superior de la base de reglas.
   - **Default One (Predeterminado)**: coloca la regla después de la regla que aparece.

   En su política de seguridad, las reglas de Device-ID deben preceder a cualquier regla existente que se aplique a los dispositivos.
9. Repita este proceso para cada recomendación de regla de políticas para crear reglas que permitan el acceso de cada objeto de dispositivo a los destinos necesarios.
10. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 4 | Habilite Device-ID en cada zona donde desee usar Device-ID para detectar dispositivos y hacer cumplir su política de seguridad.

De forma predeterminada, Device-ID asigna todas las subredes en las zonas donde lo habilita. Puede modificar qué subredes asigna Device-ID en la **lista de inclusión** y la **lista de exclusión**.

Como práctica recomendada, habilite Device-ID en la zona de origen para detectar dispositivos y hacer cumplir la política de seguridad. Solo debe habilitar Device-ID para zonas internas.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Seleccione la zona donde desee habilitar Device-ID.
3. **Habilite la identificación del dispositivo** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 5 | **Commit (Confirmar)** los cambios.

STEP 6 | Verifique que su política de seguridad sea correcta.

1. Seleccione **Policies (Políticas)** y, a continuación, seleccione la regla que creó a partir de la recomendación de regla de políticas.

   IoT Security asigna una **descripción** que contiene el objeto de dispositivo de origen y las **etiquetas** para identificar el objeto de dispositivo de origen y que esta regla sea una recomendación de IoT Security (Seguridad de IoT).

   Los nombres de los objetos de dispositivo deben ser únicos.
2. Seleccione la pestaña **Source (Origen)** y, a continuación, verifique el **perfil del dispositivo de origen**.
3. Seleccione la pestaña **Destination (Destino)** y verifique el **perfil del dispositivo de destino**.
4. Seleccione la pestaña **Application (Aplicación)** y verifique las **aplicaciones**.
5. Seleccione la pestaña **Actions (Acciones)** y verifique la **acción** (el valor predeterminado es **Allow [Permitir]**).
6. Utilice Explore (Explorar) para verificar que CDL recibe sus logs y revisar los logs que CDL recibe.

STEP 7 | Cree objetos de dispositivo personalizados para cualquier dispositivo que no tenga recomendaciones de reglas de la política de IoT Security (Seguridad de IoT).

Por ejemplo, no puede proteger dispositivos como ordenadores portátiles y smartphones mediante recomendaciones de reglas de políticas, por lo que debe crear manualmente objetos de dispositivo para que estos tipos de dispositivos los utilicen en su política de seguridad. Para obtener más información sobre los objetos de dispositivo personalizados, consulte Gestión de Device-ID.

STEP 8 | Utilice los objetos de dispositivo para hacer cumplir las reglas de políticas y para supervisar e identificar problemas potenciales.

La siguiente lista incluye algunos casos de uso de ejemplo para objetos de dispositivo.

© 2020 Palo Alto Networks, Inc.

- Utilice objetos de dispositivo de origen y objetos de dispositivo de destino en las políticas de seguridad, autenticación, QoS y descifrado.
- Utilice el log de descifrado para identificar errores y conocer los activos con un descifrado más crítico.
- Vea la actividad de los objetos de dispositivo en ACC para realizar un seguimiento de los nuevos dispositivos y su comportamiento.
- Utilice objetos de dispositivo para crear un informe personalizado (por ejemplo, para informes de incidentes o auditorías).

© 2020 Palo Alto Networks, Inc.

Gestión de Device-ID

Realice las siguientes tareas según sea necesario para asegurarse de que sus recomendaciones de reglas de políticas y los objetos de dispositivo estén actualizados, o para restaurar las asignaciones de recomendaciones de reglas de políticas.

STEP 1 | Actualice su recomendación de regla de políticas siempre que la columna **New Updates Available (Nuevas actualizaciones disponibles)** muestre **Yes (Sí)** para esa recomendación.

A medida que los dispositivos adquieran nuevas capacidades, IoT Security actualizará las recomendaciones de reglas de políticas para aconsejar qué tráfico o protocolos adicionales deben permitir el cortafuegos o Panorama. Consulte la seguridad de IoT diariamente para obtener actualizaciones y actualice sus recomendaciones de reglas de políticas lo antes posible.

1. En la aplicación IoT Security (Seguridad de IoT), **edite** las reglas de políticas y, a continuación, haga clic en **Next (Siguiente)**.
2. Seleccione la nueva recomendación y, a continuación, haga clic en **Next (Siguiente)**.
3. Haga clic en **Save (Guardar)** para guardar sus cambios.
4. En el cortafuegos o Panorama, haga clic en **Import Policy Rules (Importar reglas de políticas)** y, a continuación, haga clic en **Yes (Sí)** para confirmar que desea sobrescribir la regla actual.

   Esta acción sobrescribe la recomendación de la regla, no la regla en sí.
5. (Solo en Panorama) Repita el paso anterior para todos los grupos de dispositivos.
6. **Commit (Confirmar)** los cambios.

STEP 2 | Revise, actualice y mantenga los objetos del dispositivo en el diccionario de dispositivos.

Debe crear objetos de dispositivo para cualquier dispositivo que no tenga una recomendación de regla de la política de seguridad de IoT. Por ejemplo, no puede proteger dispositivos como ordenadores portátiles y smartphones mediante las recomendaciones de reglas de la política de seguridad de IoT, por lo que debe crear objetos de dispositivo para este tipo de dispositivos y usarlos en su política de seguridad para proteger esos dispositivos.

1. Seleccione **Objects (Objetos)** > **Devices (Dispositivos)**.
2. **Añada** un objeto de dispositivo.
3. **Examine** la lista o **busque** mediante palabras clave.

   Los resultados de la búsqueda pueden incluir varios tipos de atributos de objetos de dispositivo (por ejemplo, **Category [Categoría]** y **Profile [Perfil]**).
4. Para añadir un objeto de dispositivo personalizado, especifique un **nombre** y, opcionalmente, una **descripción** para el objeto de dispositivo.

   Utilice siempre un nombre único para cada objeto de dispositivo. No cambie las etiquetas en la descripción de los objetos de dispositivo de las recomendaciones de reglas de políticas.
5. (Solo en Panorama) Seleccione la opción **Shared (Compartido)** para que este objeto de dispositivo esté disponible para otros grupos de dispositivos.
6. Seleccione los atributos para el objeto de dispositivo (**Category [Categoría]**, **OS**, **Profile [Perfil]**, **Osfamily [Familia del SO]**, **Model [Modelo]** y **Vendor [Proveedor]**).
7. Haga clic en **OK (Aceptar)** para confirmar los cambios.

© 2020 Palo Alto Networks, Inc.

STEP 3 | En algunos casos (por ejemplo, si restaura una configuración anterior), las asignaciones de recomendaciones de regla de políticas a regla de políticas pueden perder la sincronización. También debe sincronizar las asignaciones en cada cortafuegos después de enviar las reglas de políticas de Panorama a los cortafuegos que gestiona Panorama. Para sincronizar las asignaciones, realice los siguientes pasos:

- En el cortafuegos, seleccione **Device (Dispositivo)** > **Policy Recommendation (Recomendación de políticas)** > **Sync Policy Rules (Reglas de políticas de sincronización)**.
- Para Panorama, seleccione **Panorama** > **Policy Recommendation (Recomendación de políticas)** > **Sync Policy Rules (Reglas de políticas de sincronización)**.

El cortafuegos o Panorama escanea todas las reglas en la base de reglas para buscar etiquetas que identifiquen una regla como una recomendación de regla de la política de seguridad de IoT, obtiene la información del objeto del dispositivo de origen y vuelve a llenar la base de datos de recomendación de regla de políticas local.

STEP 4 | Elimine las recomendaciones de reglas de políticas que ya no sean necesarias.

Si una recomendación de regla de políticas ya no se aplica, puede eliminarla. También debe eliminar la regla de la recomendación de regla de políticas para hacer cumplir la política de seguridad actualizada.

1. En la aplicación de seguridad de IoT, seleccione **Delete (Eliminar)**.
2. Haga clic en **Mark as Removed (Marcar como eliminado)** para seleccionar esta recomendación para su eliminación.
3. Elimine la asignación.
   - En el cortafuegos, seleccione **Device (Dispositivo)** > **Policy Recommendation (Recomendación de políticas)** > **Remove Policy Mapping (Eliminar asignación de políticas)**.
   - Para Panorama, seleccione **Device (Dispositivo)** > **Policy Recommendation (Recomendación de políticas)** > **Remove Policy Mapping (Eliminar asignación de políticas)** y, a continuación, seleccione la **ubicación** desde la que desee eliminar la asignación.
4. Haga clic en **Yes (Sí)** para confirmar la eliminación de la asignación.
5. Seleccione **Policies (Políticas)** > **Security (Seguridad)**. Para Panorama, seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Pre-Rules/Post-Rules (Reglas previas/Reglas posteriores)**.
6. Seleccione la regla para la recomendación de regla de políticas que desee eliminar y, a continuación, seleccione **Delete (Eliminar)**.
7. **Commit (Confirmar)** los cambios.

STEP 5 | Utilice comandos de la CLI para solucionar cualquier problema entre el cortafuegos y la seguridad de IoT.

© 2020 Palo Alto Networks, Inc.

Comandos de la CLI para Device-ID

Utilice los siguientes comandos de la CLI para ver información para solucionar cualquier problema entre el cortafuegos e IoT Security (Seguridad de IoT). En general, los comandos de la CLI que incluyen **eal** muestran contadores para datos salientes y los comandos de la CLI que incluyen **icd** muestran contadores para datos entrantes.

Ejemplo	Comando
Visualice contadores de creación de logs de aplicaciones mejoradas (EAL, Enhanced Application Logging), como el número de conexiones entre el cortafuegos y Cortex Data Lake y el volumen de los logs.	**show iot eal all**
Obtenga más información sobre la conexión entre el cortafuegos y Cortex Data Lake.	**show iot eal conn**
Vea un resumen de los contadores EAL por plano (plano de datos o plano de gestión), como la versión de PAN-OS y el número de serie.	**show iot eal dpi-eal**
Consulte los contadores de EAL por plano (plano de datos o plano de gestión) y por protocolo.	**show iot eal dpi-stats all**
Visualice los contadores de EAL por protocolo.	**show iot eal dpi-stats subtype dhcp|http**
Obtenga un resumen de los contadores del informe de coincidencias del perfil de información de host (HIP, Host Information Profile).	**show iot eal hipreport-eal**
Vea los contadores de tiempo de respuesta del log de EAL.	**show iot eal response-time**
Consulte los detalles del estado de la conexión al servicio perimetral entre el cortafuegos y la aplicación de IoT Security (Seguridad de IoT) y contadores para las asignaciones de dirección IP a dispositivo y recomendaciones de reglas de políticas.	**show iot icd statistics all**
Visualice los contadores para la conexión al servicio perimetral.	**show iot icd statistics conn**
Vea los contadores para las asignaciones de dirección IP a dispositivo.	**show iot icd statistics verdict**
Visualice todas las asignaciones de dirección IP a dispositivo en el cortafuegos.	**show iot ip-device-mapping-mp all**
Vea la asignación de dirección IP a dispositivo para una dirección IP específica.	**show iot ip-device-mapping-mp ip *IP-address***

© 2020 Palo Alto Networks, Inc.

Ejemplo	Comando
Visualice una lista de asignaciones de dirección IP a dispositivo en el plano de datos.	`show iot ip-device-mapping all`
Borre las asignaciones de dirección IP a dispositivo en el plano de gestión.	`debug iot clear-all type device`
Borre las asignaciones de dirección IP a dispositivo en el plano de datos.	`clear user-cache all`

© 2020 Palo Alto Networks, Inc.

Threat Prevention

El cortafuegos de última generación de Palo Alto Networks protege y defiende su red ante amenazas de productos y amenazas avanzadas persistentes (APT). Los mecanismos de detección con varios elementos del cortafuegos incluyen un enfoque basado en firmas (IPS/comando y control/antivirus), un enfoque basado en la heurística (detección de bots), un enfoque basado en Sandbox (WildFire) y un enfoque basado en análisis con el protocolo de capa 7 (App-ID).

Las amenazas de productos son explotaciones menos sofisticadas que se detectan y previenen con mayor facilidad con una combinación de funciones de antivirus, antispyware y protección contra vulnerabilidades, además de filtrado de URL e identificación de aplicaciones del cortafuegos.

Las amenazas avanzadas son cometidas por cibercriminales organizados que utilizan vectores de ataque sofisticados que tienen como objetivo su red, habitualmente para robar propiedad intelectual y datos financieros. Estas amenazas son más evasivas y requieren mecanismos de supervisión inteligentes para realizar una investigación detallada de host y de red en busca de software malintencionado. El cortafuegos de última generación de Palo Alto Networks, junto con WildFire™ y Panorama™, brinda una solución completa que intercepta y detiene la cadena de ataque, y ofrece visibilidad para evitar un incumplimiento de la seguridad en su infraestructura de red, tanto móvil como virtualizada.



Después de implementar la configuración de prevención contra amenazas, puede realizar la Exportación de los datos de la tabla de configuración para crear un informe en PDF o CSV de la configuración que se utilizará para una revisión o auditoría interna.

- Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7
- Configuración de antivirus, antispyware y protección frente a vulnerabilidades
- DNS Security
- Uso de consultas de DNS para identificar hosts infectados en la red
- Configuración de filtrado de datos
- Patrones predefinidos de filtrado de datos
- Creación de perfiles de filtrado de datos
- WildFire Inline ML
- Configuración de bloqueo de archivos
- Prevención de ataques de fuerza bruta
- Personalización de la acción y las condiciones de activación para una firma de fuerza bruta
- Habilitación de las firmas de evasión
- Supervisión de direcciones IP bloqueadas
- Categorías de firma de amenazas
- Creación de excepciones de amenazas
- Firmas personalizadas
- Obtenga más información y evalúe las amenazas
- Uso compartido de inteligencia de amenazas con Palo Alto Networks
- Recursos de prevención de amenazas

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7

Para supervisar y proteger su red de la mayoría de ataques de capa 4 y capa 7, aquí tiene un par de recomendaciones.

- Actualice a la última versión del software PAN-OS y la última versión de publicación de contenido para asegurarse de que tiene las últimas actualizaciones de seguridad. Consulte Instalación de las actualizaciones de contenido y software.
- Habilitación de DNS Security (requiere una licencia de suscripción de prevención de amenazas y seguridad DNS) para hundir solicitudes de DNS maliciosas. Palo Alto Networks recomienda utilizar las siguientes opciones de configuración de la categoría de seguridad DNS en su perfil de antispyware:

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	critical	sinkhole	extended-capture
Dynamic DNS Hosted Domains	medium	sinkhole	disable
Grayware Domains	high	sinkhole	disable
Malware Domains	high	sinkhole	disable
Parked Domains	medium	sinkhole	disable
Phishing Domains	high	sinkhole	disable
Newly Registered Domains	medium	sinkhole	disable

  - Para la configuración de la gravedad de logs, utilice la siguiente configuración:
    - Establezca Command and Control Domains (Dominios de comando y control) en **critical (crítico)**.
    - Establezca Grayware Domains (Dominios de grayware), Malware Domains (Dominios de malware) y Phishing Domains (Dominios de phishing) en high (alto).
    - Configure Dynamic DNS Hosted Domain (Dominios alojados de DNS dinámico), Newly Registered Domains (Dominios recién registrados) y Parked Domains (Dominios estacionados) en medium (medio).
  - Para la acción de política, configure todas las fuentes de firmas en **sinkhole**.
  - Para la captura de paquetes, configure Command and Control Domains (Dominios de comando y control) en **extended-capture** (captura ampliada). Deje todas las demás categorías en la configuración predeterminada.

  Para obtener más información sobre la configuración antispyware relacionada, consulte Perfil de antispyware recomendado para la puerta de enlace de Internet.
- Configure el cortafuegos para que actúe como proxy DNS y habilite las firmas de evasión.

  El proxy DNS no forma parte del motor de políticas de seguridad del cortafuegos; en su lugar, indica al cortafuegos que resuelva los nombres de host DNS mientras mantiene la asignación de dominio a IP, algo que es fundamental para evitar la evasión de TLS/HTTP.

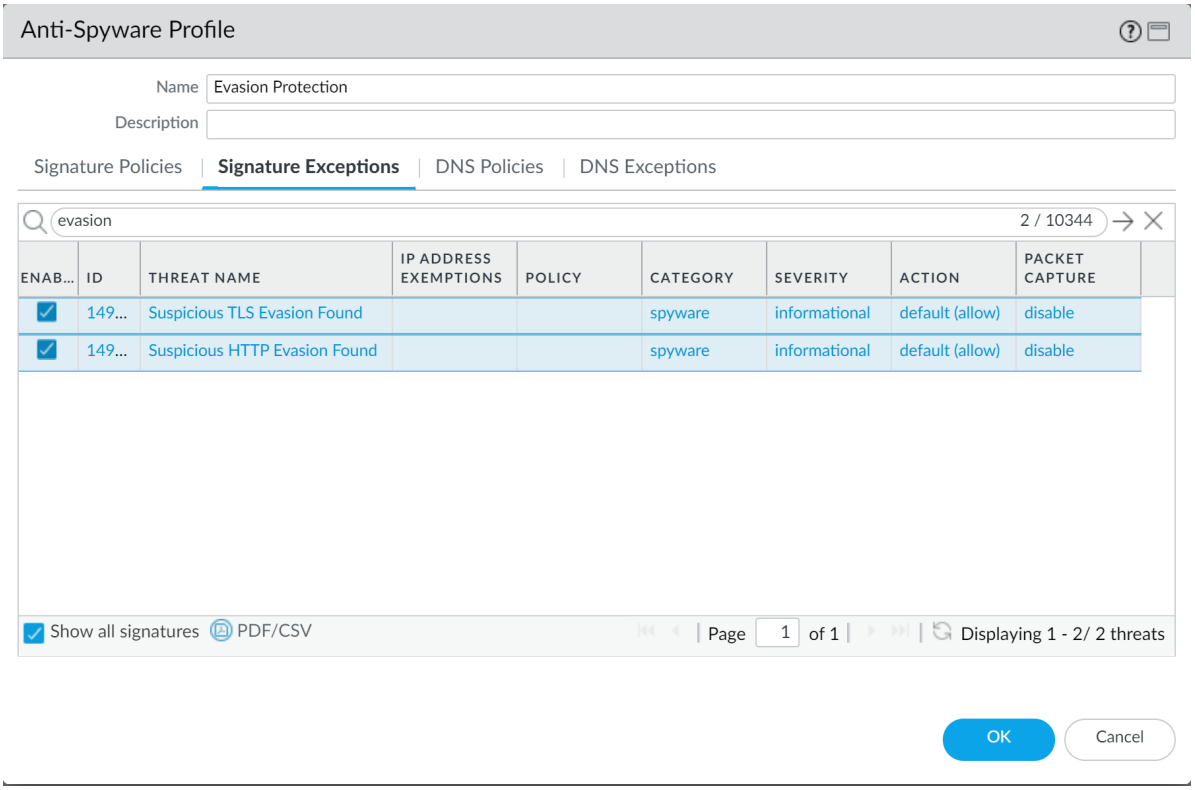
  - Configuración de un objeto proxy DNS.

    Cuando actúa como proxy DNS, el cortafuegos resuelve las solicitudes DNS y almacena en caché las asignaciones de nombre de host y direcciones IP para resolver de manera rápida y eficiente futuras consultas DNS.

© 2020 Palo Alto Networks, Inc.

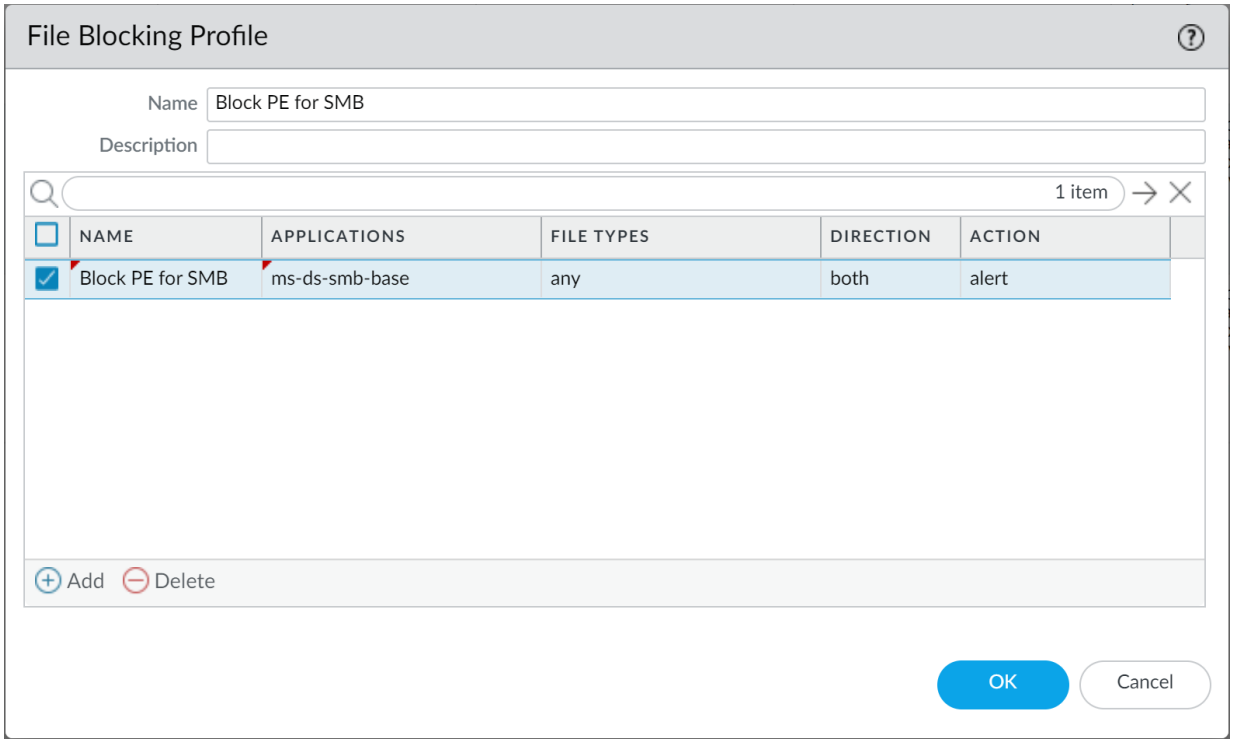
- Habilitación de las firmas de evasión

  Las firmas de evasión que detectan solicitudes HTTP o TLS elaboradas pueden enviar alertas cuando los clientes se conectan a un domino que no sea el dominio especificado en la solicitud DNS original. Asegúrese de configurar el proxy DNS antes de habilitar las firmas de evasión. Sin el proxy DNS, las firmas de evasión pueden activar alertas cuando un servidor DNS de la configuración de equilibrio de carga DNS devuelve direcciones IP diferentes (para los servidores que alojan recursos idénticos) al cortafuegos y cliente en respuesta a la misma solicitud DNS.

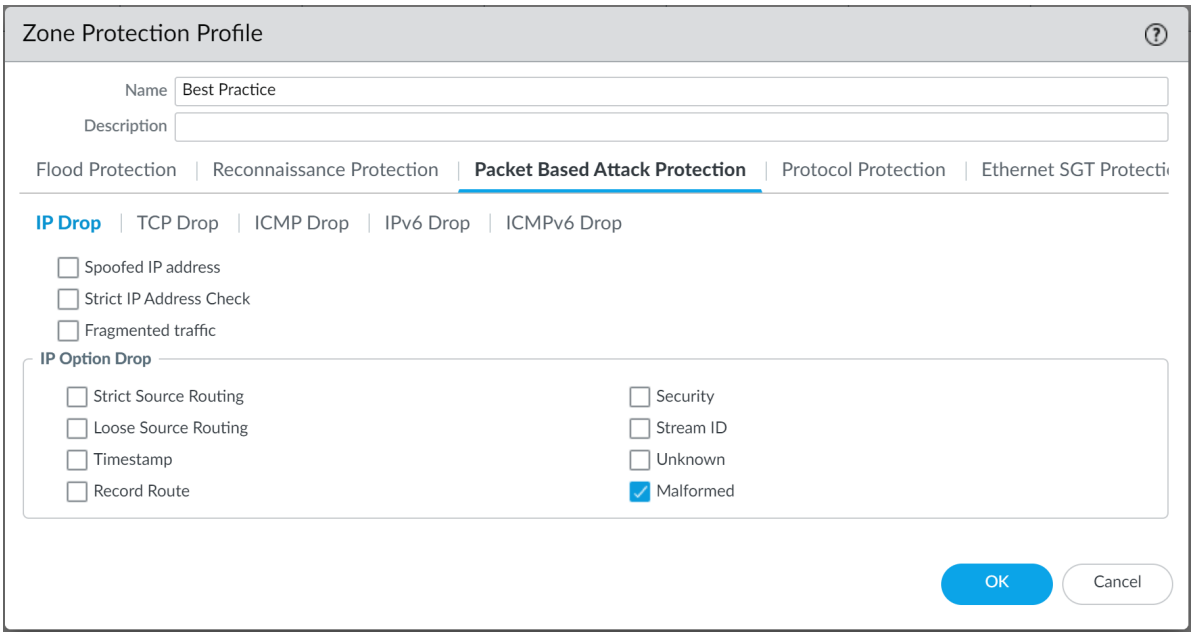


- Para los servidores, cree reglas de política de seguridad que permitan solo las aplicaciones que usted apruebe en cada servidor. Verifique que el puerto estándar para la aplicación coincida con el puerto de escucha del servidor. Por ejemplo, para garantizar que solo se permita el tráfico SMTP en su servidor de correo electrónico, configure la aplicación en **smtp** y configure el servicio en **application-default**. Si su servidor utiliza solo un subconjunto de los puertos estándar (por ejemplo, si su servidor SMTP utiliza solo el puerto 587 mientras la aplicación SMTP tiene puertos estándar definidos como 25 y 587), cree un nuevo servicio personalizado que incluya solo el puerto 587 y utilice ese nuevo servicio en su regla de política de seguridad en lugar de la opción predeterminada de la aplicación Además, asegúrese de restringir el acceso a zonas de origen y destino específicas, y a conjuntos específicos de direcciones IP.
- Bloquee todas las aplicaciones o tráfico desconocidos mediante la política de seguridad. Normalmente, las únicas aplicaciones clasificadas como tráfico desconocido son aplicaciones internas o personalizadas de su red, o posibles amenazas. El tráfico desconocido puede ser una aplicación no compatible, un protocolo anómalo o anormal, o una aplicación conocida que utiliza puertos no estándar. En cualquiera de estos casos debe bloquearse. Consulte Gestión de aplicaciones personalizadas o desconocidas.
- Configure un bloqueo de archivo para impedir que los tipos de archivo portables ejecutables (Portable Executable, PE) para el tráfico de bloque de mensajes del servidor (Server Message Block, SMB) pasen de zonas fiables a zonas no fiables (aplicaciones ms-ds-smb).

© 2020 Palo Alto Networks, Inc.



- Bloquee variantes maliciosas de PE (ejecutables portátiles) y scripts de PowerShell en tiempo real. La habilitación de WildFire Inline ML le permite analizar archivos dinámicamente mediante el aprendizaje automático en el cortafuegos. Esta capa adicional de protección antivirus complementa las firmas basadas en WildFire para proporcionar una cobertura ampliada para archivos cuyas firmas aún no existen.
- Cree un perfil de protección de zona configurado para ofrecer protección frente a los ataques basados en paquetes (**Network [Red]** > **Network Profiles [Perfiles de red]** > **Zone Protection [Protección de zona]**):
  - Seleccione la opción para descartar los paquetes IP **Malformed (Con formato incorrecto)** (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **IP Drop [Descarte de IP]**).



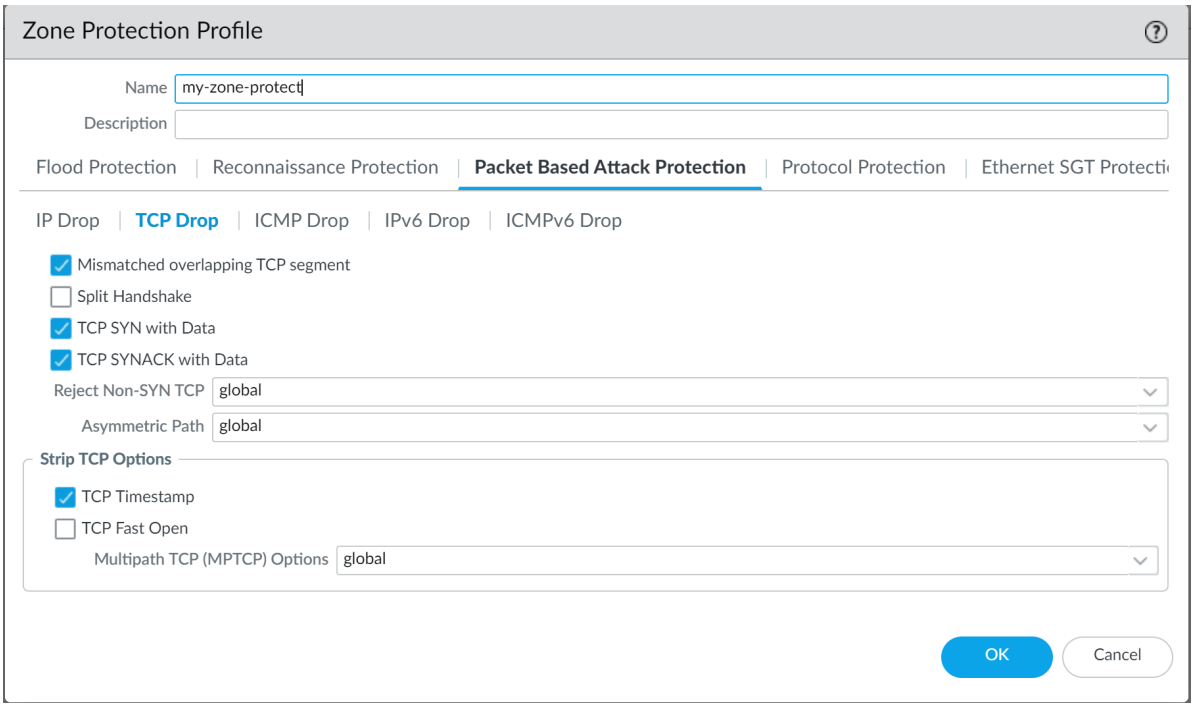
© 2020 Palo Alto Networks, Inc.

- Habilite la opción de descarte **Mismatched overlapping TCP segment (Segmento TCP superpuesto no coincidente)** (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **TCP Drop [Descarte de IP]**).

  Al establecer deliberadamente conexiones con datos superpuestos pero diferentes en ellas, los atacantes pueden intentar causar una interpretación equivocada de la intención de la conexión e inducir deliberadamente falsos positivos o falsos negativos. Los atacantes utilizan también la replicación de IP y la predicción de números de secuencia para interceptar la conexión de un usuario e introducir sus propios datos en la conexión. La selección de la opción **Mismatched overlapping TCP segment (Segmento TCP superpuesto no coincidente)** especifica que PAN-OS descarta las tramas con datos superpuestos y no coincidentes. Los segmentos recibidos son descartados cuando están dentro de otro segmento, cuando se superponen con parte de otro segmento o cuando contienen otro segmento completo.
- Habilite las opciones de descarte **TCP SYN with Data (TCP SYN con datos)** y **TCP SYNACK with Data (TCP SYNACK con datos)** (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **TCP Drop [Descarte de TCP]**).

  El descarte de paquetes SYN y SYN-ACK que contienen datos en la carga durante un protocolo de tres direcciones aumenta la seguridad al bloquear malware incluido en la carga y prevenir que extraiga datos no autorizados antes de que se complete el protocolo TCP.
- Quite las marcas de tiempo TCP de los paquetes SYN antes de que el cortafuegos envíe el paquete (**Packet Based Attack Protection [Protección contra ataque basado en paquetes]** > **TCP Drop [Descarte de TCP]**).

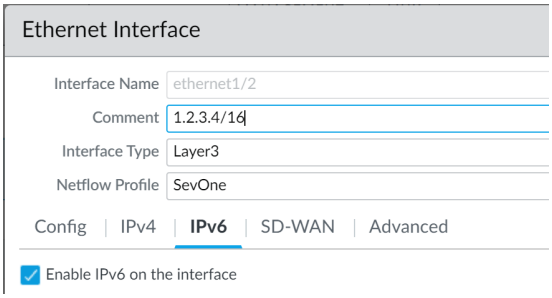
  Cuando habilita la opción **Strip TCP Options - TCP Timestamp (Quitar opciones TCP - Marca de tiempo TCP)**, la pila TCP en ambos extremos de la conexión TCP no admitirá marcas de tiempo TCP. Esto evita los ataques que utilizan distintas marcas de tiempo en varios paquetes para el mismo número de secuencia.



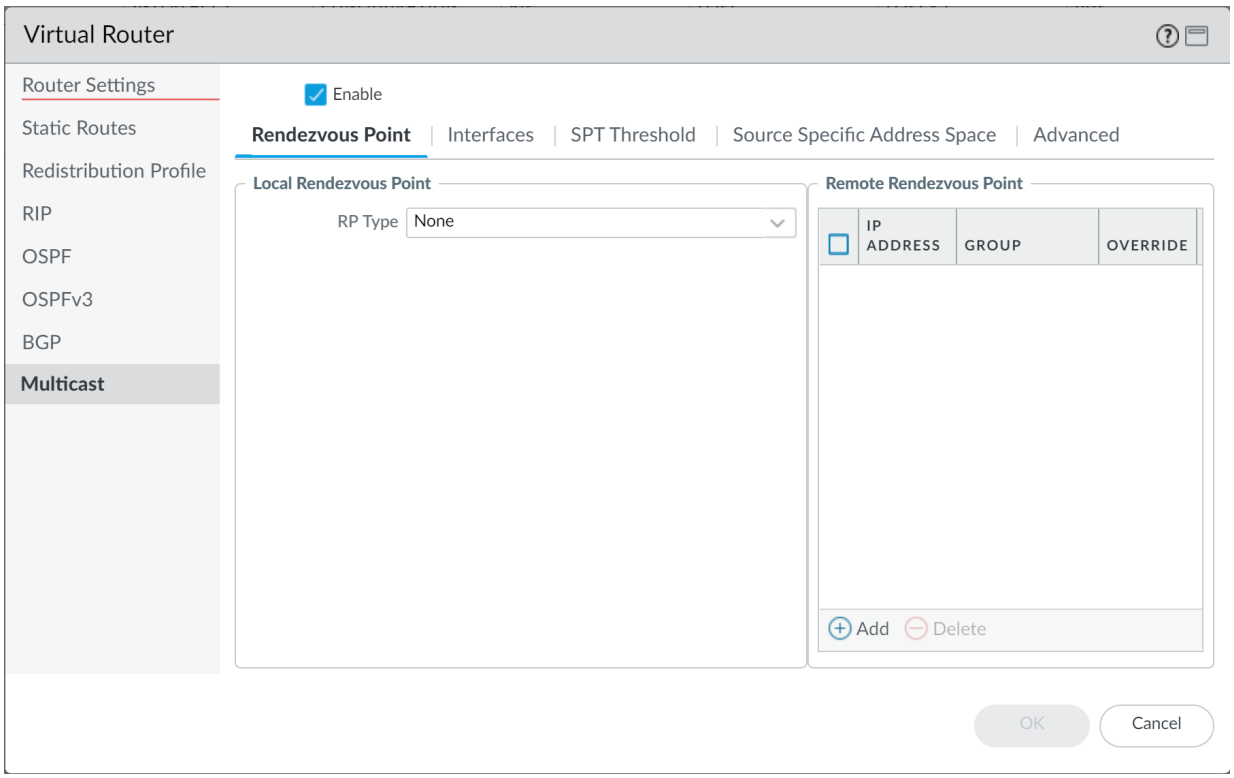
- ❑ Si configura direcciones IPv6 en sus hosts de red, asegúrese de habilitar el soporte para IPv6 si aún no está habilitado (**Network [Red]** > **Interfaces** > **Ethernet** > **IPv6**).

  La habilitación de la compatibilidad con IPv6 permite el acceso a hosts IPv6 y también filtra paquetes IPv6 encapsulados en paquetes IPv4, lo cual evita que las IPv6 en direcciones de multidifusión IPv4 se utilicen para el reconocimiento de la red.

© 2020 Palo Alto Networks, Inc.



- Habilite la compatibilidad con tráfico de multidifusión para que el cortafuegos pueda aplicar la política sobre tráfico de multidifusión (**Network [Red]** > **Virtual Router [Enrutador virtual]** > **Multicast [Multidifusión]**).



- Deshabilite las opciones **Forward datagrams exceeding UDP content inspection queue (Reenviar datagramas que superen la cola de inspección de contenido UDP)** y **Forward segments exceeding TCP content inspection queue (Reenviar segmentos que superen la cola de inspección de contenido TCP)**, disponibles en **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** > **Content-ID Settings (Configuración de Content-ID)**.

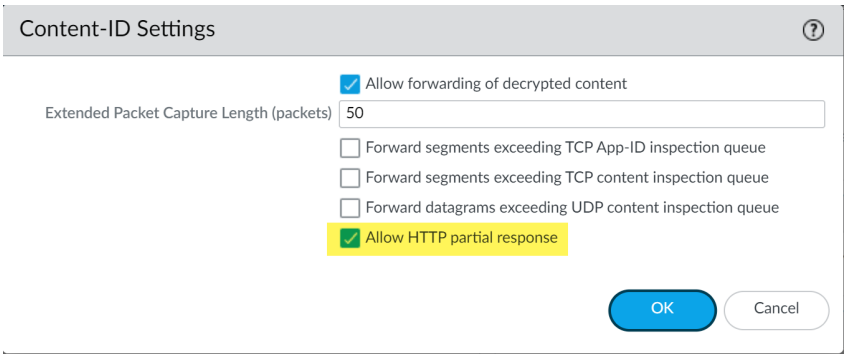
  De manera predeterminada, cuando la cola de inspección de contenido TCP o UDP está llena, el cortafuegos omite la inspección en los segmentos TCP o los datagramas UDP que superen el límite de la cola de 64. Si deshabilita esta opción, garantiza la inspección del contenido de todos los datagramas TCP y UDP que permite el cortafuegos. Solo en circunstancias concretas (por ejemplo, si la plataforma del cortafuegos no tiene el tamaño apropiado para un caso de uso), afecta al rendimiento deshabilitar este ajuste.
- Deshabilite **Allow HTTP partial response (Habilitar respuesta parcial HTTP)** (**Device [Dispositivo]** > **Setup [Configurar]** > **Content-ID [ID de contenido]** > **Content-ID Settings [Configuración de ID de contenido]**).

  La opción de respuesta parcial HTTP permite a un cliente recuperar solo parte de un archivo. Cuando un cortafuegos de próxima generación en una transferencia identifica y omite un archivo malicioso,

© 2020 Palo Alto Networks, Inc.

finaliza la sesión TCP con un paquete RST. Si el explorador web implementa la opción de intervalo de encabezado HTTP, puede comenzar una nueva sesión para recuperar solo la parte restante del archivo, lo cual evita que el cortafuegos active la misma firma nuevamente debido a la falta de contexto en la sesión inicial y, al mismo tiempo, permite que el explorador web vuelva a armar el archivo y envíe el contenido malintencionado. Al deshabilitar esta opción, evita que esto pase.

La inhabilitación de esta opción no debería afectar el rendimiento del dispositivo. Sin embargo, la recuperación de la interrupción de la transferencia del archivo HTTP podría verse afectada. Además, la inhabilitación de esta opción puede afectar los servicios de multimedia de transmisión, como Netflix, Windows Server Updates Services (WSUS) y las actualizaciones de contenido de Palo Alto Networks.



- Cree un perfil de protección contra vulnerabilidades para bloquear las anomalías de protocolo y todas las vulnerabilidades con gravedad baja y alta.

  Una anomalía de protocolo ocurre cuando el comportamiento de un protocolo se desvía del uso estándar y de cumplimiento. Por ejemplo, un paquete con formato incorrecto, una aplicación escrita de manera deficiente o una aplicación que se ejecuta en un puerto no estándar se considerarían anomalías y podrían usarse como herramientas de evasión.

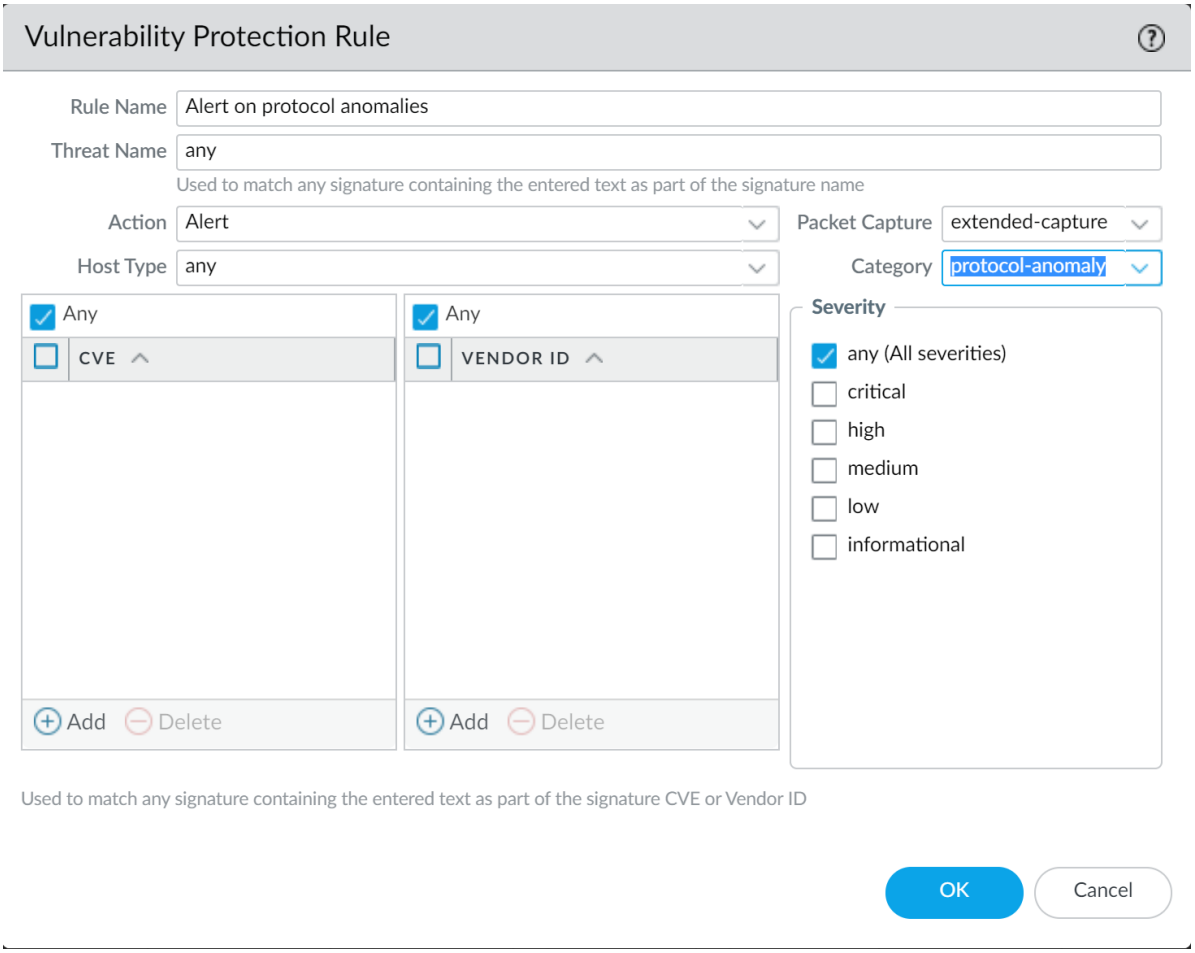
  Si su red es crítica; es decir, si la prioridad más alta de la empresa es la disponibilidad de la aplicación, debe comenzar por alertar sobre las anomalías del protocolo durante un periodo para garantizar que no haya aplicaciones internas críticas que utilicen protocolos establecidos de una manera no estándar. Si detecta que ciertas aplicaciones críticas activan firmas de anomalía de protocolo, puede excluir dichas aplicaciones del cumplimiento de anomalía de protocolo. Para esto, añada otra regla al perfil de protección de vulnerabilidades que permita las anomalías del protocolo y adjunte el perfil a la regla de política de seguridad que aplica el tráfico hacia y desde las aplicaciones críticas.

  Asegúrese de que las reglas del perfil de protección de vulnerabilidades y las reglas de la política de seguridad que permita las anomalías de protocolo para las aplicaciones internas críticas se indiquen por encima de las reglas que bloquean las anomalías de protocolo. El tráfico se evalúa en función de las reglas de política de seguridad y las reglas de los perfiles de protección de vulnerabilidades desde arriba hacia abajo, y se aplica en función de la primera regla de coincidencia.

  - Comience por alertas sobre las anomalías de protocolo:

    Cree una regla de perfil de protección de vulnerabilidades con la opción **Action (Acción)** configurada en Alert (Alerta), la opción **Category (Categoría)** configurada en protocol-anomaly (protocolo-anomalía) y la opción **Severity (Gravedad)** configurada en Any (Cualquiera). Supervise el tráfico para determinar si alguna aplicación interna crítica utiliza protocolos establecidos de maneras no estándar. Si detecta que esto es así, continúe permitiendo las anomalías de protocolo para dichas aplicaciones y luego bloquee las anomalías de protocolo para las demás aplicaciones.

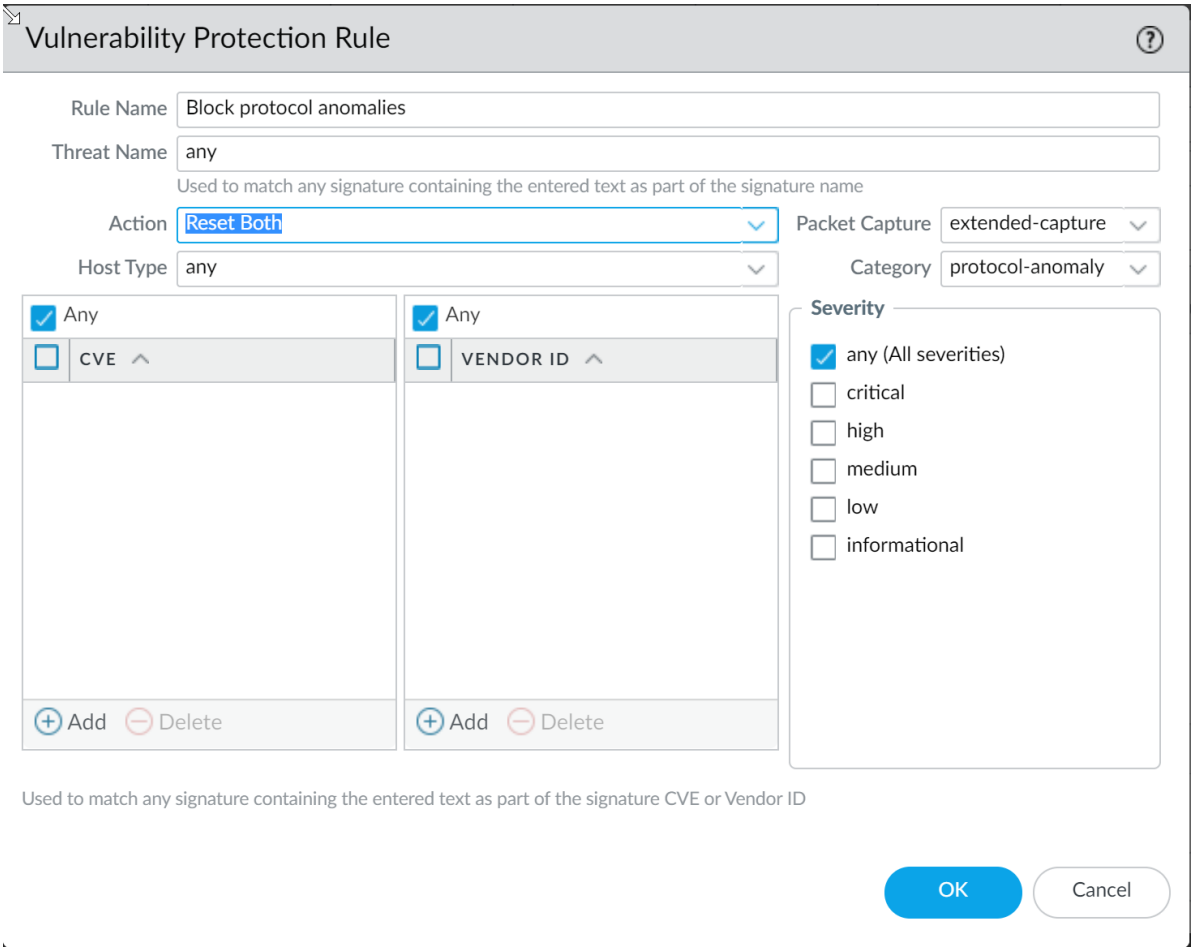
© 2020 Palo Alto Networks, Inc.



- Bloquee las anomalías de protocolo:

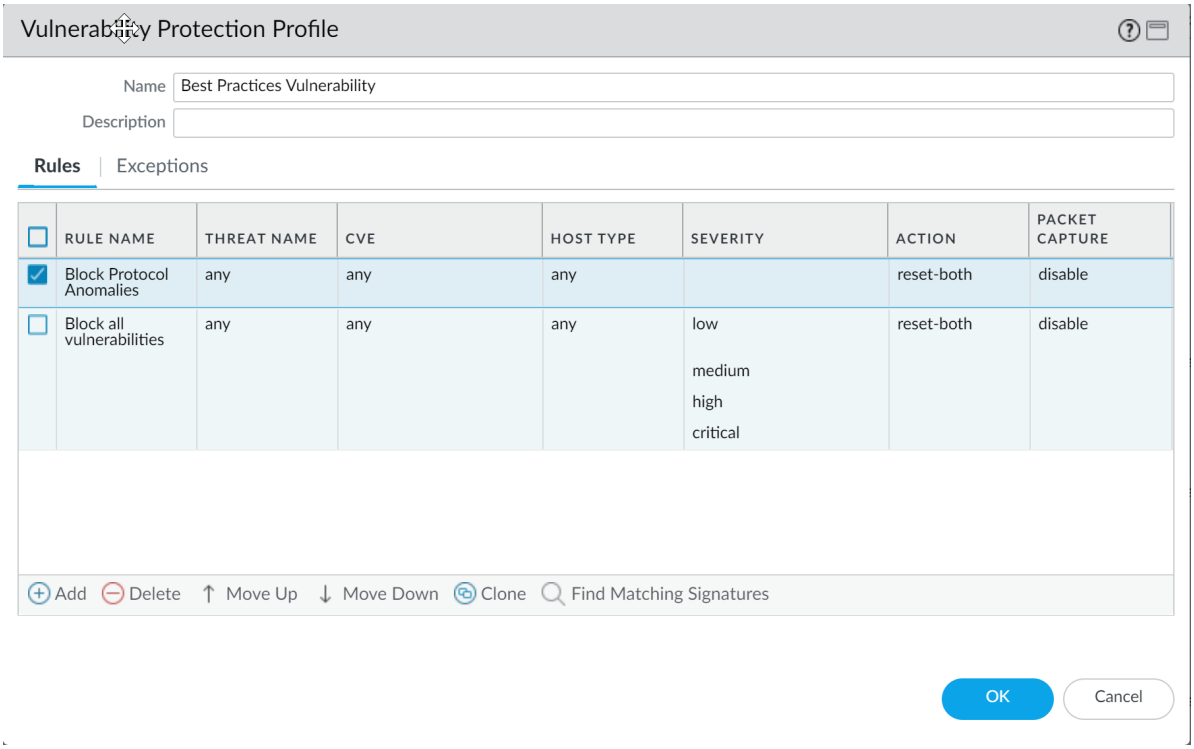
  Cree una regla de perfil de protección de vulnerabilidades con la opción **Category (Categoría)** configurada en protocol-anomaly (protocolo-anomalía), la regla **Action (Acción)** configurada en Reset Both (Restablecer ambos) y la opción **Severity (Gravedad)** configurada en Any (Cualquiera).

© 2020 Palo Alto Networks, Inc.



- Opcionalmente, permita las anomalías de protocolo para las aplicaciones críticas que utilizan protocolos establecidos de una manera no estándar. Para ello, cree una regla de perfil de protección de vulnerabilidades que permita anomalías de protocolo: configure la regla **Action (Acción)** en Allow (Permitir), la opción **Category (Categoría)** en protocol-anomaly (protocolo-anomalía) y la opción **Severity (Gravedad)** en any (cualquiera). Adjunte la regla de perfil de protección de vulnerabilidad a la regla de política de seguridad que aplique el tráfico hacia y desde las aplicaciones críticas.
- Añada otra regla al perfil de protección contra vulnerabilidades para bloquear todas las vulnerabilidades con gravedad baja y alta. Esta regla debe indicarse después de la regla que bloquea las anomalías de protocolo.

© 2020 Palo Alto Networks, Inc.



- Continúe adjuntando los siguientes perfiles de seguridad a sus reglas de políticas de seguridad para proporcionar una protección basada en firmas:
  - Cree un perfil antyspyware para bloquear todo el spyware con gravedad baja y alta.
  - Cree un perfil de antivirus para bloquear todo el contenido que coincida con una firma de antivirus.

© 2020 Palo Alto Networks, Inc.

Configuración de antivirus, antispyware y protección frente a vulnerabilidades

Todos los cortafuegos de próxima generación de Palo Alto Networks incluyen perfiles predefinidos de antivirus, antispyware y protección de vulnerabilidades que puede incluir en las reglas de políticas de seguridad. Incluye un perfil de antivirus predefinido, **predeterminado**, que usa la acción predeterminada para cada protocolo (bloquear tráfico HTTP, FTP y SMB y alerta de tráfico SMTP, IMAP y POP3). Hay dos perfiles predefinidos de antispyware y protección contra vulnerabilidades:

- **default (predeterminado)**: aplica la acción predeterminada a todo el spyware y eventos de protección de vulnerabilidades de gravedad crítica, alta y media de cliente y servidor. No detecta los niveles bajo e informativo.
- **estricto**: Aplica la respuesta de bloqueo a todo el spyware y eventos de protección de vulnerabilidades de gravedad crítica, alta y media de cliente y servidor y usa la acción predeterminada para los eventos bajos e informativos.

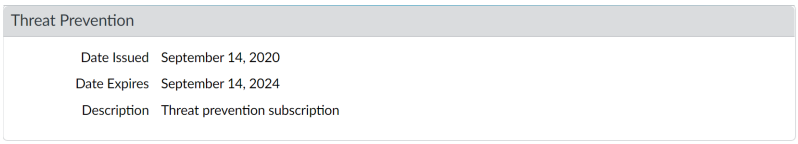
Para garantizar que el tráfico que entra en su red está libre de amenazas, incluya los perfiles predefinidos en sus políticas básicas de acceso web. Al supervisar el tráfico en su red y ampliar su base de reglas de políticas, puede diseñar perfiles más granulares para hacer frente a sus necesidades de seguridad específicas.

Use el siguiente flujo de trabajo para configurar los perfiles de seguridad de antivirus, antispyware y protección de vulnerabilidades.

Palo Alto Networks define una acción predeterminada para todas las firmas antispyware y de protección de vulnerabilidades. Para ver la acción predeterminada, seleccione Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Anti-Spyware (Antispyware) u Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Vulnerability Protection (Protección de vulnerabilidades) y luego seleccione un perfil. Haga clic en la pestaña Exceptions (Excepciones) y después en Show all signatures (Mostrar todas las firmas) para ver la lista de todas las firmas y la Action (Acción) predeterminada correspondiente. Para cambiar la acción predeterminada, debe crear un nuevo perfil y, a continuación, especificar una Action (Acción) y/o añadir excepciones de firma individuales a las Exceptions (Excepciones) en el perfil.

STEP 1 | Compruebe que tiene una suscripción de prevención de amenazas.

La suscripción de prevención de amenazas reúne en una licencia las funciones de antivirus, antispyware y protección contra vulnerabilidades. Para comprobar si posee una suscripción activa de prevención de amenazas, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que la fecha de caducidad de **Threat Prevention (Prevención de amenazas)** sea futura.



STEP 2 | Descargue la última actualización de contenido.

1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y haga clic en **Check Now (Comprobar ahora)** en la parte inferior de la página para recuperar las firmas más recientes.

© 2020 Palo Alto Networks, Inc.

2. En la columna **Actions (Acciones)**, haga clic en **Download (Descargar)** e instale las actualizaciones de antivirus más recientes y luego descargue y seleccione **Install (Instalar)** para instalar las actualizaciones más recientes de aplicaciones y protección contra amenazas.

STEP 3 | Programe actualizaciones de contenido.



Lea Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y amenazas *para obtener información importante sobre la implementación de actualizaciones.*

1. Seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y luego haga clic en **Schedule (Programar)** para recuperar automáticamente las actualizaciones de firmas de **antivirus** y **aplicaciones y amenazas**.
2. Especifique la frecuencia y momento de las actualizaciones:
   - **download-only (solo descarga)**: el cortafuegos descarga automáticamente las actualizaciones más recientes según el cronograma que usted defina, pero debe **instalarlas** manualmente.
   - **download-and-install (descargar e instalar)**: el cortafuegos descarga e instala automáticamente las actualizaciones según el cronograma que usted defina.
3. Haga clic en **OK (Aceptar)** para guardar el cronograma actualizado, no se necesita confirmar.
4. (Opcional) Defina un **Threshold (Umbral)** para indicar una cantidad mínima de horas transcurridas desde que una actualización está disponible para que el cortafuegos la descargue. Por ejemplo, configurar el **Threshold (Umbral)** en **10** significa que el cortafuegos no descargará una actualización hasta que tenga al menos 10 horas, independientemente del cronograma.
5. (HA únicamente) Decida si elegirá la opción **Sync To Peer (Sincronizar con el peer)**, que permite que el peer sincronice las actualizaciones de contenido después de descargar e instalar (el cronograma de actualización no sincroniza entre los peers; usted debe configurar manualmente el cronograma en ambos peers).

   Existen consideraciones adicionales para decidir si usará la opción **Sync To Peer (Sincronizar con el peer)** y cómo, según su implementación HA:

   - **HA activo/pasivo**: si los cortafuegos utilizan el puerto MGT para las actualizaciones de contenido, programe ambos cortafuegos para que descarguen e instalen las actualizaciones de forma independiente. Sin embargo, si los cortafuegos utilizan un puerto de datos para las actualizaciones de contenido, el cortafuegos pasivo no descargará ni instalará actualizaciones, a menos y hasta que esté activo. Para mantener los cronogramas sincronizados en ambos cortafuegos al usar un puerto de datos para las actualizaciones, programa actualizaciones en ambos cortafuegos y luego habilite **Sync To Peer (Sincronizar con el peer)** para que, sea cual fuera el cortafuegos activo, este descargue e instale las actualizaciones, y también las envíe al cortafuegos pasivo.
   - **HA activo/activo**: si los cortafuegos utilizan la interfaz MGT para las actualizaciones de contenido, seleccione **download-and-install (descargar a instalar)** en ambos cortafuegos, pero no habilite **Sync To Peer (Sincronizar con el peer)**. Sin embargo, si los cortafuegos usan un puerto de datos, seleccione **download-and-install (descargar e instalar)** en ambos cortafuegos y habilite **Sync To Peer (Sincronizar con el peer)** para que si un cortafuegos asume un estado activo-secundario, el cortafugos activo-primario descargue e instale las actualizaciones y las envíe al cortafuegos activo-secundario.

STEP 4 | (Opcional) Cree perfiles de seguridad personalizados para antivirus, antispyware y protección de vulnerabilidades.

O bien, puede usar los perfiles estricto o predeterminado predefinido.



Para apostar por una estrategia de seguridad óptima, realice una transición segura *a los* perfiles de seguridad recomendados.

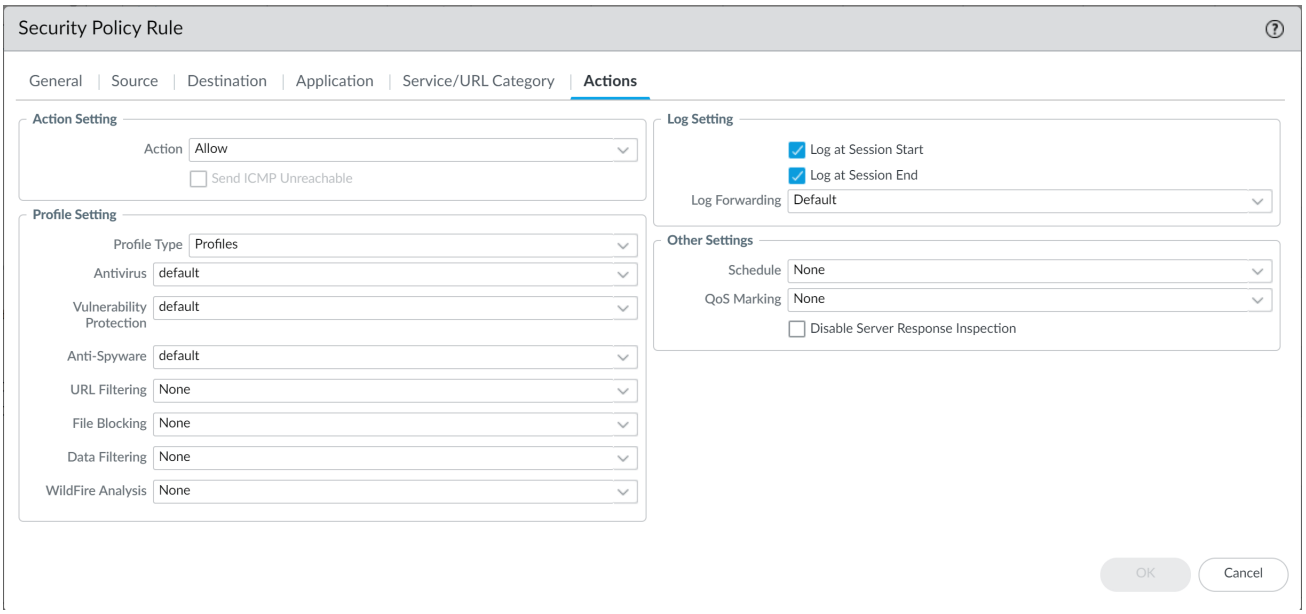
© 2020 Palo Alto Networks, Inc.

- Para crear perfiles antivirus personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus** y **Add (Añadir)** para añadir un nuevo perfil. Siga los pasos para realizar la transición al perfil de antivirus adecuado para alcanzar su objetivo sin problemas.
- Para crear perfiles antispyware personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antispyware** y **Add (Añadir)** para añadir un nuevo perfil. Siga los pasos para realizar la transición al perifil de antispyware adecuado para alcanzar su objetivo sin problemas.
- Para crear perfiles de protección de vulnerabilidades personalizados, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección de vulnerabilidades)** y **Add (Añadir)** para añadir un nuevo perfil. Siga los pasos para realizar la transición al perifil de protección frente a vulnerabilidades adecuado para alcanzar su objetivo sin problemas.

STEP 5 | Adjunte perfiles de seguridad a sus reglas de política de seguridad.

Cuando configura el cortafuegos con una regla de política de seguridad que utiliza un perfil de protección de vulnerabilidades para bloquear las conexiones, el cortafuegos automáticamente bloquea el tráfico en el hardware (consulte Supervisión de direcciones IP bloqueadas).

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla que desea modificar.
2. En la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)**.
3. Seleccione los perfiles de seguridad que creó para **Antivirus**, **Anti-Spyware** y **Vulnerability Protection (Protección de vulnerabilidades)**.



STEP 6 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

DNS Security

DNS Security es un servicio de Threat Prevention en continuo desarrollo que permite proteger la red y defenderla de amenazas avanzadas mediante DNS. Este servicio aprovecha el aprendizaje automático y el análisis predictivo avanzados para ofrecer análisis de las solicitudes de DNS en tiempo real, así como generar y distribuir con rapidez firmas de DNS diseñadas específicamente para la defensa contra el malware que usa DNS para el tráfico de comando y control (command-and-control, C2) y el robo de datos. Gracias a la combinación con una arquitectura de nube ampliable, franquea el acceso a un sistema escalable de inteligencia contra amenazas, que mantiene actualizadas las medidas de protección de la red.

- Información sobre DNS Security
- Medidas de protección y firmas de DNS ofrecidas en la nube
- Análisis de seguridad DNS
- Habilitación de DNS Security

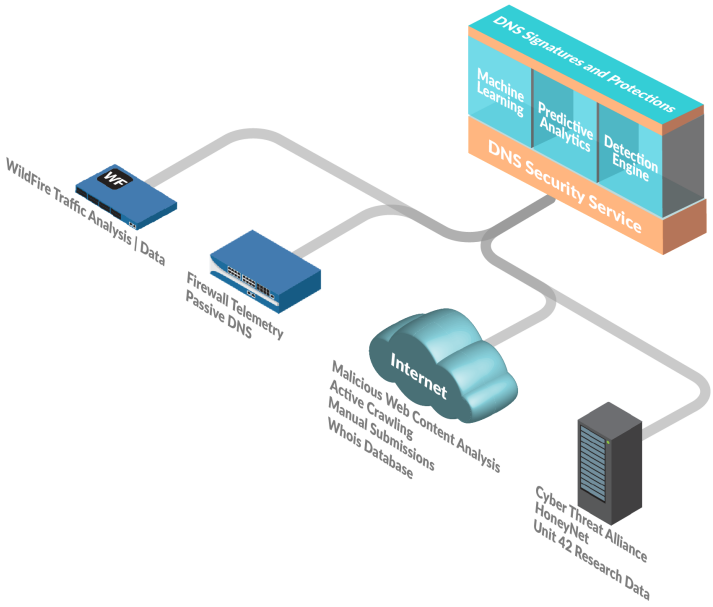
Información sobre DNS Security

Si dispone de una licencia activa de Threat Prevention, puede configurar los cortafuegos con sinkholing de las solicitudes del sistema de nombres de dominio (domain name system, DNS) usando la lista de dominios que genera Palo Alto Networks. Estas listas de firmas de DNS vienen con los paquetes de actualizaciones del antivirus y de WildFire e incluyen las amenazas más pertinentes en el momento de la publicación para permitir la protección y la correcta aplicación de las políticas. Puede acceder a estas listas de forma local y también puede personalizarlas. Para mejorar la cobertura contra las amenazas que utilizan DNS, la suscripción a DNS Security franquea a los usuarios el acceso en tiempo real a las medidas de protección generadas a partir del análisis predictivo avanzado. Identifique de forma proactiva las amenazas ocultas en el tráfico de DNS y comparta los resultados mediante un servicio en la nube con escalabilidad infinita que aplica técnicas como la detección de algoritmos de generación de dominios (domain generation algorithm, DGA), la detección de tunelización de DNS y el aprendizaje automático. Como las medidas de protección y las firmas de DNS se almacenan en una arquitectura basada en la nube, disfruta de acceso a la base de datos completa (y en continua ampliación) de firmas generadas a partir de numerosos orígenes de datos. Así dispone de una defensa en tiempo real contra las diversas amenazas por DNS que plantean los dominios malintencionados recién generados. Para combatir futuras amenazas, se van publicando versiones de contenido que actualizan las funciones de análisis, detección y prevención del servicio.

Para acceder al servicio DNS Security, debe tener una licencia válida de Threat Prevention y de DNS Security.

En este flujo de trabajo se ilustra cómo utiliza el servicio DNS Security diversos orígenes de datos para generar las firmas de DNS:

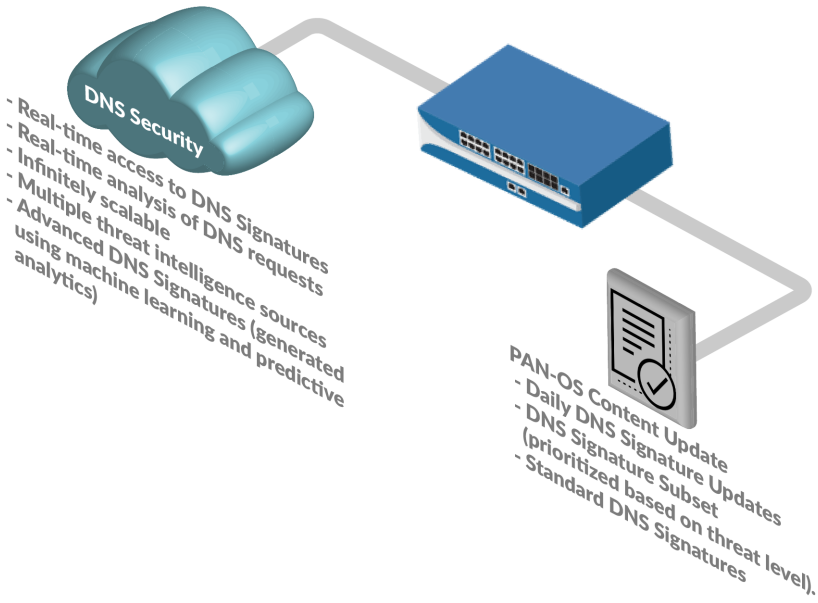
© 2020 Palo Alto Networks, Inc.



Medidas de protección y firmas de DNS ofrecidas en la nube

Como DNS Security es un servicio basado en la nube, franquea el acceso a una fuente de medidas de protección y firmas de DNS con escalabilidad infinita para defender su organización de los dominios malintencionados. Palo Alto Networks genera las medidas de protección y las firmas de dominios a partir de multitud de orígenes, entre otros, análisis del tráfico con WildFire, DNS pasivo, rastreo activo de internet, análisis de contenido web malintencionado, análisis del entorno de pruebas de URL, redes trampa, inversión del diseño de los algoritmos de generación de dominios (domain generation algorithm, DGA), datos de telemetría, búsquedas con WHOIS, equipo de investigación Unidad 42 y orígenes de datos externos, como Cyber Threat Alliance. Esta base de datos en la nube bajo demanda franquea a los usuarios el acceso a todo el conjunto de firmas de DNS de Palo Alto Network, incluidas las que se generan con técnicas avanzadas de análisis y con análisis en tiempo real de solicitudes de DNS. Los conjuntos de firmas de DNS se pueden descargar para disponer de ellos en una ubicación local. Se incluyen en los paquetes de actualizaciones del antivirus y de WildFire, con un límite fijo de 100 000 firmas. No se incluyen las firmas generadas mediante análisis avanzados. Para facilitar la entrada de las firmas de DNS nuevas que se generan a diario, la base de datos en la nube franquea a los usuarios el acceso instantáneo a las firmas recién añadidas, lo que ahorra descargar las actualizaciones. Si la red se queda sin conexión o deja de estar disponible por cualquier otro motivo, el cortafuegos utiliza el conjunto de firmas de DNS descargado.

© 2020 Palo Alto Networks, Inc.



Análisis de seguridad DNS

El servicio de seguridad de DNS realiza un análisis de solicitudes DNS en tiempo real mediante análisis predictivos y aprendizaje automático en varias fuentes de datos DNS. Esto se utiliza para generar protecciones para amenazas basadas en DNS a las que se puede acceder en tiempo real mediante la configuración del perfil de seguridad antispyware conectado a una regla de la política de seguridad. Cada categoría de amenaza DNS (el origen de firma DNS) le permite definir acciones de política independientes, así como un nivel de gravedad de log para un tipo de firma específico. Esto le permite crear políticas de seguridad específicas basadas en la naturaleza de la amenaza de acuerdo con los protocolos de seguridad de su red. Palo Alto Networks también genera y mantiene una lista de dominios explícitamente permitidos basada en métricas de PAN-DB y Alexa. Estos dominios de listas permitidas son de acceso frecuente y se sabe que no tienen contenido malicioso. Las categorías de seguridad DNS y la lista de permitidos se actualizan y se pueden ampliar a través de las publicaciones de contenido de PAN-OS.

Puede ver los datos de estadísticas de DNS de su organización generados por el servicio DNS Security Cloud (Nube de seguridad DNS) mediante AutoFocus. Esto proporciona una evaluación visual rápida que describe el desglose de las solicitudes DNS que pasan a través de su red según las categorías DNS disponibles. También puede recuperar la información del dominio, así como los detalles de la transacción, como la latencia y TTL, con el comando **`test dns-proxy dns-signature fqdn <domain>`**.

Tras la actualización a PAN-OS 10.0 y posterior, el origen de seguridad DNS se redefine en nuevas categorías para proporcionar controles granulares ampliados; como resultado, las nuevas categorías sobrescribirán la acción definida previamente y adquirirán la configuración predeterminada. Asegúrese de volver a aplicar cualquier configuración de captura de paquetes, gravedad de log y sinkhole adecuados para las categorías de seguridad DNS recién definidas.

El servicio de seguridad DNS admite actualmente la detección de las siguientes categorías de amenazas DNS:

- **Command and Control Domains (Dominios de comando y control)**: C2 incluye URL y dominios utilizados por malware o sistemas comprometidos para comunicarse encubiertamente con el servidor remoto de

© 2020 Palo Alto Networks, Inc.

un atacante para recibir comandos maliciosos o cancelar el filtrado de datos (esto incluye la detección de túnel DNS y la detección DGA) .

  - **DNS Tunnel Detection (Detección de túnel DNS)**: los atacantes pueden utilizar la tunelización del sistema de nombres de dominio (DNS, Domain Name System) para codificar dentro de las consultas y las respuestas de DNS los datos de programas y protocolos ajenos a dicho sistema. Así abren un canal trasero con el que pueden transferir archivos o acceder de forma remota al sistema. La detección de túneles de DNS emplea el aprendizaje automático para analizar las cualidades de comportamiento de las consultas de DNS, que incluyen análisis de frecuencia de n-gramas, entropía, frecuencia de consultas y patrones para determinar si las consultas coinciden con ataques basados en la tunelización de DNS. Si se combina con las acciones automatizadas de las políticas del cortafuegos, permite detectar al instante el tráfico de comando y control (command-and-control, C2) o el robo de datos que se ocultan en los túneles de DNS, así como bloquearlos automáticamente en función de las reglas de las políticas definidas.
  - **DGA Detection (Detección de DGA)**: los algoritmos de generación de dominios (DGA, Domain Generation Algorithm) se emplean para generar dominios (por lo general, en grandes cantidades) de forma automática con el fin de establecer un canal malintencionado de comunicaciones de comando y control (command-and-control, C2). El malware basado en DGA (como Pushdo, Bankpatch y CryptoLocker) limita los dominios que se bloquean ocultando la ubicación de sus servidores de C2 activos entre un elevado número de posibles sospechosos. Se puede generar con algoritmos basados en distintos factores, como la hora, las claves criptográficas u otros valores únicos. Aunque la mayoría de los dominios generados con DGA no se resuelve, es preciso identificar todos para ofrecer una defensa integral contra amenazas concretas. El análisis de DGA determina la probabilidad de que el dominio se haya generado de forma automática, no manual. Para ello, se invierte el diseño y se analizan otras técnicas que se suelen emplear en los DGA. Palo Alto Networks se sirve de estas características para identificar y bloquear en tiempo real las amenazas basadas en DGA ya conocidas.
- **Dynamic DNS Hosted Domains (Dominios alojados de DNS dinámico)**: los servicios DDNS (Dynamic DNS, DNS dinámico) proporcionan una asignación entre los nombres de host y las direcciones IP casi en tiempo real para seguir cambiando las direcciones IP vinculadas a un dominio específico cuando las IP estáticas no estén disponibles. Esto proporciona a los atacantes un método para infiltrarse en las redes mediante el uso de servicios DDNS para cambiar las direcciones IP que albergan los servidores de comando y control. Las campañas de malware y los kits de explotación pueden utilizar los servicios DDNS como parte de su estrategia de distribución de carga útil. Al utilizar dominios DDNS como parte de su infraestructura de nombre de host, los atacantes pueden cambiar la dirección IP asociada con registros DNS determinados y evitar la detección más fácilmente. La seguridad DNS detecta la explotación de los servicios DDNS mediante el filtrado y la referencia cruzada de datos DNS de varios orígenes para generar listas de candidatos que luego se validan para maximizar la precisión.
- **Malware Domains (Dominios de malware)**: los dominios maliciosos alojan y distribuyen malware, y pueden incluir sitios web que intentan instalar diversas amenazas (como archivos ejecutables, scripts, virus o descargas no autorizadas). Los dominios maliciosos se distinguen de los dominios C2 en que envían cargas útiles maliciosas a su red a través de un origen externo, mientras que con C2, los endpoints infectados normalmente intentan conectarse a un servidor remoto para recuperar instrucciones adicionales u otro contenido malicioso.
- **Newly Registered Domains (Dominios recién registrados)**: los dominios recién registrados son dominios nuevos, nunca registrados, que un operador o entidad de TLD ha agregado recientemente. Aunque se pueden crear nuevos dominios con fines legítimos, la gran mayoría se usa a menudo para facilitar actividades maliciosas, como operar como servidores C2 o para usarse para distribuir malware, spam o PUP/adware. Palo Alto Networks detecta los dominios recién registrados mediante la supervisión de feeds específicos (logs de dominio y registradores) y el uso de archivos de zona, DNS pasivo y datos de WHOIS para detectar campañas de registro.
- **Phishing Domains (Dominios de phishing)**: los dominios de phishing intentan atraer a los usuarios para que envíen datos confidenciales, como información personal o credenciales de usuario, haciéndose pasar por sitios web legítimos mediante phishing o pharming. Estas actividades maliciosas se pueden realizar a través de campañas de ingeniería social (mediante las que un origen aparentemente fiable manipula a los usuarios para que envíen información personal por correo electrónico u otras formas de comunicaciones

© 2020 Palo Alto Networks, Inc.

electrónicas) o mediante la redirección del tráfico web, que dirige a los usuarios a sitios fraudulentos que parecen legítimos.

- **Grayware Domains (Dominios grayware)** (disponibles con la instalación de la versión 8290 de contenido de PAN-OS y posteriores): los dominios de grayware generalmente no representan una amenaza de seguridad directa. Sin embargo, pueden facilitar vectores de ataque, producir varios comportamientos indeseables o simplemente pueden contener contenido cuestionable/ofensivo. Aquí se incluyen sitios web que intentan engañar a los usuarios para que otorguen acceso remoto, contienen adware y otras aplicaciones no solicitadas (como criptominería, secuestradores y programas potencialmente no deseados [PUP, Potentially Unwanted Program]), implementan acciones de ocultación de identificación de dominios mediante técnicas de flujo rápido, dominios de typosquatting y varios sitios que promueven actividades ilegales o estafas.
- **Parked Domains (Dominios estacionados)** (disponible con la instalación de la versión 8318 de contenido de PAN-OS y versiones posteriores): los dominios estacionados suelen ser sitios web inactivos que alojan contenido limitado, a menudo en forma de anuncios de clic que pueden generar ingresos para la entidad anfitriona, pero que generalmente no contienen contenido que sea útil para el usuario final. Aunque a menudo funcionan como un marcador de posición legítimo o una simple molestia benigna, también podrían usarse como un posible vector para la distribución de malware.
- **Proxy Avoidance and Anoymizers (Evasión de proxy y anonimizadores)** (disponible con la instalación de la versión 8340 de contenido de PAN-OS y posterior): la evasión de proxy y anonimizadores hace referencia al tráfico de los servicios que se utilizan para eludir las políticas de filtrado de contenido. Los usuarios que intentan eludir las políticas de filtrado de contenido de una organización a través de los servicios de proxy anonimizador están bloqueados en el nivel de DNS.

Habilitación de DNS Security

Para habilitar el sinkhole de DNS para consultas de dominio mediante la seguridad de DNS, debe activar su suscripción de seguridad DNS, crear (o modificar) una política antispyware para hacer referencia al servicio de seguridad DNS, configurar la gravedad del log y la configuración de la política para cada categoría de firma DNS y, a continuación, adjuntar el perfil a una regla de políticas de seguridad.

STEP 1 | Activación de licencias de suscripción.

STEP 2 | Configure los ajustes de la política de firmas de DNS para enviar las consultas de DNS de malware al sinkhole definido.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Cree un perfil, modifique uno existente o seleccione uno de los perfiles predeterminados y clónelo.
3. En **Name (Nombre)**, especifique el nombre del perfil y, si lo desea, proporcione una descripción.
4. Seleccione la pestaña **DNS Policies (Políticas DNS)**.
5. En la columna **Signature Source (Origen de firma)**, debajo del encabezado DNS Security (Seguridad DNS), hay orígenes de firma DNS configurables individualmente, que le permiten definir acciones de política independientes, así como un nivel de gravedad de logs.

   Palo Alto Networks recomienda cambiar la configuración predeterminada de las políticas DNS para los orígenes de firmas para garantizar una cobertura óptima, así como para ayudar con la respuesta y corrección de incidencias. Siga las prácticas recomendadas para configurar su configuración de seguridad DNS como se describe en Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7.

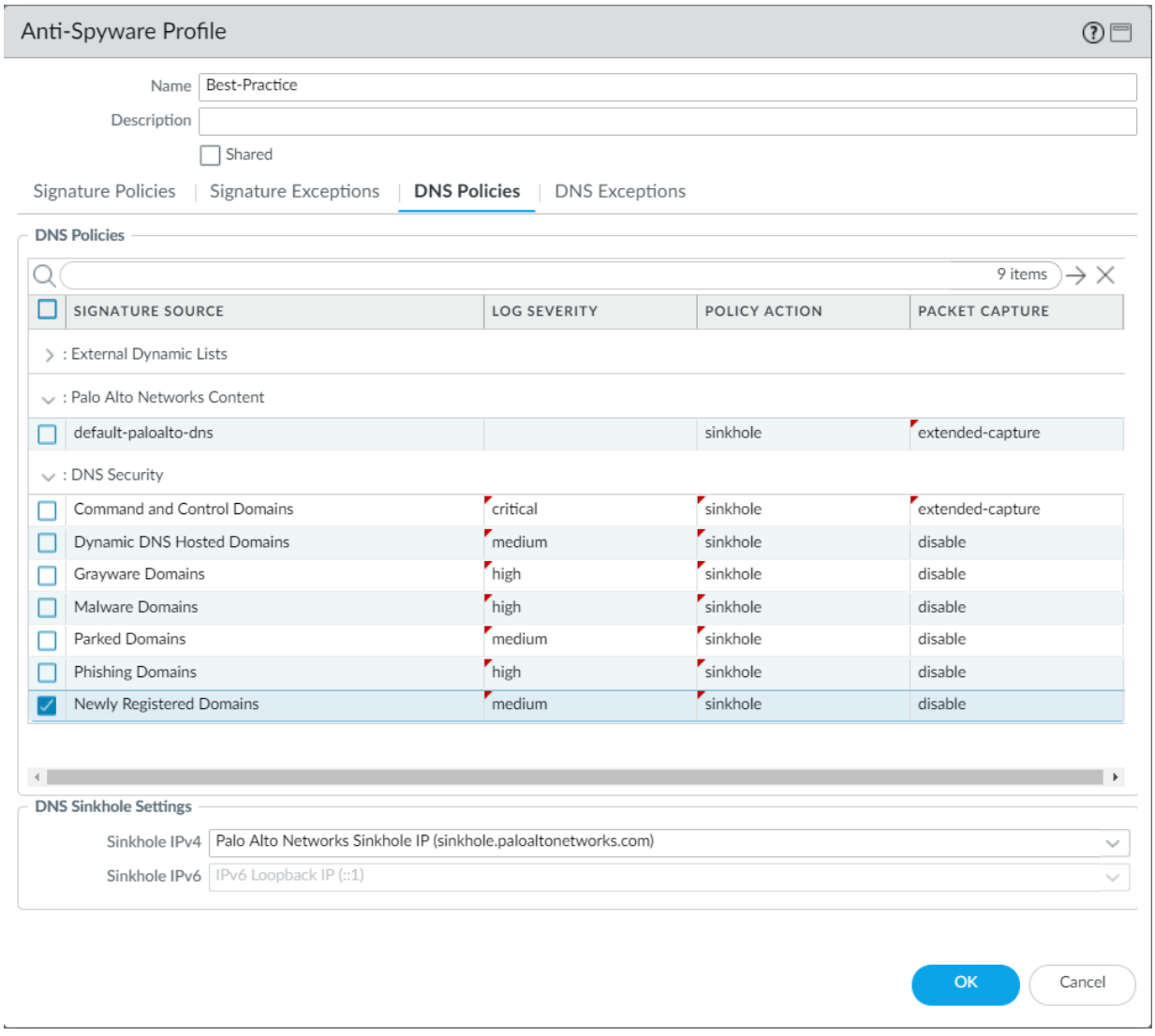
   - Especifique el nivel de gravedad del log que se registra cuando el cortafuegos detecta un dominio que coincide con una firma DNS. Para obtener más información sobre los distintos niveles de gravedad de los logs, consulte Niveles de gravedad de amenazas.

© 2020 Palo Alto Networks, Inc.

- Seleccione la acción que se debe ejecutar cuando se realizan búsquedas de DNS en sitios de malware conocidos con el origen de la firma de DNS Security. Las opciones son alert (alertar), allow (permitir), block (bloquear) o sinkhole. Verifique que la acción configurada es sinkhole.
- En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

6. En la sección **DNS Sinkhole Settings (Configuración de sinkhole de DNS)**, verifique que está habilitada la opción **Sinkhole**. Para su comodidad, la dirección del sinkhole predeterminado (sinkhole.paloaltonetworks.com) está configurada para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección por medio de actualizaciones de contenido.

   Si desea cambiar la dirección de **Sinkhole IPv4 (IPv4 de sinkhole)** o **Sinkhole IPv6 (IPv6 de sinkhole)** por un servidor local de la red o por una dirección de bucle invertido, consulte Configuración de la dirección IP del sinkhole en un servidor local de la red.
7. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.



STEP 3 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.

© 2020 Palo Alto Networks, Inc.

2. En **Security Policy Rule (Regla de política de seguridad)**, seleccione o cree la regla.
3. En la pestaña **Actions (Acciones)**, marque la casilla de verificación **Log at Session End (Crear log al cerrar sesión)** para habilitar la creación de logs.
4. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. En el menú desplegable **Anti-Spyware (Antispyware)**, seleccione el perfil nuevo o modificado.
5. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 4 | Compruebe que la acción de política esté forzada.

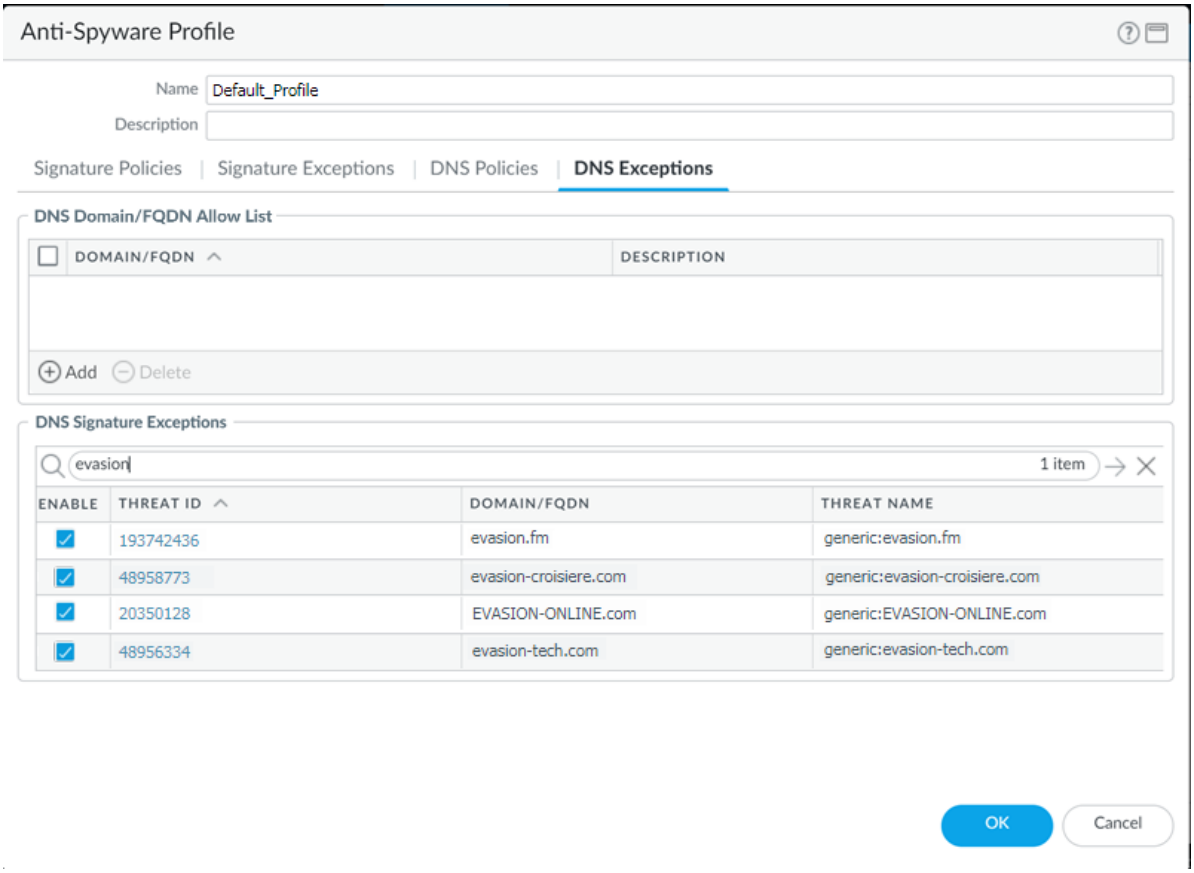
1. Acceda a los siguientes dominios de prueba para comprobar que se está aplicando la acción de política para un tipo de amenaza determinado:
   - C2: test-c2.testpanw.com
   - DNS Tunneling (Tunelización de DNS): test-dnstun.testpanw.com
   - DGA: test-dga.testpanw.com
   - Dynamic DNS (DNS dinámico): test-ddns.testpanw.com
   - Malware: test-malware.testpanw.com
   - Newly Registered Domains (Dominios registrados recientemente): test-nrd.testpanw.com
   - Phishing: test-phishing.testpanw.com
   - Grayware: test-grayware.testpanw.com
   - Parked (Estacionado): test-parked.testpanw.com
   - Proxy Avoidance and Anonymizers (Evasión de proxy y anonimizadores): test-proxy.testpanw.com
2. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.

STEP 5 | Identifique los hosts infectados con los logs de tráfico.

STEP 6 | (Opcional) Añada excepciones de firmas de dominios para evitar falsos positivos.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Seleccione el perfil que desea modificar.
3. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
4. Introduzca el nombre o el FQDN de la firma de DNS que se debe excluir para buscarla.
5. Active la casilla de verificación para cada **ID de amenaza** cuya firma desea excluir de la aplicación.
6. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

© 2020 Palo Alto Networks, Inc.



STEP 7 | (Opcional) Añada una lista de permisos para especificar una lista de dominios DNS/FQDN que se permita explícitamente.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Seleccione el perfil que desea modificar.
3. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
4. Para **añadir** una nueva **lista de permitidos de FQDN**, proporcione el dominio DNS o la ubicación del FQDN y una descripción.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

STEP 8 | (Opcional) Verifique la conectividad de su cortafuegos con el servicio de seguridad DNS. Si no puede comunicarse con el servicio, verifique que el siguiente dominio no esté bloqueado: dns.service.paloaltonetworks.com.

Utilice el siguiente comando de la CLI en el cortafuegos para verificar la disponibilidad de conexión de su cortafuegos con el servicio de seguridad DNS.

```
show dns-proxy dns-signature info
```

Por ejemplo:

```
show dns-proxy dns-signture info

Cloud URL: dns.service.paloaltonetworks.com:443
```


© 2020 Palo Alto Networks, Inc.

```
Telemetry URL: io.dns.service.paloaltonetworks.com:443

Last Result: None

Last Server Address:

Parameter Exchange: Interval 300 sec

Allow List Refresh: Interval 43200 sec

Request Waiting Transmission: 0

Request Pending Response: 0

Cache Size: 0
```

STEP 9 | (Opcional) Recupere los detalles de la transacción de un dominio específico, como la latencia, TTL y la categoría de firma.

Use el siguiente comando CLI en el cortafuegos para revisar los detalles de la lista.

```
test dns-proxy dns-signature fqdn
```

Por ejemplo:

```
test dns-proxy dns-signature fqdn www.yahoo.com

DNS Signature Query [ www.yahoo.com ]

Completed in 178 ms

DNS Signature Response

Entries: 2

Domain                              Category        GTID                 TTL
-------------------------------------------------------------------------------------
*.yahoo.com                         Benign          0
 86400
  www.yahoo.com                     Benign          0                    3600
```

STEP 10 | (Opcional) Configure los ajustes de tiempo de espera de búsqueda de firma DNS. Si el cortafuegos no puede recuperar un veredicto de firma en el tiempo asignado debido a problemas de conectividad, se pasa la solicitud, incluidas todas las respuestas DNS posteriores. Puede verificar la latencia media para comprobar que las solicitudes se encuentren dentro del periodo configurado. Si la latencia media supera el periodo configurado, considere actualizar la configuración a un valor que sea superior a la latencia media para evitar que el tiempo de espera de las solicitudes se agote.

1. En la CLI, emita el siguiente comando para ver la latencia media.

```
show dns-proxy dns-signature
counters
```

El tiempo de espera predeterminado es de 100 milisegundos.

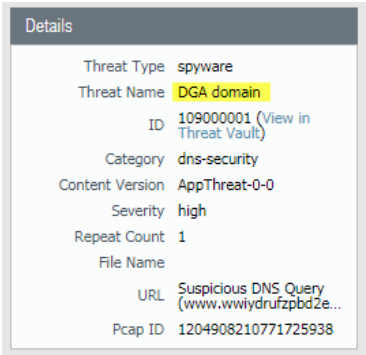
© 2020 Palo Alto Networks, Inc.

2. Desplácese hacia abajo a través del resultado hasta la sección de latencia en el encabezado de la API de consulta de firma y compruebe que la latencia media se encuentre dentro del periodo de espera definido. Esta latencia indica la cantidad de tiempo que tarda, de media, en recuperar un veredicto de firma del servicio de seguridad de DNS. Puede encontrar estadísticas de latencia adicionales para varios periodos de latencia inferiores a las medias.

```
Signature query API:
  .
  .
  .
     [latency   ] :
        max    1870 (ms)  min    16(ms)  avg    27(ms)
          50 or less : 47246
          100 or less : 113
          200 or less : 25
          400 or less : 15
                 else : 21
```

3. Si la latencia media está coherentemente por encima del valor de tiempo de espera predeterminado, puede aumentar la configuración para que las solicitudes se encuentren dentro de un periodo determinado. Seleccione **Device (Dispositivo) > Content-ID** y actualice la configuración de **Realtime Signature Lookup (Consulta de firma en tiempo real)**.
4. Confirme los cambios.

Para ver consultas DNS de sinkhole, consulte los logs de amenazas del cortafuegos (**Monitor > Logs** y, a continuación, seleccione el tipo de log de la lista):



© 2020 Palo Alto Networks, Inc.

Uso de consultas de DNS para identificar hosts infectados en la red

La acción de sinkhole de DNS de los perfiles de antispyware permite que el cortafuegos genere respuestas falsas a las consultas de DNS de dominios malintencionados conocidos o dominios personalizados, de modo que se identifiquen los hosts de la red infectados con malware. Un host comprometido puede iniciar la comunicación con un servidor de comando y control (command-and-control, C2); si logra establecer la conexión, un atacante puede controlar de forma remota el host infectado con el fin de infiltrase más en la red o de filtrar datos.

Las consultas DNS a cualquier dominio incluido en la lista de firmas de DNS de Palo Alto Networks se envían a un sinkhole a una dirección IP de servidor de Palo Alto Networks.

El cortafuegos puede recurrir a dos orígenes de firmas de DNS para identificar los dominios malintencionados y de C2:

- (Threat Prevention obligatorio) Firmas de DNS locales: el cortafuegos puede usar este conjunto descargado y limitado de firmas de DNS para identificar los dominios malintencionados. El cortafuegos obtiene nuevas firmas de DNS como parte de las actualizaciones diarias del antivirus.
- (DNS Security obligatorio) Firmas de DNS Security: el cortafuegos accede al servicio en la nube DNS Security de Palo Alto Networks para buscar dominios malintencionados en la base de datos completa de firmas de DNS. DNS Security proporciona algunas firmas en exclusiva para detectar ataques de C2 que usan técnicas de aprendizaje automático, como los algoritmos de generación de dominios (domain generation algorithm, DGA) y la tunelización de DNS.

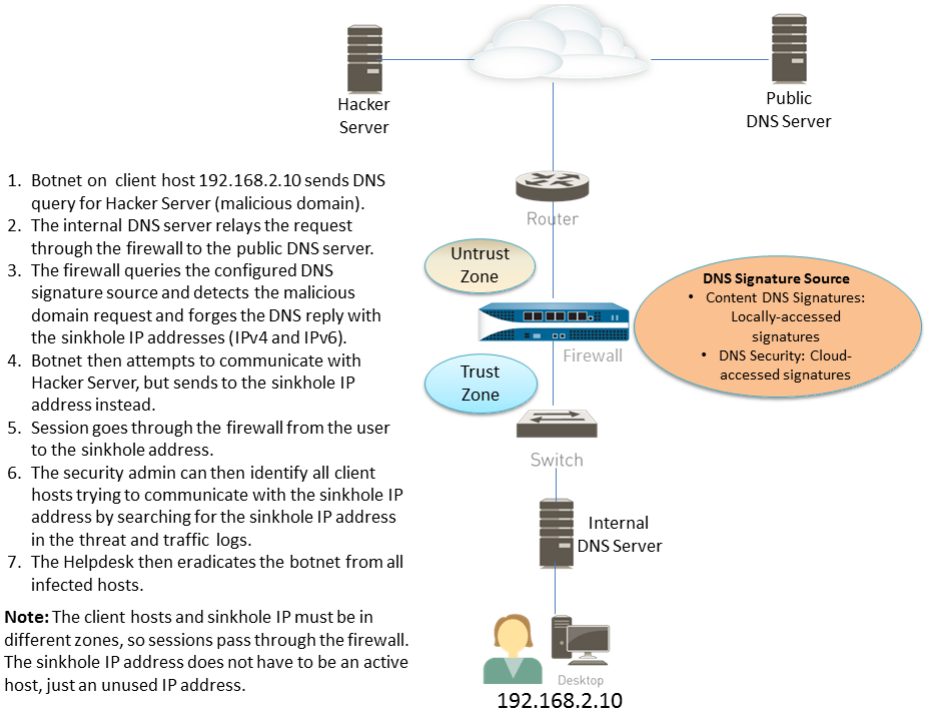
Las consultas de DNS de dominios realizadas en el conjunto local de firmas de DNS o en el conjunto de firmas de DNS Security se redirigen a un servidor de Palo Alto Networks, y el host no puede acceder al dominio malintencionado. Los temas siguientes aportan información para habilitar el sinkholing de DNS con el fin de identificar los hosts infectados.

- Consulte Funcionamiento del sinkholing de DNS.
- Configuración del sinkholing de DNS.
- Configuración del sinkholing de DNS para una lista de dominios personalizados.
- Habilitación de DNS Security para enviar los dominios de C2 al sinkhole.
- Configuración de la dirección IP del sinkhole en un servidor local de la red.
- Consulta de hosts infectados que intentan conectar a dominios malintencionados.

Funcionamiento del sinkholing de DNS

La función de sinkholing de DNS facilita la identificación de hosts infectados en la red protegida mediante tráfico DNS en situaciones en las que el cortafuegos no puede ver la consulta de DNS del cliente infectado (es decir, el cortafuegos no puede ver el originador de la consulta de DNS). En una implementación típica, donde el cortafuegos está antes del servidor DNS local, el log de amenazas identificará la resolución DNS local como el origen del tráfico en lugar del host infectado. Al hacer el sinkholing de las consultas de DNS de malware, se resuelve este problema de visibilidad, ya que se generan respuestas falsas a las consultas de los hosts clientes dirigidas a dominios malintencionados. De ese modo, si los clientes intentan conectarse a dominios malintencionados (mediante comando y control [command-and-control, C2], por ejemplo), se conectan, en cambio, a la dirección IP predeterminada de sinkhole de Palo Alto Networks o a la dirección IP que defina el usuario según el procedimiento Configuración del sinkholing de DNS para una lista de dominios personalizados. Así, resulta muy sencillo identificar los hosts infectados en los logs de tráfico.

© 2020 Palo Alto Networks, Inc.



Configuración del sinkholing de DNS

Para habilitar el sinkholing de DNS, vincule el perfil predeterminado de antispyware a una regla de la política de seguridad (consulte Configuración de antivirus, antispyware y protección frente a vulnerabilidades). Las consultas de DNS sobre cualquier dominio incluido en el origen de firmas de DNS de Palo Alto Networks que especifique se resuelven en la dirección IP predeterminada de sinkhole de Palo Alto Networks. En la actualidad, se utilizan una dirección IPv4 (sinkhole.paloaltonetworks.com) y una dirección IPv6 de bucle invertido (::1). Esta dirección está sujeta a cambios y puede actualizarse con actualizaciones de contenido.

STEP 1 | Habilite el sinkholing de DNS para la lista personalizada de dominios en una lista dinámica externa.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Modifique un perfil existente o seleccione uno de los perfiles por defecto existentes y duplíquelo.
3. Asigne un nombre al perfil en **Name (Nombre)** y, a continuación, seleccione la pestaña **DNS Policies (Políticas DNS)**.
4. Verifique que **default-paloalto-dns** esté presente en el **origen de firma**.
5. (Opcional) En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

STEP 2 | Verifique los ajustes de sinkholing en el perfil de antispyware.

1. En la pestaña **DNS Policies (Políticas DNS)**, verifique que **Policy Action (Acción de políticas)** en las consultas DNS sea **sinkhole**.
2. En la sección DNS Sinkhole Settings (Configuración de sinkhole de DNS), verifique que está habilitada la opción **Sinkhole**. Para su conveniencia, la dirección IP del sinkhole por defecto se configura para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

© 2020 Palo Alto Networks, Inc.

Si desea cambiar la dirección de **Sinkhole IPv4 (IPv4 de sinkhole)** o **Sinkhole IPv6 (IPv6 de sinkhole)** por un servidor local de la red o por una dirección de bucle invertido, consulte Configuración de la dirección IP del sinkhole en un servidor local de la red.

3. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 3 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de la política de seguridad.
2. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs.
3. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. Haga clic en el menú desplegable **Anti-Spyware** y seleccione el nuevo perfil.
4. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 4 | Para comprobar que se aplica la acción de la política, supervise la actividad del cortafuegos.

1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.

Configuración del sinkholing de DNS para una lista de dominios personalizados

Para habilitar el sinkholing para una lista personalizada de dominios, debe crear una lista externa dinámica que incluya los dominios, habilite la acción de sinkhole en un perfil antispyware y adjunte el perfil a una regla de política de seguridad. Cuando un cliente intenta acceder a un dominio malintencionado de la lista, el cortafuegos falsifica la dirección IP de destino en el paquete al servidor por defecto de Palo Alto Networks o a una dirección IP definida por el usuario para el sinkholing.

Para cada dominio personalizado incluido en la lista dinámica externa, el cortafuegos general las firmas de spyware basadas en DNS. La firma se denomina Custom Malicious DNS Query <domain name> y es del tipo spyware con gravedad media; cada firma es un hash de 24 bytes del nombre de dominio.

Cada modelo de cortafuegos admite un máximo de 50 000 nombres de dominio en una o más listas dinámicas, pero no se fuerza un límite máximo para ninguna otra lista.

STEP 1 | Habilite el sinkholing de DNS para la lista personalizada de dominios en una lista dinámica externa.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Modifique un perfil existente o seleccione uno de los perfiles por defecto existentes y duplíquelo.
3. Asigne un nombre al perfil en **Name (Nombre)** y, a continuación, seleccione la pestaña **DNS Policies (Políticas DNS)**.
4. Seleccione una EDL a partir del origen de firma de **External Dynamic Lists (Listas dinámicas externas)**.

   Si ya ha creado una lista dinámica externa de tipo: Lista de dominio, puede seleccionarla aquí. La lista no muestra listas dinámicas externas de tipo URL o direcciones IP que pueda haber creado.

5. Configure la lista dinámica externa del perfil Anti-Spyware (consulte Configuración del cortafuegos para acceder a una lista dinámica externa). El **Type (Tipo)** está preconfigurado en **Domain List (Lista de dominios)**.

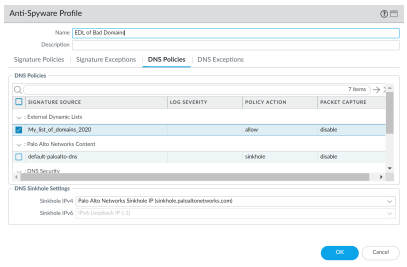
© 2020 Palo Alto Networks, Inc.

6. (Opcional) En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

STEP 2 | Verifique los ajustes de sinkholing en el perfil de antispyware.

1. En la pestaña **DNS Policies (Políticas DNS)**, verifique que **Policy Action (Acción de políticas)** en las consultas DNS sea **sinkhole**.
2. En la sección DNS Sinkhole Settings (Configuración de sinkhole de DNS), verifique que está habilitada la opción **Sinkhole**. Para su conveniencia, la dirección IP del sinkhole por defecto se configura para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

   Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.



3. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 3 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de la política de seguridad.
2. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs.
3. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. Haga clic en el menú desplegable **Anti-Spyware** y seleccione el nuevo perfil.
4. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 4 | Compruebe que la acción de política esté forzada.

1. Visualice las entradas de lista dinámica externa que pertenezcan a la lista de dominio y acceda a un dominio desde la lista.
2. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.

STEP 5 | Verifique si las entradas en la lista dinámica externa se ignoraron u omitieron.

Use el siguiente comando CLI en el cortafuegos para revisar los detalles de la lista.

```
request system external-list show type domain name <list_name>
```

Por ejemplo:

© 2020 Palo Alto Networks, Inc.

```
request system external-list show type domain name
My_List_of_Domains_2015
vsys1/EBLDomain:
Next update at : Thu May 21 10:15:39 2015
Source : https://1.2.3.4/My_List_of_Domains_2015
Referenced : Yes
Valid : Yes
Number of entries : 3
domains:www.example.com
baddomain.com
qqq.abcedfg.com
```

STEP 6 | (Opcional) Recupere la lista dinámica externa a pedido.

Para forzar que el cortafuegos recupere la lista actualizada a pedido en lugar de hacerlo en el siguiente intervalo de actualización (la frecuencia de **Repeat** que definió para la lista dinámica externa), use el siguiente comando CLI:

```
request system external-list refresh type domain name  <list_name>
```

Como alternativa, puede usar la interfaz del cortafuegos para recuperar una lista dinámica externa del servidor web.

Configuración de la dirección IP del sinkhole en un servidor local de la red

Por defecto, la función de sinkholing está habilitada para todas las firmas DNS de Palo Alto Network, y la dirección IP de sinkhole está configurada para acceder a un servidor de Palo Alto Network. Use las instrucciones de esta sección si desea configurar la dirección IP de sinkhole en un servidor local de la red.

Debe obtener las direcciones IPv4 e IPv6 para usar como direcciones IP de sinkhole, debido a que el software malintencionado puede realizar consultas de DNS mediante uno o ambos protocolos. La dirección de sinkhole de DNS debe estar una zona distinta de la de los hosts de cliente para garantizar que, cuando un host infectado intentar iniciar una sesión con la dirección IP de sinkhole, se enrutará a través del cortafuegos.

Las direcciones de sinkhole se deben reservar con este fin y no es necesario asignarlas a un host físico. Además, puede utilizar un servidor honey-pot (trampa) como host físico para analizar más detenidamente el tráfico malintencionado.

Para los siguientes pasos de configuración, se utilizan las siguientes direcciones de sinkhole de DNS de ejemplo:

Dirección de sinkhole de DNS IPv4: 10.15.0.20

Dirección de sinkhole de DNS IPv6: fd97:3dec:4d27:e37c:5:5:5:5

STEP 1 | Configure la interfaz de sinkhole y la zona.

El tráfico de la zona en la que se encuentran los hosts de cliente se debe enrutar a la zona en la que se ha definido la dirección IP de sinkhole para que se registre el tráfico.

© 2020 Palo Alto Networks, Inc.

Utilice una zona específica para el tráfico de sinkhole, ya que el host infectado enviará tráfico a esta zona.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione una interfaz para configurar como su interfaz de sinkhole.
2. En la lista desplegable **Tipo de interfaz**, seleccione **Capa3**.
3. Para añadir una dirección IPv4, seleccione la pestaña **IPv4**, seleccione **Static (Estático)** y, a continuación, haga clic en **Add (Añadir)**. En este ejemplo, añada 10.15.0.20 como la dirección IPv4 de DNS sinkhole.
4. Seleccione la pestaña **IPv6**, haga clic en **Static (Estático)** y, a continuación, haga clic en **Add (Añadir)** y especifique una dirección IPv6 y una máscara de subred. En este ejemplo, fd97:3dec:4d27:e37c::/64 es la dirección de sinkhole IPv6.
5. Haga clic en **OK (Aceptar)** para guardar.
6. Para añadir una zona para el sinkhole, seleccione **Network (Red)** > **Zones (Zonas)** y haga clic en **Add (Añadir)**.
7. Especifique un **Name (Nombre)** para la zona.
8. En la lista desplegable **Type (Tipo)**, seleccione **Layer3**.
9. En la sección **Interfaces**, haga clic en **Añadir** y añada la interfaz que ha configurado.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | Habilite el sinkholing DNS.

Por defecto, el sinkholing está habilitado para todas las firmas DNS de Palo Alto Networks. Para cambiar la dirección de sinkhole a su servidor local, consulte el paso Verificar los ajustes de sinkholing en el perfil anti-spyware. en Configuración del sinkholing de DNS para una lista de dominios personalizados.

STEP 3 | Edite la regla de la política de seguridad que permite el tráfico de los hosts de cliente de la zona fiable a la zona no fiable para incluir la zona de sinkhole como un destino y adjuntar el perfil de antispyware.

La modificación de las reglas de política de seguridad que permiten el tráfico desde hosts clientes en la zona fiable hacia la zona no fiable garantiza la identificación del tráfico de hosts infectados. Al añadir la zona de sinkhole como un destino en la regla, permite que los clientes infectados envíen consultas de DNS falsas al sinkhole de DNS.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Seleccione una regla existente que permita el tráfico de la zona del host de cliente a la zona que no es de confianza.
3. En la pestaña **Destination (Destino)**, seleccione **Add (Añadir)** para añadir la zona de sinkhole. Esto permite que el tráfico del host de cliente fluya hasta la zona de sinkhole.
4. En la pestaña **Actions**, seleccione la casilla de verificación **Log at Session Start** para habilitar el registro de logs. De este modo, garantiza que el tráfico de los hosts de cliente de la zona de confianza se registre al acceder a las zonas que no son de confianza o de sinkhole.
5. En la sección **Profile Setting (Ajuste de perfil)**, seleccione el perfil de **Antispyware** en el que ha habilitado el sinkholing de DNS.
6. Haga clic en **OK (Aceptar)** para guardar la regla de política de seguridad y, a continuación, en **Commit (Confirmar)**.

STEP 4 | Para confirmar que podrá identificar los hosts infectados, compruebe si el tráfico desde el host cliente de la zona de confianza hasta la nueva zona de sinkhole se está registrando.

En este ejemplo, el cliente de host infectado es 192.168.2.10 y la dirección IPv4 de sinkhole es 10.15.0.20.

© 2020 Palo Alto Networks, Inc.

1. En un host de cliente de la zona de confianza, abra un símbolo del sistema y ejecute el siguiente comando:

```
C:\>ping <sinkhole address>
```

   La salida del siguiente ejemplo muestra la solicitud de ping a la dirección de sinkhole de DNS en 10.15.0.2 y el resultado, que es `Request timed out` debido a que en este ejemplo la dirección IP de sinkhole no se ha asignado a un host físico:

```
C:\>ping 10.15.0.20
Pinging 10.15.0.20 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 10.15.0.20:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2. En el cortafuegos, seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y encuentre la entrada de log con el origen 192.168.2.10 y el destino 10.15.0.20. Esto confirma que el tráfico para la dirección IP de sinkhole atraviesa las zonas del cortafuegos.

   Puede buscar o filtrar los logs y mostrar solo los logs con el destino 10.15.0.20. Para ello, haga clic en la dirección IP (10.15.0.20) en la columna Destination (Destino), lo que añadirá el filtro (addr.dst en 10.15.0.20) al campo de búsqueda. Haga clic en el icono Aplicar filtro a la derecha del campo de búsqueda para aplicar el filtro.

STEP 5 | Compruebe que el sinkholing de DNS esté configurado correctamente.

Está simulando la acción que un host cliente infectado realizaría cuando una aplicación malintencionada intenta una notificación de instalación.

1. Detecte un dominio malintencionado que esté incluido en la base de datos de firmas de antivirus actual del cortafuegos para comprobar el sinkholing.
   1. Seleccione **Device (Dispositivo)** > **Dynamic (Dinámico) Updates (Actualizaciones)** y en la sección **Antivirus**, haga clic en el enlace **Release Notes (Notas de versión)** para la base de datos de antivirus instalada actualmente. También puede buscar las notas de versión del antivirus que enumeran las actualizaciones de firma incrementales en la sección de actualizaciones dinámicas del sitio de asistencia técnica de Palo Alto Networks.
   2. En la segunda columna de las notas de la versión, busque un elemento de línea con una extensión de dominio (por ejemplo, com, edu o net). En la columna de la izquierda se muestra el nombre del dominio. Por ejemplo, en la versión de antivirus 1117-1560, hay un elemento en la columna de la izquierda llamado "tbsbana" y en la columna de la derecha se muestra "net".

      A continuación se muestra el contenido de las notas de la versión para este elemento de línea:

```
conficker:tbsbana 1
variants: net
```

2. En el host de cliente, abra un símbolo del sistema.
3. Realice la acción NSLOOKUP para una dirección URL identificada como un dominio malintencionado conocido.

   Por ejemplo, si se usa la dirección URL `track.bidtrk.com`:

```
C:\>nslookup
 track.bidtrk.com
```


© 2020 Palo Alto Networks, Inc.

```
Server: my-local-dns.local
Address: 10.0.0.222
Non-authoritative answer:
Name: track.bidtrk.com.org
Addresses: fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```

En la salida, observe que la acción NSLOOKUP para el dominio malintencionado se ha falsificado mediante las direcciones IP de sinkhole que configuramos (10.15.0.20). Dado que el dominio coincide con una firma DNS malintencionada, se realiza la acción sinkhole.

4. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y busque la entrada de log de amenaza correspondiente para comprobar si se ha realizado la acción correcta en la solicitud NSLOOKUP.
5. Haga ping a **`track.bidtrk.com`**, lo que genera tráfico de red para la dirección de sinkhole.

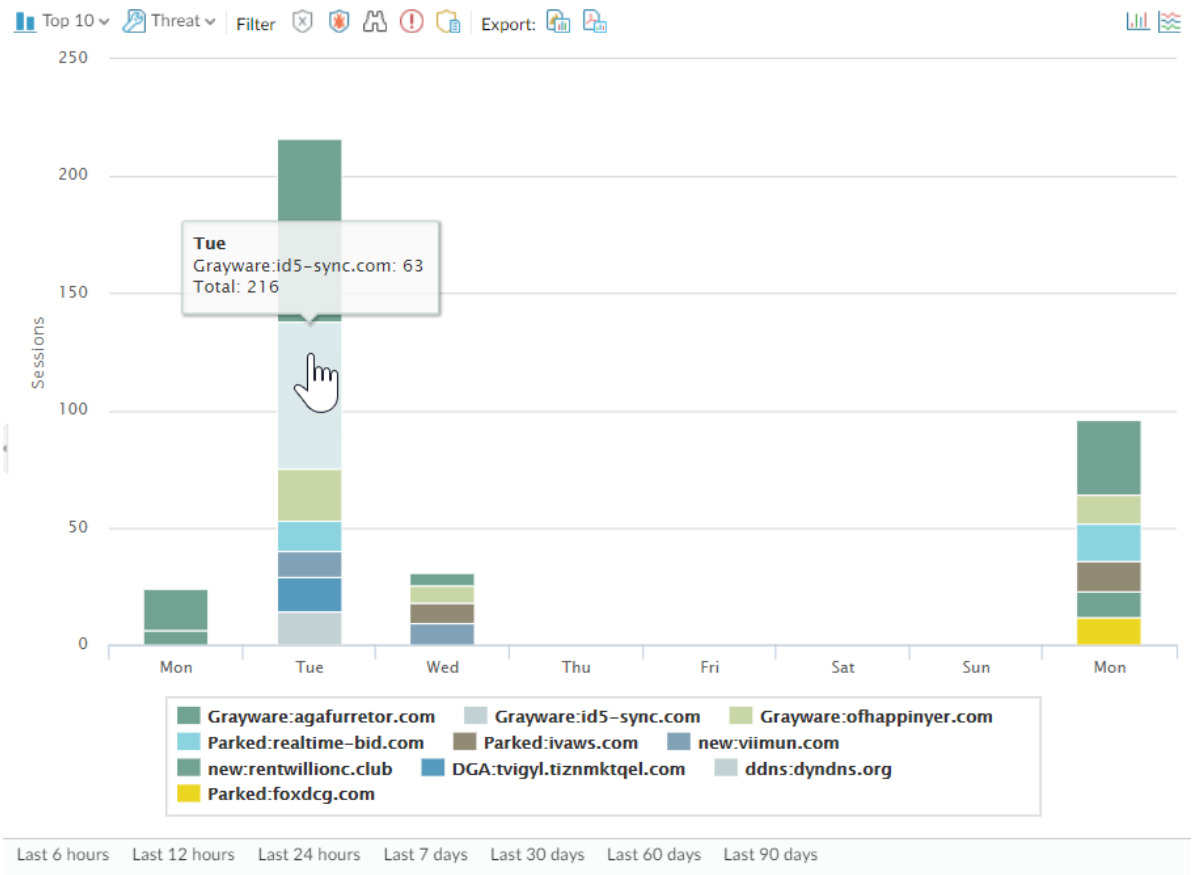
Consulta de hosts infectados que intentan conectar a dominios malintencionados

Después de configurar la función de sinkholing de DNS y comprobar si el tráfico para un dominio malintencionado se dirige a la dirección de sinkhole, debe supervisar regularmente el tráfico para la dirección de sinkhole para poder hacer un seguimiento de los hosts infectados y eliminar la amenaza.

- Utilice Appscope para identificar los hosts de cliente infectados.
  1. Seleccione **Monitor (Supervisar)** > **App Scope** y seleccione **Threat Monitor (Supervisor de amenazas)**.
  2. Haga clic en el botón **Mostrar spyware** de la parte superior de la página mostrada.
  3. Seleccione un intervalo de tiempo.

     En la siguiente captura de pantalla se muestran tres casos de consultas de DNS sospechosas, generadas cuando el host de cliente de prueba realizó una acción NSLOOKUP en un dominio malintencionado conocido. Haga clic en el gráfico para ver más detalles del evento.

© 2020 Palo Alto Networks, Inc.



- Configure un informe personalizado para identificar todos los hosts de cliente que envían tráfico a la dirección IP de sinkhole, que es 10.15.0.20 en este ejemplo.

  Reenvíe la información a un gestor de SNMP, a un servidor Syslog o a Panorama para habilitar las alertas para estos eventos.

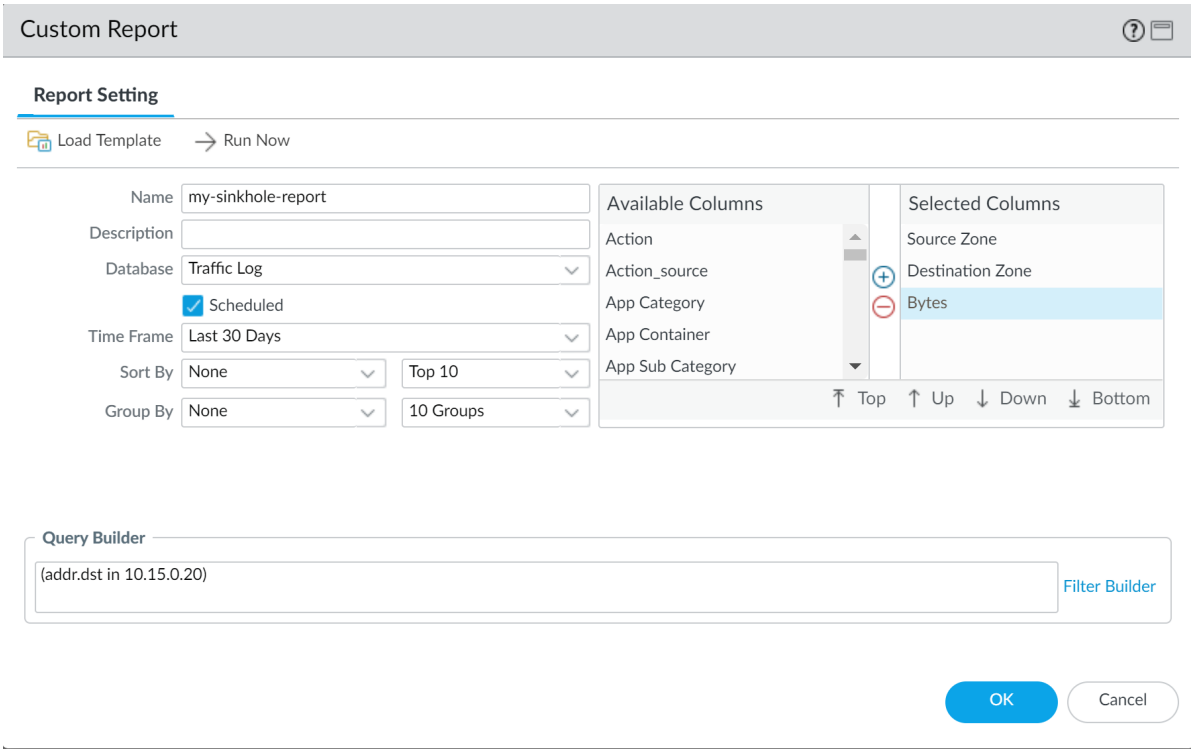
  En este ejemplo, el host de cliente infectado realiza una acción NSLOOKUP para un dominio malintencionado conocido incluido en la base de datos de firmas DNS de Palo Alto Networks. A continuación, la consulta se envía al servidor DNS local, el cual reenvía la solicitud a través del cortafuegos a un servidor DNS externo. La política de seguridad del cortafuegos con el perfil de antispyware configurado coincide con la consulta enviada a la base de datos de firmas DNS, la cual falsifica a continuación la respuesta mediante la dirección de sinkhole de 10.15.0.20 y fd97:3dec:4d27:e37c:5:5:5:5. El cliente intenta iniciar una sesión y el log de tráfico registra la actividad con el host de origen y la dirección de destino, que ahora se dirige a la dirección de sinkhole falsa.

  La visualización del log de tráfico en el cortafuegos permite identificar cualquier host de cliente que envíe tráfico a la dirección de sinkhole. En este ejemplo, los logs muestran que la dirección de origen 192.168.2.10 ha enviado la consulta de DNS malintencionada. A continuación, el host se puede buscar y limpiar. Sin la opción de sinkhole de DNS, el administrador solo vería el servidor DNS local como el sistema que ha realizado la consulta y no vería el host de cliente infectado. Si intenta ejecutar un informe en el log de amenazas mediante la acción “sinkhole”, el log muestra el servidor DNS local, pero no el host infectado.

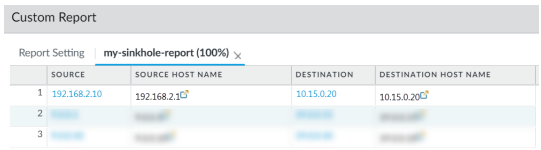
  1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
  2. Haga clic en **Add (Añadir)** y asigne un **Name (Nombre)** al informe.

© 2020 Palo Alto Networks, Inc.

3. Defina un informe personalizado que capture el tráfico para la dirección de sinkhole del modo siguiente:
   - **Base de datos**: seleccione **Registro de tráfico**.
   - **Scheduled (Programado)**: habilite **Scheduled (Programado)** para que el informe se ejecute cada noche.
   - **Período de tiempo**: 30 días.
   - **Selected Columns (Columnas seleccionadas)**: seleccione **Source address (Dirección de origen)** o **Source User (Usuario de origen)** (si ha configurado User-ID) para identificar el host de cliente infectado en el informe y seleccione **Destination address (Dirección de destino)**, la cual será la dirección de sinkhole.
   - En la sección de la parte inferior de la pantalla, cree una consulta personalizada para el tráfico de la dirección de sinkhole (10.15.0.20 en este ejemplo). Puede especificar la dirección de destino en la ventana **Query Builder (Generador de consultas)** (**addr.dst en 10.15.0.20**) o seleccionar lo siguiente en cada columna y hacer clic en **Add (Añadir)**: Connector = and, Attribute = Destination Address, Operator = in y Value = 10.15.0.20. Haga clic en **Add (Añadir)** para añadir la consulta.



4. Haga clic en **Run Now (Ejecutar ahora)** para ejecutar el informe. El informe muestra todos los hosts de cliente que han enviado tráfico a la dirección de sinkhole, lo que indica que es probable que estén infectados. A continuación, puede hacer un seguimiento de los hosts y comprobarlos para detectar spyware.



5. Para ver los informes programados que se han ejecutado, seleccione **Monitor (Supervisar)** > **Reports (Informes)**.

© 2020 Palo Alto Networks, Inc.

Data Filtering

Use los perfiles de filtrado de datos para prevenir que información delicada, confidencial y exclusiva salga de su red. Gracias a los patrones predefinidos, los ajustes integrados y las opciones personalizables, resulta muy fácil proteger los archivos que contienen determinadas propiedades (como títulos o autores de documentos), números de tarjetas de crédito, información regulada de distintos países (como números de la seguridad social) y etiquetas externas de prevención de pérdida de datos (data loss prevention, DLP).

- **Patrones de datos predefinidos**: filtre con facilidad los patrones de uso común, como los números de las tarjetas de crédito. Los patrones predefinidos de filtrado de datos también sirven para identificar determinada información regulada de distintos países, como el número de la seguridad social de EE. UU., el número de identificación del INSEE francés y el número de identificación fiscal de Nueva Zelanda. Muchos de esos patrones permiten cumplir estándares como el Reglamento General de Protección de Datos (RGPD) de la UE o las leyes estadounidenses de seguros médicos (Health Insurance Portability and Accountability Act, HIPAA) o de servicios financieros (Gramm-Leach-Bliley).
- **Compatibilidad integrada con Azure Information Protection y TITUS Classification System**: las propiedades predefinidas de los archivos permiten filtrar el contenido en función de las etiquetas de Azure Information Protection y de TITUS. Las etiquetas de Azure Information Protection se almacenan en los metadatos, así que debe comprobar que conoce el GUID de las etiquetas que debe filtrar el cortafuegos.
- **Patrones de datos personalizados para soluciones de DLP**: si utiliza alguna solución externa de DLP de terminales para señalar que hay contenido confidencial en las propiedades de los archivos, cree un patrón de datos personalizado para identificar las propiedades y los valores etiquetados por dicha solución y, a continuación, registre o bloquee los archivos que detecte el perfil de filtrado de datos basándose en el patrón.

Creación de perfiles de filtrado de datos

Los perfiles de filtrado de datos sirven para evitar que la información confidencial salga de la red.

Para empezar, cree un patrón de datos que especifique los tipos y los campos de información que debe filtrar el cortafuegos. Luego, vincule ese patrón al perfil de filtrado de datos que especifica cómo se debe aplicar el contenido que filtra el cortafuegos. Añada el perfil de filtrado de datos a una regla de la política de seguridad para empezar a filtrar el tráfico que coincida con ella.

STEP 1 | Defina un nuevo objeto de patrón de datos para detectar la información que desea filtrar.

1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **Data Patterns (Patrones de datos)** y luego **Add (Añadir)** para añadir un nuevo objeto.
2. Proporcione un nombre descriptivo para el nuevo objeto en **Name (Nombre)**.
3. (Opcional) Seleccione **Shared (Compartido)** si desea que el patrón de datos esté disponible para lo siguiente:
   - **Every virtual system (vsys) on a multi-vsys firewall (Cada sistema virtual [vsys] en un cortafuegos de varios vsys)**: si no está marcada (deshabilitada), el patrón de datos está disponible solo para el sistema virtual seleccionado en la pestaña **Objects (Objetos)**.
   - **Every device group on Panorama (Cada grupo de dispositivos en Panorama)**: si no está marcada (deshabilitada), el patrón de datos está disponible solo para el grupo de dispositivos seleccionado en la pestaña **Objects (Objetos)**.
4. ((Opcional, Panorama únicamente) Seleccione **Disable override (Deshabilitar cancelación)** para evitar que los administradores cancelen la configuración de este objeto de patrón de datos en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo

© 2020 Palo Alto Networks, Inc.

que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.

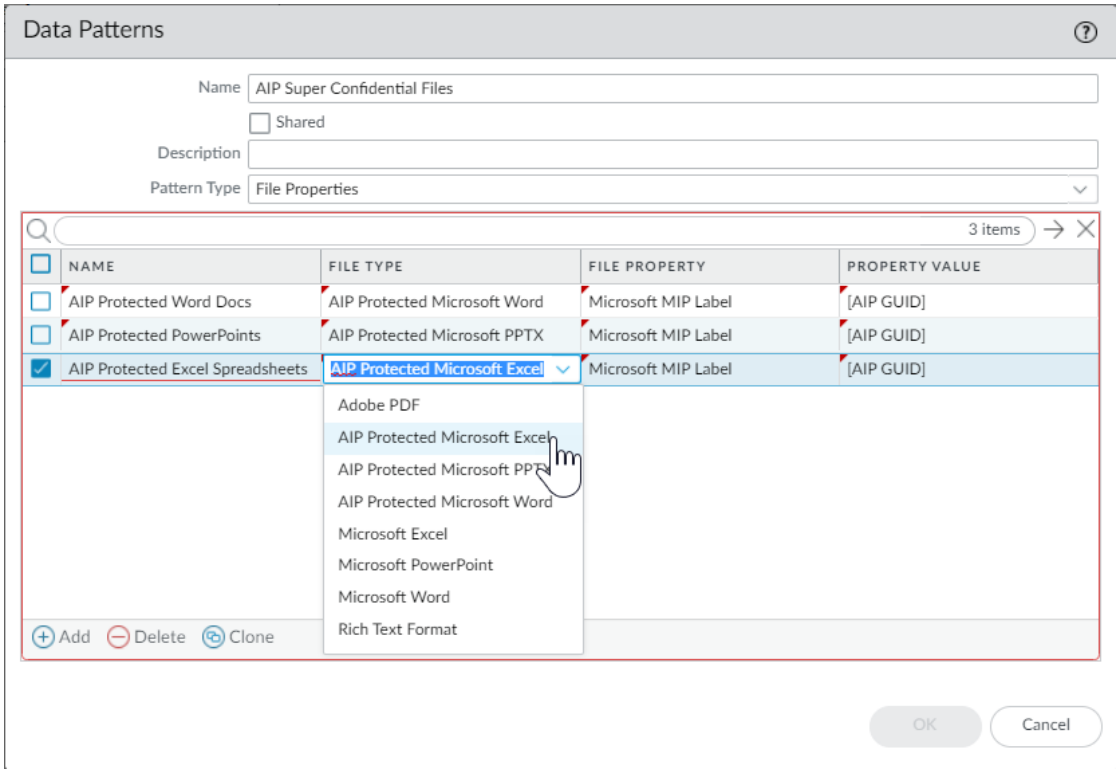
5. (Opconal: Panorama únicamente) Seleccione **Data Capture (Captura de datos)** para recopilar automáticamente los datos bloqueados por el filtro.

   Especifique una contraseña para Manage Data Protection (Gestionar protección de datos) en la página Settings (Configuración) para ver sus datos capturados (Device [Dispositivo] > Setup [Configuración] > Content-ID > Manage Data Protection [Gestionar protección de datos]).

6. Configure el **Pattern Type (Tipo de patrón)** con una de las siguientes opciones:
   - **Predefined Pattern (Patrón predefinido)**: filtre tarjetas de crédito, números de la seguridad social e información de identificación personal para cumplir varios estándares, como el Reglamento General de Protección de Datos (RGPD) de la UE o las leyes estadounidenses de seguros médicos (Health Insurance Portability and Accountability Act, HIPAA) o de servicios financieros (Gramm-Leach-Bliley).
   - **Regular Expression (Expresión regular)**: filtre patrones de datos personalizados.
   - **File Properties (Propiedades de archivo)**: filtre según propiedades de archivo y los valores asociados.
7. Seleccione **Add (Añadir)** para añadir una nueva regla al objeto de patrón de datos.
8. Especifique el patrón de datos según el **Pattern Type (Tipo de patrón)** que seleccionó para este objeto:
   - **Predefined (Predefinido)**: seleccione el nombre en **Name (Nombre)** y, a continuación, el patrón predefinido por el que se deben filtrar los datos.
   - **Regular Expression (Expresión regular):** especifique un **Name (Nombre)** descriptivo, seleccione el **File Type (Tipo de archivo)** (uno o varios) que desea analizar y luego el **Data Pattern (Patrón de datos)** específico que desea que el cortafuegos detecte.
   - **File Properties (Propiedades de archivo):** especifique un **Name (Nombre)** descriptivo, seleccione el **File Type (Tipo de archivo)** y la **File Property (Propiedad de archivo)** que desea analizar, e ingrese el **Property Value (Valor de propiedad)** específico que desea que el cortafuegos detecte.
     - **Para filtrar los documentos clasificados con TITUS**: seleccione uno de los tipos de archivos protegidos distinto de AIP y configure **File Property (Propiedad de archivo)** en TITUS GUID (GUID de TITUS). Introduzca el GUID de la etiqueta de TITUS en **Property Value (Valor de propiedad)**.
     - **Para filtrar los documentos con etiquetas de Azure Information Protection**: seleccione cualquier valor en **File Type (Tipo de archivo)**, excepto Rich Text Format (Formato RTF). Tras elegir el tipo de archivo, configure Microsoft MIP Label (Etiqueta de Microsoft Information Protection) en **File Property (Propiedad de archivo)** e introduzca el GUID de la etiqueta de Azure Information Protection en **Property Value (Valor de propiedad)**.

© 2020 Palo Alto Networks, Inc.



9. Haga clic en **OK (Aceptar)** para guardar el patrón de datos.

STEP 2 | Añada el objeto del patrón de datos a un perfil de filtrado de datos.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Data Filtering (Filtrado de datos)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de datos.
2. Proporcione un nombre descriptivo para el nuevo perfil en **Name (Nombre)**.
3. Haga clic en **Add (Añadir)** para añadir una nueva regla de perfil y seleccione el patrón de datos creado en el otro paso.
4. Especifique las **Applications (Aplicaciones)**, **File Types (Tipos de archivo)** y qué **Direction (Dirección)** de tráfico (carga o descarga) desea filtrar según el patrón de datos.

   Debe seleccionar el mismo tipo de archivo antes definido para el patrón de datos o bien un tipo que incluya el tipo de archivo del patrón de datos. Por ejemplo, podría definir el objeto de patrón de datos y el perfil de filtrado de datos para analizar todos los documentos de Microsoft Office. También podría definir el objeto de patrón de datos de modo que coincida solo con presentaciones de Microsoft PowerPoint, aunque el perfil de filtrado de datos analice todos los documentos de Microsoft Office.

   Si un objeto de patrón de datos se adjunta a un perfil de filtrado de datos y los tipos de archivo configurados no se alinean entre los dos, el perfil no filtrará correctamente los documentos que coincidan con el objeto de patrón de datos.
5. Configure el **Alert Threshold (Umbral de alerta)** para especificar las veces que el patrón de datos debe detectarse en un archivo para que se active una alerta.
6. Configure el **Block Threshold (Umbral de bloqueo)** para bloquear los archivos que contengan al menos esta cantidad de instancias del patrón de datos.
7. Configure la **Log Severity (Gravedad de log)** registrada para los archivos que coinciden con esta regla.
8. Haga clic en **OK (Aceptar)** para guardar el perfil de filtrado de datos.

STEP 3 | Aplique el ajuste del filtrado de datos al tráfico.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
2. Seleccione **Actions (Acciones)** y defina Profile Type (Tipo de perfil) en **Profiles (Perfiles)**.
3. Vincule el perfil de filtrado de datos creado en el paso 2 a la regla de la política de seguridad.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | (Recomendado) Evite que los exploradores web reanuden sesiones que el cortafuegos ha finalizado.



Esta opción garantiza que, cuando el cortafuegos detecte y luego descarte un archivo delicado, el explorador web no pueda reanudar la sesión en un intento por recuperar el archivo.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** y edite la configuración de Content-ID.
2. Borre la opción **Allow HTTP partial response (Habilitar respuesta parcial HTTP)**.
3. Haga clic en **OK (Aceptar)**.

STEP 5 | Supervise los archivos que el cortafuegos está filtrando.

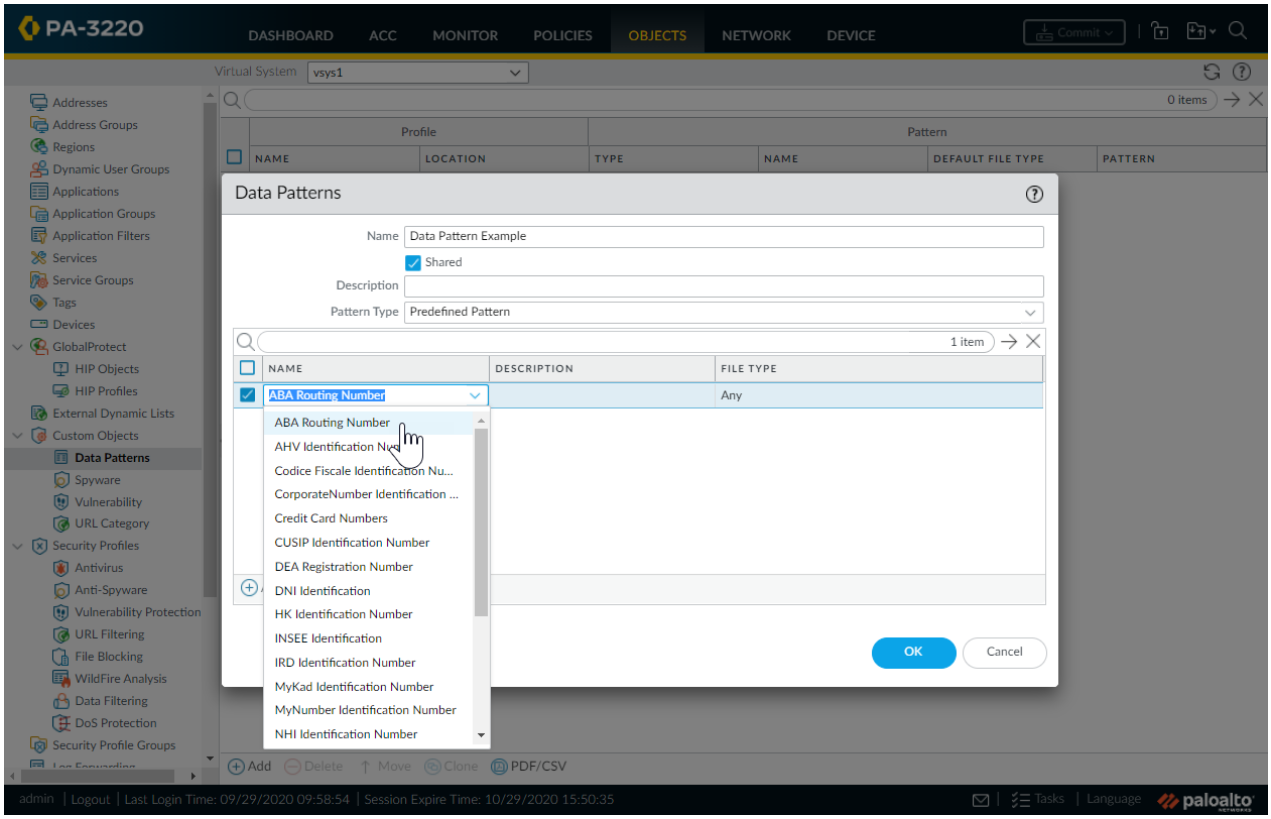
Seleccione **Monitor (Supervisar)** > **Data Filtering (Filtrado de datos)** para visualizar los archivos que el cortafuegos ha detectado y bloqueado según sus ajustes de filtrado de datos.

Patrones predefinidos de filtrado de datos

Para cumplir estándares como el Reglamento General de Protección de Datos (RGPD) de la UE o las leyes estadounidenses de seguros médicos (Health Insurance Portability and Accountability Act, HIPAA) o de servicios financieros (Gramm-Leach-Bliley), el cortafuegos proporciona patrones de datos predefinidos. Puede usar estos patrones para evitar que tipos comunes de información confidencial, como los números de las tarjetas de crédito o de la seguridad social, salgan de la red.

Para localizar los patrones de datos predefinidos, seleccione **Objects (Objetos) > Custom Objects (Objetos personalizados) > Data Patterns (Patrones de datos)** y haga clic en **Add (Añadir)** para crear un objeto. A continuación, configure **Pattern Type (Tipo de patrón)** en **Predefined Pattern (Patrón predefinido)** y haga clic en **Add (Añadir)** para añadir una regla nueva al objeto de patrón de datos. Seleccione un patrón de datos en la lista que aparece en la columna **Name (Nombre)**.

© 2020 Palo Alto Networks, Inc.



Si la información que desea proteger no figura en la lista de patrones predefinidos, cree uno personalizado con una expresión regular.

Estos son los patrones de datos disponibles:

Patrón	Description (Descripción)
Credit Card Numbers (Números de tarjetas de crédito)	Números de tarjetas de crédito de 16 cifras
Social Security Numbers (Números de la seguridad social)	Números de la seguridad social de 9 cifras con guiones
Social Security Numbers (without dash separator) (Números de la seguridad social sin guiones)	Números de la seguridad social de 9 cifras sin guiones
ABA Routing Number (Número de ruta de ABA)	Número de ruta de la asociación bancaria estadounidense American Bankers Association
AHV Identification Number (Número de identificación de AHV)	Alters- und Hinterlassenenversicherungsnummer: número de los seguros suizos de planes de pensiones y pensiones de supervivencia
Codice Fiscale Identification Number (Número de identificación de Codice Fiscale)	Número de identificación fiscal de Italia

© 2020 Palo Alto Networks, Inc.

Patrón	Description (Descripción)
CorporateNumber Identification Number (Número de identificación de persona jurídica)	Código de identificación fiscal de Japón
CUSIP Identification Number (Número de identificación CUSIP)	Número de identificación de la comisión encargada de uniformar los instrumentos financieros (Committee on Uniform Security Identification Procedures) de la ABA estadounidense
DEA Registration Number (Número de registro de la DEA)	EE. UU. Número de registro de la dirección estadounidense de lucha contra la droga (Drug Enforcement Administration)
DNI Identification Number (DNI)	Número del documento nacional de identidad de España
HK Identification Number (Número de identificación de Hong Kong)	Número de identificación de residentes en Hong Kong
INSEE Identification Number (Número de identificación del INSEE)	Número de identificación del instituto nacional de estadística de Francia
IRD Identification Number (Número de identificación fiscal)	Número de identificación fiscal de Nueva Zelanda
MyKad Identification Number (Número de identificación de MyKad)	Número del documento de identidad de Malasia
MyNumber Identification Number (Número de identificación personal)	Número de identificación fiscal y de la seguridad social de Japón
NHI Identification Number (Número de la seguridad social)	Número de la seguridad social de Nueva Zelanda
NIF Identification Number (NIF)	Número de identificación fiscal de España
NIN Identification Number (Número de identificación de Taiwán)	Número del documento de identidad de Taiwán
NRIC Identification Number (Número de identificación de Singapur)	Número del documento nacional de identidad de Singapur
Permanent Account Identification Number (Número de identificación de cuenta permanente)	Número de cuenta permanente de los ciudadanos indios
PRC Identification Number (Número de identificación de China)	Número de identificación de residentes de la República Popular China
PRN Identification Number (Número de residencia permanente)	Número del registro de residentes de la República de Corea

© 2020 Palo Alto Networks, Inc.

Patrón	Description (Descripción)
Republic of South Korea Resident Registration (Registro de residentes en Corea del Sur)	Número del registro de residentes de la República de Corea

© 2020 Palo Alto Networks, Inc.

WildFire Inline ML

La opción WildFire Inline ML (Aprendizaje automático en línea de WildFire) presente en el perfil de antivirus permite que el plano de datos del cortafuegos aplique el aprendizaje automático en archivos ejecutables portátiles (PE, Portable Executable) y scripts de PowerShell en tiempo real. Esta capa de protección antivirus complementa las firmas basadas en WildFire para proporcionar una cobertura ampliada para archivos cuyas firmas aún no existen. Cada modelo de aprendizaje automático en línea detecta dinámicamente archivos maliciosos de un tipo específico mediante la evaluación de los detalles del archivo, incluidos los campos y patrones del descodificador, para formular una clasificación de alta probabilidad de un archivo. Esta protección se extiende a variantes de amenazas actualmente desconocidas y futuras que coinciden con características que Palo Alto Networks ha identificado como maliciosas. Para mantenerse al día con los últimos cambios en el panorama de las amenazas, se añaden o actualizan modelos de aprendizaje automático en línea a través de lanzamientos de contenido. Para poder habilitar WildFire Inline ML (Aprendizaje automático en línea de WildFire), debe poseer una suscripción activa a WildFire.

La protección basada en aprendizaje automático en línea también se puede habilitar para detectar URL maliciosas en tiempo real como parte de su configuración de filtrado de URL. Para obtener más información, consulte ML en línea de filtrado de URL.

El aprendizaje automático en línea de WildFire no es compatible en el dispositivo virtual VM-50 o VM50L.

Configuración de WildFire Inline ML (Aprendizaje automático en línea de WildFire)

Para habilitar su configuración de WildFire Inline ML (Aprendizaje automático en línea de WildFire), adjunte el perfil de antivirus configurado con los ajustes de aprendizaje en línea a una regla de la política de seguridad (consulte Configuración de antivirus, antispyware y protección frente a vulnerabilidades).

WildFire Inline ML (Aprendizaje automático en línea de WildFire) no es compatible actualmente en el dispositivo virtual VM-50 o VM50L.

STEP 1 | Para aprovechar WildFire Inline ML (Aprendizaje automático en línea de WildFire), debe tener una suscripción activa a WildFire para analizar los archivos ejecutables de Windows.

Verifique que tenga una suscripción a WildFire. Para verificar las suscripciones para las que tiene licencias actualmente, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.

WildFire License

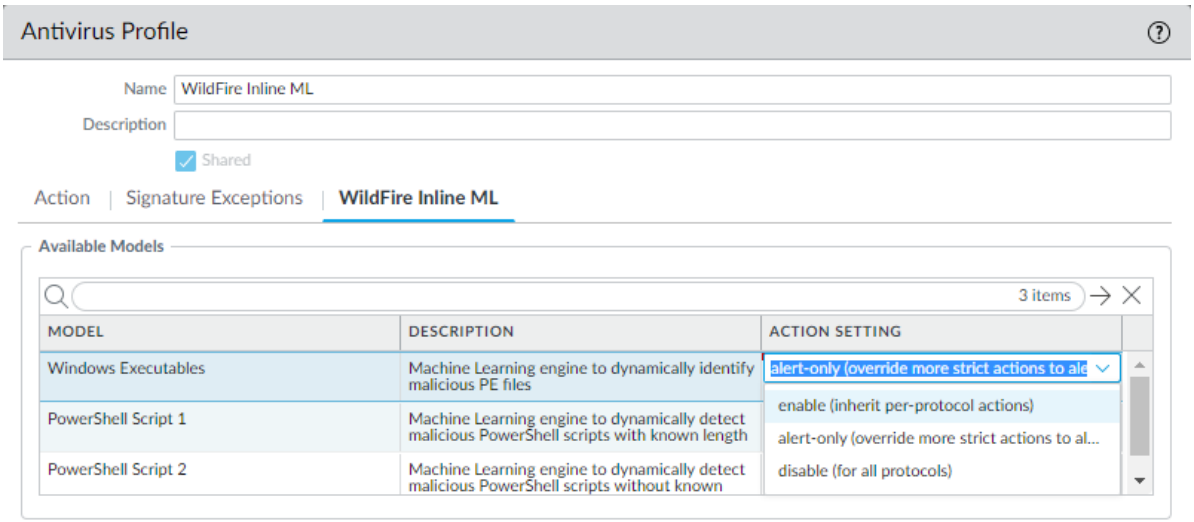
Date Issued	July 25, 2019
Date Expires	July 25, 2020
Description	WildFire signature feed, integrated WildFire logs, WildFire API

STEP 2 | Cree un nuevo perfil o actualice sus perfiles de seguridad de antivirus existentes para utilizar los modelos de WildFire Inline ML (Aprendizaje automático en línea de WildFire) en tiempo real.

1. Seleccione un **perfil de antivirus** existente o cree uno nuevo (seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Antivirus** y **añada** un nuevo perfil.

© 2020 Palo Alto Networks, Inc.

2. Configure su perfil de antivirus.
3. Seleccione la pestaña **WildFire Inline ML (Aprendizaje automático en línea de WildFire)** y aplique una **configuración de acción** para cada modelo de WildFire Inline ML (Aprendizaje automático en línea de WildFire). Esto aplica la configuración de las acciones de WildFire Inline ML (Aprendizaje automático en línea de WildFire) configuradas para cada protocolo en función del modelo. Actualmente, hay tres motores de clasificación disponibles: Archivos ejecutables de Windows, scripts de PowerShell 1 y scripts de PowerShell 2.



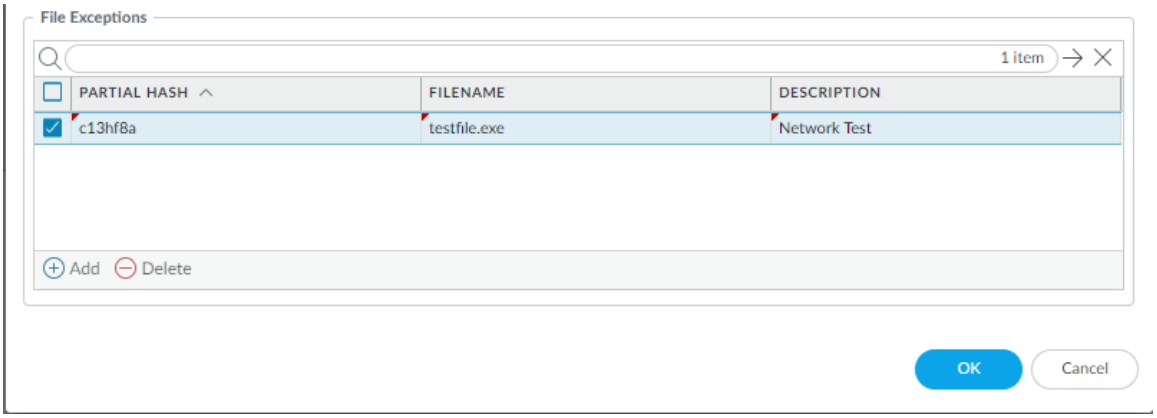
- **enable (inherit per-protocol actions) [habilitar (heredar acciones según el protocolo)]**: WildFire inspecciona el tráfico de acuerdo con sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de decodificadores de la pestaña **Action (Acción)**.
- **alert-only (override more strict actions to alert) [solo alerta (sobrescribir acciones más estrictas para la alerta)]**: WildFire inspecciona el tráfico según sus selecciones en la columna WildFire Inline ML Action (Acción de aprendizaje automático en línea de WildFire) en la sección de descodificadores de la pestaña **Action (Acción)** y cancela cualquier acción con un nivel de gravedad superior a `alert (alerta)` (`drop (descartar)`, `reset-client (restablecer cliente)`, `reset-server (restablecer servidor)`, `reset-both (restablecer ambos)`) `alert (alerta)`, que permite que el tráfico pase mientras sigue generando y guardando una alerta en los logs de amenazas.
- **disable (for all protocols) [deshabilitar (para todos los protocolos)]**: WildFire permite que el tráfico pase sin ninguna acción de la política.

4. Haga clic en **OK (Aceptar)** para salir de la ventana de configuración del perfil de antivirus y **confirmar** su nueva configuración.

STEP 3 | (Opcional) Añada excepciones de archivo a su perfil de seguridad de antivirus si encuentra falsos positivos. Puede añadir los detalles de la excepción del archivo directamente a la lista de excepciones o especificar un archivo de los logs de amenazas.

- Añada excepciones de archivos directamente a la lista de excepciones.
  1. Seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Antivirus**.
  2. Seleccione un perfil de antivirus para el que desee excluir archivos específicos y, a continuación, seleccione **WildFire Inline ML (Aprendizaje automático en línea de WildFire)**.
  3. Añada el hash, el nombre de archivo y la descripción del archivo que desee excluir de la aplicación.

© 2020 Palo Alto Networks, Inc.



4. Haga clic en **OK (Aceptar)** para guardar el perfil de antivirus y, a continuación, **confirme** las actualizaciones.

- Añada excepciones de archivos a partir de las entradas de los logs de amenazas.

1. Seleccione **Monitor (Supervisar) > Logs > Threat (Amenaza)** y filtre los logs por el tipo de amenaza **ml-virus (virus de aprendizaje automático)**. Seleccione un log de amenazas para un archivo para el que desee crear una excepción de archivo.
2. Vaya a la **vista de log detallada** y desplácese hacia abajo hasta el panel **Details** y, a continuación, seleccione **Create Exception (Crear excepción)**.



3. Añada una **descripción** y haga clic en **OK (Aceptar)** para añadir la excepción del archivo.
4. La nueva excepción de archivo se puede encontrar en la lista **File Exceptions (Excepciones de archivo)** en **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Antivirus > WildFire Inline ML (Aprendizaje automático en línea de WildFire)**.

STEP 4 | (Opcional) Verifique el estado de la conectividad del cortafuegos con el servicio en la nube de aprendizaje automático en línea.

Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

```
show mlav cloud-status
```

Por ejemplo:

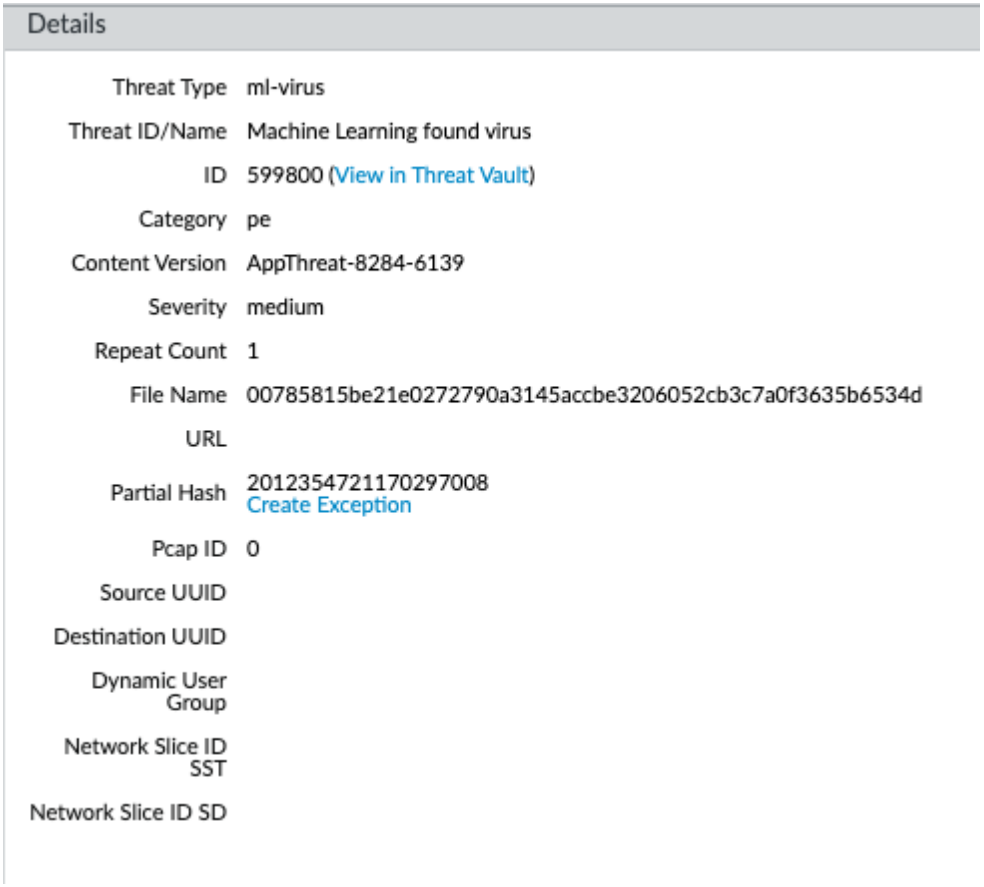
```
show mlav cloud-status

MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
Cloud connection:              connected
```

Si no puede conectarse al servicio en la nube de aprendizaje automático en línea, verifique que el siguiente dominio no esté bloqueado: ml.service.paloaltonetworks.com.

Para ver información sobre los archivos que se han detectado con WildFire Inline ML (Aprendizaje automático en línea de WildFire), examine los logs de amenazas (**Monitor (Supervisar) > Logs > Threat (Amenaza)** y, a continuación, seleccione el tipo de log de la lista). Los archivos que se han analizado con WildFire inline ML (Aprendizaje automático en línea de WildFire) están etiquetados con el tipo de amenaza **ml-virus (virus de aprendizaje automático)**:

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Configuración de bloqueo de archivos

Los perfiles de bloqueo de archivos le permiten identificar tipos de archivos específicos que desee bloquear o supervisar. En la mayor parte del tráfico (incluido el de su red interna), bloquee los archivos que transportan amenazas a ciencia cierta o que no tienen ninguna utilidad real de carga o descarga. Actualmente, estos incluyen archivos por lotes, DLL, archivos de clase Java, archivos de ayuda, accesos directos de Windows (.lnk), y archivos BitTorrent. Además, para brindar protección contra descargas ocultas, permita la carga o la descarga de ejecutables y archivos comprimidos (.zip y .rar) pero con la confirmación obligatoria de los usuarios. De ese modo, advierten si el navegador intenta descargar algo sin su conocimiento. En cuanto a las reglas de las políticas que permiten la navegación web general, aplique medidas más estrictas con el bloqueo de archivos, ya que existe mucho más riesgo de que los usuarios descarguen accidentalmente archivos malintencionados. Vincule un perfil de bloqueo de archivos más estricto a este tipo de tráfico, que bloquee también los archivos portables ejecutables (portable executable, PE).

Al aplicar el bloqueo de archivos a una regla de la política de seguridad, puede definir sus propios perfiles de bloqueo de archivos o bien elegir uno de los perfiles predefinidos que se explican a continuación. Puede clonar y editar los perfiles predefinidos, que están disponibles con la versión de contenido 653 y las actualizaciones posteriores. Después, siga los pasos para realizar la transición segura a los perfiles de bloqueo de archivos recomendados para mantener la disponibilidad de las aplicaciones mientras configura los ajustes recomendados para el bloqueo de archivos:

- **basic file blocking (bloqueo de archivo básico)**: adjunte este perfil para las reglas de política de seguridad que permiten el tráfico hacia y desde las aplicaciones menos sensibles para bloquear archivos que habitualmente se incluyen en campañas de ataques de malware o que no tienen un caso de uso real para la carga/descarga. Este perfil bloquea la carga y descarga de archivos PE (.scr, .cpl, .dll, .ocx, .pif, .exe), archivos Java (.class, .jar), archivos de ayuda (.chm, .hlp) y otros archivos posiblemente malintencionados, incluidos .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. Además, solicita a los usuarios una confirmación al intentar descargar archivos rar o zip cifrados. Esta regla alerta sobre todos los otros tipos de archivo, a fin de brindarle visibilidad completa de todos los tipos de archivo que entran a la red y que salen de ella.
- **strict file blocking (bloqueo de archivo estricto)**: use este perfil más estricto en las reglas de política de seguridad que permiten el acceso a sus aplicaciones más delicadas. Este perfil bloquea los mismos tipos de archivo que el otro perfil, y además bloquea archiso flash, .tar, codificación multinivel, .cab, .msi, y archivos rar y zip cifrados.

Estos perfiles predefinidos están diseñados para brindar la posición más segura para su red. Sin embargo, si tiene aplicaciones de misión crítica que dependen de algunas de las aplicaciones que están bloqueadas en estos perfiles predeterminados, puede clonar los perfiles y modificarlos según fuera necesario. Use los perfiles modificados solo para los usuarios que deban cargar o descargar tipos de archivos peligrosos. Además, para reducir la superficie de ataque, asegúrese de usar otras medidas de seguridad para garantizar que los archivos que sus usuarios están cargando y descargando no supongan una amenaza para su organización. Por ejemplo, si debe permitir la descarga de archivos PE, asegúrese de enviar todos los archivos PE desconocidos a WildFire para su análisis. Además, mantenga una política de filtrado de URL estricta para garantizar que los usuarios no puedan descargar contenido de sitios web conocidos por alojar contenido malintencionado.

STEP 1 | Cree el perfil de bloqueo de archivos.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **File Blocking (Bloqueo de archivos)** y **Add (Añadir)** para añadir un perfil.
2. En **Name (Nombre)**, ingrese un nombre para el perfil de bloqueo de archivos, por ejemplo, **`Block_EXE`**.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Introduzca una descripción en **Description**, como **`Bloquear la descarga de archivos exe desde sitios web por parte de usuarios`**.
4. (Opcional) Especifique que el perfil sea **Shared (Compartido)** con:
   - **Every virtual system (vsys) on a multi-vsys firewall (Cada sistema virtual [vsys] en un cortafuegos de varios vsys)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el sistema virtual seleccionado en la pestaña **Objects (Objetos)**.
   - **Every device group on Panorama (Cada grupo de dispositivos en Panorama)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el grupo de dispositivos seleccionado en la pestaña **Objects (Objetos)**.
5. (Opcional, Panorama únicamente) Seleccione **Disable override (Deshabilitar cancelación)** para evitar que los administradores cancelen la configuración de este perfil de bloqueo de archivos en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden cancelar la configuración de cualquier grupo de dispositivos que hereda el perfil.

STEP 2 | Configure las opciones de bloqueo de archivos.

1. Haga clic en **Add (Añadir)** y defina una regla para el perfil.
2. En **Name**, ingrese un nombre para la regla; por ejemplo, **`BlockEXE`**.
3. Seleccione **Any (Cualquiera)** o especifique una o más **Applications (Aplicaciones)** para filtrar, tal como **web-browsing (navegación web)**.

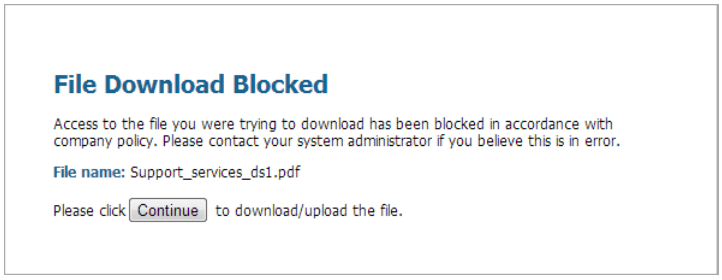
   Solo los exploradores web pueden mostrar la página de respuesta (mensaje para continuar) que permite a los usuarios confirmar que su elección de otra aplicación derive en tráfico bloqueado para esas aplicaciones, debido a que no se muestra un mensaje a los usuarios que les permita continuar.
4. Seleccione **Any (Cualquiera)** o especifique uno o más **File Types (Tipos de archivo)**, tal como **exe**.
5. Especifique la **Direction (Dirección)**, tal como **download (descarga)**.
6. Especifique la **Action (Acción)** (**alert [alertar]**, **block [bloquear]** o **continue [continuar]**). Por ejemplo, seleccione **continue (continuar)** a fin de solicitar una confirmación a los usuarios para permitirles descargar un archivo ejecutable (.exe). O bien, puede elegir **block (bloquear)** para bloquear archivos especificados o puede configurar el cortafuegos para que active un **alert (alerta)** cuando un usuario descargue un archivo ejecutable.
7. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Aplique el perfil de bloqueo de archivos a una política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla de política existente o seleccione **Add (Añadir)** para crear una nueva regla según se describe en Configuración de una política de seguridad básica.
2. En la pestaña **Actions (Acciones)**, seleccione el perfil de bloqueo de archivo en el paso anterior. En este ejemplo, el nombre de perfil es **`Block_EXE`**.
3. Seleccione **Commit (Confirmar)** para confirmar la configuración.

STEP 4 | Para comprobar su configuración de bloqueo de archivos, acceda a un ordenador de endpoint en la zona fiable del cortafuegos y trate de descargar un archivo ejecutable desde un sitio web en la zona no fiable. Debería aparecer una página de respuesta. Haga clic en **Continue (Continuar)** para confirmar que puede descargar el archivo. También puede establecer otras acciones, como **alert (alertar)** o **block (bloquear)**, que no proporcionarán al usuario una página que le pregunte si desea continuar. A continuación se muestra la página de respuesta predeterminada de File Blocking (Bloqueo de archivos):

© 2020 Palo Alto Networks, Inc.



STEP 5 | (Opcional) Defina páginas de respuesta de bloqueo de archivos personalizadas (**Device [Dispositivo]** > **Response Pages [Páginas de respuesta]**). Esto le permite ofrecer más información a los usuarios cuando ven una página de respuesta. Puede incluir información como la información de políticas de empresa e información de contacto de un departamento de soporte técnico.

Cuando crea un perfil de bloqueo de archivos con la acción continue (continuar), únicamente puede elegir la aplicación de web-browsing (navegación web). Si elige cualquier otra aplicación, el tráfico que coincida con la política de seguridad no fluirá hacia el cortafuegos debido a que los usuarios no tendrán una opción de continuar. Además, deberá configurar y habilitar una política de descifrado para los sitios web HTTPS.

Compruebe sus logs para determinar la aplicación utilizada para comprobar esta función. Por ejemplo, si está usando Microsoft Sharepoint para descargar archivos, incluso aunque esté usando un navegador web para acceder al sitio, la aplicación en realidad es `sharepoint-base` *o* `sharepoint-document`*. (Puede resultar útil configurar el tipo de aplicación como Any [Cualquiera] para la comprobación).*

© 2020 Palo Alto Networks, Inc.

Prevención de ataques de fuerza bruta

Un ataque de fuerza bruta utiliza un gran volumen de solicitudes/respuestas de la misma dirección IP de origen o destino para introducirse en un sistema. El atacante emplea un método de ensayo y error para adivinar la respuesta a un reto o una solicitud.

El perfil de protección contra vulnerabilidades del cortafuegos incluye firmas para protegerle de ataques de fuerza bruta. Cada firma tiene un ID, nombre de amenaza y gravedad, y se activa cuando se registra un patrón. El patrón especifica las condiciones y el intervalo en los que el tráfico se identifica como un ataque de fuerza bruta; algunas firmas están asociadas a otra firma secundaria de una gravedad menor que especifica el patrón con el que debe coincidir. Cuando un patrón coincide con la firma o la firma secundaria, activa la acción predeterminada de la firma.

Para aplicar la protección:

- Adjunte el perfil de protección frente a vulnerabilidades a una regla de la política de seguridad. Consulte Configuración de antivirus, antispyware y protección frente a vulnerabilidades.
- Instale actualizaciones de contenido que incluyan nuevas firmas para proteger ante amenazas emergentes. Consulte Instalación de las actualizaciones de contenido y software.

© 2020 Palo Alto Networks, Inc.

Personalización de la acción y las condiciones de activación para una firma de fuerza bruta

El cortafuegos incluye dos tipos de firmas de fuerza bruta predefinidas: firma principal y firma secundaria. Una firma secundaria es una única incidencia de un patrón de tráfico que coincide con la firma. Una firma principal está asociada a una firma secundaria y se activa cuando se producen varios eventos dentro de un intervalo de tiempo, que coinciden con el patrón de tráfico definido en la firma secundaria.

Por lo general, una firma secundaria tiene de manera predeterminada la acción *permitir*, porque un único evento no es indicativo de un ataque. Esto garantiza que el tráfico legítimo no se bloquee y evita generar logs de amenaza para los eventos que no merecen atención. Palo Alto Networks le recomienda que no cambie la acción predeterminada sin antes considerarlo detenidamente.

En la mayoría de los casos, la firma de fuerza bruta es un evento destacado debido a su patrón recurrente. Si fuera necesario, puede realizar una de las siguientes opciones para personalizar la acción para una firma de fuerza bruta:

- Cree una regla para modificar la acción predeterminada para todas las firmas de la categoría de fuerza bruta. Puede optar por permitir, alertar, bloquear, restablecer o descartar el tráfico.
- Defina una excepción para una firma específica. Por ejemplo, puede buscar y definir una excepción para CVE.

Para una firma principal, puede modificar tanto las condiciones de activación como la acción; para una firma secundaria, solamente puede modificar la acción.



Para mitigar un ataque de manera eficaz, especifique la acción Bloquear dirección IP en lugar de la acción Eliminar o Restablecer para la mayoría de firmas de fuerza bruta.

STEP 1 | Cree un nuevo perfil de protección contra vulnerabilidades.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)** y **Add (Añadir)** para añadir un perfil.
2. Especifique un nombre en **Name** para el perfil de protección frente a vulnerabilidades.
3. (Opcional) Introduzca una **descripción**.
4. (Opcional) Especifique que el perfil sea **Shared (Compartido)** con:
   - **Every virtual system (vsys) on a multi-vsys firewall (Cada sistema virtual [vsys] en un cortafuegos de varios vsys)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el sistema virtual seleccionado en la pestaña **Objects (Objetos)**.
   - **Every device group on Panorama (Cada grupo de dispositivos en Panorama)**: si no está marcada (deshabilitada), el perfil está disponible únicamente para el grupo de dispositivos seleccionado en la pestaña **Objects (Objetos)**.
5. (Opcional, Panorama únicamente) Seleccione **Disable override (Deshabilitar cancelación)** para evitar que los administradores cancelen la configuración de este perfil de protección frente a vulnerabilidades en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden cancelar la configuración de cualquier grupo de dispositivos que hereda el perfil.

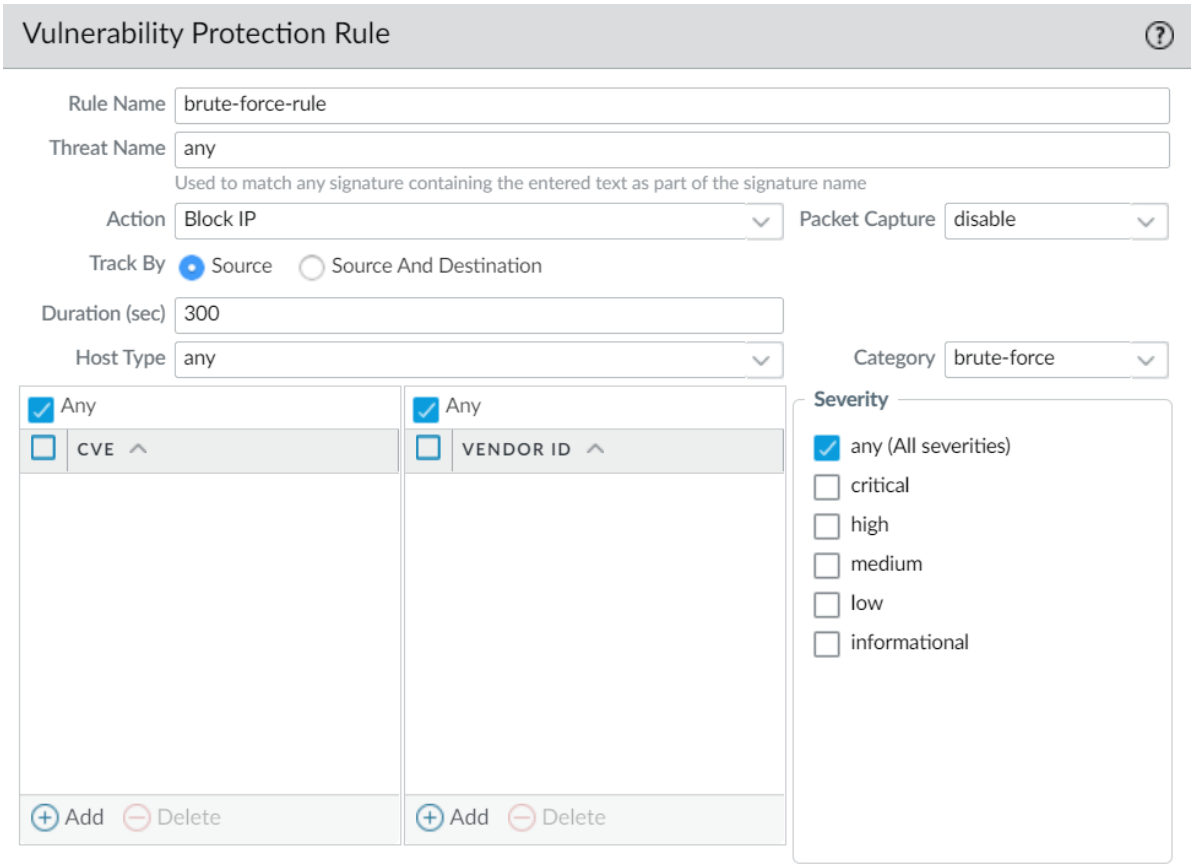
STEP 2 | Cree una regla que defina la acción para todas las firmas de una categoría.

1. En la pestaña **Rules (Reglas)**, seleccione **Add (Añadir)** e ingrese un **Rule Name (Nombre de regla)** para una nueva regla.

© 2020 Palo Alto Networks, Inc.

2. (Opcional) Especifique un nombre de amenaza específico (el valor predeterminado es **any [cualquiera]**).
3. Establezca la **Acción**. En este ejemplo, está establecida como **Block IP**.

   Si configura un perfil de protección frente a vulnerabilidades para bloquear IP, el cortafuegos primero utiliza hardware para bloquear las direcciones IP. Si el tráfico de ataques excede la capacidad de bloqueo del hardware, el cortafuegos utiliza mecanismos de bloqueo de software para bloquear las direcciones IP restantes.
4. Establezca la **Categoría** como **Fuerza bruta**.
5. (Opcional) Si bloquea, especifique el **Host Type (Tipo de host)** en el cual desea bloquear: **server (servidor)** or **client (cliente)** (el predeterminado es **any (cualquiera)**).
6. Consulte el paso 3 para personalizar la acción para una firma específica.
7. Consulte el paso 4 para personalizar el umbral de activación para una firma principal.



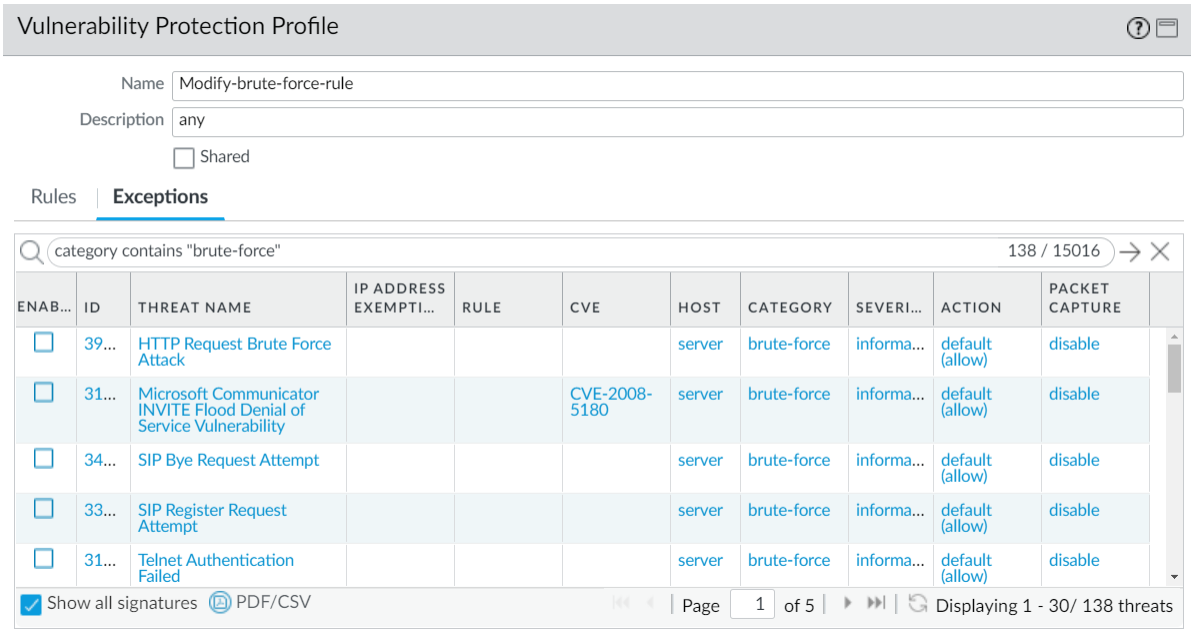
8. Haga clic en **OK (Aceptar)** para guardar la regla y el perfil.

STEP 3 | (Opcional) Personalice la acción para una firma específica.

1. En la pestaña **Exceptions (Excepciones)**, seleccione **Show all signatures (Mostrar todas las firmas)** para buscar la firma que desee modificar.

   Para ver todas las firmas de la categoría de fuerza bruta, busque por `category contains 'brute-force'`.
2. Para editar una firma específica, haga clic en la acción predeterminada predefinida en la columna Acción.

© 2020 Palo Alto Networks, Inc.



3. Defina la acción. **Allow (Permitir)**, **Alert (Alertar)**, **Block Ip (Bloquear IP)** o **Drop (Descartar)**. Si selecciona **Block Ip (Bloquear IP)**, realice estas tareas adicionales:
    1. Especifique el **Time (Tiempo)** (en segundos) después del cual activar la acción.
    2. Especifique **Track By (Rastrear por)** y bloquee la dirección IP usando **IP source (Origen de IP)** o **IP source and destination (Origen y destino de IP)**.
4. Haga clic en **OK (Aceptar)**.
5. Para cada firma modificada, seleccione la casilla de verificación de la columna **Enable (Habilitar)**.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Personalice las condiciones de activación para una firma principal.

Una firma principal que pueda editarse se marcará con este icono: .

En este ejemplo, los criterios de búsqueda fueron la categoría brute force y CVE-2008-1447.

1. Modifique ( ) el atributo de tiempo y los criterios de agregación para la firma.
2. Para modificar el umbral de activación, especifique el **Number of Hits (Número de resultados)** por cantidad de **seconds (segundos)**.
3. Especifique si agregar el número de resultados (**Aggregation Criteria [Criterios de agregación]**) por **source (origen)**, **destination (destino)** u **source-and-destination (origen y destino)**.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Añada este nuevo perfil a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
2. En la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** como el **Profile Type (Tipo de perfil)** para el Profile Setting (Ajuste de perfil).
3. Seleccione su perfil de **Vulnerability Protection (Protección frente a vulnerabilidades)**.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Confirme los cambios.

1. Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Habilitación de las firmas de evasión

Las firmas de evasión de Palo Alto Networks detectan solicitudes HTTP o TLS manipuladas y pueden alertar en instancias en las que un cliente se conecta a un dominio que no es el dominio especificado en la solicitud DNS. Las firmas de evasión son eficaces únicamente cuando el cortafuegos está habilitado para actuar como un proxy DNS y resolver las solicitudes de nombre de dominio. La práctica recomendada es realizar los siguientes pasos para habilitar las firmas de evasión.

STEP 1 | Habilite un cortafuegos que sea un intermediario entre los clientes y los servidores, y que actúe como proxy DNS.

Realice la Configuración de un objeto proxy DNS, que incluye los siguientes pasos:

- Especifique las interfaces en las cuales desea que el cortafuegos escuche las solicitudes DNS.
- Defina el servidor DNS con el que se comunicará el cortafuegos para resolver las solicitudes DNS.
- Configure las entradas estáticas de FQDN a dirección IP que el cortafuegos puede resolver localmente, sin tener que conectarse con un servidor DNS.
- Habilite el almacenamiento en caché de asignaciones resueltas de nombre de host a dirección IP.

STEP 2 | Obtenga la versión más reciente de contenido sobre aplicaciones y amenazas (versión 579 o posterior).

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Seleccione **Check Now** para descargar las últimas actualizaciones de contenido de aplicaciones y amenazas.
3. Descargue e instale la versión de contenido 579 de aplicaciones y amenazas (o posterior).

STEP 3 | Defina cómo el cortafuegos debe aplicar acciones al tráfico que coincide con las firmas de evasión.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** y **Add (Añadir)** para añadir o modificar un perfil antispyware.
2. Seleccione **Exceptions (Excepciones)** y seleccione **Show all signatures (Mostrar todas las firmas)**.
3. Filtre las firmas en función de la palabra clave `evasion`.
4. Para todas las firmas de evasión, configure **Action (Acciones)** en un ajuste que no sea el de permitir o la acción por defecto (la acción por defecto para las firmas de evasión es permitir). Por ejemplo, establezca que la **Action (Acción)** para las ID de firmas 14978 y 14984 sea **alert (alertar)** o **drop (descartar)**.
5. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware actualizado.
6. Adjunte el perfil de antispyware a una regla de política de seguridad: Seleccione **Policies (Políticas)** > **Security (Seguridad)**, seleccione la política deseada para modificarla y, a continuación, haga clic en la pestaña **Actions (Acciones)**. En Profile Settings (Configuración del perfil), haga clic en el menú desplegable junto a **Anti-Spyware**, seleccione el perfil antispyware que acaba de modificar para aplicar las firmas de evasión.

STEP 4 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Supervisión de direcciones IP bloqueadas

El cortafuegos mantiene una lista de bloqueo de las direcciones IP de origen que está bloqueando. Cuando el cortafuegos bloquea una dirección IP de origen, tal como cuando configura alguna de las siguientes reglas de política, bloquea el tráfico en el hardware antes de que esos paquetes utilicen recursos de búfer de paquetes o CPU:

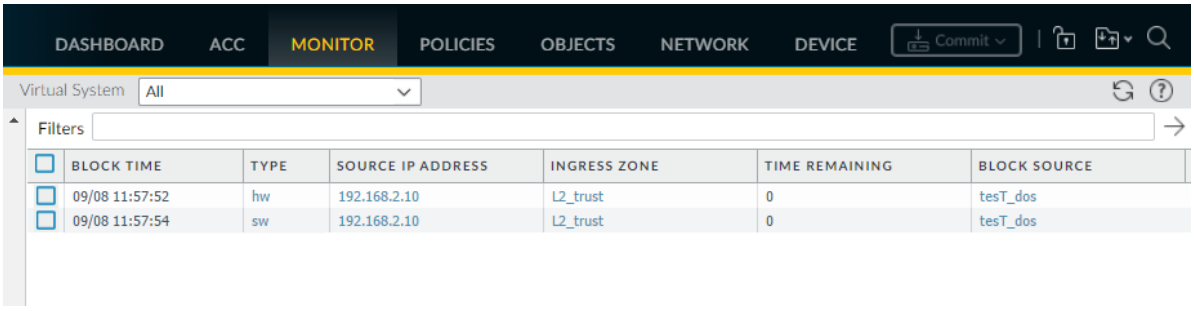
- Una regla de política de protección DoS clasificada con la acción de **Protect (Proteger)** (una política de protección DoS clasificada especifica que las conexiones entrantes coinciden con una dirección IP, dirección IP de destino o par de dirección IP de origen y destino, y está asociada con un perfil de protección DoS clasificado, según se describe en Protección DoS contra inundaciones de nuevas sesiones).
- Una regla de política de seguridad que utiliza un perfil de protección frente a vulnerabilidades.

El bloqueo de direcciones IP de hardware se admite en los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series.

Puede ver la lista de bloqueo, obtener información detallada sobre una dirección IP en la lista de bloqueo o ver cuentas de direcciones que el hardware y software están bloqueando. Puede eliminar una dirección IP de la lista si considera que no deben bloquearse. Puede cambiar el origen de la información detallada sobre direcciones en la lista. También puede cambiar por cuánto tiempo el hardware bloqueará las direcciones IP.

- Visualice las entradas en la lista de bloqueo.
  1. Seleccione **Monitor (Supervisar)** > **Block IP List (Lista de bloqueo de IP)**.

     Las entradas en la lista de bloqueo indican en la columna Type (Tipo) si fueron bloqueadas por hardware (hw) o software (sw).
  2. Observe lo siguiente en la parte inferior de la pantalla:
     - Recuento de **Total Blocked IPs (IP totales bloqueadas)** en relación con el número de direcciones IP bloqueadas que admite el cortafuegos.
     - El porcentaje de la lista de bloqueo que ha usado el cortafuegos.
  3. Para filtrar las entradas mostradas, seleccione un valor en una columna (que crea un filtro en el campo **Filters [Filtros]**) y aplique el filtro (→). De lo contrario, el cortafuegos muestra las primeras 1000 entradas.
  4. Ingrese un número de **Page (Página)** o haga clic en las flechas en la parte inferior de la pantalla para avanzar en las páginas de entradas.
  5. Para ver detalles sobre una dirección en la lista de bloqueo, pase el ratón sobre una dirección IP de origen y haga clic en la flecha hacia abajo. Haga clic en el enlace **Who Is**, que muestra información de Network Solutions Who Is acerca de la dirección.



- Elimine entradas de la lista de bloqueo.

© 2020 Palo Alto Networks, Inc.

Elimine una entrada si determina que no se debe bloquear la dirección IP. Luego, revise la regla de la política que ha provocado que el cortafuegos bloquee la dirección.

1. Seleccione **Monitor (Supervisar)** > **Block IP List (Lista de bloqueo de IP)**.
2. Seleccione una o más entradas y haga clic en **Delete (Eliminar)**.
3. (Opcional) Seleccione **Clear All (Borrar todo)** para eliminar todas las entradas de la lista.

- Deshabilite o vuelva a habilitar el bloqueo de direcciones IP de hardware para fines de solución de problemas.

  Si bien el bloqueo de direcciones IP de hardware está deshabilitado, el cortafuegos continúa realizando el bloqueo de direcciones IP de software que usted ha configurado.

```
> set system setting hardware-acl-blocking [enable | disable]
```

  Para conservar los recursos de la CPU y del búfer de paquetes, deje habilitado el bloqueo de direcciones IP de hardware, a menos que el servicio técnico de Palo Alto Networks le pida que lo deshabilite, por ejemplo, si se va a depurar un flujo de tráfico.

- Ajuste la cantidad de segundos que las direcciones IP bloqueadas por el hardware permanecerán en la lista de bloqueo (el intervalo es de 1 a 3600; el valor predeterminado es 1).

```
> set system setting hardware-acl-blocking duration <seconds>
```

  Mantenga una duración más breve para las entradas de lista de bloqueo de hardware que para las entradas de lista de bloqueo de software, a fin de reducir la probabilidad de superar la capacidad de bloqueo del hardware.

- Cambie el sitio web predeterminado para encontrar más información sobre una dirección IP de Network Solutions Who Is a otro sitio web.

```
# set deviceconfig system ip-address-lookup-url <url>
```

- Visualice los recuentos de direcciones IP bloqueadas por hardware y software; por ejemplo, para ver la tasa de ataques.

  Visualice la suma total de entradas de direcciones IP en la tabla de bloqueo de hardware y la lista de bloqueo (bloqueadas por hardware y software):

```
> show counter global name flow_dos_blk_num_entries
```

  Visualice el recuento de entradas de direcciones IP en la tabla de bloqueo de hardware que fueron bloqueadas por hardware:

```
> show counter global name flow_dos_blk_hw_entries
```

  Visualice el recuento de entradas de direcciones IP en la lista de bloqueo que fueron bloqueadas por software:

© 2020 Palo Alto Networks, Inc.

```
> show counter global name flow_dos_blk_sw_entries
```

- Visualice la información de la lista de bloqueo por ranura en un cortafuegos de la serie PA-7000.

```
> show dos-block-table software filter slot <slot-number>
```


© 2020 Palo Alto Networks, Inc.

Categorías de firma de amenazas

Existen tres tipos de firmas de amenazas de Palo Alto Networks; cada una para detectar diferentes amenazas a medida que el cortafuegos analiza el tráfico de red:

- Firmas de antivirus: detectan antivirus y malware encontrados en tipos de archivos y ejecutables.
- Firmas antispyware: detectan actividad de comando y control (command-and-control, C2), en la que el spyware en un cliente infectado recopila datos o se comunica con un atacante remoto sin el consentimiento del usuario.
- Firmas de vulnerabilidades: detecta fallos en el sistema que un atacante podría intentar aprovechar.

La gravedad de una firma indica el riesgo del evento detectado, y la acción predeterminada de una firma (por ejemplo, bloquear o alertar) es la forma en que Palo Alto Networks recomienda que aplique el tráfico coincidente.

Debe configurar la protección de antivirus, de antispyware y de vulnerabilidades para indicarle al cortafuegos qué acción debe realizar cuando detecta una amenaza, y puede usar fácilmente los perfiles de seguridad predeterminados para comenzar a bloquear amenazas sobre la base de las recomendaciones de Palo Alto Networks. Para cada tipo de firma, categoría e incluso firmas específicas, puede continuar modificando o creando perfiles nuevos para detectar de manera más detallada amenazas potenciales.

La siguiente tabla detalla todas las posibles categorías de firma por tipo (antivirus, spyware y vulnerabilidades) e incluye la actualización de contenido (aplicaciones y amenazas, antivirus o WildFire) que proporcionan las firmas en cada categoría. También puede visitar la base de datos de amenazas de Palo Alto Networks para Más información sobre las firmas de amenazas.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
Firmas de antivirus		
apk	Antivirus WildFire o WildFire privado	Archivos maliciosos de las Aplicaciones de Android (Android Application, APK).
dmg	Antivirus WildFire o WildFire privado	Archivos maliciosos de imagen de disco (disk image, DMG) de Apple que se usan con Mac OS X.
flash	Antivirus WildFire o WildFire privado	Los applets de Adobe Flash y el contenido de Flash insertado en páginas web.
java-class	Antivirus	Applets de Java (tipos de archivo JAR/Class).
macho	Antivirus WildFire o WildFire privado	Los archivos de objeto Mach (Mach-O) son ejecutables, bibliotecas y códigos de objetos que son nativos de Mac OS X.

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
office	Antivirus WildFire o WildFire privado	Archivos de Microsoft Office, como documentos (DOC, DOCX, RTF), libros (XLS, XLSX) y presentaciones de PowerPoint (PPT, PPTX).
openoffice	Antivirus WildFire o WildFire privado	Documentos de Office Open XML (OOXML) 2007+.
pdf	Antivirus WildFire o WildFire privado	Archivos con formato de documento portable (Portable document format, PDF).
pe	Antivirus WildFire o WildFire privado	Los archivos Ejecutables portátiles (Portable executable, PE) pueden ejecutarse automáticamente en un sistema de Microsoft Windows y solo deben permitirse cuando están autorizados. Estos tipos de archivos incluyen: • Código objeto. • Fuentes (FON). • Archivos de sistema (SYN). • Archivos de controladores (DRV). • Elementos del panel de control de Windows (CPL). • Bibliotecas de enlaces dinámicos (dynamic-link libraries, DLL). • OCX (bibliotecas para controles personalizados OLE o controles ActiveX). • SCR (secuencias de comandos que pueden usarse para ejecutar otros archivos). • Archivos de la Interfaz de firmware extensible (Extensible Firmware Interface, EFI), que se ejecutan entre un SO y el firmware para facilitar actualizaciones de dispositivos y operaciones de inicio. • Archivos de información de programa (Program information files, PIF).
pkg	Antivirus WildFire o WildFire privado	Paquetes de instalación de software (PKG) de Apple, que se usan con Mac OS X.
Firmas de spyware		
Adware	Aplicaciones y amenazas	Detecta programas que muestran anuncios potencialmente no deseados. Algunos adware modifican los exploradores para destacar e incluir un hipervínculo a las palabras claves buscadas con más frecuencia en páginas web; estos enlaces redirigen a los usuarios a los sitios web de anuncios. El

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		adware también puede recuperar actualizaciones de un servidor de comando y control (command-and-control, C2) e instalar estas actualizaciones en un explorador o en el sistema de un cliente. Las protecciones nuevas en esta categoría son escasas.
autogen	Antivirus	Estas firmas basadas en la carga útil detectan el tráfico de comando y control (command-and-control, C2) y se generan automáticamente. En gran medida, las firmas autogeneradas pueden detectar el tráfico de C2 incluso cuando el host de C2 es desconocido o cambia con rapidez.
backdoor	Aplicaciones y amenazas	Detecta un programa que permite a un atacante obtener acceso remoto no autorizado a un sistema.
Botnet	Aplicaciones y amenazas	Indica la actividad de botnet. Un botnet es una red de ordenadores infectados con malware ("bots") que un atacante controla. El atacante puede controlar de manera central cada ordenador de un botnet para llevar a cabo una acción coordinada simultáneamente (por ejemplo, iniciar un ataque DoS).
browser-hijack	Aplicaciones y amenazas	Detecta un complemento o software que modifica la configuración del explorador. Un secuestrador de explorador podría controlar la búsqueda automática o realizar un seguimiento de la actividad de los usuarios y enviar esta información a un servidor de C2. Las protecciones nuevas en esta categoría son escasas.
cryptominer (criptominado)	Aplicaciones y amenazas	(A veces conocido como cryptojacking o minería) Detecta el intento de descarga o el tráfico de red generado por programas maliciosos diseñados para utilizar recursos informáticos para extraer criptomonedas sin el conocimiento del usuario. Los binarios de criptominado se entregan con frecuencia mediante un descargador de scripts de shell que intenta determinar la arquitectura del sistema y eliminar otros procesos de minería en el sistema. Algunas minerías se ejecutan dentro de otros procesos, como un navegador web que representa una página web maliciosa.
data-theft	Aplicaciones y amenazas	Detecta a un sistema que envía información a un servidor de C2 conocido. Las protecciones nuevas en esta categoría son escasas.
dns	Antivirus	Detecta solicitudes de DNS para conectarse a dominios maliciosos. Las firmas de WildFire DNS y DNS detectan los mismos dominios maliciosos; sin embargo, las firmas DNS están

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		incluidas en la actualización de contenido de antivirus diaria y las firmas WildFire DNS están incluidas en las actualizaciones de WildFire que emite protecciones cada 5 minutos.
dns-security	Antivirus	Detecta solicitudes de DNS para conectarse a dominios maliciosos. dns-security incluye firmas de dns y de dns-wildfire, además de las firmas únicas que genera el servicio DNS Security.
dns-wildfire	WildFire o WildFire privado	Detecta solicitudes de DNS para conectarse a dominios maliciosos. Las firmas de WildFire DNS y DNS detectan los mismos dominios maliciosos; sin embargo, las firmas DNS están incluidas en la actualización de contenido de antivirus diaria y las firmas WildFire DNS están incluidas en las actualizaciones de WildFire que emite protecciones cada 5 minutos.
downloader (descargador)	Aplicaciones y amenazas	(También conocido como droppers [instaladores troyanos], stagers [escalonamientos] o loaders [cargadores]) Detecta programas que usan una conexión a Internet para conectarse a un servidor remoto para descargar y ejecutar malware en el sistema comprometido El caso de uso más común es que un descargador se implemente como la culminación de la *etapa uno* de un ciberataque, donde la ejecución de la carga útil obtenida del descargador se considera *etapa dos*. Los scripts de shell (Bash, PowerShell, etc.), los troyanos y los documentos de señuelos maliciosos (también conocidos como maldocs), como archivos PDF y Word, son tipos de descargadores comunes.
fraud (fraude)	Aplicaciones y amenazas	(Incluidos el robo de formularios, el phishing y las estafas) Detecta el acceso a sitios web comprometidos para los que se ha determinado que incorporan código JavaScript malicioso para recopilar información confidencial del usuario (por ejemplo, nombre, dirección, correo electrónico, número de tarjeta de crédito, CVV y fecha de vencimiento) de los formularios de pago que se capturan en las páginas de pago de los sitios web de comercio electrónico.
hacktool (herramienta de hackeo)	Aplicaciones y amenazas	Detecta el tráfico generado por las herramientas de software que utilizan los actores malintencionados para realizar reconocimientos, atacar u obtener acceso a sistemas vulnerables, exfiltrar datos o crear un canal de comando y control para controlar de forma secreta un sistema informático sin autorización. Estos programas están fuertemente asociados con malware y ciberataques. Las herramientas de hacking pueden implementarse de manera benigna cuando se utilizan en operaciones de Red y Blue Team, pruebas de penetración e I+D. El uso o posesión

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		de estas herramientas puede ser ilegal en algunos países, independientemente de su intención.
Registrador de pulsaciones de teclas	Aplicaciones y amenazas	Detecta programas que permiten a los atacantes rastrear la actividad del usuario de manera secreta mediante el registro de pulsaciones de teclas y capturas de pantalla. Los registradores de pulsaciones de teclas usan varios métodos de C2 para enviar periódicamente logs e informes a una dirección de correo electrónico predefinida o a un servidor de C2. Mediante la vigilancia de las pulsaciones de teclas, un atacante podría recuperar las credenciales que le brindarían el acceso a la red.
networm	Aplicaciones y amenazas	Detecta un programa que se replica automáticamente y se transmite de sistema en sistema. Los networm podrían usar recursos compartidos o aprovechar fallas de seguridad para acceder a los sistemas objetivo.
Kit de phishing (suplantación de identidad)	Aplicaciones y amenazas	Detecta cuando un usuario intenta conectar a una página de destino del kit de phishing (generalmente después de recibir un correo electrónico con un enlace al sitio malicioso). Un sitio web de phishing engaña a los usuarios para enviar credenciales que un atacante puede robar para obtener acceso a la red.  *Además de bloquear el acceso a las páginas de destino del kit de phishing, habilite la autenticación multifactor y la prevención de phishing de credenciales para evitar los ataques de phishing en todas las etapas.*
post-exploitation	Aplicaciones y amenazas	Detecta la actividad que indica la etapa de post-exploitation de un ataque, en el que un atacante intenta evaluar el valor de un sistema en riesgo. Esto podría incluir evaluar la confidencialidad de los datos almacenados en el sistema, y la utilidad del sistema en comprometer más la red.
webshell	Aplicaciones y amenazas	Detecta web shells y tráfico web shell, incluida la detección de implantes y la interacción de comando y control. Los web shells primero deben implantarlos un actor malintencionado en el host comprometido, la mayoría de las veces apuntando a un servidor web o marco. La comunicación posterior con el archivo de web shell con frecuencia permite que un actor malintencionado establezca un punto de apoyo en el sistema y realice la enumeración de servicios y redes, la exfiltración de datos y la ejecución remota de código en el contexto del usuario del servidor web. Los tipos de web shell más comunes son los scripts de marcado PHP, .NET y Perl. Los atacantes

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		también pueden utilizar servidores web infectados con web shells (los servidores web pueden ser sistemas internos o conectados a Internet) para atacar otros sistemas internos.
spyware	Aplicaciones y amenazas	Detecta una comunicación C2 de salida. Estas firmas están autogeneradas o creadas manualmente por los investigadores de Palo Alto Networks.  *Las firmas de spyware y autogen detectan la comunicación de C2 saliente; sin embargo, las firmas de autogen están basadas en la carga útil y pueden detectar exclusivamente comunicaciones de C2 con hosts de C2 que sean desconocidas o cambien con rapidez.*
Firmas de vulnerabilidad		
brute force	Aplicaciones y amenazas	Una firma brute-force detecta varias incidencias de una condición en un período de tiempo determinado. Mientras la actividad aislada podría ser benigna, la firma brute-force indica que la frecuencia y velocidad en la cual ocurre la actividad es sospechosa. Por ejemplo, un solo fallo de inicio de sesión en el FTP no indica una actividad maliciosa. Sin embargo, varios inicios de sesión en el FTP con errores en un breve período de tiempo probablemente indiquen que un atacante está probando combinaciones de contraseñas para acceder al servidor FTP. Puede ajustar la acción y las condiciones del activador para las firmas brute force.
code execution	Aplicaciones y amenazas	Detecta una vulnerabilidad de ejecución de código que un atacante puede aprovechar para ejecutar código en un sistema con los privilegios de un usuario con la sesión iniciada.
code-obfuscation	Aplicaciones y amenazas	Detecta código que se transformó para ocultar determinados datos y, al mismo tiempo, conserva su función. El código oculto es difícil o imposible de leer, por lo que no es evidente qué comandos ejecuta el código o con qué programa está diseñado para interactuar. Lo más común es que los actores maliciosos oculten código para disimular malware. Con menor frecuencia, algunos programadores legítimos podrían ocultar código para proteger la privacidad y la propiedad intelectual o para mejorar la experiencia del usuario. Por ejemplo, determinados tipos de ocultación (como la minificación) reducen el tamaño del archivo, lo que disminuye los tiempos de carga del sitio web y el uso del ancho de banda.

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
dos	Aplicaciones y amenazas	Detecta un ataque de denegación de servicio (denial-of-service, DoS), en el que un atacante intenta que un sistema objetivo no esté disponible, interrumpiendo temporalmente el sistema y los servicios y aplicaciones dependientes. Para llevar a cabo un ataque DoS, un atacante podría producir una inundación de tráfico en un sistema objetivo o enviar información que provoque fallos. Los ataques DoS despojan a los usuarios legítimos (como empleados, miembros y titulares de cuenta) del servicio o recursos al cual esperan acceder.
exploit-kit	Aplicaciones y amenazas	Detecta una página de destino del kit de exploits. Las páginas de destino del kit de exploits con frecuencia contienen varios exploits que apuntan a una o varias vulnerabilidades y exposiciones comunes (common vulnerabilities and exposures, CVE), para varios exploradores y complementos. Debido a que las CVE objetivo cambian con rapidez, las firmas exploit-kit se activan sobre la base de la página de destino del kit de exploits y no de las CVE. Cuando un usuario visita un sitio web con un kit de exploits, este analiza las CVE objetivo e intenta proporcionar de forma silenciosa una carga útil maliciosa al ordenador de la víctima.
info-leak	Aplicaciones y amenazas	Detecta una vulnerabilidad de software que un atacante podría aprovechar para robar información confidencial o de propiedad. Con frecuencia, podría existir un info-leak porque las comprobaciones integrales no existen para proteger los datos, y los atacantes pueden aprovechar las info-leaks enviando solicitudes manipuladas.
insecure-credentials (credenciales no seguras)	Aplicaciones y amenazas	Detecta el uso de contraseñas débiles, comprometidas y predeterminadas del fabricante para software, dispositivos de red y dispositivos de IoT.
Desbordamiento	Aplicaciones y amenazas	Detecta una vulnerabilidad de desbordamiento, en la que el atacante podría aprovechar la falta de comprobaciones apropiadas. Un ataque exitoso podría conllevar una ejecución remota de código con los privilegios de aplicación, servidor o sistema operativo.
phishing	Aplicaciones y amenazas	Detecta cuando un usuario intenta conectar a una página de destino del kit de phishing (generalmente después de recibir un correo electrónico con un enlace al sitio malicioso). Un sitio web de phishing engaña a los usuarios para enviar credenciales que un atacante puede robar para obtener acceso a la red.

© 2020 Palo Alto Networks, Inc.

Categoría de amenaza	Actualización de contenido que proporciona estas firmas	Description (Descripción)
		 *Además de bloquear el acceso a las páginas de destino del kit de phishing, habilite la autenticación multifactor y la prevención de phishing de credenciales para evitar los ataques de phishing en todas las etapas.*
protocol-anomaly	Aplicaciones y amenazas	Detecta anomalías de protocolo, en las que el comportamiento de un protocolo se desvía del uso estándar y de cumplimiento. Por ejemplo, un paquete con formato incorrecto, una aplicación escrita de manera deficiente o una aplicación que se ejecuta en un puerto no estándar se considerarían anomalías y podrían usarse como herramientas de evasión. La acción recomendada es bloquear las anomalías de protocolo de cualquier gravedad.
sql-injection	Aplicaciones y amenazas	Detecta una técnica de hacking común en la que un atacante inserta consultas SQL en las solicitudes de una aplicación para leer o modificar una base de datos. Este tipo de técnica se usa con frecuencia en sitios web que no realizan limpiezas integrales de las entradas de usuario.

© 2020 Palo Alto Networks, Inc.

Creación de excepciones de amenazas

Palo Alto Networks define una acción predeterminada recomendada (como un bloqueo o una alerta) para las firmas de amenazas. Puede utilizar una ID de amenaza para excluir una firma de amenaza de la aplicación o modificar la acción que aplica el cortafuegos para esa firma de amenaza. Por ejemplo, puede modificar la acción para las firmas de amenazas que causan falsos positivos en su red.

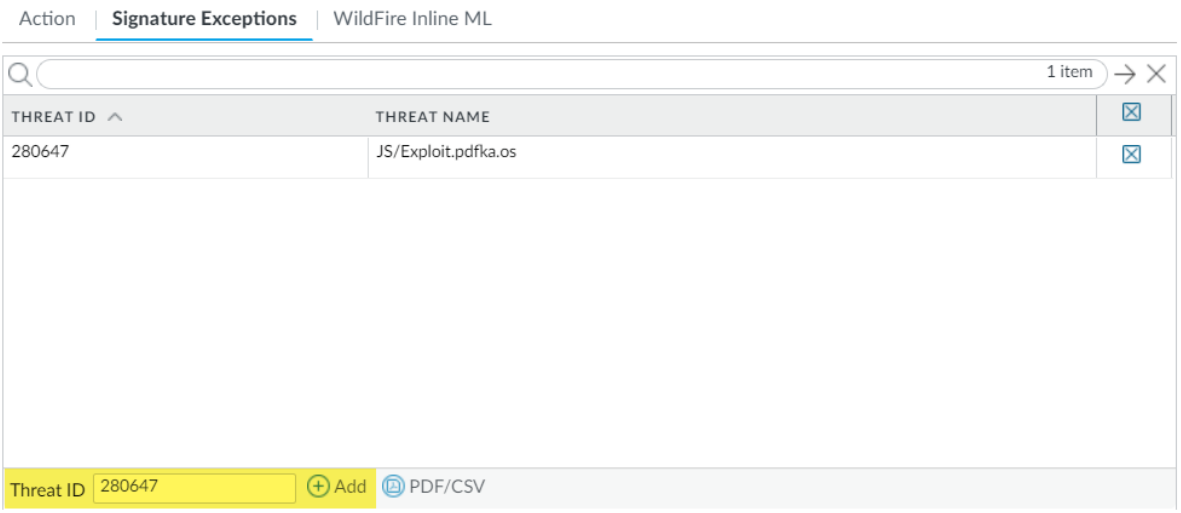
Configure las excepciones de las amenazas para antivirus, vulnerabilidad, spyware y firmas de DNS para cambiar la aplicación del cortafuegos para una amenaza. Sin embargo, antes de comenzar, asegúrese de que el cortafuegos detecte y aplique acciones ante amenazas en función de la configuración predeterminada de las firmas:

- Obtenga las actualizaciones más recientes de amenazas de antivirus, amenazas y aplicaciones, y firmas de WildFire.
- Establezca antivirus, antispyware y protección frente a vulnerabilidades y aplique estos perfiles de seguridad a su política de seguridad.

STEP 1 | Excluya las firmas del antivirus de la aplicación de acciones.

A pesar de que puede utilizar un perfil de antivirus para excluir firmas de antivirus, no puede cambiar la acción que aplica el cortafuegos a una firma de antivirus determinada. Sin embargo, puede definir la acción que el cortafuegos aplicará a los virus que encuentre en diferentes tipos de tráfico editando los decodificadores (Objects [Objetos] > Security Profiles [Perfiles de seguridad] > Antivirus > <antivirus-profile> > Antivirus).

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Antivirus**.
2. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antivirus o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **Signature Exception (Excepción de firma)**.
3. Haga clic en **Add (Añadir)** para añadir la **Threat ID (ID de amenazas)** de la firma de amenazas que desea excluir de la aplicación de acciones del cortafuegos.

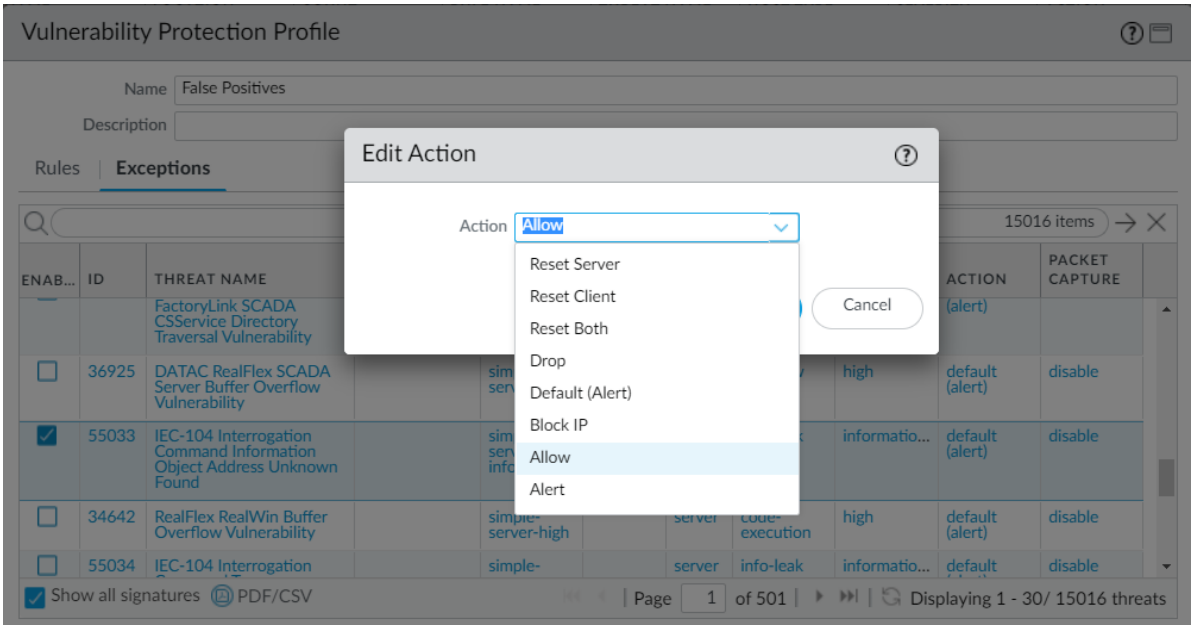


4. Haga clic en **OK (Aceptar)** para guardar el perfil de antivirus.

STEP 2 | Modifique la aplicación de acciones para las vulnerabilidades y las firmas de spyware (excepto las firmas de DNS; pase a la próxima opción para modificar la aplicación de acciones para las firmas de DNS, que son un tipo de firma de spyware).

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)** u **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)**.
2. **Añada** o modifique un perfil existente de protección frente a vulnerabilidades o antispyware del que desee excluir la firma de amenazas y, a continuación, seleccione **Signature Exceptions (Excepciones de firma)** para los perfiles de protección antispyware o **excepciones** para los perfiles de protección frente a vulnerabilidades.
3. Haga clic en **Show all signatures (Mostrar todas las firmas)** y realice el filtro para seleccionar la firma en la que desea modificar las reglas de aplicación.
4. Marque la casilla de la columna **Enable (Habilitar)** que corresponde a la firma cuya aplicación desea modificar.
5. Seleccione la **Action (Acción)** que desea que aplique el cortafuegos en esta firma de amenaza.

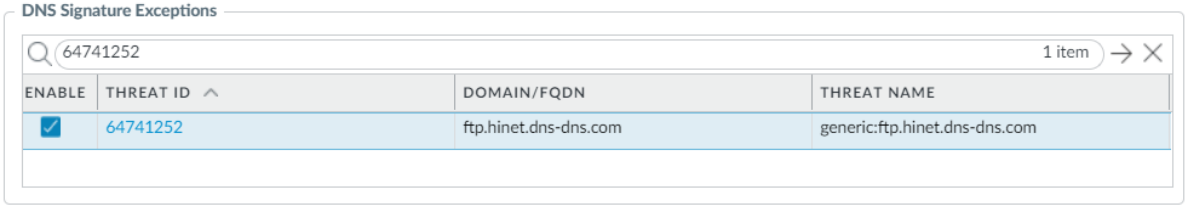


   En el caso de las firmas que desea excluir de la aplicación de acciones debido a que provocan falsos positivos, configure **Allow (Permitir)** como **Action (Acción)**.
6. Haga clic en **OK (Aceptar)** para guardar su perfil nuevo o modificado antispyware o de protección frente a vulnerabilidades.

STEP 3 | Modifique la aplicación para las firmas de DNS.

De manera predeterminada, el DNS busca los nombres de host maliciosos que las firmas de DNS detectan y envían a un sinkhole.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
3. Busque el ID de amenaza de DNS para la firma de DNS que desee excluir de la aplicación y seleccione la casilla de la firma correspondiente:



© 2020 Palo Alto Networks, Inc.

4. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

© 2020 Palo Alto Networks, Inc.

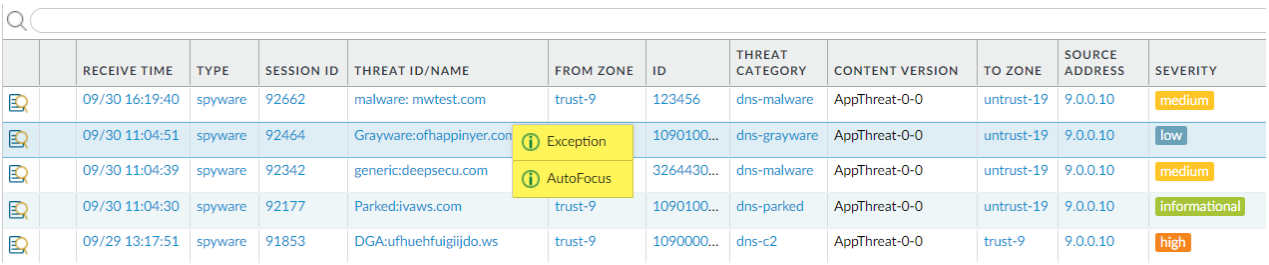
Firmas personalizadas

Puede crear firmas de amenazas personalizadas para detectar y bloquear tráfico específico. Cuando un servidor de gestión Panorama es el encargado de administrar el cortafuegos, el ThreatID se asigna a la amenaza personalizada correspondiente en el cortafuegos para permitir que este genere un log de amenazas con el ThreatID personalizado configurado. Visite nuestra guía para obtener más información sobre las firmas de amenazas y aplicaciones personalizadas.

© 2020 Palo Alto Networks, Inc.

Supervisión y obtención de informes sobre amenazas

Las funciones Threat Vault (Baúl de amenazas) y AutoFocus se incluyen en el cortafuegos con el fin de hacer visible la naturaleza de las amenazas que detecta el cortafuegos y para proporcionar una perspectiva más completa de cómo un artefacto se adapta al tráfico de red de su organización (un artefacto es una propiedad, una actividad o un comportamiento asociado a un archivo, un enlace de correo electrónico o una sesión). Puede obtener información contextual inmediata sobre una amenaza o cambiar la investigación sobre amenazas del cortafuegos a la base de datos de amenazas y AutoFocus sin inconvenientes.



Además, puede utilizar las Categorías de firma de amenazas, que clasifican los tipos de eventos de amenazas, para reducir la visualización de ciertos tipos de actividad de amenazas o para crear informes personalizados.

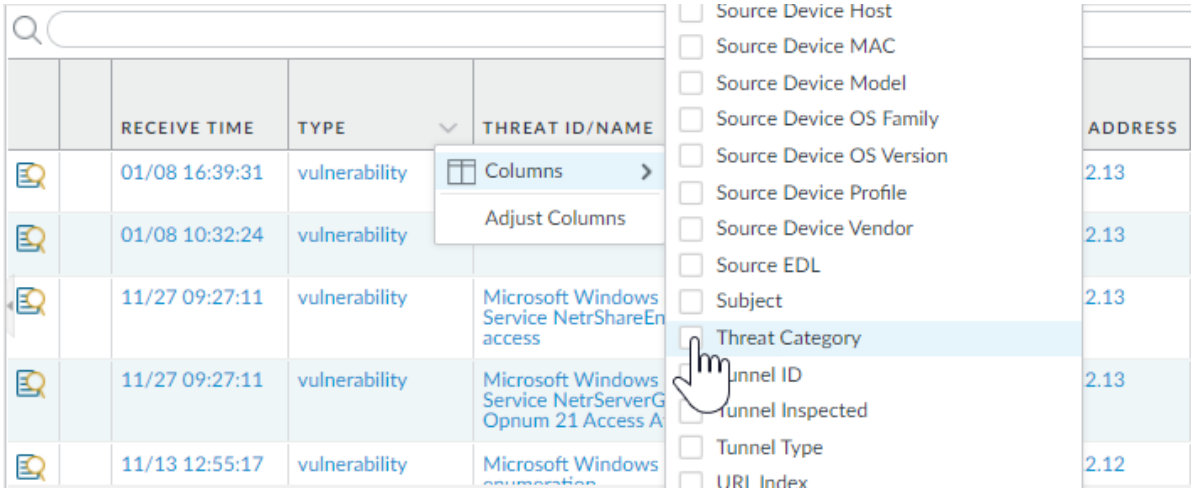
- Supervisión de actividad y creación de informes personalizados en función de las categorías de amenazas
- Más información sobre las firmas de amenazas
- Inteligencia contra amenazas de AutoFocus para el tráfico de red

Supervisión de actividad y creación de informes personalizados en función de las categorías de amenazas

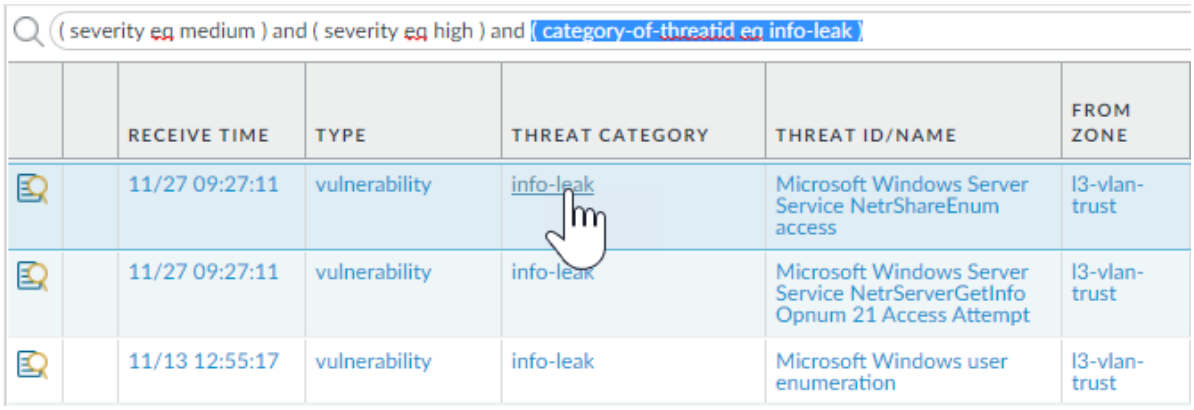
Las categorías de amenazas clasifican los diferentes tipos de firmas de amenazas para ayudarle a comprender y establecer conexiones entre los eventos que detectan las firmas de amenazas. Las categorías de amenazas son subconjuntos de tipos de firmas de amenazas más amplios: spyware, vulnerabilidad, antivirus y firmas DNS. Las entradas de log de amenazas muestran la **categoría de amenaza** de cada evento registrado.

- Filtre los logs de amenaza por categoría de amenaza.
  1. Select **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**.
  2. Añada la columna Threat Category (Categoría de amenaza) para ver la categoría de amenaza de cada entrada de log:

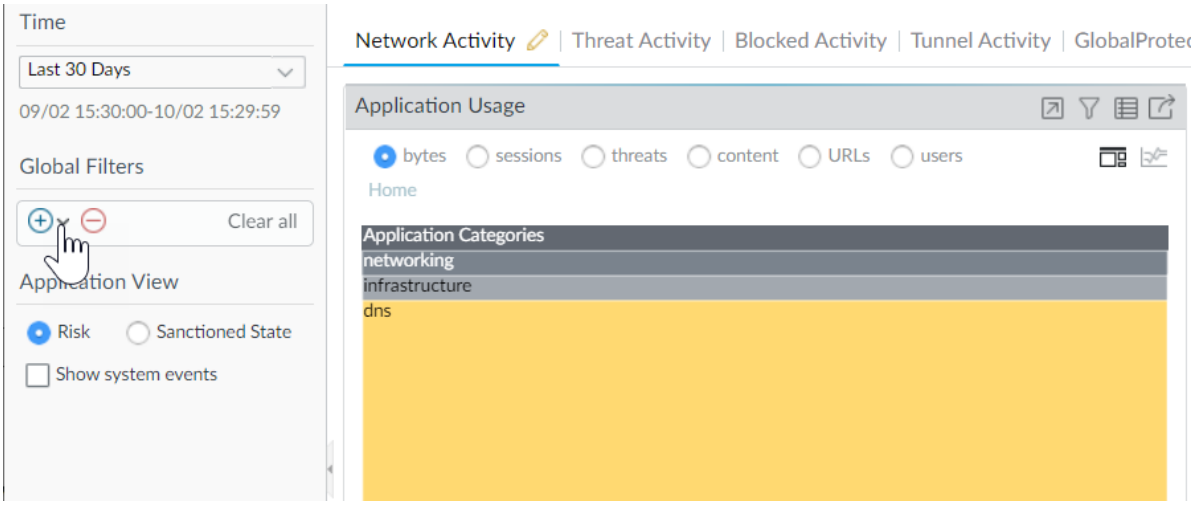
© 2020 Palo Alto Networks, Inc.



3. Para implementar un filtro en función de la categoría de amenaza:
   - Utilice el generador de consultas de log para añadir un filtro con la categoría de amenaza **Attribute (Atributo)** y en el campo **Value (Valor)**, introduzca una categoría de amenaza.
   - Seleccione la categoría de amenaza de cualquier entrada del log para añadir esa categoría al filtro:

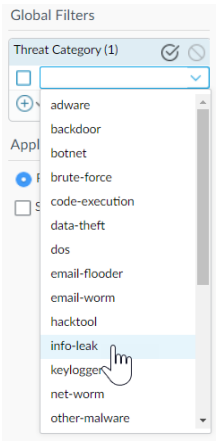


- Filtre la actividad del ACC por categoría de amenaza.
  1. Seleccione **ACC** y añada una categoría de amenaza como filtro global:



  2. Seleccione la categoría de amenaza que se utilizará para filtrar todas las pestañas de ACC.

© 2020 Palo Alto Networks, Inc.



- Cree informes personalizados basados en las categorías de amenazas para recibir información sobre tipos específicos de amenazas que detectó el cortafuegos.
  1. Seleccione **Monitor (Supervisar)** > **Manage Custom reports (Gestionar informes personalizados)** para añadir un nuevo informe personalizado o modificar uno existente.
  2. Seleccione la **Database (Base de datos)** que se utilizará como el origen del informe personalizado. En este caso, seleccione **Threat (Amenaza)** de cualquiera de los dos tipos de orígenes de la base de datos, base de datos de resumen y logs detallados. Los datos de la base de datos de resumen se resumen para permitir una respuesta más rápida cuando se generan informes. La generación de logs detallados requiere más tiempo, pero estos proporcionan un conjunto de datos detallados y completos de cada entrada del log.
  3. En el generador de consultas de log, añada un filtro de informes con el atributo **Threat Category (Categoría de amenaza)** y en el campo Value (Valor), seleccione una categoría de amenaza en la que se basará su informe.
  4. Para comprobar la configuración del nuevo informe, seleccione **Run now (Ejecutar ahora)**.
  5. Haga clic en **OK (Aceptar)** para guardar el informe.

Más información sobre las firmas de amenazas

Los logs de amenazas del cortafuegos registran todas las amenazas que el cortafuegos detecta en función de las firmas de amenazas (Configuración de antivirus, antispyware y protección frente a vulnerabilidades) y el ACC muestra una descripción general de las principales amenazas en su red. Cada evento que registra el cortafuegos incluye una ID que identifica la firma de amenaza asociada.

Puede utilizar el ID de amenazas encontrada con un log de amenaza o entrada de ACC para realizar las siguientes tareas:

- Compruebe con facilidad si una firma de amenazas se configuró como una excepción de su política de seguridad (Creación de excepciones de amenazas).
- Busque la información de Threat Vault más reciente sobre una amenaza específica. Debido a que Threat Vault está integrada con el cortafuegos, puede ver detalles de las amenazas directamente en el contexto del cortafuegos o iniciar una búsqueda de Threat Vault en una nueva ventana del explorador para detectar una amenaza registrada por el cortafuegos.

Si se deshabilita una firma, la firma UTID podría reutilizarse para una nueva firma.

Revise las notas de versión de la actualización de contenido para obtener notificaciones relacionadas con las firmas nuevas y deshabilitadas. Las firmas podrían deshabilitarse en los siguientes casos: la actividad que detecta la firma proviene de atacantes, la firma generó

© 2020 Palo Alto Networks, Inc.

importantes falsos positivos o la firma se consolidó con otras firmas similares en una sola firma (optimización de la firma).

STEP 1 | Confirme que el cortafuegos está conectado a Threat Vault.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración **Logging and Reporting (Creación de logs e informes)** como **Enable Threat Vault Access (Habilitar el acceso a la cámara de amenazas)**. El acceso a Threat Vault se habilita de manera predeterminada.

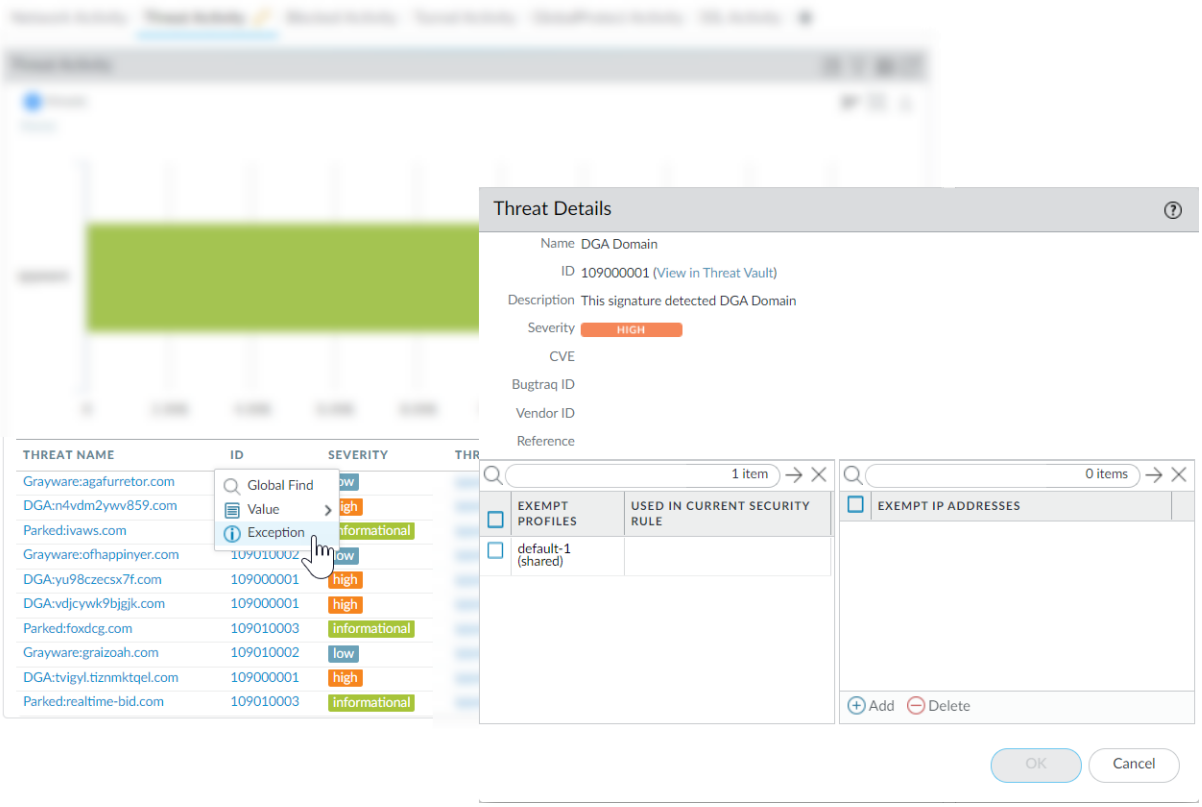
STEP 2 | Busque el ID de amenazas de las amenazas que detecta el cortafuegos.

- Para ver cada evento de amenaza que detecta el cortafuegos basado en las firmas de amenazas, seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)**. Puede encontrar el ID de una entrada de amenaza de la columna ID o seleccionar la entrada de log para ver los detalles del log, que incluye el ID de amenaza.
- Para acceder a una descripción general de las amenazas principales de la red, seleccione **ACC** > **Threat Activity (Actividad de amenazas)** y observe el widget de Threat Activity (Actividad de amenazas). La columna ID muestra el ID de amenazas de cada amenaza que se muestra.
- Para ver los detalles de las amenazas que puede configurar como excepciones de amenazas (es decir, el cortafuegos aplica la amenaza de manera diferente a la acción predeterminada definida para la firma de amenazas) seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware/Vulnerability Protection (Antispyware/protección contra vulnerabilidades)**. Haga clic en **Add (Añadir)** para añadir un perfil o modifique uno existente, y haga clic en la pestaña **Exceptions (Excepciones)** para ver las excepciones configuradas. Si no se configuran excepciones, puede filtrar por firmas de amenazas o seleccione **Show all signatures (Mostrar todas las firmas)**.

STEP 3 | Coloque el cursor sobre un **Threat Name (Nombre de amenaza)** o el **ID** de amenazas para abrir el menú desplegable, y haga clic en **Exception (Excepción)** para revisar los detalles de la amenaza y cómo se configura el cortafuegos para aplicar la amenaza.

Por ejemplo, obtenga más información sobre una amenaza principal ilustrada en el ACC:

© 2020 Palo Alto Networks, Inc.



STEP 4 | Revise los **Threat Details (Detalles de amenaza)** más recientes de la amenaza e inicie una búsqueda de Threat Vault en función del ID de amenazas.

- Los detalles de amenazas que se muestran incluyen la información de Threat Vault más reciente para la amenaza, los recursos que puede utilizar para obtener más información sobre la amenaza y los CVE asociados a la amenaza.
- Seleccione **View in Threat Vault (Ver en Threat Vault)** para abrir una búsqueda Threat Vault en una nueva ventana del explorador y buscar la información más reciente que tiene la base de datos de amenazas de Palo Alto Networks para esta firma de amenazas.

STEP 5 | Compruebe si una firma de amenazas se configuró como una excepción de su política de seguridad.

- Si la columna **Used in current security rule (Utilizada en la regla de seguridad actual)** está vacía, el cortafuegos aplica la amenaza en función de la acción de la firma predeterminada recomendada (por ejemplo, bloquear o crear alerta).
- Una marca de verificación en la columna **Used in current security rule (Utilizada en la regla de seguridad actual)** indica que una regla de la política de seguridad se configuró para aplicar una acción no predeterminada a la amenaza (por ejemplo, permitir), en función de la configuración de **Exempt Profiles (Perfiles de exclusión)** asociada.

La columna Used in security rule (Utilizada en la regla de seguridad actual) no indica si la regla de la política de seguridad está habilitada; solo indica si la regla de la política de seguridad se configuró con una exención de amenaza. Seleccione Policies (Políticas) > Security (Seguridad) para comprobar si una regla indicada de la política de seguridad está habilitada.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Haga clic en **Add (Añadir)** para añadir una dirección IP para filtrar la excepción de amenaza o ver las **Exempt IP Addresses (Direcciones IP exentas)** existentes.

Configure una dirección IP de exención para aplicar una excepción de amenaza solo cuando la sesión asociada cuente con una dirección IP de origen o de destino coincidente; en el caso de las otras sesiones, la amenaza se aplica en función de la acción de la firma predeterminada.

Inteligencia contra amenazas de AutoFocus para el tráfico de red

Con una suscripción de AutoFocus válida, puede comparar la actividad de su red con los datos de amenazas más recientes disponibles en el portal de AutoFocus. Al conectar su cortafuegos, AutoFocus desbloqueará las siguientes funciones:

- Visualización de resúmenes de inteligencia de AutoFocus relativos a los artefactos de sesión registrados en los logs del cortafuegos.
- Inicio de búsquedas con AutoFocus de artefactos de los logs del cortafuegos.

El resumen de inteligencia de AutFocus revela la prevalencia de un artefacto en su red y a escala global. Los veredictos de WildFire y las etiquetas de AutoFocus que se enumeran para el artefacto indican si el artefacto supone un riesgo para la seguridad.

- Resumen de inteligencia de AutoFocus
- Habilitación de la inteligencia contra amenazas AutoFocus
- Visualice y actúe en función de los datos del resumen de inteligencia de AutoFocus

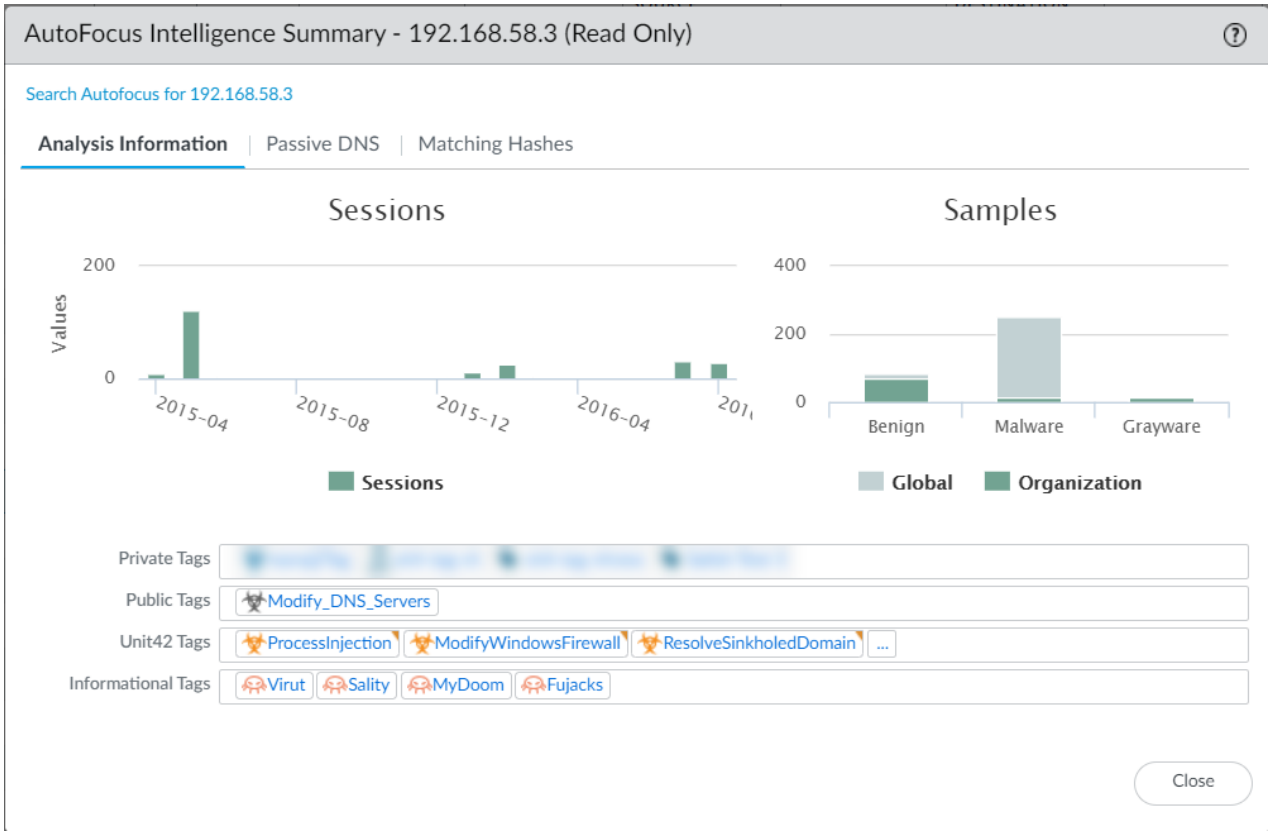
También puede supeditar la aplicación de la política a los hallazgos de AutoFocus:

- Exporte los artefactos de AutoFocus (direcciones IP, URL y dominios) y utilícelos en listas dinámicas externas.
- Use los extractores de AutoFocus como orígenes de las listas dinámicas externas.

Resumen de inteligencia de AutoFocus

El resumen de inteligencia de AutoFocus ofrece una vista centralizada de la información sobre un artefacto que AutoFocus extrajo de la inteligencia de amenazas que se recopilar a partir de otros usuarios de AutoFocus, WildFire, la base de datos de filtrado de URL de PAN-DB, la Unidad 42 y la inteligencia de código abierto.

© 2020 Palo Alto Networks, Inc.



Resumen de inteligencia de AutoFocus	
Analysis Information	La pestaña Analysis Information (Información del análisis) muestra la siguiente información: • Sesiones: la cantidad de veces que se inició sesión en su cortafuegos y se detectaron muestras asociadas al artefacto. • Muestras: una comparación de las muestras de la organización y muestras globales asociadas al artefacto o agrupadas por veredicto de WildFire (benigna, malware o greyware). *Global* se refiere a muestras de todas los envíos de WildFire, mientras que *organización* se refiere solo a muestras enviadas a WildFire por su organización. • Etiquetas coincidentes: las etiquetas de AutoFocus que coinciden con el artefacto. Las etiquetas de AutoFocus indican si un artefacto está vinculado con malware o ataques dirigidos.
DNS pasivo	La pestaña Passive DNS (DNS pasivo) muestra el historial de DNS pasivo que incluye el artefacto. El historial de DNS pasivo se basa en la inteligencia de DNS global en AutoFocus; no se limita a la actividad de DNS en su red. El historial de DNS pasivo consiste en lo siguiente: • La solicitud de dominio • El tipo de solicitud DNS • La dirección IP o el dominio producto de la resolución de la solicitud DNS (las direcciones IP privadas no se muestran) • La cantidad de veces que se realizó la solicitud • La fecha y la hora en la que la solicitud se vio por primera y última vez

© 2020 Palo Alto Networks, Inc.

Resumen de inteligencia de AutoFocus	
Matching Hashes	La pestaña Matching Hashes (Hashes coincidentes) muestra las 5 muestras coincidentes que se detectaron más recientemente. La información de las muestras incluye: • El hash SHA256 de la muestra • El tipo de archivo de la muestra • La fecha y la hora en la que WildFire analizó la muestra y le asignó un veredicto de WildFire • El veredicto de WildFire para la muestra • La fecha y la hora en la que WildFire actualizó el veredicto de WildFire para la muestra (si corresponde)

Habilitación de la inteligencia contra amenazas AutoFocus

Active la licencia de AutoFocus y habilite en el cortafuegos la comunicación con AutoFocus. Una vez configurado, puede ver el Resumen de inteligencia de AutoFocus de los logs o los artefactos del centro de control de aplicaciones (application command center, ACC) para evaluar la penetración en la red y las amenazas asociadas.

STEP 1 | Verifique que la licencia de AutoFocus esté activada en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** para comprobar que la licencia del dispositivo de AutoFocus esté instalada y sea válida (compruebe la fecha de vencimiento).
2. Si el cortafuegos no muestra la licencia, consulte Activación de licencias de suscripción.

STEP 2 | Conecte el cortafuegos a AutoFocus.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de AutoFocus.
2. En **AutoFocus URL (URL de AutoFocus)**, introduzca lo siguiente:

   `https://autofocus.paloaltonetworks.com:10443`
3. Utilice el campo **Query Timeout** para configurar el plazo para que el cortafuegos intente consultar a AutoFocus los datos de inteligencia de amenazas. Si el portal de AutoFocus no responde antes del final del período especificado, el cortafuegos cerrará la conexión.

   Se recomienda configurar el tiempo de espera de consulta en el valor predeterminado de 15 segundos. Las consultas de AutoFocus se optimizan para completarse dentro de este período.
4. Seleccione **Enabled (Habilitado)** para permitir que el cortafuegos se conecte a AutoFocus.
5. Haga clic en **OK (Aceptar)**.
6. Seleccione **Commit** para confirmar los cambios y conservar los ajustes de AutoFocus tras el reinicio.

STEP 3 | Conecte AutoFocus al cortafuegos.

1. Inicie sesión en el portal de AutoFocus: https://autofocus.paloaltonetworks.com
2. Seleccione **Settings**.
3. Seleccione **Add new** para añadir sistemas remotos.
4. Escriba un nombre descriptivo en **Name** para identificar el cortafuegos.
5. Seleccione **PanOS** como el System Type.
6. Introduzca la **dirección** IP del cortafuegos.
7. Haga clic en **Save changes** para añadir el sistema remoto.

© 2020 Palo Alto Networks, Inc.

8. Haga clic en **Save changes** nuevamente en la página Settings para asegurarse de que el cortafuegos se haya añadido correctamente.

STEP 4 | Compruebe la conexión entre el cortafuegos y AutoFocus.

1. En el cortafuegos, seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)**.
2. Verifique que puede evaluar los artefactos del cortafuegos con AutoFocus.

Visualice y actúe en función de los datos del resumen de inteligencia de AutoFocus

Interactúe con el resumen de inteligencia de AutoFocus para mostrar más información sobre un artefacto o extender su búsqueda de artefactos a AutoFocus. Las etiquetas de AutoFocus revelan si el artefacto se asocia a ciertos tipos de malware o comportamiento malicioso.

STEP 1 | Confirme que el cortafuegos está conectado a AutoFocus.

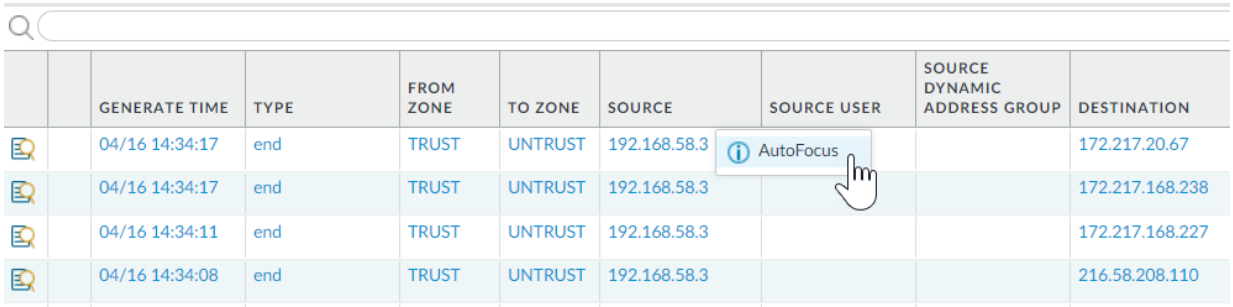
Garantice la Habilitación de la inteligencia contra amenazas AutoFocus del cortafuegos (se requiere una suscripción activa de AutoFocus).

STEP 2 | Busque artefactos para investigar.

Puede ver un resumen de inteligencia de AutoFocus de los artefactos cuando realiza las siguientes acciones:

- Visualización de logs (solo tráfico, amenaza, filtrado de URL, envíos de WildFire, filtrado de datos y logs unificados).
- Visualización de entradas de lista dinámica externa.

STEP 3 | Coloque el cursor sobre un artefacto para abrir el menú desplegable y haga clic en **AutoFocus**.



El resumen de inteligencia de AutoFocus solo se encuentra disponible en los siguientes tipos de artefactos:

Dirección IP

URL

Dominio

Agente de usuario

Nombre de la amenaza (solo para las amenazas de los virus de subtipos y wildfire)

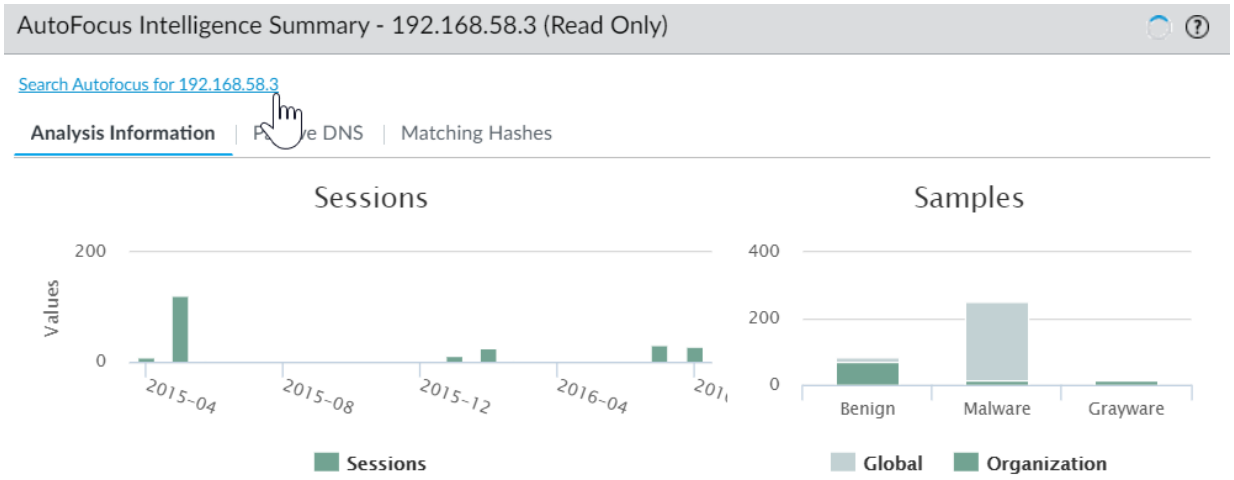
Filename

Hash SHA-256

STEP 4 | Inicie una búsqueda en AutoFocus para buscar el artefacto para el que abrió el resumen de inteligencia de AutoFocus.

© 2020 Palo Alto Networks, Inc.

Haga clic en el enlace **Search AutoFocus for... (Buscar en AutoFocus...)** en la parte superior de la ventana de resumen de inteligencia de AutoFocus. Los resultados de la búsqueda incluyen todos los ejemplos asociados al artefacto. Alterne entre las pestañas **My Samples (Mis ejemplos)** y **All Samples (Todos los ejemplos)** y compare la cantidad de muestras para determinar la omnipresencia del artefacto en su organización.



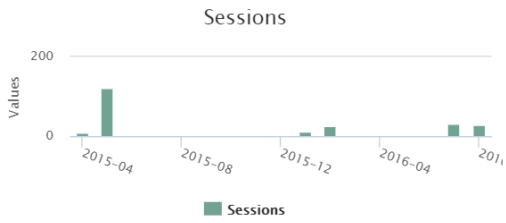
STEP 5 | Inicie una búsqueda en AutoFocus para buscar otros artefactos en el resumen de inteligencia de AutoFocus.

Haga clic en los siguientes artefactos para determinar su omnipresencia en su organización:

- Veredictos de WildFire en la pestaña Analysis Information (Información del análisis)
- URL y direcciones IP en la pestaña Passive DNS (DNS pasivo)
- Hashes SHA256 en la pestaña Matching Hashes (Hashes coincidentes)

STEP 6 | Vea la cantidad de sesiones asociadas al artefacto de su organización por mes.

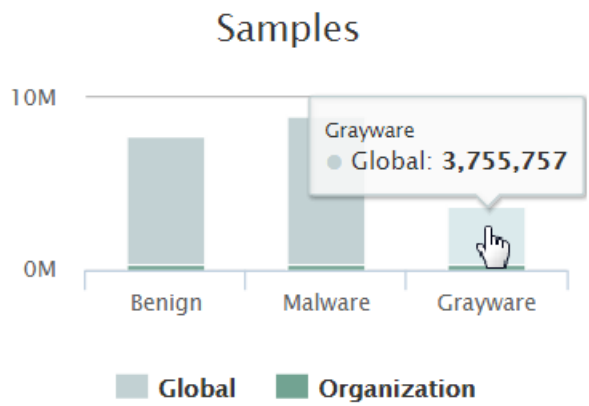
Coloque el cursor sobre las barras de sesiones.



STEP 7 | Vea la cantidad de ejemplos asociados al artefacto por alcance y veredicto de WildFire.

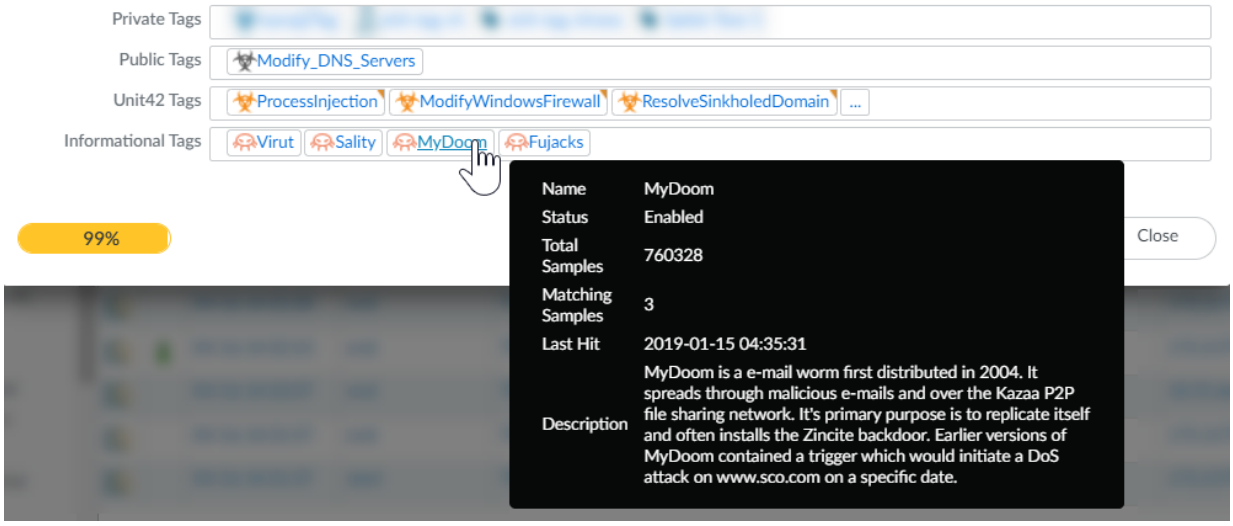
Coloque el cursor sobre las barras de ejemplos.

© 2020 Palo Alto Networks, Inc.



STEP 8 | Vea más detalles sobre las etiquetas coincidentes de AutoFocus

Coloque el cursor sobre una etiqueta coincidente para ver la descripción de la etiqueta y otros detalles de la etiqueta.



STEP 9 | Vea otros ejemplos asociados a la etiqueta coincidente.

Haga clic en una etiqueta coincidente para que Autofocus inicie una búsqueda de esa etiqueta. Los resultados de la búsqueda incluyen todos los ejemplos que coinciden con la etiqueta.

Las etiquetas de la unidad 42 identifican las amenazas y las campañas que suponen un riesgo directo de seguridad. Haga clic en la etiqueta coincidente Unit 42 (Unidad 42) para ver cuántos ejemplos de su red están asociados a la amenaza que identifica la etiqueta.

STEP 10 | Busque más etiquetas coincidentes para un artefacto.

Haga clic en la elipsis (...) para que Autofocus inicie una búsqueda del artefacto. La columna Tags (Etiquetas) en los resultados de la búsqueda muestra más etiquetas que coinciden con el artefacto, lo que le brinda una idea de otras instancias de malware, comportamientos maliciosos, actores de amenazas, explotaciones o campañas donde se detecta el artefacto habitualmente.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Uso compartido de inteligencia de amenazas con Palo Alto Networks

La telemetría es el proceso de recolección y transmisión de datos para su análisis. Cuando habilita la telemetría en el cortafuegos, el cortafuegos recopila y envía periódicamente información sobre aplicaciones, amenazas y el estado del dispositivo a Palo Alto Networks. El uso compartido de la inteligencia de amenazas ofrece los siguientes beneficios:

- Mejor vulnerabilidad y firmas de spyware para usted y otros clientes del mundo. Por ejemplo, cuando un evento de amenaza desencadena firmas de vulnerabilidad o spyware, el cortafuegos comparte las URL asociadas a la amenaza con el equipo de investigación de amenazas de Palo Alto Networks para que puedan clasificar adecuadamente las URL como maliciosas.
- Pruebas y evaluaciones rápidas de las firmas de amenazas experimentales sin impacto en su red, de modo que se pueden suministrar firmas de prevención de amenazas críticas a todos los clientes de Palo Alto Networks con mayor rapidez.
- Mejora la precisión y la capacidad para detectar malware dentro del filtrado de URL de PAN-DB, las firmas de comando y control (C2) basadas en DNS y WildFire.

Palo Alto Networks utiliza la inteligencia de amenazas que se extrae de la telemetría para proporcionarle estos beneficios a usted y a otros usuarios de Palo Alto Networks. Todos los usuarios de Palo Alto Networks se benefician con el uso compartido de los datos de telemetría de cada usuario, lo que convierte a la telemetría en un enfoque impulsado por una comunidad para la prevención de amenazas. Palo Alto Networks no comparte sus datos de telemetría con otros clientes u organizaciones externas.

Para obtener más información sobre la telemetría, incluidos sus beneficios, usos y configuración, consulte Telemetría de dispositivos.

© 2020 Palo Alto Networks, Inc.

Recursos de prevención de amenazas

Para obtener más información sobre las prácticas recomendadas de prevención de amenazas, consulte las siguientes fuentes:

- Creación de firmas de amenazas personalizadas
- Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7
- Prácticas recomendadas de filtrado de URL
- Prácticas recomendadas para Zero Trust
- Prácticas recomendadas de protección DoS y de zonas

Para ver una lista de las amenazas y aplicaciones que los productos de Palo Alto Networks pueden identificar, utilice los siguientes enlaces:

- Applipedia: ofrece información sobre las aplicaciones que Palo Alto Networks puede identificar.
- Threat Vault: enumera todas las amenazas que pueden identificar los productos de Palo Alto Networks. Puede buscar por Vulnerabilidad, Spyware o Virus. Haga clic en el icono de detalles junto al número de ID para obtener más información acerca de una amenaza.

descifrado

Los cortafuegos de Palo Alto Networks pueden descifrar e inspeccionar el tráfico hacer visibles las amenazas y controlar los protocolos, la verificación de certificados y la gestión de fallos. El descifrado puede aplicar políticas en el tráfico cifrado de modo que el cortafuegos lo gestione de acuerdo con sus ajustes de seguridad configurados. Descifre el tráfico para evitar que el contenido malicioso cifrado entre en su red y que el contenido confidencial salga de ella como tráfico cifrado. La habilitación del descifrado puede incluir la preparación de claves y certificados necesarios para el descifrado, la creación de perfiles y políticas de descifrado y la configuración de un reflejo de puerto de descifrado.

- Descripción general del descifrado
- Conceptos de descifrado
- Preparación para implementar el descifrado
- Definición del tráfico para descifrar
- Configuración del proxy SSL de reenvío
- Configuración de la inspección de entrada SSL
- Configuración del Proxy SSH
- Configuración de una verificación del certificado de servidor para el tráfico sin descifrar
- Exclusiones de descifrado
- Bloqueo de exportación de claves privadas
- Permisos para que los usuarios excluyan el descifrado SSL
- Deshabilitación temporal del descifrado SSL
- Configuración del reflejo del puerto de descifrado
- Verificación de descifrado
- Solución de problemas y supervisión del descifrado
- Agente de descifrado
- Activación de las licencias gratuitas para usar las funciones de descifrado

© 2020 Palo Alto Networks, Inc.

Descripción general del descifrado

Los protocolos de descifrado de Capa de sockets seguros (Secure Sockets Layer, SSL) y Shell seguro (Secure Shell, SSH) aseguran el tráfico entre dos entidades, como un servidor web y un cliente. El SSL y el SSH encapsulan el tráfico y cifran los datos de modo que sean ininteligibles para todas las entidades, excepto para el cliente y el servidor que cuentan con los certificados para garantizar la confianza entre los dispositivos y las claves para decodificar los datos. Descifre el tráfico de SSL y SSH para lo siguiente:

- Evite que el malware camuflado como tráfico cifrado se introduzca en su red. Por ejemplo, un atacante pone en riesgo un sitio web que usa el cifrado SSL. Los empleados visitan ese sitio web y descargan un exploit o malware sin darse cuenta. El malware usa el endpoint del empleado infectado para moverse lateralmente por la red y poner en riego otros sistemas.
- Evite que la información confidencial salga de la red.
- Asegúrese de que las aplicaciones correctas se ejecuten en una red segura.
- Descifre el tráfico de manera selectiva. Por ejemplo, cree una política y un perfil de descifrado para excluir del descifrado el tráfico de los sitios financieros o médicos.

El descifrado del cortafuegos de Palo Alto Networks se basa en políticas y puede descifrar, examinar y controlar las conexiones SSL y SSH entrantes y salientes. Una política de descifrado le permite especificar el tráfico para descifrar por destino, origen, servicio o categoría de URL y bloquear, restringir o reenviar el tráfico especificado conforme a la configuración de seguridad en el perfil de descifrado asociado. Un perfil de descifrado controla los protocolos SSL, la verificación de certificados y las comprobaciones de fallos para evitar que el tráfico que use algoritmos débiles o modos no compatibles acceda a la red. El cortafuegos usa certificados y claves para descifrar el tráfico y convertirlo a texto sin formato y luego aplica ajustes de seguridad y App-ID en el tráfico de texto sin formato, lo que incluye el descifrado, antivirus, vulnerabilidades, antispyware, filtrado de URL y perfiles de bloqueo de archivos. Después de descifrar y examinar el tráfico, el cortafuegos vuelve a cifrar el tráfico de texto sin cifrar a medida que sale del cortafuegos para asegurar su privacidad y seguridad.

El cortafuegos proporciona tres tipos de reglas de política de descifrado: El proxy SSL de reenvío para controlar el tráfico de salida SSL, la inspección de entrada de SSL para controlar el tráfico de entrada de SSL y el proxy SSH para controlar el tráfico SSL de transmisión mediante túneles. Puede adjuntar un perfil de descifrado a una regla de política para aplicar la configuración de acceso detallada al tráfico, como comprobaciones para los certificados de servidores, modos no compatibles y fallos.

El descifrado SSL (tanto el proxy de reenvío como la inspección de entrada) requiere certificados para establecer el cortafuegos como un tercero de confianza, y para establecer la confianza entre un cliente y un servidor para asegurar una conexión SSL/TLS. También puede usar certificados cuando excluye servidores del descifrado SSL por motivos técnicos (el sitio interrumpe el descifrado debido a un certificado fijado, cifrados no compatibles o autenticación mutua). El descifrado SSH no requiere certificados.



Use la lista de recomendaciones de descifrado para planificar, implementar y mantener la implementación de descifrado.

Puede integrar un módulo de seguridad de hardware (hardware security module, HSM) con un cortafuegos para permitir una seguridad mejorada para las claves privadas usadas en el proxy de reenvío SSL y en el descifrado de inspección entrante SSL. Para saber más sobre el almacenamiento y la generación de claves con un HSM, así como sobre la integración del HSM en el cortafuegos, consulte Claves seguras con módulos de seguridad de hardware.

También puede usar el reflejo de descifrado para reenviar tráfico descifrado como texto sin cifrar a una solución de terceros para el archivo y los análisis adicionales.

© 2020 Palo Alto Networks, Inc.

Si permite el reflejo de descifrado, tenga en cuenta las leyes y normativas locales sobre qué tráfico puede reflejar y dónde y cómo puede almacenarlo, porque todo el tráfico reflejado, incluida la información confidencial, se reenvía en texto sin cifrar.

© 2020 Palo Alto Networks, Inc.

Conceptos de descifrado

Revise los siguientes temas para obtener más información sobre las funciones de descifrado y la asistencia técnica:

- Políticas de claves y certificados para el descifrado
- Proxy SSL de reenvío
- Perfil de descifrado del proxy SSL de reenvío
- Inspección de entrada SSL
- Perfil de descifrado de inspección de entrada SSL
- Perfil de descifrado de la configuración de protocolo SSL
- Proxy SSH
- Perfil de descifrado del proxy SSH
- Perfil SSL para configuración sin cifrado
- Descifrado SSL para certificados de criptografía de curva elíptica (ECC).
- Compatibilidad del secreto perfecto y permanente (PFS) para el descifrado SSL
- Descifrado SSL y nombres alternativos del asunto (SAN)
- Descifrado TLSv1.3
- Asistencia de alta disponibilidad para sesiones descifradas
- Reflejo de descifrado
- Agente de descifrado

Políticas de claves y certificados para el descifrado

Las claves son cadenas de números que suelen generarse mediante una operación matemática con números aleatorios y números primos altos. Las claves transforman las cadenas (como contraseñas y secretos compartidos) de texto normal sin cifrar a texto cifrado y de texto cifrado a texto normal sin cifrar. Las claves pueden ser simétricas (se usa la misma clave para cifrar y descifrar) o asimétricas (se usa una clave para el cifrado y una clave relacionada matemáticamente para el descifrado). Cualquier sistema puede generar una clave.

Los certificados X.509 se usan para establecer la confianza entre un cliente y un servidor a fin de establecer una conexión SSL. Un cliente que intente autenticar un servidor (o un servidor que autentique un cliente) conoce la estructura del certificado X.509 y por ello sabe cómo extraer la información de identificación del servidor de los campos del certificado, como el FQDN o dirección IP (llamados *nombre común* o *CN* en el certificado) o el nombre de la organización, departamento o usuario para el que se emitió el certificado. Una entidad de certificación (certificate authority, CA) debe emitir todos los certificados. Cuando la CA verifica un cliente o servidor, la CA emite el certificado y lo firma con su clave privada.



Si dispone de dos CA (Device (Dispositivo) > Certificate Management (Gestión de certificado) > Device Certificates (Certificados de dispositivo)) con el mismo asunto y clave, y una CA caducada, elimine (personalizado) o deshabilite (predefinido) la CA caducada. Si no elimina o deshabilita una CA caducada, el cortafuegos puede crear una cadena en la CA caducada si está habilitada en la cadena de confianza y provocar una página de bloqueo.

Cuando se aplica una política de descifrado al tráfico, una sesión entre el cliente y el servidor se establece solo si el cortafuegos confía en la CA que firma el certificado del servidor. Para establecer esa confianza, el cortafuegos debe tener el certificado de la CA raíz del servidor en su lista de certificados de confianza (CTL) y usar la clave pública de ese certificado de CA raíz para comprobar la firma. A continuación, el cortafuegos presenta una copia del certificado del servidor con la firma del certificado de reenvío fiable al cliente para que lo autentique. También puede configurar el cortafuegos para que utilice una CA de empresa como certificado de reenvío fiable para el proxy SSL de reenvío. Si el cortafuegos no tiene el certificado de CA de

© 2020 Palo Alto Networks, Inc.

raíz del servidor en su CTL, presentará una copia del certificado de servidor firmado por el certificado de reenvío no fiable al cliente. El certificado no fiable de reenvío garantiza que a los clientes les aparezca un mensaje con una advertencia de certificación cuando intenten acceder a los sitios alojados en un servidor con certificados que no sean de confianza.

Para obtener más información sobre los certificados, consulte Gestión de certificados.

Para controlar las CA de confianza en las que confía su cortafuegos, use la pestaña Device (Dispositivo) > Certificate Management (Gestión de certificados) > Certificates (Certificados) > Default Trusted Certificate Authorities (Entidades de certificación de confianza predeterminadas) en la interfaz web del cortafuegos.

La siguiente tabla describe los distintos certificados que usan los cortafuegos de Palo Alto Networks para el descifrado.

Certificados utilizados con el descifrado	Description (Descripción)
Certificado de reenvío confiable (utilizado para el descifrado de proxy SSL de reenvío)	Es el certificado que presenta el cortafuegos a los clientes durante el descifrado si el sitio con el que el cliente intenta conectar tiene un certificado firmado con una CA en la que confía el cortafuegos. Para configurar que el certificado de reenvío confiable del cortafuegos se presente a los clientes cuando el certificado del servidor esté firmado por una CA confiable, consulte Configuración de proxy SSL de reenvío. Por defecto, el cortafuegos determina el tamaño de clave que debe usar para el certificado cliente en función del tamaño de clave del servidor de destino. Sin embargo, puede consultar Configuración del tamaño de clave para los certificados de servidor proxy SSL. Para mayor seguridad, almacene la clave privada asociada con el certificado de reenvío confiable en un módulo de seguridad de hardware (consulte Almacenamiento de claves privadas en un HSM). *Realice una copia de seguridad de la clave privada asociada con el certificado de CA de reenvío confiable (no la clave principal del cortafuegos) en un repositorio seguro de modo que si ocurre un problema con el cortafuegos, pueda acceder al certificado de CA de reenvío confiable de todas maneras. Para mayor seguridad, almacene la clave privada asociada con el certificado de reenvío confiable en un módulo de seguridad de hardware (consulte Almacenamiento de claves privadas en un HSM).*
Certificado de reenvío no confiable (utilizado para el descifrado de proxy SSL de reenvío)	Es el certificado que presenta el cortafuegos a los clientes durante el descifrado si el sitio con el que el cliente intenta conectar tiene un certificado firmado con una CA en la que el cortafuegos NO confía. Para configurar un certificado de reenvío no confiable en el cortafuegos, consulte Configuración de proxy SSL de reenvío.
Inspección de entrada SSL	Los certificados de los servidores de su red en los que desea realizar la inspección de entrada SSL del tráfico destinado a estos servidores. Importe los certificados del servidor en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Certificados utilizados con el descifrado	Description (Descripción)
	Desde la versión PAN-OS 8.0, los cortafuegos emplean el algoritmo Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) para realizar comprobaciones estrictas de los certificados. Eso significa que, si el cortafuegos usa un certificado intermedio, debe volver a importarlo al cortafuegos desde el servidor web después de actualizar a PAN-OS 8.0 o a una versión posterior y combinar el certificado del servidor con el certificado intermedio (es decir, instalar un certificado encadenado). Si no lo hace, fallan las sesiones de inspección de entrada de SSL que incluyen un certificado intermedio en la cadena. Para instalar un certificado encadenado: **1.** *Abra cada uno de los archivos de certificado (.cer) en un editor de texto, como el Bloc de notas.* **2.** *Pegue todos los certificados seguidos con el certificado del servidor en primer lugar.* **3.** *Guarde los cambios como un archivo de texto (.txt) o de certificado (.cer); tenga en cuenta que el nombre no puede incluir espacios en blanco.* **4.** *Importe el certificado combinado (encadenado) al cortafuegos.*

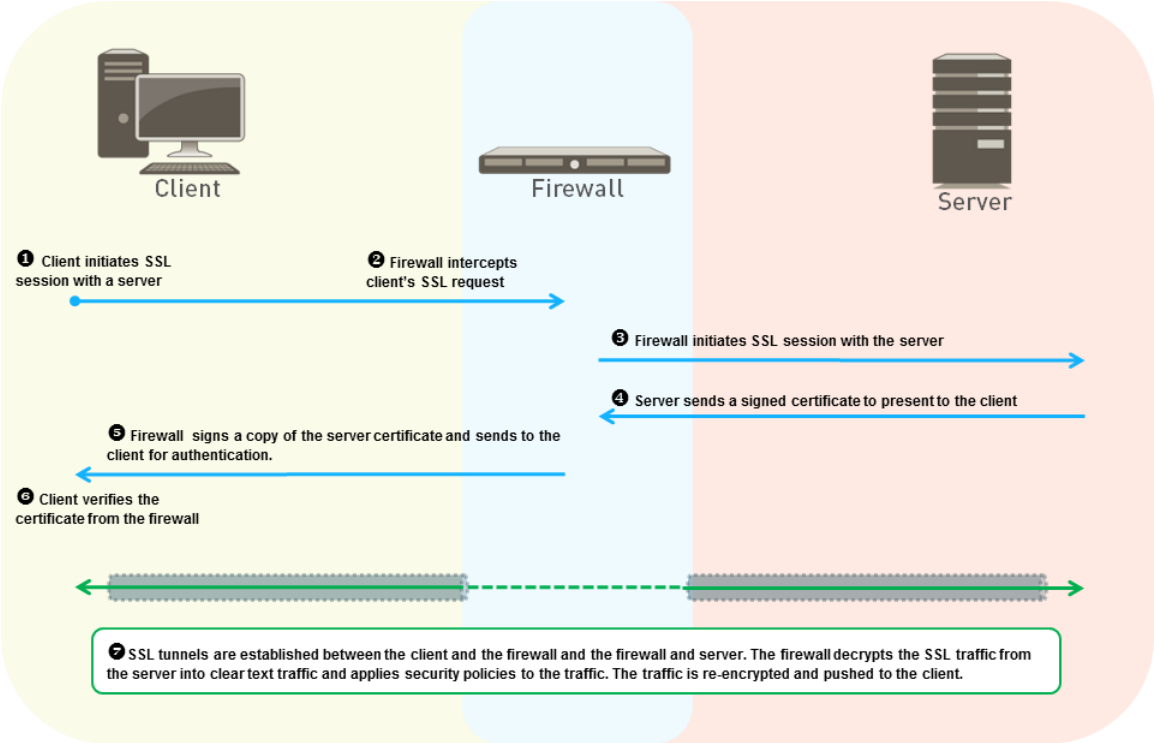
Proxy SSL de reenvío

Cuando configura el cortafuegos para descifrar tráfico SSL que se dirige a sitios externos, funciona como un proxy SSL de reenvío. Utilice una política de descifrado del proxy SSL de reenvío para descifrar y examinar el tráfico SSL/TLS de usuarios internos a Internet. El descifrado de proxy SSL de reenvío evita que el malware oculto como tráfico cifrado SSL entre en su red corporativa mediante el descifrado del tráfico, de modo que el cortafuegos pueda aplicar perfiles de descifrado y perfiles y políticas de seguridad en el tráfico.

En el descifrado del proxy SSL de reenvío, el cortafuegos es un intermediario (man-in-the-middle) que se encuentra entre el cliente interno y el servidor externo. El cortafuegos usa certificados para representar de manera clara al cliente ante el servidor y el servidor ante el cliente, de modo que el cliente cree que se está comunicando directamente con el servidor (aunque la sesión del cliente sea con el cortafuegos) y el servidor cree que se está comunicando directamente con el cliente (aunque la sesión del servidor también sea con el cortafuegos). El cortafuegos utiliza certificados para establecerse como agente externo de confianza (man-in-the-middle) para la sesión entre el cliente y el servidor (si desea información detallada sobre los certificados, consulte Políticas de claves y certificados para el descifrado).

La siguiente figura muestra este proceso en detalle. Consulte la Configuración del proxy SSL de reenvío para obtener más información detallada sobre la configuración del proxy SSL de reenvío.

© 2020 Palo Alto Networks, Inc.

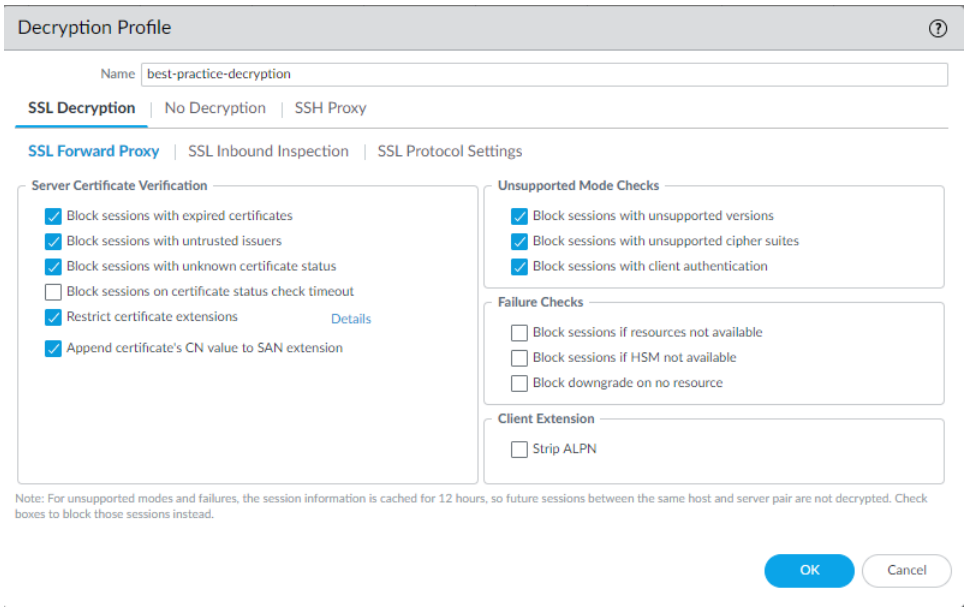


1. El cliente interno de su red intenta iniciar una sesión TLS con un servidor externo.
2. El cortafuegos intercepta la solicitud de certificado SSL del cliente. Para el cliente, el cortafuegos actúa como el servidor externo, aunque la sesión segura establecida sea con el cortafuegos, no con el servidor real.
3. El cortafuegos reenvía la solicitud de certificado SSL del cliente al servidor para iniciar una sesión diferente con el servidor. Para el servidor, el cortafuegos luce como el cliente, el servidor desconoce que existe un intermediario (man-in-the-middle) y verifica el certificado.
4. El servidor envía al cortafuegos un certificado firmado destinado al cliente.
5. El cortafuegos analiza el certificado del servidor. Si el certificado del servidor está firmado por una CA en la que el cortafuegos confía y cumple con los perfiles y políticas configurados, el cortafuegos genera una copia del certificado del servidor confiable de reenvío SSL y la envía al cliente. Si el certificado del servidor está firmado por una CA en la que el cortafuegos no confía, el cortafuegos genera una copia del certificado del servidor no confiable de reenvío SSL y la envía al cliente. La copia del certificado que genera y envía el cortafuegos al cliente contiene extensiones del certificado del servidor original y se denomina un certificado de *personificación* porque no es el certificado real del servidor. Si el cortafuegos no confía en el servidor, el cliente verá un mensaje de advertencia de página bloqueada que indica que el sitio con el que intenta conectarse no es confiable, y si permite que los usuarios opten por excluir el descifrado SSL, el cliente tendrá la opción de continuar o finalizar la sesión.
6. El cliente verifica el certificado de personificación del cortafuegos. Luego, el cliente inicia un intercambio de clave de sesión con el servidor, en el que el cortafuegos realiza una conexión proxy de la misma manera que lo hace con los certificados. El cortafuegos reenvía la clave de cliente al servidor y realiza la copia de la personificación de la clave del servidor para el cliente, de modo que el cortafuegos permanece como un proxy "invisible", el cliente y el servidor creen que su sesión está establecida entre ellos, pero existen dos sesiones diferentes, una entre el cliente y el cortafuegos, y otra entre el cortafuegos y el servidor. Ahora todas las partes tienen los certificados y claves necesarios y el cortafuegos puede descifrar el tráfico.
7. Todo el tráfico de la sesión SSL pasa por el cortafuegos de manera trasparente entre el cliente y el servidor. El cortafuegos descifra el tráfico SSL, aplica políticas y perfiles de seguridad y perfiles de descifrado en el tráfico, vuelve a cifrar el tráfico y, luego, lo reenvía.

© 2020 Palo Alto Networks, Inc.

Perfil de descifrado del proxy SSL de reenvío

El perfil de descifrado de proxy SSL de reenvío (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **SSL Decryption [Descifrado SSL]** > **SSL Forward Proxy [Proxy SSL de reenvío]**) controla la verificación del servidor, las comprobaciones de modo de sesión y las comprobaciones de fallos para el tráfico SSL/TLS de salida definido en las políticas de descifrado de proxy de reenvío a las que adjunta el perfil. La siguiente figura muestra las recomendaciones generales para la configuración del perfil de descifrado de proxy de reenvío, pero la configuración que use también depende de las reglas de cumplimiento de seguridad de su empresa y de las leyes y normativas locales. También hay recomendaciones específicas para los perfiles de descifrado de puerta de enlace de Internet del perímetro y para los perfiles de descifrado del centro de datos.

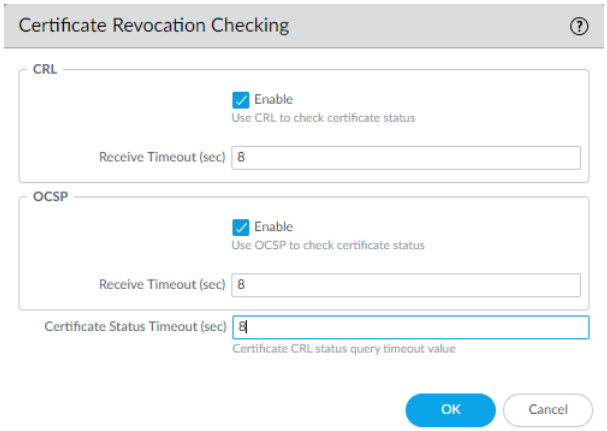


Verificación de certificado de servidor:

- **Bloquear sesiones con certificados caducados:** siempre marque esta casilla para bloquear sesiones con servidores que contengan certificados caducados y evitar el acceso a sitios posiblemente inseguros. Si no marca esta casilla, los usuarios podrán conectarse y realizar transacciones con sitios potencialmente maliciosos y ver mensajes de advertencia cuando intenten conectarse, pero no se evitará la conexión.
- **Bloquear sesiones con emisores no confiables:** siempre marque esta casilla para bloquear sesiones con servidores que contengan emisores de certificados no confiables. Un emisor no confiable puede indicar ataques por desconocidos, ataques de reproducción o de otro tipo.
- **Bloquear sesiones con estado de certificado desconocido:** bloquea la sesión SSL/TLS cuando el estado de revocación de certificado del servidor muestra el estado "desconocido". Debido a que el estado del certificado puede ser desconocido por varios motivos, en el caso de la seguridad general del descifrado, si marca esta casilla de verificación, se aumenta demasiado la seguridad. Sin embargo, en áreas de mayor seguridad de la red como los centros de datos, tiene sentido marcar esta casilla de verificación.
- **Bloquear sesiones al agotar el tiempo de espera de comprobación de estado de certificado**: bloquear o no las sesiones si la comprobación de estado agota el tiempo de espera depende de la posición de cumplimiento de seguridad de su empresa, porque es un punto intermedio entre una seguridad más estricta y una mejor experiencia de usuario. La verificación de estado del certificado examina la lista de revocación de certificados (Certificate Revocation List, CRL) en un servidor de revocación o usa un Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) para definir si la CA emisora revocó el certificado y no se debe confiar en él. Sin embargo, los servidores de revocación pueden tardar en responder, lo que puede provocar que se agote el tiempo de espera de la sesión y el cortafuegos bloquee la sesión aunque el certificado sea válido. Si selecciona **Block sessions on certificate status check timeout (Bloquear sesiones al agotar el tiempo de espera de comprobación de estado de**

© 2020 Palo Alto Networks, Inc.

certificado) y el servidor de revocación tarda en responder, puede usar **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Configuración de descifrado)** y hacer clic en **Certificate Revocation Checking (Comprobación de revocación de certificados)** para modificar el valor predeterminado del tiempo de espera de cinco segundos a otro valor. Por ejemplo, puede aumentar el valor del tiempo de espera a ocho segundos, como se muestra en la siguiente figura. Habilite la comprobación de revocación de certificados de CRL y de OCSP porque los certificados de servidor pueden contener URL de CRL en la extensión del Punto de distribución de CRL (CRL Distribution Point, CDP) o URL de OCSP en la extensión de certificado de Acceso a la información de la entidad (Authority Information Access, AIA).



- **Restringir extensiones de certificados:** si marca esta casilla, se limitan las extensiones de certificados en el certificado del servidor al uso de claves y el uso de claves extendido, y se bloquean los certificados con otras extensiones. Sin embargo, en ciertas implementaciones, algunas otras extensiones de certificados pueden ser necesarias, por lo que solo debe marcar esta casilla si su implementación no requiere otras extensiones de certificados.
- **Adjuntar valor de CN del certificado a la extensión de SAN:** marcar esta casilla garantiza que cuando un explorador requiere que un certificado de servidor use un Nombre alternativo de asunto (Subject Alternative Name, SAN) y no admite la coincidencia de certificado sobre la base del Nombre común (Common Name, CN), si el certificado no tiene una extensión de SAN, los usuarios podrán acceder igualmente a los recursos web solicitados porque el cortafuegos añade la extensión de SAN (sobre la base del CN) al certificado de personificación.

Comprobaciones de modo no admitidas. Si no bloquea sesiones con modos no admitidos, los usuarios reciben un mensaje de advertencia si se conectan con servidores posiblemente inseguros y pueden hacer clic en ese mensaje e ingresar al sitio potencialmente peligroso. Bloquear estas sesiones lo protege de servidores que utilicen algoritmos y versiones de protocolo riesgosas y débiles:

- **Bloqueo de sesiones con versiones no admitidas**: cuando configure el Perfil de descifrado de la configuración de protocolo SSL, especifique la versión mínima del protocolo SSL que permite en su red a fin de bloquear protocolos débiles y, de ese modo, reducir la superficie de ataque. Siempre marque esta casilla para bloquear sesiones con versiones de protocolo SSL/TLS débiles que decidió no admitir.
- **Bloquear sesiones con conjuntos de cifrados no admitidos:** siempre marque esta casilla para bloquear sesiones si el cortafuegos no admite el conjunto de cifrados especificado en el protocolo de enlace. Configure qué algoritmos admite el cortafuegos en la pestaña **SSL Protocol Settings (Configuración del protocolo SSL)** del perfil de descifrado.
- **Bloquear sesiones con autenticación de cliente:** si no tiene aplicaciones críticas que requieren la autenticación de cliente, bloquéela porque el cortafuegos no puede descifrar este tipo de sesiones. El cortafuegos necesita los certificados tanto del cliente como del servidor para realizar el descifrado bidireccional, pero con la autenticación del cliente, el cortafuegos solo conoce el certificado del servidor. Esto interrumpe el descifrado para las sesiones con autenticación de cliente. Cuando marca esta casilla, el cortafuegos bloquea todas las sesiones con autenticación de cliente, excepto aquellas de los sitios

© 2020 Palo Alto Networks, Inc.

en la lista de exclusión del descifrado SSL (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**).

Si no **bloquea sesiones con autenticación de cliente**, cuando el cortafuegos intenta descifrar una sesión que usa la autenticación de cliente, permite la sesión y añade una entrada en su caché de exclusión de descifrado local que contiene la dirección IP/URL del servidor, la aplicación y el perfil de descifrado para su Caché de exclusión de descifrado local.



Es posible que deba permitir el tráfico en su red de sitios que usen la autenticación de cliente y que no estén en los sitios predefinidos en la lista de exclusión de descifrado SSL. Cree un perfil de descifrado que permita las sesiones con autenticación de cliente. Añádalo a la regla de política de descifrado que se aplica solo a los servidores que tienen la aplicación. Para aumentar aún más la seguridad, puede requerir la autenticación multifactor para completar el proceso de inicio de sesión del usuario.

Comprobación de fallos:

- **Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles)**: si bloquea sesiones cuando no hay recursos de procesamiento de cortafuegos disponibles, este descarta el tráfico cuando no tiene los recursos para descifrar el tráfico. Si no bloquea las sesiones cuando el cortafuegos no puede procesar el descifrado debido a la falta de recursos, el tráfico que desee descifrar entrará en la red cifrado aún y, por lo tanto, no se inspeccionará. Sin embargo, bloquear sesiones cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la experiencia de usuario, en comparación con una seguridad más estricta. De manera alternativa, considere usar modelos de cortafuegos con mayor potencia de procesamiento, de modo que pueda descifrar más tráfico.
- **Bloquear sesiones si HSM no está disponible:** si usa o no un Módulo de seguridad de hardware (HSM, Hardware Security Module) para almacenar sus claves privadas depende de sus reglas de cumplimiento acerca de dónde debe provenir la clave privada y cómo desea administrar el tráfico cifrado si el HSM no está disponible. Por ejemplo, si su empresa exige el uso de un HSM para la firma de claves privadas, entonces, bloquea las sesiones si el HSM no está disponible. Sin embargo, si su empresa es menos estricta en este aspecto, entonces puede considerar no bloquear sesiones si el HSM no está disponible. (Si el HSM no está disponible, el cortafuegos puede procesar el descifrado de los sitios para los cuales tiene almacenado en caché la respuesta del HSM, pero no para otros sitios). La acción recomendada en este caso depende de las políticas de su empresa. Si el HSM es crítico para su empresa, ejecútelo en el par de alta disponibilidad (high-availability, HA) (PAN-OS 8.1 admite dos miembros en un par de HA de HSM).
- **Block downgrade on no resource (Bloquear el cambio a una versión anterior sin recurso)**: con esta opción, se evita que el cortafuegos cambie de una versión TLSv1.3 a TLSv1.2 si este no tiene recursos de procesamiento TLSv1.3 disponibles. Si bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, descartará el tráfico que usa TLSv1.3 en lugar de degradarlo a TLSv1.2. Si no bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, se degradará a TLSv1.2. Sin embargo, bloquear el cambio a una versión anterior cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la experiencia de usuario, en comparación con una seguridad más estricta. Es posible que desee crear una política y un perfil de descifrado independientes para regular el descifrado del tráfico sensible para el que no desee degradar la versión TLS.

© 2020 Palo Alto Networks, Inc.

Inspección de entrada SSL

Use la Inspección de entrada SSL para descifrar y examinar el tráfico SSL/TLS entrante de un cliente a un servidor de red objetivo (cualquier servidor para el que tenga el certificado y pueda importarlo en el cortafuegos) y bloquee las sesiones sospechosas. Por ejemplo, si un empleado se ha conectado remotamente a un servidor web alojado en la red de la empresa e intenta añadir documentos internos restringidos a su carpeta de Dropbox (que usa SSL para la transmisión de datos), la inspección de entrada SSL puede asegurar que los datos confidenciales no salgan de la red segura de la empresa mediante un bloqueo o restricción de la sesión.

En el cortafuegos, debe instalar el certificado y la clave privada para cada servidor en el que desee realizar una inspección de entrada SSL. También debe instalar el certificado de clave pública y el de clave privada en cada cortafuegos que realice una inspección de entrada SSL. La forma en que el cortafuegos lleva a cabo la inspección de entrada SSL depende del tipo de clave negociada: Rivest, Shamir, Adleman (RSA) o Confidencialidad directa total (Perfect Forward Secrecy, PFS).

Para las claves de RSA, el cortafuegos realiza la inspección de entrada SSL sin finalizar la conexión. A medida que la sesión cifrada fluye por el cortafuegos, este realiza una copia de ella de manera clara y la descifra de modo que el cortafuegos pueda aplicar la política apropiada en el tráfico.



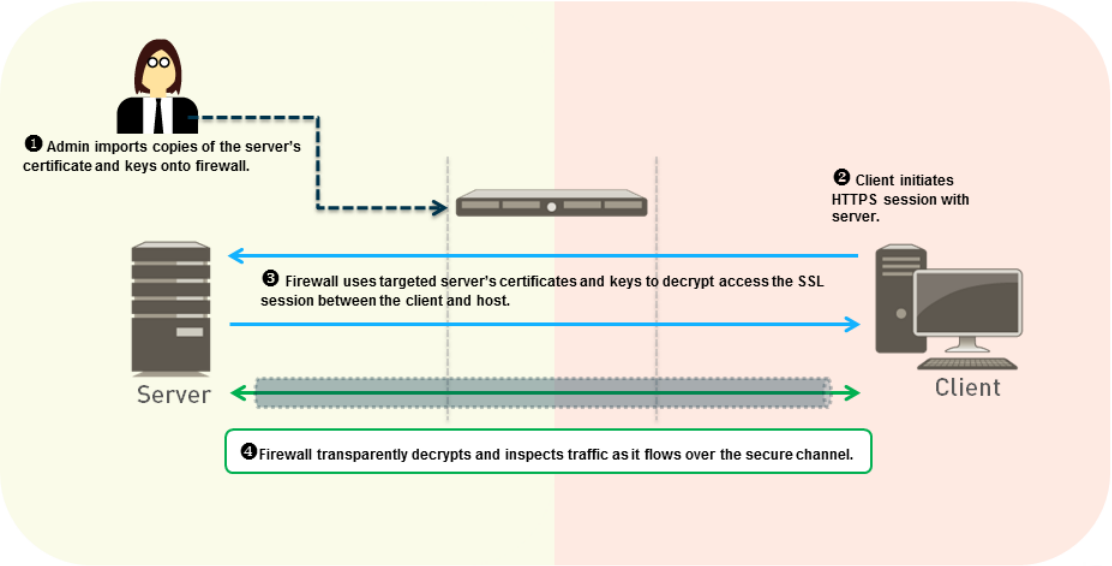
Cuando configura el perfil de descifrado de la configuración del protocolo SSL para el tráfico de inspección de entrada SSL, cree diferentes perfiles para los servidores con diferentes capacidades de seguridad. Por ejemplo, si un conjunto de servidores admite solo RSA, la configuración del protocolo SSL solo necesita admitir RSA. Sin embargo, la configuración del protocolo SSL para los servidores que son compatibles con PFS debe admitir PFS. Ajuste la configuración del protocolo SSL para el nivel más alto de seguridad que admita el servidor, pero verifique el rendimiento para garantizar que los recursos del cortafuegos puedan administrar una mayor carga de procesamiento que requieren los protocolos y algoritmos de seguridad más altos.

Para las claves PFS que usan Diffie-Hellman exchange (DHE) o Elliptic Curve Diffie-Hellman exchange (ECDHE), el cortafuegos actúa como un proxy intermediario entre el cliente externo y el servidor interno. Dado que PFS genera una clave nueva con cada sesión, el cortafuegos no puede simplemente copiar y descifrar el flujo SSL de entrada a medida que pasa, el cortafuegos debe actuar como un dispositivo proxy.

La siguiente figura muestra cómo funciona la inspección de entrada SSL cuando el algoritmo de intercambio de claves es RSA. Cuando el algoritmo de intercambio de claves es PFS, el cortafuegos funciona como un proxy (crea una sesión segura entre el cliente y el cortafuegos, y otra sesión entre el cortafuegos y el servidor) y debe generar una nueva clave de sesión para cada sesión segura.

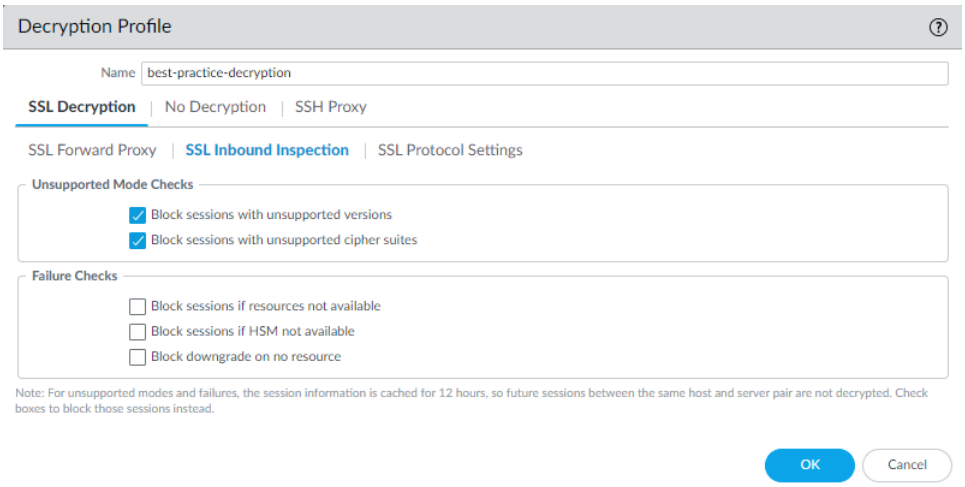
Consulte Configuración de la inspección de entrada SSL para obtener información detallada sobre la habilitación de esta función.

© 2020 Palo Alto Networks, Inc.



Perfil de descifrado de inspección de entrada SSL

El perfil de descifrado de inspección de entrada SSL (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **SSL Decryption [Descifrado SSL]** > **SSL Inbound Inspection [Inspección de entrada SSL]**) controla las comprobaciones de modo y de fallos de sesión para el tráfico SSL/TLS de entrada definido en las políticas de descifrado de inspección de entrada a las cuales adjunta el perfil. La siguiente figura muestra las recomendaciones generales para la configuración del perfil de descifrado de inspección de entrada, pero la configuración que use también depende de las reglas de cumplimiento de seguridad de su empresa y de las leyes y normativas locales.



Comprobaciones de modo no admitidas. Si no bloquea sesiones con modos no admitidos, los usuarios reciben un mensaje de advertencia si se conectan con servidores posiblemente inseguros y pueden hacer clic en ese mensaje e ingresar al sitio potencialmente peligroso. Bloquear estas sesiones lo protege de servidores que utilicen algoritmos y versiones de protocolo riesgosas y débiles:

1. **Block sessions with unsupported versions (Bloqueo de sesiones con versiones no admitidas)**: cuando configure el Perfil de descifrado de la configuración de protocolo SSL, especifique la versión mínima del protocolo TLS que permite en su red a fin de bloquear protocolos débiles y, de ese modo, reducir la superficie de ataque. Siempre marque esta casilla para bloquear sesiones con versiones de protocolo SSL y TLS débiles que decidió no admitir.

© 2020 Palo Alto Networks, Inc.

2. **Bloquear sesiones con conjuntos de cifrados no admitidos:** siempre marque esta casilla para bloquear sesiones si el cortafuegos no admite el conjunto de cifrados especificado en el protocolo de enlace. Configure qué algoritmos admite el cortafuegos en la pestaña **SSL Protocol Settings (Configuración del protocolo SSL)** del perfil de descifrado.

Comprobación de fallos:

- **Block sessions if resources not available (Bloquear sesiones si los recursos no están disponibles)**: si bloquea sesiones cuando no hay recursos de procesamiento de cortafuegos disponibles, este descarta el tráfico cuando no tiene los recursos para descifrar el tráfico. Si no bloquea las sesiones cuando el cortafuegos no puede procesar el descifrado debido a la falta de recursos, el tráfico que desee descifrar entrará en la red cifrado aún y, por lo tanto, no se inspeccionará. Sin embargo, bloquear sesiones cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la experiencia de usuario, en comparación con una seguridad más estricta. De manera alternativa, considere usar modelos de cortafuegos con mayor potencia de procesamiento, de modo que pueda descifrar más tráfico.
- **Bloquear sesiones si HSM no está disponible:** si usa o no un Módulo de seguridad de hardware (HSM, Hardware Security Module) para almacenar sus claves privadas depende de sus reglas de cumplimiento acerca de dónde debe provenir la clave privada y cómo desea administrar el tráfico cifrado si el HSM no está disponible. Por ejemplo, si su empresa exige el uso de un HSM para la firma de claves privadas, entonces, bloquea las sesiones si el HSM no está disponible. Sin embargo, si su empresa es menos estricta en este aspecto, entonces puede considerar no bloquear sesiones si el HSM no está disponible. (Si el HSM no está disponible, el cortafuegos puede procesar el descifrado de los sitios para los cuales tiene almacenado en caché la respuesta del HSM, pero no para otros sitios). La acción recomendada en este caso depende de las políticas de su empresa. Si el HSM es crítico para su empresa, ejecútelo en el par de alta disponibilidad (high-availability, HA) (PAN-OS 8.1 admite dos miembros en un par de HA de HSM).
- **Block downgrade on no resource (Bloquear el cambio a una versión anterior sin recurso)**: con esta opción, se evita que el cortafuegos cambie de una versión TLSv1.3 a TLSv1.2 si este no tiene recursos de procesamiento TLSv1.3 disponibles. Si bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, descartará el tráfico que usa TLSv1.3 en lugar de degradarlo a TLSv1.2. Si no bloquea el cambio a una versión anterior, cuando el cortafuegos se quede sin recursos TLSv1.3, se degradará a TLSv1.2. Sin embargo, bloquear el cambio a una versión anterior cuando los recursos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no esta comprobación de fallos depende de la posición de cumplimiento de seguridad de su empresa y de la importancia de la experiencia de usuario, en comparación con una seguridad más estricta. Es posible que desee crear una política y un perfil de descifrado independientes para regular el descifrado del tráfico sensible para el que no desee degradar la versión TLS.

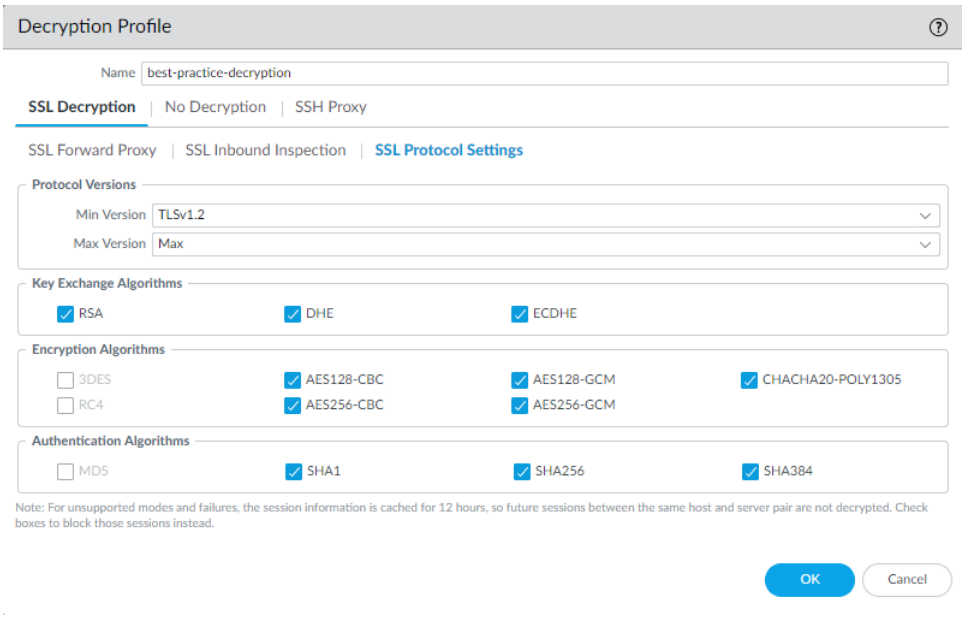
Perfil de descifrado de la configuración de protocolo SSL

La configuración del protocolo SSL (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **SSL Decryption [Descifrado SSL]** > **SSL Protocol Settings [Configuración del protocolo SSL]**) controla si permite versiones de protocolo SSL/TLS vulnerables y algoritmos de cifrado y de autenticación débiles. La configuración del protocolo SSL se aplica al tráfico de inspección de entrada SSL y al proxy SSL de reenvío de salida. Esta configuración no se aplica al tráfico de proxy SSL o al tráfico que no descifra.

La siguiente figura muestra las recomendaciones generales para la configuración del protocolo SSL. También hay recomendaciones específicas para los perfiles de descifrado de puerta de enlace de Internet del perímetro y para los perfiles de descifrado del centro de datos.

© 2020 Palo Alto Networks, Inc.

Cuando configure los ajustes del protocolo SSL para el tráfico de inspección de entrada SSL, cree diferentes perfiles para los servidores con diferentes capacidades de seguridad. Por ejemplo, si un conjunto de servidores admite solo RSA, la configuración del protocolo SSL solo necesita admitir RSA. Sin embargo, la configuración del protocolo SSL para los servidores que son compatibles con PFS debe admitir PFS. Ajuste la configuración del protocolo SSL para el nivel más alto de seguridad que admita el servidor objetivo que protege, pero verifique el rendimiento para garantizar que los recursos del cortafuegos puedan administrar la mayor carga de procesamiento que requieren los protocolos y algoritmos de seguridad más alta.



Versiones de protocolo:

- Configure la **Min Version (Versión mínima)** en **TLSv1.2** para proporcionar la mayor seguridad; los sitios comerciales que valoran la seguridad admiten TLSv1.2. Si un sitio (o una categoría de sitios) solo admite cifrados más débiles, revise el sitio y determine si tiene una aplicación comercial legítima. Si es así, realice una excepción únicamente para ese sitio. Configure un perfil de descifrado con una **Min Version (versión mínima)** que coincida con el cifrado más estricto que admita el sitio y luego aplique el perfil en una regla de política de descifrado que limite el cifrado débil a solo el sitio o los sitios en cuestión. Si el sitio no tiene una aplicación comercial legítima, no debilite su seguridad para admitir este sitio; los protocolos (y cifrados) débiles contienen vulnerabilidades conocidas que los atacantes pueden aprovechar.

  Si el sitio pertenece a una categoría de sitios que no necesita con fines comerciales, use el filtrado de URL para bloquear el acceso a la categoría completa. No permita algoritmos de autenticación o cifrado débiles salvo que deba admitir sitios heredados importantes y, cuando realice excepciones, cree un perfil de descifrado diferente que permita el protocolo más débil solo para esos sitios. No cambie la versión del perfil de descifrado principal que aplica a la mayoría de los sitios a TLSv1.1 solo para incorporar algunas excepciones.

  La página web SSL Pulse de Qualys SSL Labs proporciona estadísticas actualizadas sobre los porcentajes de diferentes cifrados y protocolos en uso en los 150 000 sitios más populares del mundo, de modo que pueda ver las tendencias y comprender lo amplio que es el soporte en el mundo de protocolos y cifrados más seguros.
- Configure la **Max Version (Versión máxima)** en **Max (Máxima)** en lugar de configurarla en una versión determinada, de modo que a medida que los protocolos mejoren, el cortafuegos admita automáticamente los mejores protocolos más nuevos. Tanto si adjunta un perfil de descifrado a una regla

© 2020 Palo Alto Networks, Inc.

de política de descifrado que rige el tráfico de entrada (Inspección de entrada SSL) o el de salida (proxy SSL de reenvío), evite los algoritmos débiles.



Si su política de descifrado admite aplicaciones móviles (muchas de las cuales utilizan certificados fijados), configure Max Version (Versión máx.) en TLSv1.2. Puesto que TLSv1.3 cifra la información del certificado que no se cifró en versiones anteriores de TLS, el cortafuegos no puede añadir automáticamente exclusiones de descifrado basadas en la información del certificado, lo que afecta a algunas aplicaciones móviles. Por lo tanto, si habilita TLSv1.3, el cortafuegos puede eliminar parte del tráfico de aplicaciones móviles a no ser que cree una política de no descifrado para ese tráfico.

Si conoce las aplicaciones móviles que usa para su empresa, considere la posibilidad de crear una política y un perfil de descifrado independientes para esas aplicaciones. De esa forma, podrá habilitar TLSv1.3 para el resto del tráfico de aplicaciones.

Algoritmos de intercambio de clave: Deje las tres casillas marcadas (valor predeterminado) para admitir los intercambios de claves RSA y PFS (DHE y ECDHE) a no ser que la versión mínima esté configurada en TLSv1.3, que solo admite ECDHE.



Para que se admita el tráfico HTTP/2, debe dejar marcada la casilla ECDHE.

Algoritmos de cifrado: Cuando configure la versión de protocolo mínima en TLSv1.2, los algoritmos 3DES y RC4 más antiguos y débiles se desmarcan (bloquean) de forma automática. Cuando establezca la versión mínima del protocolo en TLSv1.3, los algoritmos 3DES, RC4, AES128-CBC y AES256-CBC se bloquean automáticamente. Para cualquier tráfico para el que deba permitir un protocolo TLS más débil, cree un perfil de descifrado independiente y aplíquelo solo al tráfico de ese sitio, y anule la selección de las casillas correspondientes para permitir el algoritmo. Si permite el tráfico que utiliza los algoritmos 3DES o RC4, expondrá la red a un riesgo excesivo. Si el bloqueo de 3DES o RC4 evita que se pueda acceder a un sitio que debe usar en la empresa, cree un perfil de descifrado y directiva diferente para ese sitio. No debilite el descifrado para ningún otro sitio.

Algoritmos de autenticación: El cortafuegos bloquea automáticamente el algoritmo MD5 más antiguo y más débil. Si TLSv1.3 es la versión mínima, el cortafuegos también bloqueará SHA1. No permita el tráfico autenticado por MD5 en su red; SHA1 es el algoritmo de autenticación más débil que debe permitir. Si ningún sitio necesario utiliza SHA1, bloquee el tráfico SHA1 para reducir aún más la superficie de ataque.

Proxy SSH

En una configuración Proxy SSH, el cortafuegos se encuentra entre un cliente y un servidor. El proxy SSH permite que el cortafuegos descifre sesiones SSH entrantes y salientes, y garantiza que los atacantes no usen SSH para canalizar contenido y aplicaciones no deseadas. El descifrado SSH no requiere de certificados y el cortafuegos genera automáticamente la clave que se usa para el descifrado SSH cuando se inicia el cortafuegos. Durante el proceso de inicio, el cortafuegos comprueba si ya existe una clave. Si no es así, el cortafuegos genera una clave. El cortafuegos usa la clave para descifrar sesiones SSH para todos los sistemas virtuales configurados en el cortafuegos y todas las sesiones SSH v2.

SSH permite la canalización, que puede ocultar tráfico malicioso del descifrado. El cortafuegos no puede descifrar tráfico dentro de un túnel SSH. Puede bloquear todo el tráfico del túnel SSH configurando una regla de política de seguridad para la aplicación **ssh-tunnel** con la opción **Action (Acción)** configurada en **Deny (Rechazar)** (junto con la regla de la política de seguridad para permitir tráfico desde la aplicación **ssh**).

Las sesiones de canalización SSH pueden canalizar paquetes de Windows X11 y TCP. Una conexión SSH puede contener varios canales. Cuando aplica un perfil de descifrado SSH al tráfico, en cada canal de la conexión, el cortafuegos examina el App-ID del tráfico e identifica el tipo de canal. El tipo de canal puede ser uno de los siguientes:

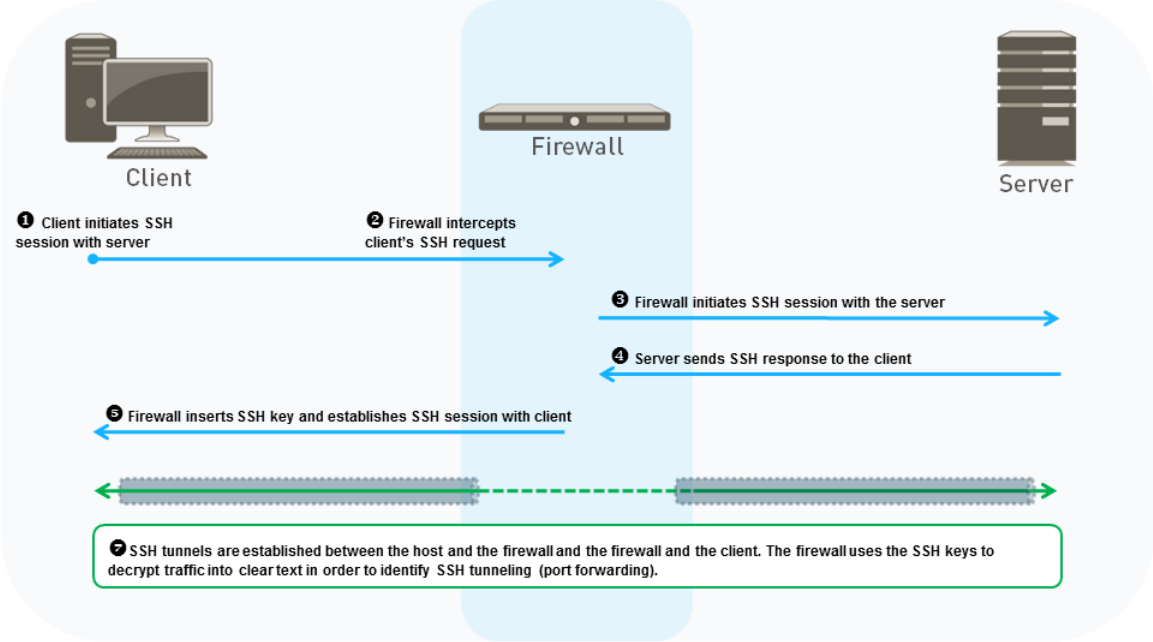
© 2020 Palo Alto Networks, Inc.

- sesión
- X11
- forwarded-tcpip
- direct-tcpip

Cuando el tipo de canal es sesión, el cortafuegos identifica el tráfico como tráfico SSH permitido como FTP o SCP. Cuando el tipo de canal es X11, forwarded-tcpip, or direct-tcpip, el cortafuegos identifica el tráfico como tráfico de canalización SSH y lo bloquea.

Limite el uso de SSH a administradores que necesitan gestionar dispositivos de red, registre todo el tráfico SSH y considere configurar una autenticación multifactor para ayudar a garantizar que solo los usuarios legítimos puedan usar SSH para acceder a dispositivos, lo que reduce la superficie de ataque.

La siguiente figura muestra cómo funciona el cifrado de proxy SSH. Consulte la Configuración de proxy SSH para conocer cómo habilitar el descifrado de proxy SSH.



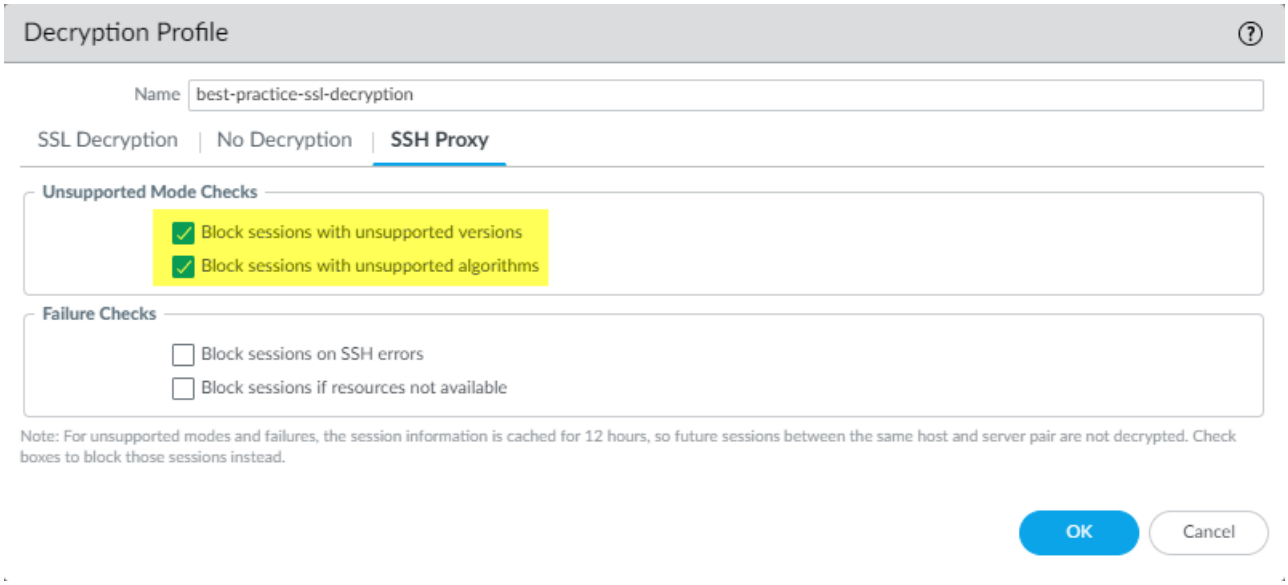
Cuando el cliente envía una solicitud SSH al servidor para iniciar una sesión, el cortafuegos intercepta la solicitud y la reenvía al servidor. El cortafuegos intercepta la respuesta del servidor y la reenvía al cliente. Esta acción establece dos túneles SSH diferentes, uno entre el cortafuegos y el cliente y otro entre el cortafuegos y el servidor, y en donde el cortafuegos funciona como proxy. A medida que el tráfico fluye entre el cliente y el servidor, el cortafuegos comprueba si el tráfico SSH se enruta normalmente o si usa un túnel SSH (reenvío de puertos). El cortafuegos no realiza una inspección de amenazas y contenido en los túneles SSH; sin embargo, si el cortafuegos identifica túneles SSH, bloquea el tráfico de túnel SSH y restringe el tráfico conforme a las políticas de seguridad configuradas.

Perfil de descifrado del proxy SSH

El perfil de descifrado del proxy SSH (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **SSH Proxy [Proxy SSH]**) controla las comprobaciones de modo y de fallos de sesión para el tráfico SSH definido en las políticas de descifrado del proxy SSH a las cuales adjunta el perfil. La siguiente figura muestra las recomendaciones generales para la configuración del perfil de descifrado de proxy SSH, pero la configuración que use también depende de las reglas de cumplimiento de seguridad de su empresa y de las leyes y normativas locales.

© 2020 Palo Alto Networks, Inc.

El cortafuegos no realiza la inspección de contenido y amenazas en los túneles SSH (reenvío de puerto). Sin embargo, el cortafuegos distingue entre la aplicación SSH y la aplicación de túnel SSH. Si el cortafuegos identifica túneles SSH, bloquea el tráfico por el túnel SSH y restringe el tráfico conforme a las políticas de seguridad configuradas.



Comprobaciones de modo no admitidas. El cortafuegos admite SSHv2. Si no bloquea sesiones con modos no admitidos, los usuarios reciben un mensaje de advertencia si se conectan con servidores posiblemente inseguros y pueden hacer clic en ese mensaje e ingresar al sitio potencialmente peligroso. Bloquear estas sesiones lo protege de servidores que utilicen algoritmos y versiones de protocolo riesgosas y débiles:

1. **Bloquear sesiones con versiones no compatibles:** el cortafuegos tiene un conjunto de versiones admitidas predefinidas. Marque esta casilla para bloquear el tráfico con versiones débiles. Siempre marque esta casilla para bloquear sesiones con versiones de protocolo débiles para reducir la superficie de ataque.
2. **Bloquear sesiones con algoritmos no compatibles:** el cortafuegos tiene un conjunto de algoritmos admitidos predefinidos. Marque esta casilla para bloquear el tráfico con algoritmos débiles. Siempre marque esta casilla para bloquear sesiones con algoritmos no compatibles para reducir la superficie de ataque.

Comprobación de fallos:

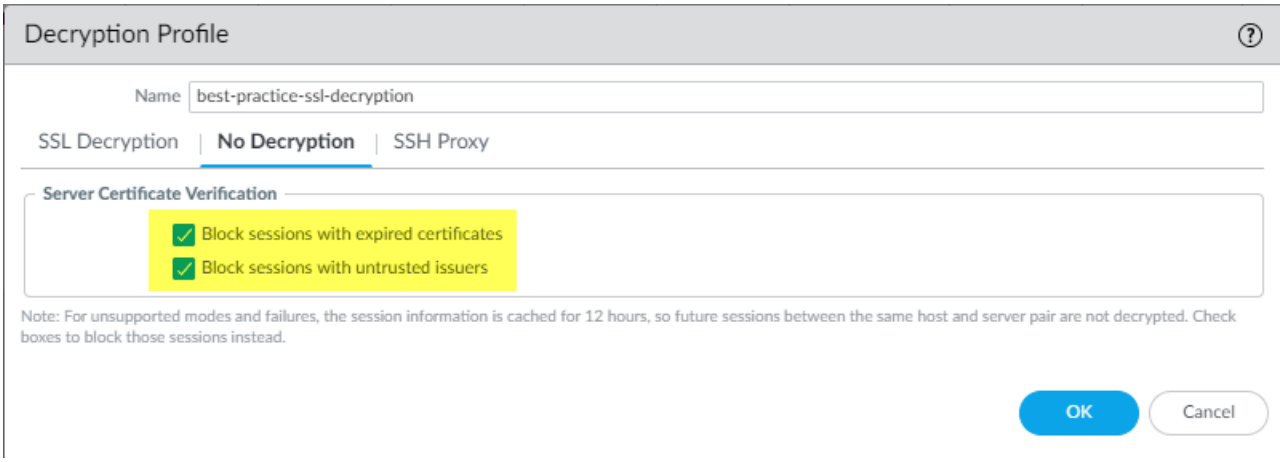
- **Bloquear sesiones al encontrar errores de SSH**: marque esta asilla para finalizar la sesión si se producen errores de SSH.
- **Bloquear sesiones si los recursos no están disponibles:** si no bloquea sesiones cuando los recursos de procesamiento del cortafuegos no están disponibles, el tráfico cifrado que desea descifrar ingresa a la red cifrado, lo que puede permitir conexiones potencialmente peligrosas. Sin embargo, bloquear sesiones cuando los recursos de procesamiento del cortafuegos no están disponibles puede afectar la experiencia del usuario porque los sitios a los que acceden los usuarios con normalidad, por el momento no están disponibles. Implementar o no las comprobaciones de fallas depende de la posición de cumplimiento de seguridad de su empresa y de la importancia que su empresa le dé a la experiencia de usuario, en comparación con una seguridad más estricta. De manera alternativa, considere usar modelos de cortafuegos con mayor potencia de procesamiento, de modo que pueda descifrar más tráfico.

Perfil para configuración sin cifrado

Los perfiles de configuración sin cifrado (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **No Decryption [Sin descifrado]**) realizan comprobaciones de verificación del servidor para el tráfico que elija

© 2020 Palo Alto Networks, Inc.

no descifrar. Adjunte un perfil de configuración sin cifrado a una política de descifrado que defina el tráfico que se excluirá del descifrado. (No utilice la política para excluir el tráfico que no pueda descifrar porque un sitio rompa el descifrado por motivos técnicos como un certificado fijado o una autenticación mutua. En cambio, añada el nombre de host a la Lista de exclusión de descifrado). La siguiente figura muestra las recomendaciones generales para la configuración del perfil de No descifrado, pero la configuración que use también depende de las reglas de cumplimiento de seguridad de su empresa y de las leyes y normativas locales.



- **Block sessions with expired certificates (Bloquear sesiones con certificados caducados)**: marque esta casilla para bloquear sesiones con servidores que contengan certificados caducados y evitar el acceso a sitios posiblemente inseguros. Si no marca esta casilla, los usuarios podrán conectarse y realizar transacciones con sitios potencialmente maliciosos y ver mensajes de advertencia cuando intenten conectarse, pero no se evitará la conexión.
- **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)**: marque esta casilla para bloquear sesiones con servidores que contengan emisores de certificados no confiables. Un emisor no confiable puede indicar ataques por desconocidos, ataques de reproducción o de otro tipo.

No adjunte un perfil de configuración sin cifrado a las políticas de descifrado para el tráfico TLSv1.3 que no descifre. A diferencia de las versiones anteriores, TLSv1.3 cifra la información del certificado, por lo que el cortafuegos no tiene visibilidad de los datos del certificado y, por lo tanto, no puede bloquear sesiones con certificados caducados o emisores que no sean de confianza, por lo que el perfil no tendrá ningún efecto. (El cortafuegos puede realizar comprobaciones de certificados con TLSv1.2 y versiones anteriores, ya que esos protocolos no cifran la información del certificado y debe aplicar un perfil de configuración sin cifrado a su tráfico). Sin embargo, debe crear una política de descifrado para el tráfico TLSv1.3 que no descifre porque el cortafuegos no registra el tráfico no cifrado a no ser que una política de descifrado controle ese tráfico.

(Se aplica a TLSv1.2 y versiones anteriores) Si elige permitir sesiones con emisores no fiables (no recomendado) y solo bloquear sesiones con certificados caducados, puede que la sesión con un emisor de confianza y caducado se bloquee inadvertidamente. Cuando el almacén de certificados del cortafuegos contiene una CA de confianza válida y autofirmada, y el servidor envía una CA caducada en la cadena de certificados, el cortafuegos no verifica su almacén de certificados. En cambio, el cortafuegos bloquea la sesión en función de la CA caducada cuando debería encontrar el delimitador alternativo, válido y de confianza, y permitir la sesión en base a ese certificado autofirmado de confianza.

Para evitar esto, además de activar Bloquear sesiones con certificados caducados, habilite Bloquear sesiones con emisores no fiables. Esto obliga al cortafuegos a verificar su almacén de certificados, buscar la CA de confianza autofirmada y permitir la sesión.

© 2020 Palo Alto Networks, Inc.

Descifrado SSL para certificados de criptografía de curva elíptica (ECC).

El cortafuegos descifra automáticamente tráfico SSL de los sitios web y las aplicaciones con certificados ECC, que incluye certificados de algoritmos de firma digital de curva elíptica (ECDSA). A medida que las organizaciones realizan la transición hacia el uso de los certificados de ECC para aprovechar las claves fuertes y el pequeño tamaño de los certificados, puede continuar conservando la visibilidad, y habilitar el tráfico de aplicaciones y sitios web con protección de ECC de manera segura.

El descifrado para sitios web y aplicaciones que utiliza certificados de ECC no admite tráfico que se refleja hacia el cortafuegos; el tráfico cifrado que utiliza certificados de ECC debe pasar mediante el cortafuegos directamente para que este lo descifre.

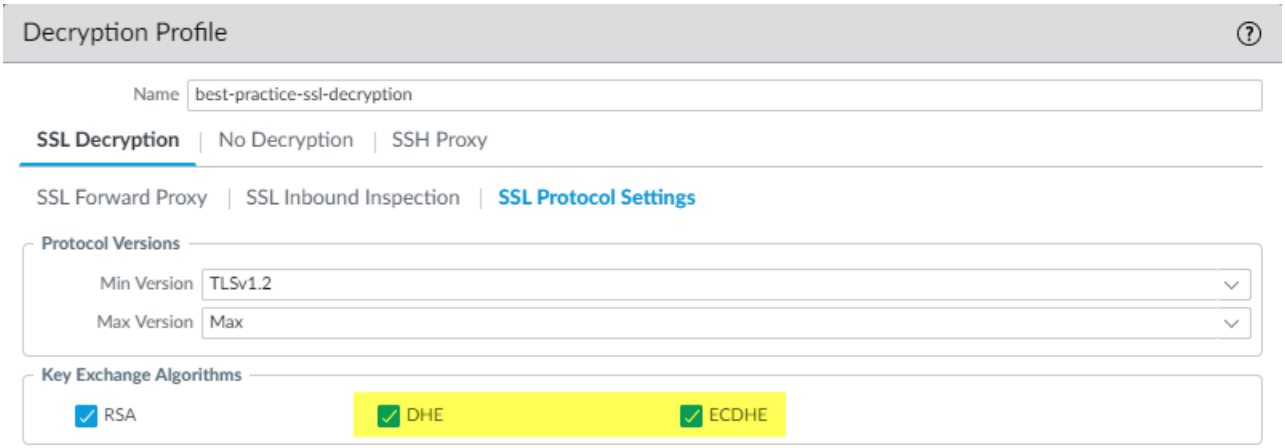
Puede utilizar un módulo de seguridad de hardware (HSM, Hardware Security Module) para almacenar las claves privadas asociadas a los certificados de ECDSA. Para el tráfico TLSv1.3, PAN-OS admite HSM solo para el proxy SSL de reenvío. No es compatible con HSM para la inspección de SSL entrante.

Compatibilidad del secreto perfecto y permanente (PFS) para el descifrado SSL

El PFS es un protocolo de comunicación segura que evita el peligro de que una sesión cifrada ponga en peligro a varias sesiones cifradas. Con PFS, un servidor genera claves privadas únicas para cada sesión segura que establece con un cliente. Si una clave privada de un servidor está en riesgo, solo la sesión establecida con esa clave es vulnerable; un atacante no puede recuperar datos de sesiones pasadas y futuras debido a que el servidor establece cada una de ellas en conexión con una clave generada única. El cortafuegos descifra sesiones SSL establecidas con algoritmos de intercambio de claves PFS, y conserva la protección de PFS para sesiones pasadas y futuras.

La compatibilidad para PFS basado en Diffie-Hellman (DHE) y PFS basado en Diffie-Hellman (ECDHE) de curva elíptica se habilita de forma predeterminada (**Objects [Objetos]** > **Decryption Profile [Perfil de descifrado]** > **SSL Decryption [Descifrado SSL]** > **SSL Protocol Settings [Configuración de protocolo SSL]**).

Si utiliza algoritmos de intercambio de claves DHE o ECDHE para permitir la Compatibilidad del PFS para el descifrado SSL, puede utilizar un Módulo de seguridad de hardware (hardware security module, HSM) para almacenar las claves privadas para la inspección entrante de SSL.

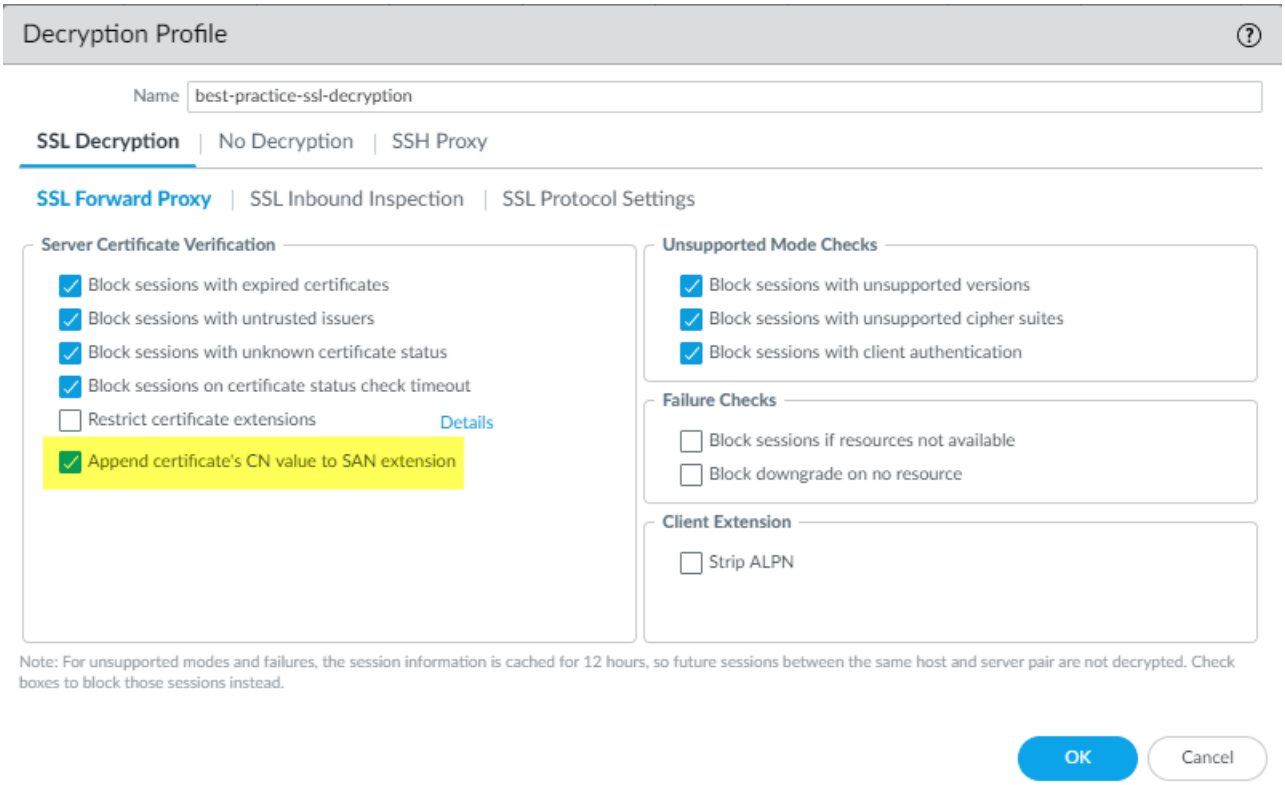


© 2020 Palo Alto Networks, Inc.

Descifrado SSL y nombres alternativos del asunto (SAN)

Algunos navegadores requieren que los certificados de servidor utilicen un nombre alternativo del asunto (Subject Alternative Name, SAN) para especificar los dominios que protege el certificado y ya no admitir coincidencias de certificados en función de un nombre común (common name, CN) de certificado de servidor. Los SAN permiten que un certificado de servidor proteja varios nombres; los CN se definen menos que los SAN y pueden proteger un dominio o todos los subdominios de primer nivel de un dominio. Sin embargo, si un certificado de servidor contiene únicamente un CN, los navegadores que requieren un SAN no permitirán que los usuarios finales se conecten a los recursos de web solicitados. El cortafuegos puede añadir un SAN al certificado de personificación que genera para establecerse como un agente externo fiable durante el descifrado SSL. Cuando un certificado de servidor únicamente contiene un CN, un cortafuegos que realiza el descifrado SSL copia el CN del certificado de servidor al SAN del certificado de personificación. El cortafuegos presenta el certificado de personificación con el SAN al cliente y el navegador puede admitir la conexión. Los usuarios finales pueden continuar accediendo a los recursos que necesitan y el cortafuegos puede descifrar las sesiones.

Para habilitar la compatibilidad del SAN con el tráfico SSL descifrado, actualice el perfil de descifrado adjunto a la política de descifrado relevante: seleccione **Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)** > **SSL Decryption (Descifrado SSL)** > **SSL Forward Proxy (Proxy SSL de reenvío)** > **Append Certificate's CN Value to SAN Extension (Adjuntar el valor de CN del certificado a la extensión SAN)**.



Descifrado TLSv1.3

Puede descifrar, obtener visibilidad completa y prevenir amenazas conocidas y desconocidas en el tráfico TLSv1.3. TLSv1.3 es la última versión del protocolo TLS, que proporciona mejoras de rendimiento y seguridad de las aplicaciones. Sus políticas de descifrado existentes funcionan con TLSv1.3 cuando configura el perfil de descifrado asociado para usar TLSv1.3 como la versión mínima del protocolo o para usar TLSv1.3 o Max como la versión máxima del protocolo. El cortafuegos admite el descifrado TLSv1.3

© 2020 Palo Alto Networks, Inc.

para el proxy de reenvío, la inspección de entrada, el agente de descifrado y la duplicación del puerto de descifrado.

Para utilizar TLSv1.3, el cliente y el servidor deben poder negociar cifrados TLSv1.3. Para los sitios web que no son compatibles con TLSv1.3, el cortafuegos selecciona una versión anterior del protocolo TLS compatible con el servidor.

El cortafuegos admite los siguientes algoritmos de descifrado para TLSv1.3:

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

Si el perfil de descifrado que aplica al tráfico descifrado especifica la **versión máxima** del protocolo como **Max (Máx.)**, el perfil es compatible con TLSv1.3 y usa automáticamente TLSv1.3 con sitios que admiten TLSv1.3. De lo contrario, para admitir TLSv1.3, configure la **versión máxima** en **Max (Máx.)**. Cuando actualice a PAN-OS 10.0, todos los perfiles de descifrado con la **versión máxima** establecida en **Max [Máx.]** se restablecen a **TLSv1.2** para proporcionar soporte automático para aplicaciones móviles que utilizan certificados anclados y evitan que el tráfico se descarte.

No todas las aplicaciones admiten el protocolo TLSv1.3. Siga las prácticas recomendadas de descifrado, configure la **versión mínima** del protocolo TLS en **TLSv1.2** y deje la **versión máxima** configurada como **Max (Máx.)**. Si las necesidades comerciales requieren permitir un protocolo TLS más débil, cree un perfil de descifrado SSL separado con una **versión mínima** que permita el protocolo más débil y adjúntelo a una política de descifrado que defina el tráfico que necesita permitir con el más débil.

Si su política de descifrado admite aplicaciones móviles (muchas de las cuales utilizan certificados fijados), configure **Max Version (Versión máx.)** en **TLSv1.2**. Puesto que TLSv1.3 cifra la información del certificado que no se cifró en versiones anteriores de TLS, el cortafuegos no puede añadir automáticamente exclusiones de descifrado basadas en la información del certificado, lo que afecta a algunas aplicaciones móviles. Por lo tanto, si habilita TLSv1.3, el cortafuegos puede eliminar parte del tráfico de aplicaciones móviles a no ser que cree una política de no descifrado para ese tráfico. Si conoce las aplicaciones móviles que usa para su empresa, considere la posibilidad de crear una política y un perfil de descifrado independientes para esas aplicaciones. De esa forma, podrá habilitar TLSv1.3 para el resto del tráfico.



No adjunte un perfil de configuración sin cifrado a las políticas de descifrado para el tráfico TLSv1.3 que no descifre. Un cambio con respecto a las versiones anteriores de TLS es que TLSv1.3 cifra la información del certificado, por lo que el cortafuegos ya no tiene visibilidad de esos datos y, por lo tanto, no puede bloquear sesiones con certificados caducados o emisores que no sean de confianza, por lo que el perfil no tiene ningún efecto. (El cortafuegos puede realizar comprobaciones de certificados con TLSv1.2 y versiones anteriores, ya que esos protocolos no cifran la información del certificado y debe aplicar un perfil de configuración sin cifrado a su tráfico). Sin embargo, debe crear una política de descifrado para el tráfico TLSv1.3 que no descifre porque el cortafuegos no registra el tráfico no cifrado a no ser que una política de descifrado controle ese tráfico.

Si se permiten modos no admitidos en Perfil de descifrado de la configuración de protocolo SSL, el cortafuegos añade automáticamente el tráfico a Caché de exclusión de descifrado local. El cortafuegos aún descifra e inspecciona el tráfico que se ha degradado de TLSv1.3 a TLSv1.2 y el **motivo** que se muestra en la caché para añadir el servidor a la caché es TLS13_UNSUPPORTED.

Si cambia de PAN-OS 10.0 a una versión anterior, cualquier perfil de descifrado que especifique TLSv1.3 como la **versión mínima** o la **versión máxima** cambia a la versión compatible más alta. Por ejemplo, la degradación de PAN-OS 10.0 a PAN-OS 9.1 reemplazaría TLSv1.3 por TLSv1.2. Si un dispositivo Panorama en PAN-OS 10.0 envía la configuración a dispositivos que ejecutan versiones anteriores de PAN-OS, cualquier perfil de descifrado que especifique TLSv1.3 como la **versión mínima** o la **versión máxima** también cambia a la versión compatible más alta.

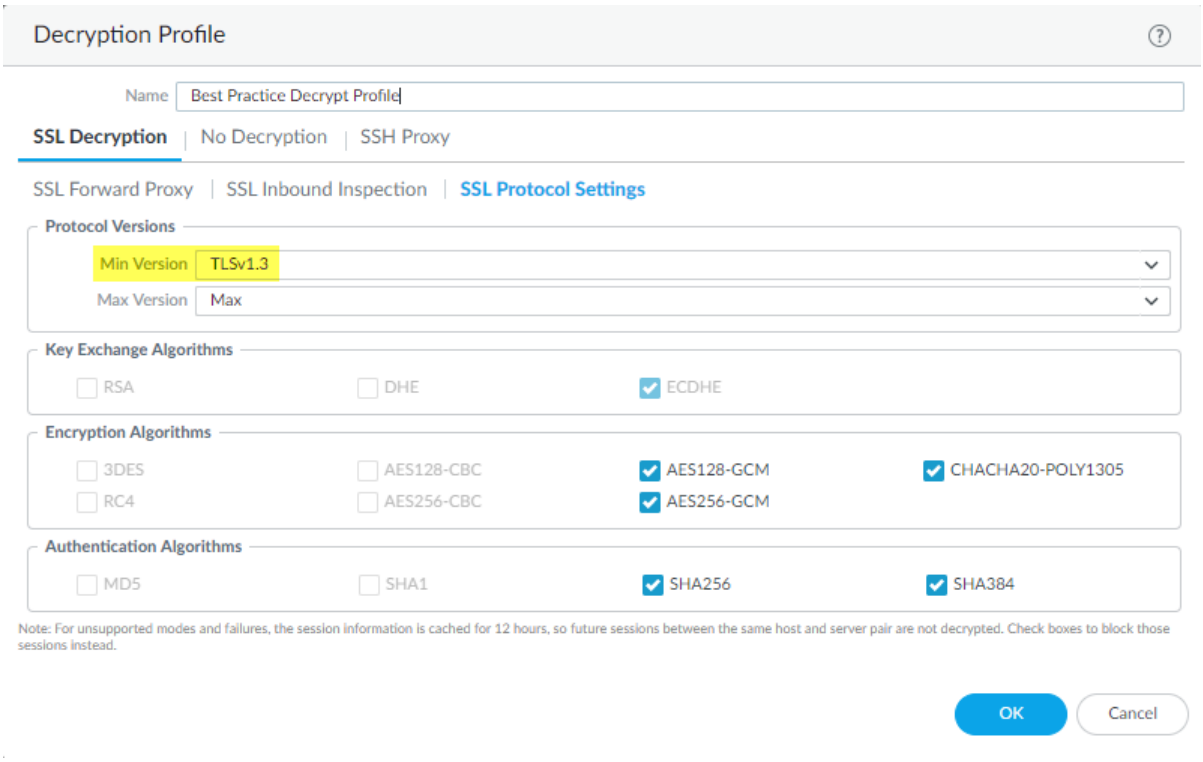
© 2020 Palo Alto Networks, Inc.

Para el tráfico TLSv1.3, PAN-OS admite módulos de seguridad de hardware (HSM, Hardware Security Module) solo para el proxy SSL de reenvío. No es compatible con HSM para la inspección de SSL entrante.

Puede configurar un perfil de descifrado SSL que establezca TLSv1.3 como la versión de protocolo mínima permitida para lograr la seguridad más estricta. Sin embargo, algunas aplicaciones no son compatibles con TLSv1.3 y es posible que no funcionen si TLSv1.3 es el protocolo mínimo permitido. Aplique un perfil que establezca TLSv1.3 como la versión mínima solo al tráfico de aplicaciones que solo admita TLSv1.3.

1. Cree un nuevo perfil de descifrado SSL o edite un perfil existente (**Objects [Objetos]** > **Decryption [Descifrado]** > **Decryption Profile [Perfil de descifrado]**).

   Si el perfil es nuevo, especifique un **nombre** de perfil.
2. Seleccione **SSL Protocol Settings (Configuración del protocolo SSL)**.
3. Cambie la **versión mínima** a **TLSv1.3**.



   El uso de **Max (Máx.)** para la **versión máxima** garantiza que el tráfico que controla el perfil puede utilizar la versión de protocolo más potente disponible. La **versión mínima** establece la versión más débil del protocolo que puede usar el tráfico. Establecer la versión mínima en **TLSv1.3** significa que el tráfico debe usar TLSv1.3 (o superior) y que las versiones de protocolo más débiles están bloqueadas. (La regla de política de descifrado define el tráfico que controla el perfil).

   Cuando configure TLSv1.3 como la **versión mínima**, deberá usar Perfect Forward Secrecy (Compatibilidad del secreto perfecto y permanente, PFS) y los algoritmos más débiles de intercambio de claves, cifrado y autenticación no estarán disponibles.
4. Configure cualquier otra configuración de perfil de descifrado que necesite establecer o cambiar.
5. Haga clic en **OK (Aceptar)** para guardar el perfil.
6. Adjunte el perfil a la regla de políticas de descifrado correspondiente para aplicarlo al tráfico adecuado.

© 2020 Palo Alto Networks, Inc.

Asistencia de alta disponibilidad para sesiones descifradas

El cortafuegos admite la sincronización de alta disponibilidad (HA, High Availability) solo para las sesiones SSL entrantes descifradas si las sesiones se establecieron utilizando algoritmos de intercambio de claves no PFS. El cortafuegos no admite la sincronización de HA para ningún otro tráfico descifrado. El cortafuegos descifra las nuevas sesiones que se inician después de la conmutación por error según la política de descifrado.

La siguiente tabla muestra la compatibilidad de sincronización de HA para sesiones descifradas después de una conmutación por error:

Tipo de sesión	Intercambio de claves PFS	Intercambio de claves que no son PFS
Sesión SSL entrante (descifrado de inspección entrante)	Sin sincronización de HA; el cortafuegos descarta la sesión.	Se produce la sincronización de HA; el cortafuegos permite la sesión pero no la descifra.
Sesiones SSL salientes (descifrado de proxy SSL de reenvío)	Sin sincronización de HA; el cortafuegos descarta la sesión.	Sin sincronización de HA; el cortafuegos descarta la sesión.

Reflejo de descifrado

El reflejo de descifrado permite crear una copia del tráfico descifrado desde un cortafuegos y enviarla a una herramienta de recopilación de tráfico, como NetWitness o Solera, que pueda recibir capturas de paquetes sin formato para su archivo o análisis. Aquellas organizaciones que necesitan la captura integral de datos con fines forenses o históricos o para prevenir la fuga de datos (Data Leak Prevention, DLP), pueden instalar una licencia gratuita para habilitar la función.

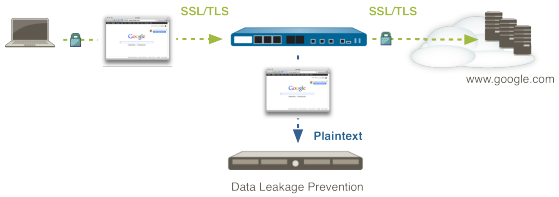
Después de instalar la licencia, conecte la herramienta de recopilación de tráfico directamente a una interfaz Ethernet en el cortafuegos y configure el **tipo de interfaz** en **Decrypt Mirror (Reflejo de descifrado)**. El cortafuegos simula un protocolo de enlace TCP con la herramienta de recopilación y, a continuación, envía cada paquete de datos (a través de esa interfaz) descifrado como texto sin formato.

El reflejo del puerto de descifrado no está disponible en la serie VM para las plataformas de nube pública (AWS, Azure, Google Cloud Platform) y VMware NSX.

Tenga en cuenta que el descifrado, almacenamiento, inspección y uso del tráfico SSL está legislado en algunos países y puede que sea necesario tener el consentimiento del usuario para poder usar la función de reflejo del de cifrado. Además, el uso de esta función podría hacer que usuarios maliciosos con accesos administrativos al cortafuegos recopilaran nombres de usuario, contraseñas, números de la seguridad social, números de tarjetas de crédito u otra información sensible para enviarla a través de un canal cifrado. Palo Alto Networks le recomienda consultar a su asesor corporativo antes de habilitar y utilizar esta función en un entorno de producción.

El siguiente gráfico muestra el proceso del reflejo del tráfico de descifrado y la sección Configuración del reflejo del puerto de descifrado describe como otorgar una licencia a esta función y habilitarla.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Preparación para implementar el descifrado

La tarea que lleva más tiempo en la implementación del descifrado no es la configuración de perfiles y políticas de descifrado, sino la preparación para la implementación. Para ello, se trabaja con las partes interesadas para decidir qué tráfico descifrar y cuál no, se informa a los usuarios sobre los cambios en el acceso al sitio web, se desarrolla una infraestructura de clave privada (private key infrastructure, PKI) y se planifica un despliegue por etapas y con prioridades.

Establezca los objetivos para el descifrado y revise la lista de comprobación recomendada para la planificación del descifrado para garantizar que comprende las prácticas recomendadas. El objetivo recomendado es descifrar tanto tráfico como así lo permitan los recursos del cortafuegos y descifrar primero el tráfico más importante.



Realice la migración desde las reglas de políticas de seguridad basadas en puertos hasta las basadas en la aplicación antes de crear e implementar reglas de política de descifrado. Si crea reglas de descifrado sobre la base de una política de seguridad basada en puertos y, luego, realiza la migración a la política de seguridad basada en la aplicación, el cambio podría provocar que las reglas de descifrado bloqueen el tráfico que intenta permitir. Esto se debe a que las reglas de política de seguridad probablemente usen puertos predeterminados de la aplicación para evitar que el tráfico de la aplicación use puertos no estándar. Por ejemplo, el tráfico identificado como tráfico de la aplicación de navegación web (puerto predeterminado 80) puede incluir aplicaciones subyacentes que tengan diferentes puertos predeterminados, como tráfico HTTPS (puerto predeterminado 443). La regla predeterminada de la aplicación bloquea el tráfico HTTPS porque observa el tráfico descifrado con un puerto "no estándar" (443 en lugar de 80). Realizar la migración a reglas basadas en App-ID antes de implementar el descifrado significa que cuando pruebe la implementación del descifrado en las POC, descubrirá errores de configuración de la política de seguridad y deberá repararlos antes de realizar la implementación con la población general de usuarios.

Para prepararse para implementar el descifrado, utilice lo siguiente:

- Trabajo con las partes interesadas para desarrollar una estrategia de implementación de descifrado.
- Desarrollo de un plan de implementación de PKI
- Medición de la implementación de descifrado de cortafuegos
- Planificación de una implementación en etapas con prioridad

Trabajo con las partes interesadas para desarrollar una estrategia de implementación de descifrado.

Trabaje con las partes interesadas como los miembros del departamento legal, el de recursos humanos, el ejecutivo, el de seguridad y el de TI/soporte técnico para desarrollar una estrategia de implementación de descifrado. Comience por obtener las aprobaciones necesarias para descifrar tráfico y proteger la empresa. Descifrar el tráfico implica comprender cómo las normativas legales y las necesidades de la empresa afectan a lo que puede y no puede descifrar.

Identifique y priorice el tráfico que desea descifrar. Lo mejor es descifrar tanto tráfico como pueda para obtener visibilidad de las amenazas potenciales en el tráfico cifrado para evitarlas. Si el incorrecto tamaño del cortafuegos evita que descifre todo el tráfico que desea, priorice los servidores más importantes, las categorías de tráfico con mayor riesgo y los segmentos y subredes de IP menos fiables. Para ayudar a priorizar las tareas, pregúntese "¿qué sucede si este servicio se ve comprometido?" y "¿cuánto estoy dispuesto a arriesgar en relación con el nivel de rendimiento que deseo lograr?".

© 2020 Palo Alto Networks, Inc.

A continuación, identifique el tráfico que no puede descifrar porque el tráfico interrumpe el descifrado por motivos técnicos, como certificados fijados, cadenas de certificados incompletas, cifrados no compatibles o la autenticación mutua. Al descifrar sitios que interrumpen esta operación, la consecuencia técnica es el bloqueo del tráfico afectado. Evalúe los sitios web que interrumpen el descifrado desde el punto de vista técnico y pregúntese si necesita acceder a esos sitios por motivos comerciales. Si no necesita acceder a estos sitios, permita que el descifrado los bloquee. Si necesita acceder a cualquiera de estos sitios por motivos comerciales, añádalos a la lista de exclusión de descifrado SSL para excluirlos del descifrado. La lista de exclusión de descifrado SSL es exclusivamente para los sitios que interrumpen el descifrado de manera técnica.

Identifique el tráfico confidencial que *decide* no descifrar por motivos legales, normativos, personales o de otro tipo, como el tráfico financiero, médico u oficial o el tráfico de determinados ejecutivos. Este no es tráfico que interrumpe el descifrado de manera técnica, por lo que no use la lista de exclusión de descifrado SSL para excluir este tráfico del descifrado. En cambio, cree una exclusión de descifrado basada en una política para identificar y controlar el tráfico que decide no descifrar y aplique el perfil de No descifrado a la política para evitar que los servicios con problemas de certificados accedan a la red. Las exclusiones de descifrado basadas en políticas solo son para el tráfico que decide no descifrar.

Cuando planifique una política de descifrado, considere las reglas de cumplimiento de seguridad de la empresa, la política de uso del ordenador y sus objetivos comerciales. Los controles extremadamente estrictos pueden afectar a la experiencia del usuario cuando impiden que acceda a sitios no comerciales a los que el usuario suele acceder, pero podría ser necesario para instituciones gubernamentales o financieras. Existe siempre un punto intermedio entre la capacidad de uso, los costes de gestión y la seguridad. Cuánto más estricta sea la política de descifrado, mayor será la probabilidad de que no se pueda acceder a un sitio web, lo que puede generar reclamaciones por parte del usuario y posiblemente modificar la base de las reglas.



Aunque una política de descifrado estricta puede inicialmente generar algunas reclamaciones por parte de los usuarios, estos pueden llamar su atención hacia sitios web no sancionados o no deseados que están bloqueados porque usan algoritmos débiles o tienen problemas con los certificados. Use las reclamaciones como una herramienta para comprender mejor el tráfico de su red.

Los diferentes grupos de usuarios e incluso los usuarios individuales pueden requerir políticas de descifrado distintas o puede aplicar la misma política de descifrado a todos los usuarios. Por ejemplo, los ejecutivos podrían excluirse de las políticas de descifrado que se apliquen a otros empleados. Y es posible que deba aplicar diferentes políticas de descifrado a los grupos de empleados, contratistas, socios e invitados. Prepare políticas de uso de ordenador del departamento legal y de recursos humanos para distribuir a todos los empleados, contratistas, socios, invitados y los demás usuarios de red de manera que cuando implemente el descifrado, los usuarios comprendan que sus datos pueden descifrarse y analizarse en busca de amenazas.



La forma en que administra los usuarios invitados depende del acceso que estos requieran. Aísle a los invitados del resto de su red colocándolos en una VLAN diferente y en un SSID separado para el acceso inalámbrico. Si los invitados no necesitan acceder a su red corporativa, no permita que lo hagan y no habrá necesidad de descifrar su tráfico. Si los invitados necesitan acceder a su red corporativa, descifre su tráfico:

- *Las empresas no controlan los dispositivos invitados. Descifre el tráfico de invitado y sométalo a su política de seguridad de invitado de modo que el cortafuegos pueda inspeccionar el tráfico y evitar amenazas. Para hacerlo, redirija a los usuarios invitados por un portal de autenticación, indíqueles cómo descargar e instalar el certificado de CA y notifíqueles claramente que su tráfico se descifrará. Incluya el proceso en la política de uso de ordenadores y privacidad de su empresa.*
- *Cree reglas de política de descifrado y reglas de política de seguridad diferentes para controlar de manera estricta el acceso de invitados, de modo que estos solo puedan acceder a las áreas de su red que necesitan.*

© 2020 Palo Alto Networks, Inc.

De manera similar a los diferentes grupos de usuarios, decida qué dispositivos y aplicaciones debe descifrar. Las redes actuales no solo admiten dispositivos corporativos, sino también dispositivos móviles personales (bring your own device, BYOD), con usuario remoto y de otros tipos, incluidos los dispositivos de contratistas, socios e invitados. Los usuarios actuales intentan acceder a muchos sitios, tanto sancionados como no sancionados, y debe decidir la cantidad de este tráfico que desea descifrar.



Las empresas no controlan los dispositivos BYOD. Si permite dispositivos BYOD en su red, descifre su tráfico y sométalo a la misma política de seguridad que aplica en otro tráfico de red, de modo que el cortafuegos pueda inspeccionar el tráfico y evitar las amenazas. Para hacerlo, redirija a los usuarios de BYOD por un portal cautivo, indíqueles cómo descargar e instalar el certificado de CA y notifíqueles claramente que su tráfico se descifrará. Informe a los usuarios de BYOD sobre el proceso e inclúyalo en la política de uso del ordenador y privacidad de su empresa.

Decida qué tráfico desea registrar e investigue el tráfico que puede registrar. Tenga en cuenta las leyes locales relacionadas con los tipos de datos que puede registrar y almacenar, y dónde puede hacerlo. Por ejemplo, las leyes locales podrían evitar el registro y almacenamiento de logs con información personal, como datos financieros y de salud.

Decida cómo administrar los certificados incorrectos. Por ejemplo, ¿bloqueará o permitirá sesiones en las que el estado del certificado es desconocido? Comprender cómo desea administrar los certificados incorrectos determina cómo configurar los perfiles de descifrado que adjunta a las políticas de descifrado para controlar qué sesiones permitir sobre la base del estado de verificación del certificado.

Desarrollo de un plan de implementación de PKI

Planifique cómo implementar su infraestructura de clave pública (public key infrastructure, PKI). Los dispositivos de red necesitan un certificado de CA confiable de reenvío SSL para sitios de confianza y un certificado de CA no confiable de reenvío de SSL para los sitios no confiables. Genere diferentes certificados confiables y no confiables de reenvío (no firme el certificado no confiable de reenvío con la CA raíz de empresa porque este certificado debe advertir a los usuarios que están intentando acceder a sitios posiblemente no seguros). Los cortafuegos de próxima generación de Palo Alto Networks cuentan con dos métodos para generar certificados de CA para el descifrado SSL:

- **Genere los certificados CA SSL desde la CA raíz de empresa como certificados subordinados:** si tiene una PKI de empresa existente, esta es la mejor práctica. Generar un certificado subordinado desde su CA raíz de empresa facilita la implementación porque los dispositivos de red ya confían en la CA raíz de empresa, de modo que evita cualquier problema con los certificados cuando comienza la fase de implementación. Si no tiene una CA raíz de empresa, considere obtener una.
- **Genere un certificado de CA raíz autofirmado en el cortafuegos y cree certificados de CA subordinados en ese cortafuegos:** si no tiene una CA raíz de empresa, este método brinda un certificado de CA raíz autofirmado y los certificados de CA no confiables y confiables de reenvío subordinados. Con este método, debe instalar los certificados autofirmados en todos los dispositivos de su red de modo que estos reconozcan los certificados autofirmados del cortafuegos. Debido a que los certificados deben implementarse en todos los dispositivos, este método es mejor para las pruebas de concepto (proof of concept, POC) y las implementaciones pequeñas que para las grandes.



No exporte el certificado de reenvío no confiable a las Listas de certificados confiables de sus dispositivos de red. Esto es crítico porque si instala el certificado no confiable en la lista de certificados confiables, los dispositivos confiarán en los sitios web que el cortafuegos no confía. Además, los usuarios no verán las advertencias de certificación de sitios no confiables, por lo que no sabrán si los sitios no son confiables y podrán acceder a ellos, lo que expone su red a amenazas.

© 2020 Palo Alto Networks, Inc.

Independientemente de si genera certificados de reenvío confiables de su CA raíz de la empresa o usa un certificado autofirmado generado en el cortafuegos, genere otro certificado de CA confiable de reenvío subordinado para cada cortafuegos. La flexibilidad de usar diferentes CA subordinadas le permite revocar un certificado cuando retira un dispositivo (o par de dispositivos) sin afectar el resto de la implementación y reduce el impacto en cualquier situación en la que necesite revocar un certificado. Usar diferentes certificados de CA confiables de reenvío en cada cortafuegos ayuda a solucionar problemas, ya que el mensaje de error de CA que el usuario ve incluye información sobre el cortafuegos que atraviesa el tráfico. Si usa la misma CA confiable de reenvío en cada cortafuegos, pierde el nivel de detalle de esa información.

No existen beneficios de usar diferentes certificados no confiables de reenvío en distintos cortafuegos, de modo que puede usar el mismo certificado no confiable de reenvío en todos los cortafuegos. Si necesita mayor seguridad para sus claves privadas, considere almacenarlas en un HSM.

Es posible que deba realizar adaptaciones especiales para los usuarios invitado. Si los usuarios invitados no deben acceder a su red corporativa, no les permita el acceso; así no tiene que descifrar su tráfico ni crear una infraestructura que lo respalde. Si es preciso admitir invitados, consulte con el departamento jurídico si se puede descifrar su tráfico.

Si puede descifrar el tráfico de los invitados, otórgueles el mismo trato que a los dispositivos personales (bring your own device, BYOD). Al descifrar el tráfico de los invitados, sométalo a la misma política de seguridad que aplica al resto del tráfico de la red. Para hacerlo, redirija a los usuarios invitados por un portal de autenticación, indíqueles cómo descargar e instalar el certificado de la CA y notifíqueles con claridad que se va a descifrar su tráfico. Incluya el proceso en la política de uso de ordenadores y privacidad de su empresa. Asimismo, restrinja el tráfico de los invitados a las zonas a las que deben acceder.

Si no puede descifrar el tráfico de los invitados por motivos legales, aíslelo e impida el desplazamiento lateral por la red:

- Cree una zona independiente para los invitados y restrinja su acceso a ella. Para impedir el desplazamiento lateral, vede el acceso de los invitados a las demás zonas.
- Permita solo aplicaciones aprobadas, use el filtrado de URL para impedir el acceso a categorías de URL peligrosas y aplique los perfiles de seguridad recomendados.
- Aplique un perfil y una política que impidan el descifrado para evitar que los invitados accedan a sitios web con CA desconocidas o vencidas.

Todos los empleados, contratistas, socios y demás usuarios deben utilizar la infraestructura corporativa normal, y su tráfico se debe descifrar e inspeccionar.

Medición de la implementación de descifrado de cortafuegos

Descifrar el tráfico cifrado consume recursos de CPU del cortafuegos y puede afectar al rendimiento. En general, cuanto más estricta es la seguridad (más tráfico SSL para descifrar combinado con una configuración de protocolo más exigente), más recursos del cortafuegos consume el descifrado. Trabaje con SE/CE de Palo Alto Networks para medir el tamaño de la implementación del cortafuegos y evitar problemas de capacidad. Los factores que afectan el consumo de recursos de descifrado y, por lo tanto, a la cantidad de tráfico que el cortafuegos puede descifrar incluyen:

- La cantidad de tráfico SSL que desea descifrar. Esto varía de red en red. Por ejemplo, algunas aplicaciones deben descifrarse para evitar la entrada de malware y exploits en la red o la transferencia de datos no autorizada, algunas aplicaciones no pueden descifrarse debido a leyes y normativas locales o por motivos comerciales, y otras están sin cifrar y no necesitan descifrarse. Cuanto más tráfico desea descifrar, más recursos necesitará.
- La versión del protocolo de TLS. Las versiones posteriores son más seguras pero consumen más recursos. Use la versión del protocolo de TLS más nueva posible para maximizar la seguridad.

© 2020 Palo Alto Networks, Inc.

- El tamaño de la clave. Cuanto más grande es el tamaño de la clave, mejor es la seguridad, pero también más recursos consume el procesamiento de clave.
- El algoritmo de intercambio de clave. Los algoritmos de intercambio de claves efímeros de Confidencialidad directa total (Perfect Forward Secrecy, PFS), como Diffie-Hellman Ephemeral (DHE) y Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consumen más recursos de procesamiento que los algoritmos Rivest-Shamir-Adleman (RSA). Los algoritmos de intercambio de claves de PFS proporcionan mayor seguridad que los de RSA porque el cortafuegos debe generar una nueva clave de cifrado para cada sesión, pero generar la clave nueva consume más recursos del cortafuegos. Sin embargo, si un atacante pone en riesgo una clave de sesión, PFS evita que este la use para descifrar otras sesiones entre el mismo cliente y servidor, y RSA no lo hace.
- El algoritmo de descifrado. El algoritmo de intercambio de claves determina si el algoritmo de descifrado es PFS o RSA.
- El método de autenticación del certificado. RSA (no el algoritmo de intercambio de claves de RSA) consume menos recursos que el Algoritmo de firma digital de curva elíptica (Elliptic Curve Digital Signature Algorithm, ECDSA) pero ECDSA es más seguro.



La combinación del algoritmo de intercambio de claves y el método de autenticación de certificados afectan al rendimiento como se muestra en las pruebas de referencia *de RSA y ECDSA. El coste de rendimiento de PFS compensa la mayor seguridad que logra PFS, pero es posible que PFS no sea necesario para todos los tipos de tráfico. Puede ahorrar en ciclos de CPU del cortafuegos mediante el uso de RSA para el tráfico que desea descifrar e inspeccionar en busca de amenazas, pero no tiene mucho sentido.*

- Los tamaños de transacciones promedio. Por ejemplo, los tamaños pequeños de transacciones promedio consumen más potencia de procesamiento para descifrarlos. Mida el tamaño de la transacción promedio de todo el tráfico, luego mida el tamaño de la transacción promedio del tráfico en el puerto 443 (puerto predeterminado para el tráfico cifrado de HTTPS) para saber la proporción del tráfico cifrado que se dirige al cortafuegos en relación con el tráfico total y los tamaños de transacción promedio. Elimine los valores atípicos como las transacciones inusualmente grandes para obtener una medición auténtica del tamaño de la transacción promedio.
- El modelo y los recursos del cortafuegos. Los modelos de cortafuegos más nuevos tienen más potencia de procesamiento que los anteriores.

La combinación de estos factores determina cómo el descifrado consume recursos de procesamiento del cortafuegos. Para utilizar mejor los recursos del cortafuegos, debe conocer los riesgos de los datos que protege. Si los recursos del cortafuegos son un problema, use un descifrado más sólido para el tráfico de mayor prioridad y use un descifrado que consuma menos procesamiento para descifrar e inspeccionar el tráfico de menor prioridad hasta que pueda aumentar los recursos disponibles. Por ejemplo, puede usar RSA en lugar de ECDHE y ECDSA para el tráfico que no sea confidencial o de alta prioridad para así conservar los recursos del cortafuegos y usar el descifrado basado en PFS para tráfico confidencial de mayor prioridad. (De todas maneras, está realizando el descifrado y la inspección del tráfico de menor prioridad, pero compensa el menor consumo de recursos de procesamiento con el uso de algoritmos que no son tan seguros como PFS). La clave es saber los riesgos de los diferentes tipos de tráfico y administrarlos en consecuencia.

Mida el rendimiento del cortafuegos de modo que sepa los recursos que actualmente están disponibles, lo que le ayudará a saber si necesita más recursos de cortafuegos para descifrar el tráfico que desea. Medir el rendimiento del cortafuegos también establece una línea de base para las comparaciones de rendimiento tras implementar el descifrado.

Cuando mida el tamaño de la implementación del cortafuegos, tome como base no solo sus necesidades actuales, sino también las futuras. Incluya margen para el crecimiento del tráfico de descifrado porque Gartner prevee que para el 2019, más del 80 por ciento del tráfico web de las empresas estará cifrado y más del 50 por ciento de las nuevas campañas de malware usarán diferentes formas de cifrado. Colabore con los representantes de Palo Alto Networks y aproveche su experiencia en la dimensión de los cortafuegos para ayudarle a medir la implementación del descifrado del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Planificación de una implementación en etapas con prioridad

Planifique la implementación de descifrado de una manera controlada, parte por parte. No realice una implementación completa del descifrado de una sola vez. Lleve a cabo pruebas y asegúrese de que el descifrado funcione según lo planeado y que los usuarios comprendan qué hace y por qué. La implementación del descifrado de esta manera facilita la resolución de problemas si algo no funciona según lo esperado y ayuda a los usuarios a adaptarse a los cambios.

Informar a las partes interesadas, empleados y otros usuarios como contratistas y socios es una parte fundamental, ya que la configuración del descifrado puede cambiar su capacidad de acceder a algunos sitios web. Los usuarios deben comprender cómo responder ante situaciones en las que no pueden acceder a un sitio web que antes sí estaba disponible y qué información deben proporcionarle al soporte técnico. Los miembros del soporte técnico deben comprender qué se implementa y cuándo, y cómo ayudar a los usuarios cuando tienen un problema. Antes de implementar el descifrado a la población general:

- Identifique a los primeros usuarios que respaldarán el descifrado y que puedan ayudar a otros empleados que tengan preguntas durante la implementación completa. Reclute la ayuda de los gerentes de departamento y ayúdelos a comprender los beneficios del descifrado del tráfico.
- Configure pruebas de concepto (proof of concept, POC) en cada departamento con los primeros usuarios y otros empleados que comprendan por qué es importante el descifrado del tráfico. Informe a los participantes de la POC sobre los cambios y cómo comunicarse con el soporte técnico si tienen problemas. De esta forma, las POC de descifrado se convierten en una oportunidad para trabajar con el soporte técnico para realizar POC sobre cómo respaldar el descifrado y desarrollar el método más sencillo para adoptar la implementación general. La interacción entre los usuarios de POC y el soporte técnico también le permite ajustar políticas y la forma en que se comunica con los usuarios.

  Las POC le permiten experimentar con la priorización de qué descifrar primero, de modo que cuando introduzca por etapas el descifrado a la población general, su experiencia en las POC le ayude a comprender cómo introducir progresivamente el descifrado de diferentes categorías de URL. Determine la forma en que el descifrado afecta las CPU del cortafuegos y el uso de la memoria para ayudarle a comprender si el tamaño del cortafuegos es correcto o si necesita una actualización. Las POC también pueden revelar aplicaciones que interrumpen el descifrado por motivos técnicos (pues el descifrado bloquea su tráfico), que se deben añadir a la lista de exclusión de descifrado.

  Cuando configure las POC, configure también un grupo de usuarios que pueda certificar la preparación operativa y los procedimientos previos a la implementación general.
- Informe a los usuarios antes de la implementación general y planifique la información para los nuevos usuarios a medida que se unen a la empresa. Esta es una fase esencial de la implementación del descifrado ya que esta pueda afectar los sitios web que los usuarios antes visitaban pero que no eran seguros, y que ya no están disponibles. La experiencia de POC ayuda a identificar los puntos más importantes que debe comunicar.
- Introduzca progresivamente el descifrado. Puede lograrlo de varias maneras. Puede descifrar primero el tráfico con mayor prioridad (por ejemplo, las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos) y luego, descifre más a medida que gane experiencia. Como alternativa, puede adoptar un enfoque más conservador y descifrar primero las categorías de URL que no afecten a su empresa (entonces, si algo no funciona, no se producirán problemas que afecten a la empresa), por ejemplo, las fuentes de noticias. En todos los casos, la mejor manera de introducir progresivamente el descifrado es descifrar algunas categorías de URL, tener en cuenta los comentarios del usuario, ejecutar informes para garantizar que el descifrado funcione según lo esperado y, luego, descifrar de manera gradual algunas categorías de URL más y verificar, y así sucesivamente. Planifique realizar exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo.

  Si permite que los usuarios opten por excluir el descifrado SSL (los usuarios ven una página de respuesta que les permite optar por excluir el descifrado y finalizar la sesión sin visitar el sitio o entrar en el sitio y aceptar que el tráfico se descifre), infórmeles sobre lo que es, por qué lo ven y cuáles son sus opciones.

© 2020 Palo Alto Networks, Inc.

- Cree programas de implementación realistas que le den tiempo para evaluar cada etapa de la implementación.



Coloque cortafuegos en posiciones en las que puedan ver todo el tráfico de red, de modo que el tráfico cifrado no obtenga acceso a su red porque se omite el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Definición del tráfico para descifrar

Una regla de política de descifrado le permite definir tráfico que desea que el cortafuegos descifre y tráfico que decide excluir del descifrado porque es personal o debido a normativas locales.

Adjunte un perfil de descifrado a cada regla de política de descifrado para habilitar comprobaciones de certificados, comprobaciones de modo de sesión, comprobaciones de fallos y comprobaciones de algoritmos y protocolos, en función del perfil. Estas comprobaciones evitan las conexiones arriesgadas, como sesiones con emisores de certificados no confiables, protocolos, cifrados y algoritmos débiles, y servidores que presentan problemas con los certificados.

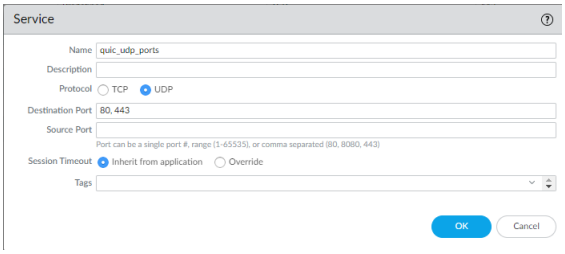
Revise la lista de comprobación recomendada para la planificación de la implementación del descifrado para garantizar que comprende las prácticas recomendadas.

Bloquee el acceso a todas las categorías de filtrado de URL peligrosas conocidas, como malware, phishing, DNS dinámico, desconocidas, de comando y control, extremistas, de infracción de derechos de autor, de anonimización y anulación de proxy, de dominio recién registrado, grayware y estacionadas. Si debe permitir alguna de estas categorías por motivos comerciales, descífrelas y aplique perfiles de seguridad estrictos en el tráfico.

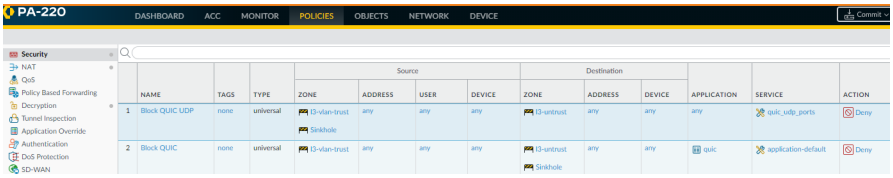
Las categorías de URL que siempre debe descifrar si las permite incluyen: almacenamiento y copia de seguridad en línea, correo electrónico basado en la Web, hosting web, sitios y blogs personales, y redes de entrega de contenido.

En la política de seguridad, bloquee el protocolo de Conexiones UDP rápidas en Internet (Quick UDP Internet Connections, QUIC) salvo que por motivos comerciales deba permitir el tráfico del explorador cifrado. Chrome y algunos otros exploradores establecen sesiones con QUIC en lugar de TLS, pero QUIC usa cifrado de propiedad que el cortafuegos no puede descifrar, por lo que tráfico potencialmente peligroso puede entrar en la red como tráfico cifrado. Bloquear QUIC obliga al explorador a volver a TLS y permite que el cortafuegos descifre el tráfico.

Cree una regla de políticas de seguridad para bloquear QUIC en sus puertos de servicio UDP (80 y 443) y cree una regla independiente para bloquear la aplicación QUIC. Para la regla que bloquea los puertos UDP 80 y 443, cree un servicio (Objects (Objetos) > Services (Servicios)) que incluya los puertos UDP 80 y 443:



Utilice el servicio para especificar los puertos UDP que se bloquearán para QUIC. En la segunda regla, bloquee la aplicación QUIC:



© 2020 Palo Alto Networks, Inc.

- Creación de un perfil de descifrado
- Creación de una regla de política de descifrado

Creación de un perfil de descifrado

Un perfil de descifrado le permite realizar comprobaciones en el tráfico descifrado y el tráfico SSL que *decide* excluir del descifrado. (Si un servidor interrumpe el descifrado SSL desde el punto de vista técnico debido a la fijación del certificado u otros motivos, añada el servidor a la lista de exclusión de descifrado). En función de sus necesidades, cree perfiles de descifrado para realizar lo siguiente:

- Bloquee sesiones sobre la base del estado del certificado, entre lo que se incluye bloquear sesiones con certificados caducados, emisores no confiables, estados de certificados desconocidos, tiempos de espera de comprobación de estados de certificados y extensiones de certificados.
- Bloquee sesiones con versiones y conjuntos de cifrados no compatibles, y que requieren el uso de la autenticación de cliente.
- Bloquear sesiones si los recursos para realizar el descifrado no están disponibles o si un módulo de seguridad de hardware no está disponible para firmar certificados.
- Defina las versiones de protocolo e intercambio de claves, cifrado y algoritmos de autenticación permitidos para el tráfico de inspección de entrada SSL y proxy SSL de reenvío en la configuración del protocolo SSL.

No debilite el perfil de descifrado principal que se aplica a la mayoría de los sitios para adaptarse a sitios más débiles. En cambio, cree uno o más perfiles de descifrado diferentes para los sitios que debe respaldar pero que no admiten algoritmos y cifrados sólidos. Además, puede crear perfiles de descifrado diferentes para distintas categorías de URL para ajustar la seguridad frente al rendimiento del tráfico que contiene material no confidencial. Sin embargo, siempre debe descifrar e inspeccionar todo el tráfico que pueda.

Después de crear un perfil de descifrado, adjúntelo a una regla de la política de descifrado; entonces, el cortafuegos aplicará la configuración del perfil de descifrado al tráfico que coincida con la regla de la política de descifrado.

Los cortafuegos de Palo Alto Networks incluyen un perfil de descifrado por defecto que puede usar para aplicar las versiones del protocolo recomendado básico y los conjuntos de cifras para el tráfico descifrado. Sin embargo, se recomienda habilitar controles de descifrado más estrictos, como se describe en Perfil de descifrado del proxy SSL de reenvío, Perfil de descifrado de inspección de entrada SSL y Perfil de descifrado de la configuración de protocolo SSL.



Evite admitir protocolos o algoritmos débiles porque contienen vulnerabilidades conocidas que los atacantes pueden aprovechar. Si debe permitir un protocolo o algoritmo más débil para admitir un socio o contratista clave que usa sistemas heredados con protocolos débiles, cree un perfil de descifrado diferente para la excepción y adjúntelo a una regla de política de descifrado que se aplique al perfil solo en el tráfico relevante (por ejemplo, la dirección IP de origen del socio). No permita el protocolo débil en todo el tráfico.

STEP 1 | Crear un nuevo perfil de descifrado.

Seleccione **Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)**, haga clic en **Add (Añadir)** para añadir una regla de perfil de descifrado o modifíquela, y asigne a la regla un nombre descriptivo en **Name (Nombre)**.

STEP 2 | (Opcional) Permita que la regla del perfil sea de **Shared (Uso compartido)** en cada sistema virtual de un cortafuegos o cada grupo de dispositivos de Panorama.

© 2020 Palo Alto Networks, Inc.

STEP 3 | (Reflejo de descifrado únicamente) Habilite una interfaz Ethernet que el cortafuegos pueda utilizar para copiar y reenviar el tráfico descifrado.

Independientemente de esta tarea, siga los pasos para realizar la Configuración del reflejo del puerto de descifrado. Tenga en cuenta las normativas de privacidad locales que puedan prohibir el reflejo o el control del tipo de tráfico que puede reflejar. El reflejo del puerto de descifrado requiere una licencia de reflejo del puerto de descifrado.

STEP 4 | (Opcional) Bloquee y controle el tráfico entrante o de túnel de SSL:



A pesar de que aplicar un perfil de descifrado para descifrar tráfico es opcional, lo mejor siempre es aplicar un perfil de descifrado a las reglas de política para proteger su red de amenazas cifradas. No puede protegerse de las amenazas si no puede verlas.

Seleccione **SSL Decryption**:

- Seleccione **SSL Forward Proxy (Proxy SSL de reenvío)** para configurar los ajustes para verificar los certificados, aplicar versiones del protocolo y conjuntos de cifrados, y realizar comprobaciones de fallos en el tráfico descifrado SSL. Estos ajustes están activos únicamente cuando este perfil se adjunta a una regla de política de descifrado que está configurada para realizar el descifrado proxy de reenvío SSL.
- Seleccione **SSL Inbound Inspection (Inspección de SSL entrante)** para configurar los ajustes para aplicar las versiones de protocolo y los conjuntos de cifrado, y realizar comprobaciones de fallos en el tráfico de entrada de SSL. Estos ajustes están activos únicamente cuando este perfil se adjunta a una regla de política de descifrado que lleva a cabo la inspección de entrada de SSL.
- Seleccione **SSL Protocol Settings (Configuración del protocolo SSL)** para configurar los ajustes que controlan las versiones mínima y máxima del protocolo y el intercambio de claves, cifrado y algoritmos de autenticación que se deben aplicar al tráfico descifrado de SSL. Estos ajustes están activos cuando este perfil se adjunta a una regla de política de descifrado que está configurada para realizar el descifrado proxy de reenvío SSL o la inspección entrante SSL.

STEP 5 | (Opcional) Bloquee y controle el tráfico (por ejemplo, una categoría URL) para la cual decida crear una exclusión de descifrado basada en una política.



A pesar de que aplicar un perfil de descifrado al tráfico que decida no descifrar es opcional, lo mejor siempre es aplicar un perfil de descifrado a las reglas de política para proteger su red de las sesiones con certificados caducados o emisores no confiables.

Seleccione **No Decryption (Sin descifrado)** para configurar el Perfil para configuración sin cifrado y marque las casillas de verificación **Block sessions with expired certificates (Bloquear sesiones con certificados caducados)** y **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)** para validar los certificados del tráfico que se excluye del descifrado. Cree exclusiones basadas en políticas solo para el tráfico que decida no descifrar. Si un servidor interrumpe el descifrado por motivos técnicos, no cree una exclusión basada en políticas, añada el servidor a la lista de exclusión de descifrado SSL (**Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión del descifrado SSL]**).

Estos ajustes están activos únicamente cuando el perfil de descifrado se adjunta a una regla de política de descifrado que deshabilita el descifrado para cierto tráfico.

STEP 6 | (Opcional) Bloquee y controle el tráfico SSH descifrado.

Seleccione **SSH Proxy (Proxy SSH)** para configurar el Perfil de descifrado del proxy SSH y realice la configuración para aplicar las versiones de protocolos compatibles y para bloquear sesiones si los recursos del sistema no están disponibles para realizar el descifrado.

© 2020 Palo Alto Networks, Inc.

Estos ajustes están activos únicamente cuando el perfil de descifrado se adjunta a una regla de política de descifrado que descifra el tráfico SSH.

STEP 7 | Añada el perfil de descifrado cuando cree una regla de política de descifrado.

El cortafuegos aplica el perfil de descifrado y la configuración del perfil en el tráfico que coincide con la regla de política de descifrado.

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Creación de una regla de política de descifrado

Cree una regla de política de descifrado para definir el tráfico que descifrará el cortafuegos y el tipo de descifrado que desea que el cortafuegos realice: descifrado de Proxy de reenvío SSL, Inspección entrante de SSL o Proxy SSH. También puede utilizar una regla de la política de descifrado para definir el Reflejo de descifrado.

STEP 1 | Añada una nueva regla a la política de descifrado.

Seleccione **Policies (Políticas)** > **Decryption (Descifrado)**, haga clic en **Add (Añadir)** para añadir una nueva regla a la política de descifrado y proporcione un nombre descriptivo a la regla de la política en **Name (Nombre)**.

STEP 2 | Configure la regla de descifrado para que coincida con el tráfico en función de la red y los objetos de política:

- **Firewall security zones**: seleccione **Source** y/o **Destination** y busque el tráfico en función de la **Source Zone** y/o la **Destination Zone**.
- **Direcciones IP, objetos de dirección o grupos de direcciones**: seleccione **Source (Origen)** o **Destination (Destino)** para buscar el tráfico en función de la **Source Address (Dirección de origen)** o la **Destination Address (Dirección de destino)**. O bien, seleccione **Negate** para excluir la lista de direcciones de origen del descifrado.
- **Users (Usuarios)**: seleccione **Source (Origen)** y configure el **Source User (Usuario de origen)** para el cual se debe descifrar el tráfico. Puede descifrar el tráfico de un usuario o grupo específico, o descifrar el tráfico de ciertos tipos de usuarios, tal como usuarios desconocidos o usuarios previo al inicio de sesión (usuarios que se conectaron a GlobalProtect pero que aún no iniciaron sesión).
- **Ports and protocols (Puertos y protocolos):** seleccione **Service/URL Category (Categoría de URL/servicio)** para configurar la regla de buscar el tráfico en función del servicio. Por defecto, la regla de política se configura para descifrar **todo** el tráfico en los puertos TCP y UDP. Puede **añadir** un servicio o grupo de servicios y, opcionalmente, configurar la regla en **application-default (aplicación-predeterminada)** para que coincida únicamente con los puertos predeterminados de la aplicación.



La configuración predeterminada de la aplicación puede ser útil cuando crea una exclusión de descifrado basada en una política. Puede excluir del descifrado las aplicaciones que se ejecutan en sus puertos por defecto, a la vez que continúa descifrando las mismas aplicaciones cuando son detectadas en puertos no estándar.

- **URLs and URL categories**: seleccione Service/URL Category y descifre el tráfico en función de:
  - Una lista de URL en host externo que el cortafuegos recupera para la aplicación de la política (consulte **Objects [Objetos]** > **External Dynamic Lists [Listas dinámicas externas]**).
  - Categorías de URL predefinidas de Palo Alto Networks, que facilitan el descifrado de categorías enteras de tráfico permitido. Esta opción también resulta útil cuando crea exclusiones de descifrado basadas en políticas, ya que permite excluir sitios confidenciales por categorías en lugar de individualmente. Por ejemplo, aunque puede crear una categoría de URL personalizada para

© 2020 Palo Alto Networks, Inc.

agrupar sitios que no desea descifrar, también puede excluir del descifrado los sitios financieros o relacionados con la salud en función de las categorías de URL predefinidas de Palo Alto Networks. Además, puede bloquear categorías de URL peligrosas y crear páginas sencillas para comunicar el motivo por el que los sitios están bloqueados o para permitir que los usuarios excluyan el descifrado de SSL.

Sírvase de las categorías de URL predefinidas de alto y medio riesgo para crear una regla de la política de descifrado que descifre todo el tráfico de las URL con esos grados de riesgo. Incluya la regla en la base de reglas para descifrar e inspeccionar todo el tráfico peligroso, pero colóquela al final para que la precedan todas las excepciones de descifrado y, de ese modo, no se descifre ninguna información confidencial. Ahora bien, si algunos sitios de medio o alto riesgo a los que permite el acceso contienen información de identificación personal u otra clase de datos confidenciales que no se deben descifrar, bloquee esos sitios para impedir el tráfico cifrado peligroso y, al mismo tiempo, problemas de privacidad. También puede crear una regla que impida el descifrado para manejar el tráfico confidencial.

- Categorías de URL personalizadas (consulte **Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**). Por ejemplo, puede crear una categoría de URL personalizada para especificar un grupo de sitios a los que necesita acceder con fines comerciales pero que no son compatibles con los protocolos y algoritmos más seguros, y luego aplicar un perfil de descifrado personalizado para permitir los algoritmos y protocolos menos estrictos solo en estos sitios (de esta forma, no se disminuye la seguridad si cambia el perfil de descifrado a la versión anterior que usa para la mayoría de los sitios).

STEP 3 | Configure la regla de modo que descifre el tráfico coincidente o excluya el tráfico coincidente del descifrado.

Seleccione **Options (Opciones)** y configure la **Action (Acción)** de la regla de política:

Para descifrar el tráfico coincidente:

1. Configure **Action (Acción)** en **Decrypt (Descifrado)**.
2. Configure el **Type (Tipo)** de descifrado que realizará el cortafuegos en el tráfico coincidente:
   - Proxy SSL de reenvío
   - Inspección entrante de SSL. Si desea habilitar la inspección entrante de SSL, seleccione también el **Certificate (Certificado)** para el servidor interno de destino del tráfico entrante de SSL.
   - Proxy SSH

Para excluir del descifrado el tráfico coincidente:

Configure **Action (Acción)** en **No Decrypt (Sin descifrado)**.

STEP 4 | (Opcional) Seleccione un **Decryption Profile (Perfil de descifrado)** para realizar comprobaciones adicionales en el tráfico que coincide con la regla de la política.



A pesar de que aplicar un perfil de descifrado para descifrar tráfico es opcional, lo mejor siempre es aplicar un perfil de descifrado a las reglas de política para proteger su red de amenazas cifradas. No puede protegerse de las amenazas si no puede verlas.

Por ejemplo, adjunte un perfil de descifrado a una regla de la política para garantizar que los certificados del servidor sean válidos y para bloquear sesiones utilizando protocolos o cifrado no compatible. Para llevar a cabo la Creación de un perfil de descifrado, seleccione **Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)**.

1. Cree una regla de política de descifrado o abra una regla existente para modificarla.
2. Seleccione **Options (Opciones)**y seleccione un **Decryption Profile (Perfil de descifrado)** para bloquear y controlar los diferentes aspectos del tráfico que coincide con la regla.

© 2020 Palo Alto Networks, Inc.

Los ajustes de la regla del perfil que el cortafuegos aplica al tráfico coincidente dependen de la **Action (Acción)** de la regla de política (descifrar o no descifrar) y del **Type (Tipo)** de la regla de política (proxy SSL de reenvío, inspección de entrada SSL o proxy SSH). Esto le permite usar los diferentes perfiles de descifrado con distintos tipos de reglas de política de descifrado que se aplican a diferentes tipos de tráfico y usuarios.

3. Haga clic en **OK (Aceptar)**.

STEP 5 | Configuración de logs de descifrado (establezca esta opción si se van a registrar enlaces TLS correctos e incorrectos y se va configurar el reenvío de logs de descifrado).

STEP 6 | Haga clic en **OK (Aceptar)** para guardar la política.

STEP 7 | Seleccione el próximo paso para habilitar completamente el cortafuegos para que descifre el tráfico:

- Configuración del proxy SSL de reenvío
- Configuración de la inspección de entrada SSL
- Configuración del proxy SSH
- Cree exclusiones de descifrado basadas en políticas para el tráfico que *decida* no descifrar y añada sitios que interrumpan el descifrado por motivos técnicos, como certificados fijados o autenticación mutua en la lista de exclusión de descifrado SSL.

© 2020 Palo Alto Networks, Inc.

Configuración del proxy SSL de reenvío

Para permitir que el cortafuegos realice el descifrado de proxy SSL de reenvío, debe configurar los certificados necesarios para establecer el cortafuegos como un agente externo fiable (proxy) para la sesión entre el cliente y el servidor. El cortafuegos puede usar certificados firmados por una entidad de certificación (certificate authority, CA) de la empresa o certificados autofirmados generados en el cortafuegos como *certificados de reenvío de confianza* para autenticar la sesión SSL con el cliente.

- (Práctica recomendada) **Certificados firmados por CA de la empresa:** Una CA de la empresa puede emitir un certificado de firma que el cortafuegos puede utilizar para firmar los certificados de los sitios que requieran un descifrado SSL. Cuando el cortafuegos confía en la CA que firmó el certificado del servidor de destino, el cortafuegos puede enviar una copia del certificado del servidor de destino al cliente firmado por la CA de la empresa. Esta es la mejor opción ya que generalmente todos los dispositivos de red ya confían en la CA de la empresa (en general, esta ya está instalada en el almacenamiento de confianza de CA de los dispositivos) y no necesita implementar el certificado en los endpoints, por lo tanto, el proceso de implementación es más fluido.
- **Certificados autofirmados:** El cortafuegos puede actuar como una CA y generar certificados autofirmados que puede usar para firmar los certificados de sitios en los que se requiere el descifrado SSL. El cortafuegos puede firmar una copia del certificado del servidor para presentarla al cliente y establecer la sesión SSL. Este método requiere que instale los certificados autofirmados en todos los dispositivos de su red de modo que estos reconozcan los certificados autofirmados del cortafuegos. Debido a que los certificados deben implementarse en todos los dispositivos, este método es mejor para las pruebas de concepto (proof of concept, POC) y las implementaciones pequeñas que para las grandes.

Además, configure un *certificado de reenvío no confiable* para que el cortafuegos lo presente a los clientes cuando el certificado esté firmado por una CA en la que el cortafuegos no confía. Esto garantiza que a los clientes les aparezca un mensaje con una advertencia sobre el certificado cuando intenten acceder a sitios con certificados que no sean de confianza.



Independientemente de si genera certificados de reenvío confiables de su CA raíz de la empresa o usa un certificado autofirmado generado en el cortafuegos, genere otro certificado de CA confiable de reenvío subordinado para cada cortafuegos. La flexibilidad de usar diferentes CA subordinadas le permite revocar un certificado cuando retira un dispositivo (o par de dispositivos) sin afectar el resto de la implementación y reduce el impacto en cualquier situación en la que necesite revocar un certificado. Usar diferentes certificados de CA confiables de reenvío en cada cortafuegos ayuda a solucionar problemas, ya que el mensaje de error de CA que el usuario ve incluye información sobre el cortafuegos que atraviesa el tráfico. Si usa la misma CA confiable de reenvío en cada cortafuegos, pierde el nivel de detalle de esa información.

Después de configurar los certificados de reenvío fiables y no fiables necesarios para el descifrado proxy de reenvío SSL, cree una regla de política de descifrado para definir el tráfico que desea que el cortafuegos descifre y cree un perfil de descifrado para aplicar revisiones y controles SSL en el tráfico. La política de descifrado descifra el tráfico SSL de transmisión mediante túneles que coincide con la regla en tráfico de texto sin cifrar. El cortafuegos bloquea y restringe el tráfico sobre la base del perfil de descifrado adjunto a la política de descifrado y de la política de seguridad del cortafuegos. El cortafuegos vuelve a cifrar el tráfico a medida que sale de él.

STEP 1 | Asegúrese de que las interfaces adecuadas están configuradas como interfaces de Virtual Wire, capa 2 o capa 3.

© 2020 Palo Alto Networks, Inc.

Visualice las interfaces configuradas en la pestaña **Network (Red)** > **Interfaces** > **Ethernet**. La columna **Interface Type (Tipo de interfaz)** muestra si una interfaz está configurada para ser una interfaz de **Virtual Wire**, **Layer 2** o**Layer 3**. Puede seleccionar una interfaz para modificar su configuración, incluido qué tipo de interfaz es.

STEP 2 | Configure el certificado de reenvío confiable para que el cortafuegos lo presente a los clientes cuando una CA confiable haya firmado el certificado del servidor. Puede usar un certificado firmado por una CA empresarial o un certificado autofirmado como el certificado de reenvío fiable.

(Práctica recomendada) Use un certificado firmado por una CA de la empresa como el certificado de reenvío confiable. Cree un certificado de reenvío confiable con un nombre único en cada cortafuegos:

1. Genere una solicitud de firma de certificado (Certificate Signing Request, CSR) para que la CA de empresa lo firme y valide.
    1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y haga clic en **Generate (Generar)**.
    2. Introduzca un **Certificate Name (Nombre de certificado)**. Use un nombre único para cada cortafuegos.
    3. En la lista desplegable **Signed By (Firmado por)**, seleccione **External Authority (CSR) (Autoridad externa [CSR])**.
    4. (Opcional) Si su CA de empresa lo requiere, añada **Certificate Attributes (Atributos del certificado)** para identificar más información detallada del cortafuegos, como el país o el departamento.
    5. Haga clic en **Generate (Generar)** para guardar la CSR. El certificado pendiente ahora se muestra en la pestaña **Device Certificates (Certificados de dispositivos)**.
2. Exporte la CSR:
    1. Seleccione el certificado pendiente que aparece en la pestaña **Device Certificates (Certificados de dispositivos)**.
    2. Haga clic en **Export (Exportar)**para descargar y guardar el archivo del certificado.

        Deje Exportar clave privada sin seleccionar para garantizar que la clave privada permanezca protegida en el cortafuegos.
    3. Haga clic en **OK (Aceptar)**.
3. Proporcione el archivo del certificado a su CA de empresa. Cuando reciba el certificado firmado de la CA de la empresa de su CA de la empresa, guárdelo para importarlo en el cortafuegos.
4. Importe el certificado firmado por la CA de empresa al cortafuegos:
    1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y haga clic en **Import (Importar)**.
    2. Introduzca el nombre del certificado pendiente en **Certificate Name (Nombre de certificado)** de manera exacta. El **nombre del certificado** que introduzca debe coincidir exactamente con el nombre del certificado pendiente a fin de que este se valide.
    3. Seleccione el **Certificate File (Archivo del certificado)** que recibió de su CA de empresa.
    4. Haga clic en **OK (Aceptar)**. El certificado se muestra como válido con las casillas de verificación Clave y CA seleccionadas.
5. Seleccione el certificado validado para habilitarlo como **Forward Trust Certificate (Certificado de reenvío confiable)** y utilizarlo para el descifrado del proxy SSL de reenvío.
6. Haga clic en **OK (Aceptar)** para guardar el certificado de reenvío fiable firmado por la CA de empresa.

Use un certificado autofirmado como el certificado de reenvío confiable:

1. Cree un certificado de CA raíz autofirmado.
2. Haga clic en el certificado de CA raíz autofirmado (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **Certificates [Certificados]** > **Device Certificates [Certificados de**

© 2020 Palo Alto Networks, Inc.

dispositivo]) para abrir la **Certificate information (Información del certificado)** y, luego, haga clic en la casilla de verificación **Trusted Root CA (CA raíz de confianza)**.

3. Haga clic en **OK (Aceptar)**.
4. Genere nuevos certificados de CA subordinados para cada cortafuegos:
    1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.
    2. Haga clic en **Generate (Generar)** en la parte inferior de la ventana.
    3. Introduzca un **Certificate Name (Nombre de certificado)**.
    4. Escriba un **Common Name (Nombre común)**, como 192.168.2.1. Debería ser la dirección IP o el FQDN que aparecerá en el certificado. En este caso estamos usando la IP de la interfaz fiable. Evite usar espacios en este campo.
    5. En el campo **Signed By (Firmado por)**, seleccione el certificado de CA raíz autofirmado que creó.
    6. Haga clic en la casilla de verificación **Certificate Authority (Autoridad del certificado)** para habilitar el cortafuegos para que emita el certificado. Al seleccionar esta casilla de verificación, se crea una entidad de certificación (CA) en el cortafuegos que se importará a los exploradores de los clientes, de modo que los clientes confíen en el cortafuegos como CA.
    7. Seleccione **Generar** el certificado.
5. Haga clic en el nuevo certificado para modificarlo y en la casilla de verificación **Forward Trust Certificate (Certificado de reenvío confiable)** para configurar el certificado como certificado de reenvío confiable.
6. Haga clic en **OK (Aceptar)** para guardar el certificado de reenvío fiable autofirmado.
7. Repita este procedimiento para generar un certificado de CA subordinado único en cada cortafuegos.

STEP 3 | Distribuya el certificado de reenvío fiable a los almacenes de certificados del sistema cliente.

Si utiliza un certificado firmado por una CA de empresa como el certificado de reenvío confiable para el descifrado de proxy SSL de reenvío y los sistemas cliente ya tienen la CA de empresa instalada en la lista de CA raíz de confianza local, puede omitir este paso. (Los sistemas cliente confían en los certificados de CA subordinados que genera en el cortafuegos porque la CA raíz de empresa confiable los firmó).

Si no instala el certificado de reenvío confiable en los sistemas cliente, los usuarios verán advertencias de certificación en cada sitio SSL que visiten.

En un cortafuegos configurado como portal GlobalProtect:

Esta opción es compatible con las versiones de SO cliente de Windows y Mac, y requiere la instalación del agente GlobalProtect 3.0.0 o posterior en los sistemas cliente.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y, luego, seleccione una configuración de portal existente o haga clic en **Add (Añadir)** para añadir una nueva.
2. Seleccione **Agent (Agente)** y luego seleccione una configuración de agente existente o seleccione **Add (Añadir)** para añadir una nueva.
3. Haga clic en **Add (Añadir)** para añadir el certificado de CA raíz confiable autofirmado del cortafuegos a la sección de CA raíz confiable. Después de que GlobalProtect distribuya el certificado de CA raíz confiable del cortafuegos a los sistemas cliente, estos últimos confían en los certificados de CA subordinados del cortafuegos porque los clientes confían en el certificado de CA raíz del cortafuegos.
4. Seleccione **Install in Local Root Certificate Store** para que el portal de GlobalProtect distribuya automáticamente el certificado y lo instale en el almacén de certificados en los sistemas cliente de GlobalProtect.
5. Haga clic en **OK** dos veces.

Sin GlobalProtect:

© 2020 Palo Alto Networks, Inc.

Exporte el certificado de CA raíz confiable del cortafuegos de modo que pueda importarlo en los sistemas cliente. Resalte el certificado y haga clic en **Export (Exportar)** en la parte inferior de la ventana. Elija el formato PEM.



No seleccione la casilla de verificación Export private key (Exportar clave privada). La clave privada debe permanecer en el cortafuegos y no debe exportarse a los sistemas cliente.

Importe el certificado de CA raíz confiable del cortafuegos a la lista de CA raíz de confianza del explorador de los sistemas cliente para que los clientes confíen en él. Al importar en el explorador del cliente, asegúrese de añadir el certificado al almacén de certificados de entidades de certificación raíz de confianza. En sistemas Windows, la ubicación de importación predeterminada es el almacén de certificados personales. También puede simplificar este proceso utilizando la opción de implementación centralizada, como un Objeto de política de grupo (Group Policy Object, GPO) de Active Directory.

STEP 4 | Configure el certificado de reenvío no confiable (use el mismo certificado de reenvío no confiable para todos los cortafuegos).

1. Haga clic en **Generar** en la parte inferior de la página de certificados.
2. Introduzca un **Certificate Name (Nombre de certificado)**, como mi-reenvio-ssl-nofiable.
3. Defina el **Common Name (Nombre común)**, por ejemplo 192.168.2.1. Deje **Signed By (Firmado por)** en blanco.
4. Haga clic en la casilla de verificación **Certificate Authority (Autoridad del certificado)** para habilitar el cortafuegos para que emita el certificado.
5. Haga clic en **Generar** para generar el certificado.
6. Haga clic en **OK (Aceptar)** para guardar.
7. Haga clic en el nuevo certificado mi-reenvio-ssl-nofiable para modificarlo y habilite la opción **Forward Untrust Certificate (Certificado de reenvío no confiable)**.



No exporte el certificado de reenvío no confiable a las Listas de certificados confiables de sus dispositivos de red. No instale el certificado de reenvío no confiable en sistemas cliente. Esto es crítico porque si instala el certificado no confiable en la lista de certificados confiables, los dispositivos confiarán en los sitios web que el cortafuegos no confía. Además, los usuarios no verán las advertencias de certificación de sitios no confiables, por lo que no sabrán si los sitios no son confiables y podrán acceder a ellos, lo que expone su red a amenazas.

8. Haga clic en **OK (Aceptar)** para guardar.

STEP 5 | (Opcional) Configure el tamaño de clave de los certificados proxy SSL de reenvío que el cortafuegos presenta a los clientes. Por defecto, el cortafuegos determina el tamaño de clave que debe en función del tamaño de clave del certificado del servidor de destino.

STEP 6 | Cree una regla de política de descifrado para definir el tráfico que el cortafuegos debe descifrar y cree un perfil de descifrado para aplicar controles SSL al tráfico.



A pesar de que los perfiles de descifrado son opcionales, lo mejor es incluir uno con cada regla de política de descifrado a fin de evitar que protocolos y algoritmos débiles y vulnerables permitan el tráfico cuestionable en la red.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)**, añada o modifique una regla existente y defina el tráfico que se debe descifrar.
2. Seleccione **Options (Opciones)** y:

© 2020 Palo Alto Networks, Inc.

- Configure la **Action (Acción)** de la regla en **Decrypt (Descifrar)** para descifrar el tráfico coincidente.
- Configure el **tipo** de regla en **SSL Forward Proxy**.
- (Opcional pero recomendado) Configure o seleccione un **Decryption Profile (Perfil de descifrado)** existente para bloquear y controlar diferentes aspectos del tráfico descifrado (por ejemplo, cree un perfil de descifrado para realizar comprobaciones de certificados y aplicar conjuntos de cifrados y versiones de protocolo sólidas).

3. Haga clic en **OK (Aceptar)** para guardar.

STEP 7 | Habilite el cortafuegos para que reenvíe tráfico SSL descifrado para el análisis de WildFire.

Esta opción requiere una licencia WildFire activa y es una práctica recomendada de WildFire*.*

STEP 8 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 9 | Elija su próximo paso:

- Habilitar a los usuarios para que excluyan el descifrado SSL..
- Configure las exclusiones de descifrado para deshabilitar el descifrado de ciertos tipos de tráfico.

© 2020 Palo Alto Networks, Inc.

Configuración de la inspección de entrada SSL

Utilice la Inspección de entrada SSL para descifrar e inspeccionar el tráfico SSL entrante destinado a un servidor de red (puede realizar la inspección de entrada SSL para cualquier servidor si carga el certificado de este en el cortafuegos). Con una política de descifrado de inspección de entrada SSL habilitada, el cortafuegos descifra todo el tráfico SSL identificado por la política en texto no cifrado y lo inspecciona. El cortafuegos bloquea, restringe o permite el tráfico en función del perfil de descifrado adjunto a la política y de la política de seguridad que se aplica al tráfico, lo que incluye todos los perfiles de antivirus, protecciones contra vulnerabilidades, antispyware, filtrado de URL y bloqueo de archivos. Lo mejor es habilitar el cortafuegos para el reenvío de tráfico SSL descifrado para el análisis de WildFire y la generación de firmas.

La configuración de la Inspección de entrada SSL incluye la instalación del certificado del servidor de destino en el cortafuegos, la creación de una política de descifrado de inspección de entrada SSL y la aplicación de un perfil de descifrado en la política.

La inspección de SSL entrante no admite la redirección del portal de autenticación. Para utilizar el redireccionamiento y el descifrado del portal de autenticación, debe utilizar el proxy SSL de reenvío.

STEP 1 | Asegúrese de que las interfaces adecuadas estén configuradas como interfaces de modo tap, cable virtual, capa 2 o capa 3.

No puede utilizar una interfaz de modo tap en la inspección entrante de SSL si el cifrado negociado incluye algoritmos de intercambio de claves PFS (DHE y ECDHE).

Visualice las interfaces configuradas en la pestaña **Network (Red)** > **Interfaces** > **Ethernet**. La columna **Interface Type (Tipo de interfaz)** muestra si una interfaz está configurada para ser una interfaz de **Virtual Wire**, **Layer 2** o**Layer 3**. Puede seleccionar una interfaz y modificar su configuración, incluido qué tipo de interfaz es.

STEP 2 | Asegúrese de que el certificado del servidor de destino esté instalado en el cortafuegos.

En la interfaz web, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates** > **Device Certificates (Certificados de dispositivos)** para ver los certificados instalados en el cortafuegos.

Para importar el certificado del servidor de destino en el cortafuegos:

1. En la pestaña **Device Certificates (Certificados de dispositivos)**, seleccione **Import (Importar)**.
2. Introduzca un **Certificate Name (Nombre de certificado)** descriptivo.
3. Busque y seleccione el **archivo del certificado** del servidor de destino.
4. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree una regla de política de descifrado para definir el tráfico que el cortafuegos debe descifrar y cree un perfil de descifrado para aplicar controles SSL al tráfico.

A pesar de que los perfiles de descifrado son opcionales, lo mejor es incluir uno con cada regla de política de descifrado a fin de evitar que protocolos y algoritmos débiles y vulnerables permitan el tráfico cuestionable en la red.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)**, añada o modifique una regla existente y defina el tráfico que se debe descifrar.

© 2020 Palo Alto Networks, Inc.

2. Seleccione **Options (Opciones)** y:
   - Configure la **Action (Acción)** de la regla en **Decrypt (Descifrar)** para descifrar el tráfico coincidente.
   - Configure el **Type (Tipo)** de regla en **SSL Inbound Inspection (Inspección de entrada SSL)**.
   - Seleccione el **Certificate (Certificado)** para el servidor interno que es el destino del tráfico SSL entrante.
   - (Opcional pero recomendado) Configure o seleccione un **Decryption Profile (Perfil de descifrado)** para bloquear y controlar varios aspectos del tráfico descifrado (por ejemplo, cree un perfil de descifrado para finalizar sesiones con algoritmos y conjuntos de cifrados no compatibles).

     Cuando configure el #unique_567 para el tráfico de inspección de entrada SSL, cree diferentes perfiles para los servidores con diferentes capacidades de seguridad. Por ejemplo, si un conjunto de servidores admite solo RSA, la configuración del protocolo SSL solo necesita admitir RSA. Sin embargo, la configuración del protocolo SSL para los servidores que son compatibles con PFS debe admitir PFS. Ajuste la configuración del protocolo SSL para el nivel más alto de seguridad que admita el servidor, pero verifique el rendimiento para garantizar que los recursos del cortafuegos puedan administrar una mayor carga de procesamiento que requieren los protocolos y algoritmos de seguridad más altos.
3. Haga clic en **OK (Aceptar)** para guardar.

STEP 4 | Habilite el cortafuegos para que reenvíe tráfico SSL descifrado para el análisis de WildFire.

Esta opción requiere una licencia WildFire activa y es una práctica recomendada de WildFire.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 6 | Elija su próximo paso...

- Habilitar a los usuarios para que excluyan el descifrado SSL..
- Configure las exclusiones de descifrado para deshabilitar el descifrado de ciertos tipos de tráfico.

© 2020 Palo Alto Networks, Inc.

Configuración del Proxy SSH

La configuración de SSH Proxy (Proxy SSH) no requiere certificados y la clave utilizada para descifrar sesiones SSH se genera automáticamente en el cortafuegos durante el inicio. Si el descifrado SSH está habilitado, el cortafuegos descifra el tráfico SSH, y bloquea o restringe el tráfico SSH en función de su política de descifrado y la configuración del perfil de descifrado. El tráfico vuelve a cifrarse a medida que sale del cortafuegos.

STEP 1 | Asegúrese de que las interfaces adecuadas están configuradas como interfaces de Virtual Wire, capa 2 o capa 3. El descifrado solo se puede realizar en Virtual Wire, interfaces de capa 2 o capa 3.

Visualice las interfaces configuradas en la pestaña **Network (Red)** > **Interfaces** > **Ethernet**. La columna **Interface Type (Tipo de interfaz)** muestra si una interfaz está configurada para ser una interfaz de **Virtual Wire**, **Layer 2** o**Layer 3**. Puede seleccionar una interfaz para modificar su configuración, incluido qué tipo de interfaz es.

STEP 2 | Cree una regla de la política de descifrado para definir el tráfico que debe descifrar el cortafuegos y cree un perfil de descifrado para aplicar comprobaciones al tráfico de SSL.

A pesar de que los perfiles de descifrado son opcionales, lo mejor es incluir uno con cada regla de política de descifrado a fin de evitar que protocolos y algoritmos débiles y vulnerables permitan el tráfico cuestionable en la red.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)**, añada o modifique una regla existente y defina el tráfico que se debe descifrar.
2. Seleccione **Options (Opciones)** y:
   - Configure la **Action (Acción)** de la regla en **Decrypt (Descifrar)** para descifrar el tráfico coincidente.
   - Configure el **tipo** de regla en **SSL Proxy**.
   - (Opcional pero recomendado) Configure o seleccione un **Decryption Profile (Perfil de descifrado)** para bloquear y controlar varios aspectos del tráfico descifrado (por ejemplo, cree un perfil de descifrado para finalizar sesiones con versiones no compatibles y algoritmos no admitidos).
3. Haga clic en **OK (Aceptar)** para guardar.

STEP 3 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 4 | (Opcional) Continúe con las Exclusiones de descifrado para deshabilitar el descifrado de diferentes tipos de tráfico.

© 2020 Palo Alto Networks, Inc.

Configuración de una verificación del certificado de servidor para el tráfico sin descifrar

Cree políticas de no descifrado para el tráfico que *elija* no descifrar porque es personal, confidencial o está sujeto a leyes y normativas locales. Por ejemplo, puede optar por no descifrar el tráfico de determinados ejecutivos o el tráfico entre los usuarios de finanzas y los servidores de finanzas que contienen información personal. (No excluya el tráfico que no puede descifrar porque un sitio rompe el descifrado por motivos técnicos como un certificado fijado o una autenticación mutua por una política. En cambio, añada el nombre de host a la Lista de exclusión de descifrado).

Sin embargo, el hecho de que usted no descifre el tráfico no quiere decir que deba dejar todo el tráfico sin descifrar en su red. Se recomienda que aplique un perfil de no descifrado para el tráfico descifrado para bloquear sesiones con certificados caducados y emisores no confiables.

STEP 1 | Cree una regla de política de descifrado para identificar el tráfico sin descifrar y cree un perfil de descifrado para bloquear las sesiones incorrectas.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y añada o modifique una regla existente para identificar el tráfico sin descifrar.
2. Seleccione **Options (Opciones)** y:
   - Configure la regla **Action (Acción)** en **No Decrypt (No descifrar)** de modo que el cortafuegos no descifre el tráfico que coincida con la regla.
   - Ignore la regla **Type (Tipo)** porque el tráfico no está descifrado.
   - (Opcional pero recomendado) Configure o seleccione un perfil de descifrado para el tráfico no descifrado a fin de bloquear las sesiones que tengan certificados vencidos y emisores de certificados poco fiables.

   No adjunte un perfil que no sea de descifrado a las políticas de descifrado para el tráfico TLSv1.3 que no descifre, ya que el cortafuegos no puede leer la información del certificado cifrado, por lo que no puede realizar comprobaciones de certificados. Sin embargo, debe crear una política de descifrado para el tráfico TLSv1.3 que no descifre, ya que el tráfico no cifrado no se registra a no ser que una política de descifrado controle ese tráfico.

STEP 2 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 3 | Elija su próximo paso:

- Habilitar a los usuarios para que excluyan el descifrado SSL..
- Configure las exclusiones de descifrado para deshabilitar el descifrado de ciertos tipos de tráfico.

© 2020 Palo Alto Networks, Inc.

Exclusiones de descifrado

Puede excluir dos tipos de tráfico del descifrado:

- Tráfico que interrumpe el descifrado *por motivos técnicos* (el descifrado bloquea el tráfico), como certificados fijados, cadenas de certificados incompletas, cifrados no compatibles o la autenticación mutua (el intento de descifrado del tráfico provoca que se bloquee). Palo Alto Networks proporciona una lista predefinida de exclusión de descifrado SSL (**Device [Dispositivo]** > **Certificate management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**) que excluye hosts con aplicaciones y servicios que se conoce que interrumpen el descifrado desde el punto de vista técnico del descifrado SSL predeterminado. Si encuentra sitios que interrumpen el descifrado desde el punto de vista técnico no están en la lista de exclusión de descifrado SSL, puede añadirlos a la lista manualmente por nombre de host del servidor. El cortafuegos bloquea los sitios cuyas aplicaciones y servicios interrumpen el descifrado de manera técnica, salvo que los añada a la lista de exclusión del descifrado SSL.

  Si el perfil de descifrado permite **modos no admitidos** (sesiones con autenticación de cliente, versiones no admitidas o conjuntos de cifrado no admitidos), el cortafuegos añade automáticamente servidores y aplicaciones que utilizan los modos no admitidos permitidos a su caché de exclusión de descifrado SSL local. (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]** > **Show Local Exclusion Cache [Mostrar caché de exclusión]**). Cuando se bloquean los modos no admitidos, aumenta la seguridad, pero también se bloquea la comunicación con aplicaciones que usan esos modos.
- Tráfico que *decide* no descifrar por motivos comerciales, normativos, personales o de otro tipo, como el tráfico financiero, médico, sanitario u oficial. Puede excluir el tráfico del descifrado en función de la fuente, destino, categoría de URL y servicio.

Puede usar asteriscos (*) como comodines para crear exclusiones de descifrado para varios nombres de host asociados a un dominio. Los asteriscos se comportan de la misma manera que los símbolos de intercalación (^) para las excepciones de categoría de URL: cada asterisco controla un subdominio variable (etiqueta) en el nombre de host. Esto le permite crear exclusiones tanto muy específicas como muy generales. Por ejemplo:

- mail.*.com coincide con mail.company.com, pero no con mail.company.sso.com.
- *.company.com coincide con tools.company.com, pero no con eng.tools.company.com.
- *.*.company.com coincide con eng.tools.company.com, pero no con eng.company.com.
- *.*.*.company.com coincide con corp.exec.mail.company.com, pero no con corp.mail.company.com.
- mail.google.* coincide con mail.google.com, pero no con mail.google.uk.com.
- mail.google.*.* coincide con mail.google.co.uk, pero no con match mail.google.com.

Por ejemplo, usar comodines para excluir video-stats.video.google.com del descifrado, pero no excluir video.google.com del descifrado, excluya *.*.google.com.



*Independientemente de la cantidad de comodines tipo asterisco que precedan a un nombre de host (sin una etiqueta que no sea de comodín que preceda al nombre de host), el nombre de host coincide con la entrada. Por ejemplo, *.google.com, *.*.google.com y *.*.*.google.com todos coinciden con google.com. Sin embargo, *.dev.*.google.com bo coincide con google.com porque una etiqueta (dev) no es un comodín.*

Para aumentar la visibilidad del tráfico y reducir la superficie de ataque tanto como fuera posible, no realice excepciones de descifrado salvo que sea necesario.

- Exclusiones predefinidas de descifrado de Palo Alto Networks
- Exclusión de un servidor del descifrado por motivos técnicos
- Caché de exclusión de descifrado local
- Creación de una exclusión al descifrado basada en la política

© 2020 Palo Alto Networks, Inc.

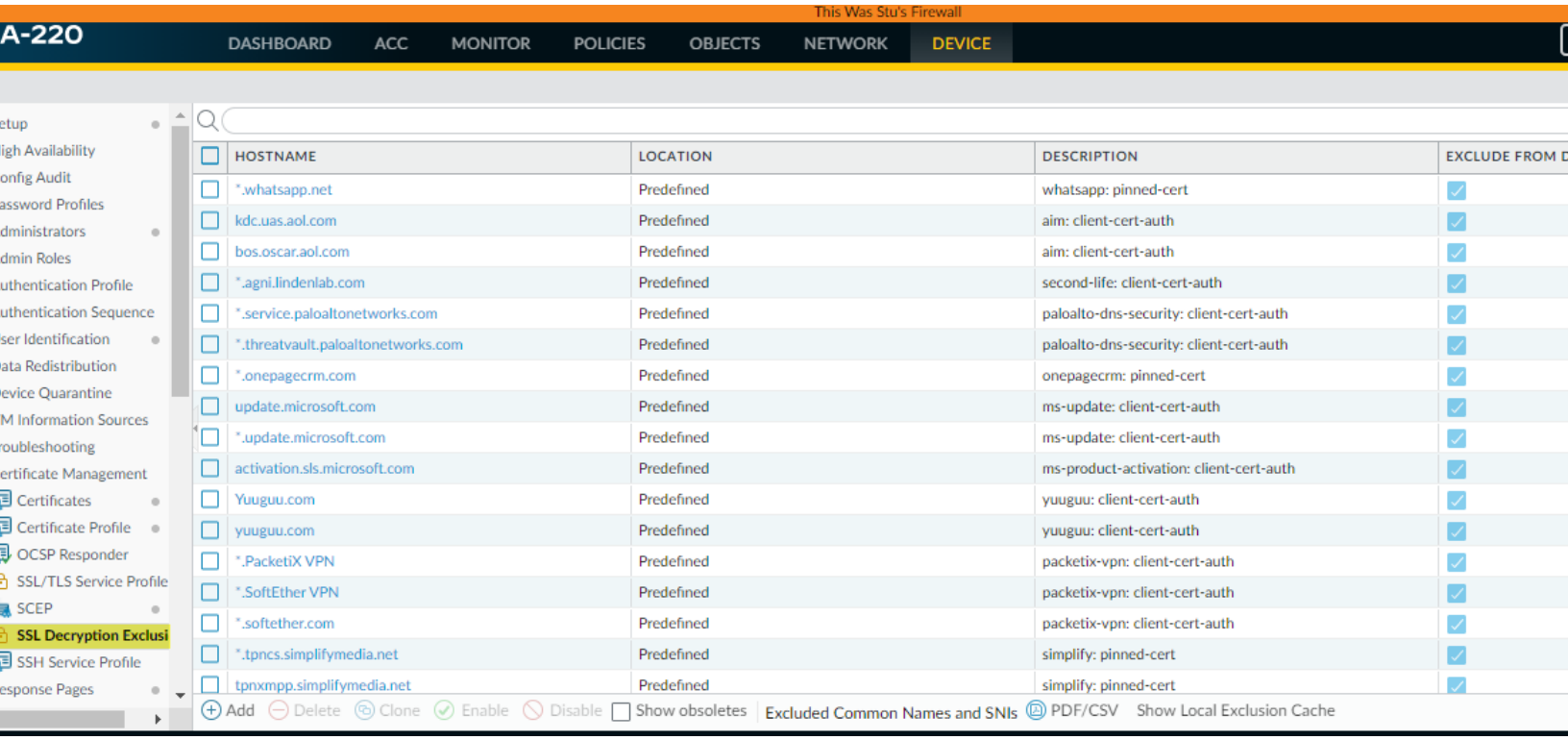
Exclusiones predefinidas de descifrado de Palo Alto Networks

El cortafuegos proporciona una lista predefinida de exclusión de descifrado SSL para excluir del descifrado los sitios comúnmente usados que lo interrumpen por motivos técnicos, como certificados fijados y autenticación mutua. Las exclusiones predefinidas del descifrado están habilitadas de forma predeterminada y Palo Alto Networks proporciona exclusiones de descifrado predefinidas nuevas y actualizadas al cortafuegos como parte de la actualización de contenido de aplicaciones y amenazas (o la actualización de contenido de aplicaciones si no tiene una licencia de prevención de amenazas). El cortafuegos no descifra tráfico que coincide con exclusiones predefinidas y permite el tráfico cifrado en función de la política de seguridad que rige ese tráfico. Sin embargo, el cortafuegos puede inspeccionar el tráfico cifrado o ejecutar la política en él.

*La lista de exclusión de descifrado de SSL **no** se aplica a los sitios que decide no descifrar por motivos legales, normativos, comerciales, de privacidad o de otro tipo, sino a los sitios que interrumpen el descifrado por motivos técnicos, pues el descifrado bloquea su tráfico. Para el tráfico que decide no descifrar, como direcciones IP, usuarios, categorías de URL, servicios e incluso zonas completas,* cree una exclusión de descifrado basada en políticas*.*

Debido a que el tráfico de los sitios de la lista de exclusión de descifrado SSL permanece cifrado, el cortafuegos no inspecciona el tráfico ni proporciona otra aplicación de seguridad. Puede deshabilitar una exclusión predefinida. Por ejemplo, puede elegir deshabilitar las exclusiones predefinidas para aplicar una política de seguridad estricta que permita solo aplicaciones y servicios que el cortafuegos pueda inspeccionar y en la cuales pueda aplicar una política de seguridad. Sin embargo, el cortafuegos bloquea los sitios cuyas aplicaciones y servicios interrumpen el descifrado desde el punto de vista técnico si no están permitidos en la lista de exclusión de descifrado SSL.

Puede ver y gestionar todas las exclusiones de descifrado SSL predefinidas de Palo Alto Networks directamente en el cortafuegos (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusions [Exclusiones de descifrado SSL]**).



© 2020 Palo Alto Networks, Inc.

Hostname (Nombre del host) muestra el nombre del host que aloja la aplicación o servicio que interrumpe el descifrado desde el punto de vista técnico. También puede seleccionar **Add (Añadir)** para añadir hosts para excluir un servidor del descifrado por motivos técnicos si no está en la lista predefinida.

Description (Descripción) muestra el motivo por el cual el cortafuegos no puede descifrar el tráfico del sitio, por ejemplo **pinned-cert** (un certificado fijado) o **client-cert-auth** (autenticación de cliente).

El cortafuegos elimina automáticamente exclusiones de cifrado SSL predefinidas y habilitadas de la lista cuando se vuelven obsoletas (cuando una aplicación que sufrió una interrupción causada por el descifrado ahora se admite con descifrado). **Show Obsoletes (Mostrar obsoletas)** comprueba si alguna exclusión predefinida y deshabilitada permanece en la lista y ya no es necesaria. El cortafuegos no elimina automáticamente las exclusiones de descifrado predefinidas y deshabilitadas de la lista, puede seleccionarlas y hacer clic en **Delete (Eliminar)** para eliminar las entradas obsoletas.

Puede seleccionar la casilla de verificación del nombre del host y hacer clic en **Disable (Deshabilitar)** para eliminar sitios predefinidos de la lista. Use la lista de exclusión de descifrado SSL solo para los sitios que interrumpen el descifrado por motivos técnicos, no la use en sitios que decida no descifrar.

Exclusión de un servidor del descifrado por motivos técnicos

Si el descifrado interrumpe una aplicación o un servicio importantes por motivos técnicos (pues el descifrado bloquea su tráfico), puede añadir el nombre de host del sitio que los aloja a la lista predefinida de exclusión de descifrado de SSL de Palo Alto Networks para crear una excepción de descifrado personalizada. El cortafuegos no descifra, inspecciona ni aplica la política de seguridad en el tráfico permitido por la lista de exclusión de descifrado SSL porque este permanece cifrado. Por lo tanto, asegúrese de que los sitios que añade a la lista realmente sean sitios con aplicaciones o servicios necesarios para la empresa. Por ejemplo, algunas aplicaciones personalizadas internas que son imprescindibles para la empresa pueden interrumpir el descifrado y puede añadirlas a la lista, de modo que el cortafuegos permita el tráfico cifrado de la aplicación personalizada.



*La lista de exclusión de descifrado SSL **no** es para los sitios que elige no descifrar por motivos legales, normativos, comerciales, de privacidad o de otro tipo, solo es para los sitios que interrumpen el descifrado desde el punto de vista técnico. Para el tráfico (direcciones IP, usuarios, categorías de URL, servicios e incluso zonas completas) que elige no descifrar,* cree una exclusión de descifrado basada en una política*.*

Los motivos por los que los sitios interrumpen el descifrado desde el punto de vista técnico incluyen certificados fijados, autenticación de cliente, cadenas incompletas de certificados y cifrados no compatibles. Casi todos los navegadores que permiten la fijación de claves públicas de HTTP (HTTP public key pinning, HPKP) admiten el descifrado del proxy de reenvío siempre que instale el certificado de CA empresarial o la cadena de certificados en el cliente.



Si el motivo técnico de excluir un sitio del descifrado es una cadena incompleta de certificados, el cortafuegos de próxima generación no repara automáticamente la cadena como sí lo haría el explorador. Si necesita añadir un sitio a la lista de exclusión de descifrado SSL, revíselo manualmente para asegurarse de que es un sitio comercial legítimo, luego descargue los certificados que falten de la CA secundaria y cárguelos e impleméntelos *en el cortafuegos.*

Después de añadir un servidor a la lista de exclusión de descifrado SSL, el cortafuegos compara el nombre de host del servidor que usa para definir la exclusión de descifrado con el nombre común (common name, CN) en el certificado que presenta un servidor. Si un solo servidor aloja varios sitios web con diferentes

© 2020 Palo Alto Networks, Inc.

certificados, el cortafuegos compara el nombre del host con la indicación del nombre de servidor (server name indication, SNI) que presenta el cliente para indicar el servidor al cual desea conectarse.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **SSL Decryption Exclusions (Exclusiones de descifrado SSL)**.

STEP 2 | Haga clic en **Add (Añadir)** para añadir una nueva exclusión de descifrado, o seleccione una entrada personalizada existente para modificarla.

STEP 3 | Introduzca el **hostname (nombre de host)** del sitio web o la aplicación que desea excluir del descifrado.

El nombre de host distingue entre mayúsculas y minúsculas.

Puede utilizar comodines para excluir varios nombres de host asociados a un dominio. El cortafuegos excluye todas las sesiones donde el servidor presenta un CN que coincide con el dominio del descifrado.

Asegúrese de que el campo del nombre de host sea único para cada entrada personalizada. Si una exclusión predefinida coincide con una entrada personalizada, la entrada personalizada tiene prioridad.

STEP 4 | (Opcional) Seleccione **Shared (Uso compartido)** para compartir una exclusión en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple.

STEP 5 | Haga clic en **Exclude (Excluir)** para excluir la aplicación del descifrado. De manera alternativa, si modifica una exclusión de descifrado existente, puede desmarcar esta casilla de verificación para comenzar a descifrar una entrada que, previamente, se excluía del descifrado.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar la nueva entrada de exclusión.

Caché de exclusión de descifrado local

El cortafuegos puede añadir servidores a la caché de exclusión de descifrado local (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]** > **Show Local Exclusion Cache [Mostrar caché de exclusión local]**) y excluir su tráfico del descifrado automáticamente durante 12 horas si ese tráfico interrumpe el descifrado por motivos técnicos, como un certificado fijo o un certificado no admitido. Cuando el perfil de descifrado permite modos no admitidos (sesiones con autenticación de cliente, versiones no admitidas o conjuntos de cifrado no compatibles) y el tráfico permitido utiliza un modo no admitido, el dispositivo añade automáticamente el servidor a la caché de exclusión local y omite el descifrado. El cortafuegos no descifra, inspecciona ni aplica la política de seguridad en el tráfico que permite la caché de exclusión de descifrado local porque el tráfico permanece cifrado. Asegúrese de que los sitios que excluye del descifrado (mediante la aplicación de un perfil de descifrado que permita modos no admitidos) sean sitios con aplicaciones o servicios que necesite para su empresa.

El bloqueo de modos no admitidos bloquea la comunicación con aplicaciones que usan esos modos para aumentar la seguridad. La autenticación del cliente es un motivo común para excluir aplicaciones del descifrado, por lo que la práctica recomendada es bloquear las versiones no admitidas y los cifrados no admitidos y permitir la autenticación del cliente en el perfil de descifrado. Si el perfil de descifrado permite la autenticación del cliente, cuando un cliente inicie una sesión con un servidor que requiera que el cliente se autentique, en lugar de bloquear el tráfico porque el cortafuegos no pueda descifrarlo, el cortafuegos agregará la aplicación y el servidor a la caché de exclusión local y permitirá el tráfico.

Si permite el tráfico de sitios que usan autenticación de cliente y no se encuentran en los sitios predefinidos en la lista de exclusión de descifrado SSL, cree un perfil de descifrado

© 2020 Palo Alto Networks, Inc.

que permita sesiones con autenticación de cliente. Añada el perfil a la regla de políticas de descifrado que se aplica solo a los servidores que tienen la aplicación. Para aumentar aún más la seguridad, puede requerir la autenticación multifactor para completar el proceso de inicio de sesión del usuario. También puede añadir el sitio a la lista de exclusión de descifrado SSL para omitir el descifrado sin utilizar una política de descifrado explícita.

El cortafuegos añade entradas de caché de exclusión de descifrado SSL local basadas en la política y el perfil de descifrado que controla el tráfico de la aplicación. Si no bloquea las **verificaciones de modo no admitido** en el perfil de descifrado, el cortafuegos añade entradas a la caché de exclusión de descifrado SSL local en los siguientes casos:

- El cliente solo admite TLSv1.2 y el servidor solo admite TLSv1.3. En la caché local, el motivo que se muestra para esa exclusión es SSL_UNSUPPORTED.
- El cliente admite TLSv1.3 y TLSv1.2, y el servidor solo admite TLSv1.2. En ese caso, la columna **Reason (Motivo)** muestra TLS13_UNSUPPORTED.

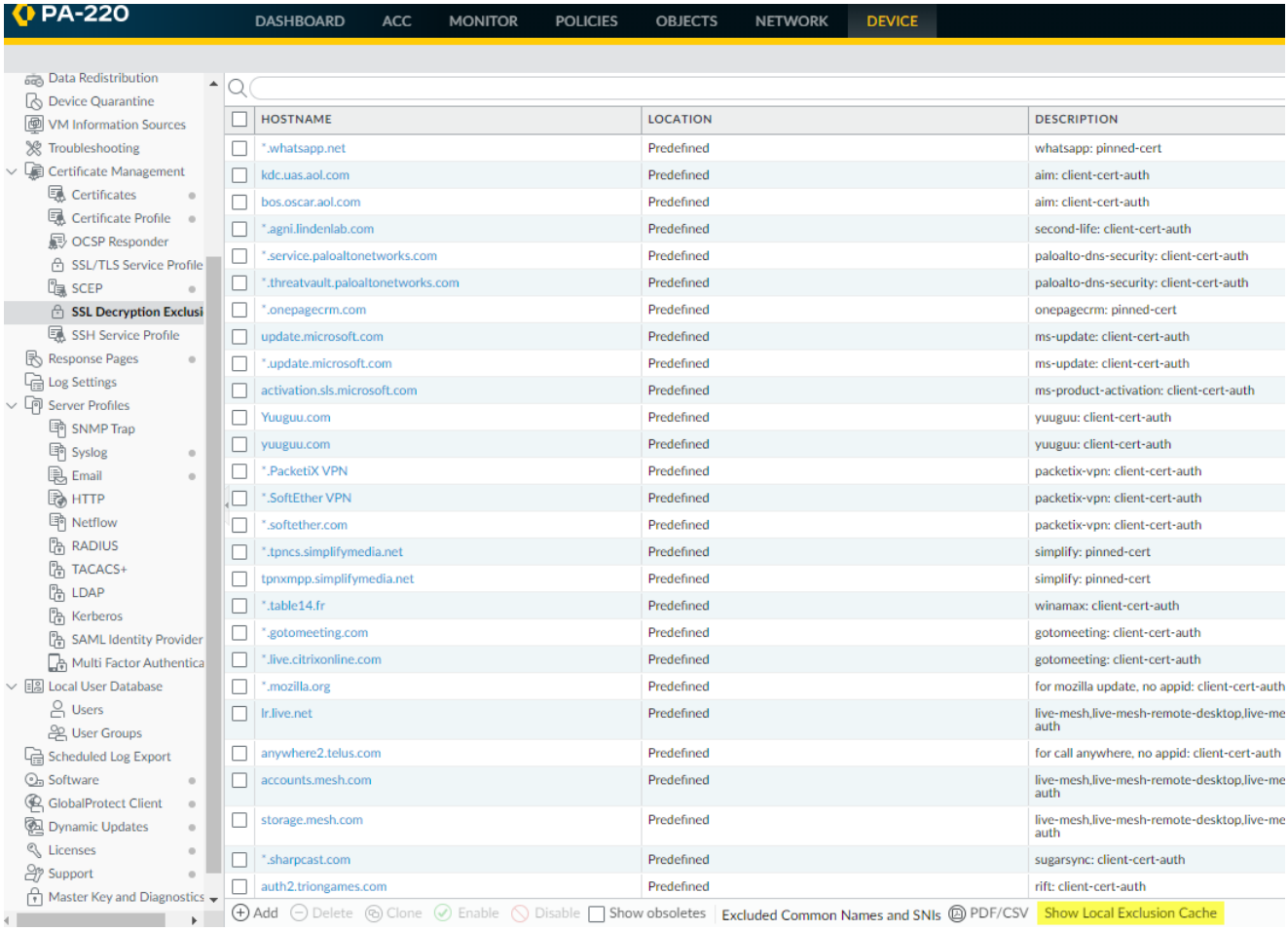
  

  Cuando el motivo para añadir un servidor a la caché de exclusión de descifrado SSL local es TLS13_UNSUPPORTED, el cortafuegos cambia el protocolo a TLSv1.2 a una versión anterior y el cortafuegos descifra e inspecciona el tráfico.
- El cliente anuncia un cifrado específico que el servidor no admite.
- El cliente anuncia una curva específica que el servidor no admite.

La caché local contiene un máximo de 1024 entradas. No puede añadir exclusiones locales a la caché de exclusión de descifrado SSL local manualmente (pero puede añadir exclusiones de descifrado a la lista de exclusión de descifrado SSL manualmente).

Debe tener acceso administrativo de superusuario o de administración de certificados para ver la caché de exclusión de descifrado SSL local. Para verlo, vaya a **Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]** y, a continuación, haga clic en **Show Local Exclusion Cache (Mostrar caché de exclusión local)** cerca de la parte inferior de la pantalla. La caché de exclusión local muestra la aplicación, el servidor, el motivo de la inclusión en la caché, el perfil de descifrado que controla el tráfico y más información para cada entrada. Puede seleccionar y eliminar entradas de la caché local manualmente.

© 2020 Palo Alto Networks, Inc.



También puede eliminar las entradas almacenadas en caché mediante la CLI:

```
clear ssl-decrypt exclude-cache [server <value>] [application <value>]
```

Si alguien intenta acceder al mismo servidor antes de que caduque la entrada de la caché local (12 horas), el cortafuegos hace coincidir la sesión con la entrada de la caché, omite el descifrado y permite el tráfico. El cortafuegos vacía la caché de exclusión local si cambia la política o el perfil de descifrado, ya que esos cambios pueden afectar la clasificación de la sesión. Si la caché se llena, el cortafuegos depura las entradas más antiguas a medida que llegan las nuevas.

Creación de una exclusión al descifrado basada en la política

Las exclusiones de descifrado basadas en políticas son para excluir el tráfico que *decide* no descifrar. Puede crear una exclusión de descifrado basada en la política sobre la base de cualquier combinación de origen, destino, servicio o categoría de URL del tráfico. Los ejemplos de tráfico que puede elegir no descifrar incluyen los siguientes:

- Tráfico que no se debe descifrar nunca porque contiene información de identificación personal u otra clase de datos confidenciales, como datos financieros, médicos, sanitarios u oficiales de las categorías de URL Filtering.
- Tráfico que tiene su origen o destino en ejecutivos u otros usuarios cuyo tráfico no se debe descifrar.
- Es posible que algunos dispositivos como los servidores financieros deban excluirse del descifrado.

© 2020 Palo Alto Networks, Inc.

- Según la empresa, algunas compañías pueden valorar la privacidad y la experiencia del usuario más que la seguridad de algunas aplicaciones.
- Las leyes o normativas locales que prohíben el descifrado de cierto tráfico.

  Un ejemplo de no descifrar tráfico por cumplimiento normativo o legal es el Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR) de la Unión Europea (UE). El GDPR de la UE exigirá una protección sólida de todos los datos personales de todos los individuos. El GDPR afecta a todas las empresas, incluidas las extranjeras, que recopilan o procesan los datos personales de los residentes en la UE.

  Las diferentes reglas de cumplimiento y normativas pueden tratar los mismos datos de manera distinta en diferentes países o regiones. Las empresas generalmente pueden descifrar información en sus centros de datos corporativos porque la empresa tiene la propiedad de la información. Lo mejor es descifrar tanto tráfico como sea posible de modo que pueda verlo y aplicar la protección de seguridad apropiada en él.

Puede usar las categorías de URL predefinidas para excluir categorías enteras de sitios web del descifrado. También puede crear categorías de URL personalizadas o listas dinámicas externas (external dynamic list, EDL) para definir listas personalizadas de URL que no desea descifrar.

En entornos como los de Office 365 que tienen direcciones IP dinámicas o en entornos donde realiza cambios frecuentes a la lista de URL que desea excluir del descifrado, con frecuencia es preferible usar una EDL en lugar de una categoría de URL para especificar las URL excluidas. El uso de las EDL trae menos problemas en los entornos dinámicos porque, cuando se editan, las categorías de URL se modifican dinámicamente, sin tener que hacer clic en **Commit (Confirmar)**; sin embargo, cuando edita las categorías de URL personalizadas, los cambios no se aplican hasta que haga clic en **Commit (Confirmar)**.

Si crea una EDL o una categoría de URL personalizada con todas las categorías que no se deben descifrar, basta una regla de la política de descifrado para regir el tráfico cifrado que desea permitir. Aplique a esa regla un perfil que impida el descifrado. Además, como tiene la posibilidad de añadir categorías a las EDL o las categorías de URL personalizadas, resulta muy sencillo excluir el tráfico del descifrado y mantener limpia la base de reglas.

Tal como hace con las reglas de la política de seguridad, el cortafuegos compara el tráfico entrante con las reglas de la política de descifrado en el orden en que aparecen en su base de reglas. Coloque las reglas de exclusión del descifrado al principio de la base de reglas para evitar que se descifre accidentalmente el tráfico confidencial o el tráfico que no se debe descifrar por motivos legales o normativos.

Si crea exclusiones de descifrado basadas en políticas, lo mejor es colocar las siguientes reglas de exclusión en lo más alto de la base de reglas de descifrado, en el siguiente orden:

1. Excepciones basadas en direcciones IP para servidores de destino confidenciales.
2. Excepciones basadas en usuarios de origen para ejecutivos y otros usuarios o grupos.
3. Excepciones basadas en EDL o URL personalizadas para URL de destino.
4. Excepciones basadas en categorías de URL predefinidas y confidenciales a las URL de destino de categorías enteras, como los datos financieros, médicos, sanitarios y oficiales.

Coloque las reglas que descifran tráfico después de estas en la base de reglas de descifrado.

STEP 1 | Excluya el tráfico de descifrado en función de los criterios coincidentes.

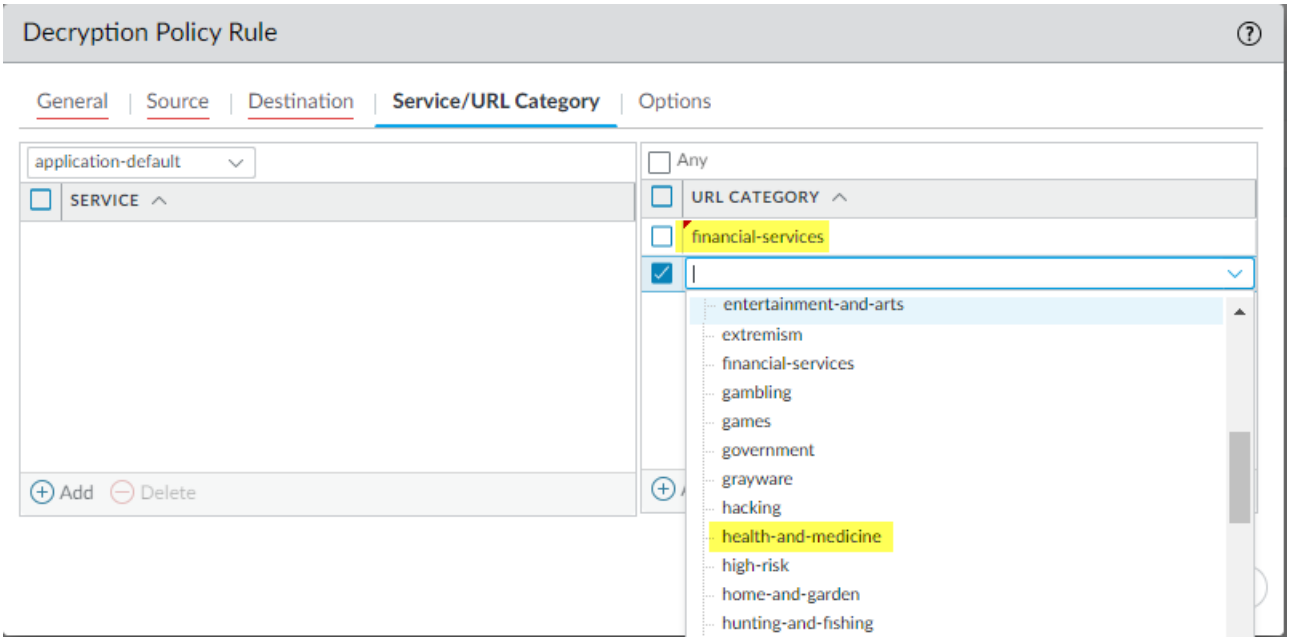
Este ejemplo muestra cómo excluir el tráfico categorizado como financiero o sanitario del descifrado del proxy SSL de reenvío.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y haga clic en **Add (Añadir)** para añadir una regla, o modifique una regla de la política de seguridad.
2. Defina el tráfico que desea excluir del descifrado.

   En este ejemplo:

   1. Otorgue a la regla un nombre descriptivo en **Name**, como No-Descifrar-Estado-Financiero.
   2. Establezca **Any (Todos)** como los valores de **Source (Origen)** y **Destination (Destino)** para aplicar la regla No-Decrypt-Finance-Health a todo el tráfico de SSL destinado a un servidor externo.
   3. Seleccione **URL Category (Categoría URL)** y **Add (Añadir)** para añadir las categorías de URL servicios-financieros y salud-y-medicina.



3. Seleccione **Options** y configure la regla en **No Decrypt**.
4. (Opcional, pero recomendado) Cree un perfil que no sea de descifrado y adjúntelo a la regla con el objetivo de validar los certificados para las sesiones que el cortafuegos no descifre. Configúrelo en **Block sessions with expired certificates (Bloquear sesiones con certificados caducados)** o **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)**.

   Excepción: No adjunte un perfil que no sea de descifrado a las políticas de descifrado para el tráfico TLSv1.3 que no descifre, ya que el cortafuegos no puede leer la información del certificado cifrado, por lo que no puede realizar comprobaciones de certificados. Sin embargo, debe crear una política de descifrado para el tráfico TLSv1.3 que no descifre, ya que el tráfico no cifrado no se registra a no ser que una política de descifrado controle ese tráfico.
5. Haga clic en **OK (Aceptar)** para guardar la política de descifrado No-Descifrar-Estado-Financiero

STEP 2 | Coloque la regla de exclusión de descifrado en la parte superior de su base de reglas de política de descifrado.

El cortafuegos aplica las reglas de descifrado en el tráfico entrante en la secuencia de la base de reglas y ejecuta la primera regla que coincide con el tráfico.

Seleccione la política **No-Decrypt-Finance-Health** (**Decryption [Descifrado]** > **Policies [Políticas]**), y haga clic en **Move Up (Mover hacia arriba)** hasta que aparezca en la parte superior de la lista, o puede arrastrar y soltar la regla.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Guarde la configuración.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Bloqueo de exportación de claves privadas

Puede bloquear permanentemente la exportación de claves privadas para certificados cuando los genera o los importa en PAN-OS o Panorama. El bloqueo de la exportación de claves privadas desde sus dispositivos PAN-OS refuerza su postura de seguridad porque evita que los administradores deshonestos u otros actores maliciosos hagan un mal uso de las claves. Los administradores con funciones que incluyen la gestión de certificados pueden bloquear la exportación de claves privadas. No puede bloquear claves que ya existen en un dispositivo; solo puede bloquear claves en el momento en que las genera o las importa en PAN-OS.

Si un administrador bloquea la exportación de una clave privada, ningún administrador podrá exportar esa clave, ni siquiera los administradores de superusuario. Si necesita exportar una clave privada desde un dispositivo PAN-OS, vuelva a generar el certificado y la clave sin seleccionar la opción para bloquear la exportación de la clave privada.

Para cambiar a una versión anterior de PAN-OS, primero debe eliminar los certificados cuyas claves privadas estén bloqueadas. Si no los elimina antes de intentar cambiar a una versión anterior, aparecerá un mensaje de error en el que se le solicitará que elimine esos certificados. No podrá cambiar a una versión anterior hasta que los elimine. Después de cambiar a una versión anterior, vuelva a importar o regenere los certificados eliminados si los necesita.



Si utiliza una infraestructura de clave pública (PKI) empresarial para generar certificados y claves privadas, bloquee la exportación de claves privadas, ya que puede instalarlas en nuevos cortafuegos y Panorama desde la entidad de certificación (CA) de su empresa, por lo que no hay ningún motivo para realizar la exportación a partir de PAN-OS.

Si genera certificados autofirmados en el cortafuegos o Panorama y aplica la opción de bloqueo de la exportación de la clave privada, no podrá exportar el certificado y la clave a otros dispositivos PAN-OS.

Puede exportar e importar el estado del dispositivo (**Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**) incluso si bloquea la exportación de claves privadas. Incluimos las claves privadas en device state imports and exports (importaciones y exportaciones del estado del dispositivo), pero los administradores no pueden leerlas ni decodificarlas.



Puede importar o cargar la configuración de un cortafuegos en otro cortafuegos si la clave maestra es la misma en ambos cortafuegos. Si la clave maestra es diferente en los cortafuegos, la importación o carga de la configuración no funciona y se produce un error en la confirmación al leer los certificados.

- Generación de una clave privada y su bloqueo
- Importación de una clave privada y su bloqueo
- Importación de una clave privada para la puerta de enlace de IKE y su bloqueo
- Verificación del bloqueo de la clave privada

Generación de una clave privada y su bloqueo

Bloquee la exportación de una clave privada para evitar su uso incorrecto después de generar un certificado.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

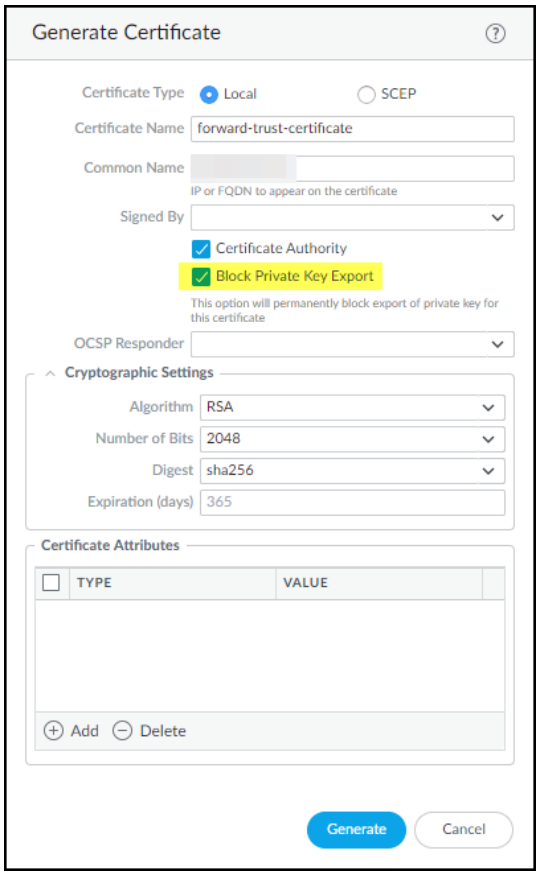
© 2020 Palo Alto Networks, Inc.

Si hay más de un sistema virtual, seleccione una ubicación en **Location (Ubicación)** o la opción **Shared (Compartido)** para el certificado.

STEP 2 | Seleccione **Generar** el certificado.

STEP 3 | Seleccione **Block Private Key Export (Bloquear exportación de claves privadas)** para evitar que alguien exporte el certificado.

Consulte Generación de un certificado para obtener información sobre los otros campos del certificado.



STEP 4 | Haga clic en **Generar** para generar el nuevo certificado.

También puede generar un certificado y bloquear su clave privada para que no se exporte mediante el comando operativo de la CLI:

```
admin@pa-220> request certificate generate block-private-keys yes
```

El comando de la CLI anterior también puede incluir el certificado y otros parámetros que no se muestran.

Importación de una clave privada y su bloqueo

Bloquee la exportación de una clave privada para evitar su uso incorrecto después de importar un certificado.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.

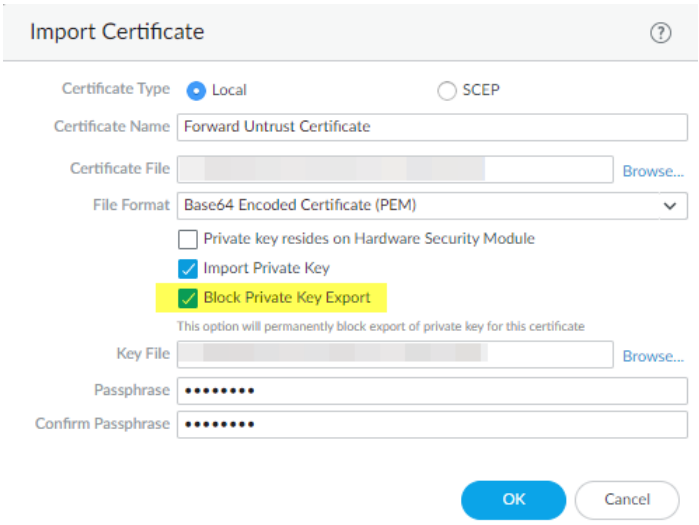
Si hay más de un sistema virtual, seleccione una ubicación en **Location (Ubicación)** o la opción **Shared (Compartido)** para el certificado.

STEP 2 | **Importe** el certificado.

STEP 3 | Seleccione **Import Private Key (Importar clave privada)** para activar la opción de bloquear la exportación de claves privadas.

STEP 4 | Seleccione **Block Private Key Export (Bloquear exportación de claves privadas)** para evitar que alguien exporte el certificado.

Consulte Importación de un certificado y una clave privada para obtener información sobre otros campos de importación de certificados.



STEP 5 | Haga clic en **OK (ACEPTAR)** para importar el certificado.

Si utiliza el comando de la CLI operativa de SCP para importar un certificado o para importar una clave privada para un certificado, puede bloquear aún la exportación de la clave privada:

- ***admin@pa-220> scp import private-key block-private-key ...***

Los comandos de la CLI anteriores también pueden incluir palabras clave para especificar el origen, el nombre del certificado y otros parámetros que no se muestran.

*Si utiliza el comando de la CLI operativa de SCP para exportar un certificado e incluir su clave privada (**scp export certificate passphrase <phrase> remote-port <1-65536> to <destination> certificate-name <name> include-key <yes | no> format <der | pem | pkcs10 | pkcs12>**), y si la clave privada del certificado está bloqueada, el comando falla y devuelve un mensaje de error porque no puede exportar una clave privada bloqueada.*

© 2020 Palo Alto Networks, Inc.

Importación de una clave privada para la puerta de enlace de IKE y su bloqueo

Bloquee la exportación de una clave privada para evitar su uso incorrecto después de generar un certificado para la autenticación de puerta de enlace de IKE.

STEP 1 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)**.

STEP 2 | **Añada** una nueva puerta de enlace IKE.

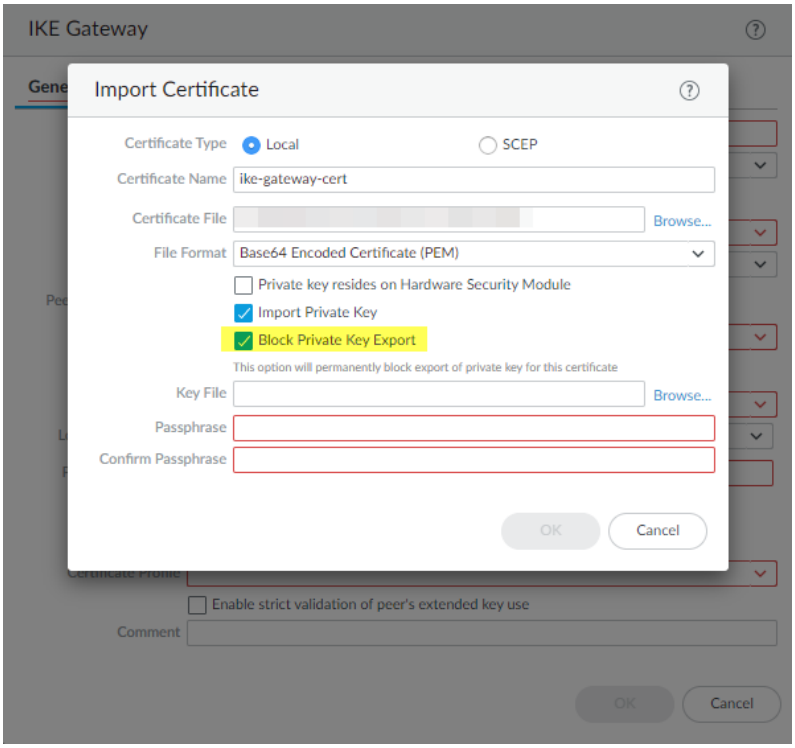
STEP 3 | En la pestaña **General**, para **Authentication (Autenticación)**, seleccione **Certificate (Certificado)**.

STEP 4 | Para **Local Certificate (Certificado local)**, seleccione **Import (Importar)** o **Generate (Generar)** según desee importar un certificado existente o crear uno.

STEP 5 | Introduzca la información del certificado. Si está importando el certificado, seleccione **Import Private Key (Importar clave privada)** para activar la casilla de verificación **Block Private Key Export (Bloquear exportación de claves privadas)**.

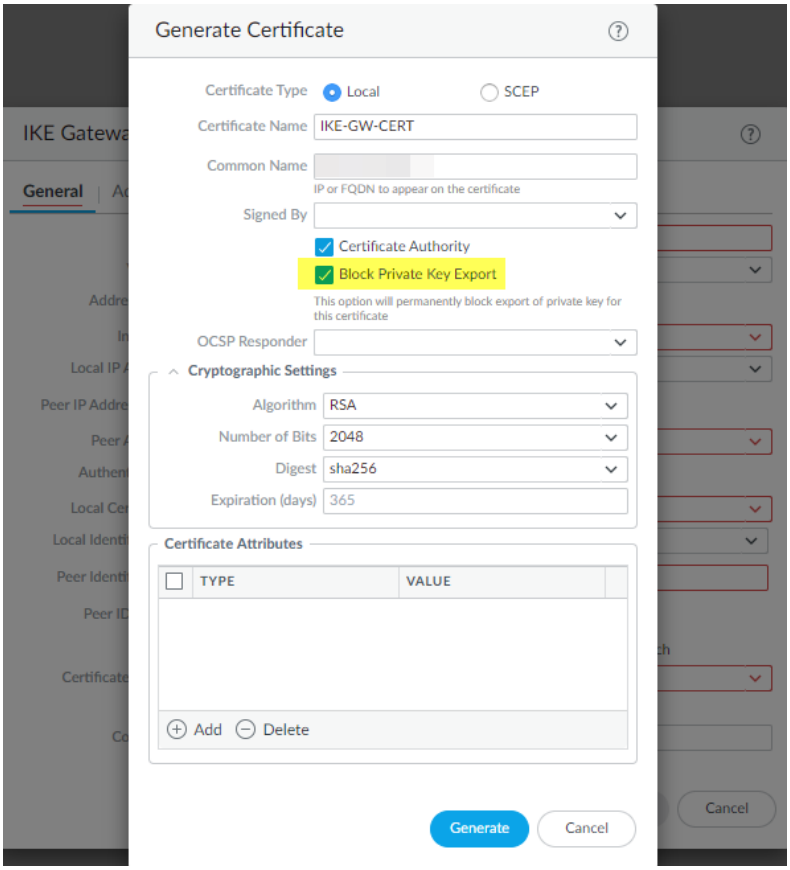
STEP 6 | Seleccione **Block Private Key Export (Bloquear exportación de claves privadas)** para evitar que alguien exporte la clave.

Para importar un certificado, especifique y confirme la **frase de contraseña** y, a continuación, haga clic en **OK (Aceptar)**



Para generar un certificado, haga clic en **Generate (Generar)**.

© 2020 Palo Alto Networks, Inc.



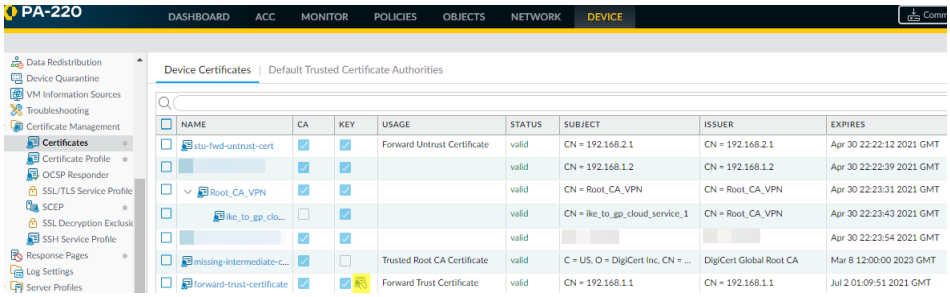
STEP 7 | Especifique la **frase de contraseña**, confírmela y, a continuación, haga clic en **OK (Aceptar)**.

Verificación del bloqueo de la clave privada

Puede verificar si se bloquea la exportación de una clave privada de varias formas.

- Meditante la comprobación de la columna **Key (Clave)** en **Device (Dispositivo)** > **Certificate Management (Gestión de dispositivos)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**.

  En este ejemplo, el certificado de confianza de reenvío está bloqueado:



- Si intenta exportar un certificado cuya clave privada está bloqueada para la exportación, la casilla de verificación **Export Private Key (Exportar clave privada)** no estará disponible y no podrá exportar la clave. Solo podrá exportar el certificado.

© 2020 Palo Alto Networks, Inc.

- Utilice el siguiente comando operativo de la CLI para ver todos los certificados en el dispositivo o en un vsys determinado que tenga claves privadas bloqueadas para la exportación:

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

- Utilice el siguiente comando operativo de la CLI para verificar si la clave privada de un certificado determinado está bloqueada para la exportación:

```
admin@pa-220> request certificate is-blocked certificate-name <name>
```

  Si se bloquea la exportación del certificado, el comando devuelve **yes (sí)** y si el certificado no está bloqueado, el comando devuelve **no**.

© 2020 Palo Alto Networks, Inc.

Permisos para que los usuarios excluyan el descifrado SSL

En situaciones de confidencialidad de la privacidad, es posible que desee alertar a sus usuarios que el cortafuegos está descifrando determinado tráfico web y permitirles continuar en el sitio entendiendo que su tráfico está descifrado o finalizar la sesión y bloquear la entrada al sitio. (No hay una opción para visitar el sitio y también evitar el descifrado).

La primera vez que un usuario intente explorar un sitio HTTPS o una aplicación que coincida con la política de descifrado, el cortafuegos mostrará una página de respuesta que notifica al usuario que la sesión va a descifrarse. Los usuarios pueden permitir el descifrado y acceder a la página haciendo clic en **Yes (Sí)** o excluir el descifrado haciendo clic en **No** y finalizar la sesión. La elección de permitir el descifrado se aplica a todos los sitios HTTPS a los que los usuarios intenten acceder en las próximas 24 horas, después de lo cual el cortafuegos vuelve a mostrar la página de respuesta. Los usuarios que opten por excluir el descifrado SSL no podrán acceder a la página web solicitada ni a ningún otro sitio HTTPS durante un minuto. Una vez transcurrido el minuto, el cortafuegos vuelve a mostrar la página de respuesta la próxima vez que los usuarios intentan acceder a un sitio HTTPS.

El cortafuegos incluye una página de exclusión del descifrado SSL predefinida que puede habilitar. También puede personalizar la página con su propio texto o imágenes. Sin embargo, lo mejor es no permitir a los usuarios que excluyan el descifrado.

Las páginas de respuesta personalizadas más grandes que el tamaño máximo admitido no se descifran ni muestran a los usuarios. En PAN-OS 8.1.2 y versiones anteriores de PAN-OS 8.1, las páginas de respuesta personalizadas en un sitio descifrado no pueden superar los 8191 bytes; el tamaño máximo se aumenta a 17 999 bytes en PAN-OS 8.1.3 y versiones posteriores.

STEP 1 | (Opcional) Personalizar la página de exclusión del descifrado SSL

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el enlace **Página de exclusión de descifrado de SSL**.
3. Seleccione la página **Predefinido** y haga clic en **Exportar**.
4. Con el editor de textos de HTML que prefiera, edite la página.
5. Si desea añadir una imagen, aloje la imagen en un servidor web accesible desde sus sistemas de usuario final.
6. Añada una línea al HTML para señalar la imagen. Por ejemplo:

```
<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?1382722588"/>
```

7. Guarde la imagen editada con un nuevo nombre de archivo. Asegúrese de que la página conserva su codificación UTF-8.
8. De nuevo en el cortafuegos, seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
9. Seleccione el enlace **Página de exclusión de descifrado de SSL**.
10. Haga clic en **Import (Importar)** y, a continuación, introduzca la ruta y el nombre de archivo en el campo **Import File (Importar archivo)** o **Browse (Examinar)** para encontrar el archivo.
11. (Opcional) Seleccione el sistema virtual en el que se debe usar esta página de inicio de sesión en la lista desplegable **Destination (Destino)** o seleccione shared (compartido) para que esté disponible para todos los sistemas virtuales.

© 2020 Palo Alto Networks, Inc.

12. Haga clic en **OK (Aceptar)** para importar el archivo.
13. Seleccione la página de respuesta que acaba de importar y haga clic en **Close (Cerrar)**.

STEP 2 | Active la exclusión de descifrado SSL

1. En la página **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**, haga clic en el enlace **Disabled (Deshabilitado)**.
2. Seleccione **Página de exclusión de SSL** y haga clic en **ACEPTAR**.
3. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 3 | Compruebe que la página de exclusión aparece cuando intenta desplazarse a un sitio.

Desde un navegador, vaya a un sitio cifrado que coincida con su política de descifrado.

Compruebe si se muestra la nueva página de respuesta de exclusión de descifrado SSL.



© 2020 Palo Alto Networks, Inc.

Deshabilitación temporal del descifrado SSL

En algunos casos puede que desee deshabilitar temporalmente el descifrado SSL. Por ejemplo, si implementó el descifrado SSL de manera muy precipitada y algo no funciona correctamente pero no está seguro qué puede ser y tiene muchas reglas para examinar, puede usar la CLI para desactivar de manera temporal el descifrado y tomarse el tiempo necesario para analizar y resolver el problema. Después de solucionar el problema, puede usar la CLI para volver a activar el descifrado SSL. Debido a que deshabilitar temporalmente y volver a habilitar el descifrado con la CLI no requiere una operación de confirmación, puede hacerlo sin interrumpir el tráfico de red.

Los siguientes comandos de CLI deshabilitan temporalmente y vuelven a habilitar el descifrado sin una confirmación.



El comando para deshabilitar el descifrado SSL no persiste en la configuración después de reiniciar. Si desactiva el descifrado de manera temporal y luego reinicia el cortafuegos, independientemente de si el problema se resolvió, el descifrado se vuelve a activar.

- Deshabilitación del descifrado SSL

```
set system setting
ssl-decrypt skip-ssl-decrypt yes
```

- Rehabilitación del descifrado SSL

```
set system setting
ssl-decrypt skip-ssl-decrypt no
```


© 2020 Palo Alto Networks, Inc.

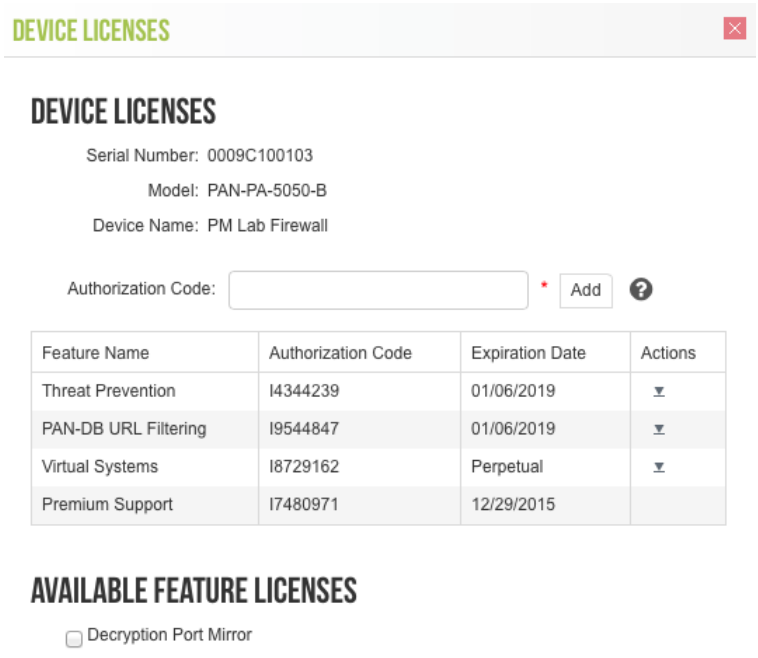
Configuración del reflejo del puerto de descifrado

Antes de que pueda habilitar el Decryption Mirroring (Reflejo de descifrado), debe obtener e instalar una licencia de reflejo del puerto de descifrado. La licencia es gratuita y puede habilitarse a través del portal de asistencia técnica como se describe en el siguiente procedimiento. Después de instalar la licencia de reflejo del puerto de descifrado y reiniciar el cortafuegos, puede habilitar el reflejo del puerto de descifrado.

Tenga en cuenta que el descifrado, almacenamiento, inspección y uso del tráfico SSL está regulado en algunos países y puede que sea necesario tener el consentimiento del usuario para poder usar la función de reflejo del cifrado. Además, el uso de esta función podría hacer que usuarios maliciosos con accesos administrativos al cortafuegos recopilaran nombres de usuario, contraseñas, números de la seguridad social, números de tarjetas de crédito u otra información sensible para enviarla a través de un canal cifrado. Palo Alto Networks le recomienda consultar a su asesor corporativo antes de habilitar y utilizar esta función en un entorno de producción.

STEP 1 | Solicite una licencia para cada cortafuegos en el que desee habilitar el reflejo del puerto de descifrado.

1. Inicie sesión en el sitio web de Asistencia técnica de Palo Alto Networks y desplácese a la pestaña **Assets (Activos)**.
2. Seleccione la entrada para el cortafuegos para el que desea obtener una licencia y seleccione **Actions**.
3. Seleccione **Reflejo de puerto de descifrado**. Aparecerá un aviso legal.
4. Si está de acuerdo con los requisitos y las posibles implicaciones legales, y desea configurar el reflejo de puerto de descifrado, haga clic en **I understand and wish to proceed (Comprendo las condiciones y deseo continuar)**.
5. Haga clic en **Activate (Activar)**.



STEP 2 | Instale la licencia de reflejo del puerto de descifrado en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

1. Desde la interfaz web del cortafuegos, seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Haga clic en **Recuperar claves de licencia del servidor de licencias**.
3. Verifique que la licencia se ha activado en el cortafuegos.



4. Reinicie el cortafuegos (**Device [Dispositivo]** > **Setup [Configuración]** > **Operations [Operaciones]**). Esta función no estará disponible para su configuración hasta que no vuelva a cargarse PAN-OS.

STEP 3 | Habilite el cortafuegos para que reenvíe tráfico descifrado. Se necesitan permisos de superusuario para realizar este paso.

En un cortafuegos con un único sistema virtual:

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.
2. Seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.
3. Haga clic en **OK (Aceptar)** para guardar.

En un cortafuegos con varios sistemas virtuales:

1. Seleccione **Device (Dispositivo)** > **Virtual System (Sistema virtual).**
2. Seleccione un sistema virtual para su edición o cree un nuevo sistema virtual seleccionando **Añadir**.
3. Seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.
4. Haga clic en **OK (Aceptar)** para guardar.

STEP 4 | Habilite una interfaz Ethernet que se usará para el reflejo de descifrado.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Seleccione la interfaz Ethernet que quiera configurar para el reflejo del puerto de descifrado.
3. Seleccione Reflejo de descifrado como el Tipo de interfaz.

   Este tipo de interfaz solo aparece si la licencia de Reflejo de puerto de descifrado está instalada.
4. Haga clic en **OK (Aceptar)** para guardar.

STEP 5 | Habilite el reflejo de tráfico descifrado.

1. Seleccione **Objects (Objetos)** > **Decryption Profile (Perfil de descifrado)**.
2. Seleccione una interfaz en **Interface**, que se usará para el **reflejo de descifrado**.

   El menú desplegable Interfaz contiene todas las interfaces Ethernet que se han definido como el tipo: **Reflejo de descifrado**.
3. Especifique si desea reflejar el tráfico descifrado antes o después de aplicar las políticas.

   De manera predeterminada, el cortafuegos reflejará todo el tráfico descifrado en la interfaz antes de la búsqueda de políticas de seguridad, lo que le permitirá reproducir eventos y analizar el tráfico que genere una amenaza o active una acción de descarte. Si solamente desea reflejar el tráfico descifrado después de aplicar las políticas de seguridad, seleccione la casilla de verificación Reenviado solo. Con esta opción, solamente se reflejará el tráfico reenviado a través del cortafuegos. Esta opción es de utilidad si está reenviando el tráfico descifrado a otros dispositivos de detección de amenazas, como un dispositivo de DLP u otro sistema de prevención de intrusiones (IPS).
4. Haga clic en **OK (Aceptar)** para guardar el perfil de descifrado.

STEP 6 | Adjunte la regla de perfiles de descifrado (con el reflejo de puerto de descifrado habilitado) a una regla de políticas de descifrado. Se reflejará todo el tráfico descifrado en función de la regla de políticas.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)**.
2. Haga clic en **Añadir** para configurar una política de descifrado o seleccione una política de descifrado existente para editarla.
3. En la pestaña **Options (Opciones)**, seleccione **Decrypt (Descifrado)** y el **Decryption Profile (Perfil de descifrado)** creado en el paso 4.
4. Haga clic en **OK (Aceptar)** para guardar la política.

STEP 7 | Guarde la configuración.

Haga clic en **Commit (Confirmar)**.

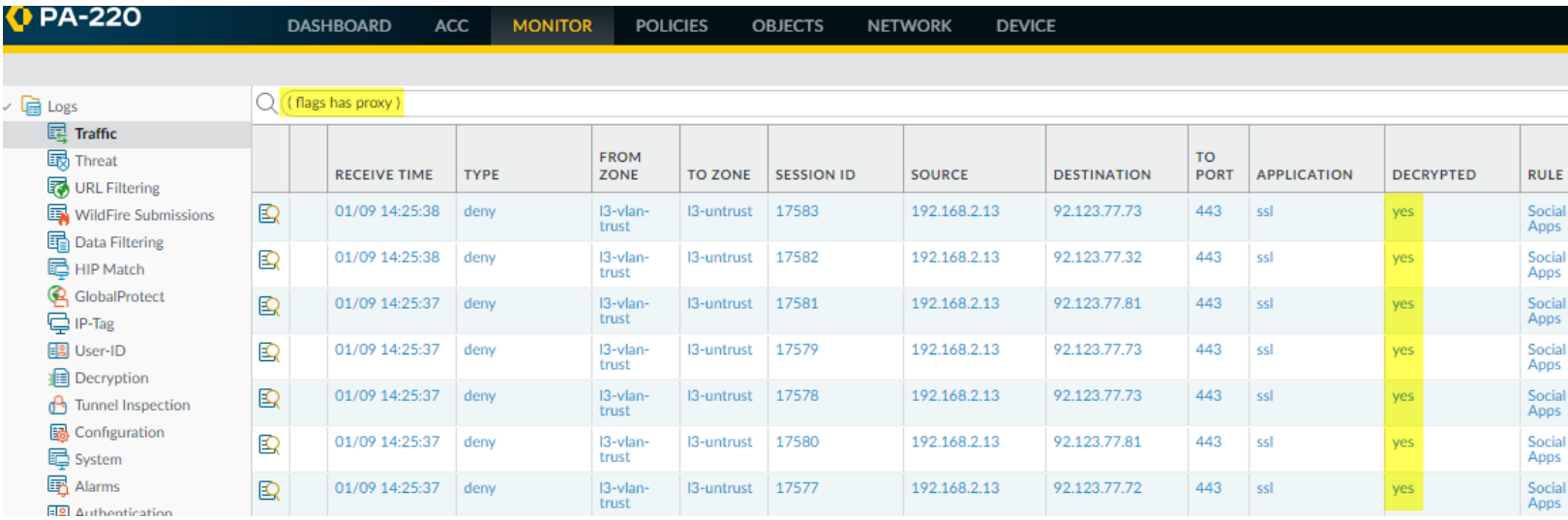
© 2020 Palo Alto Networks, Inc.

Verificación de descifrado

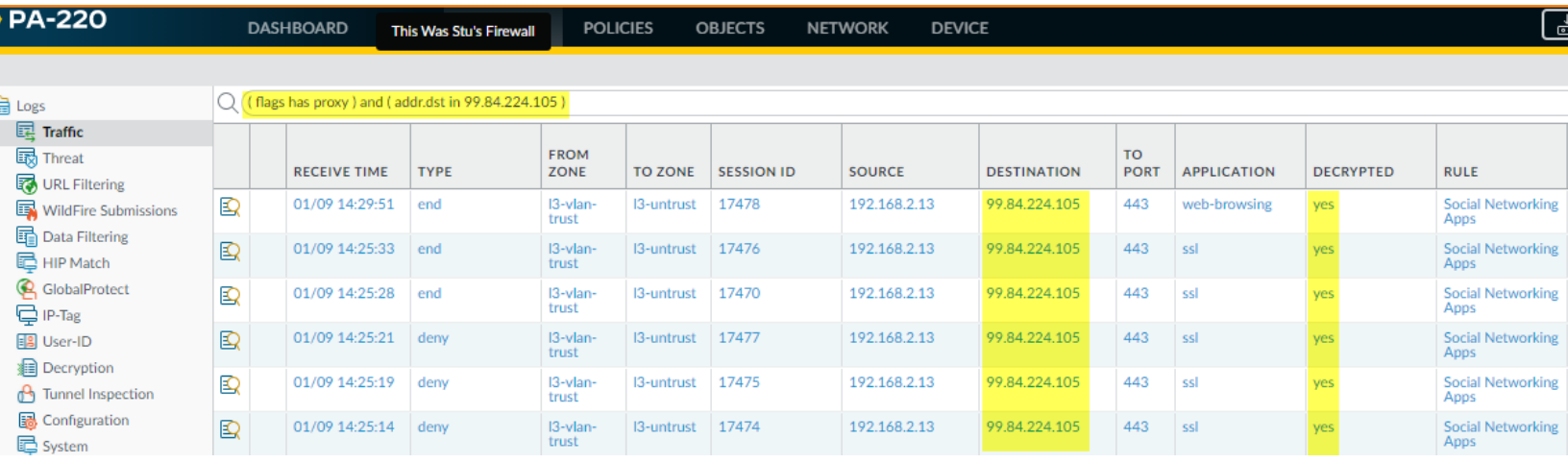
Después de configurar un perfil de descifrado recomendado y aplicarlo al tráfico, puede verificar tanto los logs de descifrado (introducidos en PAN-OS 10.0) como los logs de tráfico para verificar que el cortafuegos está descifrando el tráfico que quiere descifrar y no tráfico que no desea descifrar. Este tema le muestra cómo verificar el descifrado mediante logs de tráfico. Además, siga las recomendaciones de descifrado posteriores a la implementación para mantener la implementación.

- **Ver sesiones de tráfico descifrado:** filtre los logs de tráfico (**Monitor [Supervisar]** > **Logs [Logs]** > **Traffic [Tráfico]**) con el filtro `( flags has proxy )`.

  Este filtro muestra solo los logs en los que está activado el marcador de proxy SSL, es decir, solo el tráfico descifrado; cada entrada de log tiene el valor "yes" (sí) en la columna **Decrypted (Descifrado)**.



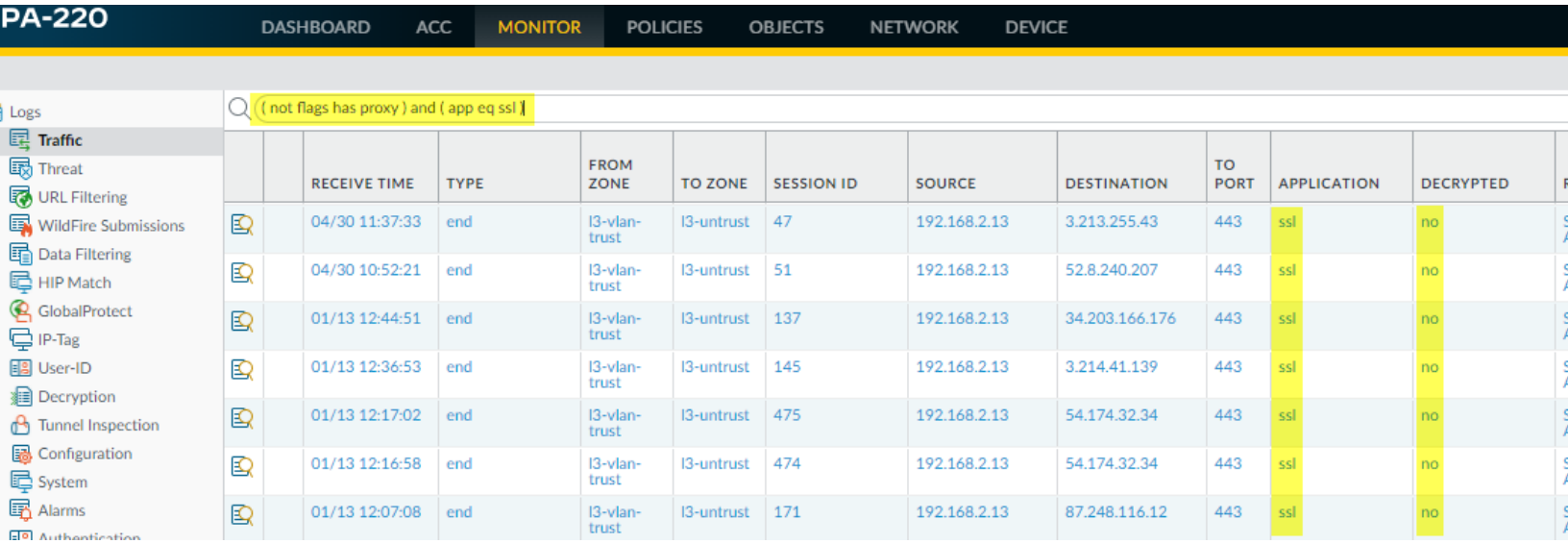
Puede filtrar el tráfico de una manera más detallada añadiendo más términos al filtro. Por ejemplo, puede filtrar el tráfico descifrado que va solo a la dirección IP de destino 99.84.224.105 añadiendo el filtro `( addr.dst in 99.84.224.105 )`:



© 2020 Palo Alto Networks, Inc.

- **Ver sesiones de tráfico SSL que no están descifradas**: filtre los logs de tráfico (**Monitor [Supervisión]** > **Logs** > **Traffic [Tráfico]**) con el filtro `(not flags has proxy) y (app eq ssl)`.

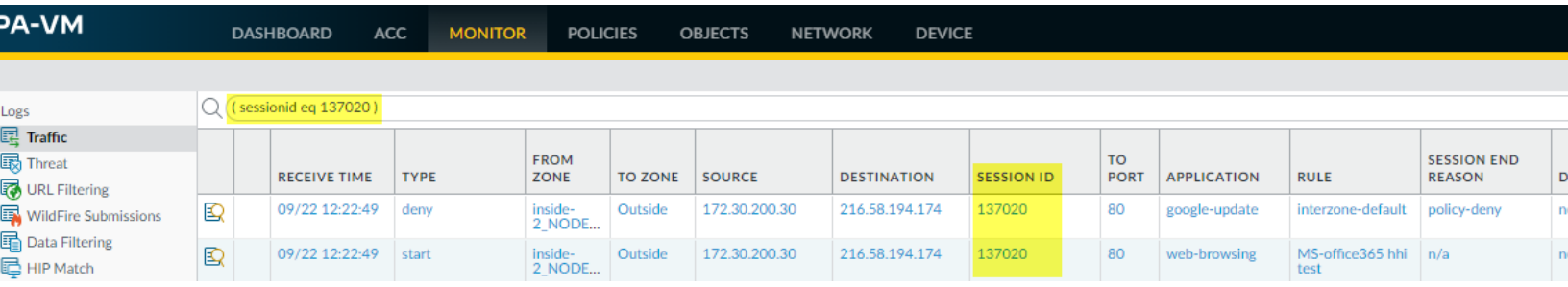
  Este filtro muestra solo los logs en los que el marcador de proxy SSL está desactivado (es decir, solo el tráfico cifrado) y el tráfico es tráfico SSL; cada entrada de log tiene el valor **no** en la columna **Decrypted (Descifrado)** y el valor **ssl** en la columna **Application (Aplicación)**.



De forma similar al ejemplo, para ver los logs de tráfico descifrado, puede añadir términos para filtrar el tráfico que no descifra de una manera más detallada.

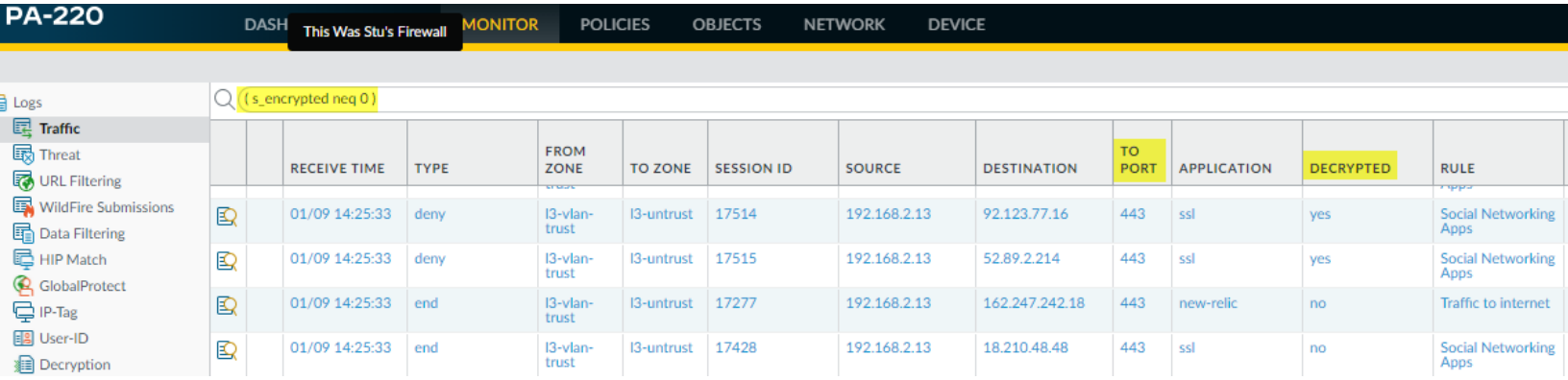
- **Ver el log de una sesión determinada:** para ver el log de tráfico de una sesión determinada, filtre por el ID de la sesión.

  Por ejemplo, para ver el log de una sesión con el ID 137020, filtre con el término `(sessionid eq 137020)`. Puede encontrar el número de ID en la columna Session ID (ID de sesión) en el resultado del log, como se muestra en las pantallas anteriores. Si no se muestra la columna Session ID (ID de sesión), añada la columna al resultado.

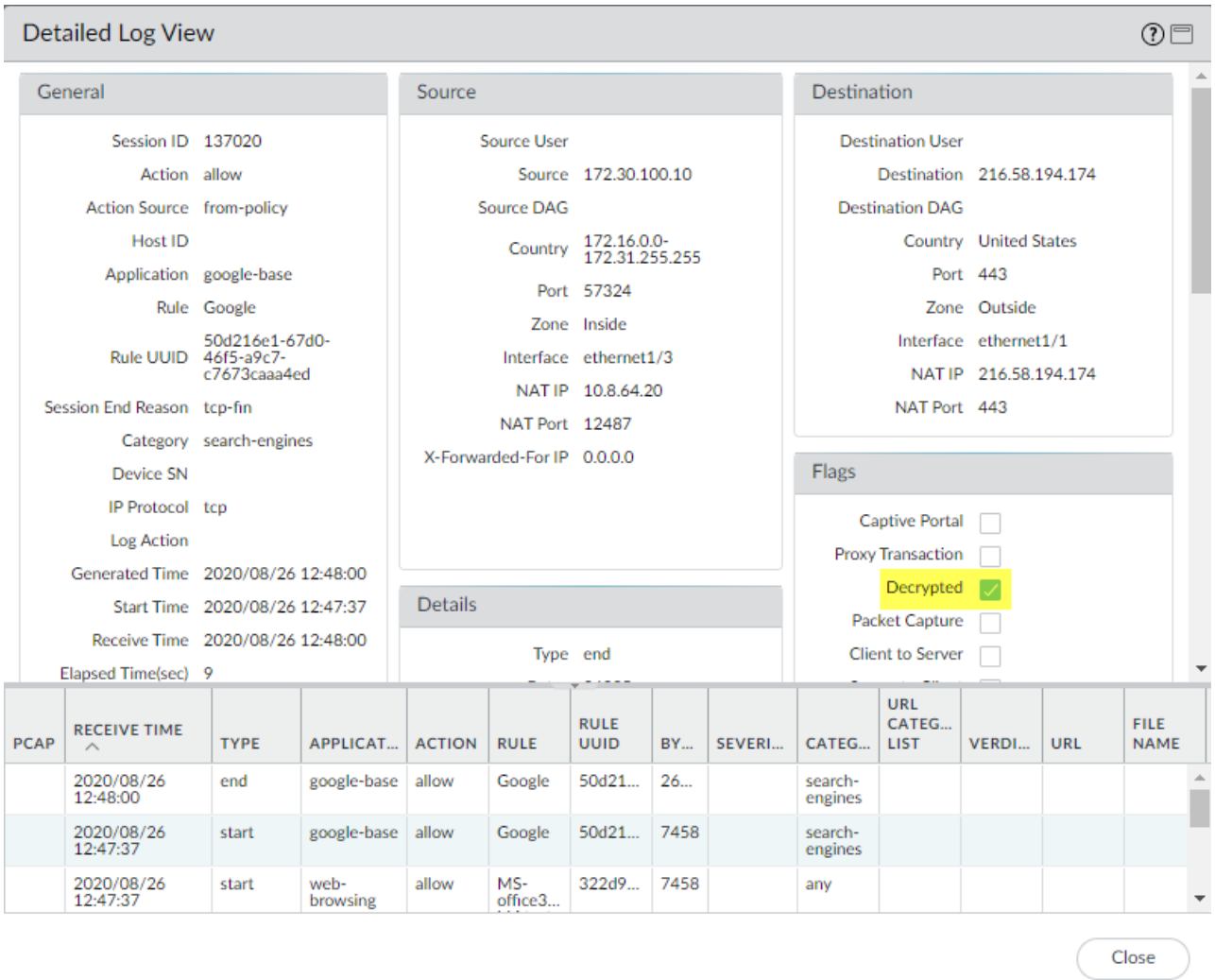


- **View All TLS and SSH Traffic (Ver todo el tráfico TLS y SSH)**: filtre los logs de tráfico (**Monitor [Supervisar]** > **Logs** > **Traffic [Tráfico]**) para ver el tráfico TLS y SSH cifrado y sin descifrar. Utilice el filtro `( s_encrypted neq 0 )`:

© 2020 Palo Alto Networks, Inc.



- **Desglosar detalles:** para ver más información sobre una entrada de log determinada, haga clic en la lupa para ver los detalles del log. Por ejemplo, para el ID de sesión 137020 (mostrado en el punto anterior), el log detallado luce de esta manera:



La casilla de la marca de **Decrypted (Descifrado)** proporciona una segunda manera de verificar si se descifró el tráfico.

© 2020 Palo Alto Networks, Inc.

También puede realizar capturas de paquetes anteriores y posteriores del tráfico descifrado para ver cómo procesa el cortafuegos el tráfico SSL y realiza acciones en los paquetes, o lleva a cabo una inspección detallada del paquete.

© 2020 Palo Alto Networks, Inc.

Solución de problemas y supervisión del descifrado

Las herramientas de resolución de problemas ofrecen una visibilidad mejorada del tráfico TLS para que pueda supervisar su implementación de descifrado. Las herramientas le permiten diagnosticar y resolver problemas de descifrado rápida y fácilmente, reforzar las debilidades en su implementación de descifrado y solucionar problemas de descifrado para mejorar su estrategia de seguridad. Por ejemplo, puede realizar las siguientes tareas:

- Identificar el tráfico que causa fallos de descifrado por identificación de nombre de servicio (SNI, Service Name Identification) y aplicación.
- Identificar el tráfico que utiliza protocolos y algoritmos débiles.
- Examinar la actividad de descifrado correcta e incorrecta en la red.
- Ver información detallada sobre sesiones individuales.
- Hacer uso del descifrado de perfiles y patrones
- Supervisar estadísticas e información detalladas de descifrado sobre adopción, fallos, versiones, algoritmos, etc.

Las siguientes herramientas ofrecen visibilidad completa del protocolo de enlace TLS y lo ayudan a solucionar problemas y supervisar su implementación de descifrado:

- **ACC** > **SSL Activity (Actividad SSL)**: los cinco widgets ACC en esta pestaña (introducidos en PAN-OS 10.0) ofrecen detalles sobre la actividad de descifrado correcta y no correcta en su red, incluidos los fallos de descifrado, las versiones de TLS, los intercambios de claves y la cantidad y el tipo de tráfico descifrado y no cifrado.
- **Monitor (Supervisor)** > **Logs** > **Decryption (Descifrado)**: el log de descifrado (introducido en PAN-OS 10.0) proporciona información completa sobre sesiones individuales que coincida con una política de descifrado (utilice una política de no descifrado para el tráfico que no descifre) y sobre las sesiones de GlobalProtect cuando habilite el log de descifrado en la configuración del portal de GlobalProtect o de las puertas de enlace de GlobalProtect. Seleccione qué columnas mostrar para ver información, como aplicación, SNI, nombre de política de descifrado, índice de error, versión de TLS, versión de intercambio de claves, algoritmo de cifrado, tipos de claves de certificado y muchas otras características. Filtre la información en columnas para identificar el tráfico que utiliza versiones y algoritmos de TLS particulares, errores particulares o cualquier otra característica que desee investigar. De manera predeterminada, las políticas de descifrado registran solo los protocolos de enlace TLS incorrectos. Dependiendo del almacenamiento de log disponible, puede configurar las políticas de descifrado para registrar también los protocolos de enlace TLS correctos.
- **Local Decryption Exclusion Cache (Caché de exclusión de descifrado local)**: hay dos construcciones para los sitios que rompen el descifrado por razones técnicas como la autenticación del cliente o los certificados fijados y, por lo tanto, deben excluirse del descifrado: la lista de exclusión de descifrado SSL y la caché de exclusión de descifrado local. La lista de exclusión de descifrado SSL contiene los sitios que Palo Alto Networks ha identificado que rompen técnicamente el descifrado. Las actualizaciones de contenido mantienen la lista actualizada y puede añadir sitios a la lista manualmente. La caché de exclusión de descifrado local añade automáticamente sitios que los usuarios locales detecta que rompen el descifrado por razones técnicas y los excluye del descifrado, siempre que el perfil de descifrado aplicado al tráfico permita modos no admitidos (si los modos no admitidos están bloqueados, el tráfico se bloquea en lugar de añadirse a la caché local).
- **Custom Report Templates for Decryption (Plantillas de informes personalizados para descifrado)**: puede crear informes personalizados (**Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**) mediante cuatro plantillas predefinidas que resumir la actividad de descifrado (introducido en PAN-OS 10.0).

© 2020 Palo Alto Networks, Inc.

La metodología general de resolución de problemas es utilizar los nuevos widgets ACC para identificar el tráfico que causa problemas de descifrado y, a continuación, utilizar el nuevo log de descifrado y las plantillas de informes personalizados para profundizar en los detalles y obtener contexto sobre ese tráfico, lo que le permite diagnosticar problemas con precisión y mucho más fácilmente que en el pasado. Comprender los problemas de descifrado y sus causas le permite seleccionar la forma adecuada de solucionar cada problema, como:

- Modificar las reglas de la política de descifrado (una regla de política define el tráfico al que afecta la regla, la acción realizada en ese tráfico, la configuración del log y el perfil de descifrado aplicado al tráfico)
- Modificar los perfiles de descifrado (protocolos y algoritmos aceptables para el tráfico que define una regla de política de descifrado, además de comprobaciones de fallos, comprobaciones de modo no admitido para elementos como cifrados y versiones no admitidos, comprobaciones de certificados, etc.)
- Agregar sitios que rompen el descifrado por razones técnicas en la lista de exclusión de descifrado SSL
- Evalúe las decisiones de seguridad sobre los sitios a los que sus empleados, clientes y socios realmente necesitan acceder y determine qué sitios puede bloquear cuando estos utilicen protocolos o algoritmos de descifrado débiles.

Los objetivos deben poder descifrar todo el tráfico que pueda descifrar (se trata de una práctica recomendada de descifrado) para que pueda inspeccionarlo y gestionar correctamente el tráfico que no descifre.

Cuando actualiza PAN-OS 10.0, el dispositivo ocupa el 1 % del espacio de log y lo asigna a los logs de descifrado. El paso 3 en Configuración de logs de descifrado le muestra cómo modificar la asignación de espacio de log para proporcionar más espacio para los logs de descifrado.

Si cambia de PAN-OS 10.0 o posterior a PAN-OS 9.1 o anterior, las funciones introducidas en PAN-OS 10.0 (log de descifrado, widgets de actividad SSL en el ACC y plantillas de descifrado de informes personalizados) se eliminan de la interfaz de usuario. Las referencias a los logs de descifrado también se eliminan de los perfiles de reenvío de logs. Además, la caché de exclusión de descifrado local solo se puede ver mediante la CLI en PAN-OS 9.1 y versiones anteriores (PAN-OS 10.0 añadió la caché local a la interfaz de usuario).

Si envía configuraciones de Panorama en PAN-OS 10.0 o posterior a dispositivos que ejecutan PAN-OS 9.1 o anterior, Panorama elimina las funciones introducidas en PAN-OS 10.0.

- Widgets del Centro de control de aplicaciones de descifrado
- Log de descifrado
- Plantillas de informes personalizados de descifrado
- Ejemplos de flujo de trabajo de solución de problemas de descifrado

Widgets del Centro de control de aplicaciones de descifrado

Los widgets del Centro de control de aplicaciones (ACC, Application Command Center) para el descifrado (**ACC** > **SSL Activity [Actividad SSL]**) introducidos en PAN-OS 10.0 funcionan con Log de descifrado para ayudarlo a diagnosticar y resolver problemas de descifrado rápida y fácilmente. Utilice el widget de **SSL Activity (Actividad SSL)** para ver y analizar la actividad de descifrado de la red, como el número de sesiones descifradas y no descifradas, la cantidad de tráfico que utilizan las diferentes versiones del protocolo TLS, los motivos más comunes de los fallos de descifrado, y conocer qué aplicaciones e identificaciones de nombre de servidor (SNI, Server Name Identification) utilizan cifrados y algoritmos débiles. A continuación, utilice los logs de descifrado para profundizar en las sesiones y diagnosticar el problema exacto para tomar las medidas adecuadas.

PAN-OS 10.0 introdujo cinco nuevos widgets de descifrado. Utilice la información que ofrecen los widgets para identificar políticas y perfiles de descifrado configurados incorrectamente y para tomar decisiones informadas sobre qué tráfico permitir y qué tráfico bloquear:

- **Traffic Activity (Actividad de tráfico)**: muestra la actividad de SSL/TLS en comparación con la actividad que no es de SSL/TLS por número total de sesiones o por cantidad de tráfico en bytes.

© 2020 Palo Alto Networks, Inc.

- **SSL/TLS Traffic (Tráfico SSL/TLS)**: muestra la cantidad de tráfico descifrado y no descifrado por número de sesiones o cantidad de tráfico en bytes. Entre los motivos por las que el tráfico no se descifra se encuentran los siguientes.
  - No se aplicó ninguna política de descifrado al tráfico.
  - La política de descifrado eximía intencionalmente el tráfico del descifrado (por ejemplo, una política de no descifrado).
  - La política de descifrado estaba configurada incorrectamente y el tráfico estaba destinado al descifrado, pero no se descifró.
  - El sitio estaba en la lista de exclusiones de descifrado SSL (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**), que contiene sitios que Palo Alto Networks ha identificado que rompen el descifrado por razones técnicas, como certificados fijados o autenticación de clientes. Para estos sitios, el cortafuegos pasa por alto el descifrado.
  - El sitio está en la caché de exclusión de descifrado local, que contiene sitios que encuentran los usuarios locales y que impiden el descifrado por motivos técnicos.

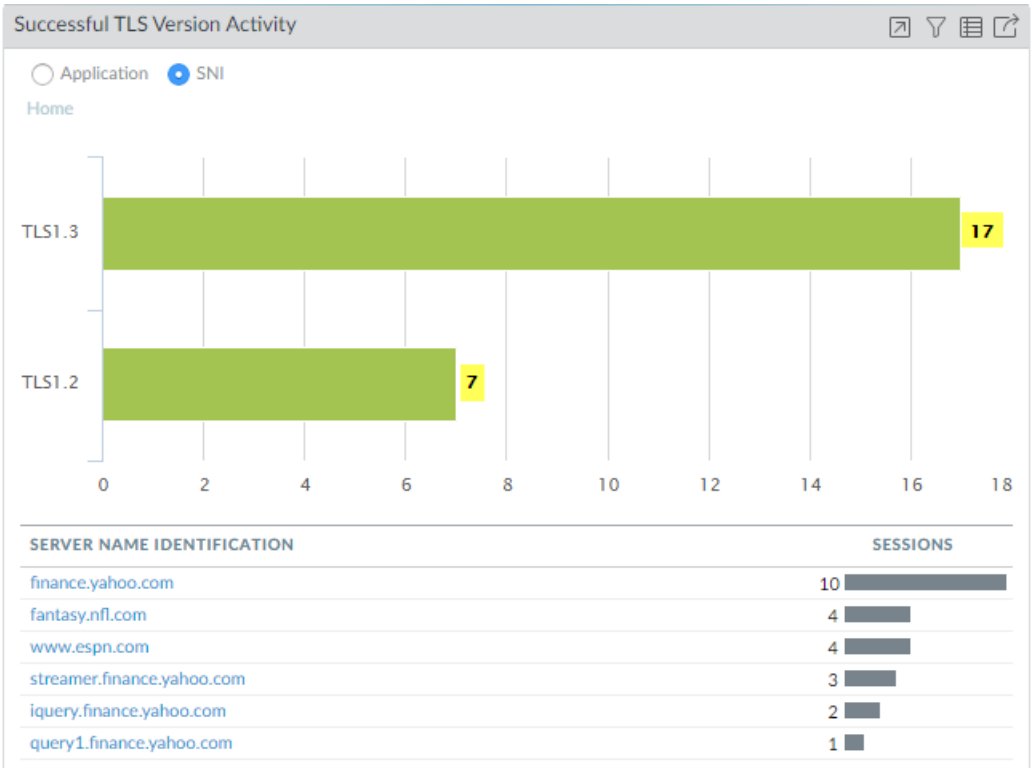
El ACC solo completa los siguientes tres widgets con datos del tráfico que controla una política de descifrado. Si no aplica una política de descifrado al tráfico, ese tráfico no completa estos widgets.

- **Decryption Failure Reasons (Motivos de error de descifrado)**: muestra los motivos de los fallos de descifrado: protocolo, certificado, versión, cifrado, HSM, recursos, reanudación o problemas de funciones por SNI. Utilice esta información para detectar problemas causados por una política de descifrado o una configuración incorrecta del perfil o por el tráfico que utiliza protocolos o algoritmos débiles no compatibles. Haga clic en un motivo de fallo para profundizar y aislar el número de sesiones por SNI que experimentó el fallo o haga clic en un SNI para ver todos los errores de descifrado para ese SNI.
- **Successful TLS Version Activity (Actividad de la versión TLS correcta)**: muestra las conexiones TLS correctas por versión TLS para aplicaciones o SNI (las SNI están disponibles solo para el proxy de reenvío), por lo que puede evaluar el riesgo que está asumiendo si permite versiones más débiles del protocolo TLS. La identificación de aplicaciones y SNI que utilizan protocolos débiles le permite evaluar cada una y decidir si necesita permitir el acceso a ellas por motivos empresariales. Si no necesita la aplicación para fines empresariales, es posible que desee bloquear el tráfico en lugar de permitir que reduzca el riesgo. Haga clic en una versión de TLS para profundizar y ver las SNI o las aplicaciones que usaron esa versión de TLS. Haga clic en una aplicación o una SNI para profundizar y ver cuántas de esas aplicaciones o sesiones de SNI usaron cada versión de TLS.
- **Successful Key Exchange Activity (Actividad de intercambio de claves correcta)**: muestra la actividad de intercambio de claves correcta por algoritmo para aplicaciones o SNI (las SNI solo están disponibles para el proxy de reenvío). Haga clic en un algoritmo de intercambio de claves para ver la actividad de ese algoritmo o haga clic en una aplicación o SNI para ver la actividad del algoritmo de intercambio de claves para esa aplicación o SNI.

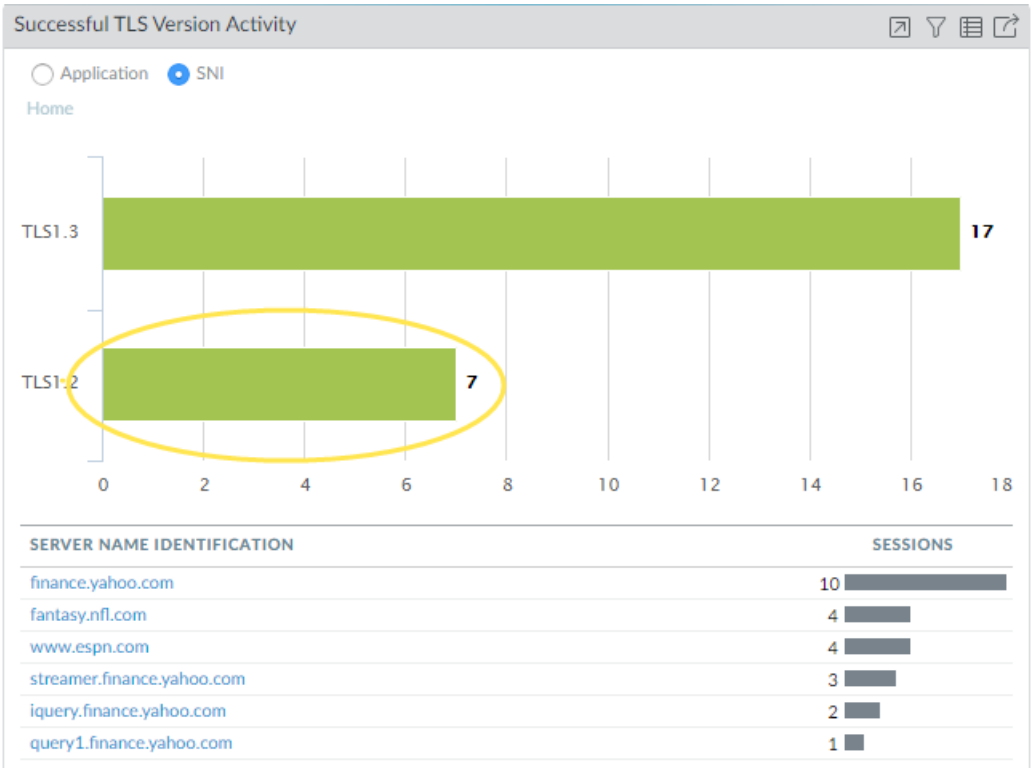
El siguiente ejemplo de profundización en los datos de ACC muestra cómo examinar la actividad correcta de la versión de TLS:

1. El widget **Successful TLS Version Activity (Actividad de versión de TLS correcta)** muestra que 17 sesiones usaron TLSv1.3 y 7 sesiones usaron TLSv1.2. La lista de SNI muestra las SNI de destino y el número de sesiones por SNI.

© 2020 Palo Alto Networks, Inc.

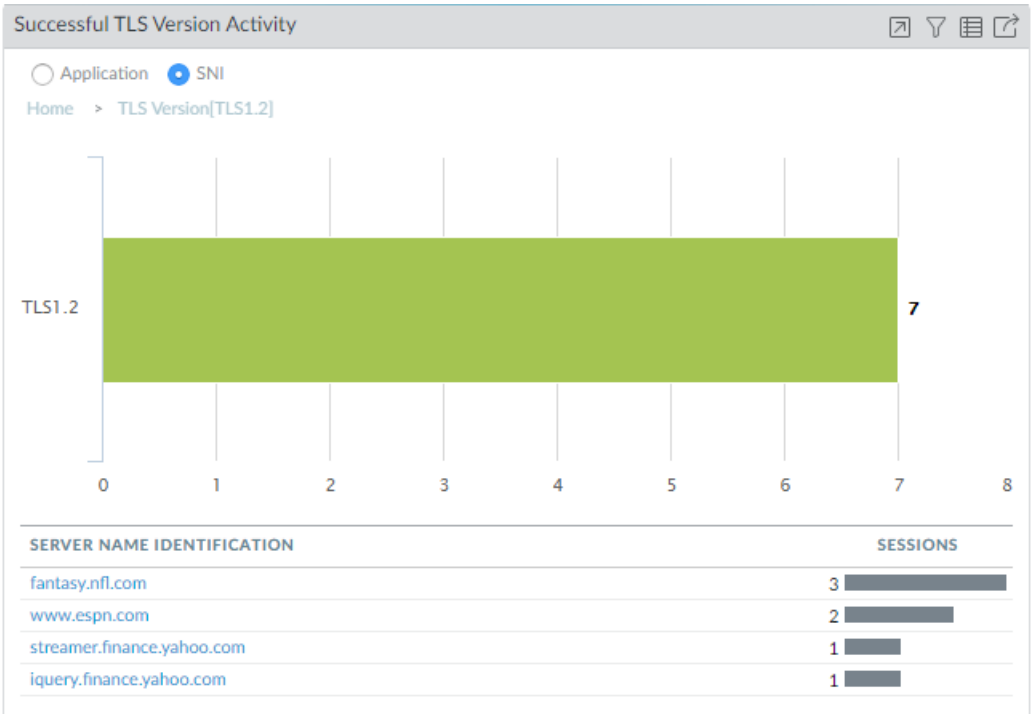


2. Para ver qué SNI usaron TLSv1.2, haga clic en la barra verde etiquetada como TLS1.2.

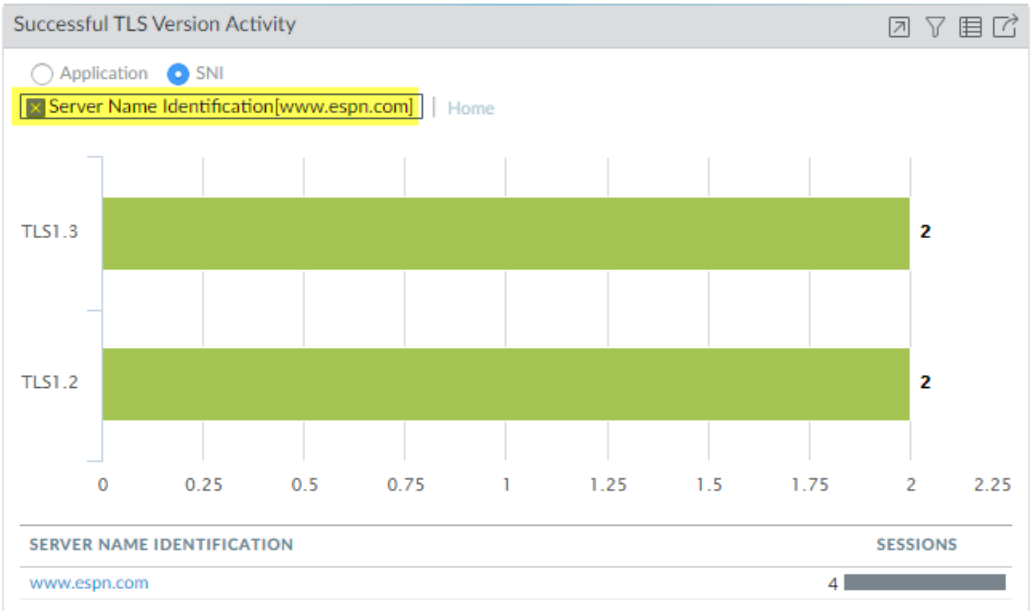


3. Ahora puede ver que las siete sesiones TLSv1.2 se distribuyeron entre cuatro servidores.

© 2020 Palo Alto Networks, Inc.



4. Al hacer clic en **Home (Inicio)** se vuelve a la pantalla de inicio. Ahora, al hacer clic en www.espn.com, SNI nos muestra qué versiones de TLS utilizó. Podemos ver que dos de las cuatro sesiones usaron TLSv1.3 y dos usaron TLSv1.2.



Para cualquier widget de descifrado, haga clic en el icono Jump to Logs (Ir a logs) para ir directamente a los logs de descifrado que corresponden a los datos en la ACC:



En el ejemplo anterior, en cualquier punto de la investigación, podría saltar a los logs de descifrado para una mayor profundización de los datos. Por ejemplo, puede examinar los logs de las sesiones individuales que usaron TLSv1.2 para averiguar por qué no usaron TLSv1.3.

© 2020 Palo Alto Networks, Inc.

Los widgets de ACC de descifrado muestran el nombre de la aplicación descifrada según el App-ID de Palo Alto Networks. Para completar la ACC, el cortafuegos solo puede identificar aplicaciones que tienen un App-ID de Palo Alto Networks; el cortafuegos no puede completar la ACC con aplicaciones personalizadas o aplicaciones que no tienen un App-ID. Las actualizaciones de contenido actualizan los App-ID con regularidad. Otros motivos por los que la aplicación puede aparecer como incompleta o desconocida son los siguientes:

- El cortafuegos eliminó la sesión antes de que pudiera identificar la aplicación.
- Los logs de descifrado dependen de los logs de tráfico para completar el campo de la aplicación de log de descifrado. Sin embargo, si el log de tráfico no se finaliza en 60 segundos o menos, el log de tráfico no completa la aplicación en el log de descifrado y la aplicación se muestra como incompleta o desconocida.

Log de descifrado

El log de descifrado (**Monitor (Supervisar)** > **Logs** > **Decryption (Descifrado)**) proporciona información completa sobre las sesiones que coinciden con una política de descifrado para ayudarlo a obtener contexto sobre ese tráfico con el fin de diagnosticar y resolver con precisión y facilidad los problemas de descifrado. El cortafuegos no registra el tráfico si este no coincide con una política de descifrado. Si desea registrar el tráfico que no descifre, cree una exclusión de descifrado basada en políticas y para las políticas que rigen el tráfico TLSv1.2 y anteriores, aplique un perfil sin descifrado al tráfico.

PAN-OS admite logs de descifrado para los siguientes tipos de tráfico:

- Forward Proxy (Proxy de reenvío): varios campos solo muestran información para el tráfico de Forward Proxy (Proxy de reenvío), incluida la CA raíz (solo para certificados de confianza) y Server Name Identification (Identificación del nombre del servidor, SNI).
- Inspección de entrada.
- No Decrypt (Sin cifrado) (tráfico excluido del descifrado por la política de descifrado).

  El cortafuegos muestra menos información porque la sesión permanece cifrada. Para el tráfico TLSv1.3 sin descifrar, no hay información del certificado porque TLSv1.3 cifra la información del certificado.
- GlobalProtect: cubre GlobalProtect Gateway (Puerta de enlace de GlobalProtect), GlobalProtect Portal (Portal de GlobalProtect) y GlobalProtect Clientless VPN (VPN sin cliente de GlobalProtect) (solo de cliente a cortafuegos).

  GlobalProtect no es compatible con TLSv1.3.
- Reflejo de descifrado
- Decryption Broker (Agente de descifrado) (mostrado como Forward Proxy [Proxy de reenvío] en la columna **Proxy Type [Tipo de proxy]**).

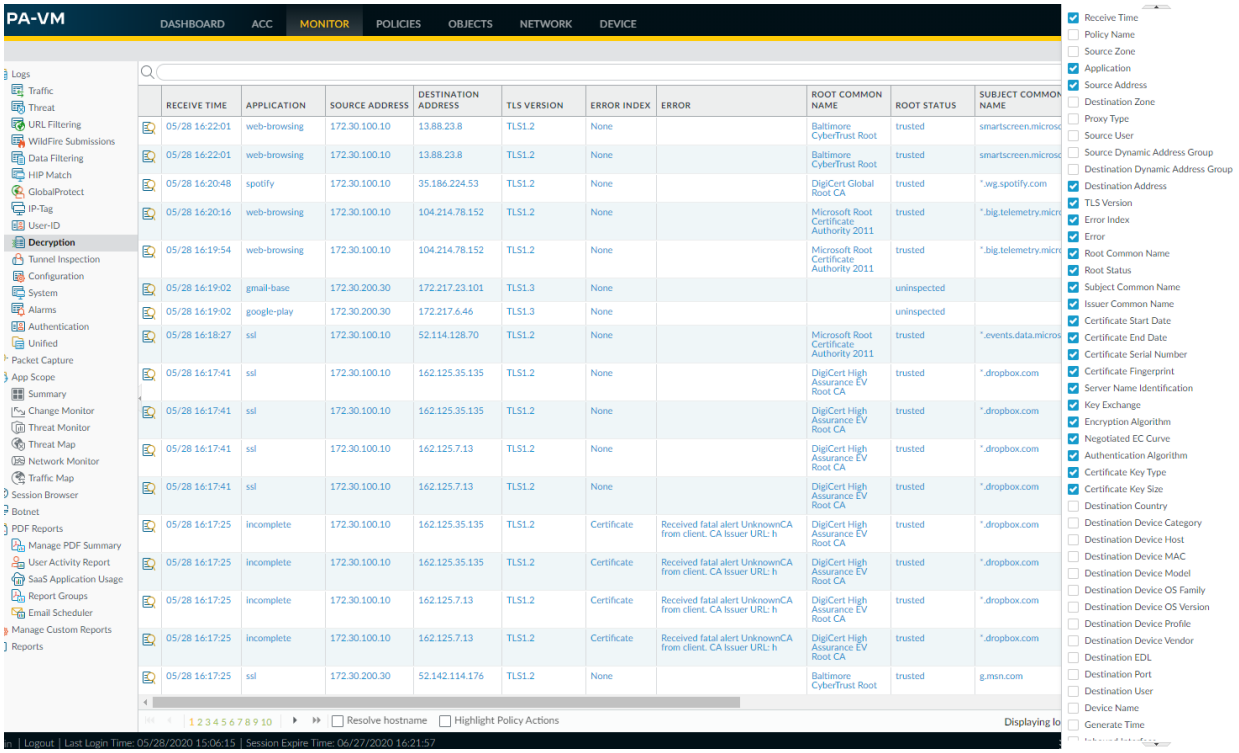
No todos los tipos de tráfico admiten todos los parámetros. Parámetros no compatibles mediante tipo de proxy y versión de TLS *proporciona una lista completa de parámetros no admitidos para cada tipo de tráfico de descifrado.*

Los datos para el tráfico del proxy de reenvío se basan en si el protocolo de enlace TLS es correcto o no. Para los protocolos de enlace TLS fallidos, el cortafuegos envía datos de error para el tramo de la transacción que provocó el error, ya sea de cliente a cortafuegos o de cortafuegos a servidor. En los protocolos de enlace TLS correctos, los datos provienen del tramo que se completa primero correctamente, que generalmente es de cliente a cortafuegos.

Los logs de descifrado no son compatibles con el tráfico de proxy SSH. Además, la información del certificado no está disponible para los logs de reanudación de sesiones.

© 2020 Palo Alto Networks, Inc.

De forma predeterminada, el cortafuegos registra todo el tráfico de protocolo de enlace TLS fallido. También puede registrar el tráfico de protocolo de enlace TLS correcto si así lo desea. Puede ver hasta 62 columnas de información de log, como aplicación, SNI, nombre de política de descifrado, índice de error, versión de TLS, versión de intercambio de claves, algoritmo de cifrado, tipos de claves de certificado y muchas otras características:



Haga clic en el icono de la lupa ( ) para ver la vista de log detallada de una sesión.

El log de descifrado aprende el App-ID de cada sesión del log de tráfico, por lo que los logs de tráfico deben estar habilitados para ver el App-ID en el log de descifrado. Si los logs de tráfico están deshabilitados, el App-ID se muestra como incompleto. Por ejemplo, una gran parte del tráfico de GlobalProtect es tráfico dentro de la zona (de zona no fiable a zona no fiable), pero la política intrazona predeterminada no habilita los logs de tráfico. Para ver el App-ID para el tráfico intrazona de GlobalProtect, debe habilitar el log de tráfico para el tráfico intrazona.

Otra razón por la que el App-ID puede mostrarse como incompleto es que para sesiones largas, el cortafuegos puede generar el log de descifrado antes de que se complete el log de tráfico (el log de tráfico se genera normalmente al final de la sesión). En esos casos, el App-ID no está disponible para el log de descifrado. Además, cuando el protocolo de enlace TLS falla y genera un log de errores, el App-ID no está disponible porque el error termina la sesión antes de que el cortafuegos pueda determinar el App-ID. En estos casos, la aplicación puede mostrarse como ssl o incompleta.

Para solucionar problemas, use los widgets de ACC de descifrado (**ACC** > **SSL Activity (Actividad de SSL)**) para identificar el tráfico que causa problemas de descifrado y, a continuación, use el log de descifrado y Plantillas de informes personalizados de descifrado para profundizar en los detalles.

Cuando reenvíe logs de descifrado para su almacenamiento, asegúrese de proteger adecuadamente el transporte y el almacenamiento de logs, ya que los logs de descifrado contienen información confidencial.

© 2020 Palo Alto Networks, Inc.

Cuando los logs de descifrado están habilitados, el cortafuegos envía registros HTTP/2 como logs de inspección de túnel (cuando los logs de descifrado están deshabilitados, los logs de HTTP/2 se envían como logs de tráfico), por lo que debe verificar los logs de inspección de túnel en lugar de los logs de tráfico para eventos HTTP/2. Además, debe habilitar la inspección del contenido del túnel para obtener el App-ID para el tráfico HTTP/2.

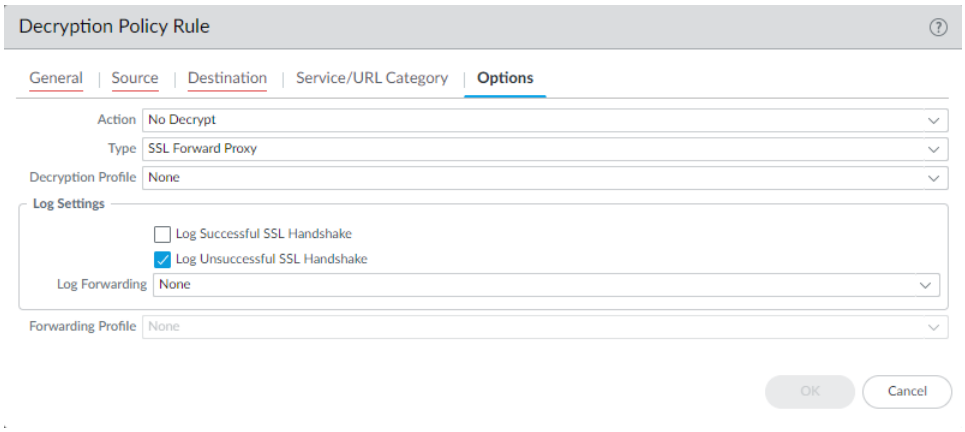
- Configuración de logs de descifrado
- Reparación de cadenas de certificado incompletas
- Errores de logs de descifrado, índices de error y máscaras de bits

Configuración de logs de descifrado

El cortafuegos genera logs de descifrado para sesiones regidas por una política de descifrado, incluidas las sesiones con una política que no sea de descifrado. Configure el log de descifrado en la política de descifrado que controla el tráfico que desee registrar.

STEP 1 | Configure el tráfico de descifrado en el que desea iniciar sesión en la política de descifrado (**Policies (Políticas)** > **Decryption (Descifrado)**).

De forma predeterminada, el cortafuegos solo registra los protocolos de enlace TLS incorrectos:

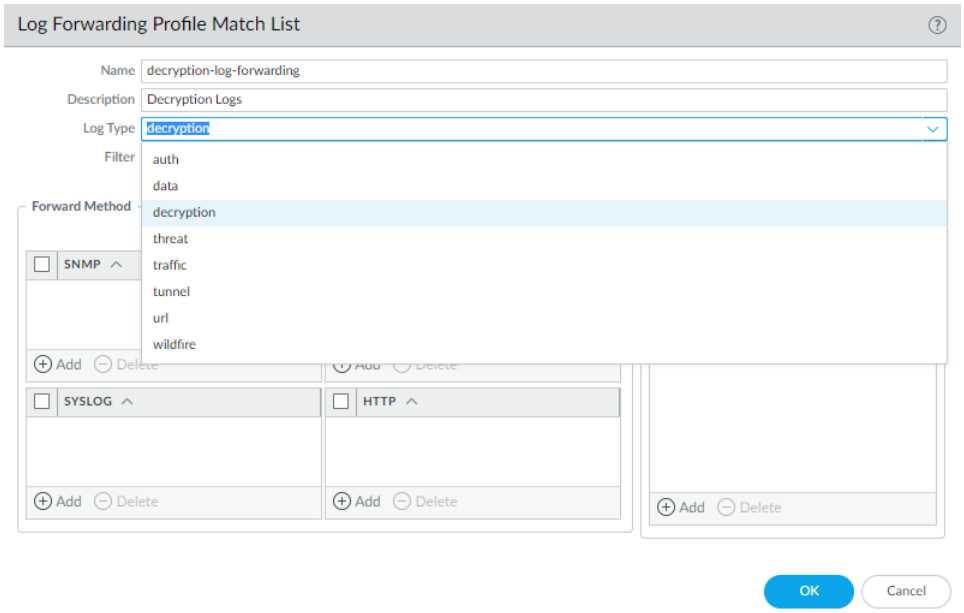


Registre los protocolos de enlace correctos, así como los protocolos de enlace incorrectos, para obtener visibilidad de todo el tráfico descifrado que permitan los recursos disponibles de su dispositivo (no descifre el tráfico privado o confidencial; siga las prácticas recomendadas de descifrado y descifre la mayor cantidad de tráfico que pueda).

STEP 2 | Cree un perfil de reenvío de logs para reenviar los logs de descifrado a los recopiladores de logs, otros dispositivos de almacenamiento o administradores específicos y, a continuación, especifique el perfil en el campo **Log Forwarding (Reenvío de logs)** de la pestaña **Options (Opciones)** de la política de descifrado.

Para reenviar los logs de descifrado, debe configurar un perfil de reenvío de logs (**Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**) para especificar el **tipo de log** y el método de reenvío de logs.

© 2020 Palo Alto Networks, Inc.

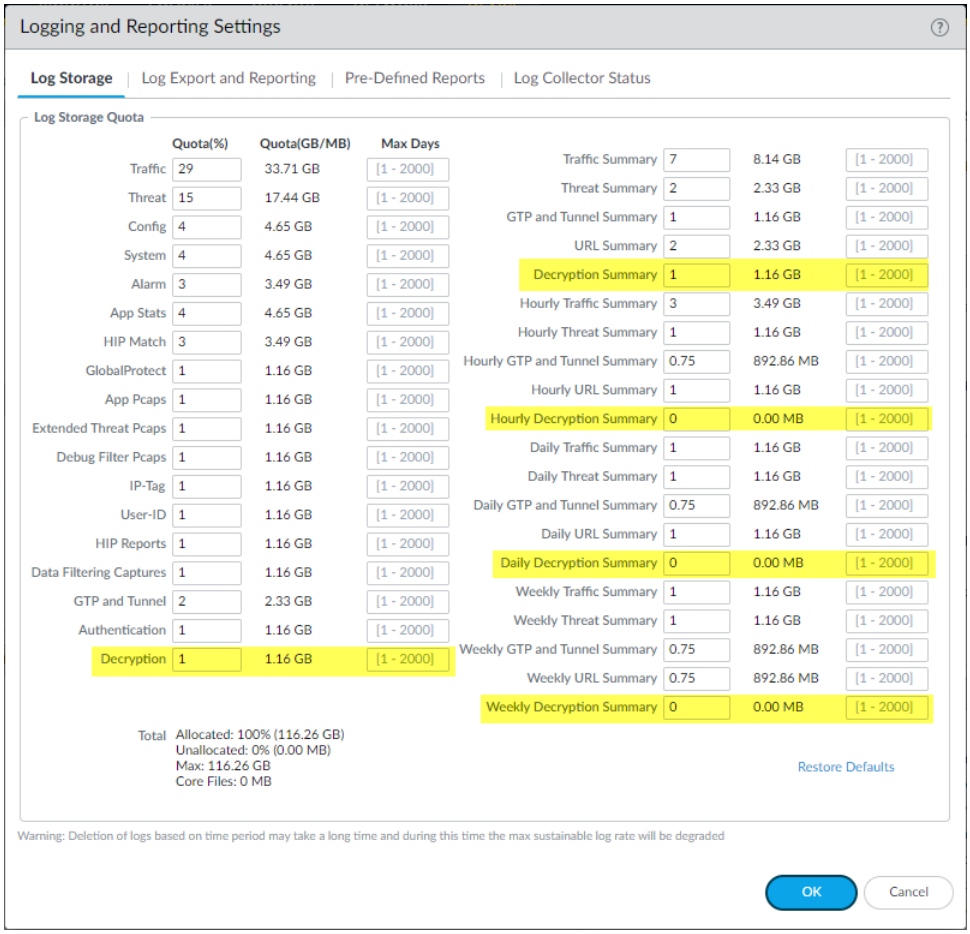


Si reenvía logs de descifrado, asegúrese de que los logs se almacenen de forma segura porque contienen información confidencial.

STEP 3 | Si registra un protocolo de enlace TLS correcto además de un protocolo de enlace TLS incorrecto, configure una cuota de espacio de almacenamiento de log más grande (**Device (Dispositivo)** > **Setup (Configuración)** > **Management (Administración)** > **Logging and Reporting Settings (Configuración de creación de logs e informes)** > **Log Storage (Almacenamiento de logs)**) para los registros de descifrado en el cortafuegos.

La cuota predeterminada (asignación) es el uno por ciento de la capacidad de almacenamiento de logs del dispositivo para los logs de descifrado y el uno por ciento para el resumen general de descifrado. No hay una asignación predeterminada para los resúmenes de descifrado por hora, por día o por semana.

© 2020 Palo Alto Networks, Inc.



Son muchos los factores que determinan la cantidad de almacenamiento que puede necesitar para los logs de descifrado y dependen de su implementación. Por ejemplo, tenga en cuenta estos factores:

- La cantidad de tráfico TLS que pasa a través del cortafuegos.
- La cantidad de tráfico TLS que descifra.
- Su uso de otros logs (evalúe de qué logs debería tener capacidad para asignar a los logs de descifrado).
- Si registra tanto los protocolos de enlace TLS correctos como los incorrectos, probablemente necesite mucha más capacidad de la que necesita si solo registra protocolos de enlace TLS incorrectos. Según la cantidad de tráfico que descifre, los logs de descifrado pueden consumir tanta capacidad como los logs de tráfico o los logs de amenazas, y pueden requerir una compensación entre ellos si la capacidad del dispositivo ya está totalmente suscrita.

La asignación combinada total de cuotas de logs no puede exceder el 100 % de los recursos de log de cortafuegos disponibles.

Es posible que deba experimentar para encontrar la cuota adecuada para cada categoría de log en su implementación particular. Si solo registra los protocolos de enlace erróneos, puede comenzar con el predeterminado o aumentar la asignación al dos o tres por ciento. Si registra tanto los protocolos de enlace correctos como los incorrectos, puede comenzar asignando aproximadamente la mitad del espacio a los logs de descifrado que asigna a los logs de tráfico. Los logs de los que toma el espacio para asignarlos a los logs de descifrado dependen de su tráfico, su negocio y sus requisitos de supervisión.

© 2020 Palo Alto Networks, Inc.

Errores de logs de descifrado, índices de error y máscaras de bits

Las columnas **Error Index (Índice de errores)** y **Error** del log de descifrado proporcionan información sobre la categoría y los detalles del error de descifrado, respectivamente. También puede ver el error y la información del índice de errores en la sección Handshake Details (Detalles del protocolo de enlace) de la vista de log detallada (haga clic en para cualquier entrada de registro). El **índice de errores** del log de descifrado indica una de las ocho categorías de errores:

Índice de errores	Error (posibles errores mostrados para el índice de errores)
Certificado	Errores como certificados no válidos, certificados caducados, certificados de cliente no admitidos, revocaciones y fallos de verificación OCSP/CRL, CA de emisores que no son de confianza (sesiones firmadas por una raíz que no es de confianza, que incluye cadenas de certificados incompletas) y otros errores de certificado. *Cuando el cortafuegos no tiene un certificado intermedio porque el sitio no envió la cadena de certificados completa, puede buscar e instalar el certificado que falta en* Reparación de cadenas de certificado incompletas.
Cifrado	Errores de cifrado no admitidos en los que se dan las siguientes características: • El cliente intenta negociar un cifrado que admita el cortafuegos, pero que el perfil de descifrado aplicado al tráfico no sea compatible. • El cliente intenta negociar un cifrado que el cortafuegos no admite. • (Poco frecuente) La inspección entrante está habilitada y las capacidades del servidor no coinciden con la configuración del perfil de descifrado. El mensaje de error incluye el valor de máscara de bits de cifrado del cliente admitido y el valor de máscara de bits de cifrado del perfil de descifrado admitido. Utilice los valores de la máscara de bits para identificar el cifrado que el cliente intentó utilizar y para enumerar los valores de cifrado que admite el perfil de descifrado, tal y como se describe más adelante en este tema.
Función	Errores como protocolos de enlace TLS de gran tamaño o protocolos de enlace desconocidos, cadenas de certificados de gran tamaño (más de cinco certificados) y otras funciones no admitidas.
HSM	Errores del módulo de almacenamiento de hardware (HSM, Hardware Storage Module), como solicitudes desconocidas, elementos no encontrados en la configuración, tiempos de espera de solicitudes y otros errores y fallos de HSM.
Protocolo	Errores como fallos en el protocolo de enlace TLS, discrepancias de claves públicas y privadas, errores Heartbleed, fallos en el intercambio de claves TLS y otros errores del protocolo TLS. Los errores de protocolo se muestran cuando el servidor no es compatible con los protocolos que admite el cliente, el servidor utiliza tipos de certificado que el cortafuegos no admite y errores generales del protocolo TLS.
Recurso	Errores de tipo memoria insuficiente.
Reanudación	Errores de reanudación de la sesión relacionados con los ID y vales de la sesión de reanudación, las entradas de la sesión de reanudación en la caché del cortafuegos y otros errores de reanudación de la sesión.

© 2020 Palo Alto Networks, Inc.

Índice de errores	Error (posibles errores mostrados para el índice de errores)
versión	Errores relacionados con las discrepancias entre las versiones del perfil de descifrado y el cliente y las discrepancias entre las versiones del cliente y del servidor. El mensaje de error incluye valores de máscara de bits que identifican el cliente compatible y las versiones del perfil de descifrado. Utilice los valores de la máscara de bits para identificar el cifrado que el cliente intentó utilizar y para enumerar los valores de cifrado que admite el perfil de descifrado, tal y como se describe más adelante en este tema.



Si no existe una categoría de descripción de error adecuada para un error, el mensaje predeterminado es General TLS protocol error (Error general de protocolo TLS).

La información de errores de log de cifrado y versión incluye valores de máscara de bits que se convierten en valores reales mediante los comandos operativos de la CLI:

- Los valores de la máscara de bits de error de versión identifican discrepancias entre las versiones del protocolo TLS que utilizan el cliente y el servidor, y también identifican las discrepancias del protocolo TLS entre el cliente y el perfil de descifrado aplicado al tráfico. El comando de la CLI para convertir las máscaras de bits de error de versión es:

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-version <bitmask-value>
  ```

  El comando devuelve la versión de TLS que coincide con la máscara de bits.
- Los valores de máscara de bits de error de cifrado identifican el cifrado y otras discrepancias entre el cliente y el perfil de descifrado aplicado al tráfico.

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-value>
  ```

  El comando devuelve el cifrado que coincide con la máscara de bits.

Filtre el log de descifrado para encontrar la versión y los errores de cifrado, conecte los valores de la máscara de bits para las sesiones con errores en el comando de la CLI apropiado, obtenga los valores de la versión del protocolo o el cifrado que provocó el error y utilice la información para actualizar la política o el perfil de descifrado si desea permitir el acceso al sitio en cuestión.

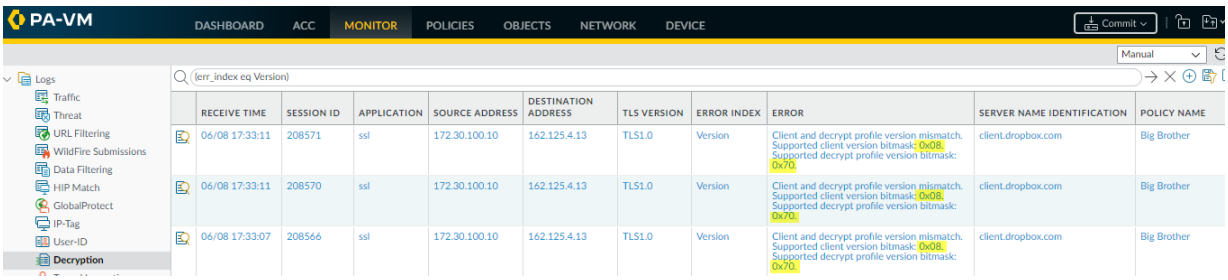
- Errores de versión
- Errores de cifrado
- Estado raíz con el valor "Uninspected" (No inspeccionado)

Errores de versión

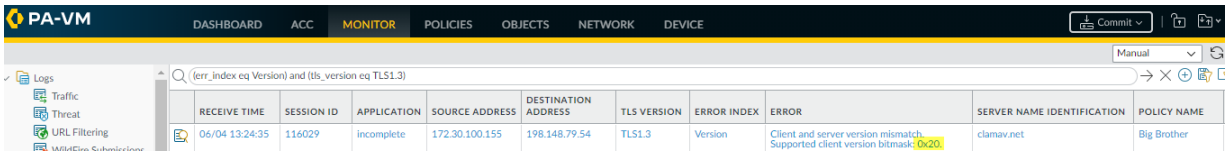
Para identificar y corregir errores de discrepancia de versiones, realice el siguiente procedimiento:

1. Filtre el log de descifrado para identificar errores de versión mediante el filtro **`(err_index eq Version)`**. Los valores resaltados son valores de máscara de bits:

© 2020 Palo Alto Networks, Inc.



Puede filtrar el log de descifrado de muchas formas. Por ejemplo, para ver solo los errores de la versión TLSv1.3, use el filtro **`(err_index eq Version) y (tls_version eq TLS1.3)`**:



2. Inicie sesión en la CLI y busque los valores de la máscara de bits. Los errores de versión en la primera captura de pantalla (los mismos errores para las tres sesiones) muestran un problema con un cliente y una discrepancia en el perfil de descifrado: la máscara de bits de la versión del cliente compatible es 0x08 y la máscara de bits de la versión del perfil de descifrado compatible es 0x70:

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

Este resultado muestra que el cliente solo admite TLSv1.0.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

Este resultado muestra que el perfil de descifrado admite TLSv1.1, TLSv1.2 y TLSv1.3, pero no TLSv1.0. Ahora sabe que el problema es que el cliente solo admite una versión muy antigua del protocolo TLS y el perfil de descifrado adjunto a la regla de política de descifrado que controla el tráfico no permite el tráfico TLSv1.0.

Lo siguiente que debe hacer es decidir qué acción tomar. Puede actualizar el cliente para que acepte una versión TLS más segura. Si el cliente requiere TLSv1.0 por alguna razón, puede continuar dejando que el cortafuegos continúe bloqueando el tráfico, puede actualizar el perfil de descifrado para permitir todo el tráfico TLSv1.0 (no recomendado) o puede crear una política de descifrado y perfil que permitan TLSv1.0 y aplicarlo solo a los dispositivos cliente que deben usar TLSv1.0 y no pueden admitir un protocolo más seguro (la opción más segura para permitir el tráfico).

© 2020 Palo Alto Networks, Inc.

El error de versión en la segunda captura de pantalla muestra un problema diferente: una discrepancia entre la versión del cliente y la del servidor. El error indica que la máscara de bits del cliente compatible es 0x20:

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

El resultado muestra que el cliente solo admite TLSv1.2. Puesto que el servidor no es compatible con TLSv1.2, es posible que solo admita TLSv1.3 o que solo admita TLSv1.1 o inferior (protocolos menos seguros). Puede utilizar Wireshark u otra herramienta de análisis de paquetes para conocer qué versión de TLS admite el servidor. Dependiendo de lo que admita el servidor, puede realizar las siguientes acciones:

- Si el servidor solo admite TLSv1.3, puede editar el perfil de descifrado para que admita TLSv1.3.
- Si el servidor solo admite TLSv1.1 o una versión inferior, evalúe si necesita acceder a ese servidor por motivos empresariales. Si no es así, considere bloquear el tráfico para aumentar la seguridad. Si necesita acceder al servidor con fines empresariales, cree o añada el servidor a una política de descifrado que se aplique solo a los servidores y sitios a los que necesita acceder para su empresa; no permita el acceso a todos los servidores que usan versiones TLS menos seguras.

3. Para encontrar la política de descifrado que controla el tráfico de la sesión, verifique la columna **Policy Name (Nombre de la política)** en el log (o haga clic en el icono de la lupa junto al log de descifrado para ver la información en la sección General de la vista de log detallada). En el ejemplo anterior, el nombre de la política de descifrado es Big Brother (Gran Hermano). Para encontrar la política y el perfil de descifrado, diríjase a **Policies (Políticas)** > **Decryption (Descripción)**, seleccione la política denominada Big Brother (Gran Hermano) y, a continuación, seleccione la pestaña **Options (Opciones)**. **Decryption profile (Perfil de descifrado)** muestra el nombre del perfil de descifrado.

   Diríjase a **Objects (Objetos)** > **Decryption (Descripción)** > **Decryption Profile (Perfil de descifrado)**, seleccione el perfil de descifrado adecuado y edítelo para solucionar el problema de la versión.

Errores de cifrado

Usar el log de descifrado para buscar errores de cifrado es similar a buscar errores de versión: se filtra el log para encontrar errores y obtener máscaras de bits de error. A continuación, vaya a la CLI, convierta la máscara de bits al valor de error y, a continuación tome las medidas adecuadas para solucionar el problema. Por ejemplo:

1. Filtre el log de descifrado para identificar errores de cifrado mediante el filtro **`(err_index eq Cipher)`**. Por ejemplo, examinemos un error de cifrado con el **Error** message `Unsupported cipher. Supported client cipher bitmask: 0x80000000. Support decrypt profile cipher bitmask 0x60f79980.`
2. Inicie sesión en la CLI y busque los valores de la máscara de bits:

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher 0x80000000
```

```
CHACHA_PLY1305_SHA256
```


© 2020 Palo Alto Networks, Inc.

Este resultado muestra que el cliente intentó negociar un cifrado compatible con el cortafuegos (si la máscara de bits es todo ceros (`0x0000000`, entonces el cliente intentó negociar un cifrado que el cortafuegos no admite):

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher 0x80000000
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

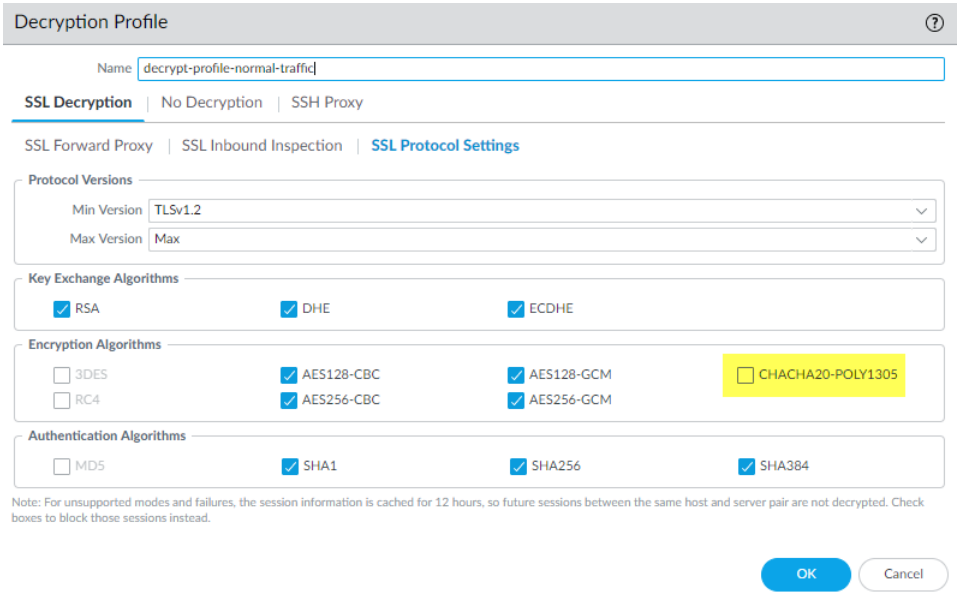
Esta salida muestra que el perfil de descifrado que controla el tráfico admite muchos cifrados, pero no admite el cifrado que el cliente está intentando utilizar.

Para solucionar este problema de modo que el cortafuegos permita y descifre el tráfico, debe añadir soporte para el cifrado que falta al perfil de descifrado.

3. Consulte el log de descifrado o el **nombre de política** de la vista de log detallada para obtener el nombre de la política de descifrado que controla el tráfico. Diríjase a **Policies (Políticas)** > **Decryption (Descripción)** y seleccione la política. En la pestaña **Options (Opciones)**, busque el nombre del perfil de descifrado. A continuación, diríjase a **Objects (Objetos)** > **Decryption (Descripción)** > **Decryption Profile (Perfil de descripción)**, seleccione el perfil de descifrado adecuado y edítelo para solucionar el problema de la versión.

   En este ejemplo, el perfil de descifrado no admite el cifrado TLS13_WITH_CHACHA_POLY1305_SHA256, por lo que el cliente no puede conectarse:

© 2020 Palo Alto Networks, Inc.



Para solucionar el problema, seleccione la opción de algoritmo de cifrado **CHACHA20-POLY1305** (la configuración **Max Version (Versión máx.)** de **Max (Máx.)** significa que el perfil ya es compatible con TLSv1.3 y la configuración del algoritmo de autenticación ya incluye SHA256, por lo que solo faltaba el soporte del algoritmo de cifrado) y, a continuación, **confirme** la configuración. Después de confirmar la configuración, el perfil de descifrado admite el cifrado que falta y las sesiones de descifrado para el tráfico se realizan correctamente.

Si el cortafuegos no admite un conjunto de cifrado y necesita permitir el tráfico con fines comerciales, cree una política y un perfil de descifrado que se aplique solo a ese tráfico. En el perfil de descifrado, deshabilite la opción Block sessions with unsupported cipher suites (Bloquear sesiones con conjuntos de cifras no compatibles).

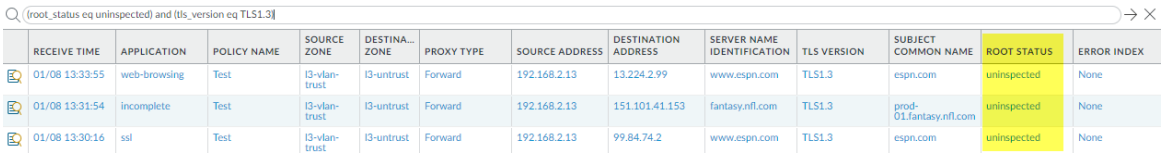
.

Estado raíz con el valor "Uninspected" (No inspeccionado)

En algunos casos, la columna **Root Status (Estado raíz)** muestra el valor **uninspected (no inspeccionado)**. Hay varias razones por las que el cortafuegos no pudo inspeccionar el estado de la raíz, entre ellas las siguientes:

- Reanudación de la sesión.
- El tráfico no se descifró porque una política de no descifrado controlaba el tráfico, por lo que el cortafuegos no descifró el tráfico.
- Se produjo un error de descifrado antes de que el cortafuegos pudiera inspeccionar el certificado del servidor.

Filtre el log de descifrado **`(root_status eq uninspected) y (tls_version eq TLS1.3)`** para ver las sesiones de descifrado para las que el estado de la raíz es uninspected (no inspeccionado):



© 2020 Palo Alto Networks, Inc.

Reparación de cadenas de certificado incompletas

No todos los sitios web envían su cadena de certificados completa, aunque el estándar RFC 5246 TLSv1.2 requiere servidores autenticados para proporcionar una cadena de certificados válida que conduzca a una entidad de certificación aceptable. Si habilita el descifrado y aplica un perfil de descifrado de proxy de reenvío que habilite **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)** en la política de descifrado (en el caso de que falte un certificado intermedio en la lista de certificados que el servidor del sitio web presente al cortafuegos), no se podrá construir la cadena de certificados en el certificado superior (raíz). En estos casos, el cortafuegos presenta su certificado de no fiable de reenvío al cliente porque el cortafuegos no puede construir la cadena en el certificado raíz y no se puede establecer la confianza sin el certificado intermedio que falta.

El cortafuegos solo tiene certificados raíz en su almacén de Default Trusted Certificate Authorities (Entidades de certificación fiables predeterminadas).

Si un sitio web con el que necesita comunicarse para fines empresariales tiene uno o más certificados intermedios que faltan y el perfil de descifrado bloquea las sesiones con emisores que no son fiables, podrá encontrar y descargar el certificado intermedio que falta e instalarlo en el cortafuegos como una CA raíz de confianza para que el cortafuegos confíe en el servidor del sitio. (La alternativa es ponerse en contacto con el propietario del sitio web y pedirle que configure su servidor para que envíe el certificado intermedio durante el protocolo de enlace).

Si permite sesiones con emisores que no son de confianza en el perfil de descifrado, el cortafuegos establece sesiones incluso si el emisor no es fiable; sin embargo, es una práctica recomendada bloquear las sesiones con emisores que no sean fiables para mayor seguridad.

STEP 1 | Busque sitios web que provoquen errores de cadena de certificados incompletos.

1. Filtre el log de descifrado para identificar las sesiones de descifrado que fallaron debido a una cadena de certificados incompleta.

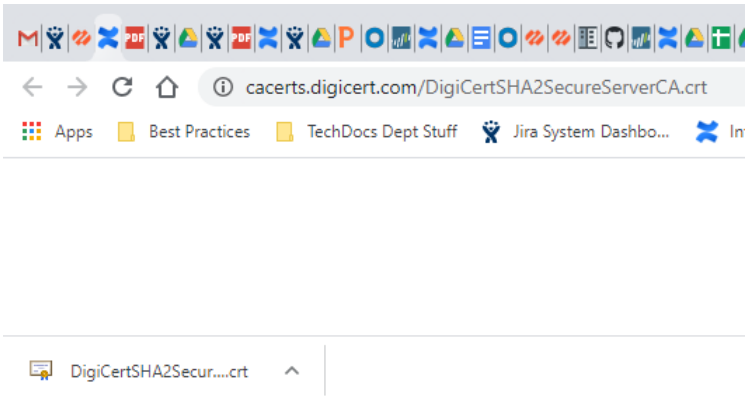
   En el campo de filtro, escriba la consulta **`(err_index eq Certificate) y (error contains 'http')`**. Esta consulta filtra los logs de errores de certificado que contienen la cadena "http", que busca todas las entradas de error que contienen la URL del emisor de CA (a menudo llamada URI). La URL del emisor de CA es la información de acceso a la información de autoridad (AIA, Authority Information Access) para el emisor de CA.
2. Haga clic en una entrada de la columna **Error** que comience por "Received fatal alert UnknownCA from client. CA Issuer URL:" (Se recibió una alerta fatal de CA desconocida del cliente: URL de emisor de CA) seguida del URI.



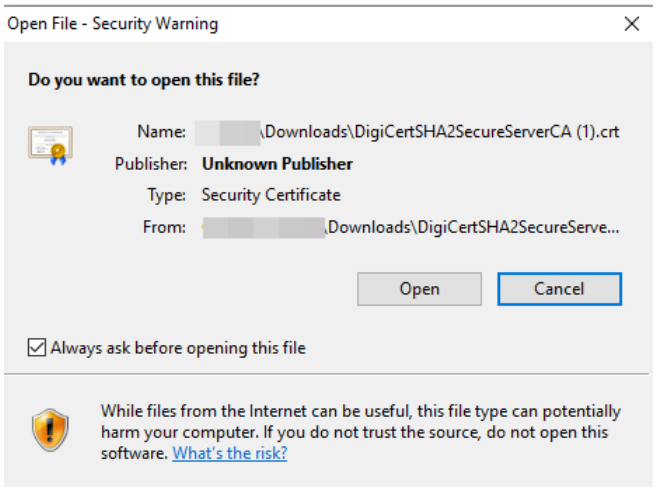
   El cortafuegos añade automáticamente el error seleccionado a la consulta y muestra la ruta completa del URI (la ruta completa del URI puede estar truncada en la columna **Error**).

STEP 2 | Copie y pegue el URI en su navegador y, a continuación, pulse Intro para descargar el certificado intermedio que falta.

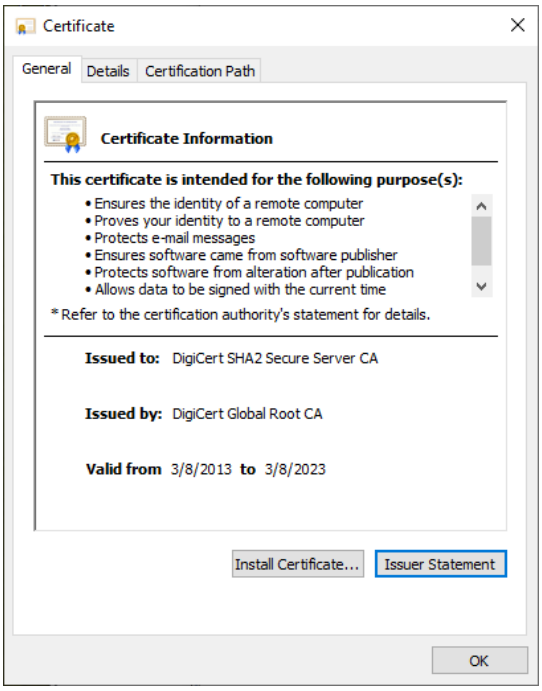
© 2020 Palo Alto Networks, Inc.



STEP 3 | Haga clic en el certificado para abrir el cuadro de diálogo.

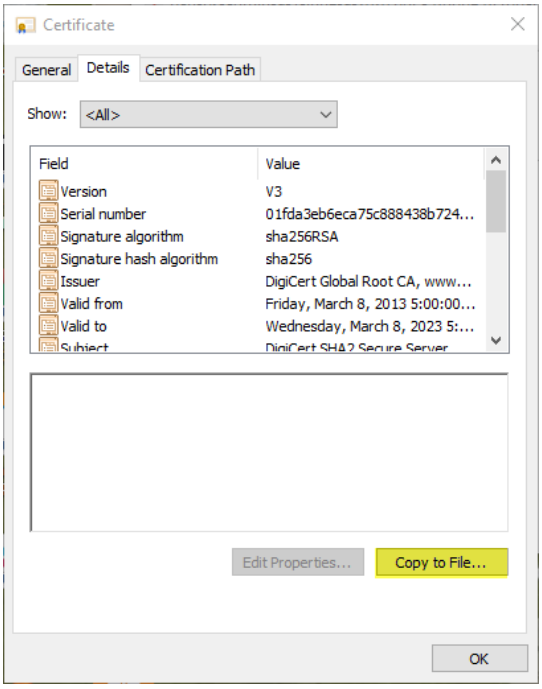


STEP 4 | Haga clic en **Open (Abrir)** para abrir el archivo de certificado.



© 2020 Palo Alto Networks, Inc.

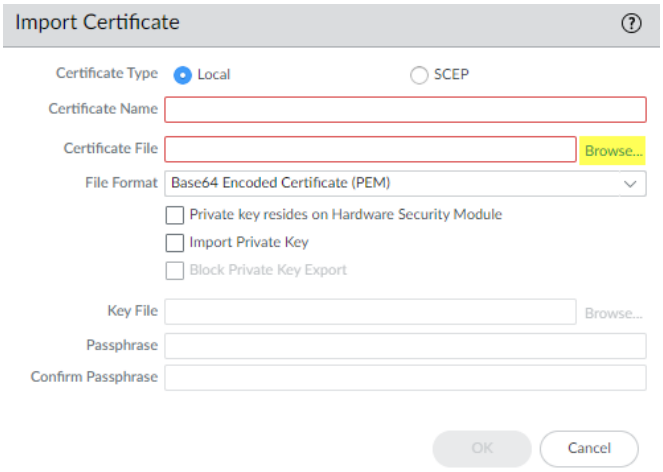
STEP 5 | Seleccione la pestaña **Details (Detalles)** y, a continuación, haga clic en **Copy to File... (Copia a archivo...)**.



Siga las instrucciones de exportación. El certificado se copia en la carpeta que designó como carpeta de descarga predeterminada.

STEP 6 | Importe el certificado al cortafuegos.

1. Diríjase a **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y, a continuación, seleccione **Import (Importar)**.
2. **Busque** la carpeta donde almacenó el certificado intermedio que falta y selecciónelo. Deje **File Format (Formato de archivo)** establecido en **Base64 Encoded Certificate (PEM) (Certificado codificado en Base64 [PEM])**.

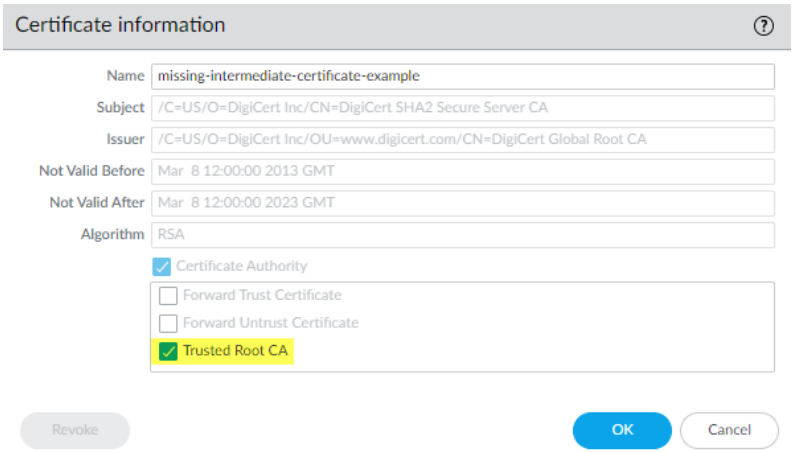


3. Asigne un nombre al certificado y especifique cualquier otra opción que desee utilizar. A continuación, haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Cuando se haya importado el certificado, seleccione el certificado de la lista **Device Certificates (Certificados del dispositivo)** para abrir el cuadro de diálogo Certificate Information (Información del certificado).

STEP 8 | Seleccione **Trusted Root CA (CA raíz de confianza)** para marcar el certificado como CA raíz de confianza en el cortafuegos y, luego, haga clic en **OK (Aceptar)**.



En **Device (Dispositivo)** > **Certificate Management (Gestión de dispositivos)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)**, el certificado importado aparece ahora en la lista de certificados. Marque la columna **Usage (Uso)** para confirmar que el estado es **Trusted Root CA Certificate (Certificado de CA raíz de confianza)** para verificar que el cortafuegos considera que el certificado es una CA raíz de confianza.

STEP 9 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 10 | Con este procedimiento, se ha reparado la cadena de certificados rota.

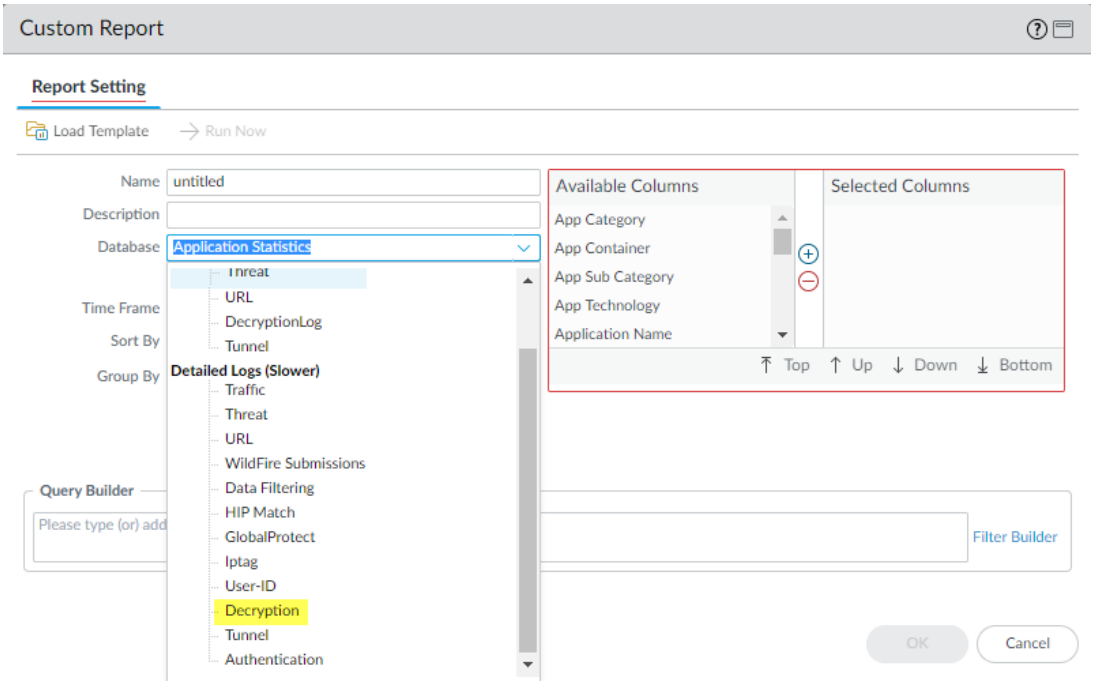
El cortafuegos no bloquea el tráfico porque el emisor de CA ya no es de confianza. Repita este proceso para todos los certificados intermedios que faltan para reparar sus cadenas de certificados.

Plantillas de informes personalizados de descifrado

Puede crear informes personalizados y generarlos para eventos de descifrado basados en campos de log de descifrado y plantillas personalizadas. Seleccione campos de log para incluirlos en informes personalizados y elija plantillas para refinar la consulta de log:

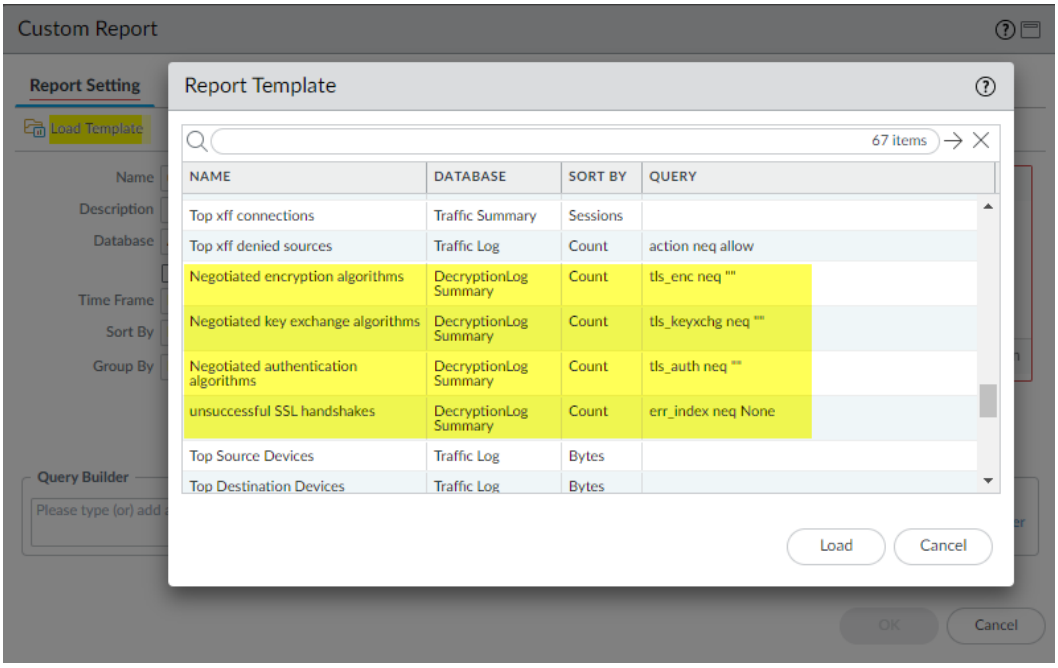
1. **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)**.
2. **Añada** un informe personalizado.
3. Para configurar los campos de log de descifrado que se utilizarán en el informe personalizado, seleccione **Decryption (Descifrado)** como **Database (Base de datos)**.

© 2020 Palo Alto Networks, Inc.



La lista **Available Columns (Columnas disponibles)** cambia para coincidir con las columnas disponibles en el log de descifrado. Seleccione y añada las columnas (información) que desee incluir en el informe personalizado. Si no desea perfeccionar más el informe personalizado, haga clic en **OK (Aceptar)** para generar el informe.

4. Si lo desea, perfeccione la salida del informe de descifrado personalizado mediante el generador de consultas y las cuatro plantillas introducidas en PAN-OS 10.0. Para seleccionar una plantilla para filtrar la salida del informe, haga clic en **Cargar plantilla** y seleccione una de las cuatro plantillas de descifrado:



La columna **Query (Consulta)** muestra la consulta de filtro que representa cada plantilla. **Cargue** la consulta deseada y, a continuación, haga clic en **OK (Aceptar)** para generar el informe personalizado.

© 2020 Palo Alto Networks, Inc.

Parámetros no compatibles mediante tipo de proxy y versión de TLS

Los campos del log de descifrado muestran los parámetros de la sesión de descifrado para cada tipo de proxy de descifrado. Sin embargo, por razones como la compatibilidad con la versión, las partes cifradas de los protocolos de enlace TLS, la disponibilidad de la información, etc., algunos parámetros no están disponibles para todos los tipos de proxy o versiones de TLS. La siguiente tabla muestra los parámetros de log de descifrado no admitidos por tipo de proxy y versión de TLS.

Tipo de proxy	Parámetro no admitido	Versión de TLS
Proxy de reenvío	Negotiated EC Curve (Curva EC negociada)	TLSv1.3
Inspección de entrada	Server Name Identification (Identificación del nombre del servidor) Root Common Name (Nombre común raíz)	All (Todas)
	Negotiated EC Curve (Curva EC negociada)	TLSv1.3
Sin descifrar (acción <t1> Sin descifrar </t1> en la regla de política de descifrado)	Negotiated EC Curve (Curva EC negociada) Server Name Identification (Identificación del nombre del servidor)	TLSv1.2
	Negotiated EC Curve (Curva EC negociada) Server Name Identification (Identificación del nombre del servidor) Información del certificado (todos los campos de información del certificado, por ejemplo, fecha de inicio del certificado, fecha de finalización del certificado, tipo de clave del certificado, etc.)	TLSv1.3
Agente de descifrado	Negotiated EC Curve (Curva EC negociada)	TLSv1.3
Portal GlobalProtect	Server Name Identification (Identificación del nombre del servidor) Root Common Name (Nombre común raíz) Decryption policy name (Nombre de la política de descifrado) App-ID	All (Todas)
Puerta de enlace GlobalProtect	Server Name Identification (Identificación del nombre del servidor) Decryption policy name (Nombre de la política de descifrado) App-ID	All (Todas)

© 2020 Palo Alto Networks, Inc.

Tipo de proxy	Parámetro no admitido	Versión de TLS
Clientless SSLVPN (SSLVPN sin cliente)	Server Name Identification (Identificación del nombre del servidor)	All (Todas)
SSH	Decryption Log Not Supported (Log de descifrado no compatible)	
Texto no cifrado	Decryption Log Not Supported (Log de descifrado no compatible)	

Ejemplos de flujo de trabajo de solución de problemas de descifrado

Los Log de descifrado y los widgets de actividad SSL en el Centro de control de aplicaciones (ACC) proporcionan potentes herramientas de resolución de problemas de descifrado que funcionan de forma independiente y conjunta. Cuando comprenda cómo utilizar estas herramientas, podrá investigar y solucionar una amplia gama de problemas de descifrado.

Los siguientes ejemplos le muestran cómo utilizar las herramientas de resolución de problemas para identificar, investigar y solucionar problemas de descifrado. Aplique estos métodos para solucionar cualquier problema que encuentre en su implementación de descifrado.

- Investigación de motivos de error de descripción
- Solución de problemas de conjuntos de cifrado no compatibles
- Identificación de protocolos y conjuntos de cifrado débiles
- Identificación de certificados de CA no fiables
- Solución de problemas de certificados expirados
- Solución de problemas de certificados revocados
- Solución de problemas de certificados fijados

Investigación de motivos de error de descripción

Las razones más comunes de los fallos de descifrado son errores de protocolo TLS, errores de versión de cifrado (desajustes de versión de cliente y servidor y también desajustes de versión de cliente y perfil de descifrado) y errores de certificado. Para investigar errores de descifrado, comience con el Centro de control de aplicaciones (ACC, Application Command Center) para identificar fallos y, a continuación, vaya a los logs de descifrado para profundizar en los detalles.

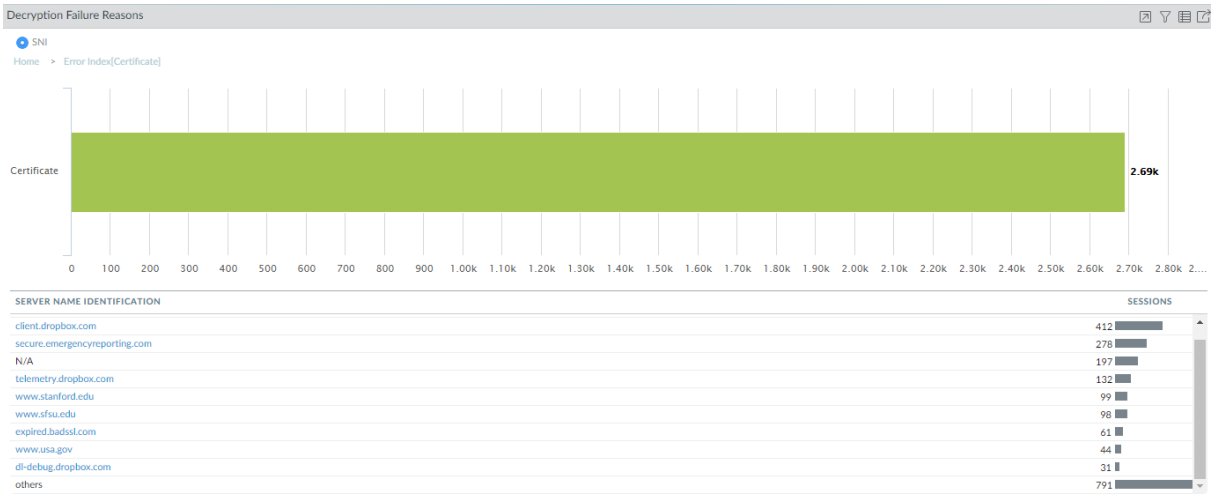
STEP 1 | Comience su investigación en **ACC** > **SSL Activity (Actividad SSL)** y observe el widget de motivos de fallo de descifrado.

© 2020 Palo Alto Networks, Inc.



En este ejemplo, investigamos los errores de certificado. Puede utilizar el mismo proceso para investigar errores de versión y protocolo.

STEP 2 | Haga clic en la barra verde junto a **Certificate (Certificado)** para ver qué hosts (SNI) experimentaron errores de certificado y consultar una lista de los hosts que experimentaron la mayor cantidad de errores de certificado.



STEP 3 | Diríjase a **Monitor (Supervisar)** > **Logs** > **Decryption (Descifrado)** para profundizar en los logs.

Utilice la consulta **`(err_index eq Certificate)`** para filtrar los logs de descifrado para ver todas las sesiones de descifrado que experimentaron errores de certificado.

© 2020 Palo Alto Networks, Inc.

(err_index eq Certificate)

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 11:17:14	203671	ssl	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:14	203669	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203666	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203663	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203598	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203576	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/08 11:16:18	203575	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

La columna **Error** muestra el motivo del error del certificado. Para filtrar todas las sesiones de descifrado que tuvieron el mismo error, haga clic en el mensaje de error para añadirlo a la consulta y, a continuación, ejecutar la consulta. Por ejemplo, para encontrar todos los errores basados en recibir una alerta fatal del cliente, si se hace clic en el error, se produce la consulta **`(err_index eq Certificate) y (error eq 'Received fatal alert CertificateUnknown from client')`**:

(err_index eq Certificate) and (error eq 'Received fatal alert CertificateUnknown from client')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205206	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123732	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

Para filtrar los errores de certificado que recibió un host específico, añada esa SNI a la consulta en lugar de agregar el texto del mensaje de error. Por ejemplo, para encontrar todos los errores de certificado de expired.badssl.comm, utilice la consulta **`(err_index eq Certificate) y (sni eq 'expired.badssl.com')`**:

(err_index eq Certificate) and (sni eq 'expired.badssl.com')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/02 17:17:20	12959	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12957	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12955	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12958	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12956	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12951	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:11:48	12802	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt

La columna **Error** muestra el motivo específico de cada error de certificado asociado con expired.badssl.com.

Una vez que sepa el motivo del problema del certificado que provocó el error de descifrado, podrá solucionarlo. Por ejemplo, si la cadena de certificados está incompleta, puede reparar la cadena de certificados incompleta. Si un certificado está caducado, puede notificarlo al administrador del sitio o crear una excepción basada en políticas si necesita acceder al sitio.

© 2020 Palo Alto Networks, Inc.

Solución de problemas de conjuntos de cifrado no compatibles

Identificar los conjuntos de cifrado no compatibles en el log de descifrado y solucionar sus problemas es un aspecto de la investigación de error de versión que merece la pena examinar por sí solo.

STEP 1 | En el log de descifrado (**Monitor [Supervisar]** > **Logs** > **Decryption [Descifrado]**), use la consulta **`(error contains 'Client and decrypt profile mismatch'`** para identificar todas las discrepancias de versiones del conjunto de cifrado.

Al filtrar los logs para estas discrepancias, se detectan todas las instancias en las que el cliente y la compatibilidad con el conjunto de cifrado del perfil de descifrado no coinciden.

(error contains 'Client and decrypt profile version mismatch')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

Para detectar todas las sesiones de descifrado que experimentaron el mismo error, haga clic en el mensaje de error para añadirlo a la consulta y eliminar la consulta original, por ejemplo:

(error eq 'Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. ')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:51	99251	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:51	99250	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:46	99249	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:46	99248	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 08:41:21	98685	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

Los códigos hexadecimales identifican la versión exacta que admite el cliente y la versión exacta que admite el perfil de descifrado.

STEP 2 | Inicie sesión en la CLI y busque los valores de la máscara de bits.

Los errores muestran una discrepancia entre el cliente y el perfil de descifrado. La máscara de bits del cliente admitida es 0x08 y la de descifrado es 0x70:

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```


© 2020 Palo Alto Networks, Inc.

Este resultado muestra que el cliente solo admite TLSv1.0.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

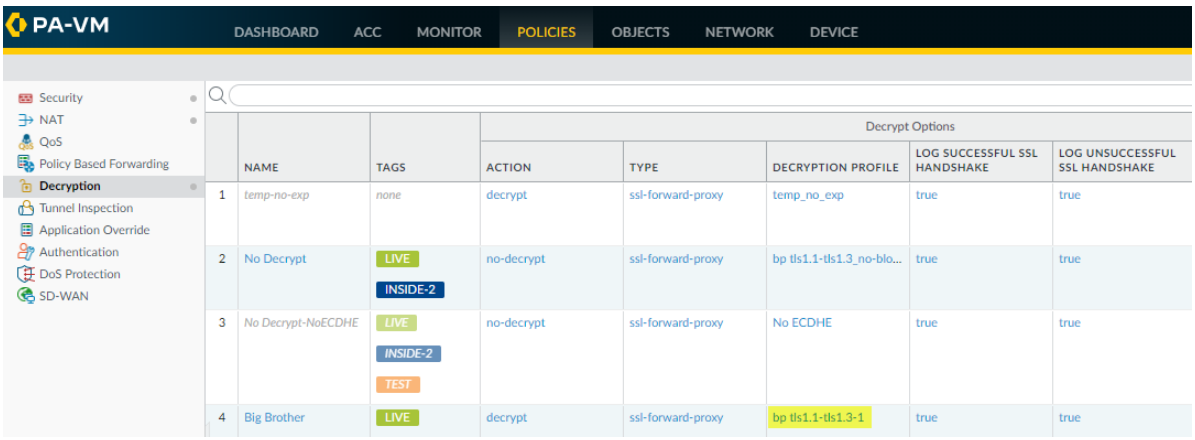
Este resultado muestra que el perfil de descifrado admite TLSv1.1, TLSv1.2 y TLSv1.3, pero no TLSv1.0. Ahora sabe que el cliente solo admite una versión antigua del protocolo TLS y el perfil de descifrado adjunto a la regla de política de descifrado que controla el tráfico no permite esa versión.

STEP 3 | Decida qué acción tomar.

Puede actualizar el cliente para que acepte una versión TLS más segura. Si el cliente requiere TLSv1.0 por alguna razón, puede continuar dejando que el cortafuegos continúe bloqueando el tráfico, puede actualizar el perfil de descifrado para permitir todo el tráfico TLSv1.0 (no recomendado) o puede crear una política de descifrado y perfil que permitan TLSv1.0 y aplicarlo solo a los dispositivos cliente que deben usar TLSv1.0 y no pueden admitir un protocolo más seguro (la opción más segura para permitir el tráfico).

STEP 4 | Si elige editar el perfil de descifrado, para encontrar la política de descifrado que controla el tráfico de la sesión, verifique la columna **Policy Name (Nombre de la política)** en el log (o haga clic en el icono de la lupa junto al log de descifrado para ver la información en la sección General de la vista de registro detallada).

1. En este ejemplo, el nombre de la política de descifrado es Big Brother (Gran Hermano); para encontrar el perfil de descifrado, diríjase a **Policies (Políticas)** > **Decryption (Descifrado)** y active la columna **Decryption Profile (Perfil de descifrado)**.



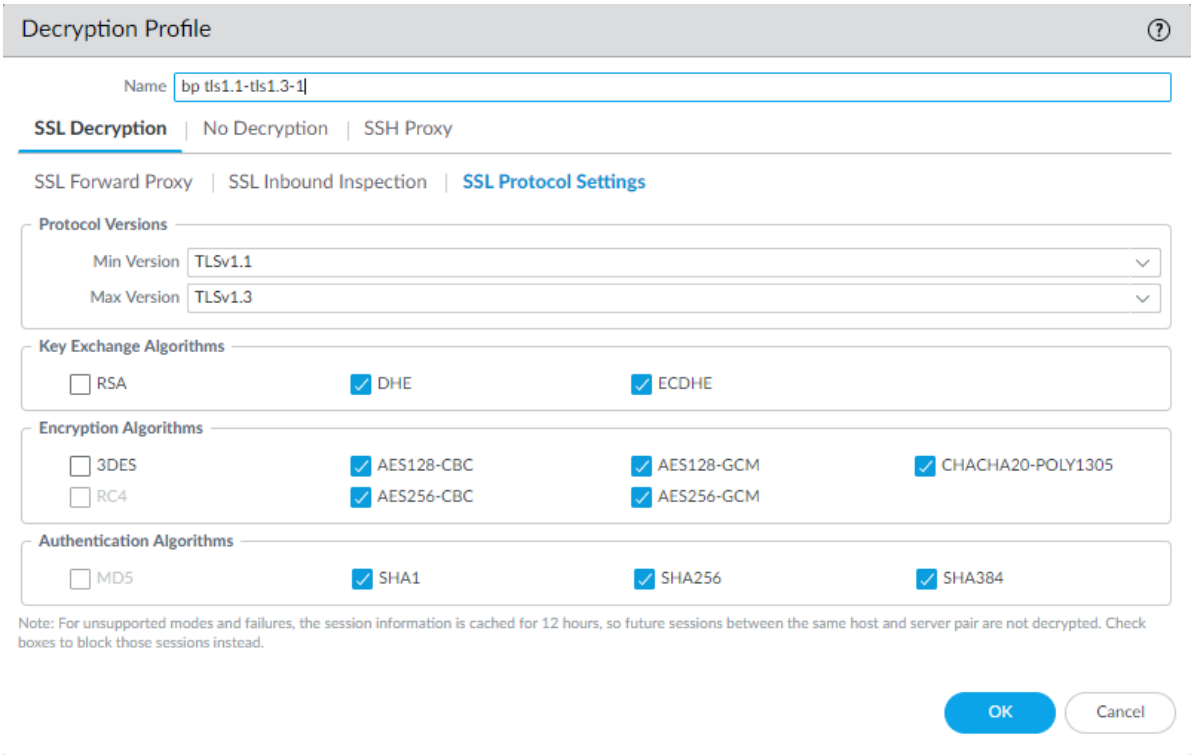
El nombre del perfil de descifrado es **bp tls1.1-tls1.3-1**. También puede seleccionar la política Big Brother (Gran Hermano) y, a continuación, seleccionar la pestaña **Options (Opciones)** para ver el nombre del perfil de descifrado.

Diríjase a **Objects (Objetos)** > **Decryption (Descripción)** > **Decryption Profile (Perfil de descifrado)**, seleccione el perfil de descifrado adecuado y edítelo para solucionar el problema de la versión.

2. Diríjase a **Objects (Objetos)** > **Decryption (Descifrado)** > **Decryption Profile (Perfil de descifrado)**.

© 2020 Palo Alto Networks, Inc.

Seleccione el perfil de descifrado **bp tls1.1-tls1.3-1** y haga clic en la pestaña **SSL Protocol Settings (Configuración del protocolo SSL)**.



La versión mínima del protocolo TLS (**Min Version [Versión mín.]**) que admite el perfil es TLSv1.1. Para permitir el tráfico que bloquea la falta de coincidencia de versiones, puede cambiar la **versión mínima** a TLSv1.0. Sin embargo, una opción más segura es actualizar el cliente para usar una versión reciente del protocolo TLS. Si no puede actualizar el cliente, puede crear una política y un perfil de descifrado que se apliquen solo a ese usuario, dispositivo o dirección de origen (y a cualquier usuario, dispositivo o dirección de origen similar para que una política y un perfil controlen todos de este tráfico) en lugar de aplicar una política general de descifrado que permita el tráfico TLSv1.0.

Identificación de protocolos y conjuntos de cifrado débiles

Los protocolos TLS y los conjuntos de cifrado débiles (algoritmos de cifrado, algoritmos de autenticación, algoritmos de intercambio de claves y curvas EC negociadas) debilitan su estrategia de seguridad y son más fáciles de explotar para los actores maliciosos que los protocolos TLS y los conjuntos de cifrado sólidos.

Hay cinco campos en las entradas del log de descifrado que muestran el protocolo y los conjuntos de cifrado para una sesión de descifrado:

TLS VERSION	ENCRYPTION ALGORITHM	KEY EXCHANGE	AUTHENTICATI... ALGORITHM	NEGOTIATED EC CURVE
TLS1.2	AES_128_GCM	ECDHE	SHA256	secp256r1
TLS1.2	AES_256_GCM	ECDHE	SHA384	secp256r1

Rastree versiones antiguas y vulnerables de TLS y conjuntos de cifrado para tomar decisiones informadas sobre si permitir conexiones con servidores y aplicaciones que puedan comprometer su estrategia de seguridad.

Los ejemplos de este tema muestran cómo:

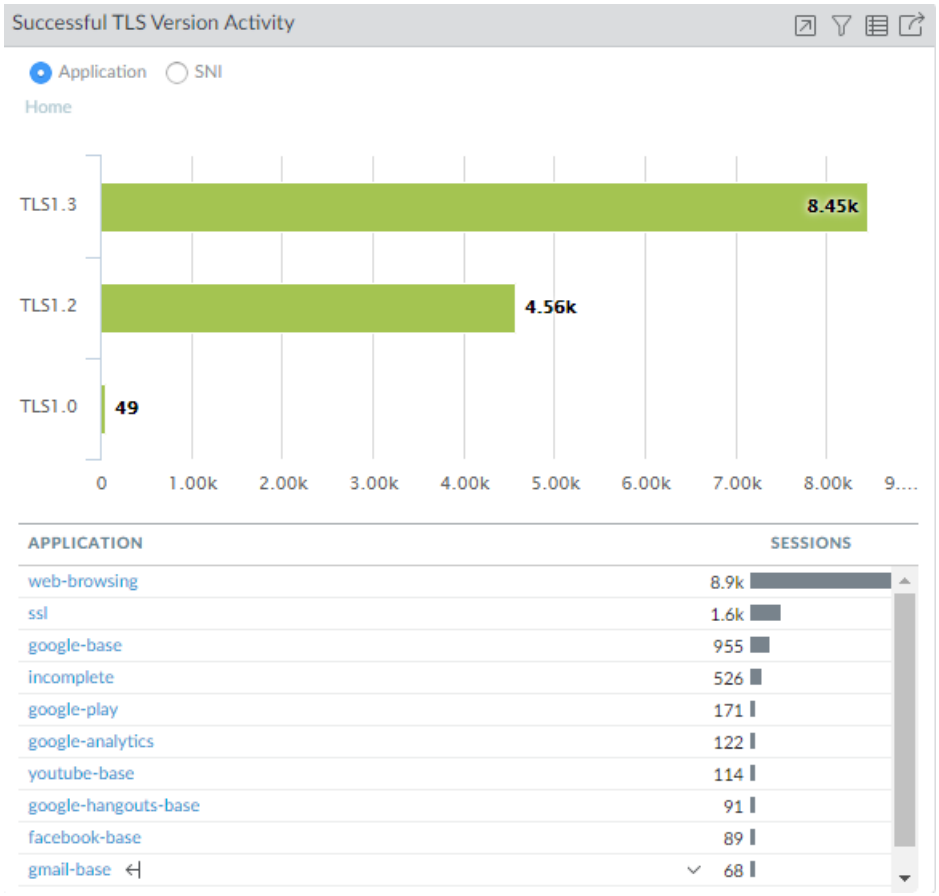
© 2020 Palo Alto Networks, Inc.

- Identificar el tráfico que utiliza versiones del protocolo TLS menos seguras.
- Identificar el tráfico que utiliza un algoritmo de intercambio de claves en particular.
- Identificar el tráfico que utiliza un algoritmo de autenticación particular.
- Identificar el tráfico que utiliza un algoritmo de cifrado particular.

Estos ejemplos le muestran cómo utilizar las herramientas de resolución de problemas de descifrado de varias formas para que pueda aprender a utilizarlas para solucionar cualquier problema de descifrado con el que se pueda encontrar.

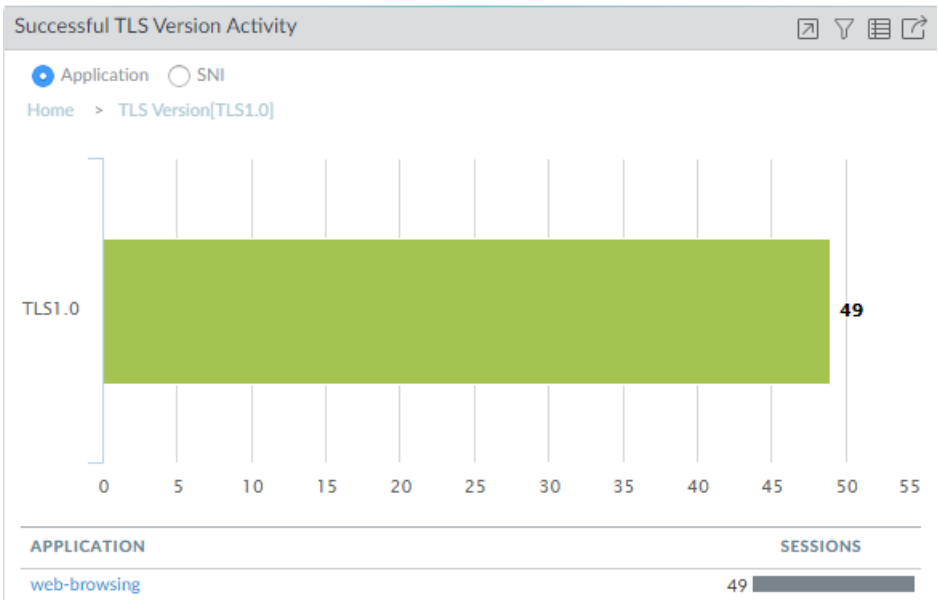
Puede usar Wireshark u otros analizadores de paquetes para verificar si el cliente o el servidor provocaron un problema, las versiones de cliente y servidor TLS y otra información del conjunto de cifrado. Esto puede ayudar a analizar las discrepancias de versiones y otros problemas.

- **TLS Protocols (Protocolos TLS)**: identifique el tráfico que usa versiones más antiguas y menos seguras del protocolo TLS para que pueda evaluar si permitir el acceso a servidores y aplicaciones que usan protocolos débiles.
  1. Primero verifique el Centro de comando de aplicaciones (ACC, Application Command Center) para ver si el cortafuegos permite protocolos débiles (**ACC** > **SSL Activity [Actividad de SSL]** > **Successful TLS Version Activity [Actividad de versión de TLS correcta]**) y para obtener una visión general de la actividad.



La mayor parte de la actividad de TLS correcta en este ejemplo es la actividad de TLSv1.2 y TLSv1.3. Sin embargo, hay algunos casos de tráfico TLSv1.0 permitido. Hagamos clic en el número **49** para profundizar en la actividad de TLSv1.0 y ver qué aplicaciones están haciendo conexiones TLSv1.0 correctas:

© 2020 Palo Alto Networks, Inc.

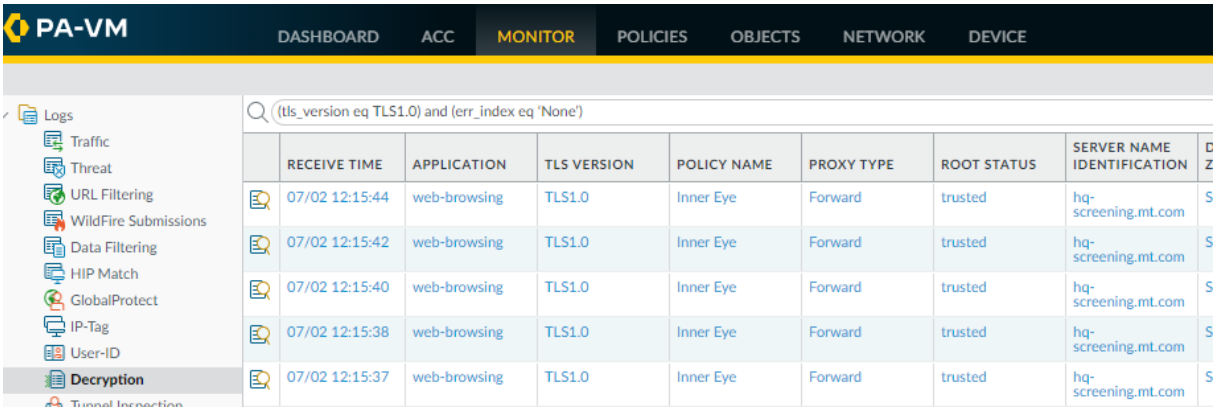


Vemos que el cortafuegos está permitiendo el tráfico identificado como tráfico de navegación web. Para obtener información sobre qué es ese tráfico de navegación web TLSv1.0 y por qué está permitido, iremos a los logs de descifrado.

2. Filtre el log de descifrado para verificar los detalles de la actividad TLSv1.0.

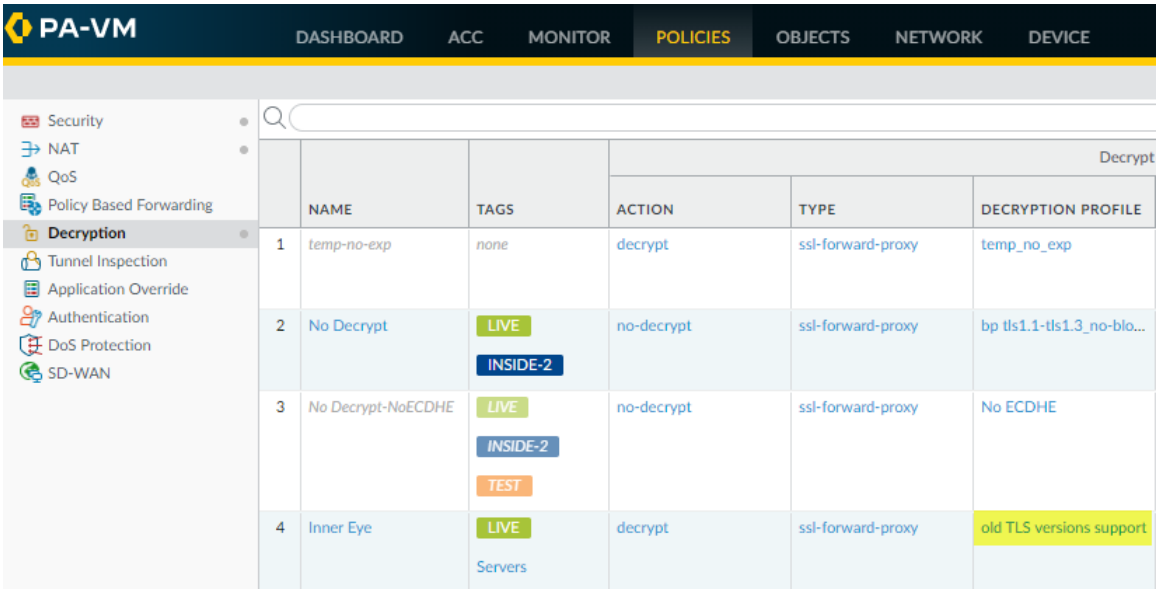
   Utilice la consulta **`(tls_version eq TLS1.0) y (err_index eq 'None')`** para ver sesiones de descifrado de TLSv1.0 correctas.

   Los logs de descifrado muestran una actividad TLS correcta solo si habilita el log de protocolos de enlace TLS correctos en la política de descifrado cuando Configuración de logs de descifrado. Si el log de protocolos de enlace TLS correctos está deshabilitado, no puede verificar esta información.

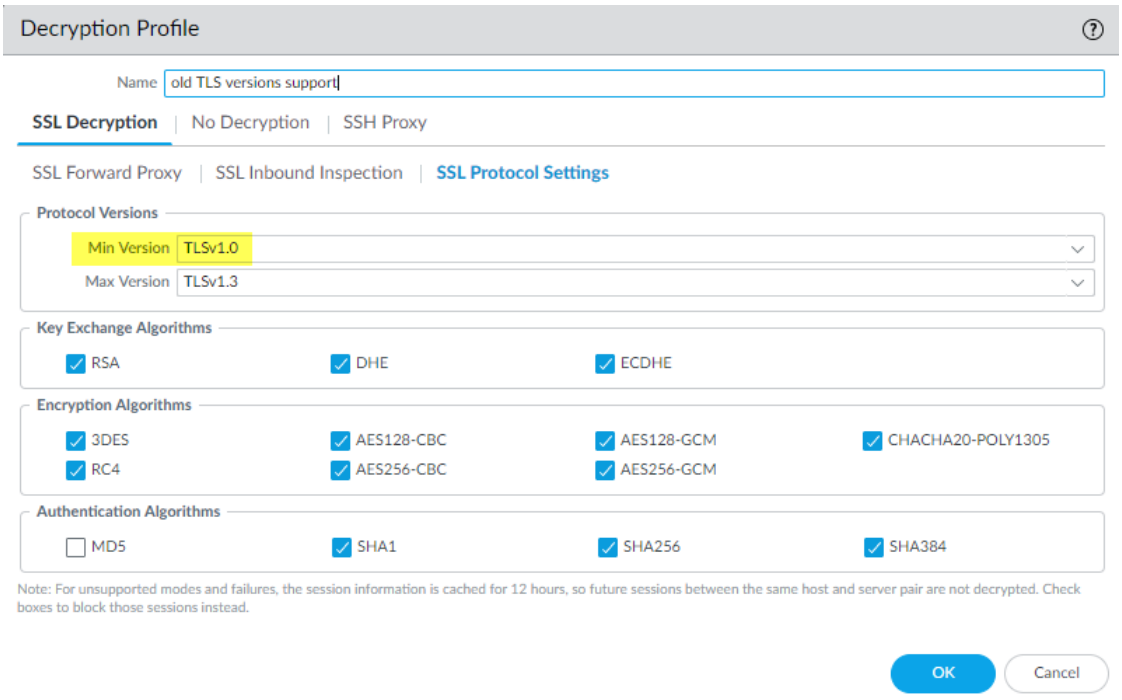


El log de descifrado nos muestra que el nombre de la política de descifrado que controla el tráfico es **Inner Eye** y que el nombre del host es **hq-screening.mt.com**. Ahora conocemos el sitio que usa TLSv1.0 y podemos verificar la política de descifrado (**Policies [Políticas]** > **Decryption [Descifrado]**) para encontrar el perfil de descifrado que controla el tráfico y saber por qué se permite el tráfico:

© 2020 Palo Alto Networks, Inc.



Vemos que el perfil de descifrado asociado con la política es **old TLS versions support (compatibilidad con versiones de TLS antiguas)**. Verificamos el perfil (**Objects [Objetos]** > **Decryption [Descripción]** > **Decryption Profile [Perfil de descripción]**) y observamos la configuración del protocolo SSL para averiguar exactamente cuál es el tráfico que permite el perfil:



El perfil permite el tráfico TLSv1.0. Lo siguiente que debe hacer es decidir si desea permitir el acceso al sitio (¿necesita acceso para fines empresariales?) o si desea bloquearlo.

Otro escenario común que da como resultado que el cortafuegos permita el tráfico que usa protocolos menos seguros es cuando ese tráfico no está descifrado. Cuando filtra el log de descifrado para el tráfico TLSv1.0, si la columna **Proxy Type (Tipo de proxy)** contiene el valor **No Decrypt (Sin descifrado)**, una política sin descifrado controla el tráfico, por lo que el cortafuegos no lo descifra

© 2020 Palo Alto Networks, Inc.

ni inspecciona. Si no desea permitir el protocolo débil, modifique el perfil de descifrado para que bloquee el tráfico TLSv1.0.

Hay muchas formas de filtrar el log de descifrado para encontrar aplicaciones y sitios que utilizan protocolos débiles, por ejemplo:

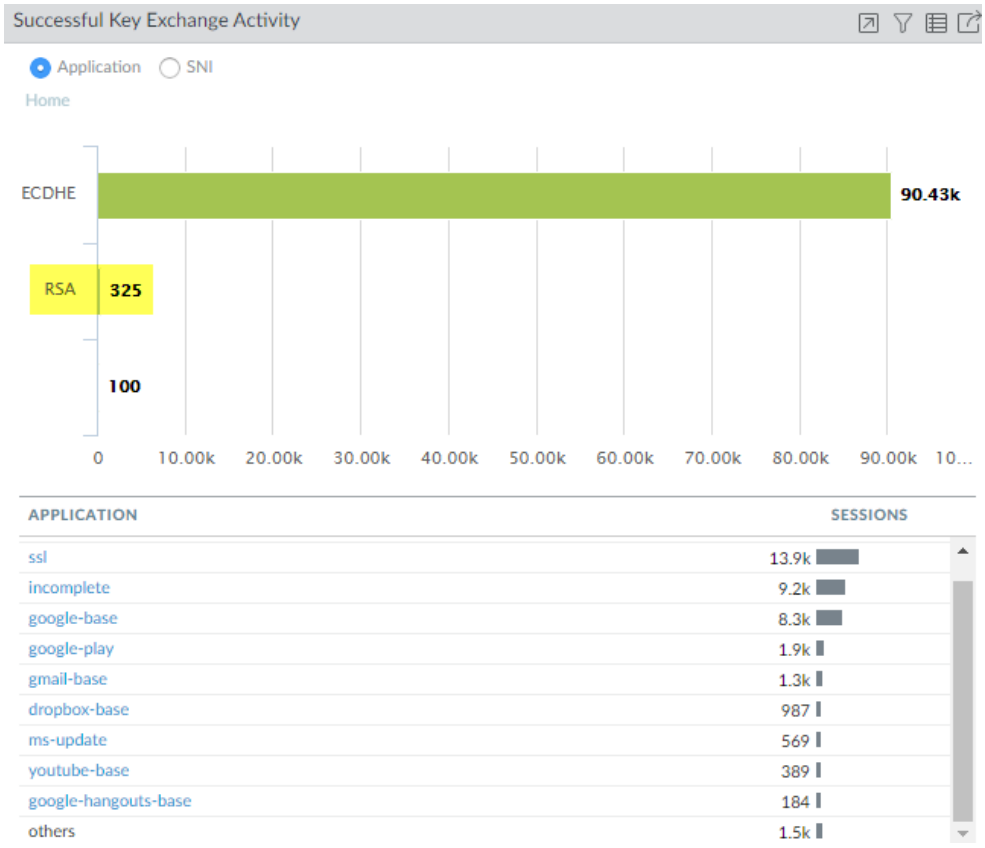
- En lugar de filtrar solo para protocolos de enlace TLSv1.0 correctos, filtre los protocolos de enlace TLSv1.0 correctos y no correctos mediante la consulta **`(tls_version eq TLS1.0)`**.
- Filtre solo para los protocolos de enlace TLSv1.0 fallidos mediante la consulta **`(tls_version eq TLS1.0) y (err_index neq 'None')`**.
- Filtre todos los protocolos menos seguros (TLSv1.1 y anteriores) mediante la consulta **`(tls_version leq tls1.1)`**.

Si desea filtrar los logs para otras versiones de TLS, simplemente reemplace **`TLS1.0`** o **`TLS1.1`** por otra versión de TLS.

3. Decida qué acción tomar para los sitios que usan protocolos TLS débiles.
   - Si no necesita acceder al sitio con fines empresariales, la acción más segura es bloquear el acceso al sitio editando la política de descifrado y el perfil de descifrado que controlan el tráfico. La columna **Policy Name (Nombre de política)** del log de descifrado proporciona el nombre de la política y la política de descifrado muestra el perfil de descifrado adjunto (pestaña **Options [Opciones]**).
   - Si necesita acceder al sitio con fines empresariales, considere la posibilidad de crear una política de descifrado y un perfil de descifrado que se apliquen solo a ese sitio (o a ese sitio y otros sitios similares) y bloquee el resto del tráfico que utilice protocolos menos seguros.

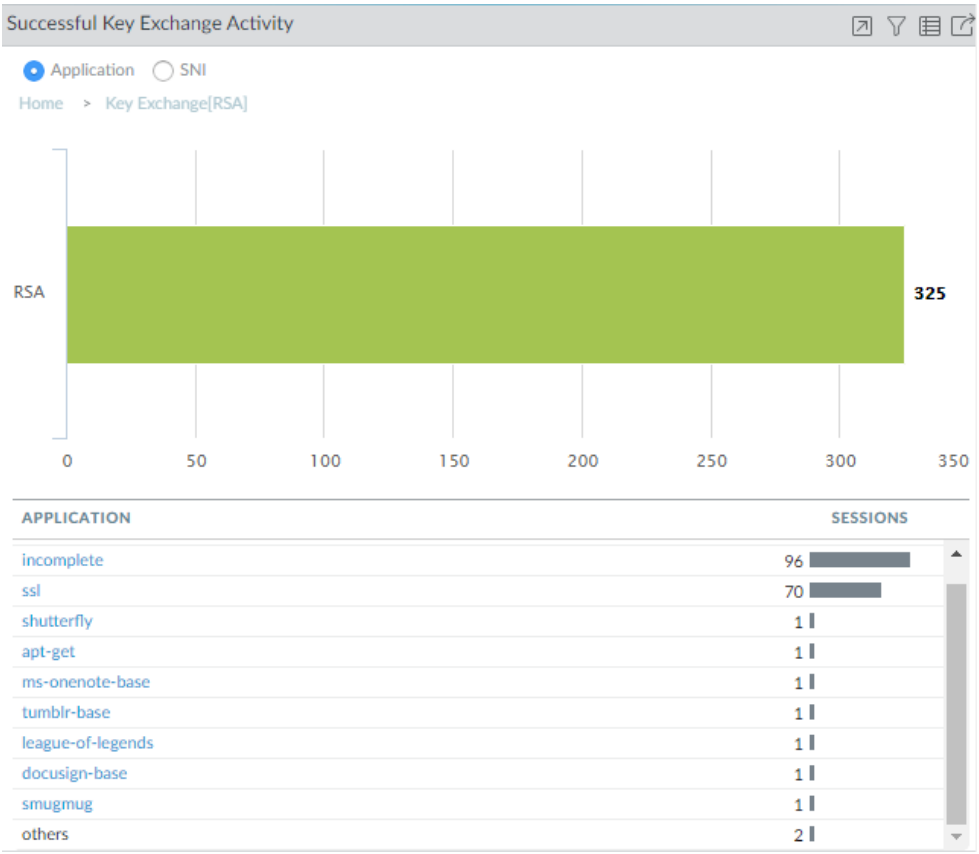
- **Key Exchange (Intercambio de claves)**: permite identificar el tráfico que utiliza algoritmos de intercambio de claves menos seguros.
  1. Comience por verificar el Centro de control de aplicaciones (ACC, Application Command Center) para ver qué algoritmos de intercambio de claves permite el cortafuegos (**ACC** > **SSL Activity [Actividad SSL]** > **Successful Key Exchange Activity [Actividad de intercambio de claves correcta]**) y para obtener una visión general de la actividad.

© 2020 Palo Alto Networks, Inc.



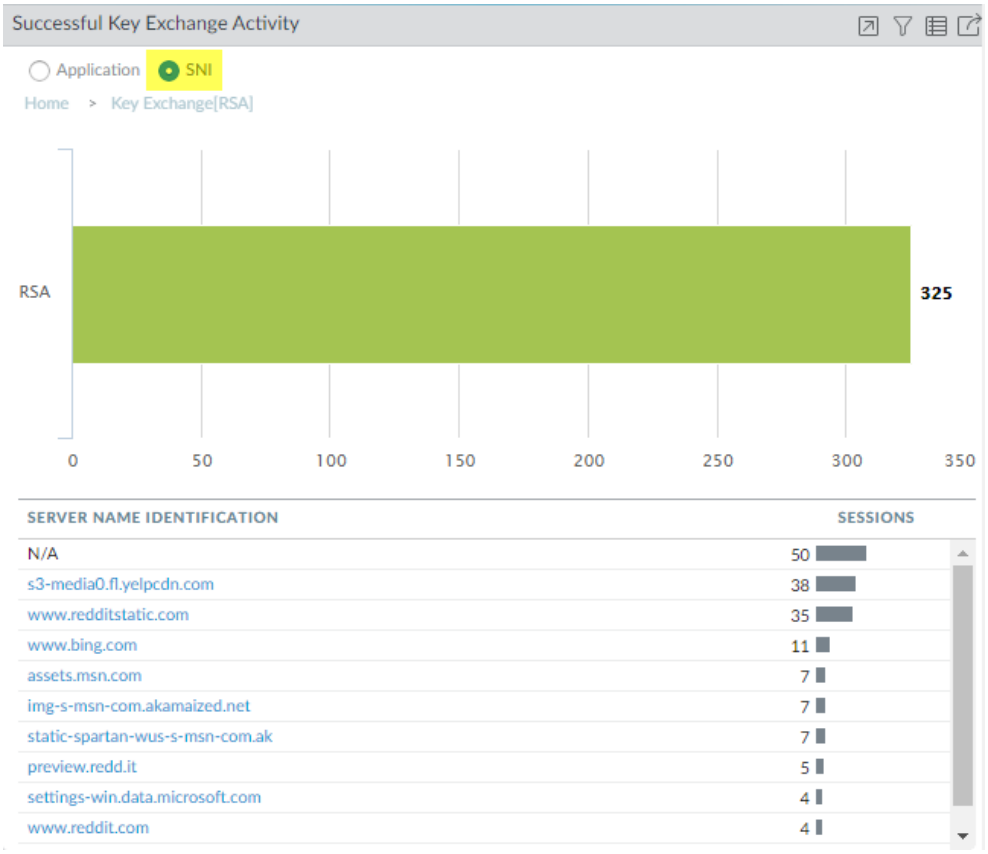
La mayoría de los intercambios de claves utilizan el algoritmo seguro de intercambio de claves ECDHE. Sin embargo, algunas sesiones de intercambio de claves utilizan el algoritmo RSA menos seguro y algunas utilizan otro algoritmo de claves. Para comenzar a investigar el tráfico que utiliza intercambios de claves RSA, por ejemplo, haga clic en el número **325** para profundizar en los datos.

© 2020 Palo Alto Networks, Inc.



El desglose muestra las aplicaciones que utilizan intercambios de claves RSA. También podemos hacer clic en el botón de opción **SNI** para ver los intercambios de claves RSA por SNI:

© 2020 Palo Alto Networks, Inc.



Con esta información, podemos ir a los logs para obtener más contexto sobre el uso del intercambio de claves RSA.

2. Vaya al log de descifrado (**Monitor [Supervisar]** > **Logs** > **Decryption [Descifrado]**) y fíltrelos para las sesiones de descifrado que utilizan la clave RSA intercambiar mediante la consulta **`(tls_keyxchg eq RSA)`**:

(tls_keyxchg eq RSA)

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
	06/04 09:29:50	92884	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
	06/04 09:29:50	92887	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
	06/04 09:29:44	92998	ssl	172.30.200.30	74.120.19.22	TLS1.2	None		No Decrypt
	06/04 09:29:24	92882	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:24	92880	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:23	92874	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:23	92873	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/03 22:30:11	36522	vudu	172.30.100.155	208.79.221.210	TLS1.2	None		Big Brother
	06/03 20:08:57	16896	ssl	172.30.200.30	66.117.28.86	TLS1.2	None		No Decrypt
	06/03 20:08:22	16947	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt

En la columna **Nombre de política** del log, vemos que la política de descifrado **No Decrypt (Sin descifrado)** controla la mayor parte del tráfico que utiliza intercambios de claves RSA y puede deducir que el cortafuegos no descifra el tráfico y lo permite sin inspección. Debido a que el tráfico no se descifra, el cortafuegos no puede identificar la aplicación y lo muestra como **ssl**. Si no desea permitir

© 2020 Palo Alto Networks, Inc.

el tráfico que utiliza intercambios de claves RSA, modifique el perfil de descifrado adjunto a la política de descifrado que controla el tráfico.

Puede añadir a la consulta para filtrar aún más los resultados de un SNI o una aplicación en particular vista en el ACC o en la primera consulta del log de descifrado.

3. Decida qué acción realizar para el tráfico que utiliza algoritmos de intercambio de claves menos seguros.

   Bloquee el acceso a sitios que utilicen protocolos de intercambio de claves menos seguros a menos que necesite acceder a ellos con fines empresariales. Para esos sitios, considere la posibilidad de crear una política de descifrado y un perfil de descifrado que se apliquen solo a ese sitio (o a ese sitio y otros sitios similares) y bloquee el resto del tráfico que utilice algoritmos de intercambio de claves menos seguros.

- Utilice los logs de descifrado para identificar las sesiones que utilizan algoritmos de autenticación más antiguos y menos seguros.

  Filtre el log de descifrado para identificar algoritmos de autenticación más antiguos y menos seguros.

  Por ejemplo, para identificar todas las sesiones que usan el algoritmo SHA1, use la consulta **`(tls_auth eq SHA)`**:

  (tls_auth eq SHA)

	RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM
	06/08 23:12:02	213635	ssl	TLS1.2	None		No Decrypt		SHA
	06/08 11:16:02	203438	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:16:02	203439	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:15:01	203437	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:45:32	196795	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196794	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/04 13:38:36	117329	web-browsing	TLS1.2	None		Big Brother	inegi.org.mx	SHA
	06/04 13:35:01	116980	web-browsing	TLS1.2	None		Big Brother	rupress.org	SHA

  Puede realizar adiciones a la consulta para profundizar más en los resultados. Por ejemplo, puede añadir una SNI en particular, una versión de intercambio de claves (como el filtrado de sesiones SHA1 que también usan intercambios de claves RSA), una versión de TLS o cualquier otra métrica que se encuentre en una columna de log de descifrado.

- Utilice los logs de descifrado para identificar las sesiones que utilizan un algoritmo de cifrado determinado.

  Por ejemplo, para identificar todas las sesiones que utilizan el algoritmo de cifrado AES-128-CBC, utilice la consulta **`(tls_enc eq AES_128_CBC)`**:

© 2020 Palo Alto Networks, Inc.

(tls_enc eq AES_128_CBC)

RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM	ENCRYPTION ALGORITHM
06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA	AES_128_CBC
06/04 13:26:57	116215	web-browsing	TLS1.2	None		Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
06/04 13:26:43	116215	web-browsing	TLS1.2	Protocol	General TLS protocol error	Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
06/04 13:22:11	115821	web-browsing	TLS1.2	None		Big Brother	mvps.org	SHA256	AES_128_CBC
06/04 12:52:15	113040	web-browsing	TLS1.2	None		Big Brother	toysfortots.org	SHA256	AES_128_CBC
06/04 12:51:18	112955	web-browsing	TLS1.2	None		Big Brother	autoriteitpersoonsgegevens.nl	SHA	AES_128_CBC
06/04 12:44:47	112338	web-browsing	TLS1.2	None		Big Brother	uvigo.es	SHA256	AES_128_CBC
06/04 12:31:41	111224	web-browsing	TLS1.2	None		Big Brother	foodallergy.org	SHA256	AES_128_CBC
06/04 12:07:37	109129	web-browsing	TLS1.2	None		Big Brother	capitalone360.com	SHA	AES_128_CBC

Puede realizar adiciones a la consulta para profundizar más en los resultados.

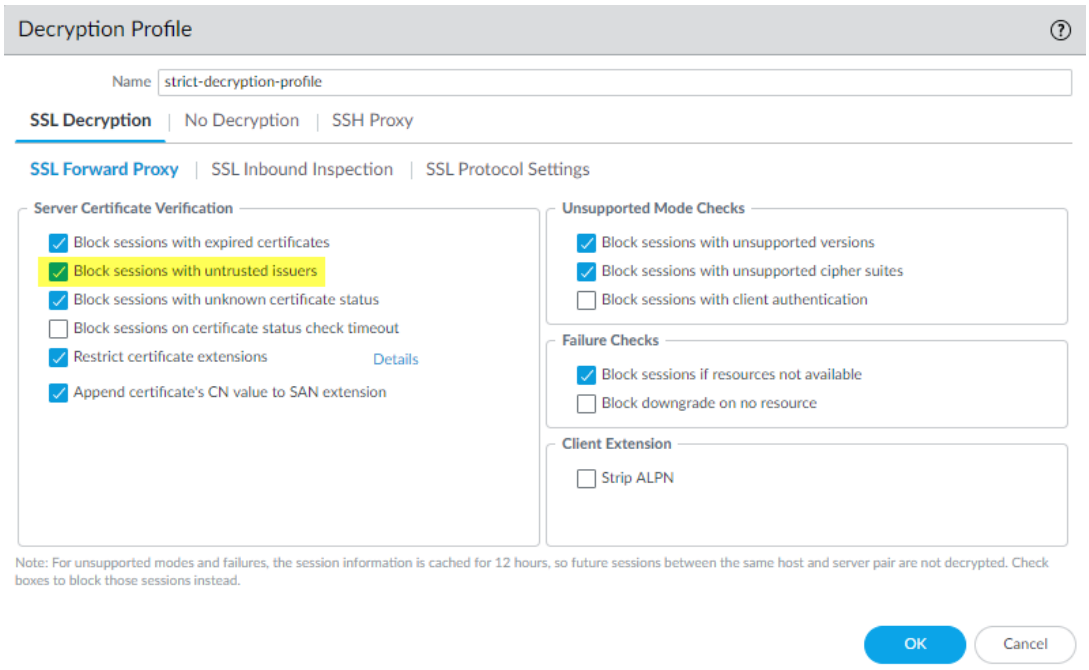
Entre los ejemplos de consultas para encontrar otros algoritmos de cifrado más antiguos se incluyen: `(tls_enc eq DES_CBC)`, `(tls_enc eq 3DES_EDE_CBC)` y `(tls_enc eq DES40_CBC)`.

- Utilice esta metodología y el generador de filtros de logs para crear consultas para investigar las curvas ECC negociadas y cualquier otra información que encuentre en el log de descifrado.

Identificación de certificados de CA no fiables

El bloqueo del acceso a sitios con certificados de CA que no son de confianza y los certificados autofirmados por una CA raíz que no es fiable es una práctica recomendada. Esto se debe a que los sitios con CA que no son de confianza pueden indicar un ataque de intermediario, un ataque de repetición u otra actividad maliciosa.

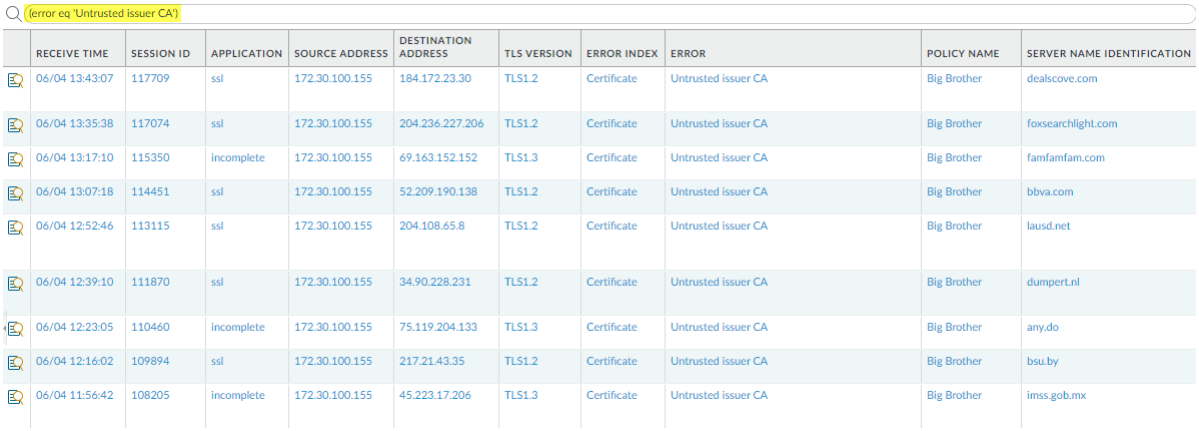
STEP 1 | Asegúrese de **bloquear sesiones con emisores no fiables** en el perfil de descifrado de proxy de reenvío (**Objects [Objetos]** > **Decryption [Descripción]** > **Decryption Profiles [Perfiles de descifrado]**) para bloquear sitios con CA que no son de confianza.



© 2020 Palo Alto Networks, Inc.

Cuando bloquea sesiones con emisores que no son de confianza en el perfil de descifrado, el log de descifrado (**Monitor (Supervisar)** > **Logs** > **Decryption (Descifrado)**) registra el error.

STEP 2 | Filtre el log para identificar las sesiones que fallaron debido a certificados revocados mediante la consulta **`(error eq 'Untrusted issuer CA')`**.



RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION
06/04 13:43:07	117709	ssl	172.30.100.155	184.172.23.30	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dealscove.com
06/04 13:35:38	117074	ssl	172.30.100.155	204.236.227.206	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	foxsearchlight.com
06/04 13:17:10	115350	incomplete	172.30.100.155	69.163.152.152	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	famfamfam.com
06/04 13:07:18	114451	ssl	172.30.100.155	52.209.190.138	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bbva.com
06/04 12:52:46	113115	ssl	172.30.100.155	204.108.65.8	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	lausd.net
06/04 12:39:10	111870	ssl	172.30.100.155	34.90.228.231	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dumpert.nl
06/04 12:23:05	110460	incomplete	172.30.100.155	75.119.204.133	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	any.do
06/04 12:16:02	109894	ssl	172.30.100.155	217.21.43.35	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bsu.by
06/04 11:56:42	108205	incomplete	172.30.100.155	45.223.17.206	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	imss.gob.mx

STEP 3 | (Opcional) Vuelva a verificar la fecha de caducidad del certificado en el sitio de Qualys SSL Labs.

Especifique el nombre de host del servidor (columna **Server Name Identification (Identificación de nombre de servidor)** del log de descifrado) en el campo **Hostname (Nombre de host)** y **envíelo** para ver la información del certificado para el host.

Solución de problemas de certificados expirados

Si sigue las prácticas recomendadas de descifrado y **bloquea sesiones con certificados caducados** en el perfil de descifrado de proxy de reenvío o en el perfil sin descifrado, el cortafuegos bloquea la sesión si un servidor presenta un certificado caducado. Sin embargo, si el sitio al que necesita acceder por razones empresariales permite que su certificado caduque, las conexiones a ese sitio pueden bloquearse y es posible que no sepa por qué.

Puede utilizar el log de descifrado para comprobar si hay certificados caducados y si hay certificados que expirarán pronto, de modo que pueda estar al tanto de la situación y tomar las medidas adecuadas.

STEP 1 | Filtre el log de descifrado para certificados caducados mediante la consulta **`(error eq 'Expired server certificate')`**.

© 2020 Palo Alto Networks, Inc.

(error eq 'Expired server certificate')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	POLICY NAME
06/04 16:19:49	121352	incomplete	172.30.100.10	34.225.62.221	TLS1.3	Certificate	Expired server certificate	www.stanford.edu	Big Brother
06/04 13:43:26	117747	incomplete	172.30.100.155	104.197.149.89	TLS1.3	Certificate	Expired server certificate	phone.com	Big Brother
06/04 13:41:03	117572	incomplete	172.30.100.155	208.117.9.16	TLS1.3	Certificate	Expired server certificate	netcarshow.com	Big Brother
06/04 13:38:51	117379	ssl	172.30.100.155	69.172.200.184	TLS1.2	Certificate	Expired server certificate	royal.gov.uk	Big Brother
06/04 13:36:27	117150	ssl	172.30.100.155	107.21.104.61	TLS1.2	Certificate	Expired server certificate	www.uthscsa.edu	Big Brother
06/04 13:34:53	117004	incomplete	172.30.100.155	66.115.56.251	TLS1.3	Certificate	Expired server certificate	gunsamerica.com	Big Brother
06/04 13:33:17	116853	incomplete	172.30.100.155	34.107.140.234	TLS1.3	Certificate	Expired server certificate	skiplagged.com	Big Brother
06/04 13:32:45	116798	ssl	172.30.100.155	104.236.4.58	TLS1.2	Certificate	Expired server certificate	uploading.com	Big Brother
06/04 13:31:28	116655	incomplete	172.30.100.155	35.186.201.59	TLS1.3	Certificate	Expired server certificate	shared.com	Big Brother
06/04 13:29:32	116507	ssl	172.30.100.155	147.139.136.53	TLS1.2	Certificate	Expired server certificate	beautynesia.id	Big Brother
06/04 13:28:56	116426	incomplete	172.30.100.155	45.55.105.190	TLS1.3	Certificate	Expired server certificate	designbundles.net	Big Brother

Esta consulta identifica los servidores que generan errores de `certificado de servidor caducado` El cortafuegos bloquea el acceso a esos servidores debido al certificado caducado.

STEP 2 | (Opcional) Vuelva a verificar la fecha de caducidad del certificado en el sitio de Qualys SSL Labs.

Especifique el nombre de host del servidor (columna **Server Name Identification (Identificación de nombre de servidor)** del log de descifrado) en el campo **Hostname (Nombre de host)** y **envíelo** para ver la información del certificado para el host.

STEP 3 | Filtre el log de descifrado (**Monitor [Supervisar]** > **Logs** > **Decryption [Descifrado]**) para los certificados que caducarán pronto mediante una consulta que identifique las próximas fecha de finalización del certificado.

Por ejemplo, si la fecha de hoy es el 1 de febrero de 2020 y desea darse dos meses para evaluar y prepararse en caso de que los sitios no actualicen sus certificados, consulte el log de descifrado para los certificados que vencen el 1 de abril de 2020 o antes (**`notafter leq '2020/4/01')`**):

(notafter leq '2020/4/01')

RECEIVE TIME	APPLICATION	POLICY NAME	PROXY TYPE	SERVER NAME IDENTIFICATION	ROOT STATUS	TLS VERSION	CERTIFICATE START DATE	CERTIFICATE END DATE
01/09 14:25:38	incomplete	Test 2	Forward	a4.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a2.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a3.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
01/09 14:25:38	incomplete	Test 2	Forward	a.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43

La columna **Certificate End Date (Fecha de finalización del certificado)** muestra la fecha efectiva en la que vence el certificado.

STEP 4 | Determine la acción que tomar para los sitios con certificados caducados.

- Si no necesita acceder al sitio con fines empresariales, la acción más segura es continuar bloqueando el acceso al sitio.
- De lo contrario, realice una de las siguientes acciones:

© 2020 Palo Alto Networks, Inc.

- Póngase en contacto con el administrador del sitio con el certificado caducado y notifique que necesita actualizar o renovar su certificado.
- Cree una política de descifrado que se aplique solo a los sitios con certificados caducados que necesite para fines empresariales y un perfil de descifrado que permita sitios con certificados caducados. No aplique la política a ningún sitio que no necesite para fines empresariales. Cuando un sitio actualice su certificado, elimínelo de la política.

Solución de problemas de certificados revocados

Un certificado revocado ya no es válido. Puede indicar que hay problemas de seguridad con un sitio y que el certificado no es fiable, aunque también existen razones benignas por las que un certificado puede revocarse.



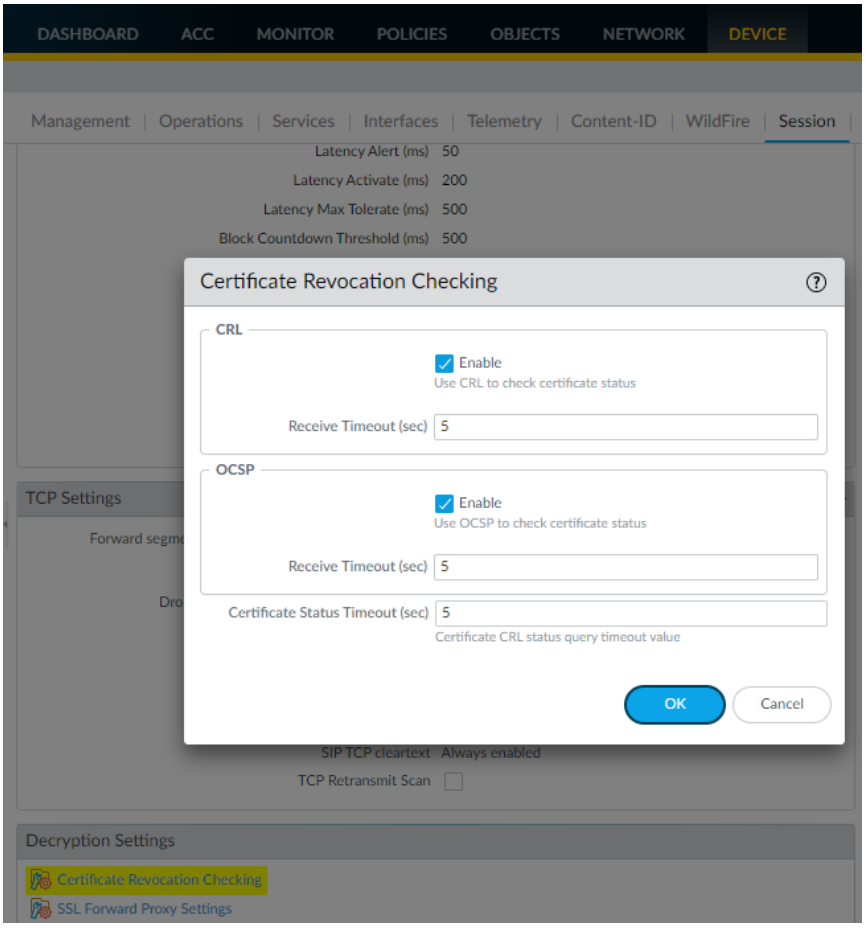
No confíe en los certificados revocados; habilite la verificación de revocación de certificados para denegar el acceso a sitios con certificados revocados.

Para descartar sesiones con certificados revocados y solucionar problemas de certificados revocados, debe habilitar la verificación de revocación de certificados. Si no habilita la verificación de revocación de certificados , el cortafuegos no buscará certificados revocados y no sabrá si un sitio tiene un certificado revocado.

STEP 1 | Habilite la verificación de revocación de certificados si aún no la ha habilitado.

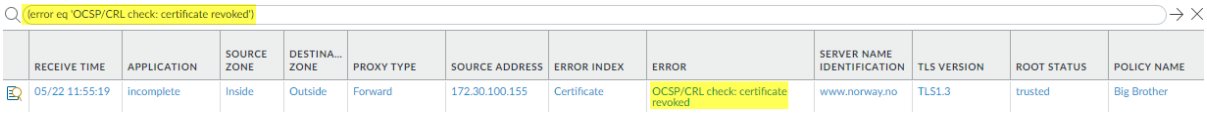
1. Diríjase a **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Configuración de descifrado)**.
2. Habilite la verificación de certificados OCSP y CRL.

© 2020 Palo Alto Networks, Inc.



Si **bloquea sesiones en el tiempo de espera de verificación del estado del certificado** en el perfil de descifrado del proxy de reenvío y le preocupa que 5 segundos no sea suficiente tiempo y pueda generar demasiadas sesiones bloqueadas por tiempos de espera, establezca el **tiempo de espera de recepción (s)** en un período más largo.

STEP 2 | Filtre el log de descifrado (**Monitor [Supervisor]** > **Logs** > **Decryption [Descifrado]**) para detectar errores de revocación de certificados mediante la consulta **`(error eq 'OCSP/CRL check: certificate revoked')`**.



STEP 3 | (Opcional) Vuelva a verificar la fecha de caducidad del certificado en el sitio de Qualys SSL Labs.

Especifique el nombre de host del servidor (columna **Server Name Identification (Identificación de nombre de servidor)** del log de descifrado) en el campo **Hostname (Nombre de host)** y **envíelo** para ver la información del certificado para el host.

Solución de problemas de certificados fijados

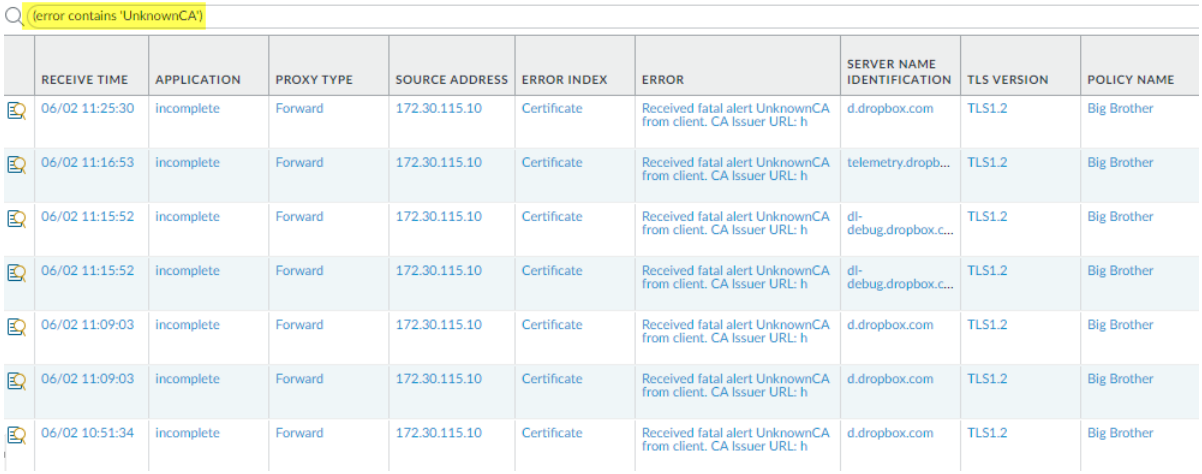
La fijación de certificados obliga a la aplicación cliente a validar el certificado del servidor con una copia conocida para garantizar que el certificado realmente provenga del servidor. La intención de los certificados anclados es proteger contra ataques de tipo man-in-the-middle (MITM) donde un dispositivo entre el cliente y el servidor reemplaza el certificado del servidor por otro certificado.

© 2020 Palo Alto Networks, Inc.

Aunque esto evita que los actores malintencionados intercepten y manipulen las conexiones, también evita el descifrado del proxy de reenvío, ya que el cortafuegos crea un certificado de suplantación en lugar del certificado del servidor para presentarlo al cliente. En lugar de una sesión que conecta el cliente y el servidor directamente, el proxy de reenvío crea dos sesiones, una entre el cliente y el cortafuegos y otra entre el cortafuegos y el servidor. Esto establece confianza con el cliente para que el cortafuegos pueda descifrar e inspeccionar el tráfico.

Sin embargo, cuando se fija un certificado, el cortafuegos no puede descifrar el tráfico porque el cliente no acepta el certificado de suplantación del cortafuegos; el cliente solo acepta el certificado que está anclado a la aplicación.

STEP 1 | Filtre el log de descifrado (**Monitor [Supervisar]** > **Logs** > **Decryption [Descifrado]**) para buscar certificados anclados mediante la consulta **`(error contains 'UnknownCA')`**.



La aplicación genera un código de error TLS (alerta) cuando no puede verificar el certificado del servidor. Diferentes aplicaciones pueden usar distintos códigos de error para indicar un certificado anclado. Los indicadores de error más comunes para los certificados anclados son UnknownCA y BadCertificate. Después de ejecutar la consulta **`(error contains 'UnknownCA')`**, ejecute la consulta **`(error contains 'BadCertificate')`** para detectar más errores de certificados fijados.

Puede usar Wireshark u otros analizadores de paquetes para verificar el error. Busque al cliente que interrumpe la conexión inmediatamente después del protocolo de enlace TLS para confirmar que se trata de un problema de certificado anclado.

STEP 2 | Decida qué hacer con los certificados anclados.

Si no necesita acceso para fines empresariales, puede dejar que el cortafuegos continúe bloqueando el acceso. Si necesita acceso, puede Exclusión de un servidor del descifrado por motivos técnicos añadiéndolo a la lista de exclusión de descifrado SSL (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **SSL Decryption Exclusion [Exclusión de descifrado SSL]**.

El cortafuegos omite el descifrado de los sitios de la lista de exclusión de descifrado SSL. El cortafuegos no puede inspeccionar el tráfico, pero el tráfico está permitido.

© 2020 Palo Alto Networks, Inc.

Agente de descifrado

El agente de descifrado le permite descargar el descifrado SSL en un cortafuegos de nueva generación de Palo Alto Networks y descifrar el tráfico solo una vez. Un cortafuegos habilitado como un agente de descifrado reenvía tráfico de texto sin cifrar a las cadenas de seguridad (conjuntos de dispositivos externos en línea) para aplicación adicional.

Esto le permite consolidar las funciones de seguridad en el cortafuegos y simplificar su implementación de seguridad de red: el agente de descifrado elimina la necesidad de una solución externa de descifrado SSL y le permite reducir el número de dispositivos externos que realizan el análisis y la aplicación de tráfico. En las redes sin un dispositivo de descifrado SSL, el agente de descifrado reduce la latencia debido a que el flujo de tráfico se descifra solo una vez.

El agente de descifrado es compatible con los dispositivos PA-7000 Series, PA-5200 Series, PA-3200 Series y los modelos VM-300, VM-500 y VM-700. Este requiere que se habilite el descifrado de proxy SSL de reenvío, en el cual el cortafuegos se establece como un agente externo fiable (o man-in-the-middle) para el tráfico de sesiones.

Las interfaces de los cortafuegos no pueden actuar como agente de descifrado y como terminal de túneles de GRE.

- Cómo funciona el agente de descifrado
- Conceptos del agente de descifrado
- Pautas de la cadena de seguridad de capa 3
- Configuración de un agente de descifrado con una o más cadenas de seguridad de capa 3
- Pautas de la cadena de seguridad de puente transparente
- Configuración del agente de descifrado con una cadena de seguridad de puente transparente
- Configuración del agente de descifrado con varias cadenas de seguridad de puente transparente

Cómo funciona el agente de descifrado

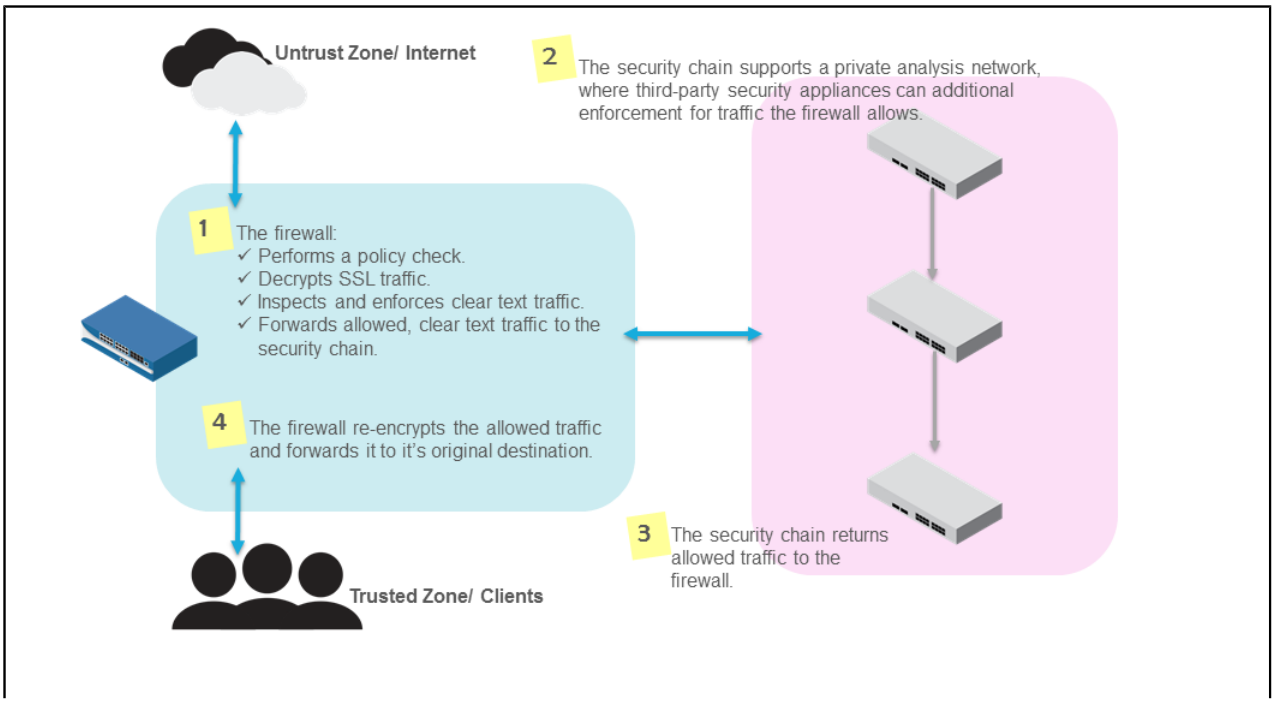
Un cortafuegos configurado para realizar descifrado de proxy SSL de reenvío puede habilitarse como agente de descifrado. El agente de descifrado utiliza interfaces de reenvío de descifrado dedicadas para conectarse con una cadena de seguridad, un conjunto de dispositivos de seguridad externos. El cortafuegos y la cadena de seguridad funcionan en conjunto como un red de análisis privado.

Después de descifrar e inspeccionar el tráfico SSL, el cortafuegos envía únicamente el tráfico sin cifrar permitido a la cadena de seguridad para aplicación y análisis adicional. Dado que la capacidad del cortafuegos para descifrar el tráfico SSL supera la velocidad de procesamiento del dispositivo de seguridad, puede permitir que distribuya sesiones SSL descifradas en varias cadenas de seguridad para evitar suscribir en exceso las cadenas. El primer dispositivo en la cadena de seguridad recibe el tráfico de texto sin cifrar, lo aplica y reenvía el tráfico permitido al siguiente dispositivo en la cadena de seguridad. El último dispositivo de la cadena de seguridad envía el resto del tráfico permitido al cortafuegos. El cortafuegos vuelve a cifrar el tráfico y lo reenvía al destino original.

Se admiten dos tipos de implementaciones de cadena de seguridad: Las cadenas de seguridad de capa 3 y las cadenas de seguridad de puente transparente. Es posible que seleccione el tipo de implementación que desea configurar en función de los dispositivos que conforman su cadena de seguridad (por ejemplo, si utiliza dispositivos con estado o sin estado). Con ambas implementaciones de cadena de seguridad, puede decidir que el cortafuegos dirija el tráfico a través de la cadena de seguridad unidireccional o bidireccionalmente en función de sus necesidades de análisis (consulteAgente de descifrado: flujo de sesión de cadena de seguridad para obtener más información sobre cómo utilizar un flujo unidireccional o bidireccional).

© 2020 Palo Alto Networks, Inc.

La siguiente figura muestra cómo funciona el agente de descifrado.



Conceptos del agente de descifrado

Un cortafuegos que actúa como agente de descifrado utiliza interfaces de reenvío de descifrado dedicadas para enviar tráfico descifrado a una cadena de seguridad (un conjunto de dispositivos de seguridad externos en línea) para un análisis adicional. Un agente de descifrado admite dos tipos de redes de cadena de seguridad (cadenas de seguridad de capa 3 y cadenas de seguridad de puente transparente) y también puede especificar que el cortafuegos dirija el tráfico por la cadena de seguridad de manera unidireccional o bidireccional. Un cortafuegos puede distribuir sesiones descifradas hasta en 64 cadenas de seguridad y puede supervisar las cadenas de seguridad para garantizar que procesen el tráfico con eficacia.

Revise los siguientes temas para obtener más información sobre las funciones y la asistencia técnica del agente de descifrado.

- Agente de descifrado: Interfaces de reenvío
- Agente de descifrado: Cadena de seguridad de capa 3
- Agente de descifrado: Cadena de seguridad de puente transparente
- Agente de descifrado: Flujo de sesión de cadena de seguridad
- Agente de descifrado: Múltiples cadenas de seguridad
- Agente de descifrado: Comprobaciones de estado de la cadena de seguridad

Agente de descifrado: Interfaces de reenvío

Un cortafuegos habilitado como un agente de descifrado utiliza un par de interfaces de capa 3 dedicadas para reenviar tráfico descifrado a una cadena de seguridad para su inspección. Las interfaces de reenvío de descifrado deben asignarse a un enrutador virtual completamente nuevo (que no posea rutas u otras interfaces configuradas que se utilicen para pasar tráfico de plano de datos); esto garantiza que las sesiones de texto sin cifrar que el cortafuegos reenvía a la cadena de seguridad para un análisis adicional se segmenten totalmente del tráfico de plano de datos.

En una implementación de agente de descifrado con una cadena de seguridad de capa 3, un par de dos interfaces de reenvío de descifrado puede admitir hasta 64 cadenas de seguridad.

© 2020 Palo Alto Networks, Inc.

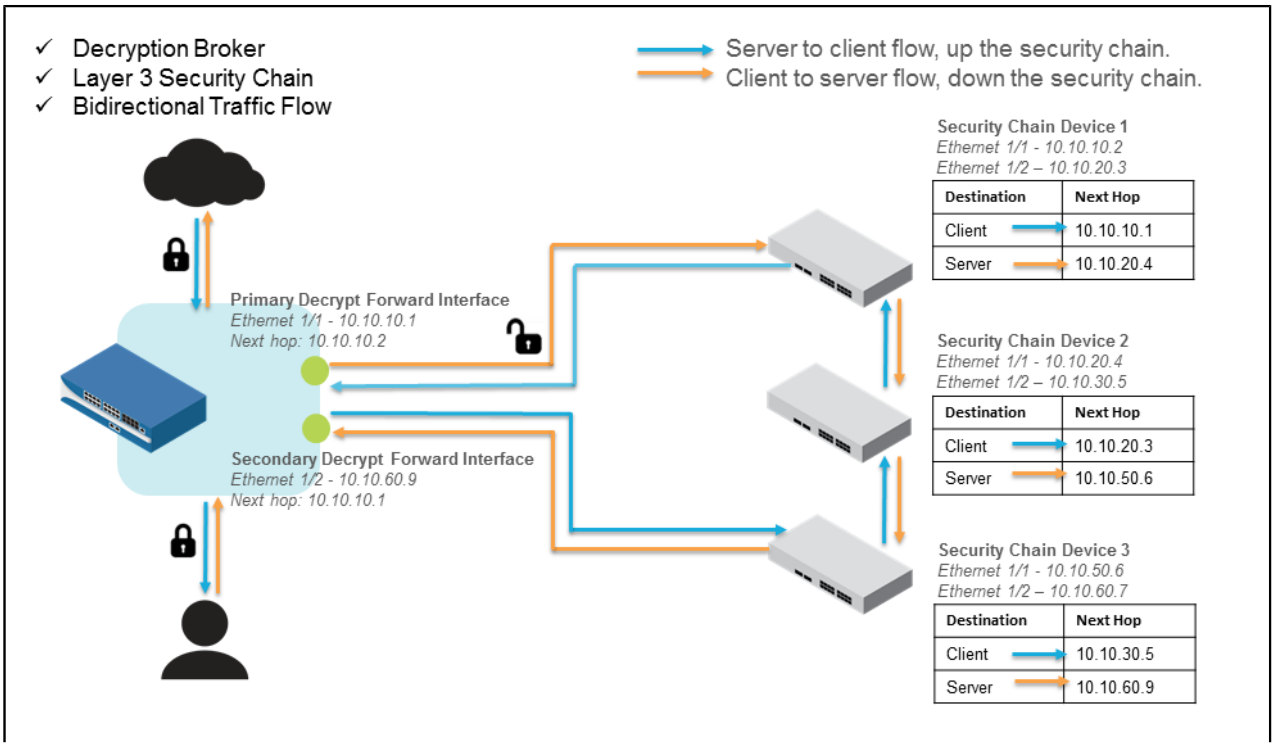
Un par de interfaces de reenvío de descifrado admite una cadena de seguridad de puente transparente. Sin embargo, puede configurar varios pares de interfaces de reenvío de descifrado para admitir varias cadena de seguridad de puente transparente.

Agente de descifrado: cadena de seguridad de capa 3

En una red de cadena de seguridad de capa 3, los dispositivos de cadena de seguridad utilizan interfaces de capa 3 para conectarse a la red de la cadena de seguridad; y cada interfaz debe tener una dirección IP y una máscara de subred asignadas. Los dispositivos de cadena de seguridad deben configurarse con rutas estáticas para dirigir el tráfico entrante y saliente al próximo dispositivo en la cadena de seguridad y de vuelta al cortafuegos.

Según el flujo de sesiones de la cadena de seguridad que seleccione (unidireccional o bidireccional), las sesiones entrantes o salientes descifradas pasan por la cadena de seguridad en la misma dirección o en direcciones opuestas.

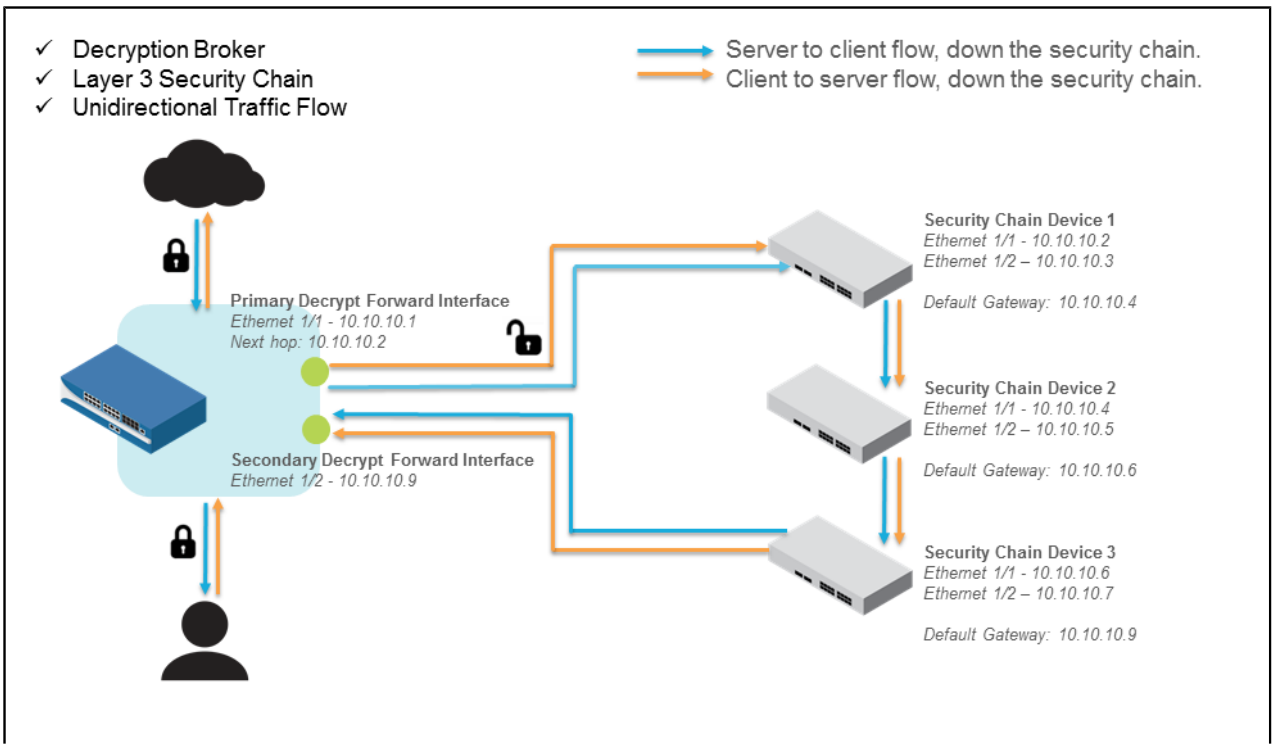
La figura a continuación muestra un cortafuegos habilitado como agente de descifrado que dirige tráfico de texto sin cifrar permitido por una cadena de seguridad de capa 3 de manera bidireccional. El cortafuegos se configura con rutas estáticas que dirigen las sesiones entrantes a zonas internas fiables donde residen los clientes (por ejemplo, a los empleados) y con una ruta predeterminada que dirige las sesiones salientes a una zona externa no fiable (internet). Para las sesiones salientes, el cortafuegos utiliza la interfaz principal dedicada al reenvío de descifrado para reenviar sesiones entrantes al primer dispositivo de la cadena de seguridad. Los dispositivos de la cadena de seguridad utilizan rutas estáticas para dirigir el tráfico al siguiente dispositivo en la línea; el siguiente salto de cada dispositivo de la cadena de seguridad es la dirección IP del puerto de entrada del dispositivo siguiente. El siguiente salto del último dispositivo de la cadena de seguridad es la interfaz de seguridad del cortafuegos dedicada al reenvío de descifrado. (El flujo de sesiones entrantes es exactamente opuesto).



De manera alternativa, la siguiente figura muestra el mismo cortafuegos habilitado como agente de descifrado que dirige el tráfico descifrado a través de una cadena de seguridad de capa 3. Sin embargo, en este ejemplo, el cortafuegos indica a todas las sesiones que fluyan por la cadena de seguridad de manera unidireccional. El cortafuegos utiliza la interfaz principal dedicada al reenvío de descifrado para reenviar

© 2020 Palo Alto Networks, Inc.

sesiones entrantes y salientes al primer dispositivo de la cadena de seguridad. El último dispositivo de la cadena de seguridad reenvía sesiones entrantes y salientes al cortafuegos.

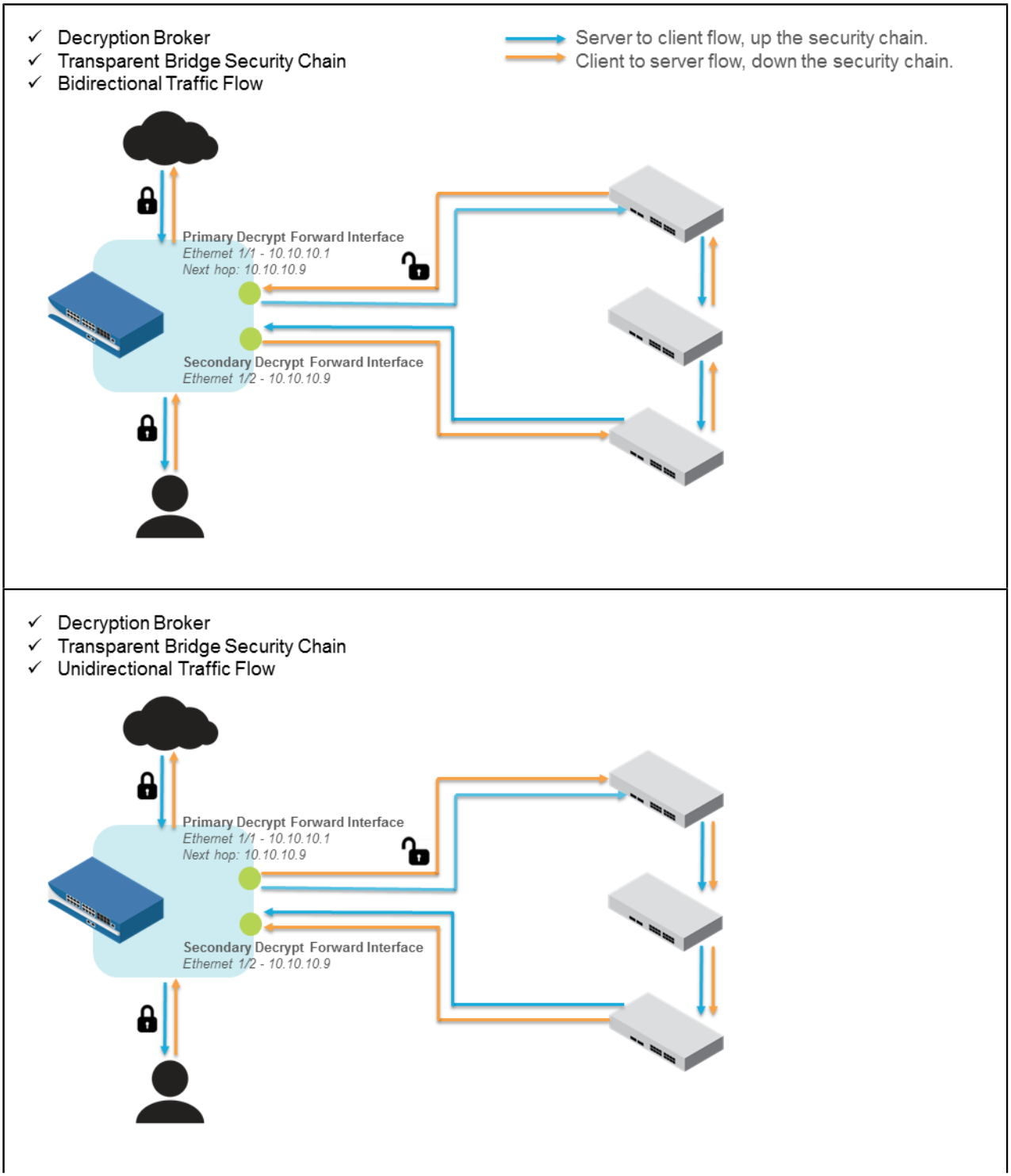


En las implementaciones de cadena de seguridad de capa 3 (bidireccional y unidireccional), el cortafuegos vuelve a cifrar el tráfico que la cadena de seguridad devuelve y lo reenvía a su destino. Realice la Configuración de un agente de descifrado con una o más cadenas de seguridad de capa 3 para comenzar con cualquiera de estas implementaciones.

Agente de descifrado: cadena de seguridad de puente transparente

En una red de cadena de seguridad de puente transparente, todos los dispositivos de la cadena de seguridad se configuran con dos interfaces conectadas a la red de la cadena de seguridad. Estas dos interfaces se configuran para funcionar en modo Puente transparente; no se les asignan direcciones IP, máscaras de subred o puertas de enlace predeterminadas, ni poseen tablas de enrutamiento local. Los dispositivos de la cadena de seguridad en modo de puente transparente se conectan en serie, uno detrás del otro. Reciben el tráfico en una interfaz, y analizan y aplican el tráfico. El tráfico egresa de la otra interfaz y se pasa al próximo dispositivo de la cadena de seguridad en línea. La primera imagen a continuación muestra una implementación de cadena de seguridad de puente transparente con un flujo de sesión bidireccional y la segunda imagen muestra una cadena de seguridad de puente transparente con un flujo de sesión unidireccional. Realice la Configuración del agente de descifrado con una cadena de seguridad de puente transparente para comenzar con cualquiera de estas implementaciones.

© 2020 Palo Alto Networks, Inc.



Agente de descifrado: flujo de sesión de cadena de seguridad

Puede especificar que el cortafuegos dirija las sesiones descifradas entrantes y salientes a través de una cadena de seguridad: en la misma dirección (unidireccional) o en direcciones opuestas (bidireccional). Por ejemplo, si tiene un dispositivo sin estado como un grabador de paquetes en una cadena de seguridad, puede permitir que el tráfico fluya de manera unidireccional por la cadena de segurida, de modo que el tráfico entrante y saliente atraviese el dispositivo en la misma dirección. El grabador de paquetes recibe el tráfico entrante y saliente en el mismo puerto y puede examinar las capturas de paquetes de ambos lados

© 2020 Palo Alto Networks, Inc.

de la sesión para detectar cambios en los valores de los encabezados de paquetes. De manera alternativa, si la cadena de seguridad incluye dispositivos como las soluciones de prevención de pérdida de datos (data loss prevention, DLP) que inspeccionan con estado el tráfico, permite que el tráfico fluya de manera bidireccional en la cadena de seguridad.

Agente de descifrado: múltiples cadenas de seguridad

Un cortafuegos habilitado como un agente de descifrado admite el reenvío de varias cadenas de seguridad (capa 3, puente transparente o una combinación de ambos) para proporcionar redundancia y equilibrar la carga de análisis, lo que evita la suscripción en exceso de una cadena de seguridad o un dispositivo de la cadena de seguridad. Debido a que es posible que la capacidad del cortafuegos para descifrar y reenviar tráfico supere la capacidad de los dispositivos de la cadena de seguridad para procesar el tráfico, puede configurar el cortafuegos para que distribuya las sesiones de texto no cifrado a varias redes de la cadena de seguridad para su inspección. El cortafuegos puede distribuir sesiones en ambos tipos de redes de la cadena de seguridad, de modo que las cadenas de seguridad puedan compartir la carga de inspección; sin embargo, los métodos para permitir la distribución de sesiones varían en función de si utiliza cadenas de seguridad de capa 3 o cadenas de seguridad de puente transparente. Un agente de descifrado que realiza el reenvío a varias cadenas de seguridad de capa 3 puede distribuir sesiones para su inspección utilizando uno de cuatro métodos:

- IP Module (Módulo IP): el cortafuegos asigna las sesiones basado en el hash del módulo de direcciones IP de origen y de destino.
- IP Hash (Hash IP): el cortafuegos asigna las sesiones basado en el hash IP de las direcciones IP de origen y de destino, y los números de puerto.
- Round Robin (Operación por turnos): el cortafuegos asigna las sesiones uniformemente a las cadenas de seguridad.
- Lowest Latency (Latencia más baja): el cortafuegos asigna más sesiones a la cadena de seguridad con menor latencia.

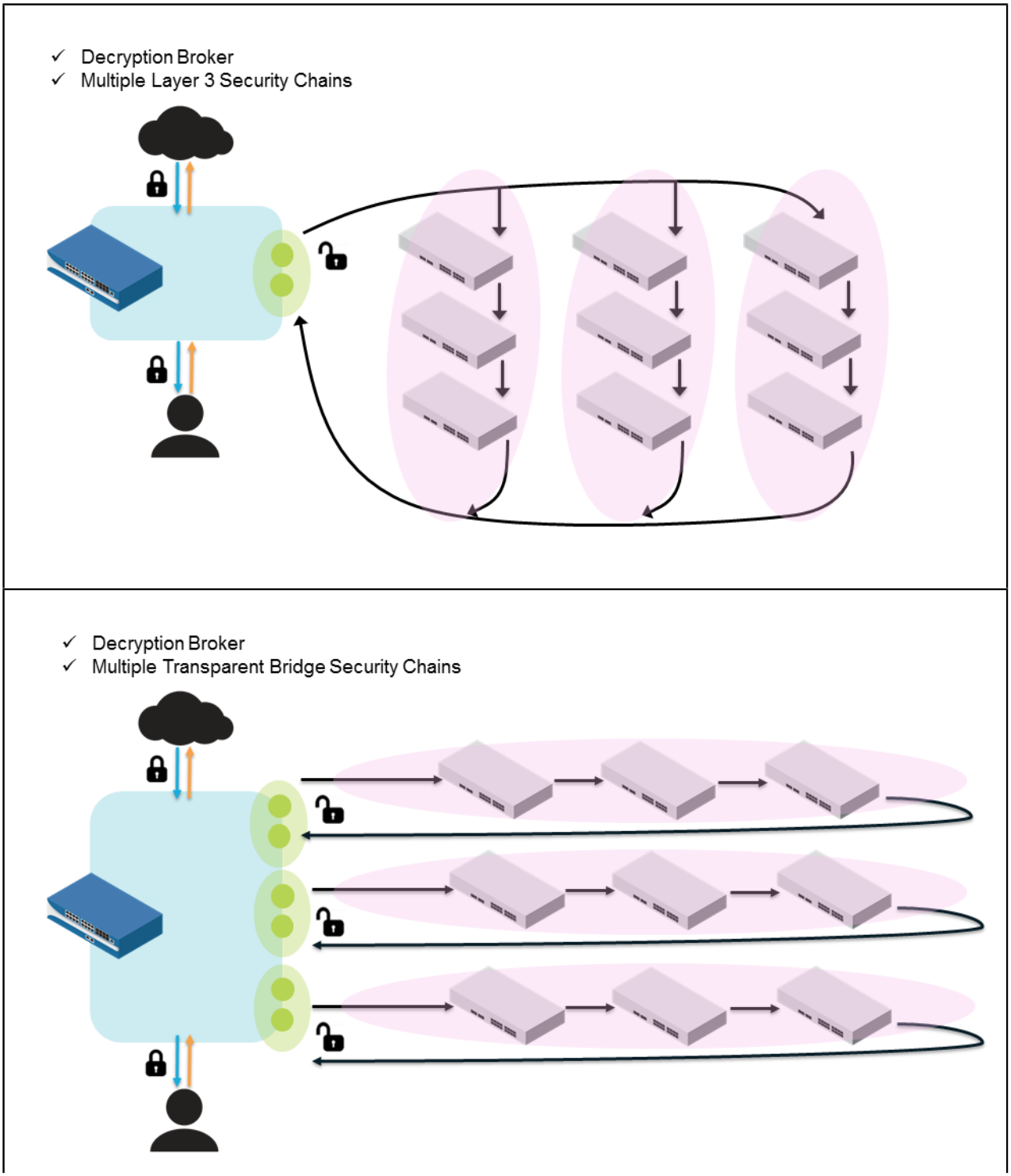
Un agente de descifrado que realiza el reenvío a varias cadenas de seguridad de puente transparente debe configurarse para realizar la distribución de sesiones basada en la política; el tráfico que coincide con una regla de la política se reenvía únicamente a la cadena de seguridad asociada a esa regla. Por ejemplo, especifique un intervalo de dirección de origen diferente para cada política de descifrado para dedicar una cadena de seguridad de puente transparente al análisis y la aplicación del tráfico que se origina en los intervalos de direcciones IP especificados.

Cuando configure varias cadenas de seguridad, asegúrese de implementar suficientes cadenas de seguridad para proporcionar exceso de capacidad en caso de un fallo en la cadena de seguridad. Si permite que el cortafuegos realice controles de estado en la cadena de seguridad y una cadena de seguridad falla, el cortafuegos continúa distribuyendo sesiones descifradas en las cadenas de seguridad con estado aceptable. Si no hay suficientes cadenas aceptables para abarcar la carga adicional, un fallo en la cadena de seguridad puede desencadenar otros fallos debido a que el resto de las cadenas de seguridad aceptables se suscriben en exceso.

La primera imagen a continuación muestra una implementación de agente de descifrado con varias cadenas de seguridad de capa 3. Tenga en cuenta que un par de interfaces de reenvío de descifrado puede reenviar tráfico descifrado a varias cadenas de seguridad de capa 3 (hasta 64).

La segunda imagen a continuación muestra una implementación de agente de descifrado con varias cadenas de seguridad de puente transparente; se requiere un par de interfaces de reenvío de descifrado para permitir el reenvío a cada cadena de seguridad de puente transparente diferente.

© 2020 Palo Alto Networks, Inc.



Agente de descifrado: comprobaciones de estado de la cadena de seguridad

Un agente de descifrado puede supervisar el estado de las cadenas de seguridad para garantizar que procesen eficazmente el tráfico descifrado. Las comprobaciones de estado periódicas supervisan lo siguiente:

- Conectividad del dispositivo de seguridad (supervisión de ruta)

© 2020 Palo Alto Networks, Inc.

- Velocidad de procesamiento y eficiencia del dispositivo de seguridad (supervisión de la latencia de HTTP)
- Capacidades de inspección de HTTP del dispositivo de seguridad (supervisión de HTTP)

Para cada tipo de supervisión que habilite, debe definir las condiciones que desea que activen un fallo en la comprobación de estado. Cuando una cadena de seguridad falla una comprobación de estado, el cortafuegos puede realizar una de las siguientes acciones:

- Bloquear las sesiones SSL existentes asignadas a la cadena de seguridad que falló. El cortafuegos solo comenzará a reenviar nuevas sesiones de descifrado a esa cadena de seguridad para su análisis cuando la cadena de seguridad pase la siguiente comprobación de estado. El flujo de tráfico debe pasar la comprobación de la política de seguridad del cortafuegos y la comprobación de la cadena de seguridad para que se le permita el acceso a internet.
- (Solo cadena de seguridad de capa 3) Permitir que el tráfico omita la cadena de seguridad que falló. Tenga en cuenta que el tráfico que omite una cadena de seguridad experimenta el descifrado del cortafuegos y la aplicación de la política de seguridad. Sin embargo, no experimenta el análisis de la cadena de seguridad. Esta opción solo es compatible con las cadenas de seguridad de capa 3. Debido a que la distribución de sesiones en cadenas de seguridad de puente transparente se basa en la política, el tráfico no puede omitir una cadena que falló, dado que el tráfico que coincide con una regla de la política se asigna a una cadena específica para la inspección.

Puede seleccionar si desea que el cortafuegos bloquee las sesiones u omita una cadena de seguridad si se produce un fallo en una cadena de seguridad en función del cumplimiento y las necesidades de utilización de la organización.

Si configura varias cadenas de seguridad, es **recomendable** implementar suficientes para ofrecer capacidad en exceso por si falla alguna. Si permite que el cortafuegos realice controles de estado en la cadena de seguridad y una cadena de seguridad falla, el cortafuegos continúa distribuyendo sesiones descifradas en las cadenas de seguridad con estado aceptable. Si no hay suficientes cadenas aceptables para abarcar la carga adicional, un fallo en la cadena de seguridad puede desencadenar otros fallos debido a que el resto de las cadenas de seguridad aceptables se suscriben en exceso.

Pautas de la cadena de seguridad de capa 3

Respete estas pautas cuando configure los dispositivos en la cadena de seguridad de capa 3 para admitir agentes de descifrado:

- Configure los dispositivos en la cadena de seguridad con interfaces de capa 3 para que se conecten a la red de la cadena de seguridad. Estas interfaces de capa 3 deben tener una dirección IP y una máscara de subred asignadas.
- No incluya dispositivos que modifiquen los encabezados IP o TCP en una cadena de seguridad o asegúrese de deshabilitar las funciones que realicen estas tareas. Si una cadena de seguridad devuelve una sesión a un cortafuegos con un encabezado IP o TCP modificado, el cortafuegos descarta la sesión dado que ya no puede identificar si coincide con la sesión predescifrada original.
- Establezca las puertas de enlace predeterminadas para los dispositivos de la cadena de seguridad:
  - En todos los dispositivos de la cadena de seguridad excepto el último dispositivo de la cadena, configure la puerta de enlace predeterminada para que sea la dirección IP del siguiente dispositivo en línea.
  - En el último dispositivo de la cadena de seguridad, configure la puerta de enlace predeterminada para que sea la dirección IP de la interfaz secundaria del cortafuegos. Esto garantiza que el último dispositivo devuelva el flujo de tráfico al cortafuegos. (Cuando configure un perfil de reenvío de descifrado, asignará una de las interfaces de reenvío de descifrado para que sea la interfaz secundaria del agente de descifrado. Consulte Objects (Objetos) > Decryption (Descifrado) > Forwarding Profile (Perfil de reenvío) > Secondary Interface (Interfaz secundaria), y utilice la dirección IP de esta interfaz.
  - Si configuró el cortafuegos para que dirija las sesiones a través de la cadena de seguridad de manera bidireccional, también debe establecer la puerta de enlace predeterminada del primer dispositivo de la cadena de seguridad como la dirección IP de la interfaz principal del cortafuegos (cuando configure

© 2020 Palo Alto Networks, Inc.

un perfil de reenvío de descifrado, asignará una de las interfaces de reenvío de descifrado como interfaz principal del agente de descifrado). Consulte Objects [Objetos] > Decryption [Descifrado] > Forwarding Profile [Perfil de reenvío] > Primary Interface [Interfaz principal], y utilice la dirección IP de esta interfaz).

- Confirme que el cortafuegos y la cadena de seguridad puedan comunicarse eficazmente: compruebe que el enrutador que dirige el tráfico entre el cortafuegos y la cadena de seguridad esté configurado correctamente y que los dispositivos de la cadena de seguridad se configuren con rutas estáticas para dirigir el tráfico de manera adecuada.
- En los dispositivos de la cadena de seguridad, no se debe originar tráfico que se enviará a una red externa. El cortafuegos bloquea el tráfico que no coincide con la sesión original previa al descifrado. Sin embargo, si un dispositivo de la cadena de seguridad requiere acceso a internet para recibir las actualizaciones, asegúrese de que el dispositivo pueda acceder a una red separada (por ejemplo, por medio del puerto de gestión del dispositivo) para facilitar las actualizaciones.
- Cuando configura varias cadenas de seguridad, se recomienda implementar suficientes cadenas de seguridad para proporcionar exceso de capacidad en caso de un fallo en la cadena de seguridad. Si permite que el cortafuegos realice controles de estado en la cadena de seguridad y una cadena de seguridad falla, el cortafuegos continúa distribuyendo sesiones descifradas en las cadenas de seguridad con estado aceptable. Si no hay suficientes cadenas aceptables para abarcar la carga adicional, un fallo en la cadena de seguridad puede desencadenar otros fallos debido a que el resto de las cadenas de seguridad aceptables se suscriben en exceso.

Configuración de un agente de descifrado con una o más cadenas de seguridad de capa 3

Realice los siguientes pasos para permitir al cortafuegos actuar como un agente de descifrado que distribuye tráfico a una cadena de seguridad de capa 3 para aplicación y análisis adicional. Habilitar el cortafuegos como agente de descifrado incluye lo siguiente:

- Configure una cadena de seguridad de capa 3 que respete las pautas de la cadena de seguridad de capa 3.
- Active la licencia libre de agente de descifrado (Licencias de descifrado). Esto incluye dirigirse al portal de asistencia al cliente de Palo Alto Networks para activar la licencia e instalar la licencia en el cortafuegos.
- Habilite al menos dos interfaces de cortafuegos como interfaces de reenvío de descifrado. Un par de interfaces de reenvío de descifrado pueden admitir hasta 64 cadenas de seguridad.
- Configure un perfil de reenvío de descifrado para permitir que el cortafuegos reenvíe sesiones descifradas a una o varias cadenas de seguridad a fin de distribuir esas sesiones entre varias cadenas de seguridad y supervisar el estado de la cadena de seguridad.

STEP 1 | Respete las pautas de la cadena de seguridad de capa 3 para asegurar que configuró su cadena de seguridad para que admita el agente de descifrado.

STEP 2 | Active la licencia libre de agente de descifrado (consulte Licencias de descifrado).

STEP 3 | Confirme que el cortafuegos puede realizar el descifrado de proxy SSL de reenvío.

Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** para añadir o modificar una regla de la política de seguridad. También puede adjuntar un perfil de descifrado a una regla de la política de descifrado para realizar comprobaciones de certificados y validar protocolos SSL. Por ejemplo, un perfil de descifrado le permite bloquear sesiones en función del estado del certificado utilizando protocolos no compatibles o conjuntos de cifrado, o si los recursos para realizar el descifrado no están disponibles.

STEP 4 | Habilite un par de interfaces de capa 3 para reenviar el tráfico descifrado.

© 2020 Palo Alto Networks, Inc.

1. Visualice las interfaces configuradas en la pestaña **Network (Red)** > **Interfaces** > **Ethernet**. La columna Interface Type (Tipo de interfaz) muestra si una interfaz está configurada para ser una interfaz de capa 3. Seleccione una interfaz de capa 3 y complete los siguientes pasos en ambas interfaces de capa 3 que desea habilitar como par de reenvío de descifrado.
2. Seleccione la pestaña Config (Configuración) y asigne la interfaz a un enrutador virtual que no tenga configuradas rutas ni interfaces para pasar tráfico del plano de datos. El enrutador virtual debe dedicarse a las interfaces de reenvío de descifrado para garantizar que las sesiones de texto sin cifrar que el cortafuegos reenvia para un análisis adicional se segmenten totalmente del tráfico de plano de datos.
3. Asigne la interfaz a una zona de seguridad. (Asigne ambas interfaces a la misma zona de seguridad).
4. En la pestaña Advanced (Opciones avanzadas), seleccione Decrypt Forward (Reenvío de descifrado).
5. Haga clic en OK (Aceptar) para guardar la configuración de la interfaz.
6. Repita estos pasos para una cantidad par de interfaces, combinándolas de a dos.
7. Asegúrese de que las interfaces habilitadas para reenviar tráfico descifrado no se utilicen para pasar otro tipo de tráfico.

STEP 5 | Cree un perfil de reenvío de descifrado para definir los ajustes del cortafuegos a fin de reenviar tráfico descifrado a una cadena de seguridad de capa 3.

1. Seleccione **Objects (Objetos)** > **Decryption (Descifrado)** > **Forwarding Profile (Perfil de reenvío)**, añada un nuevo perfil de reenvío de descifrado y asígnele un nombre descriptivo.
2. En la pestaña General, establezca Security Chain Type (Tipo de cadena de seguridad) en Routed (Con ruta) (capa 3) para configurar el cortafuegos de modo que reenvíe tráfico descifrado a una cadena de seguridad con dispositivos de capa 3.
3. Configure el sentido del flujo del tráfico de descifrado que reenvía el cortafuegos: unidireccional o bidireccional.
4. Seleccione la interfaz principal y la interfaz secundaria que utiliza el cortafuegos para comunicarse con la cadena de seguridad.

   Las interfaces principal y secundaria forman un par de interfaces de reenvío de descifrado. A continuación, únicamente se muestran las interfaces que configuró como interfaces de reenvío de descifrado. El tipo de cadena de seguridad (capa 3 o puente transparente) y la dirección del flujo de tráfico (unidireccional o bidireccional) determinan cuál de las dos interfaces reenvía tráfico de texto sin cifrar permitido a la cadena de seguridad y qué interfaz recibe el tráfico de la cadena de seguridad tras la aplicación adicional.
5. Haga clic en OK (Aceptar) para guardar el perfil de descifrado.

STEP 6 | Conecte el cortafuegos a una cadena de seguridad.

1. Seleccione la pestaña Security Chains (Cadenas de seguridad) y haga clic en Add (Añadir) para añadir una cadena de seguridad.
2. Asigne un Name (Nombre) y haga clic en Enable (Habilitar) para habilitar la cadena de seguridad.
3. Introduzca los detalles del primer dispositivo y el último dispositivo en la cadena de seguridad.

   Asigne al dispositivo un Name (Nombre) descriptivo y seleccione la dirección IPv4 del primer dispositivo en la cadena de seguridad. O puede definir un nuevo objeto de dirección para hacer referencia al dispositivo con facilidad.
4. Haga clic en OK (Aceptar) para guardar la cadena de seguridad y repita estos pasos para añadir otra cadena de seguridad. O continúe si solo añade una cadena.

STEP 7 | (Solo varias cadenas de seguridad) En la pestaña Security Chains (Cadenas de seguridad), seleccione el Session Distribution Method (Método de distribución de sesiones) que utilizará el cortafuegos para distribuir sesiones descifradas en las cadenas de seguridad.

Ajuste la distribución de sesiones para que se base en el módulo IP, el hash IP, la operación por turnos o la latencia más baja. El método de distribución de latencia más baja requiere que también permita

© 2020 Palo Alto Networks, Inc.

que el cortafuegos realice la supervisión de latencia de HTTP y la supervisión de HTTP en la cadena de seguridad.

STEP 8 | Seleccione la pestaña Health Monitor (Supervisor de estado) para permitir que el cortafuegos realice comprobaciones de estado en las cadenas de seguridad.

Si una cadena de seguridad falla una comprobación de estado, el cortafuegos puede bloquear el tráfico hasta que la cadena de seguridad pase la próxima comprobación de estado y pueda procesarlo, o el cortafuegos puede permitir que el tráfico omita una cadena de seguridad con fallos.

1. En Health Check Failure (Fallo de la comprobación de estado), especifique que el cortafuegos Bypass Security Chain (Omita la cadena de seguridad) o Block Session (Bloquee las sesiones).
2. Defina una condición de fallo de la comprobación de estado como un evento en el que se cumplen cualquiera de las condiciones de supervisión del estado (condición OR) o bien todas ellas (condición AND).
3. Habilite la supervisión de rutas, la supervisión de la latencia de HTTP o la supervisión de HTTP. Para cada tipo de supervisión que desea habilitar, defina los períodos de tiempo y recuentos que desea que activen un fallo en la comprobación de estado.

   La supervisión de latencia y la supervisión de HTTP son necesarios para admitir eficazmente la distribución de sesiones de latencia más baja (**Objects [Objetos]** > **Decryption [Descifrado]** > **Forwarding Profile [Perfil de reenvío]** > **Security Chains Session Distribution Method [Método de distribución de sesiones de la cadena de seguridad]**).

STEP 9 | Guarde el perfil de reenvío.

STEP 10 | Añada el perfil de reenvío a una regla de la política de descifrado.

El cortafuegos descifra e inspecciona el tráfico que coincide con la regla, y reenvía el tráfico de texto sin cifrar a la cadena de seguridad para una inspección y aplicación más exhaustiva.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y seleccione una regla de la política de seguridad.
2. Haga clic en Options (Opciones).
3. Configure Action (Acción) en Decrypt and Forward (Descifrado y reenvío).
4. Seleccione el perfil de reenvío que creó.
5. Haga clic en OK (Aceptar) para guardar la regla de la política y confirme los cambios.

STEP 11 | Supervise el tráfico descifrado que el cortafuegos reenvía para una inspección adicional.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y use el siguiente filtro: `(flags has decrypt-forwarded)`.
2. Compruebe los detalles de una entrada del log de tráfico y busque la etiqueta Decrypt Forwarded (Descifrado reenviado).

Pautas de la cadena de seguridad de puente transparente

Respete estas pautas cuando configure los dispositivos en la cadena de seguridad de puente transparente para admitir agentes de descifrado:

- Cada dispositivo de cadena de seguridad debe configurarse con dos interfaces en modo de puente transparente; estas dos interfaces conectan el dispositivo a la red de la cadena de seguridad. Los dispositivos de la cadena de seguridad no utilizan una tabla de enrutamiento local y a las interfaces de puente transparente no se les asignan direcciones IP, máscaras de subred o puertas de enlace predeterminadas.
- No incluya dispositivos que modifiquen los encabezados IP o TCP en una cadena de seguridad o asegúrese de deshabilitar las funciones que realicen estas tareas. Si una cadena de seguridad devuelve

© 2020 Palo Alto Networks, Inc.

una sesión a un cortafuegos con un encabezado IP o TCP modificado, el cortafuegos descarta las sesiones dado que ya no puede identificar si coincide con la sesión de cliente a servidor o de servidor a cliente original.
- Cuando configura varias cadenas de seguridad, se recomienda implementar suficientes cadenas de seguridad para proporcionar exceso de capacidad en caso de un fallo en la cadena de seguridad. Si permite que el cortafuegos realice controles de estado en la cadena de seguridad y una cadena de seguridad falla, el cortafuegos continúa distribuyendo sesiones descifradas en las cadenas de seguridad con estado aceptable. Si no hay suficientes cadenas aceptables para abarcar la carga adicional, un fallo en la cadena de seguridad puede desencadenar otros fallos debido a que el resto de las cadenas de seguridad aceptables se suscriben en exceso.

Configuración del agente de descifrado con una cadena de seguridad de puente transparente

Realice los siguientes pasos para permitir al cortafuegos actuar como un agente de descifrado que distribuye tráfico a una cadena de seguridad de puente transparente para aplicación y análisis adicional. Habilitar el cortafuegos como agente de descifrado incluye lo siguiente:

- Configure una cadena de seguridad de puente transparente que respete las pautas de la cadena de seguridad de puente transparente.
- Active la licencia libre de agente de descifrado (Licencias de descifrado). Esto incluye dirigirse al portal de asistencia al cliente de Palo Alto Networks para activar la licencia e instalar la licencia en el cortafuegos.
- Habilite un par de interfaces de cortafuegos de capa 3 como interfaces de reenvío de descifrado. Cada par de interfaces de reenvío de descifrado admite una cadena de seguridad de puente transparente. Deberá crear varios pares de interfaces de reenvío de descifrado para admitir varias cadenas de seguridad de puente transparente.
- Configure un perfil de reenvío de descifrado para permitir que el cortafuegos reenvíe sesiones descifradas a una cadena de seguridad de puente transparente y supervisar el rendimiento de la cadena de seguridad.

Incluso si planea habilitar el agente de descifrado con varias cadenas de seguridad de puente transparente, debe realizar los siguientes pasos antes.

STEP 1 | Configure una cadena de seguridad de puente transparente que respete las pautas de la cadena de seguridad de puente transparente.

STEP 2 | Active la licencia libre de agente de descifrado (consulte Licencias de descifrado).

STEP 3 | Confirme que el cortafuegos puede realizar el descifrado de proxy SSL de reenvío.

Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** para **Add (Añadir)** una regla de la política de seguridad o modificar una existente. También puede adjuntar un perfil de descifrado a una regla de la política de descifrado para realizar comprobaciones de certificados y validar protocolos SSL. Por ejemplo, un perfil de descifrado le permite bloquear sesiones en función del estado del certificado utilizando protocolos no compatibles o conjuntos de cifrado, o si los recursos para realizar el descifrado no están disponibles.

STEP 4 | Habilite un par de interfaces de capa 3 para reenviar el tráfico descifrado.

1. Visualice las interfaces configuradas en la pestaña **Network (Red)** > **Interfaces** > **Ethernet**.

   La columna Interface Type (Tipo de interfaz) muestra si una interfaz está configurada para ser una interfaz de capa 3. Seleccione una interfaz de capa 3 y complete los siguientes pasos en ambas interfaces de capa 3 que desea habilitar como par de reenvío de descifrado.

© 2020 Palo Alto Networks, Inc.

2. Seleccione la pestaña **Config (Configuración)** y asigne la interfaz a un **Virtual Router (Enrutador virtual)** sin rutas o interfaces configuradas que se utilicen para pasar tráfico del plano de datos.

   El enrutador virtual debe dedicarse a las interfaces de reenvío de descifrado para garantizar que las sesiones de texto sin cifrar que el cortafuegos reenvia para un análisis adicional se segmenten totalmente del tráfico de plano de datos.
3. Asigne la interfaz a una **Security Zone (Zona de seguridad)**. (Asigne ambas interfaces a la misma zona de seguridad).
4. En la pestaña **Advanced (Avanzado)**, seleccione **Decrypt Forward (Reenvío de descifrado)**.
5. Haga clic en **OK (Aceptar)** para guardar la configuración de la interfaz.
6. Repita estos pasos de modo que, al menos, dos interfaces estén habilitadas para el reenvío de tráfico descifrado.

   Un par de interfaces de reenvío de descifrado admite una cadena de seguridad de puente transparente. Si desea que el cortafuegos distribuya sesiones descifradas en varias cadenas de seguridad de puente transparente, habilite un par de interfaces de reenvío de descifrado por cada cadena de seguridad que desee admitir. Asegúrese de que las interfaces habilitadas para reenviar tráfico descifrado no se utilicen para pasar otro tipo de tráfico.

STEP 5 | Cree un perfil de reenvío de descifrado para definir los ajustes del cortafuegos a fin de reenviar tráfico descifrado a una cadena de seguridad de puente transparente.

1. Seleccione **Objects (Objetos)** > **Decryption (Descifrado)** > **Forwarding Profile (Perfil de reenvío)**, **Add (Añada)** un nuevo perfil de reenvío de descifrado y asígnele un **Name (Nombre)** descriptivo.
2. En la pestaña **General**, establezca **Security Chain Type (Tipo de cadena de seguridad)** en **Transparent Bridge (Puente transparente)** para configurar el cortafuegos de modo que reenvíe tráfico descifrado a una cadena de seguridad con dispositivos de puente transparente.
3. Establezca la **Flow Direction (Dirección del flujo)** para el tráfico de descifrado que reenvía el cortafuegos: **Unidireccional** o **bidireccional**.
4. Seleccione la **Primary Interface (Interfaz principal)** y la **Secondary Interface (Interfaz secundaria)** que utiliza el cortafuegos para reenviar tráfico a una cadena de seguridad.

   Las interfaces principal y secundaria forman un par de interfaces de reenvío de descifrado. A continuación, únicamente se muestran las interfaces que configuró como interfaces de reenvío de descifrado.

STEP 6 | Seleccione la pestaña **Health Monitor (Supervisor de estado)** para permitir que el cortafuegos realice comprobaciones de estado en una cadena de seguridad de puente transparente.

1. Establezca **On Health Check Failure (Fallo de la comprobación de estado)** en **Block Session (Bloquear sesión)** si desea descartar el tráfico hasta que la comprobación de estado sea correcta o establézcala en **Bypass Security Chain (Omitir cadena de seguridad)** para reenviar tráfico sin pasar por la cadena de seguridad.

   La distribución de sesiones en cadenas de seguridad de puente transparente se basa en políticas, por lo que el tráfico no puede realizar una conmutación por error en una cadena de seguridad diferente (en el modo de capa 3 sí es posible), ya que el tráfico que coincide con una regla de políticas se asigna a una cadena específica para la inspección.
2. Defina una **Health Check Failed Condition (Condición fallida de la comprobación de estado)** como un evento donde se produce cualquiera de las condiciones de supervisión de estado (una **OR Condition [Condición OR]**) o se producen todas las condiciones (una **AND Condition [Condición AND]**).
3. Habilite la **Path Monitoring (Supervisión de ruta)**, la **HTTP Latency Monitoring (Supervisión de la latencia de HTTP)** o la **HTTP Monitoring (Supervisión de HTTP)**. Para cada tipo de supervisión que desea habilitar, defina los períodos de tiempo y recuentos que desea que activen un fallo en la comprobación de estado.

   La supervisión de latencia y la supervisión de HTTP son necesarias para admitir eficazmente la distribución de sesiones de latencia más baja (**Objects [Objetos]** > **Decryption [Descifrado]** >

© 2020 Palo Alto Networks, Inc.

Forwarding Profile [Perfil de reenvío] > **Security Chains [Cadenas de seguridad]** > **Session Distribution Method [Método de distribución de sesiones]**).

STEP 7 | Guarde el perfil de reenvío.

STEP 8 | Añada el perfil de reenvío a una regla de la política de descifrado.

El cortafuegos descifra e inspecciona el tráfico que coincide con la regla, y reenvía el tráfico de texto sin cifrar a la cadena de seguridad para una inspección y aplicación más exhaustiva.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y seleccione una regla de la política de seguridad.
2. Utilice las pestañas de la regla de la política para definir el tráfico que desea reenviar a la cadena de seguridad de puente transparente.

   Por ejemplo, seleccione **Source (Origen)** y haga clic en **Add (Añadir)** para añadir un intervalo de **Source Address (Dirección de origen)** o haga clic en **New Address (Nueva dirección)** para crear un objeto de dirección nueva que identifique el tráfico que se origina en un intervalo de dirección IP concreto. La regla de la política solo aplicará el tráfico que se origine en este origen.
3. Seleccione **Options (Opciones)**.
4. Configure **Action (Acción)** en **Decrypt and Forward (Descifrado y reenvío)**.
5. Seleccione un **Transparent Bridge Forwarding Profile (Perfil de reenvío de puente transparente)**.
6. Haga clic en **OK (Aceptar)** para guardar la regla de la política y en **Commit (Confirmar)** para confirmar sus cambios.

STEP 9 | (Opcional) Realice la Configuración del agente de descifrado con varias cadenas de seguridad de puente transparente.

STEP 10 | Supervise el tráfico descifrado que el cortafuegos reenvió para una inspección adicional.

- Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y añada el filtro: `(flags has decrypt-forwarded)`.
- Compruebe los detalles de una entrada del log de tráfico y busque la etiqueta Decrypt Forwarded (Descifrado reenviado).

Configuración del agente de descifrado con varias cadenas de seguridad de puente transparente

Puede configurar el cortafuegos para que distribuya sesiones en varias cadenas de seguridad en modo de puente transparente. En cada cadena de seguridad de puente transparente que desea admitir, configure lo siguiente:

- Un par de interfaces de reenvío de descifrado que reenvían tráfico únicamente a la cadena de seguridad de puente transparente.
- Un perfil de reenvío de descifrado que especifica ajustes únicamente de la cadena de seguridad de puente transparente.
- Un regla de la política de seguridad que especifica únicamente que el tráfico descifrado concreto se reenvíe a la cadena de seguridad de puente transparente. Esto le permite distribuir sesiones con mayor uniformidad entre varias cadenas de seguridad de puente transparente (para evitar la suscripción en exceso de cualquier cadena de seguridad) en función del origen del tráfico.

STEP 1 | En primer lugar, siga los pasos de la Configuración del agente de descifrado con una cadena de seguridad de puente transparente. En cada cadena de seguridad de puente transparente que desea admitir, realice los siguientes pasos:

© 2020 Palo Alto Networks, Inc.

- En el cortafuegos, habilite un par de interfaces de capa 3 para admitir el reenvío de tráfico descifrado.
- Cree un perfil de reenvío de descifrado para definir los ajustes del cortafuegos a fin de reenviar tráfico descifrado a una cadena de seguridad de puente transparente.

STEP 2 | Adjunte cada perfil de reenvío de descifrado de puente transparente a una regla diferente de la política de descifrado.

Además de aplicar los ajustes de reenvío de descifrado al tráfico coincidente, adjuntar los perfiles de reenvío de descifrado de puente transparente a reglas de la política de descifrado le permite distribuir sesiones en cadenas de seguridad de puente transparente. Especifique un intervalo de dirección de origen diferente para cada regla de la política para dedicar una cadena de seguridad de puente transparente al análisis y la aplicación del tráfico que se origina en ese intervalo.

1. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y seleccione una regla de la política de seguridad.
2. Seleccione **Source (Origen)** y haga clic en **Add (Añadir)** para añadir un intervalo de dirección de origen o haga clic en **New Address (Nueva dirección)** para crear un objeto de dirección nueva que identifique el tráfico que se origina en un intervalo de dirección IP concreto. El único tráfico que se origina en este intervalo de dirección IP se reenvía a la cadena de seguridad de puente transparente asociada para su análisis.
3. Seleccione **Options (Opciones)**.
4. Configure **Action (Acción)** en **Decrypt and Forward (Descifrado y reenvío)**.
5. Seleccione un **Transparent Bridge Forwarding Profile (Perfil de reenvío de puente transparente)** para adjuntar a la regla de la política.
6. Haga clic en **OK (Aceptar)** para guardar la regla de la política y en **Commit (Confirmar)** para confirmar sus cambios.

STEP 3 | Continúe repitiendo estos pasos (asociar un perfil de reenvío de descifrado de puente transparente a una política de descifrado) para las cadenas de seguridad que desee admitir.

© 2020 Palo Alto Networks, Inc.

Activación de las licencias gratuitas para usar las funciones de descifrado

No se requieren licencias para descifrar el tráfico SSH y el tráfico SSL (tráfico SSL de internet o tráfico SSL a un servidor interno).

Sin embargo, debe activar una licencia libre para habilitar el agente de descifrado y el reflejo de descifrado. El requisito de licencia libre garantiza que estas funciones únicamente puedan utilizarse después de que el personal aprobado active intencionadamente la licencia asociada.

Siga estos pasos en el portal de asistencia al cliente de Palo Alto Networks para activar una licencia de una función de agente de descifrado o reflejo de descifrado.

STEP 1 | Inicie sesión en el portal de atención al cliente.

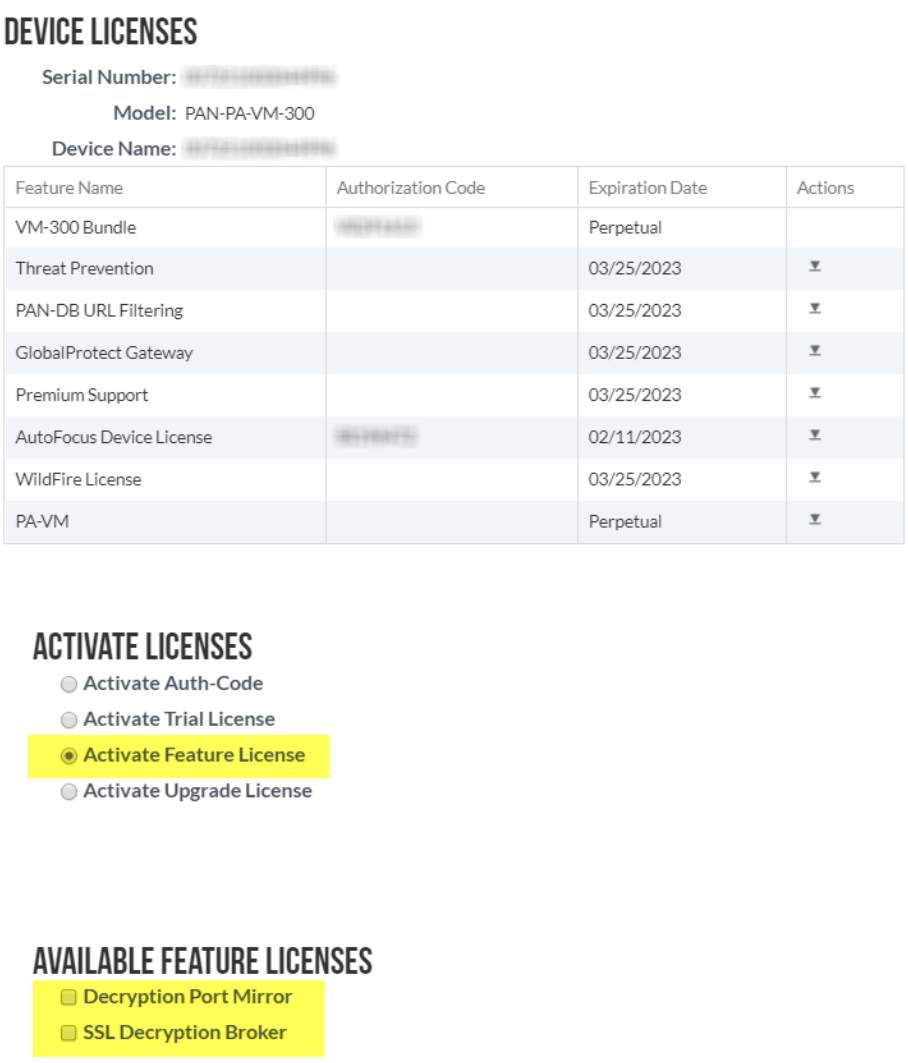
STEP 2 | Seleccione **Assets (Activos)** > **Devices (Dispositivos)** en el panel de navegación de la izquierda.

STEP 3 | Encuentre el dispositivo en el que desea habilitar el agente de descifrado o el reflejo de puerto de descifrado, y seleccione **Actions (Acciones)** (el icono del lápiz).

STEP 4 | En Activate Licenses (Activar licencias), seleccione **Activate Feature License (Activar licencia de una función)**.

STEP 5 | Seleccione la función para la que desea activar una licencia libre: **Decryption Port Mirror (Reflejo del puerto de descifrado)** o **SSL Decryption Broker (Agente de descifrado SSL)**.

© 2020 Palo Alto Networks, Inc.



STEP 6 | Haga clic en **Agree (Aceptar)** y en **Submit (Enviar)**.

STEP 7 | Instale la licencia de agente de descifrado o reflejo de descifrado en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
2. Haga clic en **Retrieve license keys from the license server (Recuperar claves de licencia del servidor de licencias)**.
3. Verifique que la licencia de **SSL Decryption Broker (Agente de descifrado SSL)** o **Decryption Port Mirror (Reflejo del puerto de descifrado)** esté activa en el cortafuegos.
4. Reinicie el cortafuegos (**Device [Dispositivo]** > **Setup [Configuración]** > **Operations [Operaciones]**). El reflejo del puerto de descifrado y el agente de descifrado no pueden configurarse hasta que el cortafuegos vuelva a cargarse.

© 2020 Palo Alto Networks, Inc.

Filtrado de URLs

El filtrado de URL de Palo Alto Networks le permite supervisar y controlar los sitios que pueden acceder los usuarios para evitar ataques de phishing controlando los sitios a los que los usuarios pueden enviar credenciales corporativas válidas, y aplicar la búsqueda segura de motores de búsqueda como Google and Bing.

- Información sobre URL Filtering
- Funcionamiento del filtrado de URLs
- ML en línea de filtrado de URL
- Casos de uso de filtrado de URL
- Categorías de URL
- Planificar la implementación de filtrado de URL
- Prácticas recomendadas de filtrado de URL
- Habilitación de PAN-DB
- Configuración de filtrado de URL
- Configuración de aprendizaje automático en línea de filtrado de URL
- Supervisión de la actividad web
- Registro solo de las páginas que visita un usuario
- Creación de una categoría de URL personalizada
- Excepciones de la categoría de URL
- Uso de una lista dinámica externa en un perfil de filtro de URL
- Habilitación del acceso a determinados sitios mediante contraseña
- Prevención de phishing de credenciales
- Forzaje de búsquedas seguras
- Páginas de respuesta de filtrado de URL
- Personalización de las páginas de respuesta de filtrado de URL
- Creación de logs del encabezado HTTP
- Solicitud para cambiar la categoría de una URL
- Solución de problemas del filtrado de URL
- Nube privada de PAN-DB

© 2020 Palo Alto Networks, Inc.

Información sobre URL Filtering

La función URL Filtering de Palo Alto Networks brinda protección frente a las amenazas web, ya que permite habilitar el acceso web de forma segura y, al mismo tiempo, controlar la interacción de los usuarios con el contenido en línea.

Con el filtrado de URL habilitado, se realizan los siguientes procedimientos en todo el tráfico web (HTTP y HTTPS) en cualquier puerto:

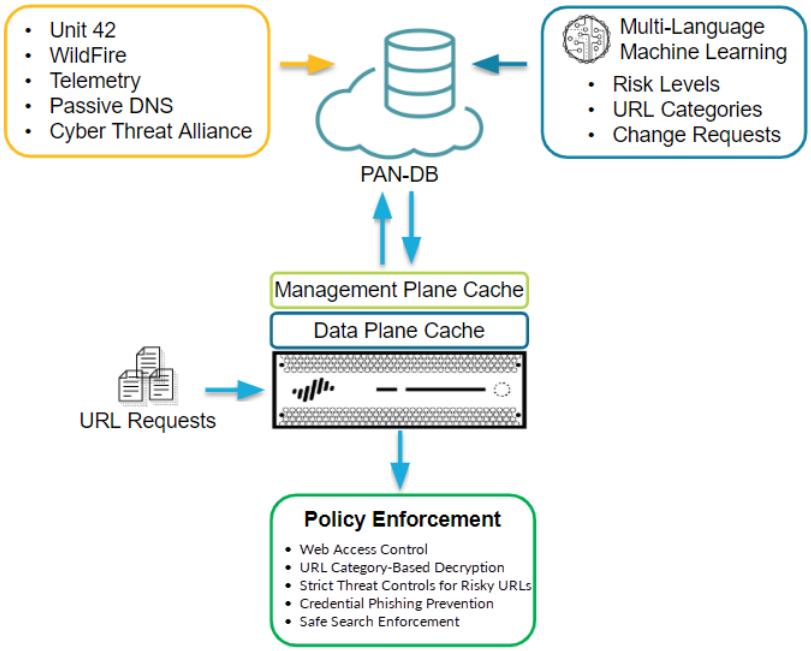
- Se compara con la base de datos de filtrado de URL, que contiene una lista de millones de sitios web que se han categorizado. Puede usar esas categorías de URL como uno de los criterios de coincidencia para aplicar la política de seguridad. También puede utilizar el filtrado de URL para imponer a los usuarios una configuración de búsqueda segura y para prevenir el robo de credenciales según la categoría de URL.
- Se realiza una inspección en busca de phishing y JavaScript malicioso mediante el aprendizaje automático en línea (ML, Machine Learning), una solución de análisis basada en cortafuegos, que puede bloquear páginas web maliciosas desconocidas en tiempo real.

Sin embargo, la solución de filtrado de URL de Palo Alto Networks, PAN-DB, le permite elegir entre la *nube pública de PAN-DB* y la *nube privada de PAN-DB*. Use la solución de nube pública si los cortafuegos de nueva generación de Palo Alto Networks de su red pueden acceder directamente a Internet. Si los requisitos de seguridad de red de su empresa prohíben que los cortafuegos accedan directamente a Internet, puede implementar una nube privada de PAN-DB en uno o más dispositivos M-600 que funcionen como servidores de PAN-DB en su red.

© 2020 Palo Alto Networks, Inc.

Funcionamiento del filtrado de URLs

PAN-DB es la base de datos en la nube de URL Filtering. En ella se clasifican los sitios web según su contenido, sus funciones y su seguridad. Una URL puede tener hasta cuatro categorías de URL, incluidas las categorías de riesgo (alto, medio y bajo), que indican la probabilidad de la exposición a las amenazas que conllevan los sitios. Como PAN-DB categoriza los sitios, los cortafuegos que tienen habilitada la función URL Filtering pueden aprovechar esa información en tiempo real para aplicar la política de seguridad.



Cuando un usuario accede a una URL que no está almacenada en caché, el cortafuegos comprueba PAN-DB para determinar la categoría del sitio y la guarda. A medida que el cortafuegos guarda nuevas entradas, elimina las URL a las que los usuarios no han accedido recientemente para que refleje con precisión el tráfico en su red.

Además, las comprobaciones integradas en las consultas en la nube de PAN-DB garantizan que el cortafuegos reciba la información de categorización de URL más reciente.

Los cortafuegos configurados para analizar URL en tiempo real mediante aprendizaje automático en el plano de datos proporcionan una capa adicional de seguridad contra sitios web de phishing y exploits de JavaScript. Los modelos de aprendizaje automático en línea que se utilizan para identificar estas amenazas basadas en URL se extienden a variantes de amenazas desconocidas y futuras que coinciden con las características que Palo Alto Networks ha identificado como maliciosas. Para mantenerse al día con los últimos cambios en el panorama de las amenazas, se añaden o actualizan modelos de aprendizaje automático en línea a través de lanzamientos de contenido.

Cuando el cortafuegos comprueba una URL en PAN-DB, también busca actualizaciones críticas, como URL que anteriormente se consideraban benignas pero que ahora son maliciosas.

Si cree que PAN-DB ha categorizado incorrectamente un sitio, puede enviar una solicitud de cambio de categoría de URL en su navegador a través de Test A Site (Probar un sitio) o directamente desde los logs del cortafuegos.

© 2020 Palo Alto Networks, Inc.



¿Sabía esto?

Técnicamente, el cortafuegos almacena en caché las URL tanto en el plano de gestión como en el de datos:

- *PAN-OS 9.0 y las versiones posteriores no descargan las bases de datos semilla de PAN-DB. En cambio, tras la activación de la licencia de filtrado de URL, el cortafuegos completa la caché a medida que se realizan consultas de URL.*
- *El plano de gestión contiene más URL y se comunica directamente con PAN-DB. Cuando el cortafuegos no consigue encontrar una categoría de URL en la memoria caché y realiza una búsqueda en PAN-DB, almacena en caché la información de la categoría recuperada en el plano de gestión. El plano de gestión pasa esa información al plano de datos, que también la almacena en caché y la usa para aplicar la política.*
- *El plano de datos contiene menos URL y recibe información del plano de gestión. Después de que el cortafuegos verifique las* listas de excepciones de categoría de URL *y las* categorías de URL personalizadas *de una URL, el siguiente lugar en el que busca es el plano de datos. Si el cortafuegos no consigue encontrar la URL categorizada en el plano de datos, verifica el plano de gestión y, si no se encuentra la información de la categoría allí, comprueba PAN-DB.*

© 2020 Palo Alto Networks, Inc.

ML en línea de filtrado de URL

El aprendizaje automático en línea del filtrado de URL permite que el plano de datos del cortafuegos aplique el aprendizaje automático en las páginas web para alertar a los usuarios cuando se detectan variantes de suplantación de identidad (phishing) y, al mismo tiempo, evita que variantes maliciosas de vulnerabilidades de JavaScript entren en su red. El aprendizaje automático en línea analiza y detecta dinámicamente contenidos maliciosos mediante la evaluación de varios detalles de la página web mediante una serie de modelos de aprendizaje automática. Cada modelo de aprendizaje automático en línea detecta contenido malicioso mediante la evaluación de los detalles del archivo, incluidos los campos y patrones del decodificador, para formular una clasificación y un veredicto de alta probabilidad, que luego se utiliza como parte de su política de seguridad web más amplia. Las URL clasificadas como maliciosas por el aprendizaje automático en línea se envían a PAN-DB para su análisis y validación adicionales. Para mantenerse al día con los últimos cambios en el entorno de las amenazas, los modelos de aprendizaje automático en línea se actualizan con regularidad y se añaden mediante lanzamientos de contenido. Los modelos de aprendizaje automático en línea de filtrado de URL se configuran a través de su perfil de filtrado de URL y requieren una licencia de filtrado de URL de PAN-DB. Además, también puede especificar excepciones de URL para excluir cualquier falso positivo que pueda encontrarse. Esto le permite crear reglas más granulares para sus perfiles con el fin de respaldar sus necesidades de seguridad específicas.

La protección basada en aprendizaje automático en línea también se puede habilitar para detectar archivos PE maliciosos y scripts de PowerShell en tiempo real como parte de la configuración de su perfil de antivirus. Para obtener más información, consulte WildFire Inline ML.



Aprendizaje automático en línea de filtrado de URL no es compatible en el dispositivo virtual VM-50 o VM50L.

© 2020 Palo Alto Networks, Inc.

Casos de uso de filtrado de URL

Hay muchas formas de usar el filtrado de URL más allá de solo bloquear y permitir ciertos sitios. Por ejemplo, puede usar varias categorías por URL para permitir a los usuarios acceder a un sitio, pero bloquear funciones concretas como enviar credenciales corporativas o descargar archivos. También puede usar categorías de URL para aplicar diferentes tipos de política, como Authentication (Autenticación), Decryption (Descifrado), QoS y Security (Seguridad).

Siga leyendo para obtener más información sobre las diferentes formas en que puede usar el filtrado de URL.

Control del acceso web según la categoría de URL

Puede crear un perfil de filtrado de URL que especifique una acción para una categoría de URL y adjuntar el perfil a una regla de políticas. El cortafuegos aplica la política en el tráfico en función de la configuración del perfil. Por ejemplo, para bloquear todos los sitios web de juego, debe establecer la acción de bloqueo para la categoría de URL *juegos* en el perfil de URL y adjuntarla a las reglas de la política de seguridad que permiten el acceso web.

Filtrado de URL de varias categorías

Cada URL puede tener hasta cuatro categorías, incluida una categoría de riesgo que indica la probabilidad con que un sitio suponga una amenaza. Cuanto más pormenorizadas son las categorizaciones de las URL, más puede distanciar el acceso web del enfoque básico de bloqueo o permiso. En cambio, puede controlar cómo sus usuarios interactúan con contenido en línea que, aunque es necesario para la empresa, es más probable que se use como parte de un ciberataque.

Por ejemplo, puede considerar que determinadas categorías de URL suponen un riesgo para su empresa, pero duda en bloquearlas directamente, ya que también proporcionan recursos o servicios valiosos (como servicios de almacenamiento en la nube o blogs). Ahora, ya puede permitir a los usuarios visitar sitios que coinciden con esos tipos de categorías de URL, al mismo tiempo que proteger la red descifrando el tráfico, inspeccionándolo y aplicando el acceso de solo lectura al contenido.

Si desea ejercer un férreo control sobre una categoría de URL concreta, configure el envío de alertas como acción del perfil de filtrado de URL al realizar el procedimiento Configuración de filtrado de URL. Luego, siga las sugerencias de Prácticas recomendadas sobre filtrado de URL: descifre la categoría de URL, bloquee las descargas de archivos peligrosas y active la prevención del phishing de credenciales.

Permiso o bloqueo de envíos de credenciales corporativas según la categoría de URL

Prevención de phishing de credenciales para habilitar el cortafuegos, detectar envíos de credenciales corporativas a los sitios y controlar esos envíos según la categoría de URL. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre el ingreso de credenciales corporativas en sitios desconocidos o la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos y aprobados.

Aplicación de la configuración de búsqueda segura

Muchos motores de búsqueda incluyen una opción de búsqueda segura que filtra las imágenes y los vídeos para adultos de los resultados de búsqueda. Puede habilitar el cortafuegos para bloquear los resultados de la búsqueda si el usuario final no utiliza la configuración de búsqueda segura más exigente y puede habilitar la búsqueda segura de manera transparente para sus usuarios. El cortafuegos admite la aplicación de

© 2020 Palo Alto Networks, Inc.

búsqueda segura para los siguientes proveedores de búsquedas: Google, Yahoo, Bing, Yandex y YouTube. Consulte cómo comenzar con Forzaje de búsquedas seguras.

Habilitación del acceso a determinados sitios mediante contraseña

Puede bloquear el acceso a un sitio para la mayoría de los usuarios y permitir que determinados usuarios accedan al sitio. Consulte cómo Habilitación del acceso a determinados sitios mediante contraseña.

Bloqueo de descargas de archivos de alto riesgo de determinadas categorías de URL

Puede bloquear las descargas de archivos de alto riesgo de las categorías de URL específicas mediante la creación de una política de seguridad con un perfil de bloqueo de archivos adjunto.

Aplicación de políticas de seguridad, descifrado, autenticación y QoS basadas en la categoría de URL

Puede aplicar diferentes tipos de políticas de cortafuegos según las categorías de URL. Por ejemplo, suponga que ha habilitado descifrado, pero desea excluir que se descifre determinada información personal. En ese caso, podría crear una regla de políticas de descifrado que excluya los sitios web que coincidan con las categorías de URL *servicios financieros* y *salud y medicina* del descifrado. Otro ejemplo sería utilizar la categoría de URL *aplicaciones de transmisión multimedia* en una política de QoS para aplicar controles de ancho de banda a los sitios web que forman parte de esta categoría.

La siguiente tabla describe las políticas que aceptan las categorías de URL como criterios de coincidencia:

Tipo de política	Description (Descripción)
Decryption (Descifrado)	También puede usar categorías de URL para descifrar gradualmente y excluir categorías de URL que puedan contener información confidencial o personal del descifrado (como servicios financieros y salud y medicina). Planifique descifrar primero el tráfico más peligroso (las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos o de alto riesgo) y luego, descifre más a medida que gane experiencia. Como alternativa, descifre primero las categorías de URL que no afecten a su empresa (si algo no funciona, no afectará a la empresa), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios del usuario, ejecute informes para garantizar que el descifrado funciona según lo esperado y, luego, descifre de manera gradual algunas categorías de URL más y así sucesivamente. Planifique realizar exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo. *Se recomienda descifrar el tráfico según las categorías de URL tanto para el filtrado de URL como para el descifrado.*
Authentication (Autenticación)	Para garantizar que los usuarios están autenticados antes de permitirles el acceso a una categoría específica, puede adjuntar una categoría de URL como criterio de coincidencia para las reglas de la política de autenticación.
QoS	Utilizan categorías de URL para asignar los niveles de rendimiento de categorías específicas de sitios web. Por ejemplo, puede que quiera permitir la

© 2020 Palo Alto Networks, Inc.

Tipo de política	Description (Descripción)
	categoría *aplicaciones de transmisión multimedia* y al mismo tiempo limitar el rendimiento añadiendo la categoría de URL a la regla políticas de QoS.
Security (Seguridad)	En las reglas de la política de seguridad, puede usar categorías de URL de dos formas: • Aplicar políticas basadas en categorías de URL seleccionándolas como criterios de coincidencia. • Adjuntar un perfil de filtrado de URL que especifique la acción de política para cada categoría. Si, por ejemplo, el grupo de seguridad de TI de su empresa necesita acceder a la categoría *hacking*, pero a todos los demás usuarios se les deniega el acceso a la categoría, deberá crear las siguientes reglas: • Una regla de la política de seguridad que permita que el grupo seguridad de TI acceda al contenido categorizado como *hacking*. La regla de la política de seguridad hace referencia a la categoría *hacking* de la pestaña **Services/ URL Category (Servicio/Categoría de URL)** y el grupo de seguridad de TI en la pestaña **Users (Usuarios)**. • Otra regla de la política de seguridad que permita acceso web general a todos los usuarios. Para esta regla, adjunte un perfil de filtrado de URL que bloquea la categoría *hacking*. Debe indicar la política que permite el acceso al *hacking* antes de la política que bloquea el *hacking*. Esto se debe a que el cortafuegos evalúa las reglas de la política de seguridad de arriba hacia abajo, por lo que cuando un usuario que forma parte del grupo de seguridad intenta acceder a un sitio de *hacking*, el cortafuegos evalúa primero la regla de políticas que permite el acceso y otorga acceso al usuario. El cortafuegos evalúa los usuarios de todos los demás grupos con respecto a la regla general de acceso web que bloquea el acceso a los sitios de *hacking*.

© 2020 Palo Alto Networks, Inc.

Categorías de URL

En PAN-DB se clasifican los sitios web según su contenido, sus funciones y su seguridad. Las URL pueden tener hasta cuatro categorías, incluidas las categorías de riesgo (alto, medio y bajo) que indican la probable exposición a las amenazas que conllevan los sitios.

Visite Test A Site (Probar sitios) para ver cómo categoriza las URL PAN-DB, para obtener más información sobre todas las categorías de URL disponibles Para enviar solicitudes de cambio de categorías de URL. También puede enviar esas solicitudes directamente en el cortafuegos; para ello, seleccione **Monitor (Supervisar)Logs (Logs)** y abra los detalles de la entrada oportuna del log. y, en URL Category (Categoría de URL), elija la opción para enviar la solicitud.

A continuación se ofrece más información sobre las categorías de URL:

- Casos de uso de filtrado de URL
- Categorías de URL centradas en la seguridad
- Categorías de URL maliciosas
- Categorías de URL verificadas
- Acciones de políticas que puede realizar según las categorías de URL

Categorías de URL centradas en la seguridad

Las categorías de URL centradas en la seguridad permiten reducir la superficie de ataque, puesto que ofrecen opciones de descifrado y aplicación específicas para los sitios que conllevan distintos grados de riesgo, aunque no se ha confirmado que son malintencionados. Los sitios web solo se clasifican con una categoría relacionada con la seguridad si cumplen sus criterios; si varía su contenido, la aplicación de la política se adapta de forma dinámica. No puede enviar solicitudes para modificar las categorías de URL centradas en la seguridad.

Categorías de URL centradas en la seguridad	
High-Risk (Riesgo alto)	Son sitios de alto riesgo los siguientes: • Sitios previamente confirmados como malware, phishing o sitios C2. Estos sitios permanecerán en esta categoría durante al menos 30 días. • Dominios desconocidos, que se clasifican como de alto riesgo hasta que PAN-DB termina de analizar y categorizar los sitios. • Sitios asociados a actividad malintencionada confirmada. Por ejemplo, una página puede ser de alto riesgo si hay hosts malintencionados en el mismo dominio, aunque la página en sí no incluya contenido malintencionado. • Sitios alojados con proveedores de servicios de internet (internet service provider, ISP) blindados. • Dominios clasificados como DDNS debido a la presencia de una configuración DNS dinámica activa. • Sitios alojados en direcciones IP de números de sistemas autónomos (autonomous system number, ASN) conocidos por permitir contenido malintencionado. **Acción de la política predeterminada y recomendada: alerta**
Medium-Risk (Riesgo medio)	Son sitios de medio riesgo los siguientes:

© 2020 Palo Alto Networks, Inc.

Categorías de URL centradas en la seguridad	
	• Todos los sitios de almacenamiento en la nube que tengan la categoría de URL **online-storage-and-backup** (almacenamiento y copia de seguridad en línea). • Sitios que se habían confirmado como de malware, de phishing o de comando y control (command-and-control, C2), pero que solo han mostrado actividad benigna durante al menos 30 días. Estos sitios permanecerán en esta categoría durante 60 días adicionales. • Direcciones IP desconocidas, que se categorización como de medio riesgo hasta que PAN-DB termina de analizar y categorizar los sitios. **Acción de la política predeterminada y recomendada: alerta**
Low-Risk (Riesgo bajo)	Los sitios que no conllevan un riesgo medio ni alto se consideran de bajo riesgo. Estos sitios han mostrado actividad benigna durante un mínimo de 90 días. **Acción de la política predeterminada y recomendada: allow**
Newly-Registered Domains (Dominios recién registrados)	Identifica los sitios que se han registrado en los 32 últimos días. Es frecuente que las campañas malintencionadas utilicen los dominios nuevos como herramientas. **Acción de la política predeterminada: alerta** **Acción de la política recomendada: block** *A menudo, los dominios recién registrados se generan a propósito o con algoritmos de generación de dominios para destinarlos a actividades malintencionadas. Lo más recomendable es bloquear esta categoría de URL.*

Categorías de URL maliciosas

Recomendamos fehacientemente que bloquee las categorías de URL que identifican contenido malicioso o de exploits. Para empezar, puede clonar el perfil predeterminado de URL Filtering que bloquea las categorías de URL de malware, phishing y comando y control por defecto. Este perfil también bloquea otras categorías, como las de contenido sospechoso, contenido para adultos, abuso de drogas, apuestas, piratería informática y armas. El bloqueo de estas categorías de URL depende de los requisitos de su empresa. Por ejemplo, es probable que un centro universitario no desee restringir el acceso de los alumnos a la mayoría de estos sitios porque es importante que haya información disponible, pero le puede interesar bloquearlos a una empresa que valore su seguridad por encima de todo.

- **command-and-control (Comando y control)**: los dominios y URL de comando y control utilizados por software malintencionado y sistemas afectados para comunicarse de manera furtiva con el servidor remoto de un atacante y recibir comandos malintencionados o filtrar datos.
- **malware**: sitios conocidos por alojar software malintencionado o usados para el tráfico de comando y control (C2). También puede exhibir Exploit Kits.
- **phishing**: conocidos por alojar paginas de suplantación de identidad o phishing para identificación personal.

© 2020 Palo Alto Networks, Inc.

- **grayware**: sitios web y servicios que no cumplen con la definición de virus o representan una amenaza de seguridad directa, pero muestran un comportamiento molesto e influyen en los usuarios para que otorguen acceso remoto o realicen otras acciones no autorizadas. El grayware incluye estafas, actividades ilegales, actividades delictivas, sitios de enriquecimiento rápido, adware y otras aplicaciones no deseadas o no solicitadas, como minería criptográfica integrada o secuestradores que cambian los elementos del navegador. Los dominios de typosquatting que no parezcan ser maliciosos y no sean propiedad del dominio objetivo se clasificarán como grayware. Antes de la versión de lanzamiento de contenido 8206, el cortafuegos colocaba el grayware en la categoría de malware o URL cuestionable. Si no está seguro sobre si bloquear el grayware, comience por alertar sobre el grayware, investigue las alertas y, después, decida si bloquear el grayware o continuar alertando sobre el grayware.
- **dynamic-dns**: hosts y nombres de dominio para sistemas que asignan direcciones IP dinámicamente y que a menudo se usan para enviar cargas de malware o tráfico C2. Además, los dominios DNS dinámicos no atraviesan el mismo proceso de examen que los dominios que están registrados por una empresa de registro de dominios reconocida, por lo cual son menos fiables.
- **unknown (desconocido)**: sitios que PAN-DB no ha identificado todavía. Si la disponibilidad es vital para la empresa y debe permitir el tráfico, avise sobre los sitios desconocidos, aplique al tráfico los perfiles recomendados de seguridad e investigue las alertas.

  Las actualizaciones en tiempo real de PAN-DB obtienen información de los sitios desconocidos tras el primer intento de acceso. Así, las URL desconocidas se identifican al instante y se convierten en URL conocidas que puede manejar el cortafuegos según la categoría que les corresponda.
- **newly-registered-domain (dominio recién registrado)**: dominios nuevos que, a menudo, se generan a propósito o con algoritmos de generación de dominios para destinarlos a actividades malintencionadas.
- **copyright-infringement (infracción de derechos de autor)**: dominios con contenido ilegal, como contenido que permite la descarga ilegal de software u otra propiedad intelectual, que podría acarrear una responsabilidad civil. Esta categoría se introdujo para permitir el cumplimiento con las leyes de protección infantil requeridas en el sector de la educación, así como también las leyes en países que exigen que los proveedores de Internet eviten que los usuarios compartan material con derechos de autor a través de su servidor.
- **extremism (extremismo)**: sitios web que promueven el terrorismo, el racismo, el fascismo u otras visiones extremistas que discriminan a personas o grupos de diferentes orígenes étnicos, religiones u otras creencias. Esta categoría se introdujo para permitir el cumplimiento con las leyes de protección infantil requeridas en el sector de la educación. En algunas regiones, la legislación y las normativas prohíben que se permita el acceso a sitios extremistas, lo que puede acarrear una responsabilidad civil.
- **proxy-avoidance-and-anonymizers (Evasión de proxy y anonimizadores)**: URL y servicios a menudo utilizados para desviar productos de filtrado de contenido.
- **questionable (cuestionable)**: sitios web que contienen humor de mal gusto, contenido ofensivo dirigido a datos demográficos específicos de individuos o grupos de personas.
- **parked**: dominios registrados por personas, que a menudo más tarde se descubre que se usan para el phishing de credenciales. Estos dominios pueden ser similares a dominios legítimos; por ejemplo, pal0alto0netw0rks.com, con la intención del phishing de credenciales o información de identificación personal. O bien, pueden ser dominios para los cuales una persona compra los derechos con la esperanza de que un día pueda ser valioso, como por ejemplo, panw.net.

Si decide alertar sobre algunas categorías en lugar de bloquearlas, puede ejercer un férreo control sobre la interacción de los usuarios con el contenido de los sitios. Por ejemplo, franquee a los usuarios el acceso a los recursos que necesitan (como blogs de desarrolladores con fines de investigación o servicios de almacenamiento en la nube), pero adopte las siguientes medidas de precaución para reducir la exposición a las amenazas web:

- ❑ Siga las prácticas recomendadas antispyware, de protección frente a vulnerabilidades y de bloqueo de archivos. Una posible medida de protección consiste en impedir la descarga de tipos de archivos peligrosos y bloquear el código JavaScript oculto de los sitios sobre los que se notifican alertas.

© 2020 Palo Alto Networks, Inc.

- Elija los objetivos del descifrado en función de las categorías de URL. Un buen punto de partida es descifrar los sitios de alto y medio riesgo.
- Muestre una página de respuesta a los usuarios cuando visiten sitios de riesgo medio y alto. Avíselos de que el sitio al que quieren acceder puede ser malintencionado y, si aún desean visitarlo, aconséjeles medidas de precaución.
- Prevenga el robo de credenciales impidiendo que los usuarios envíen sus credenciales corporativas a los sitios, incluidos los de riesgo medio y alto.

Categorías de URL verificadas

Las URL que Palo Alto Networks verifica como parte de un grupo específico de categorías no poseen un nivel de riesgo asociado; los niveles de riesgo solo se aplican a URL que *no* se han verificado. Las URL verificadas en ciertas categorías (ver más abajo) se consideran maliciosas y están bloqueadas de manera predeterminada porque el acceso a estas URL presenta un riesgo que está más allá de un nivel aceptable para la mayoría de los entornos. Las direcciones IP privadas (y los hosts) son exclusivas del entorno del host y no son visibles para PAN-DB; y como resultado, no se genera una calificación de riesgo.

Category	Acción predeterminada
Malware	Block (Bloquear)
Phishing	
Comando y control	
Grayware	
Private IP Addresses (Direcciones IP privadas)	Allowed (Permitido) (sin acción predeterminada)

Para obtener más información sobre las categorías de URL actuales, consulte: Lista completa de categorías de filtrado de URL de PAN-DB

Acciones que puede realizar según las categorías de URL

En el cortafuegos, puede usar un perfil de filtrado de URL para especificar cómo desea aplicar las categorías de URL. De manera predeterminada, el acceso al sitio para todas las categorías de URL se configura como permitido al Crear un nuevo perfil de filtrado de URL. Esto significa que los usuarios podrán navegar por todos los sitios libremente y que el tráfico no se registrará. Personalice el perfil de filtrado de URL cuando decida qué tipo de **acceso al sitio** desea aplicar para cada categoría. Para prevenir el phishing de credenciales, también puede permitir o rechazar **envíos de credenciales de usuario** según la categoría de URL (por ejemplo, puede bloquear los envíos de credenciales de usuario a sitios de riesgo medio y alto). Los usuarios pueden seguir accediendo a esos sitios, pero no pueden entrar y enviar las credenciales corporativas.

Para comenzar a aplicar las acciones que ha definido en un filtrado de URL, deberá conectar el perfil a una regla de la política de seguridad. El cortafuegos aplica las acciones de perfil en el tráfico que coincide con la regla de la política de seguridad (para obtener más información, consulte Configuración de filtrado de URL).

Aprenda a configurar un perfil recomendado de URL Filtering *para garantizar la protección contra las URL que alojan malware o contenido de intrusión.*

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)
Acceso a sitio	
alert	El sitio web está permitido y se genera una entrada de log en el log de filtrado de URL.  *Configure alert (Alerta) como Action (Acción) para las categorías de tráfico que no bloquea registrarse y proporcionar visibilidad en el tráfico.*
allow	El sitio web está permitido y no se genera ninguna entrada de log.  *No configure allow (Permitir) como Action (Acción) para las categorías de tráfico que no bloquea porque pierde visibilidad en el tráfico que no registra. En cambio, configure alert (Alerta) como Action (Acción) para las categorías de tráfico que no bloquea para el registro y proporcionar visibilidad en el tráfico.*
block	El sitio web está bloqueado y el usuario verá una página de respuesta y no podrá ir al sitio web. Se generará una entrada de log en el log de filtrado de URL. El bloqueo del acceso a un sitio para una categoría de URL también establece el bloqueo del envío de credenciales de usuario para esa categoría de URL.
continue	El usuario recibirá una página de respuesta indicando que el sitio se ha bloqueado debido a la política de la empresa, pero se le dará la opción de ir al sitio web. La acción **continue (continuar)** se suele usar para categorías que se consideran inofensivas y se usa para mejorar la experiencia del usuario mediante la posibilidad de continuar si considera que el sitio se ha categorizado incorrectamente. El mensaje de la página de respuesta se puede personalizar para incluir información detallada específica de su empresa. Se generará una entrada de log en el log de filtrado de URL.  *La página Continue (Continuar) no se mostrará correctamente en equipos cliente configurados para usar un servidor proxy.*
override	El usuario verá una página de respuesta indicando que se requiere una contraseña para permitir el acceso a los sitios web de la categoría en cuestión. Con esta opción, el administrador de seguridad o el miembro del departamento de soporte técnico proporcionaría una contraseña que concedería un acceso temporal a todos los sitios web de la categoría en cuestión. Se generará una entrada de log en el log de filtrado de URL. Configure la Habilitación del acceso a determinados sitios mediante contraseña. En las versiones anteriores, las sustituciones de categorías de URL Filtering tenían prioridad sobre las categorías de URL personalizadas. Como parte de la actualización a PAN-OS 9.0, las sustituciones de categorías de URL se han convertido en categorías de URL personalizadas, y su aplicación ya no tiene prioridad sobre las demás categorías personalizadas. En lugar de aplicar la acción que estaba definida en las versiones anteriores, se aplica la regla de la política de seguridad que tenga la acción más estricta del perfil de

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)
	URL Filtering. Las posibles acciones de los perfiles de URL Filtering son, de la más estricta a la menos dura, block (bloquear), override (sustituir), continue (continuar), alert (alertar) y allow (permitir). Por lo tanto, si tenía sustituciones de categorías de URL con la acción allow (permitir), es posible que se bloqueen tras la conversión a la categoría de URL personalizada en PAN-OS 9.0. *La página Override (Cancelar) no se mostrará correctamente en equipos cliente configurados para usar un servidor proxy.*
none	La acción **ninguno** solo se aplica a las categorías de URL personalizadas. Seleccione **none (ninguno)** para asegurarse de que si existen varios perfiles de URL, la categoría personalizada no tendrá ningún efecto en otros perfiles. Por ejemplo, si tiene dos perfiles URL y la categoría URL personalizada está configurada como **block** en un perfil, si no desea que la acción de bloquear se aplique al otro perfil, debe configurar la acción en **none**. Además, para eliminar una categoría de URL personalizada, se debe establecer en **ninguno** en cualquier perfil en el que se use.
Permisos de credenciales de usuario *Estos ajustes requieren que primero realice la* Configuración de la prevención de suplantación de identidad de credenciales*.*	
alert	Permita a los usuarios que envíen credenciales corporativas a los sitios de esta categoría de URL, pero genere un log de alerta de filtrado URL cada vez que esto ocurra.
Permitir (opción predeterminada)	Permita a los usuarios que envíen credenciales corporativas a los sitios web de esta categoría de URL.
block	Bloquee a los usuarios para que no envíen credenciales corporativas a los sitios web de esta categoría. La página de respuesta antiphishing predeterminada se muestra a los usuarios cuando acceden a sitios para los cuales los envíos de credenciales corporativas están bloqueados. Puede optar por crear una página de bloqueo personalizada para mostrar.
continue	Muestra una página de respuesta a los usuarios que solicita que seleccionen Continue (Continuar) para acceder al sitio. De manera predeterminada, la página de continuar para la prevención del phishing se muestra a los usuarios cuando estos ingresan en los sitios para los cuales no se recomienda el envío de credenciales. También puede optar por crear una página de respuesta predeterminada para mostrar, por ejemplo, si desea advertir a los usuarios contra los intentos de phishing o la reutilización de credenciales en otros sitios web.

© 2020 Palo Alto Networks, Inc.

Planificar la implementación de filtrado de URL

Al implementar URL Filtering por primera vez en la red, es recomendable que parta de una configuración básica que le aporte visibilidad sobre los patrones de actividad web, al tiempo que bloquea el contenido malintencionado confirmado:

- Empiece por un perfil pasivo (sobre todo) de URL Filtering que alerte sobre la mayoría de las categorías. Así obtiene visibilidad sobre los sitios a los que acceden los usuarios y puede decidir cuáles permitir, limitar y bloquear.
- Bloquee las categorías de URL que son malintencionadas sin ningún género de dudas: malware, phishing y comando y control (command-and-control, C2).

Como el envío de alertas sobre toda la actividad web crearía una ingente cantidad de archivos de log, puede decidir hacerlo solo al implementar el filtrado de URL por primera vez.



En ese momento, también puede reducir los logs de filtrado de URL de otro modo: marque la opción Log container page only (Crear log solo de la página contenedora) en el perfil de URL Filtering para que solamente se registre la página principal que coincida con la categoría, pero no las páginas ni categorías de la página contenedora que se carguen después.

STEP 1 | En cualquier momento, puede usar Test A Site (Probar un sitio) para ver cómo PAN-DB, la base de datos de la nube de filtrado de URL, clasifica una URL específica y para conocer todas las categorías de URL posibles.

También puede usar Test A Site (Probar un sitio) para enviar una solicitud de cambio si no está de acuerdo con cómo se clasifica una URL específica.

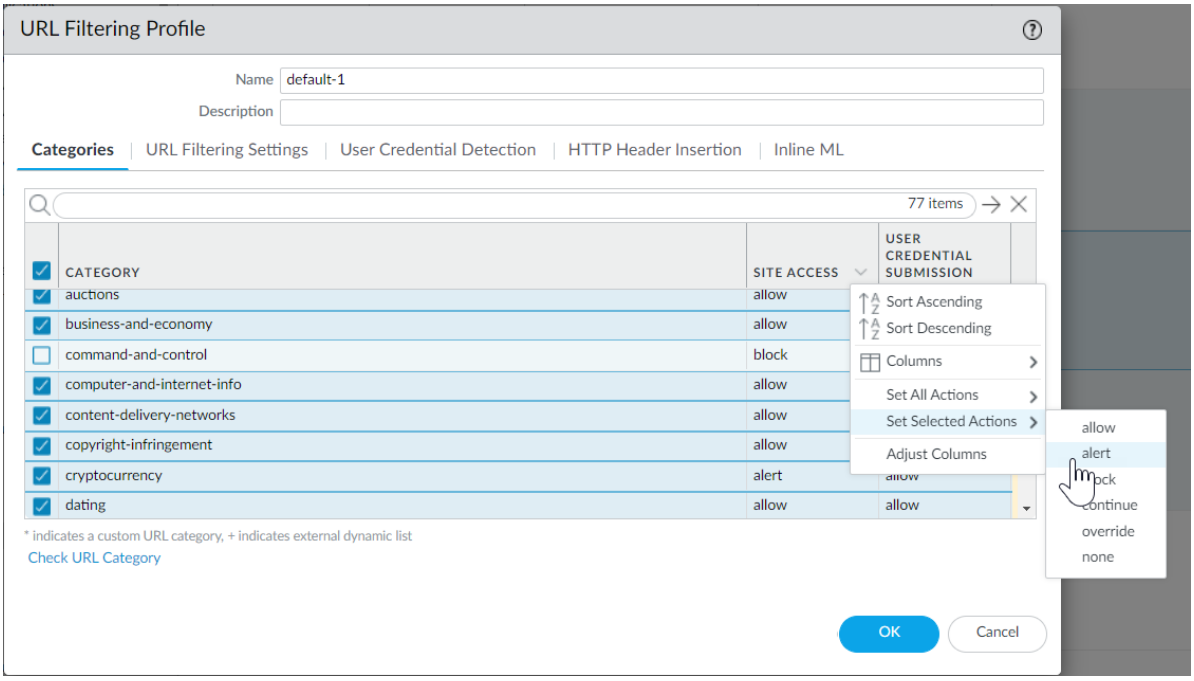
STEP 2 | Cree un perfil de filtrado de URL pasivo, que alerta en todas las categorías para que tenga visibilidad del tráfico web.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)> URL Filtering (Filtrado de URL)**.
2. Seleccione el perfil predeterminado y, a continuación, haga clic en **Duplicar**. El nuevo perfil se denominará **predeterminado-1**.
3. Seleccione el perfil **predeterminado-1** y cámbiele el nombre. Por ejemplo, cámbiele el nombre por Supervisión-URL.

STEP 3 | Configure en **alert (alertar)** la acción de todas las categorías excepto las de malware, phishing y comando y control, que deben permanecer bloqueadas.

1. En la sección que muestra todas las categorías de URL, seleccione todas las categorías y, a continuación, anule la selección de malware, comando y control y phishing.
2. A la derecha del encabezado de la columna *Acción*, pase el ratón por encima, seleccione la flecha hacia abajo, a continuación, seleccione **Establecer acciones seleccionadas** y seleccione **Alertar**.

© 2020 Palo Alto Networks, Inc.



3. **Bloquee** el acceso a categorías de URL peligrosas conocidas.

   Bloquee el acceso a las categorías de URL: malware, phishing, DNS dinámico, desconocidas, de comando y control, extremistas, de infracción de derechos de autor, de anonimización y anulación de proxy, de dominio recién registrado, grayware y estacionadas.

4. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 4 | Aplique el perfil de filtrado de URL a las reglas de política de seguridad que permiten el tráfico web para los usuarios.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la política de seguridad adecuada para modificarla.
2. Seleccione la pestaña **Acciones** y, en la sección **Ajuste de perfil**, haga clic en el menú desplegable **Filtrado de URL** y seleccione el nuevo perfil.
3. Haga clic en **OK (Aceptar)** para guardar.

STEP 5 | Guarde la configuración.

Haga clic en **Commit (Confirmar)**.

STEP 6 | Visualice los logs de filtrado de URL para consultar todas las categorías de sitios web a las que están accediendo sus usuarios. También se crean logs de las categorías bloqueadas.

Para obtener información sobre cómo visualizar los logs y generar informes, consulte Supervisión de la actividad web.

Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**. Se crea una entrada de log para cualquier sitio web que exista en una categoría de la base de datos de filtrado de URL configurada con una acción distinta de **allow (permitir)**. Los informes de filtrado de URL le ofrecen una vista de la actividad web en un periodo de 24 horas. (**Monitor (Supervisar)** > **Reports (Informes)**).

STEP 7 | Siguientes pasos:

© 2020 Palo Alto Networks, Inc.

- PAN-DB clasifica cada URL con hasta cuatro categorías, y cada URL tiene una categoría de riesgo (alta, media y baja). Aunque no se haya confirmado que los sitios de riesgo alto y medio sean sitios malintencionados, guardan una estrecha relación con sitios que sí lo son. Por ejemplo, están en el mismo dominio que sitios malintencionados o han alojado contenido malintencionado hasta hace poco. Para todo lo que no permita o bloquee, puede usar categorías de riesgo para redactar una política simple basada en la seguridad del sitio web.

  Puede tomar medidas de precaución para limitar especialmente la interacción de sus usuarios con sitios de alto riesgo, ya que puede haber algunos casos en los que desee dar acceso a sus usuarios a sitios que también puedan presentar problemas de seguridad (por ejemplo, es posible que quiera permitir que sus desarrolladores puedan usar blogs de desarrolladores para la investigación, sin embargo, los blogs son una categoría que suele albergar malware).
- Empareje el filtrado de URL con User-ID para controlar el acceso web basado en la organización o departamento, y para bloquear el envío de credenciales corporativas a sitios no autorizados:
  - El filtrado de URL previene el robo de credenciales mediante la detección de envíos de credenciales corporativas a sitios basados en la categoría de sitio. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre el ingrese de credenciales corporativas en sitios desconocidos o advierta contra la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos.
  - Añada o actualice una regla de la política de seguridad con el perfil de filtrado de URL pasivo para que se aplique a un grupo de usuarios del departamento, por ejemplo, Marketing o Ingeniería (**Policies (Políticas)** > **Security (Seguridad)** > **User (Usuario)**). Supervise la actividad del departamento y obtenga comentarios de los miembros del departamento para comprender los recursos web que son esenciales para el trabajo que realizan.
- Considere todas las formas en que puede usar el filtrado de URL para reducir su superficie de ataque y controlar el uso de la web. Por ejemplo, en el caso de un colegio, puede usar el filtrado de URL para aplicar una configuración de búsqueda segura y estricta donde los motores de búsqueda filtren las imágenes y vídeos para adultos de los resultados de búsqueda. O, si tiene un centro de operaciones de seguridad, puede proporcionar a los analistas de amenazas acceso con contraseña a sitios comprometidos o peligrosos para la investigación, que no querrá que abran organizaciones o equipos enteros.
- Siga Prácticas recomendadas de filtrado de URL.

© 2020 Palo Alto Networks, Inc.

Prácticas recomendadas de filtrado de URL

El filtrado de URL de Palo Alto Networks le protege de las amenazas basadas en la web y le proporciona una forma sencilla de supervisar y controlar la actividad web. Para aprovechar al máximo el filtrado de URL, primero cree reglas permitidas para las aplicaciones en las que confía para desarrollar su actividad empresarial. A continuación, revise las categorías de URL que clasifican el contenido malicioso y de exploits; le recomendamos que las bloquee directamente. Después, para todo lo demás, estas prácticas recomendadas pueden servirle como guía sobre cómo reducir la exposición a las amenazas basadas en la web sin limitar el acceso de sus usuarios al contenido web que necesitan.

- Antes de comenzar con el filtrado de URL, identifique las aplicaciones que desee permitir y cree las reglas de permiso de aplicaciones como parte de la creación de una política de seguridad de puerta de enlace de Internet recomendada.

  Las aplicaciones permitidas incluyen no solo las aplicaciones que usted suministra y administra para fines empresariales y de infraestructura, sino también otras aplicaciones que los usuarios pueden necesitar para desempeñar sus funciones, y las aplicaciones que usted puede elegir autorizar para uso personal.

  Una vez que haya identificado estas aplicaciones autorizadas, puede usar el filtrado de URL para controlar y proteger toda la actividad web que no esté en la lista de permisos.
- Obtenga visibilidad de la actividad web de sus usuarios para poder planificar la política de filtrado de URL de la manera más eficaz para su empresa y ponerla en práctica sin problemas. Esto incluye lo siguiente:
  - Uso de Test A Site (Probar un sitio) para ver cómo PAN-DB, la base de datos de la nube de filtrado de URL, clasifica una URL específica y para conocer todas las categorías de URL posibles.
  - Empiece por un perfil pasivo (sobre todo) de filtrado de URL que alerte sobre las categorías de URL. Así obtiene visibilidad sobre los sitios a los que acceden los usuarios y puede decidir cuáles permitir, limitar y bloquear.
  - Supervisión de la actividad web para evaluar los sitios a los que acceden sus usuarios y ver cómo se alinean con las necesidades de su empresa.
- Bloquee categorías de URL que clasifiquen contenido web malicioso y de exploits. Aunque sabemos que estas categorías son peligrosas, siempre tenga en cuenta que las categorías de URL que decida bloquear pueden depender de las necesidades de su empresa.
- Use categorías de URL para descifrar gradualmente y para excluir información confidencial o personal (como servicios financieros y salud y medicina) del descifrado.

  Planifique descifrar primero el tráfico más peligroso (las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos o de alto riesgo) y luego, descifre más a medida que gane experiencia. Como alternativa, descifre primero las categorías de URL que no afecten a su empresa (si algo no funciona, no afectará a la empresa), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios del usuario, ejecute informes para garantizar que el descifrado funciona según lo esperado y, luego, descifre de manera gradual algunas categorías de URL más y así sucesivamente. Planifique realizar exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo.

  El descifrado limitado basado en categorías de URL también es una recomendación para el descifrado.
- Prevenga el robo de credenciales mediante la habilitación del cortafuegos, la detección de envíos de credenciales corporativas a los sitios y el control de esos envíos según la categoría de URL. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre el ingreso de credenciales corporativas en sitios desconocidos o la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos y aprobados.

© 2020 Palo Alto Networks, Inc.

- Bloquee variantes maliciosas de exploits de JavaScript y ataques de phishing en tiempo real. La habilitación de ML en línea de filtrado de URL le permite analizar páginas web dinámicamente mediante el aprendizaje automático en el cortafuegos.
- Descifre, inspeccione y limite estrictamente la forma en que los usuarios interactúan con contenido de riesgo alto y medio (si decidió no bloquear ninguno de los Categorías de URL maliciosas por razones empresariales, también debe limitar estrictamente la forma en que los usuarios interactúan con esas categorías).

  El contenido web que sancione y las categorías de URL maliciosas que bloquee directamente son solo una parte de su tráfico web general. El resto del contenido al que acceden sus usuarios es una combinación de contenido benigno (riesgo bajo) y de riesgo (alto riesgo alto y medio). El contenido de riesgo alto y medio no se confirma como malicioso, pero está estrechamente relacionado con sitios que sí lo son. Por ejemplo, una URL de alto riesgo podría estar en el mismo dominio que un sitio malicioso, o quizás alojara contenido malicioso en el pasado.

  Sin embargo, muchos sitios que representan un riesgo para su empresa también proporcionan recursos y servicios valiosos a sus usuarios (los servicios de almacenamiento en la nube son un buen ejemplo). Aunque estos recursos y servicios son necesarios para las empresas, también es más probable que se utilicen como parte de un ciberataque. A continuación, le mostramos cómo controlar la forma en la que interactúan los usuarios con ese contenido potencialmente peligroso, a la vez que les proporciona una buena experiencia de usuario:

  - En un perfil de filtrado de URL, configure las categorías de riesgo alto y medio en **continue (Continuar)** para ver la página de respuesta en la que se advierte a los usuarios que están visitando un sitio potencialmente peligroso. Indíqueles cómo tomar precauciones si deciden continuar en el sitio. Si no desea solicitar a los usuarios una página de respuesta, alerte sobre las categorías de riesgo alto y medio.
  - Decrypt (Descifrar) permite descifrar sitios de riesgo alto y medio.
  - Siga las prácticas recomendadas sobre antispyware, protección frente a vulnerabilidades y el bloqueo de archivos para sitios de riesgo alto y medio. Una posible medida de protección consiste en impedir la descarga de tipos de archivos peligrosos y bloquear el código JavaScript oculto.
  - Prevenga el robo de credenciales impidiendo que los usuarios envíen sus credenciales corporativas a los sitios de riesgo medio y alto.
- Las escuelas o las instituciones educativas deben usar la aplicación segura de la búsqueda para asegurarse de que los motores de búsqueda filtren las imágenes y vídeos para adultos de los resultados de búsqueda. Incluso puede habilitar de forma transparente la búsqueda segura de usuarios.
- Habilite el cortafuegos para mantener una solicitud web inicial mientras busca la categoría de URL de un sitio web con PAN-DB.

  Cuando un usuario visite un sitio web, un cortafuegos con filtrado de URL habilitado verificará su caché local de categorías de URL para clasificar el sitio. Si el cortafuegos no encuentra la categoría de la URL en el caché, realizará una búsqueda en PAN-DB, la base de datos de URL de Palo Alto Networks. De manera predeterminada, el cortafuegos permite la solicitud web del usuario durante esta búsqueda en la nube y aplica la política cuando el servidor responde.

  Sin embargo, si elige retener solicitudes web, el cortafuegos bloquea la solicitud hasta que encuentra la categoría de URL o agota el tiempo de espera. Si se agota el tiempo de búsqueda, el cortafuegos considera que la categoría de URL no está resuelta.

  1. En **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID**, active la casilla

     Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría).

© 2020 Palo Alto Networks, Inc.

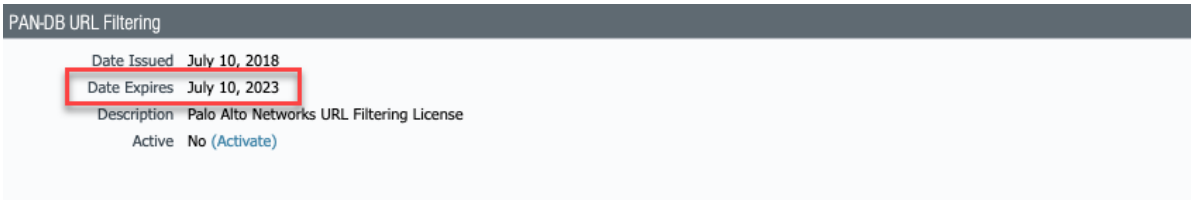
Habilitación de PAN-DB

La base de datos de filtrado de URL desarrollada por Palo Alto Networks, PAN-DB, ofrece una caché local de alto rendimiento para un rendimiento en línea máximo en las búsquedas de URL, y ofrece cobertura contra direcciones IP y URL dañinas. A medida que WildFire identifica el malware desconocido, las vulnerabilidades iniciales y las amenazas avanzadas persistentes (advanced persistent threat, APT), la base de datos PAN-DB se actualiza con información sobre las URL malintencionadas para que pueda bloquear las descargas de malware y deshabilitar las comunicaciones de comando y control (command-and-control, C2)a fin de proteger su red de las ciberamenazas. Las categorías de URL que identifican el contenido confirmado como malintencionado (malware, phishing y C2) se actualizan cada cinco minutos para que pueda gestionar el acceso a esos sitios apenas unos minutos después de su categorización.

STEP 1 | Obtenga e instale una licencia de PAN-DB URL Filtering y confirme que está instalada.

Si la licencia caduca, el cortafuegos deja de realizar el filtrado de URL de PAN-DB; la ejecución de categoría de URL, las búsquedas en la nube de URL y otras actualizaciones basadas en la nube no funcionarán hasta que instale una licencia válida.

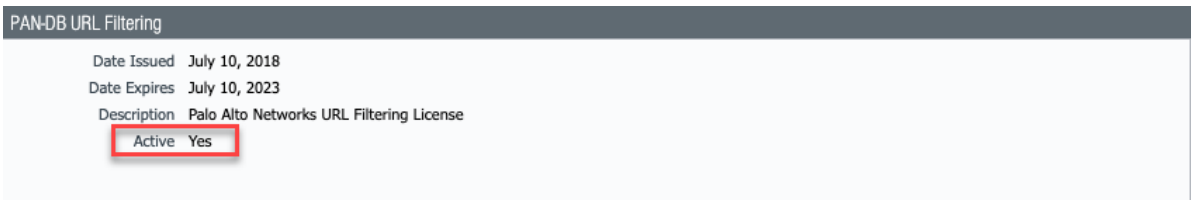
1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y, en la sección License Management (Gestión de licencias), seleccione el método de instalación de la licencia:
   - **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**
   - **Activate feature using authorization code (Activar característica mediante código de autorización)**
   - **Manually upload license key (Clave de licencia de carga manual)**
2. Después de instalar la licencia, confirme si en la sección PAN-DB URL Filtering, en el campo **Date Expires**, se muestra una fecha válida.



STEP 2 | Active el filtrado de URL de PAN-DB.

PAN-OS 9.0 y las versiones posteriores no descargan las bases de datos semilla de PAN-DB. En cambio, tras la activación de la licencia de filtrado de URL, el cortafuegos completa la caché a medida que se realizan consultas de URL.

1. Haga clic en **Activate (Activar)**. El valor en el campo Active (Activo) cambia a Yes (Sí).



STEP 3 | Programe el cortafuegos para descargar actualizaciones dinámicas para Aplicaciones y amenazas.

© 2020 Palo Alto Networks, Inc.

Se requiere una licencia de prevención de amenazas para recibir actualizaciones de contenido, la cual cubre Antivirus y Aplicaciones y amenazas.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. En el campo Schedule de la sección Aplicaciones y amenazas, haga clic en el enlace **None** para programar actualizaciones periódicas.

   Solo puede programar actualizaciones dinámicas si el cortafuegos tiene acceso directo a internet. Si las actualizaciones ya están programadas en una sección, el texto del enlace muestra la configuración de la programación.

   Las actualizaciones de aplicaciones y amenazas pueden incluir actualizaciones para el filtrado de URL en relación con la opción Safe Search Enforcement (Aplicación de búsquedas seguras).

© 2020 Palo Alto Networks, Inc.

Configuración de filtrado de URL

Después de determinar los requisitos de la política de filtrado de URL, debe tener conocimientos básicos de los tipos de sitios web y categorías de sitios web a los que están accediendo sus usuarios. Utilice esta información para crear perfiles de filtrado de URL personalizados y adjuntarlos a las reglas de la política de seguridad que permiten el acceso web. Además de gestionar el acceso web con un perfil de filtrado de URL y si tiene User-ID configurado, también puede gestionar los sitios a los cuales los usuarios pueden enviar credenciales corporativas.

STEP 1 | Cree un perfil de filtrado de URL.



Si aún no lo tiene, configure un perfil de filtrado de URL recomendado para garantizar protección contra las URL que alojan malware o contenido de exploits.

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.

STEP 2 | Defina el acceso al sitio para cada categoría de URL.

Seleccione **Categories (Categorías)** y configure el acceso al sitio para cada categoría de URL:

- **Permita** el tráfico destinado a esa categoría de URL; el tráfico permitido no está registrado.
- Seleccione **alert (alerta)** para tener visibilidad sobre los sitios a los que los usuarios están accediendo. La coincidencia de tráfico para la categoría está permitida, pero un log de filtrado de URL se genera para registrar cuando un usuario accede a un sitio de la categoría.
- Seleccione **block (bloquear)** para denegar el acceso al tráfico que coincide con la categoría y registrar en logs el tráfico bloqueado.
- Seleccione **continue (continuar)** para mostrar una página a los usuarios con una advertencia y solicitarles que hagan clic en **Continue (Continuar)** para proceder a un sitio de la categoría.
- Para permitir el acceso solo si los usuarios especifican una contraseña configurada, seleccione **override (cancelar)**. Para obtener más información, consulte Habilitación del acceso a determinados sitios mediante contraseña.

STEP 3 | Configure el perfil de filtrado de URL para detectar envíos de credenciales corporativas a sitios web que están en categorías URL permitidas.



El cortafuegos omite automáticamente la comprobación de los envíos de credenciales para App-ID™ asociados con los sitios que nunca se ha observado que alojan malware o contenido de phishing (suplantación de identidad), para garantizar un desempeño óptimo y una tasa de falsos positivos baja, incluso si habilita las comprobaciones en la categoría correspondiente. La lista de sitios en los cuales el cortafuegos omitirá la comprobación de credenciales se actualiza automáticamente a través de las actualizaciones de aplicación y contenido de prevención de amenazas.

1. Seleccione **User Credential Detection (Detección de credencial de usuario)**.
2. Seleccione uno de los Métodos para comprobar los envíos de credenciales corporativas a páginas web en la lista desplegable **User Credential Detection (Detección de credenciales de usuario)**:
   - **Use IP User Mapping (Usar asignación de usuarios IP):** comprueba el envío de nombres de usuario corporativo válidos y verifica que el nombre de usuario coincida con el usuario registrado en la dirección IP de origen de la sesión. Para utilizar este método, el cortafuegos compara el nombre de usuario enviado con su tabla de asignación de direcciones IP a nombres de usuario. Para utilizar

© 2020 Palo Alto Networks, Inc.

este método puede emplear cualquiera de los métodos de asignación de usuarios descritos en Asignar direcciones IP a los usuarios.

- **Use Domain Credential Filter (Usar filtro de credenciales de dominio)**: comprueba el envío de nombres de usuario y contraseñas válidas, y verifica que el nombre de usuario esté asignado a la dirección IP del usuario registrado. Consulte Configuración de la asignación de usuarios mediante el agente de User-ID de Windows para obtener instrucciones sobre cómo configurar User-ID para habilitar este método.
- **Use Group Mapping (Usar asignación de grupo)**: comprueba el envío de nombres de usuario válidos en función de la tabla de asignación de usuario a grupo completada al configurar el cortafuegos para la asignación de usuarios a grupos.

  Con la asignación de grupos, usted puede aplicar la detección de credenciales a **cualquier** parte del directorio o a un grupo específico, tal como grupos como TI que tienen acceso a sus aplicaciones más sensibles.



Este método es propenso a falsos positivos en entornos que no tienen nombres de usuario estructurados de manera única, por lo que solo debe usar este método para proteger sus cuentas de usuario valiosas.

3. Configure la **Valid Username Detected Log Severity (Gravedad del log detectado de nombre de usuario válido)** que el cortafuegos utilizará para la detección de logs de envío de credenciales corporativas (el valor predeterminado es media).

STEP 4 | Configure el perfil de filtrado de URL para detectar el phishing y el JavaScript malicioso en tiempo real mediante ML en línea de filtrado de URL.

STEP 5 | Habilite o bloquee a los usuarios para el envío de credenciales corporativas a sitios en función de la categoría de URL para la prevención del phishing de credenciales.



El cortafuegos omite automáticamente la comprobación de los envíos de credenciales para App-ID asociados con los sitios que nunca se ha observado que alojan malware o contenido de phishing (suplantación de identidad), para garantizar un desempeño óptimo y una tasa de falsos positivos baja, incluso si habilita las comprobaciones en la categoría correspondiente. La lista de sitios en los cuales el cortafuegos omitirá la comprobación de credenciales se actualiza automáticamente a través de las actualizaciones de aplicación y contenido de prevención de amenazas.

1. Para cada categoría de URL a la cual se permite el **acceso al sitio**, seleccione cómo desea que se manejen los **envíos de credenciales de usuario**:
   - **alert (alerta)**: permite que los usuarios envíen sus credenciales al sitio web, pero genera un log de alerta de filtrado de URL cada vez que un usuario envía credenciales a sitios de esta categoría de URL.
   - **allow (permitir)**: (predeterminado) permite que los usuarios envíen sus credenciales al sitio web.
   - **block (bloquear)**: muestra la Página de bloqueo antiphishing para bloquear a los usuarios para el envío de credenciales al sitio web.
   - **continue (continuar)**: presente la Página de continuación antiphishing para solicitar a los usuarios que hagan clic en **Continue (Continuar)** para acceder al sitio.
2. Configure el perfil de filtrado de URL para detectar envíos de credenciales corporativas a sitios web que están en categorías URL permitidas.

STEP 6 | Defina las Listas de excepción de categorías de URL para especificar los sitios web que siempre deben bloquearse o permitirse, independientemente de la categoría de URL.

© 2020 Palo Alto Networks, Inc.

Por ejemplo, para reducir los logs de filtrado de URL, es posible que desee añadir sus sitios web corporativos a la lista de permitidos para que no se generen logs para esos sitios o, si hay un sitio web que se usa demasiado y no está relacionado con el trabajo, puede añadirlo a la lista de bloqueo.

El tráfico de los sitios web que se encuentran en la lista de bloqueados siempre se bloquea independientemente de la acción de la categoría asociada. El tráfico de las URL que se encuentra en la lista de permitidos siempre está permitido.

Para obtener más información sobre el formato correcto y el uso de comodines, consulte Listas de excepción de categorías de URL.

1. Seleccione **Overrides (Cancelaciones)** e ingrese las URL o direcciones IP en la **Block List (Lista de bloqueo)**, y seleccione una acción:
   - **Bloquear**: Bloquea la dirección URL.
   - **continue (continuar)**: solicitar a los usuarios que hagan clic en **Continue (Continuar)** para ir a la página web.
   - **override (cancelar)**: se solicita a los usuarios una contraseña para ir al sitio web.
   - **alert (alertar)**: permite al usuario acceder al sitio web y añade una entrada de log de alerta en el log de URL.
2. Para la lista **Allow (Permitidas)**, introduzca las direcciones IP o URL que deberían permitirse siempre. Cada fila debe estar separada por una nueva línea.

STEP 7 | Habilite Aplicación forzada de búsquedas seguras.

STEP 8 | Registre solo Container Pages (Páginas de contenedor) para los eventos de filtrado de URL.

1. Seleccione **URL Filtering Settings (Configuración de filtrado URL)**. Habilite **Log container page only (Registrar solo página de contenedor)** (predeterminado) para que el cortafuegos registre solo la página principal que coincida con la categoría, no las páginas posteriores o las categorías que se cargaron dentro de la página del contenedor.
2. Para habilitar la creación de logs para todas las páginas y categorías, deshabilite la opción **Log container page only (Registrar solo página de contenedor)**.

STEP 9 | Habilite HTTP Header Logging (Registro de encabezado HHTTP) para uno o varios de los campos de encabezado HTTP admitidos.

Seleccione **URL Filtering Settings (Configuración de filtrado URL)** y seleccione uno o varios de los siguientes campos para registrar:

- **User-Agent (Agente de usuario)**
- **Referer (Sitio de referencia)**
- **X-Forwarded-For**

STEP 10 | Guarde el perfil de filtrado URL y confirme los cambios.

1. Haga clic en **OK (Aceptar)**.
2. Haga clic en **Commit (Confirmar)**.

Para probar la configuración de filtrado de URL, acceda a un sitio web en una categoría configurada para bloquear o continuar y, después, observe si el cortafuegos realiza la acción adecuada.

STEP 11 | Habilite **Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría)** para bloquear las solicitudes de cliente mientras el cortafuegos realiza búsquedas de categoría de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.

© 2020 Palo Alto Networks, Inc.

2. Seleccione **Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría)**.
3. Commit (Confirmar) los cambios.



Habilite esta función como práctica recomendada de filtrado de URL.

STEP 12 | Establezca la cantidad de tiempo, en segundos, antes de que se agote el tiempo de espera de una búsqueda de categoría de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **icono de engranaje**.
2. Especifique un número en **Category lookup timeout (sec) (Tiempo de espera de búsqueda de categoría (s))**.
3. Haga clic en **OK (Aceptar)**.
4. Commit (Confirmar) los cambios.

© 2020 Palo Alto Networks, Inc.

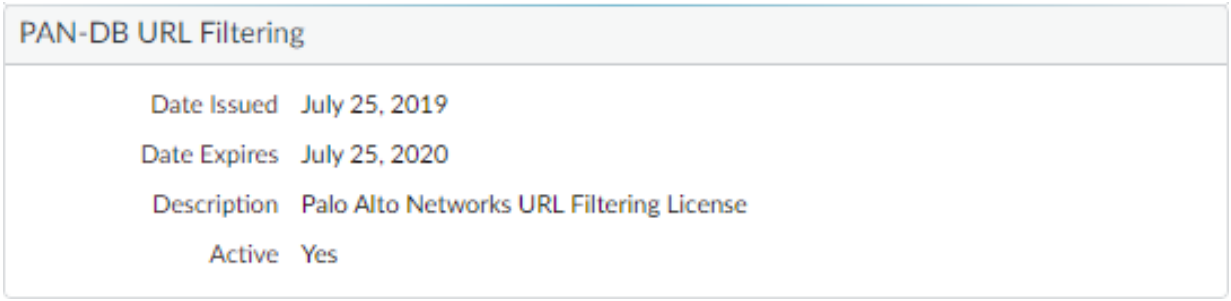
Configuración de aprendizaje automático en línea de filtrado de URL

Para habilitar su configuración de aprendizaje automático en línea de filtrado de URL, adjunte el perfil de filtrado de URL configurado con la configuración de aprendizaje automático en línea a una regla de la política de seguridad (consulte Configuración de una política de seguridad básica).

El aprendizaje automático en línea de filtrado de URL no es compatible actualmente en el dispositivo virtual VM-50 o VM50L.

STEP 1 | Para aprovechar el aprendizaje automático en línea de filtrado de URL, debe tener una suscripción activa de filtrado de URL PAN-DB para analizar páginas web en busca de JavaScript y amenazas de phishing.

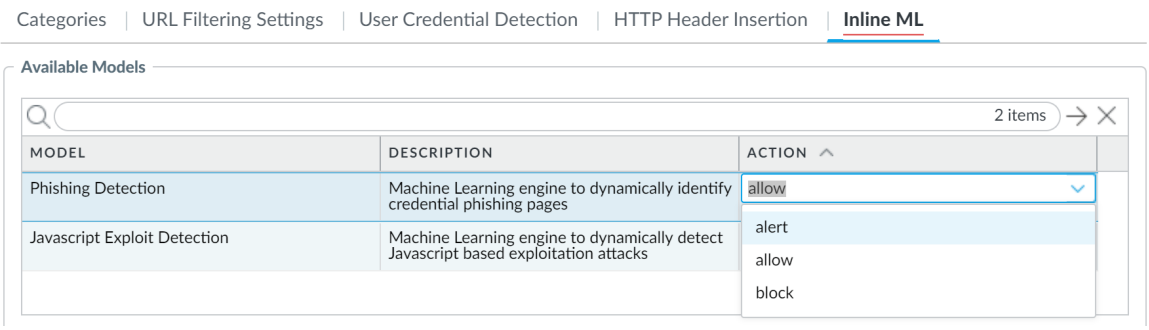
Verifique que tenga una suscripción de filtrado de URL PAN-DB. Para verificar las suscripciones para las que tiene licencias actualmente activas, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.



STEP 2 | Cree un perfil nuevo o actualice sus perfiles de seguridad de filtrado de URL existentes para utilizar el aprendizaje automático en línea de filtrado de URL.

1. Seleccione un **perfil de filtrado de URL** existente o **añada** uno nuevo (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**.
2. Seleccione **Inline ML (Aprendizaje automático en línea)** y defina una **acción** de la política para cada modelo de aprendizaje automático en línea de filtrado de URL. Esto reforzará la acción de la política seleccionada según el modelo. Actualmente, hay dos motores de clasificación disponibles: **Phishing** y **exploits de JavaScript**, uno para cada tipo de contenido malicioso de una página web.
   - **Block (Bloquear)**: cuando el cortafuegos detecta un sitio web con contenido de phishing, genera una entrada de log de filtrado de URL.
   - **Alert (Alerta)**: el cortafuegos permite el acceso al sitio web, pero también genera una entrada de log de filtrado de URL.
   - **Allow (Permitir)**: el cortafuegos que permite el acceso al sitio web no genera una entrada de log de filtrado de URL.

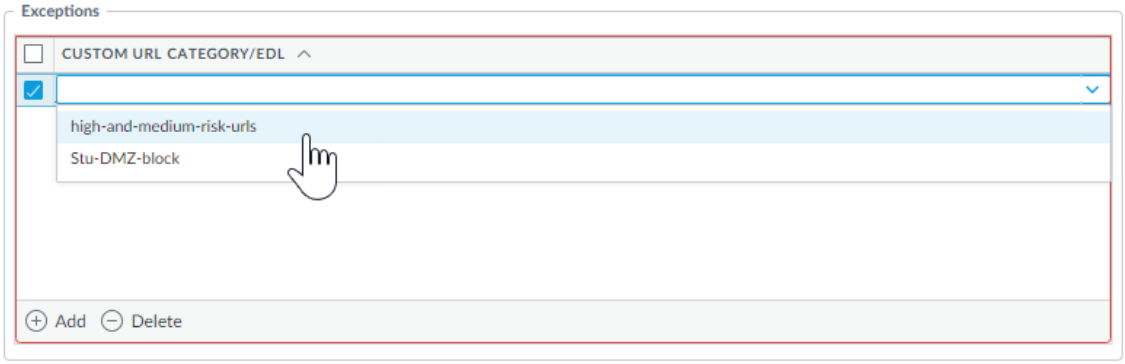
© 2020 Palo Alto Networks, Inc.



3. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de filtrado de URL y **confirmar** sus cambios.

STEP 3 | (Opcional) Añada excepciones de URL a su perfil de seguridad de filtrado de URL si encuentra falsos positivos. Puede añadir excepciones especificando una EDL desde el perfil de filtrado de URL o agregando una entrada de página web desde los logs de filtrado de URL.

- Añada una lista de excepciones de URL de EDL.
  1. Seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > URL Filtering (Filtrado de URL)**.
  2. Seleccione un perfil de filtrado de URL para el que desee excluir URL específicas y, a continuación, seleccione **Inline ML (Aprendizaje automático en línea)**.
  3. Haga clic en **Add (Añadir)** para seleccionar una lista dinámica externa basada en URL preexistente. Si no hay ninguno disponible, cree una nueva lista dinámica externa.



  4. Haga clic en **OK (Aceptar)** para guardar el perfil de filtrado de URL y **confirmar** los cambios.
- Añada excepciones de archivos a partir de las entradas de log de filtrado de URL.
  1. Seleccione **Monitor (Supervisar) > Logs > URL Filtering (Filtrado de URL)** y filtre los logs para las entradas de URL con un veredicto de aprendizaje automático en línea de **malicious-javascript (javascript malicioso)** o **phishing**. Seleccione un log de filtrado de URL para una URL para la que desea crear una excepción.
  2. Vaya a la **vista de log detallada** y desplácese hacia abajo hasta el panel **Details (Detalles)** y, a continuación, seleccione **Create Exception (Crear excepción)** que se encuentra junto al **veredicto de aprendizaje automático en línea**.



  3. Seleccione una categoría personalizada para la excepción de URL y haga clic en **OK (Aceptar)**.
  4. La nueva excepción de URL se puede encontrar en la lista a la que se añadió en **Objects (Objetos) > Custom Objects (Objetos personalizados) > URL Category (Categoría de URL)**.

© 2020 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Verifique el estado de la conectividad del cortafuegos con el servicio en la nube de aprendizaje automático en línea.

Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

```
show mlav cloud-status
```

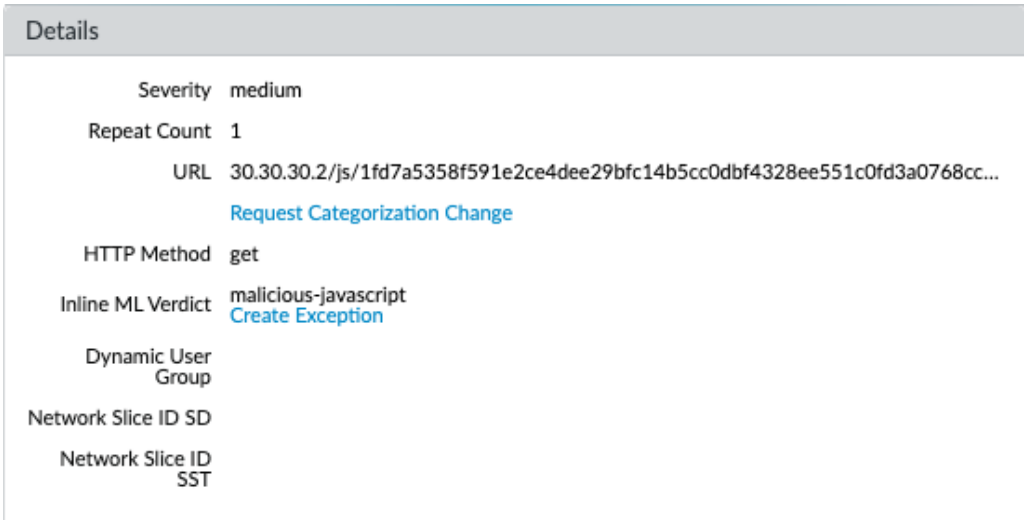
Por ejemplo:

```
show mlav cloud-status

MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
Cloud connection:              connected
```

Si no puede conectarse al servicio en la nube de aprendizaje automático en línea, verifique que el siguiente dominio no esté bloqueado: ml.service.paloaltonetworks.com.

Para ver información sobre las páginas web que se han procesado mediante el aprendizaje automático en línea de filtrado de URL, filtre los logs (**Monitor [Supervisar] > Logs > URL Filtering [Filtrado de URL]**) según el **veredicto de aprendizaje automático en línea**. Las páginas web que se ha determinado que contienen amenazas se clasifican con veredictos de **phishing** o **malicious-javascript (javascript malicioso)**. Por ejemplo:



© 2020 Palo Alto Networks, Inc.

Supervisión de la actividad web

El ACC, los informes y logs de filtrado de URL muestran toda la actividad web de los usuarios para las categorías de URL establecidas como **alert**, **block**, **continue** u **override**. Al supervisar los logs, puede obtener una mayor comprensión de la actividad web de su base de usuarios para determinar una política de acceso web.

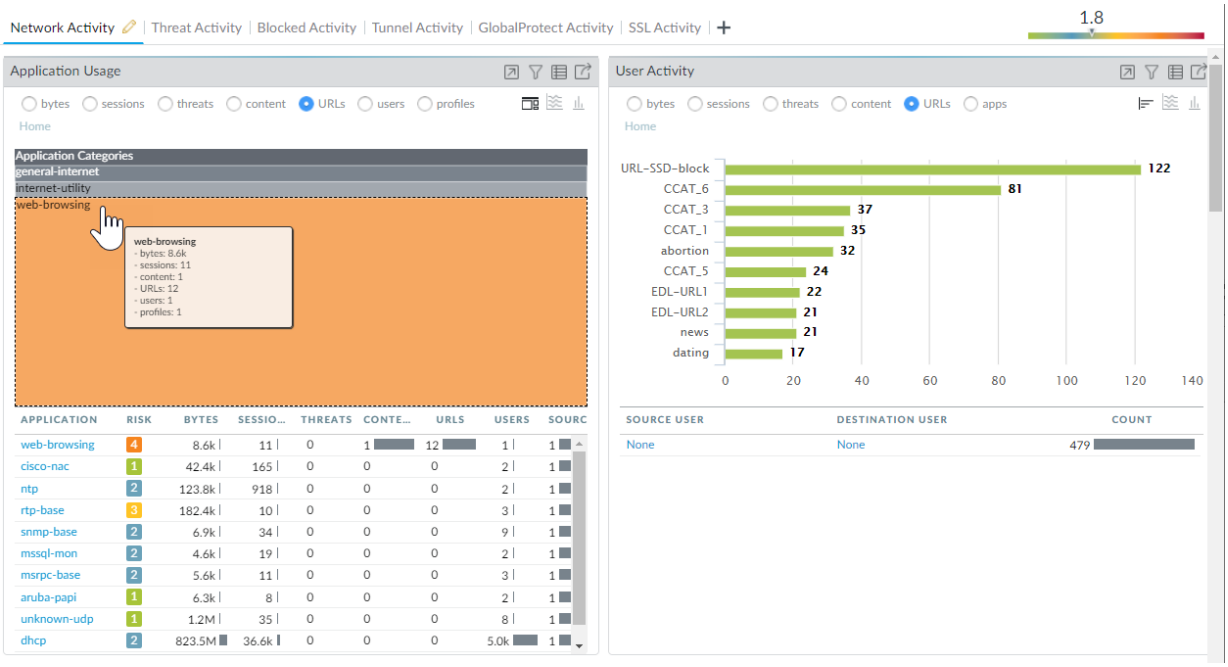
Los siguientes temas describen cómo supervisar la actividad web:

- Supervisión de la actividad web de los usuarios de red
- Visualización del informe de actividad del usuario
- Configuración de informes de filtrado de URL personalizados

Supervisión de la actividad web de los usuarios de red

Puede utilizar el ACC, los informes de filtrado de URL y los logs que se generan en el cortafuegos para supervisar la actividad de los usuarios.

- Para obtener una vista rápida de las categorías más comunes a las que acceden los usuarios de su entorno, seleccione los widgets de **ACC**. La mayoría de widgets de la pestaña **Network Activity (Actividad de red)** le permiten ordenar las URL. Por ejemplo, en el widget Uso de aplicación puede ver que la categoría de red es la categoría a la que más se accede, seguida del túnel cifrado y ssl. También puede ver la lista de **Threat Activity** y **Blocked Activity** ordenada en URL.



Vea los logs y configure las opciones de log:

- En el ACC, puede pasar directamente a los logs ( ) o seleccionar **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**.

  La acción del log para cada entrada depende de la configuración de acceso al sitio que define para la categoría correspondiente:

© 2020 Palo Alto Networks, Inc.

- **Log de alerta:** en este ejemplo, a la categoría computer-and-internet-info (Información de ordenador e internet) se le asignó la acción alert (crear alerta).

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST				outlook-web-online	alert

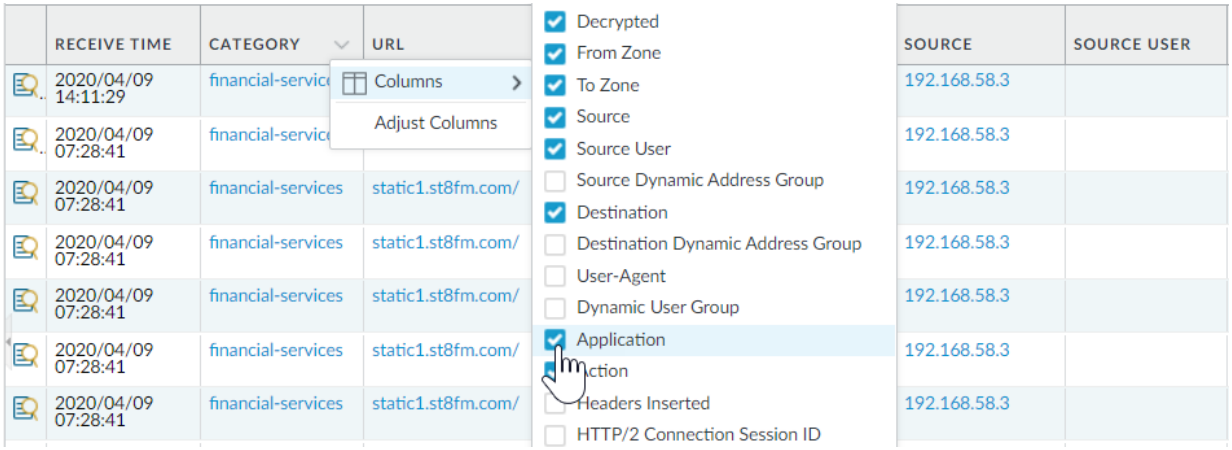
- **Log de bloqueo:** en este ejemplo, a la categoría insufficient-content (contenido insuficiente) se le asignó la acción continue (continuar). Si a la categoría se le hubiese asignado la acción block (bloquear), el log Action (Acción) sería block-url (bloquear URL).

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST				ssl	block-continue

- **Log de alerta en el sitio web cifrado:** en este ejemplo, la categoría es private-ip-addresses (direcciones IP privadas) y la aplicación es web-browsing (navegación web). Además, este log indica que el cortafuegos descifró este tráfico.

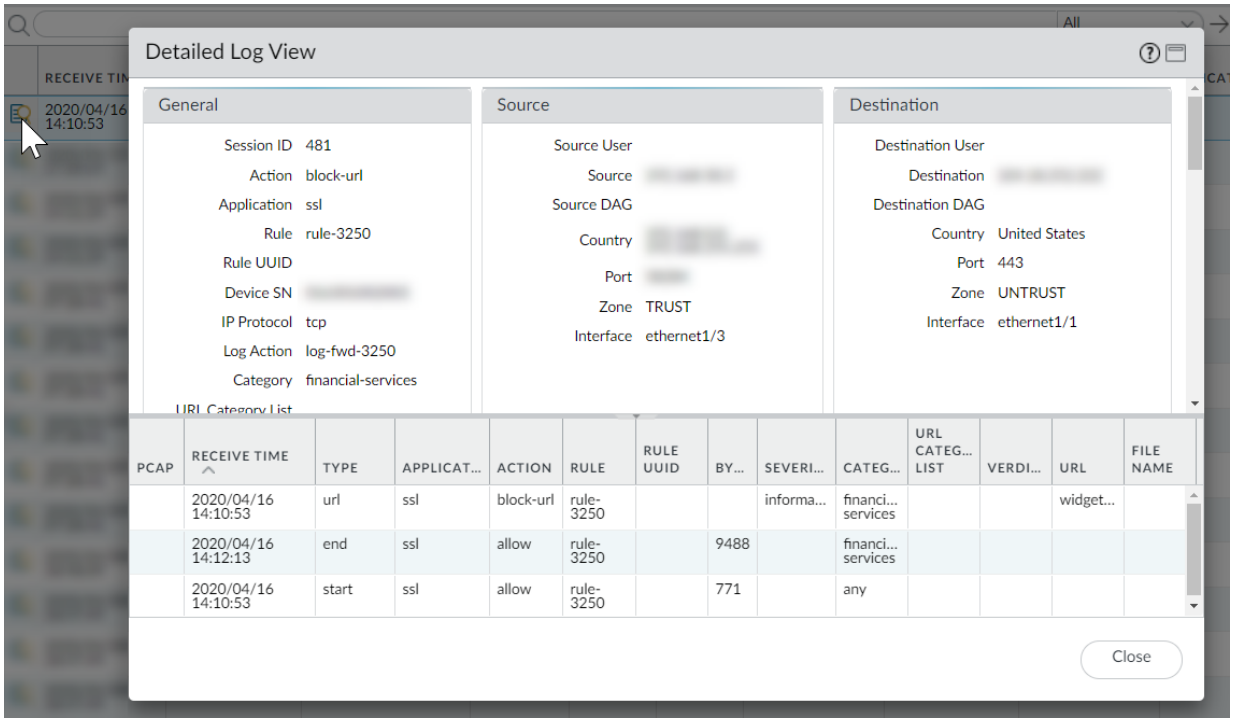
	RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/09 14:11:29	private-ip-addresses	/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3			web-browsing	alert

- También puede añadir otras columnas a su vista de log de filtrado de URL, como las zonas de origen y destino, el tipo de contenido y si se realizó o no una captura de paquetes. Para modificar qué columnas mostrar, haga clic en la flecha hacia abajo en cualquier columna y seleccione el atributo que debe mostrarse.



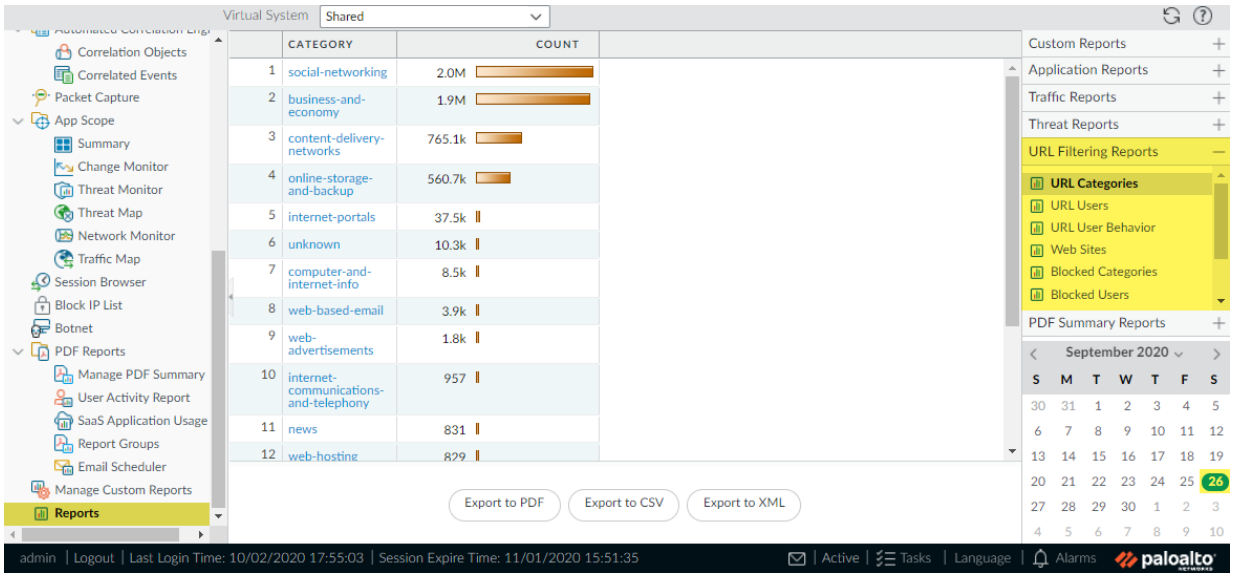
- Para ver la información detallada completa del log y/o solicitar un cambio de categoría para la URL específica a la que se accedió, haga clic en el icono de información detallada del log en la primera columna del log.

© 2020 Palo Alto Networks, Inc.



- Genere informes de filtrado de URL predefinidos en las categorías de URL, los usuarios de URL, los sitios web a los que se accede, las categorías bloqueadas, etc.

  Seleccione **Monitor (Supervisar)** > **Reports (Informes)** y, en la sección **URL Filtering Reports (Informes de filtrado de URL)**, seleccione uno de los informes. Los informes abarcan un período de 24 horas en la fecha del calendario que selecciona. También puede exportar el informe a PDF, CSV o XML.



Visualización del informe de actividad del usuario

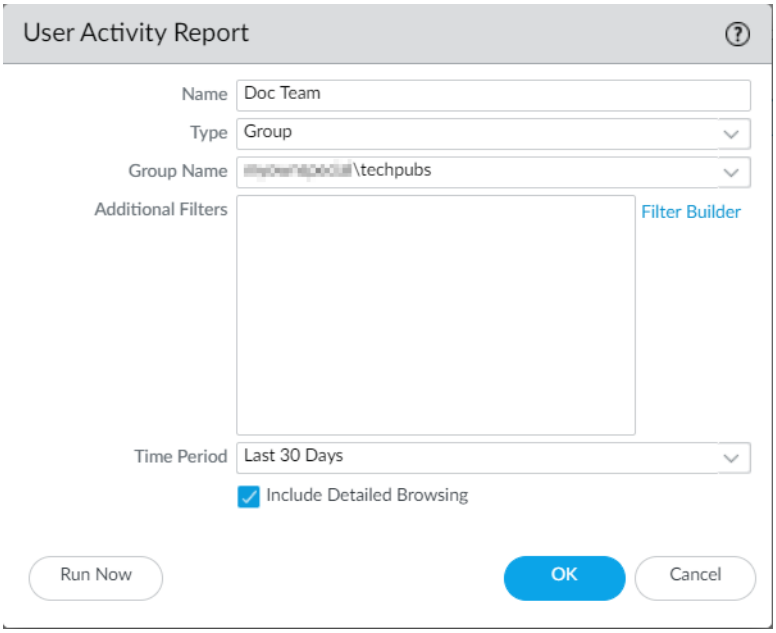
Este informe proporciona un método rápido para visualizar la actividad de un usuario o grupo y también ofrece la opción de visualizar la actividad de tiempo de exploración.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Configure un informe de actividad del usuario

1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **User Activity Report (Informe de actividad del usuario)**.
2. Haga clic en **Add (Añadir)** para añadir un informe e introduzca un nombre para él en **Name (Nombre)**.
3. Seleccione el **Type (Tipo)** de servidor:
   - Seleccione **User (Usuario)** para generar un informe para una persona.
   - Seleccione **Group (Grupo)** para seleccionar un grupo de usuarios.

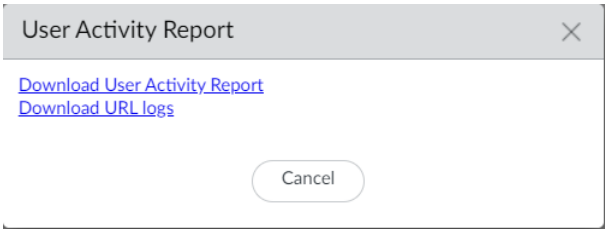
   Debe realizar la Habilitación de User-ID para poder seleccionar nombres de usuario o grupo. Si User-ID no se ha configurado, puede seleccionar el tipo User (Usuario) e introducir la dirección IP del equipo del usuario.
4. Introduzca el **Username/IP Address (Nombre de usuario/dirección IP)** de un informe de usuario o introduzca el nombre de grupo de un informe de grupo de usuarios.
5. Seleccione el periodo de tiempo. Puede seleccionar un período de tiempo existente o seleccionar **Custo (Personalizado)**.
6. Seleccione la casilla de verificación **Include Detailed Browsing (Incluir exploración detallada)** para que se incluya información de exploración en el informe.



STEP 2 | Ejecute el informe.

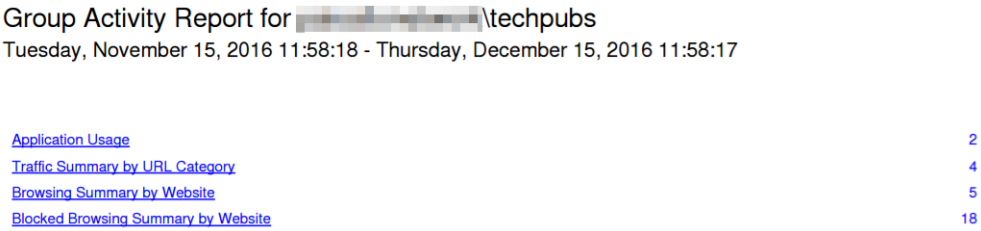
1. Haga clic en **Run now (Ejecutar ahora)**.
2. Cuando el cortafuegos termine de generar el informe, haga clic en uno de los enlaces para descargarlo:
   - Haga clic en **Download User Activity Report (Descargar informe de actividad del usuario)** para descargar una versión en PDF del informe.
   - Haga clic en **Download URL Logs (Descargar logs de URL)** para descargar un archivo CSV de las entradas de log correspondientes.

© 2020 Palo Alto Networks, Inc.

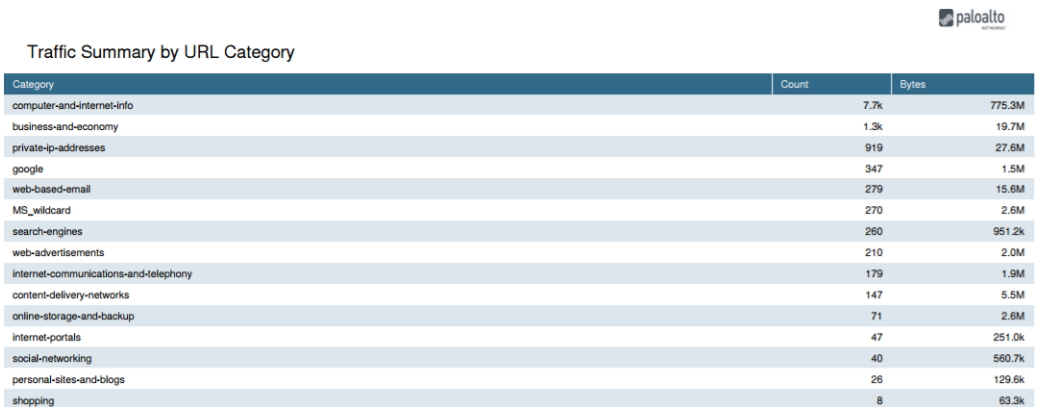


3. Tras descargar el informe, haga clic en **Cancel (Cancelar)**.
4. Si desea guardar la configuración del informe de actividad del usuario para poder ejecutar el mismo informe más tarde, haga clic en **OK (Aceptar)**; de lo contrario, haga clic en **Cancel (Cancelar)**.

STEP 3 | Vea el informe de actividad del usuario abriendo el archivo que descargó. La versión PDF del informe muestra el usuario o el grupo en el que basó el informe, el período de tiempo del informe y un índice:



STEP 4 | Haga clic en un elemento del índice para ver los detalles del informe. Por ejemplo, haga clic en **Traffic Summary by URL Category (Resumen de tráfico por categoría de URL)** para ver estadísticas para el usuario o grupo seleccionado.



Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

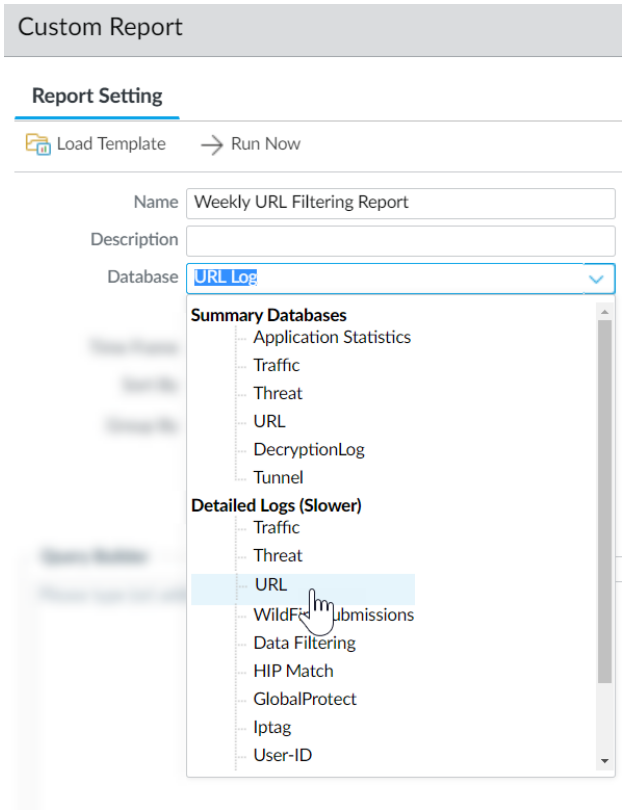
Configuración de informes de filtrado de URL personalizados

Para generar un informe detallado que puede programar para que se ejecute con regularidad, configure un informe personalizado de filtrado de URL. Puede seleccionar cualquier combinación de campos de log de filtrado de URL para realizar el informe.

STEP 1 | Añada un nuevo informe personalizado.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** y **Add (Añadir)** para añadir un informe.
2. Asigne al informe un **Name (Nombre)** único y, opcionalmente, una **Description (Descripción)**.
3. Seleccione la **Database (Base de datos)** que desea utilizar para generar el informe. Para generar un informe detallado con filtrado de URL, seleccione **URL** de la sección Detailed Logs (Logs detallados):

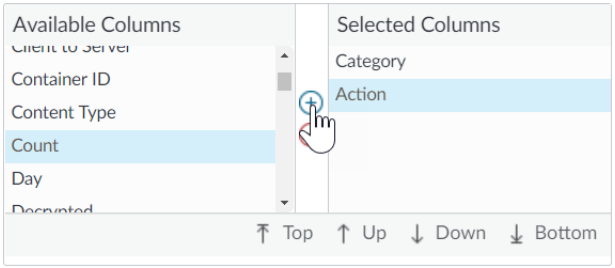
© 2020 Palo Alto Networks, Inc.



STEP 2 | Configure las opciones de informe.

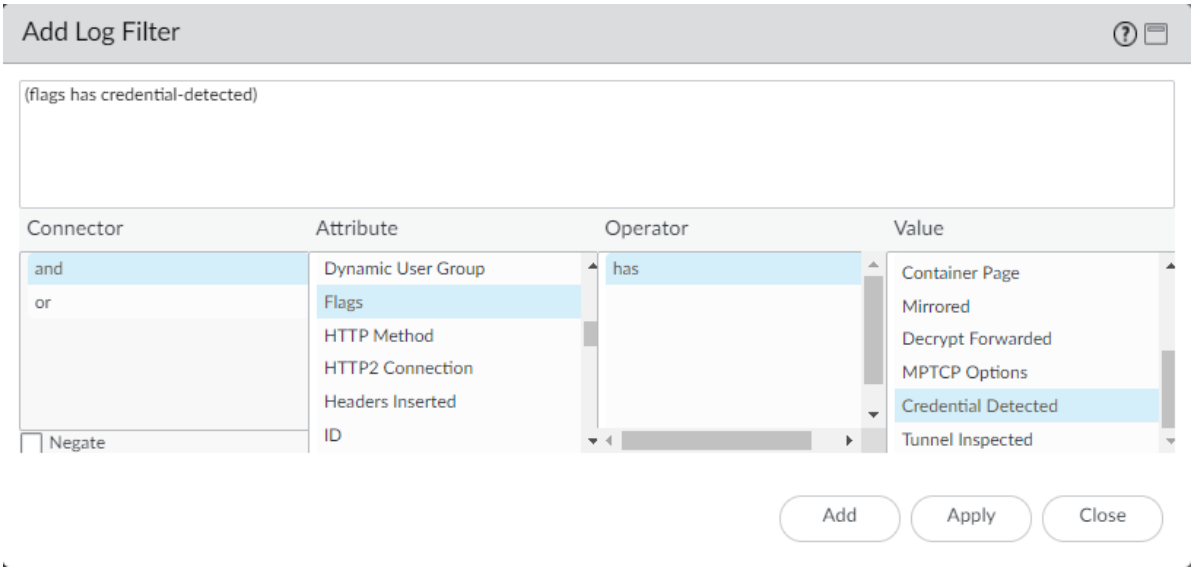
1. Seleccione un **Time Frame (Período de tiempo)** predefinido o seleccione **Custom (Personalizado)**.
2. Seleccione las columnas de logs que desea incluir en el informe de la lista de columnas disponibles y añádalas (⊕) a las columnas seleccionadas. Por ejemplo, para un informe de filtrado de URL, puede seleccionar las siguientes opciones:

   - Acción
   - Categoría de aplicación
   - Category
   - País de destino
   - Source User (Usuario de origen)
   - URL

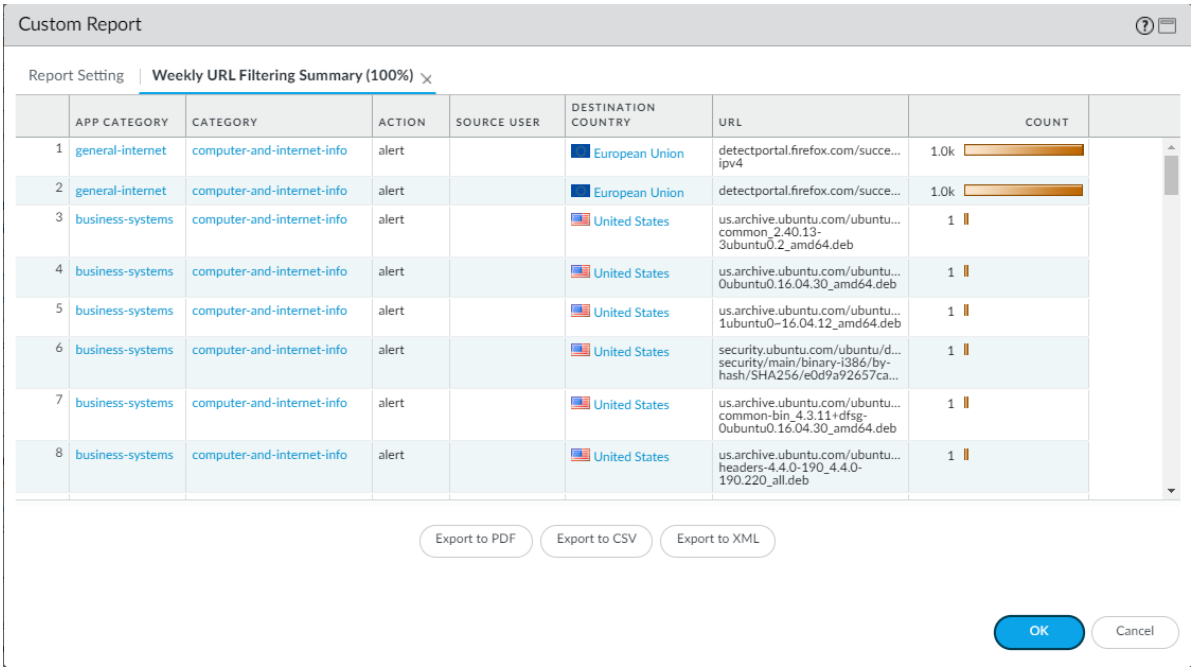


3. Si en el cortafuegos, está habilitada la Prevención de phishing de credenciales, seleccione el atributo **Flags (Marcas)**, el operador **has** y el valor **Credential Detected (Credencial detectada)** para que también se incluyan eventos en el informe que registren cuando un usuario envíe una credencial corporativa válida a un sitio.

© 2020 Palo Alto Networks, Inc.



4. (Opcional) Seleccione una opción **Sort By (Ordenar por)** para configurar el atributo que se utilizará para agregar los detalles del informe. Si no selecciona un atributo según el cual ordenar, el informe devolverá el primer número N de resultados sin ninguna agregación. Seleccione un atributo **Group By (Agrupar por)** que se utilizará como delimitador para agrupar los datos. El siguiente ejemplo muestra un informe con **Group By (Agrupar por)** la **App Category (Categoría de aplicaciones)** y **Sort By (Ordenar por)** el **Count (Conteo)** de los **Top 5 (5 principales)**.



STEP 3 | Ejecute el informe.

1. Haga clic en el icono **Run Now (Ejecutar ahora)** para generar inmediatamente el informe que aparecerá en una nueva pestaña.
2. Cuando complete la revisión del informe, vuelva a la pestaña **Report Setting (Configuración de informes)** y modifique la configuración antes de volver a ejecutar el informe, o continúe al próximo paso para programar un informe.
3. Seleccione la casilla de verificación **Schedule (Programación)** para ejecutar el informe una vez al día. Esto generará un informe diario con información detallada de la actividad web las últimas 24 horas.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 5 | Vea el informe personalizado.

1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
2. Expanda el panel **Custom Reports (Informes personalizados)** en la columna derecha y seleccione el informe que desea ver. El informe más reciente se muestra automáticamente.
3. Para ver el informe de una fecha anterior, seleccione la fecha del calendario. También puede exportar el informe a PDF, CSV o XML.

© 2020 Palo Alto Networks, Inc.

Registro solo de las páginas que visita un usuario

Una página contenedora es la página principal a la que accede un usuario al visitar un sitio web, pero se pueden cargar páginas adicionales dentro de la página principal. Si se habilita la opción **Página de contenedor de log únicamente** en el perfil de filtrado de URL (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**), solamente se registrará la página de contenedor principal y no las páginas posteriores que puedan cargarse en la página de contenedor. Dado que el filtrado de URL potencialmente puede generar muchas entradas de log, puede que quiera activar esta opción; de este modo, las entradas de log solamente incluirán esos URI cuando el nombre de archivo de la página solicitada coincida con los tipos MIME específicos. El conjunto predeterminado incluye los siguientes tipos MIME:

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml



Si ha habilitado la opción Log container page only (Registrar solo página de contenedor), puede que no siempre haya una entrada de log de URL correlacionada para amenazas detectadas por antivirus o protección frente a vulnerabilidades.

© 2020 Palo Alto Networks, Inc.

Creación de una categoría de URL personalizada

Puede crear un objeto personalizado de URL Filtering para especificar excepciones a la aplicación de las categorías de URL y para crear categorías personalizadas basadas en varias categorías de URL:

- **Defina excepciones a la aplicación de categorías de URL**: confeccione una lista personalizada de las URL que desea emplear como criterios de coincidencia de una regla de la política de seguridad. Se trata de un buen método para especificar excepciones a las categorías de URL si desea aplicar a ciertas URL medidas distintas de las que corresponden a su categoría.
- **Defina categorías de URL personalizadas basadas en varias categorías de PAN-DB**: puede limitar la aplicación a los sitios web que coincidan con un conjunto de categorías. Las páginas o los sitios web deben coincidir con *todas* las categorías definidas como parte de la categoría personalizada.

Siga estos pasos para crear una categoría de URL personalizada y defina cómo quiere que la aplique el cortafuegos:

STEP 1 | Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)**.

STEP 2 | Añada o modifique una categoría de URL personalizada y asígnele un nombre descriptivo en **Name (Nombre)**.

STEP 3 | Configure **Type (Tipo)** en **URL List (Lista de URL)** o en **Category Match (Coincidencia con categoría)**:

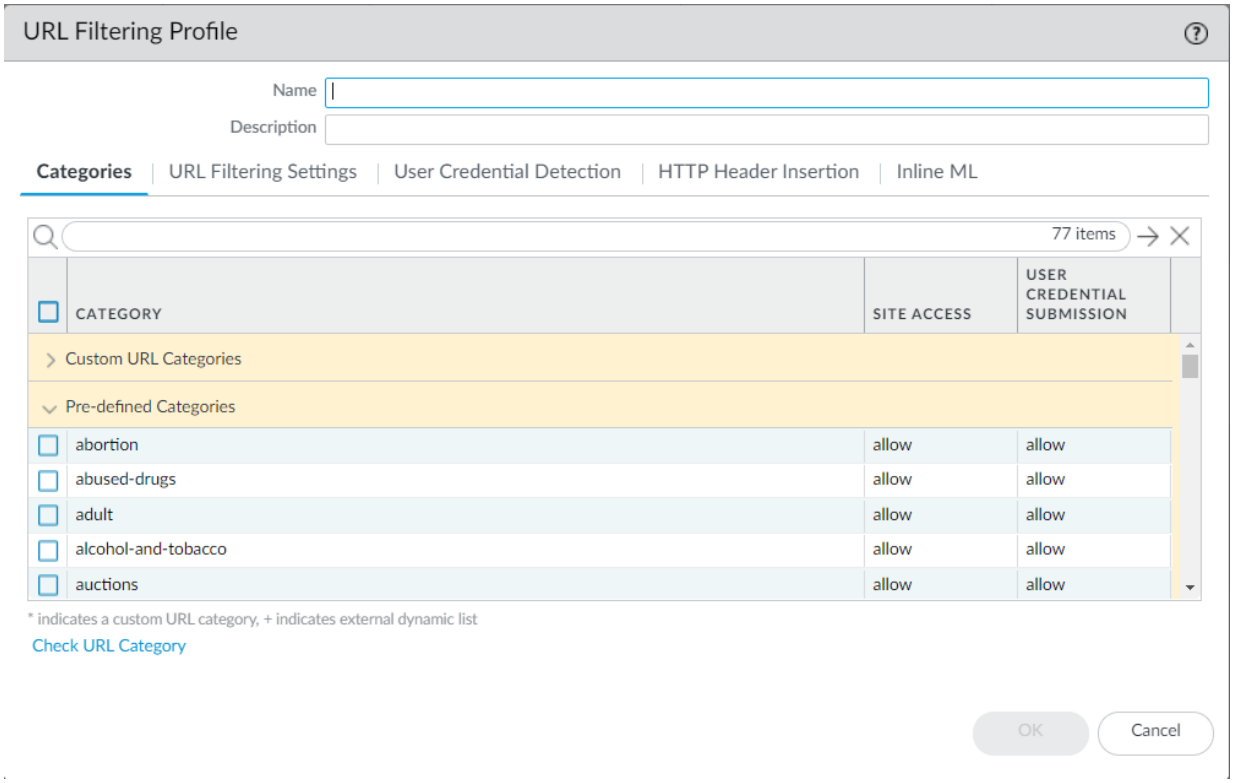
- **URL List (Lista de URL)**: añada las URL a las que desea aplicar medidas distintas de las que corresponden a su categoría. Use este tipo de lista para definir las excepciones a la aplicación de las categorías de URL o para definir la lista de URL que pertenecen a una categoría personalizada. Para obtener información sobre cómo rellenar esta lista e instrucciones para usar los comodines, consulte Excepciones de la categoría de URL.
- **Category Match (Coincidencia con categoría)**: especifique la aplicación a los sitios web que coincidan con un conjunto de categorías. Las páginas o los sitios web deben coincidir con *todas* las categorías definidas como parte de la categoría personalizada.

STEP 4 | Haga clic en **OK (Aceptar)** para guardar la categoría de URL personalizada.

STEP 5 | Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.

La nueva categoría personalizada figura en la lista del menú desplegable **Custom URL Categories (Categorías de URL personalizadas)**:

© 2020 Palo Alto Networks, Inc.



STEP 6 | Decida las medidas que desea aplicar a la categoría de URL personalizada en **Site Access (Acceso a sitios)** y **User Credential Submission (Envío de credenciales de usuarios)**. Para controlar los sitios a los que los usuarios pueden enviar credenciales corporativas, consulte Prevención de phishing de credenciales.

STEP 7 | Vincule el perfil de URL Filtering a una regla de la política de seguridad para aplicarlo al tráfico que coincida con ella.

Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Actions (Acciones)** y especifique la regla de la política de seguridad que se debe aplicar al tráfico en función del perfil de filtrado de URL que acaba de actualizar. No olvide hacer clic en **Commit (Confirmar)** para aceptar los cambios.

Si emplea las categorías de URL personalizadas como criterios de coincidencia con la política de seguridad, no hace falta que defina cómo se debe aplicar como parte del perfil de URL Filtering. Tras configurar la categoría personalizada, desplácese directamente a la regla de la política de seguridad a la que desea añadirla con Policies (Políticas) > Security (Seguridad). Seleccione Service/URL Category (Servicio/Categoría de URL) para usar la categoría de URL personalizada como criterio de coincidencia con la regla.

© 2020 Palo Alto Networks, Inc.

Excepciones de la categoría de URL

Puede excluir sitios web específicos de la aplicación de la categoría de URL, y garantizar que los sitios web se bloqueen o permitan independientemente de la categoría de URL asociada. Por ejemplo, puede bloquear una categoría de URL, pero permitir ciertos sitios de una categoría. Para crear estos tipos de excepciones a la aplicación de categorías de URL:

- Añada las direcciones IP o las URL de los sitios que desea bloquear o permitir expresamente. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** para crear una lista, tal como se explica en Creación de una categoría de URL personalizada.
- Uso de una lista dinámica externa en un perfil de filtrado de URL El beneficio de utilizar listas dinámicas externas para especificar los sitios a los que desea aplicar la acción de manera separada de sus categorías URL es que puede actualizar la lista dinámica externa sin realizar un cambio en la configuración ni confirmar los cambios en el cortafuegos.

Las siguientes pautas describen cómo rellenar la lista de bloqueados y la lista de permitidos para las categorías URL o un archivo de texto que utiliza como origen de una lista dinámica externa de URL:

- Pautas básicas para las listas de excepción de categoría de URL
- Pautas de comodines para las listas de excepción de categoría de URL
- Lista de excepción de categoría de URL: ejemplos de comodines

Pautas básicas para las listas de excepción de categoría de URL

- Introduzca las direcciones IP o URL de los sitios web que desea aplicar por separado de la categoría de URL asociada.
- Las entradas de la lista deben coincidir exactamente, y no distinguen entre mayúsculas y minúsculas.
- Introduzca la cadena que coincide exactamente con el sitio web (y, si es posible, con el subdominio concreto) en el que desea controlar el acceso. Utilice comodines para permitir que las entradas coincidan con varios subdominios del sitio web. Si desea obtener información detallada sobre la utilización de caracteres comodines, revise Pautas de comodines para las listas de excepción de categoría de URL.
- Omita `http` y `https` en las entradas de URL.
- Las entradas de URL pueden tener hasta 255 caracteres de longitud.

Pautas de comodines para las listas de excepción de categoría de URL

Puede utilizar comodines en las listas de excepción de categoría de URL para configurar con facilidad una entrada única que coincida con los subdominios y páginas de varios sitios web, sin especificar los subdominios o páginas exactos.

Respete estas pautas cuando cree entradas con comodines:

- Los siguientes caracteres se consideran separadores de token: . / ? & = ; +

  Cada cadena separada con uno o dos de estos caracteres es un token. Utilice caracteres comodines como marcadores de posición de token, que indican que un token específico puede contener cualquier valor.
- En lugar de un token, puede utilizar un asterisco (*) o un símbolo de intercalación (^) para indicar un valor de comodín.
- Los caracteres de comodín deben ser el único carácter en un token; sin embargo, una entrada puede contener varios comodines.

© 2020 Palo Alto Networks, Inc.

Cómo usar los comodines (asteriscos (*) y símbolos de intercalación (^))

*	Úselo para indicar uno o más subdominios variables. Si usa *, la entrada coincidirá con cualquier subdominio adicional, ya sea al principio o al final de la URL. Utilice una barra diagonal al final de la entrada si no desea que coincida ningún subdominio adicional más allá de ese punto. Ejemplo: • **`*.paloaltonetworks.com`** coincide con www.paloaltonetworks.com and www.paloaltonetworks.com.uk. • **`*.paloaltonetworks.com/`** coincide con www.paloaltonetworks.com, pero no con www.paloaltonetworks.com.uk.
^	Utilice esto para indicar un subdominio variable. Ejemplo: **`mail.^.com`** coincide con mail.company.com, pero no con mail.company.sso.com.

No cree una entrada con comodines de asterisco (*) consecutivos o entradas con más de nueve comodines de símbolo de intercalación (^) consecutivos; este tipo de entradas afectan negativamente al rendimiento del cortafuegos.

*Por ejemplo, no añada una entrada como **`mail.*.*.com`**; en cambio, según el rango de sitios web para el que desee controlar el acceso, introduzca **`mail.*.com`** o **`mail.^.^.com`**. Una entrada como **`mail.*.com`** coincide con un número mayor de sitios que **`mail.^.^.com`**; **`mail.*.com`** coincide con los sitios con cualquier número de subdominios y **`mail.^.^.com`** coincide con los sitios con exactamente dos subdominios.*

Lista de excepción de categoría de URL: ejemplos de comodines

En la tabla siguiente se enumeran ejemplos de entradas de las listas de excepciones de URL que utilizan comodines y ejemplos de los sitios con los que coinciden dichas entradas.

Entrada de la lista de excepción de URL	Sitios que coinciden
Conjunto de ejemplos 1	
*.company.com	eng.tools.company.com support.tools.company.com tools.company.com docs.company.com
^.company.com	tools.company.com docs.company.com

© 2020 Palo Alto Networks, Inc.

Entrada de la lista de excepción de URL	Sitios que coinciden
^.^.company.com	eng.tools.company.com support.tools.company.com
Conjunto de ejemplos 2	
mail.google.*	mail.google.com mail.google.co.uk
mail.google.^	mail.google.com
mail.google.^.^	mail.google.co.uk

© 2020 Palo Alto Networks, Inc.

Uso de una lista dinámica externa en un perfil de filtro de URL

Para proteger su red de amenazas y malware recientemente detectados, puede usar listas dinámicas externas en los perfiles de filtrado de URL. Las listas dinámicas externas le permiten actualizar la lista sin un cambio de configuración o confirmación en el cortafuegos. Una lista dinámica externa es un archivo de texto que está alojado en un servidor web externo. Puede usar esta lista para importar URL y aplicar la política en estas URL. Cuando se actualiza la lista en el servidor web, el cortafuegos recupera los cambios y aplica la política a la lista modificada sin necesidad de una confirmación en el cortafuegos.

El cortafuegos importa dinámicamente la lista en el intervalo configurado y aplica la política para las URL (se ignorarán las direcciones IP o los dominios) de la lista. Para ver directrices sobre el formato de las URL, consulte Excepciones de la categoría de URL.

Para obtener más información, consulte Lista dinámica externa.

STEP 1 | Configuración del cortafuegos para acceder a una lista dinámica externa.

- Asegúrese de que la lista no incluya direcciones IP o nombres de dominio el cortafuegos omite las entradas que no sean URL.
- Compruebe el formato de la lista (ver).
- Seleccione **URL List (Lista de URL)** de la lista desplegable Type (Tipo).

STEP 2 | Use la lista dinámica externa en un perfil de filtro de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado URL)**.
2. Seleccione **Add (Añadir)** para añadir o modifique un perfil de filtro de URL existente.
3. Asigne un nombre al perfil en **Name (Nombre)** y en la pestaña **Categories (Categorías)**, seleccione la lista dinámica externa en la lista de categorías.
4. Haga clic en Action (Acción) para seleccionar una acción más detallada para las URL en la lista dinámica externa.

   Si una URL que está incluida en una lista dinámica externa también se incluye en una categoría de URL personalizada o en las Listas de bloqueados y permitidos, la acción especificada en la categoría personalizada o la lista de bloqueados y permitidos tendrá prioridad sobre la lista dinámica externa.
5. Haga clic en **OK (Aceptar)**.
6. Adjunte el perfil de filtrado de URL a una regla de política de seguridad.
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
   2. Seleccione la pestaña **Actions (Acciones)** y, en la sección Profile Setting (Ajuste de perfil), seleccione el nuevo perfil en el menú desplegable **URL Filtering (Filtrado de URL)**.
   3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 3 | Compruebe que la acción de política esté forzada.

1. Realice la Visualización de las entradas de la lista dinámica externa para la lista de URL e intente acceder a la URL desde la lista.
2. Verifique que la acción que definió se haya aplicado en el navegador.
3. Para supervisar la actividad del cortafuegos:

© 2020 Palo Alto Networks, Inc.

1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de la red y la actividad bloqueada para la URL a la cual accedió.
2. Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)** para acceder a la vista detallada del log.

STEP 4 | Verifique si las entradas en la lista dinámica externa se ignoraron u omitieron.

En una lista de tipo URL, el cortafuegos omite las entradas que no son URL como no válidas e ignora las entradas que superan el límite máximo del modelo de cortafuegos.



Para comprobar si alcanzó el límite de un tipo de lista dinámica externa, seleccione Objects (Objetos) > External Dynamic Lists (Listas dinámicas externas) y haga clic en List Capacities (Capacidades de la lista).

Use el siguiente comando CLI en un cortafuegos para revisar los detalles de una lista.

```
request system external-list show type url name <list_name>
```

Por ejemplo:

```
request system external-list show type url name My_URL_List
vsys5/My_URL_List:
Next update at: Tue Jan 3 14:00:00 2017
Source: http://example.com/My_URL_List.txt
Referenced: Yes
Valid: Yes
Auth-Valid: Yes

Total valid entries: 3
Total invalid entries: 0
Valid urls:
www.URL1.com
www.URL2.com
www.URL3.com
```


© 2020 Palo Alto Networks, Inc.

Habilitación del acceso a determinados sitios mediante contraseña

En determinados casos, puede haber categorías de URL que desee bloquear, pero permite el acceso a determinados usuarios ocasionalmente. En este caso, debe establecer la acción de la categoría en **override (cancelar)** y establecer una contraseña de cancelación de administrador de URL en la configuración de Content-ID del cortafuegos. Cuando los usuarios intenten buscar la categoría, se les pedirá que especifiquen la contraseña de cancelación para poder acceder al sitio. Use el siguiente procedimiento para configurar la cancelación de administrador de URL:

STEP 1 | Establezca la contraseña de cancelación de administrador de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.
2. En la sección **Cancelación de administrador de URL**, haga clic en **Añadir**.
3. En el campo **Ubicación**, seleccione el sistema virtual al que se aplica esta contraseña.
4. Especifique el valor de **Contraseña** y seleccione **Confirmar contraseña**.
5. Seleccione un **SSL/TLS Service Profile**. El perfil especifica el certificado que el cortafuegos presenta al usuario si el sitio con la cancelación es un sitio HTTPS. Para obtener más información, consulte Configuración de un perfil de servicio SSL/TLS.
6. Seleccione el **Modo** para indicar al usuario que especifique la contraseña:
   - **Transparent (Transparente)**: el cortafuegos intercepta el tráfico del navegador destinado al sitio de una categoría de URL que ha configurado para la sustitución, se hace pasar por la URL de destino original y emite el mensaje HTTP 302 para solicitar la contraseña, que se aplica a cada sistema virtual.

     El explorador del cliente mostrará errores de certificado si no confía en el certificado.

   - **Redirect (Redirigir)**: el cortafuegos intercepta el tráfico HTTP o HTTPS para una categoría de URL establecida para la cancelación y redirige la solicitud a una interfaz de capa 3 en el cortafuegos mediante un redireccionamiento HTTP 302 para solicitar la contraseña de cancelación. Si selecciona esta opción, debe especificar la **Dirección** (dirección IP o nombre de host DNS) a la que se redirige el tráfico.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Establezca un período de cancelación personalizado.

1. Edite la sección Filtrado de URL.
2. Para cambiar el tiempo durante el que los usuarios pueden examinar un sitio en una categoría para la que han especificado correctamente la contraseña de cancelación, especifique un valor nuevo en el campo **URL Admin Override Timeout (Tiempo de espera de cancelación de administrador de URL)**. De forma predeterminada, los usuarios pueden acceder a los sitios de la categoría durante 15 minutos sin necesidad de volver a especificar la contraseña.
3. Para cambiar el período de tiempo durante el que los usuarios están bloqueados y no pueden acceder a un sitio configurado para la cancelación después de tres intentos fallidos de introducción de la contraseña de cancelación, especifique un valor nuevo en el campo **Tiempo de espera de bloqueo de administrador de URL**. De forma predeterminada, los usuarios permanecen bloqueados durante 30 minutos.
4. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 3 | (Solo en el modo Redirigir) Cree una interfaz de capa 3 a la que redirigir las solicitudes web para los sitios en una categoría configurada para la cancelación.

1. Cree un perfil de gestión para habilitar la interfaz de modo que muestre la página de respuesta de continuación y cancelación de filtrado de URL:
    1. Seleccione **Network (Red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
    2. Introduzca un **Nombre** para el perfil, seleccione **Páginas de respuesta** y, a continuación, haga clic en **Aceptar**.
2. Cree la interfaz de capa 3. Asegúrese de adjuntar el perfil de gestión que acaba de crear (en la pestaña **Advanced [Avanzado]** > **Other Info [Otra información]** del cuadro de diálogo Ethernet Interface [Interfaz Ethernet]).

STEP 4 | (Solo en el modo Redirigir) Para redirigir a los usuarios de forma transparente sin mostrar errores de certificado, instale un certificado que coincida con la dirección IP de la interfaz a la que va a redirigir las solicitudes web para un sitio en una categoría de URL configurada para la cancelación. Puede generar un certificado autofirmado o importar un certificado firmado por una CA externa.

Para usar un certificado autofirmado, primero debe crear un certificado de CA raíz y, a continuación, usar esa CA para firmar el certificado que usará para la cancelación de administrador de URL del modo siguiente:

1. Para crear un certificado de CA raíz, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y luego haga clic en **Generate (Generar)**. Introduzca un **Nombre de certificado**, como RootCA. No seleccione ningún valor en el campo **Firmado por** (esto es lo que indica que está autofirmado). Asegúrese de seleccionar la casilla de verificación **Autoridad del certificado** y, a continuación, haga clic en **Generar** para generar el certificado.
2. Para crear el certificado que se usará para la cancelación de administrador de URL, haga clic en **Generar**. Especifique el **Nombre del certificado** y el nombre de host DNS o la dirección IP de la interfaz como el **Nombre común**. En el campo **Signed By (Firmado por)**, seleccione la CA que creó en el paso anterior. Añada un atributo de dirección IP y especifique la dirección IP de la interfaz de capa 3 a la que redirigirá las solicitudes web para las categorías de URL con la acción de cancelación.
3. Seleccione **Generar** el certificado.
4. Para configurar clientes para que confíen en el certificado, seleccione el certificado de CA en la pestaña **Device Certificates (Certificados de dispositivos)** y haga clic en **Export (Exportar)**. A continuación deberá importar el certificado como una CA raíz de confianza en todos los exploradores de cliente, ya sea configurando manualmente el explorador o añadiendo el certificado a las raíces de confianza en un objeto de directiva de grupo (GPO) de Active Directory.

STEP 5 | Especifique qué categorías de URL requieren una contraseña de cancelación para permitir el acceso.

1. Seleccione **Objects (Objetos)** > **URL Filtering (Filtrado URL)** y seleccione un perfil de filtrado de URL existente o seleccione **Add (Añadir)** para añadir uno nuevo.
2. En la pestaña **Categorías**, establezca la acción en **Cancelar** para cada categoría que requiera una contraseña.
3. Complete las secciones restantes del perfil de filtrado de URL y, a continuación, haga clic en **Aceptar** para guardar el perfil.

STEP 6 | Aplique el perfil de filtrado de URL a las reglas de política de seguridad que permiten el acceso a los sitios que requieren la cancelación de la contraseña para el acceso.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la política de seguridad adecuada para modificarla.

© 2020 Palo Alto Networks, Inc.

2. Seleccione la pestaña **Acciones** y, en la sección **Ajuste de perfil**, haga clic en el menú desplegable **Filtrado de URL** y seleccione el perfil.
3. Haga clic en **OK (Aceptar)** para guardar.

STEP 7 | Guarde la configuración.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Prevención de phishing de credenciales

Los sitios de phishing son sitios que los atacantes disfrazan de sitios web legítimos con el objetivo de robar información del usuario, especialmente, las credenciales que proporcionan acceso a su red. Cuando un correo electrónico de phishing entra en una red, solo se necesita que un usuario haga clic en el enlace e introduzca las credenciales para que se produzca una infracción. Puede detectar y evitar los ataques de phishing en curso, y evitar el robo de credenciales, controlando los sitios que pueden recibir credenciales corporativas basadas en la categoría de URL del sitio de los usuarios. Esto le permite evitar que los usuarios envíen credenciales a sitios no fiables, además de permitir a los usuarios continuar enviando credenciales a sitios corporativos y sancionados.

La prevención de phishing de credenciales funciona mediante el análisis de los envíos de nombres de usuario y contraseñas a sitios web, y la comparación de esos envíos con las credenciales corporativas válidas. Puede seleccionar los sitios web en los que desea permitir o bloquear la recepción de credenciales corporativas en función de la categoría de URL del sitio web. Cuando el cortafuegos detecta que un usuario intenta enviar credenciales a un sitio en una categoría que ha restringido, se muestra una página de respuesta de bloqueo que evita que el usuario envíe credenciales, o se presenta una página para continuar que advierte a los usuarios contra el envío de credenciales a sitios clasificados en determinadas categorías de URL, pero aún les permite continuar el envío de credenciales. Puede personalizar las páginas de bloqueo para proporcionar información a los usuarios sobre la reutilización de las credenciales corporativas, incluso en sitios legítimos sin phishing.

Para habilitar la prevención de phishing de credenciales, debe configurar User-ID para que detecte cuando los usuarios envíen credenciales corporativas válidas a un sitio (en lugar de credenciales personales) y el Filtrado de URL para que especifique las categorías de URL en las que desea evitar que los usuarios introduzcan sus credenciales corporativas. Los siguientes temas describen los diferentes métodos que puede utilizar para detectar envíos de credenciales y brindar instrucciones para configurar la protección contra phishing de credenciales.

- Métodos para comprobar los envíos de credenciales corporativas
- Configuración de la detección de credenciales con el agente de ID de usuario basado en Windows
- Configuración de la prevención de suplantación de identidad de credenciales

Métodos para comprobar los envíos de credenciales corporativas

Antes de realizar la Configuración de la prevención de phishing de credenciales, decida el método que desea que utilice el cortafuegos para comprobar si las credenciales que se enviaron a una página web son credenciales corporativas válidas.

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
Asignación de grupos	Configuración de asignación de grupos en el cortafuegos	El cortafuegos realiza comprobaciones para determinar si el nombre de usuario que un usuario envía a un sitio restringido coincide con cualquier nombre de usuario corporativo válido. Para ello, el cortafuegos compara el nombre de usuario enviado a la lista de nombres de usuario en su tabla de asignación de usuarios a grupos para detectar cuándo los usuarios envían nombres de usuario corporativos a sitios en una categoría restringida.

© 2020 Palo Alto Networks, Inc.

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
		Este método sólo comprueba envíos de nombre de usuario corporativo basándose en la pertenencia a un grupo LDAP, lo que hace que sea sencillo de configurar, pero más propenso a falsos positivos.
Asignación de direcciones IP a usuarios	Asignaciones de direcciones IP a nombres de usuario identificadas mediante la asignación de usuarios, GlobalProtect o la política de autenticación y portal de autenticación.	El cortafuegos realiza una comprobación para determinar si el nombre de usuario que un usuario envía a un sitio restringido se asigna a la dirección IP del nombre de usuario de inicio de sesión. Para ello, el cortafuegos compara la dirección IP del nombre de usuario de inicio de sesión y el nombre de usuario enviado a un sitio web con la tabla de asignación de direcciones IP a usuarios para detectar cuando los usuarios envían nombres de usuario corporativos a sitios en una categoría restringida. Dado que este método busca una coincidencia entre la dirección IP de nombre de usuario de inicio de sesión asociado a la sesión y la tabla de asignación de dirección IP a nombre de usuario, se trata de un método eficaz para la detección de envíos de nombres de usuario corporativos, pero no detecta el envío de contraseñas corporativas. Si desea detectar el envío de nombres de usuario y contraseñas corporativas, debe utilizar el método de filtro de credenciales de dominio.
Filtro de credenciales de dominio	Agente de User-ID de Windows configurado con el elemento adicional del servicio de credenciales de User-ID - Y - Asignaciones de direcciones IP a nombres de usuario identificadas mediante la asignación de usuarios, GlobalProtect o la política de autenticación y portal de autenticación.	El cortafuegos realiza la comprobación para determinar si el nombre de usuario y la contraseña que envía un usuario coinciden con el nombre de usuario y la contraseña corporativos del mismo usuario. Para ello, el cortafuegos debe ser capaz de encontrar una coincidencia entre los envíos de credenciales con nombres de usuario y contraseñas corporativos válidos, y comprobar si el nombre de usuario enviado se correlaciona con la dirección IP del nombre de usuario de inicio de sesión de la siguiente manera: • **Para detectar nombres de usuario y contraseñas corporativos:** el cortafuegos recupera una máscara de bits segura, denominada *filtro bloom*, de un agente de User-ID de Windows con el elemento adicional de credenciales de User-ID. Este servicio adicional analiza su directorio en busca de nombres de usuario y contraseñas hash, y los descompone en una máscara de bits segura (el filtro bloom) y la envía al agente de User-ID de Windows. El cortafuegos recupera el filtro boom del agente de User-ID de Windows en intervalos regulares. Si detecta que un usuario envía credenciales a una categoría restringida, descompone el filtro bloom, y busca un nombre de usuario y contraseña hash que coincida. El

© 2020 Palo Alto Networks, Inc.

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
		cortafuegos solo puede conectarse a un agente de User-ID de Windows que ejecuta el elemento adicional del servicio de credenciales de User-ID. • **Para comprobar que las credenciales pertenezcan al nombre de usuario de inicio de sesión:** el cortafuegos busca una asignación entre la dirección IP del nombre de usuario de inicio de sesión y el nombre de usuario detectado en su tabla de asignación de direcciones IP a nombres de usuario. Para obtener más información sobre cómo funciona el método de credenciales de dominio y los requisitos para habilitar este tipo de detección, consulte Configuración de detección de credenciales con el agente de User-ID basado en Windows.

Configuración de la detección de credenciales con el agente de User-ID de Windows

El filtro de credencial de dominio permite que el cortafueogs detecte contraseñas enviadas a las páginas web. Este método de detección de credenciales requiere que el agente de User-ID de Windows y el servicio de credencial de User-ID, un complemento del agente de User-ID, estén instalados en un *controlador de dominio de solo lectura (Read-Only Domain Controller, RODC)*.

El método de detección Domain Credential Filter (Filtro de credenciales de dominio) solo se admite con el agente de User-ID de Windows. No puede configurarlo con el agente de User-ID integrado en PAN-OS.

Un RODC es un servidor Microsoft Windows que mantiene una copia de solo lectura de una base de datos de Active Directory que aloja un controlador de dominio. Cuando el controlador de dominio está ubicado en una sede corporativa; por ejemplo, los RODC pueden implementarse en ubicaciones de red remotas para proporcionar servicios de autenticación. La instalación del agente de ID de usuario en un RODC puede ser útil por algunos motivos: el acceso al directorio de controlador de dominio no es necesario para habilitar la detección de credenciales y usted puede admitir la detección de credenciales para un conjunto limitado u objetivo de usuarios. Debido a que el directorio que el RODC aloja es de solo lectura, el contenido del directorio permanece seguro en el controlador de dominio.

Como debe instalar el agente de User-ID de Windows en el RODC para garantizar la detección de credenciales, se recomienda implementar un agente distinto para este fin. No use el agente de User-ID que se instaló en el RODC para asignar direcciones IP a usuarios.

Después de instalar el agente de ID de usuario en un RODC, el servicio de credencial de ID de usuario se ejecuta en segundo plano y escanea el directorio para encontrar los hashes de nombres de usuario y contraseñas de miembros de grupo que se incluyen en la lista de la política de replicación de contraseña de RODC: puede definir quién desea que esté en la lista. El servicio de credencial de ID de usuario toma los hashes de nombre de usuario y contraseña recopilados y deconstruye los datos en un tipo de

© 2020 Palo Alto Networks, Inc.

máscara de bits denominada *filtro de eclosión*. Los filtros de eclosión son estructuras de datos compactos que proporcionan un método seguro para comprobar si un elemento (un hash de nombre de usuario o contraseña) es miembro de un conjunto de elementos (los conjuntos de credenciales que aprobó para la replicación en el RODC). El servicio de credenciales de User-ID reenvía el filtro de eclosión al agente de User-ID de Windows; el cortafuegos recupera el último filtro de eclosión del agente de User-ID a intervalos periódicos y lo utiliza para detectar envíos de hashes de nombres de usuario y contraseñas. Según su configuración, el cortafuegos luego bloquea, alerta o permite los envíos de contraseña válidos a páginas web, o muestra una página de respuesta a los usuarios que les advierte los peligros de suplantación de identidad, pero les permite continuar con el envío.

A través de este proceso, el agente de ID de usuario no almacena ni expone hashes de contraseña, ni reenvía hashes de contraseña al cortafuegos. Una vez que los hashes de contraseña se deconstruyen en un filtro de eclosión, no hay manera de recuperarlos.

STEP 1 | Configuración de la asignación de usuarios mediante el agente de ID de usuario de Windows.

> *Para habilitar la detección de credenciales, debe instalar el agente de User-ID de Windows en un RODC. Consulte la* Matriz de compatibilidad *para ver una lista de servidores compatibles. Instale un agente de User-ID distinto para esto.*

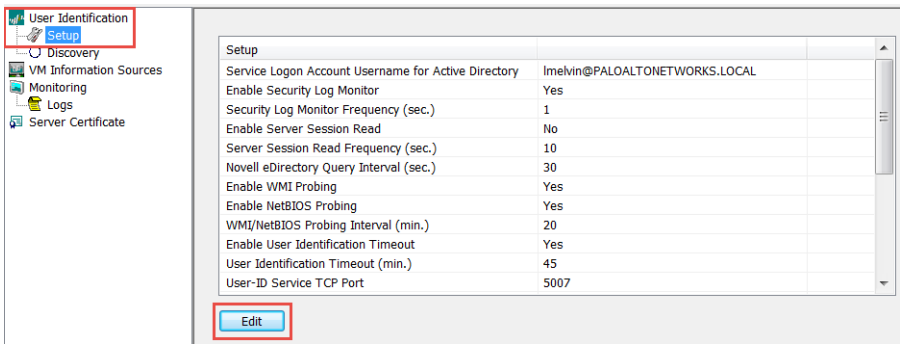
Elementos importantes para recordar al configurar la ID de usuario para habilitar la detección de filtro de credenciales de dominio:

- Debido a que la eficacia de la detección de suplantación de identidad de credenciales depende de su configuración de RODC, asegúrese de revisar también las prácticas recomendadas y las recomendaciones para la administración de RODC.
- Descargue las actualizaciones de software de ID de usuario:
  - Instalador de Windows de agente de ID de usuario: UaInstall-x.x.x-x.msi.
  - Instalador de Windows del servicio de credenciales del agente de ID de usuario: UaCredInstall64-x.x.x-x.msi.
- Instale el agente de ID de usuario y el servicio de credenciales del agente de usuario en un RODC usando una cuenta que tenga privilegios para leer Active Directory a través de LDAP (el agente de ID de usuario también necesita este privilegio).
  - El servicio de credenciales del agente de User-ID necesita permiso para iniciar sesión en la cuenta del sistema local. Para obtener más información, consulte Creación de una cuenta de servicio exclusiva para el agente de User-ID.
  - La cuenta de servicio debe formar parte del grupo de administradores locales del RODC. Para obtener más información, consulte este artículo.

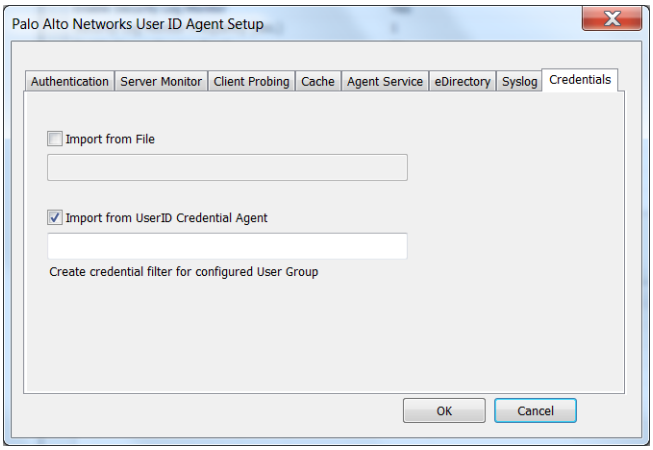
STEP 2 | Habilite el agente de ID de usuario y el servicio de credencial de agente de usuario (que se ejecuta en segundo plano para escanear las credenciales permitidas) para que comparta información.

1. En el servidor RODC, incie el agente de ID de usuario.
2. Seleccione **Setup (Configuración)** y modifique la sección Setup.

© 2020 Palo Alto Networks, Inc.



3. Seleccione la pestaña **Credentials (Credenciales)**. Esta pestaña se muestra únicamente si usted ya instaló el servicio de credenciales de agente de ID de usuario.



4. Seleccione **Import from User-ID Credential Agent (Importar del agente de credenciales de ID de usuario)**. Esto permite que el agente de ID de usuario importe el filtro de eclosión que el agente de credenciales de ID de usuario crea para representar a los usuarios y los hashes de contraseña correspondientes.
5. Haga clic en **OK (Aceptar)**, en **Save (Guardar)** para guardar los ajustes y en **Commit (Confirmar)**.

STEP 3 | En el directorio RODC, defina el grupo de usuarios para el cual desea admitir la detección de envío de credenciales.

- Confirme que los grupos que deben recibir el cumplimiento de envío de credenciales se añadan al grupo de replicación de contraseña RODC permitida.
- Verifique que ninguno de los grupos dentro del grupo de replicación de contraseña RODC permitida esté también en el grupo de replicación de contraseña no permitida. Los grupos enumerados en ambos no estarán sujetos al cumplimiento de la suplantación de identidad de credenciales.

STEP 4 | Continúe con la siguiente tarea.

Configuración de la prevención de la suplantación de identidad de credenciales en el cortafuegos.

Configuración de la prevención de suplantación de identidad de credenciales

Una vez que ha decidido cuál de los Métodos para comprobar los envíos de credenciales corporativas desea usar, realice los siguientes pasos para habilitar el cortafuegos a fin de que detecte cuando los usuarios envíen credenciales corporativas a páginas web y alerten sobre esta acción, bloqueen el envío de

© 2020 Palo Alto Networks, Inc.

credenciales o soliciten a los usuarios que acepten los riesgos de phishing (suplantación de identidad) antes de continuar con el envío de credenciales.

STEP 1 | Si aún no lo hizo, Habilite User-ID.

Cada uno de los Métodos para comprobar los envíos de credenciales corporativas exige una configuración de User-ID diferente para comprobar los envíos de credenciales corporativas:

- Si planea usar el método de asignación de grupo, que detecta si un usuario está enviando un nombre de usuario corporativo válido, asigne usuarios a grupos.
- Si planea usar el método de asignación de usuarios IP, que detecta si un usuario está enviando un nombre de usuario corporativo válido que coincide con el del usuario que inició sesión, asigne direcciones IP a usuarios.
- Si planea usar el método de filtro de credenciales de dominio, que detecta si un usuario está enviando un nombre de usuario y contraseña válidos, y si esas credenciales pertenecen al usuario que inició sesión, configure la detección de credenciales con el agente de User-ID basado en Windows y asigne direcciones IP a usuarios.

STEP 2 | Si aún no lo ha hecho, configure un perfil de filtrado de URL recomendado para garantizar protección contra las URL que se observó que alojan malware o contenido de exploits.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.
2. Bloquee el acceso a todas las categorías URL peligrosas conocidas: malware, phishing, DNS dinámico, desconocidas, de comando y control, extremistas, de infracción de derechos de autor, de anonimización y anulación de proxy, de dominio recién registrado, grayware y estacionadas.

STEP 3 | Añada una regla de políticas de descifrado para descifrar el tráfico que desea supervisar en busca de envíos de credenciales de usuario.

STEP 4 | Configure el perfil de filtrado de URL para detectar envíos de credenciales corporativas a sitios web que están en categorías URL permitidas.

El cortafuegos no verifica los envíos de credenciales para sitios de confianza, incluso si habilita las verificaciones de las categorías de URL para estos sitios, para proporcionar el mejor rendimiento. Los sitios de confianza son sitios para los que Palo Alto Networks no ha observado ningún ataque malicioso o de phishing. Las actualizaciones para esta lista de sitios de confianza se realizan a través de actualizaciones de contenido de aplicaciones y amenazas. Para ver la lista de App-ID exentos de la detección de credenciales, consulte el apartado sobre App-ID de confianza que omiten la detección del envío de credenciales *en* live.paloaltonetworks.com*.*

1. Seleccione **User Credential Detection (Detección de credencial de usuario)**.
2. Seleccione uno de los Métodos para comprobar los envíos de credenciales corporativas a páginas web en la lista desplegable **User Credential Detection (Detección de credenciales de usuario)**:

Confirme que el formato del nombre de usuario principal es idéntico al formato del nombre de usuario que proporciona el origen de User-ID.

- **Use IP User Mapping (Usar asignación de usuario IP):** comprueba el envío de nombres de usuario corporativo válidos y verifica que el nombre de usuario que inició sesión esté asignado a la dirección IP de la sesión. Para esto, el cortafuegos compara el nombre de usuario enviado y la dirección IP de origen de la sesión con su table de asignación de direcciones IP a usuarios. Para utilizar este método puede emplear cualquiera de los métodos de asignación de usuarios descritos en Asignar direcciones IP a los usuarios.

© 2020 Palo Alto Networks, Inc.

- **Use Domain Credential Filter (Usar filtro de credenciales de dominio)**: comprueba el envío de nombres de usuario y contraseñas válidas, y verifica que el nombre de usuario esté asignado a la dirección IP del usuario registrado. Consulte Configuración de detección de credenciales con el agente de User-ID de Windows para obtener instrucciones sobre cómo configurar User-ID para habilitar este método.
- **Use Group Mapping (Usar asignación de grupo)**: comprueba el envío de nombres de usuario válidos en función de la tabla de asignación de usuario a grupo completada al configurar el cortafuegos para la asignación de usuarios a grupos.

  Con la asignación de grupos, puede aplicar la detección de credenciales a cualquier parte del directorio o a grupos específicos, como los grupos que tienen acceso a sus aplicaciones más sensibles, como TI.



Este método es propenso a falsos positivos en entornos que no poseen nombres de usuario estructurados de manera inequívoca. Por ello, solo debe usar este método para proteger sus cuentas de usuario más importantes.

3. Configure la **Valid Username Detected Log Severity (Gravedad del log detectado de nombre de usuario válido)** que el cortafuegos utilizará para la detección de logs de envío de credenciales corporativas. De manera predeterminada, el cortafuegos registra estos eventos como eventos de gravedad intermedia.

STEP 5 | Bloquee (o alerte) los envíos de credenciales a sitios permitidos.

1. Seleccione **Categories (Categorías)**.
2. Para cada categoría a la cual se permite el **Site Access (Acceso al sitio)**, seleccione cómo desea que se manejen los **User Credential Submissions (Envíos de credenciales de usuario)**:
   - **alert (alerta)**: permite que los usuarios envíen sus credenciales al sitio web, pero genera un log de filtrado de URL cada vez que un usuario envía credenciales a sitios de esta categoría de URL.
   - **allow (permitir)**: (predeterminado) permite que los usuarios envíen sus credenciales al sitio web.
   - **block (bloquear)**: impide que usuarios envíen credenciales al sitio web. Cuando un usuario intenta enviar credenciales, el cortafuegos muestra la página de bloqueo antiphishing, que impide el envío de credenciales.
   - **continue (continuar)**: presenta la página de respuesta de continuación antiphishing a los usuarios cuando intentan enviar credenciales. Los usuarios deben seleccionar Continue (Continuar) en la página de respuesta para continuar con el envío.
3. Seleccione **OK (Aceptar)** para guardar el perfil de filtro de URL.

STEP 6 | Aplique el perfil de filtro URL con los ajustes de detección de credenciales a sus reglas de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
2. En la pestaña **Actions (Acciones)**, configure el **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)**.
3. Seleccione el perfil **URL Filtering (Filtrado de URL)** nuevo o actualizado para adjuntarlo a la regla de política de seguridad.
4. Seleccione **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 7 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 8 | Supervise los envíos de credenciales que el cortafuegos detecte.

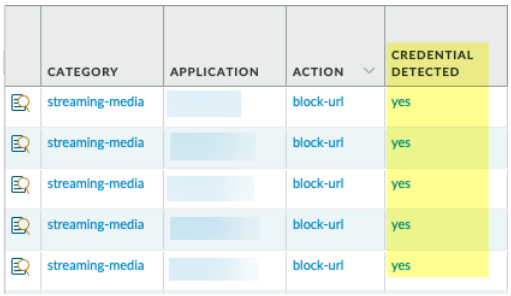


Seleccione ACC > Hosts Visiting Malicious URLs (Hosts de visitas a URL malintencionadas) para ver la cantidad de usuarios que visitaron sitios de malware y phishing.

© 2020 Palo Alto Networks, Inc.

Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**.

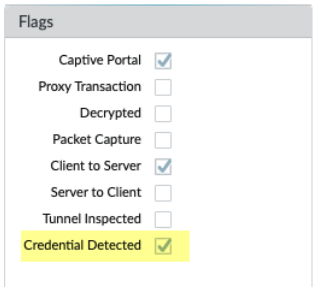
La nueva columna **Credential Detected (Credencial detectada)** indica eventos en los que el cortafuegos detectó una solicitud post HTTP que incluía una credencial válida:



	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

(Para visualizar esta columna, pase el ratón sobre cualquier encabezado de columna y haga clic en la flecha para seleccionar las columnas que desea visualizar).

Los detalles de entrada del log también indican el envío de credenciales:



STEP 9 | Valide y solucione problemas de detección del envío de credenciales.

- Use el siguiente comando CLI para visualizar las estadísticas de detección de credenciales:

```
> show user credential-filter statistics
```

El resultado de este comando varía según el método configurado para que el cortafuegos detecte envíos de credenciales. Por ejemplo, si el método Domain Credential Filter (Filtro de credenciales de dominio) está configurado en un perfil de filtrado de URL, se muestra una lista de agentes de User-ID que han reenviado un filtro de eclosión al cortafuegos, junto con la cantidad de credenciales incluidas en el filtro de eclosión.

- (Asignación de grupos únicamente) Utilice el siguiente comando CLI para ver información de asignación de grupos, incluido el número de perfiles de filtrado URL con la detección de credenciales de asignación de grupos habilitada y los nombres de usuario de los miembros del grupo que intentaron enviar las credenciales a un sitio restringido.

```
> show user group-mapping statistics
```

- (Filtro de credenciales de dominio únicamente) Utilice el siguiente comando CLI para ver todos los agentes de User-ID basados en Windows que envían asignaciones al cortafuegos:

```
> show user user-id-agent state all
```

El resultado del comando ahora muestra recuentos de filtro de eclosión que incluyen la cantidad de actualizaciones de filtro de eclosión que el cortafuegos ha recibido de cada agente, si alguna

© 2020 Palo Alto Networks, Inc.

actualización de filtro de eclosión falló en el proceso, y cuántos segundos transcurrieron desde la última actualización de filtro de eclosión.

- (Filtrado de credenciales de dominio únicamente) El agente de User-ID basado en Windows muestra los mensajes de log que el filtro de eclosión (bloom filter, BF) de referencia envía al cortafuegos. En la interfaz del agente de User-ID, seleccione Monitoring (Supervisión)**Logs**.

© 2020 Palo Alto Networks, Inc.

Forzaje de búsquedas seguras

Muchos motores de búsqueda incluyen una opción de búsqueda segura que filtra las imágenes y los vídeos para adultos del tráfico de devolución de consultas de búsqueda. Puede habilitar el cortafuegos para bloquear los resultados de la búsqueda si el usuario final no utiliza la configuración de búsqueda segura más exigente y también puede habilitar la búsqueda segura de manera transparente para sus usuarios. El cortafuegos admite la aplicación de búsqueda segura para los siguientes proveedores de búsquedas: Google, Yahoo, Bing, Yandex y YouTube. Tenga en cuenta que la búsqueda segura es una configuración de menor esfuerzo y los proveedores de servicio no garantizan que funcione en cada sitio web. Además, son los proveedores de búsqueda los que clasifican los sitios como seguros o inseguros (no Palo Alto Networks).

Para usar esta función, debe habilitar la opción **Safe Search Enforcement (Aplicación de búsquedas seguras)** en un perfil de filtrado de URL y adjuntarla a una regla de la política de seguridad. El cortafuegos bloqueará cualquier tráfico de retorno de consulta de búsqueda coincidente que no utilice la configuración de búsqueda segura más estricta. Existen dos métodos de aplicación de búsqueda segura:

- Bloqueo de resultados de búsqueda cuando la búsqueda segura estricta no está habilitada: cuando un usuario final intenta realizar una búsqueda sin habilitar primero la configuración de búsqueda segura más estricta, el cortafuegos bloquea los resultados de la consulta de búsqueda y muestra la página de bloqueo de búsqueda segura de filtrado de URL. De forma predeterminada, esta página proporciona una dirección URL al proveedor de búsquedas para configurar la búsqueda segura.
- Habilitación transparente de la búsqueda segura de usuarios: cuando un usuario final intenta realizar una búsqueda sin habilitar primero la configuración de búsqueda segura estricta, el cortafuegos bloquea los resultados de la búsqueda con un código de estado HTTP 503 y redirige la consulta de búsqueda a una URL que incluye los parámetros de búsqueda segura. Para habilitar esta función, importe una página de bloque de búsqueda segura de filtrado de URL nueva que contenga Javascript para reescribir la dirección URL de búsqueda de modo que incluya los parámetros de búsqueda segura estricta. Con esta configuración, los usuarios no verán la página de bloque, sino que serán redirigidos automáticamente a una consulta de búsqueda que fuerza las opciones de búsqueda segura más estrictas. Este método de aplicación forzada de búsquedas seguras es compatible con búsquedas Google, Yahoo y Bing.

Dado que la configuración de la búsqueda segura varía según el proveedor de búsqueda, comience por revisar las diferentes implementaciones de búsqueda segura. Existen dos maneras de aplicar la búsqueda segura: puede bloquear los resultados de la búsqueda cuando la búsqueda segura está deshabilitada o puede habilitar la búsqueda segura de manera transparente para sus usuarios:

- Configuración de búsqueda segura para proveedores de búsqueda
- Bloqueo de los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada
- Habilitación transparente de la búsqueda segura para los usuarios

Configuración de búsqueda segura para proveedores de búsqueda

La configuración de búsqueda segura varía según el proveedor de búsqueda; revise las siguientes configuraciones para obtener más información.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
Google/YouTube	Permiten la búsqueda segura en equipos individuales o en toda la red mediante la dirección IP virtual de búsqueda segura de Google: **Aplicación forzada de búsquedas seguras en Google en equipos individuales:** En la sección de ajustes de búsqueda de Google, la opción **Filter explicit results (Filtrar resultados explícitos)** habilita la función de búsqueda segura. Una vez

© 2020 Palo Alto Networks, Inc.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
	habilitada, la configuración se almacena en una cookie del explorador como `FF=` y se pasa al servidor cada vez que el usuario realiza una búsqueda en Google. La anexión de **`safe=active`** a una dirección URL de consulta de búsqueda de Google también habilita la configuración de búsqueda segura más estricta. **Aplicación forzada de búsquedas seguras en Google y YouTube mediante una dirección IP virtual** Google proporciona servidores que bloquean SafeSearch (forcesafesearch.google.com) en cada búsqueda en Google y YouTube. Si añade una entrada DNS para **`www.google.com`** y **`www.youtube.com`** (y otros subdominios correspondientes a países de Google y YouTube) que incluya un registro CNAME que apunte a **`forcesafesearch.google.com`** para la configuración de su servidor DNS, puede garantizar que todos los usuarios de su red usen la configuración de búsqueda segura estricta cada vez que realicen una búsqueda en Google o YouTube. Sin embargo, debe tener en cuenta que esa solución no es compatible con la aplicación forzada de búsquedas seguras en el cortafuegos. Así, si está usando esta opción para forzar las búsquedas seguras en Google, lo mejor es bloquear el acceso a otros motores de búsqueda del cortafuegos creando categorías de URL personalizadas y añadiéndolas a la lista de bloqueados en el perfil de filtrado de URL.  • *PAN-OS admite la aplicación de búsquedas seguras para YouTube mediante la inserción de encabezados HTTP. Actualmente, la inserción de encabezados HTTP no es compatible con HTTP/2. Para garantizar una búsqueda segura en YouTube, Inspección de App-ID y HTTP/2 cambie las conexiones HTTP/2 a HTTP/1.1 mediante la función Strip ALPN (Eliminar ALPN) en el perfil de descifrado correspondiente.* • *Si planea utilizar la solución de bloqueo SafeSearch de Google, considere la posibilidad de configurar un proxy DNS (Network [Red] > DNS Proxy [Proxy DNS]) y establecer el origen de herencia como la interfaz de capa 3 en la que el cortafuegos recibe la configuración de DNS del proveedor de servicios mediante DHCP. Debe configurar el proxy DNS con Entradas estáticas para www.google.com y www.youtube.com mediante la dirección IP local para el servidor de forcesafesearch.google.com.*
Yahoo	Permite la búsqueda segura solamente en equipos individuales. Las preferencias de búsqueda de Yahoo incluyen tres opciones de SafeSearch: **Estricta**, **Moderada** o **Desactivada**. Una vez habilitada, la configuración se almacena en una cookie del explorador como `vm=` y se pasa al servidor cada vez que el usuario realiza una búsqueda en Yahoo. La anexión de `vm=r` a una dirección URL de consulta de búsqueda de Yahoo también habilita la configuración de búsqueda segura más estricta.  *Cuando se realiza una búsqueda en Yahoo Japan (**`yahoo.co.jp`**) tras iniciar sesión con una cuenta de Yahoo, los usuarios finales*

© 2020 Palo Alto Networks, Inc.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
	deben habilitar la opción de bloqueo en SafeSearch Lock (Bloquear).
Bing	Permite la búsqueda segura en equipos individuales o mediante su programa Bing in the Classroom. La configuración de Bing incluye tres opciones de SafeSearch: **Estricta**, **Moderada** o **Desactivada**. Una vez habilitada, la configuración se almacena en una cookie del explorador como `adtl=` y se pasa al servidor cada vez que el usuario realiza una búsqueda en Bing. La anexión de **`adlt=strict`** a una dirección URL de consulta de búsqueda de Bing también habilita la configuración de búsqueda segura más estricta. El motor de búsqueda SSL de Bing no fuerza los parámetros de URL de búsqueda segura y, por lo tanto, debe considerar la posibilidad de bloquear Bing en SSL para la aplicación forzada de búsquedas seguras completa.

Bloqueo de los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada

De forma predeterminada, si habilita la aplicación forzada de búsquedas seguras, cuando un usuario intenta realizar una búsqueda sin usar la configuración de búsqueda segura más estricta, el cortafuegos bloquea los resultados de la consulta de búsqueda y muestra la página de bloque de búsqueda segura de filtrado de URL. Esta página incluye un enlace a la página de configuración de búsqueda para el proveedor de búsquedas correspondiente de modo que el usuario final pueda habilitar la configuración de búsqueda segura. Si tiene previsto usar este método predeterminado para forzar la búsqueda segura, debe comunicar la política a sus usuarios finales antes de implementarla. Consulte la información detallada sobre cómo cada proveedor de búsquedas implementa la búsqueda segura. La página de bloque de búsqueda segura de filtrado de URL predeterminada incluye un enlace a la configuración de búsqueda para el proveedor de búsquedas correspondiente. Opcionalmente, puede personalizar las páginas de respuesta de filtro URL.

Además, para habilitar la aplicación forzada de búsquedas seguras de modo que sea transparente para sus usuarios finales, configure el cortafuegos para Habilitar de forma transparente la búsqueda segura para los usuarios.

STEP 1 | Habilite la aplicación forzada de búsquedas seguras en el perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado URL)**.
2. Seleccione un perfil existente para modificarlo o duplique el perfil predeterminado para crear un nuevo perfil.
3. En la pestaña **Configuración**, seleccione la casilla de verificación **Safe Search Enforcement (Aplicación de búsquedas seguras)** para habilitarla.
4. (Opcional) Restrinja los usuarios para motores de búsqueda específicos:
   1. En la pestaña **Categories (Categorías)**, establezca la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.
   2. Para cada motor de búsqueda al que desee que los usuarios finales puedan acceder, especifique la dirección web en el cuadro de texto **Allow List (Lista de permitidos)**. Por ejemplo, para permitir a los usuarios acceder solo a las búsquedas en Google y Bing, debe especificar lo siguiente:

      `www.google.com`

© 2020 Palo Alto Networks, Inc.

```
www.bing.com
```

5. Configure otras opciones según sea necesario para:
   - Defina el acceso al sitio para cada categoría de URL.
   - Defina las listas de bloqueados y permitidos para especificar los sitios web que siempre deben bloquearse o permitirse, independientemente de la categoría de URL.
6. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 2 | Añada el perfil de filtrado de URL a la regla de la política de seguridad que permite el tráfico de clientes en la zona de confianza de Internet.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla a la cual aplicar el perfil de filtro URL que acaba de habilitar para el cumplimiento de la búsqueda segura.
2. En la pestaña **Actions (Acciones)**, seleccione el perfil de **URL Filtering (Filtrado de URL)**.
3. Haga clic en **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 3 | Habilite el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

1. Añada una categoría de URL personalizada para los sitios de búsqueda:
   1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
   2. Introduzca un nombre en **Name** para la categoría, como SearchEngineDecryption.
   3. Seleccione **Add (Añadir)** para añadir lo siguiente a la lista de sitios:

      ```
      www.bing.*
      ```

      ```
      www.google.*
      ```

      ```
      search.yahoo.*
      ```
   4. Haga clic en **OK (Aceptar)** para guardar el objeto de la categoría de URL personalizada.
2. Siga los pasos de Configuración de proxy de reenvío SSL.
3. En la pestaña **Service/URL Category (Categoría de URL/servicio)** de la regla de la política de descifrado, seleccione **Add (Añadir)** para añadir la categoría URL personalizada que acaba de crear y haga clic en **OK (Aceptar)**.

STEP 4 | (Recomendado) Bloquee el tráfico de búsqueda Bing que se ejecuta con SSL.

Dado que el motor de búsqueda SSL de Bing no cumple la configuración de búsqueda segura, para una aplicación forzada de búsquedas completo, debe rechazar todas las sesiones de Bing que se ejecutan con SSL.

1. Añada una categoría de URL personalizada para Bing:
   1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
   2. Introduzca un nombre en **Name (Nombre)** para la categoría, como EnableBingSafeSearch.
   3. Seleccione **Add (Añadir)** para añadir lo siguiente a la lista de sitios:

      ```
      www.bing.com/images/*
      ```

      ```
      www.bing.com/videos/*
      ```
   4. Haga clic en **OK (Aceptar)** para guardar el objeto de la categoría de URL personalizada.
2. Cree otro perfil de filtrado de URL para bloquear la categoría personalizada que ha creado:

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado URL)**.
2. Seleccione **Add (Añadir)** para añadir un perfil nuevo y asígnele un **Name (Nombre)** descriptivo.
3. Busque la categoría personalizada en la lista de categorías y establézcala en **block (bloquear)**.
4. Haga clic en **OK (Aceptar)** para guardar el perfil de filtro de URL.

3. Añada una regla de la política de seguridad para bloquear el tráfico SSL de Bing:
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** para añadir una regla de política que permita el tráfico de su zona fiable a Internet.
   2. En la pestaña **Actions (Acciones)**, adjunte el perfil de filtrado de URL que acaba de crear para bloquear la categoría de Bing personalizada.
   3. En la pestaña **Categoría de URL/servicio**, seleccione **Añadir** para añadir un **Nuevo servicio** y asígnele un **Nombre** descriptivo, como bingssl.
   4. Seleccione **TCP** como **Protocol (Protocolo)** y establezca **Destination Port (Puerto de destino)** en `443`.
   5. Haga clic en **OK (Aceptar)** para guardar la regla.
   6. Use la opción **Move (Mover)** para asegurarse de que esta regla está debajo de la regla que tiene el perfil de filtrado de URL con el forzaje de búsquedas seguras habilitado.

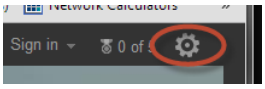
STEP 5 | Guarde la configuración.

Haga clic en **Commit (Confirmar)**.

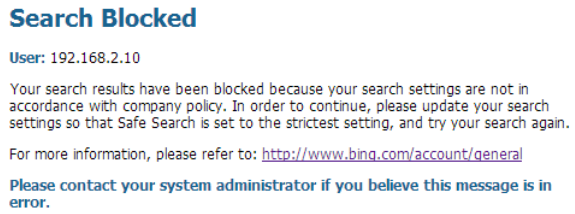
STEP 6 | Compruebe la configuración de la aplicación forzada de búsquedas seguras.

Este paso de verificación solo funciona si usa páginas de bloqueo para forzar la búsqueda segura. Si usa la aplicación forzada de búsquedas seguras transparente, la página de bloque del cortafuegos invoca la reescritura de URL con los parámetros de búsqueda segura en la cadena de consulta.

1. En un equipo detrás del cortafuegos, deshabilite la configuración de búsqueda estricta para uno de los proveedores de búsquedas admitidos. Por ejemplo, en bing.com, haga clic en el icono de **preferencias** en la barra de menús de Bing.



2. Establezca la opción **SafeSearch (Búsqueda segura)** en **Moderate (Moderada)** o **Off (Desactivada)** y haga clic en **Save (Guardar)**.
3. Realice una búsqueda en Bing y compruebe si se muestra la página de bloque de búsqueda segura de filtrado de URL en lugar de los resultados de la búsqueda:



4. Use el enlace de la página de bloque para ir a la configuración de búsqueda del proveedor de búsquedas, establezca la configuración de búsqueda segura más estricta (**Strict [Estricta]** en el caso de Bing) y, a continuación, haga clic en **Save [Guardar]**.
5. Vuelva a realizar una búsqueda en Bing y compruebe si se muestran los resultados de la búsqueda filtrada en lugar de la página de bloque.

© 2020 Palo Alto Networks, Inc.

Habilitación transparente de la búsqueda segura para los usuarios

Si desea forzar el filtrado de los resultados de la consulta de búsqueda con los filtros de búsqueda segura más estricta, pero no desea que los usuarios finales tengan que configurar las opciones manualmente, puede habilitar la aplicación forzada de búsquedas seguras transparente del modo siguiente. Esta función solo es compatible con los motores de búsqueda de Google, Yahoo y Bing, y requiere la versión de publicación de contenido 475 o posterior.

STEP 1 | Asegúrese de que el cortafuegos ejecuta la versión de publicación de contenido 475 o posterior.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Compruebe la sección **Aplicaciones y amenazas** para determinar qué actualización se está ejecutando.
3. Si el cortafuegos no está ejecutando la actualización requerida o posterior, haga clic en **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
4. Busque la actualización requerida y haga clic en **Download (Descargar)**.
5. Cuando finalice la descarga, haga clic en **Install (Instalar)**.

STEP 2 | Habilite la aplicación forzada de búsquedas seguras en el perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado URL)**.
2. Seleccione un perfil existente para modificarlo o duplique el perfil predeterminado para crear uno nuevo.
3. En la pestaña **Configuración**, seleccione la casilla de verificación **Safe Search Enforcement (Aplicación de búsquedas seguras)** para habilitarla.
4. (Opcional) Permita el acceso solo a motores de búsqueda específicos:
   1. En la pestaña **Categories (Categorías)**, establezca la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.
   2. Para cada motor de búsqueda al que desee que los usuarios finales puedan acceder, especifique la dirección web en el cuadro de texto **Allow List (Lista de permitidos)**. Por ejemplo, para permitir a los usuarios acceder solo a las búsquedas en Google y Bing, debe especificar lo siguiente:

      ```
      www.google.com
      ```

      ```
      www.bing.com
      ```
5. Configure otras opciones según sea necesario para:
   - Defina el acceso al sitio para cada categoría de URL.
   - Defina las listas de bloqueados y permitidos para especificar los sitios web que siempre deben bloquearse o permitirse, independientemente de la categoría de URL.
6. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Añada el perfil de filtrado de URL a la regla de la política de seguridad que permite el tráfico de clientes en la zona de confianza de Internet.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione una regla a la cual aplicar el perfil de filtro URL que acaba de habilitar para el cumplimiento de la búsqueda segura.
2. En la pestaña **Actions (Acciones)**, seleccione el perfil de **URL Filtering (Filtrado de URL)**.
3. Haga clic en **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 4 | (Recomendado) Bloquee el tráfico de búsqueda Bing que se ejecuta con SSL.

© 2020 Palo Alto Networks, Inc.

Dado que el motor de búsqueda SSL de Bing no cumple la configuración de búsqueda segura, para una aplicación forzada de búsquedas completo, debe rechazar todas las sesiones de Bing que se ejecutan con SSL.

1. Añada una categoría de URL personalizada para Bing:
    1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
    2. Introduzca un nombre en **Name (Nombre)** para la categoría, como EnableBingSafeSearch.
    3. Seleccione **Add (Añadir)** para añadir lo siguiente a la lista de sitios:

        `www.bing.com/images/*`

        `www.bing.com/videos/*`
    4. Haga clic en **OK (Aceptar)** para guardar el objeto de la categoría de URL personalizada.
2. Cree otro perfil de filtrado de URL para bloquear la categoría personalizada que ha creado:
    1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado URL)**.
    2. Seleccione **Add (Añadir)** para añadir un perfil nuevo y asígnele un **Name (Nombre)** descriptivo.
    3. Busque la categoría personalizada que acaba de crear en la lista de categorías y establézcala en **Bloquear**.
    4. Haga clic en **OK (Aceptar)** para guardar el perfil de filtro de URL.
3. Seleccione **Añadir** para añadir una regla de la política de seguridad para bloquear el tráfico SSL de Bing:
    1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** para añadir una regla de política que permita el tráfico de su zona fiable a Internet.
    2. En la pestaña **Actions (Acciones)**, adjunte el perfil de filtrado de URL que acaba de crear para bloquear la categoría de Bing personalizada.
    3. En la pestaña **Categoría de URL/servicio**, seleccione **Añadir** para añadir un **Nuevo servicio** y asígnele un **Nombre** descriptivo, como bingssl.
    4. Seleccione **TCP** como **Protocol (Protocolo)** y establezca **Destination Port (Puerto de destino)** en **`443`**.
    5. Haga clic en **OK (Aceptar)** para guardar la regla.
    6. Use la opción **Move (Mover)** para asegurarse de que esta regla está debajo de la regla que tiene el perfil de filtrado de URL con el forzaje de búsquedas seguras habilitado.

STEP 5 | Edite la página de bloque de búsqueda segura de filtrado de URL para sustituir el código existente por Javascript con el fin de reescribir las URL de consulta de búsqueda para forzar la búsqueda segura de forma transparente.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > **URL Filtering Safe Search Block Page (Página de bloque de búsqueda segura de filtrado de URL)**.
2. Seleccione **Predefinido** y, a continuación, haga clic en **Exportar** para guardar el archivo localmente.
3. Use un editor HTML para sustituir todo el texto de la página de bloque existente por el siguiente texto y, a continuación, guarde el archivo:

```
<html>
  <head>
    <title>Search Blocked</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta http-equiv="pragma" content="no-cache">
    <meta name="viewport" content="initial-scale=1.0">
    <style>
      #content {
      border:3px solid#aaa;
```


© 2020 Palo Alto Networks, Inc.

```
      background-color:#fff;
      margin:1.5em;
      padding:1.5em;
      font-family:Tahoma,Helvetica,Arial,sans-serif;
      font-size:1em;
      }
      h1 {
      font-size:1.3em;
      font-weight:bold;
      color:#196390;
      }
      b {
      font-weight:normal;
      color:#196390;
      }
    </style>
  </head>
  <body bgcolor="#e7e8e9">
    <div id="content">
      <h1>Search Blocked</h1>
      <p>
        <b>User:</b>
        <user/>
      </p>
      <p>Your search results have been blocked because your search
 settings are not in accordance with company policy.  In order to
 continue, please update your search settings so that Safe Search is
 set to the strictest setting. If you are currently logged into your
 account, please also lock Safe Search and try your search again.</p>
      <p>
        For more information, please refer to:
        <a href="<ssurl/>">
          <ssurl/>
        </a>
      </p>
      <p id="java_off"> Please enable JavaScript in your browser.<br></
p>
      <p><b>Please contact your system administrator if you believe this
 message is in error.</b></p>
    </div>
  </body>
  <script>
    // Grab the URL that's in the browser.
    var s_u = location.href;
    //bing
    // Matches the forward slashes in the beginning, anything, then
 ".bing." then anything followed by a non greedy slash. Hopefully the
 first forward slash.
    var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u);
    if (b_a) {
       s_u = s_u + "&adlt=strict";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
 redirected to a safer search!';
    }
    //google
    // Matches the forward slashes in the beginning, anything, then
 ".google." then anything followed by a non greedy slash. Hopefully the
 first forward slash.
    var g_a = /^.*\/\/(.+\.google\..+?)\//.exec(s_u);
```


© 2020 Palo Alto Networks, Inc.

```
    if (g_a) {
        s_u = s_u.replace(/&safe=off/ig,"");
        s_u = s_u + "&safe=active";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
 redirected to a safer search!';    }
    //yahoo
    // Matches the forward slashes in the beginning, anything, then
 ".yahoo."" then anything followed by a non greedy slash. Hopefully the
 first forward slash.
    var y_a = /^.*\/\/(.+\.yahoo\..+?)\//.exec(s_u);
    if (y_a) {
        s_u = s_u.replace(/&vm=p/ig,"");
        s_u = s_u + "&vm=r";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
 redirected to a safer search!';
    }
    document.getElementById("java_off").innerHTML = ' ';
  </script>
</html>
```

STEP 6 | Importe la página de bloque de búsqueda segura de filtrado de URL editada en el cortafuegos.

1. Para importar la página de bloque editada, seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > **URL Filtering Safe Search Block Page (Página de bloque de búsqueda segura de filtrado de URL)**.
2. Haga clic en **Import (Importar)** y, a continuación, introduzca la ruta y el nombre de archivo en el campo **Import File (Importar archivo)** o **Browse (Examinar)** para encontrar el archivo.
3. (Opcional) Seleccione el sistema virtual en el que se usará esta página de inicio de sesión en la lista desplegable **Destination** o seleccione **shared** para que esté disponible para todos los sistemas virtuales.
4. Haga clic en **OK (Aceptar)** para importar el archivo.

STEP 7 | Habilite el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

1. Añada una categoría de URL personalizada para los sitios de búsqueda:
    1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
    2. Introduzca un nombre en **Name** para la categoría, como SearchEngineDecryption.
    3. Seleccione **Add (Añadir)** para añadir lo siguiente a la lista de sitios:

        ```
        www.bing.*

        www.google.*

        search.yahoo.*
        ```
    4. Haga clic en **OK (Aceptar)** para guardar el objeto de la categoría de URL personalizada.
2. Siga los pasos de Configuración de proxy de reenvío SSL.
3. En la pestaña **Service/URL Category (Categoría de URL/servicio)** de la regla de la política de descifrado, seleccione **Add (Añadir)** para añadir la categoría URL personalizada que acaba de crear y haga clic en **OK (Aceptar)**.

STEP 8 | Guarde la configuración.

© 2020 Palo Alto Networks, Inc.

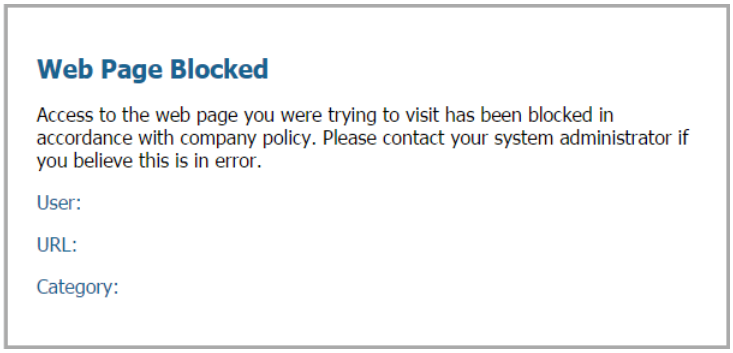
Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Páginas de respuesta de filtrado de URL

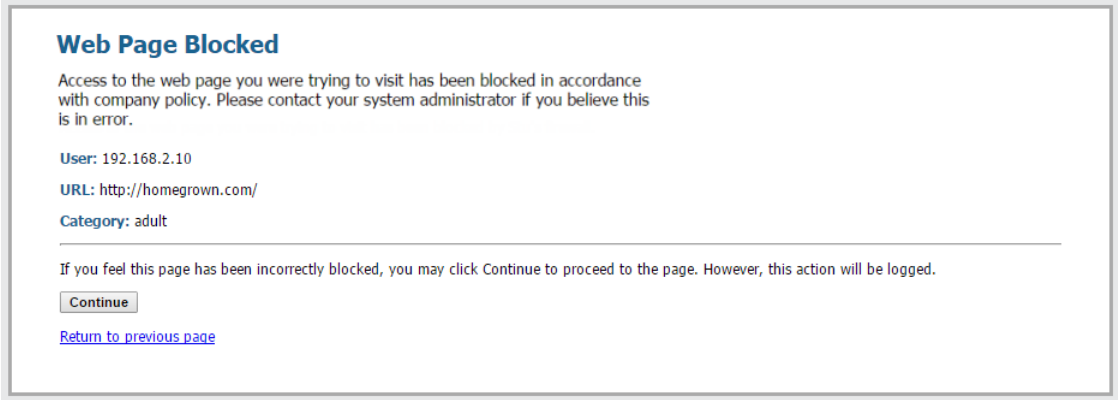
El cortafuegos proporciona tres páginas de respuesta predefinidas que se muestran de forma predeterminada cuando un usuario intenta navegar a un sitio de una categoría configurada con una de las acciones de bloqueo del perfil de filtrado URL (bloquear, continuar o cancelar) o si la opción Container Pages (Páginas de contenedor) está habilitada:

- **Página de bloqueo de coincidencia de categoría y filtro de URL**



- **Página de continuación y cancelación de filtrado de URL**

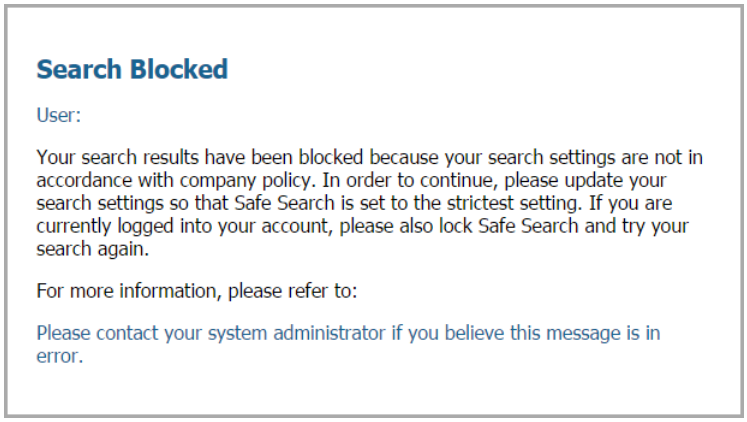
  Página con la política de bloqueo inicial que permite a los usuarios omitir el bloqueo al hacer clic en **Continue (Continuar)**. Con la cancelación de administración de URL habilitada, (Habilitación del acceso a determinados sitios mediante contraseña), después de hacer clic en **Continue (Continuar)**, el usuario debe proporcionar una contraseña para cancelar la política que bloquea la URL.



- **Página de bloque de búsqueda segura de filtrado de URL**

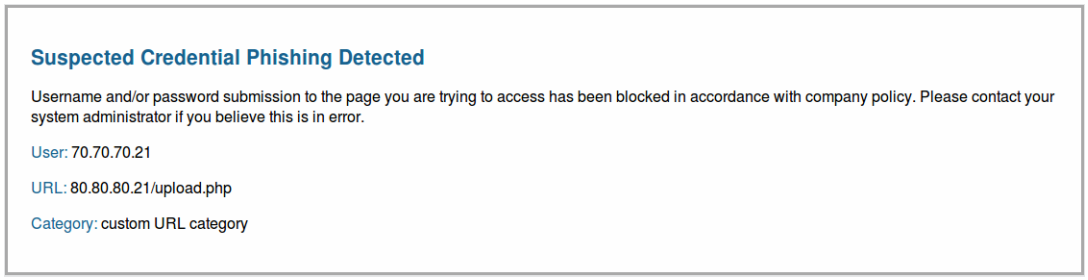
  Acceso bloqueado por una regla de política de seguridad con un perfil de filtrado de URL que tiene habilitada la opción Safe Search Enforcement (Aplicación de búsquedas seguras) (consulte Aplicación forzada de búsquedas seguras). El usuario verá esta página si se realiza una búsqueda con Google, Bing, Yahoo o Yandex y la configuración de cuenta de su explorador o motor de búsqueda para la búsqueda segura no está establecida como estricta.

© 2020 Palo Alto Networks, Inc.



- **Página de bloqueo antiphishing**

  Esta página se muestra a los usuarios cuando intentan introducir credenciales corporativas (nombres de usuario o contraseñas) en una página web, con una categoría para la cual se bloqueó la presentación de credenciales. El usuario puede seguir accediendo al sitio, pero sigue sin poder enviar credenciales corporativas válidas a formularios web asociados. Para controlar los sitios a los cuales los usuarios pueden enviar credenciales corporativas, el cortafuegos debe configurarse con User-ID y con la opción Prevent Credential Phishing (Prevenir el phishing de identidades) habilitada y basada en la categoría de URL.



- **Página de continuación antiphishing**

  Esta página advierte a los usuarios sobre el envío de credenciales (nombres de usuario y contraseñas) a un sitio web. La advertencia a los usuarios contra la presentación de credenciales puede ayudar a disuadirlos de reutilizar credenciales corporativas y educarlos sobre posibles intentos de phishing. Deben seleccionar Continue (Continuar) para introducir las credenciales en el sitio. Para controlar los sitios a los cuales los usuarios pueden enviar credenciales corporativas, el cortafuegos debe configurarse con User-ID y con la opción Prevent Credential Phishing (Prevenir el phishing de identidades) habilitada y basada en la categoría de URL.



Puede usar las páginas predefinidas o puede usar la opción de personalizar las páginas de respuesta de filtrado URL para comunicar sus políticas de uso aceptable específicas o personalización de marca

© 2020 Palo Alto Networks, Inc.

corporativa. Además, puede usar las Variables de página de respuesta de filtrado de URL para la sustitución en el momento del evento de bloqueo o añadir una de las Referencias de página de respuesta admitidas a imágenes, sonidos u hojas de estilo externos.

Table 2: Variables de página de respuesta de filtrado de URL

Variable	Uso
<user/>	El cortafuegos sustituye la variable por el nombre de usuario (si está disponible mediante User-ID) o la dirección IP del usuario cuando se muestra la página de respuesta.
<url/>	El cortafuegos sustituye la variable por la dirección URL solicitada cuando se muestra la página de respuesta.
<category/>	El cortafuegos sustituye la variable por la categoría de filtrado de URL de la solicitud bloqueada.
<pan_form/>	Código HTML para mostrar el botón **Continue (Continuar)** en la página de continuación y cancelación de filtrado de URL.

Además, puede añadir código que active el cortafuegos para mostrar el uso de distintos mensajes según la categoría de URL a la que el usuario está intentando acceder. Por ejemplo, el siguiente fragmento de código de una página de respuesta especifica que se muestre el mensaje 1 si la categoría de URL es games, el mensaje 2 si la categoría es travel o el mensaje 3 si la categoría es kids:

```
var cat = "<category/>";
switch(cat)
{
 case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break;
 case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break;
 case 'kids':
 document.getElementById("warningText").innerHTML = "Message 3";
 break;
}
```

Solo se puede cargar una página HTML en cada sistema virtual para cada tipo de página de bloqueo. Sin embargo, otros recursos como las imágenes, los sonidos y las hojas de estilos en cascada (archivos CSS) se pueden cargar de otros servidores en el momento en el que se muestra la página de respuesta en el explorador. Todas las referencias deben incluir una dirección URL completa.

Table 3: Referencias de página de respuesta

Tipo de referencia	Código HTML de ejemplo
Imagen	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`

© 2020 Palo Alto Networks, Inc.

Tipo de referencia	Código HTML de ejemplo
Sonido	`<embed src="http://simplythebest.net/sounds/WAV/ WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
Hoja de estilos	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
Hiperenlace	`<a href="http://en.wikipedia.org/wiki/ Acceptable_use_policy">View Corporate Policy</a>`

© 2020 Palo Alto Networks, Inc.

Personalización de las páginas de respuesta de filtrado de URL

El cortafuegos proporciona Páginas de respuesta de filtrado de URL predefinidas que muestran de manera predeterminada cuando se producen las siguientes condiciones:

- Un usuario intenta explorar un sitio en una categoría con acceso restringido.
- Un usuario envía credenciales corporativas válidas a un sitio con detección de credenciales habilitada (Prevención de phishing de credenciales en función de la categoría de URL).
- Registro solo de las páginas que visita un usuario bloquea un intento de búsqueda.

Sin embargo, puede crear sus propias páginas de respuesta con su marca corporativa, políticas de uso aceptable y enlaces a sus recursos internos.



Las páginas de respuesta personalizadas más grandes que el tamaño máximo admitido no se descifran ni muestran a los usuarios. En PAN-OS 8.1.2 y versiones anteriores de PAN-OS 8.1, las páginas de respuesta personalizadas en un sitio descifrado no pueden superar los 8191 bytes; el tamaño máximo se aumenta a 17 999 bytes en PAN-OS 8.1.3 y versiones posteriores.

STEP 1 | Exporte las páginas de respuesta predeterminadas.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el enlace de la página de respuesta de filtrado de URL que desee modificar.
3. Haga clic en la página de respuesta (predefinida o compartida) y, a continuación, haga clic en el enlace **Export (Exportar)** y guarde el archivo en su escritorio.

STEP 2 | Edite la página exportada.

1. Con el editor de texto de HTML que prefiera, edite la página:
   - Si desea que la página de respuesta muestre información personalizada sobre el usuario, la dirección URL o la categoría específicos que se han bloqueado, añada una o varias de las Table 2: Variables de página de respuesta de filtrado de URL admitidas.
   - Si desea incluir imágenes personalizadas (como su logotipo corporativo), un sonido, una hoja de estilos o un enlace a otra dirección URL (por ejemplo, a un documento en el que se detalla su política de uso de Internet aceptable), incluya una o varias de las Table 3: Referencias de página de respuesta admitidas.
2. Guarde la imagen editada con un nuevo nombre de archivo. Asegúrese de que la página conserva su codificación UTF-8. Por ejemplo, en el Bloc de notas, debe seleccionar **UTF-8** en la lista desplegable **Encoding (Codificación)** del cuadro de diálogo Guardar como.

STEP 3 | Importe la página de respuesta personalizada.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el enlace correspondiente a la página de respuesta de filtrado de URL que ha editado.
3. Haga clic en **Import (Importar)** y, a continuación, introduzca la ruta y el nombre de archivo en el campo **Import File (Importar archivo)** o **Browse (Examinar)** para encontrar el archivo.
4. (Opcional) Seleccione el sistema virtual en el que se usará esta página de inicio de sesión en la lista desplegable **Destination** o seleccione **shared** para que esté disponible para todos los sistemas virtuales.
5. Haga clic en **OK (Aceptar)** para importar el archivo.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Guarde las páginas de respuesta nuevas.

Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 5 | Compruebe si se muestra la nueva página de respuesta.

En un explorador, vaya a la dirección URL que activará la página de respuesta. Por ejemplo, para ver una página de respuesta modificada de filtrado de URL y coincidencia de categorías, busque la dirección URL cuyo bloqueo es requerido según la configuración de su política de filtrado de URL.

El cortafuegos utiliza los siguientes puertos para mostrar las páginas de respuesta de filtrado de URL:

- **HTTP**: 6080
- **Default TLS with firewall certificate (TLS predeterminado con certificado de cortafuegos)**: 6081
- **Custom SSL/TLS profile (Perfil SSL/TLS personalizado)**: 6082

© 2020 Palo Alto Networks, Inc.

Creación de logs del encabezado HTTP

El filtrado de URL proporciona visibilidad y control sobre el tráfico web de su red. Para aumentar la visibilidad en el contenido web, puede configurar el perfil de filtrado de URL para registrar un log de atributos de encabezado HTTP incluido en una solicitud web. Cuando un cliente solicita una página web, el encabezado HTTP incluye los campos de agente de usuario, sitio de referencia y x-forwarded-for como pares de atributo y valor, y los reenvía al servidor web. En caso de estar habilitado para la creación de logs de encabezados HTTP, el cortafuegos registra los siguientes pares de atributo y valor en los logs de filtrado URL.



También puede usar encabezados HTTP para gestionar el acceso a las aplicaciones SaaS. No necesita una licencia de filtrado de URL para realizar este procedimiento, pero debe usar un perfil de filtrado de URL para activar esta función.

Atributo	Description (Descripción)
User-Agent (Agente de usuario)	Explorador web que usa el usuario para acceder a la dirección URL (por ejemplo, Internet Explorer). Esta información se envía en la solicitud de HTTP al servidor.
Referer (Sitio de referencia)	Dirección URL de la página web que dirige al usuario a otra página web. Se trata del origen que redirige (remite) al usuario a la página web que se está solicitando.
X-Forwarded-For (XFF)	Opción del campo de encabezado de solicitud HTTP que conserva la dirección IP del usuario que ha solicitado la página web. Si tiene un servidor proxy en la red, el XFF le permite identificar la dirección IP del usuario que solicitó el contenido, en lugar de solo registrar la dirección IP del servidor proxy como dirección IP de origen que solicitó la página web.
Headers Inserted (Encabezados insertados)	El tipo de encabezado y el texto del encabezado que inserta el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Solicitud para cambiar la categoría de una URL

Si cree que una URL no se encuentra categorizada adecuadamente, puede solicitar que la categoricemos de manera diferente. Envíe una solicitud de cambio directamente en el cortafuegos o use Test A Site (Probar un sitio). Una solicitud de cambio activa PAN-DB, la nube de filtrado de URL, para hacer un análisis inmediato de la URL para la que sugiere un cambio de categoría. Si PAN-DB valida que la nueva sugerencia de categoría es precisa, se aprueba la solicitud de cambio. Si PAN-DB considera que la sugerencia de nueva categoría no es precisa, los editores humanos de investigación de amenazas y ciencia de datos de Palo Alto Networks revisan la solicitud de cambio.

Después de enviar una solicitud de cambio, recibirá un correo electrónico nuestro en el que se confirmará que hemos recibido su solicitud. Cuando completemos la investigación, recibirá un segundo correo electrónico con la confirmación de los resultados.

No puede solicitar cambiar la categoría de riesgo que recibe una URL (**high risk (riesgo alto)**, **medium risk (riesgo medio)** o **low risk (riesgo bajo)**) ni las URL clasificadas como **insufficient content (contenido insuficiente)** o **newly-registered domains (dominios recién registrados)**.

- Realización de una solicitud de cambio en línea
- Realización de una solicitud de cambio masivo
- Realización de una solicitud de cambio desde el cortafuegos

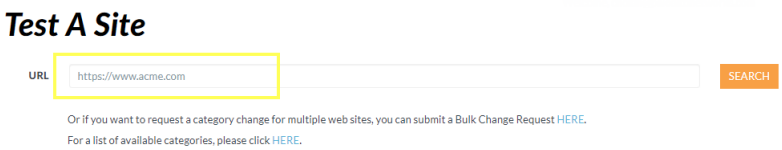
Realización de una solicitud de cambio en línea

Utilice la opción Test A Site (Probar un sitio) del filtrado de URL de Palo Alto Networks para realizar una solicitud de cambio en línea.

STEP 1 | Diríjase a Test A Site (Probar un sitio).

No es necesario iniciar sesión para enviar una solicitud de cambio, aunque deberá proporcionar su correo electrónico como parte del formulario de solicitud de cambio. Si decide no iniciar sesión, deberá realizar una prueba CAPTCHA para confirmar que es humano (inicie sesión para evitar la prueba CAPTCHA).

STEP 2 | Especifique una URL para comprobar las categorías:



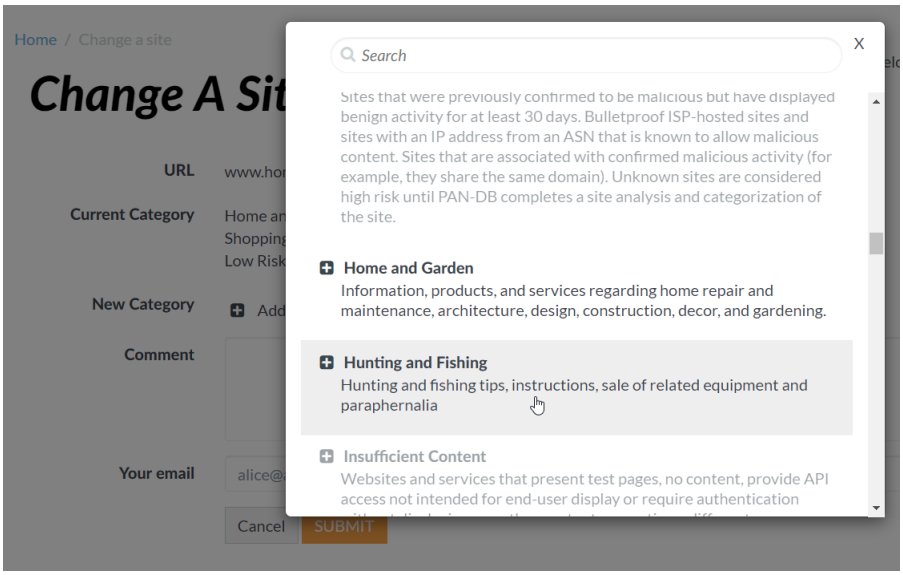
STEP 3 | Revise las categorías de URL y, si considera que no son precisas, seleccione **Request Change (Solicitar cambio)**.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Siga completando el formulario de solicitud de cambio y envíelo.

Incluya al menos una (y hasta dos) nuevas sugerencias de categoría y deje un comentario (opcional) para ofrecernos más información sobre su sugerencia.



Realización de una solicitud de cambio masivo

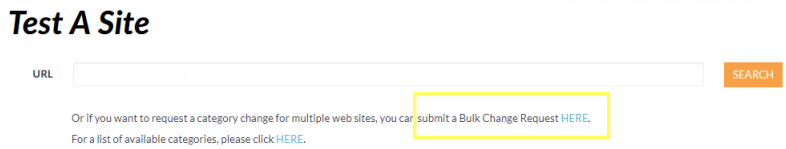
También puede usar Test A Site (Probar un sitio) para realizar una solicitud de cambio masivo si desea enviar solicitudes de cambio para varias URL a la vez.

STEP 1 | Diríjase a Test A Site (Probar un sitio).

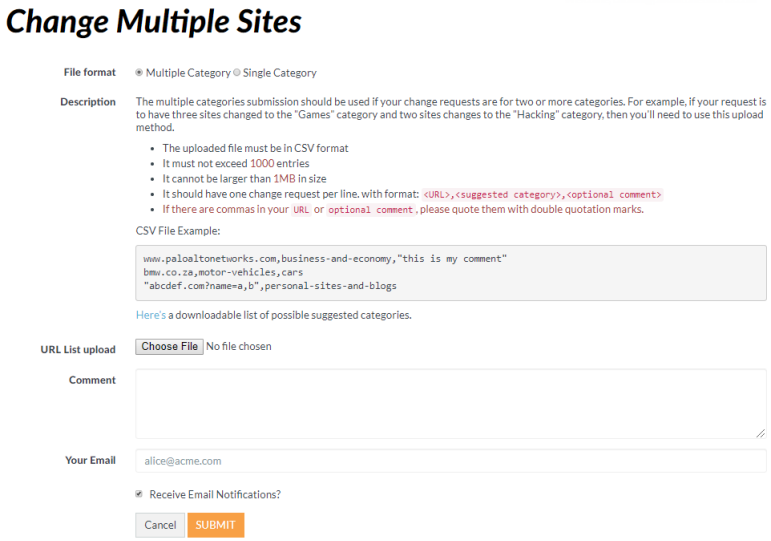
No es necesario iniciar sesión para realizar una solicitud de cambio; sin embargo, deberá proporcionar su correo electrónico para completar el formulario de solicitud de cambio. Si decide no iniciar sesión, deberá realizar una prueba CAPTCHA para confirmar que es humano (inicie sesión para evitar la prueba CAPTCHA).

STEP 2 | Elija la opción de enviar una solicitud de cambio masivo:

© 2020 Palo Alto Networks, Inc.



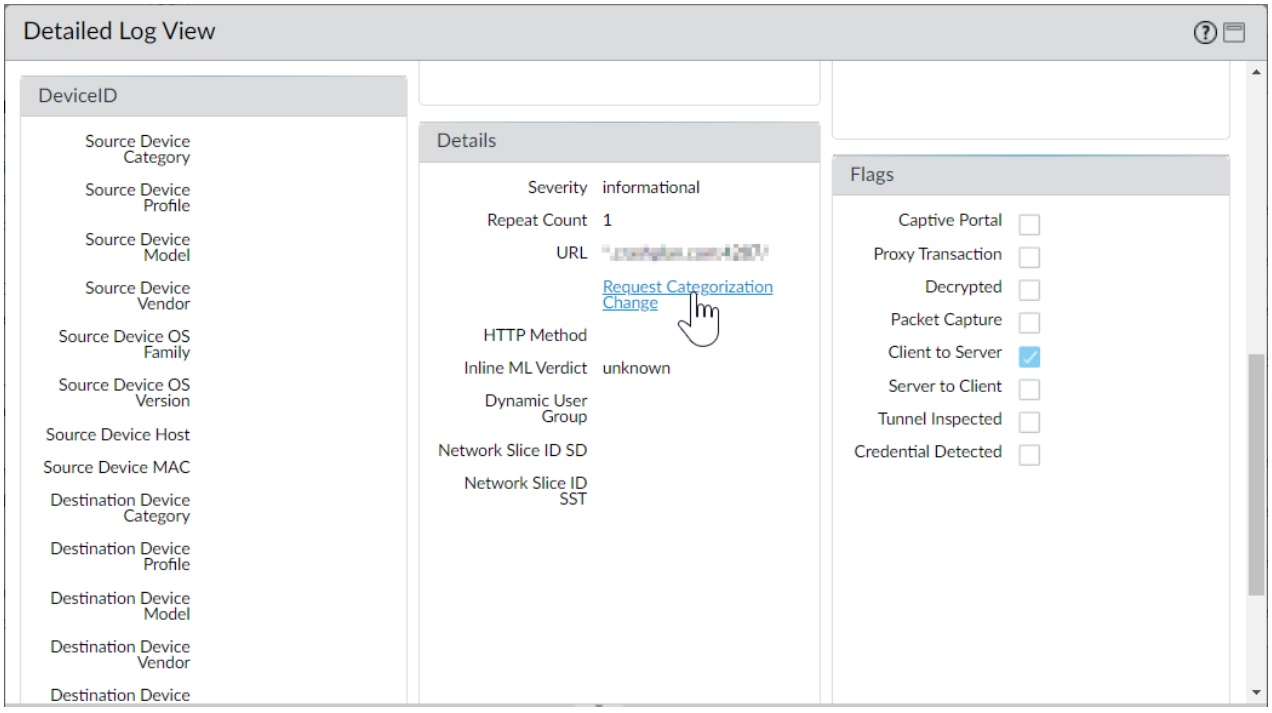
STEP 3 | Complete y envíe el formulario de solicitud de cambio masivo.



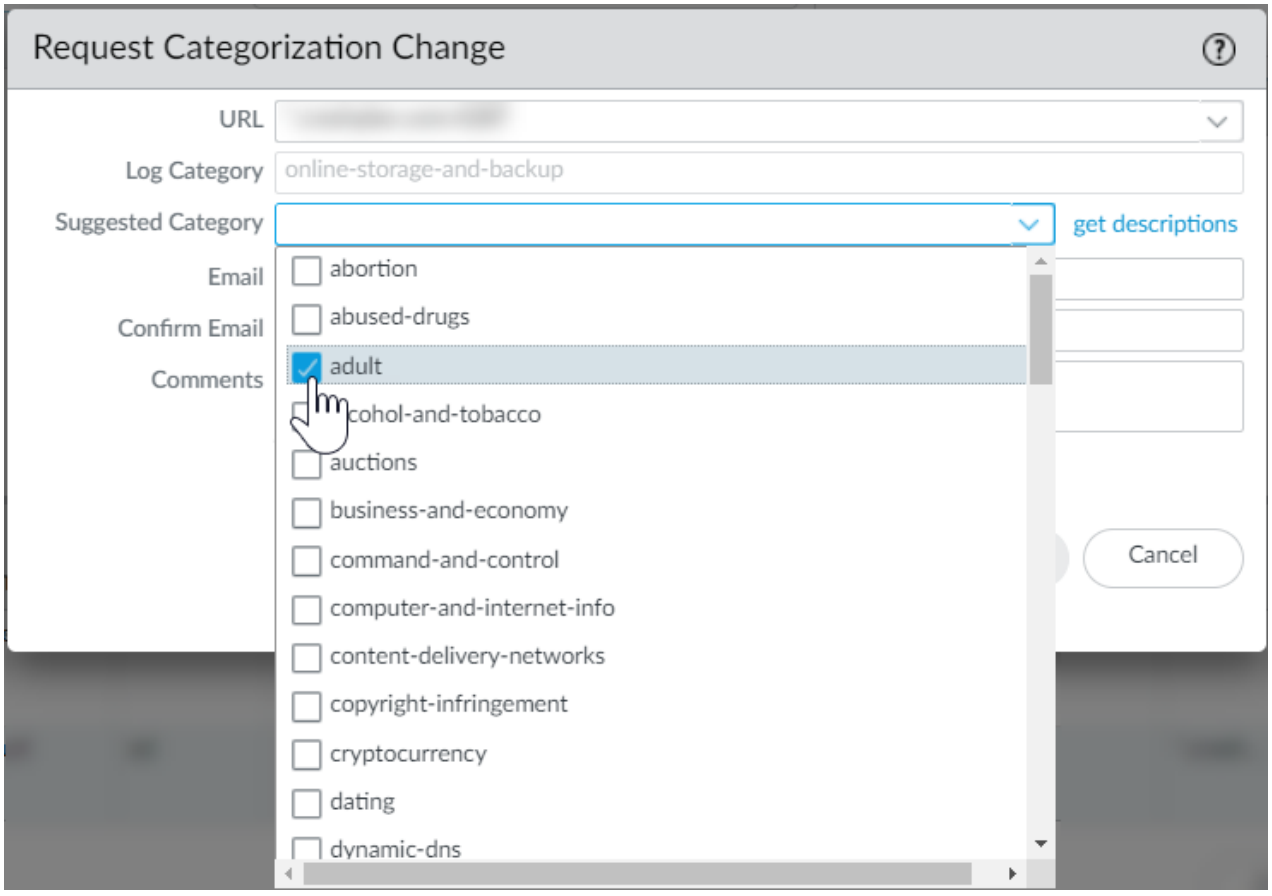
Realización de una solicitud de cambio desde el cortafuegos

También puede enviar una solicitud de cambio de categoría de URL directamente desde el cortafuegos. En los logs de filtrado de URL, los detalles para cada entrada de log incluyen una opción para **solicitar el cambio de categoría**(**Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**).

© 2020 Palo Alto Networks, Inc.



Puede completar el formulario de solicitud y enviarlo desde ahí.



© 2020 Palo Alto Networks, Inc.

Solución de problemas del filtrado de URL

En los siguientes temas se proporcionan directrices de solución de problemas para diagnosticar y resolver problemas comunes del filtrado de URL.

- Problemas en la activación de PAN-DB
- Problemas de conectividad con la nube de PAN-DB
- URL clasificadas como no resueltas
- Categorización incorrecta

Problemas en la activación de PAN-DB

Utilice el siguiente flujo de trabajo para solucionar los problemas de activación de PAN-DB.

STEP 1 | Acceda a la CLI de PAN-OS.

STEP 2 | Compruebe si PAN-DB se ha activado mediante la ejecución del siguiente comando:

```
show system setting url-database
```

Si la respuesta es `paloaltonetworks`, PAN-DB es el proveedor activo.

STEP 3 | Compruebe si el cortafuegos tiene una licencia de PAN-DB válida mediante la ejecución del siguiente comando:

```
request license info
```

Debería de ver la entrada de licencia `Feature (Función): PAN-DB URL Filtering`. Si la licencia no está instalada, deberá obtener e instalar una. Consulte Configuración de filtrado de URL.

STEP 4 | Compruebe el estado de la conexión en la nube de PAN-DB.

Problemas de conectividad con la nube de PAN-DB

Para comprobar la conectividad entre el cortafuegos y la nube de PAN-DB:

```
show url-cloud status
```

Si se puede acceder a la nube, la respuesta esperada es similar a la siguiente:

```
show url-cloud status
PAN-DB URL Filtering
License :                          valid
Current cloud server :             serverlist.urlcloud.paloaltonetworks.com
Cloud connection :                 connected
Cloud mode :                       public
URL database version - device :    20200624.20296
URL database version - cloud :     20200624.20296  ( last update time
 2020/06/24 12:39:19 )
URL database status :              good
URL protocol version - device :    pan/2.0.0
URL protocol version - cloud :     pan/2.0.0
Protocol compatibility status :    compatible
```

Si no se puede acceder a la nube, la respuesta esperada es similar a la siguiente:

© 2020 Palo Alto Networks, Inc.

```
show url-cloud status
PAN-DB URL Filtering
License :                          valid
Cloud connection :                 not connected
URL database version - device :    0000.00.00.000
URL protocol version - device :    pan/0.0.2
```

Utilice la siguiente lista de verificación para identificar y resolver problemas de conectividad:

- ¿Se muestra el campo de licencia de filtrado de URL de PAN-DB como no válido? Obtenga e instale una licencia válida de PAN-DB.
- ¿Se muestra la versión del protocolo de URL como no compatible? Actualice PAN-OS a la versión más reciente.
- ¿Puede enviar un ping al servidor de nube de PAN-DB desde el cortafuegos? Ejecute el siguiente comando para comprobarlo:

  ```
  ping source <ip-address> host serverlist.urlcloud.paloaltonetworks.com <
  ```

  Por ejemplo, si la dirección IP de su interfaz de gestión es 10.1.1.5, ejecute el siguiente comando:

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- ¿Se encuentra el cortafuegos en una configuración de HA? Compruebe que el estado de HA de los cortafuegos se encuentre en un estado activo, activo-principal o activo-secundario. El acceso a la nube de PAN-DB se bloqueará si el cortafuegos tiene un estado diferente: Ejecute el siguiente comando en cada cortafuegos del par para observar el estado:

  ```
  show high-availability state
  ```

Si aún tiene problemas de conectividad entre el cortafuegos y la nube de PAN-DB, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

URL clasificadas como no resueltas

Utilice el siguiente flujo de trabajo para solucionar problemas en los que algunas o todas las URL identificadas por PAN-DB se clasifican como no resueltas:

STEP 1 | Compruebe la conexión con la nube de PAN-DB mediante la ejecución del siguiente comando:

```
show url-cloud status
```

En el campo de conexión con la nube se debe mostrar `Conectado`. Si no se muestra `Conectado`, cualquier URL que no exista en la caché del plano de gestión se categoriza como `No resuelto`. Para solucionar este problema, consulte Problemas de conectividad con la nube de PAN-DB.

STEP 2 | Si el estado de conexión de la nube es **`Conectado`**, compruebe el uso actual del cortafuegos. Si el rendimiento del cortafuegos tiene picos, puede que las solicitudes de URL se descarten (puede que no lleguen al plano de gestión) y se categoricen como **`not-resolved`**.

Para ver los recursos del sistema, ejecute el siguiente comando y vea las columnas `%CPU` y `%MEM`:

```
show system resources
```

También puede ver los recursos del sistema en el widget System Resouces (Recursos del sistema) en el **Dashboard (Panel)** en la interfaz web.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Si el problema persiste, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

Categorización incorrecta

Es posible que, a veces, considere que algunas URL están categorizadas incorrectamente. Utilice el siguiente flujo de trabajo para determinar la categorización de una URL para un sitio y solicitar un cambio de categoría, de ser necesario.

STEP 1 | Compruebe la categoría en el plano de datos mediante la ejecución del siguiente comando:

```
show running url <URL>
```

Por ejemplo, para ver la categoría del sitio web de Palo Alto Networks, ejecute el siguiente comando:

```
show running url paloaltonetworks.com
```

Si la URL almacenada en la caché del plano de datos tiene la categoría correcta (información de equipo e internet en este ejemplo), la categorización es correcta y no es necesario realizar ninguna otra acción. Si la categoría no es correcta, vaya al paso siguiente.

STEP 2 | Compruebe la categoría en el plano de gestión mediante la ejecución del siguiente comando:

```
test url-info-host <URL>
```

Por ejemplo:

```
test url-info-host paloaltonetworks.com
```

Si la URL almacenada en la caché del plano de gestión tiene la categoría correcta, quite la URL de la caché del plano de datos mediante la ejecución del siguiente comando:

```
clear url-cache url <URL>
```

La próxima vez que el cortafuegos solicite la categoría de esta URL, la solicitud se reenviará al plano de gestión. Esto solucionará el problema y no será necesario realizar ninguna otra acción. Si esto no soluciona el problema, vaya al paso siguiente para comprobar la categoría de URL en los sistemas de la nube.

STEP 3 | Compruebe la categoría en la nube mediante la ejecución del siguiente comando:

```
test url-info-cloud <URL>
```

STEP 4 | Si la URL almacenada en la nube tiene la categoría correcta, quite la URL de las cachés del plano de datos y el plano de gestión.

Ejecute el siguiente comando para eliminar una URL de la caché del plano de datos:

```
clear url-cache url <URL>
```


© 2020 Palo Alto Networks, Inc.

Ejecute el siguiente comando para eliminar una URL de la caché del plano de gestión:

```
delete url-database url <URL>
```

La próxima vez que el cortafuegos solicite la categoría de la URL dada, la solicitud se reenviará al plano de gestión y, a continuación, a la nube. Esto debería solucionar el problema de búsqueda de categoría. Si el problema persiste, consulte el paso siguiente para enviar una solicitud de cambio de categorización.

STEP 5 | Para enviar una solicitud de cambio desde la interfaz web, vaya al log de URL y seleccione la entrada de log para la URL que desee cambiar.

STEP 6 | Haga clic en el enlace **Request Categorization (Solicitar cambio de categorización)** y siga las instrucciones. Además, para solicitar un cambio de categoría en el sitio web Test A Site (en inglés) de Palo Alto Networks, busque la URL y, a continuación, haga clic en el icono **Request Change (Solicitar cambio)**. Para ver una lista de todas las categorías disponibles con descripciones para cada categoría, consulte https://urlfiltering.paloaltonetworks.com/CategoryList.aspx.

Si la solicitud de cambio se aprueba, recibirá una notificación por correo electrónico. A continuación, tiene dos opciones para asegurarse de que la categoría de URL se actualiza en el cortafuegos:

- Espere hasta que la URL de la caché caduque y la próxima vez que un usuario acceda a la URL, la actualización de la nueva categorización se incluirá en la caché.
- Ejecute el siguiente comando para forzar la actualización en la caché:

```
request url-filtering update url <URL>
```


© 2020 Palo Alto Networks, Inc.

Nube privada de PAN-DB

La nube privada de PAN-DB es una solución local para las organizaciones que restringen el uso de los servicios en la nube. Con esta solución instalada, puede implementar uno o más dispositivos M-600 como servidores de PAN-DB en su red o centro de datos. Los cortafuegos piden a la nube privada de PAN-DB que realice búsquedas de URL, en lugar de acceder a la nube pública de PAN-DB.

El proceso para realizar búsquedas de URL, tanto en la nube privada como en la pública, es el mismo para los cortafuegos de la red. De manera predeterminada, el cortafuegos está configurado para acceder a la nube pública de PAN-DB. Si implementa una nube privada de PAN-DB, debe configurar los cortafuegos con una lista de direcciones IP o FQDN para acceder al servidor o los servidores en la nube privada.

Los cortafuegos que ejecuten PAN-OS 5.0 o versiones posteriores pueden comunicarse con la nube privada de PAN-DB.

Cuando realice el procedimiento Configuración de la nube privada de PAN-DB, puede configurar los dispositivos M-600 de modo que tengan acceso directo a internet o se mantengan completamente fuera de línea. Dado que el dispositivo M-600 requiere actualizaciones de base de datos y contenido para realizar búsquedas de URL, si el dispositivo no tiene una conexión activa a Internet, deberá descargar manualmente las actualizaciones en un servidor de su red e importar las actualizaciones con SCP en cada dispositivo M-600 de la nube privada de PAN-DB. Además, los dispositivos deben poder obtener la base de datos de valores de inicialización y cualquier otra actualización de contenido normal o crítica de los cortafuegos a los que atiende.

Para autenticar los cortafuegos que conectan con la nube privada de PAN-DB, un conjunto de certificados de servidor predeterminado se empaquetan con el dispositivo; no puede importar ni usar otro certificado de servidor para autenticar los cortafuegos. Si cambia el nombre de host del dispositivo M-600, el dispositivo genera automáticamente un nuevo conjunto de certificados para autenticar los cortafuegos.

- Dispositivo M-600 para la nube privada de PAN-DB
- Configuración de la nube privada de PAN-DB

Dispositivo M-600 para la nube privada de PAN-DB

Para implementar una nube privada de PAN-DB, necesita uno o más dispositivos M-600. El dispositivo M-600 se envía en modo Panorama, y para implementarse como nube privada de PAN-DB debe configurarse para funcionar en el modo PAN-URL-DB. En el modo PAN-URL-DB, el dispositivo ofrece los servicios de categorización de URL para empresas que no desean usar la nube pública de PAN-DB.

El dispositivo M-600, cuando se implementa como una nube privada de PAN-DB, usa dos puertos, MGT (Eth0) y Eth1; Eth2 no está disponible para su uso. El puerto de gestión se usa para el acceso administrativo al dispositivo y para obtener las últimas actualizaciones de contenido desde la nube pública de PAN-DB o desde un servidor de su red. Para una comunicación entre la nube privada de PAN-DB y los cortafuegos de la red, puede usar el puerto MGT o Eth1.

El dispositivo M-200 no se puede implementar como una nube privada de PAN-DB.

El dispositivo M-600 en modo PAN-URL-DB:

- No tiene una interfaz web, solo admite una interfaz de línea de comandos (CLI).
- No puede ser gestionado por Panorama.
- No puede implementarse en un clúster en alta disponibilidad (HA).
- No requiere una licencia de filtrado de URL. Los cortafuegos deben tener una licencia de PAN-DB URL Filtering para conectar con la nube privada de PAN-DB y consultarla.

© 2020 Palo Alto Networks, Inc.

- Se envía con un conjunto de certificados de servidor predeterminados que se usan para autenticar los cortafuegos que se conectan con la nube privada de PAN-DB. No puede importar ni usar otro certificado de servidor para autenticar los cortafuegos. Si cambia el nombre de host del dispositivo M-600, el dispositivo genera automáticamente un nuevo conjunto de certificado para autenticar los cortafuegos a los que atiende.
- Solo se puede restablecer al modo Panorama. Si desea implementar el dispositivo como recopilador de logs dedicado, cambie al modo Panorama y defínalo en el modo de recopilador de logs.

Table 4: Diferencias entre la nube pública de PAN-DB y la nube privada de PAN-DB

Diferencias	Nube pública de PAN-DB	Nube privada de PAN-DB
Actualizaciones de contenido y base de datos	Las actualizaciones de contenido (normales y críticas) y las actualizaciones de bases de datos completas se publican varias veces al día. La nube pública PAN-DB actualiza el estado de malware y phishing en las categorías de URL cada cinco minutos. El cortafuegos busca actualizaciones críticas siempre que consulta a los servidores de nubes para búsquedas de URL.	Las actualizaciones de contenido y las actualizaciones de bases de datos de URL completas están disponibles una vez al día durante la semana.
Solicitudes de categorización de URL	Envíe solicitudes de cambio de categorización de URL usando las siguientes opciones: • Sitio web de comprobación de sitios de Palo Alto Networks. • Página de configuración de perfil de filtrado de URL en el cortafuegos. • Log de filtrado de URL en el cortafuegos.	Envíe sus solicitudes de cambio de categorización de URL usando únicamente el sitio web de comprobación de sitios de Palo Alto Networks.
Consultas URL sin resolver	Si el cortafuegos no puede resolver una consulta de URL, la solicitud se envía a los servidores en la nube pública.	Si el cortafuegos no puede resolver una consulta, la solicitud se envía al dispositivo M-600 en la nube privada de PAN-DB. Si no hay coincidencia para la URL, la nube privada de PAN-DB envía una respuesta de categoría *desconocida* al cortafuegos; la solicitud no se envía a la nube pública a no ser que haya configurado el dispositivo M-600 para acceder a la nube pública de PAN-DB. Si los dispositivos M-600 que constituyen su nube privada de PAN-DB se configuran para estar completamente fuera de línea, no enviará ningún dato o análisis a la nube pública.

© 2020 Palo Alto Networks, Inc.

Configuración de la nube privada de PAN-DB

Para implementar uno o más dispositivos M-600 como una nube privada de PAN-DB en su red o centro de datos, debe completar las siguientes tareas:

- Configuración de la nube privada de PAN-DB
- Configuración de los cortafuegos para acceder a la nube privada de PAN-DB.
- Configuración de la autenticación con certificados personalizados en la nube privada de PAN-DB.

Configuración de la nube privada de PAN-DB

STEP 1 | Monte en rack el dispositivo M-600.

Consulte la M-600 Hardware Reference Guide (Guía de referencia de hardware de M-600) para obtener instrucciones.

STEP 2 | Registre el dispositivo M-600.

Si desea instrucciones sobre el registro del dispositivo M-600, consulte Registro del cortafuegos.

STEP 3 | Realice la configuración inicial del dispositivo M-600.

El dispositivo M-600 del modo PAN-DB usa dos puertos MGT (Eth0) y Eth1; Eth2 no se usa en el modo PAN-DB. El puerto de gestión se usa para el acceso administrativo al dispositivo y para obtener las últimas actualizaciones de contenido desde la nube pública de PAN-DB. Para una comunicación entre el dispositivo (servidor PAN-DB) y los cortafuegos de la red, puede usar el puerto MGT o Eth1.

1. Conéctese al dispositivo M-600 de uno de estos modos:
   - Conecte un cable serie desde un ordenador al puerto de la consola del dispositivo M-600 y conecte usando un software de emulación de terminal (9600-8-N-1).
   - Conecte un cable Ethernet RJ-45 desde un ordenador hasta el puerto MGT del dispositivo M-600. En un navegador, vaya a https://192.168.1.1. Para habilitar el acceso a esta URL tal vez deba cambiar la dirección IP del ordenador por una dirección de la red 192.168.1.0 (por ejemplo, 192.168.1.2).
2. Cuando se le indique, inicie sesión en el dispositivo. Inicie sesión usando el nombre de usuario y contraseña predeterminados (admin/admin). El dispositivo comenzará a inicializarse.
3. Configure los ajustes de acceso a la red, incluida la dirección IP para la interfaz MGT:

```
set deviceconfig system ip-address  <server-IP> netmask <netmask> default-
gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

   donde <*server-IP*> es la dirección IP que desea asignar a la interfaz de gestión del servidor, <*netmask*> es la máscara de subred, <*gateway-IP*> es la dirección IP de la puerta de enlace de red y <*DNS-IP*> es la dirección IP del servidor DNS principal.
4. Configure los ajustes de acceso a la red, incluida la dirección IP para la interfaz Eth1:

```
set deviceconfig system eth1 ip-address  <server-IP> netmask <netmask>
 default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

   donde <*server-IP*> es la dirección IP que quiere asignar a la interfaz de datos del servidor , <*netmask*> es la máscara de subred, <*gateway-IP*> es la dirección IP del gateway de red y <*DNS-IP*> es la dirección IP del servidor DNS.

© 2020 Palo Alto Networks, Inc.

5. Guarde sus cambios en el servidor PAN-DB.

   commit

STEP 4 | Cambie al modo de nube privada de PAN-DB.

1. Para cambiar al modo PAN-DB, use el siguiente comando de la CLI:

```
request system system-mode pan-url-db
```

   Puede cambiar del modo Panorama al modo PAN-DB y viceversa; y del modo Panorama al modo de recopilador de logs y viceversa. No se permite cambiar directamente desde el modo PAN-DB al modo de recopilador de logs ni viceversa. Cuando cambie el modo operativo, se activa un reinicio de datos. Con la excepción de los ajustes de acceso de gestión, todos los logs y la configuración existente se eliminarán en el reinicio.

2. Use los comandos siguientes para comprobar que el modo ha cambiado:

```
show pan-url-cloud-status
hostname: M-600
ip-address: 1.2.3.4
netmask: 255.255.255.0
default-gateway: 1.2.3.1
ipv6-address: unknown
ipv6-link-local-address: fe80:00/64
ipv6-default-gateway:
mac-address: 00:56:90:e7:f6:8e
time: Mon Apr 27 13:43:59 2015
uptime: 10 days, 1:51:28
family: m
model: M-600
serial: 0073010000xxx
sw-version: 7.0.0
app-version: 492-2638
app-release-date: 2015/03/19  20:05:33
av-version: 0
av-release-date: unknown
wf-private-version: 0
wf-private-release-date: unknown
logdb-version: 7.0.9
platform-family: m
pan-url-db: 20150417-220
system-mode: Pan-URL-DB
operational-mode: normal
```

3. Utilice el siguiente comando para comprobar la versión de la base de datos de la nube en el dispositivo:

```
show pan-url-cloud-status
Cloud status:            Up
URL database version:    20150417-220
```

STEP 5 | Instale las actualizaciones de contenido y base de datos.

El dispositivo solo almacena la versión en ejecución actualmente del contenido y una versión anterior.

© 2020 Palo Alto Networks, Inc.

Seleccione uno de los siguientes métodos de instalación de las actualizaciones de contenido y base de datos:

- Si el servidor PAN-DB tiene acceso directo a Internet, use los siguientes comandos:
  1. Para comprobar si se ha publicado una nueva versión use:

     request pan-url-db upgrade check
  2. Para consultar qué versión tiene instalada actualmente en su servidor use:

     request pan-url-db upgrade info
  3. Para descargar e instalar la última versión:
     - **request pan-url-db upgrade download latest**
     - **request pan-url-db upgrade install** *<version latest | file>*
  4. Para programar el dispositivo M-600 para que busque automáticamente actualizaciones:

     set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week *<day of week>* at *<hr:min>*
- Si el servidor PAN-DB está fuera de línea, acceda al sitio web de asistencia técnica de Palo Alto Networks para descargar y guardar las actualizaciones de contenido en un servidor SCP en su red. Entonces podrá importar e instalar las actualizaciones usando los siguientes comandos:
  - **scp import pan-url-db remote-port** *<port-number>* from username@host:path
  - **request pan-url-db upgrade install file** *<filename>*

STEP 6 | Configuración del acceso administrativo a la nube privada de PAN-DB.



El dispositivo tiene una cuenta `admin` *predeterminada. Cualquier usuario administrativo adicional que cree puede ser un superusuario (con acceso completo) o superusuario con acceso de solo lectura.*

La nube privada de PAN-DB no admite el uso de VSA de RADIUS. Si los VSA empleados en el cortafuegos o Panorama se usan para habilitar el acceso a la nube privada de PAN-DB, se producirá un fallo de autenticación.

- Para definir un usuario administrativo local del servidor PAN-DB:
  1. **configure**
  2. **set mgt-config users** *<username>* permissions role-based <superreader | superuser> yes
  3. **set mgt-config users** *<username>* password
  4. **Enter password:xxxxx**
  5. **Confirm password:xxxxx**
  6. **commit**
- Para definir un usuario administrativo con la autenticación RADIUS:
  1. Cree un perfil de servidor RADIUS.

© 2020 Palo Alto Networks, Inc.

```
set shared server-profile radius  <server_profile_name>
 server <server_name> ip-address <ip_address> port <port_no>
 secret <shared_password>
```

2. Cree un perfil de autenticación.

```
set shared authentication-profile  <auth_profile_name> user-
domain <domain_name_for_authentication> allow-list <all> method radius
 server-profile <server_profile_name>
```

3. Adjunte el perfil de autenticación al usuario.

```
set mgt-config users  <username> authentication-
profile <auth_profile_name>
```

4. Confirme los cambios.

   commit

- Para ver la lista de usuarios:

```
show mgt-config users
users {
admin {
phash fnRL/G5lXVMug;
permissions {
role-based {
superuser yes;
}
}
}
admin_user_2 {
permissions {
role-based {
superreader yes;
}
}
authentication-profile RADIUS;
}
}
```

STEP 7 | Configure los cortafuegos para acceder a la nube privada de PAN-DB.

Configuración de los cortafuegos para acceder a la nube privada de PAN-DB.

Cuando usa la nube pública de PAN-DB, cada cortafuegos accede a los servidores PAN-DB en la nube AWS para descargar la lista de servidores elegibles con los que pueda conectar para las búsquedas de URL. Con la nube privada de PAN-DB, debe configurar los cortafuegos con una lista (estática) de sus servidores de nube privada de PAN-DB que se usarán para las búsquedas de URL. La lista puede contener hasta 20 entradas; se admiten las direcciones IPv4, direcciones IPv6 y FQDN. Cada entrada de la lista (dirección IP o FQDN) debe asignarse al puerto de gestión y/o eth1 del servidor PAN-DB.

STEP 1 | Seleccione una de las siguientes opciones en función de la versión de PAN-OS del cortafuegos.

- Para cortafuegos que ejecuten PAN-OS 7.0, acceda alCLI de PAN-OS o la interfaz web del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Use el comando siguiente de la CLI para configurar el acceso a la nube privada:

```
set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
 enable
```

O en la interfaz web de cada cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID**, edite la sección URL Filtering (Filtrado de URL) e introduzca la dirección IP o FQDN del **PAN-DB Server (Servidor PAN-DB)**. La lista debe estar separada por comas.

- Con los cortafuegos que ejecuten PAN-OS 5.0, 6.0 o 6.1, use el siguiente comando de la CLI para el configurar acceso a la nube privada:

```
debug device-server pan-url-db cloud-static-list-enable <IP addresses>
 enable
```

Para eliminar las entradas de los servidores de PAN-DB privados, y permitir que los cortafuegos se conecten con la nube pública de PAN-DB, use el comando:

```
set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
 disable
```

Cuando elimine la lista de servidores de PAN-DB privados, se activará un proceso de reelección en el cortafuegos. El cortafuegos comprueba en primer lugar la lista de servidores de la nube privada de PAN-DB y, cuando no puede encontrar uno, el cortafuegos accede a los servidores PAN-DB en la nube AWS para descargar la lista de servidores elegibles con los que pueda conectar.

STEP 2 | **Commit (Confirmar)** los cambios.

STEP 3 | Para verificar que el cambio es efectivo, use el siguiente comando de la CLI en el cortafuegos:

```
show url-cloud-status
Cloud status:            Up
URL database version:    20150417-220
```

Configuración de la autenticación con certificados personalizados en la nube privada de PAN-DB.

De forma predeterminada, un servidor PAN-DB utiliza certificados predefinidos para la autenticación mutua a fin de establecer las conexiones SSL utilizadas para el acceso de gestión y la comunicación entre dispositivos. Sin embargo, puede configurar la autenticación con certificados personalizados en su lugar. Los certificados personalizados le permiten establecer una cadena de confianza única que garantiza la autenticación mutua entre su servidor PAN-DB y sus cortafuegos. En el caso de la nube privada de PAN-DB, el cortafuegos actúa como el cliente y el servidor PAN-DB actúa como el servidor.

STEP 1 | Obtenga pares de claves y certificados de una entidad de certificación (certificate authority, CA) para el servidor PAN-DB y el cortafuegos.

STEP 2 | Importe el certificado de CA para validar el certificado en el cortafuegos.

1. Inicie sesión en la CLI en el servidor PAN-DB e ingrese al modo de configuración.

```
admin@M-600> configure
```


© 2020 Palo Alto Networks, Inc.

2. Utilice TFTP o SCP para importar el certificado de CA.

```
admin@M-600# {tftp | scp} import certificate from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-name <value>
 passphrase <value> format {pkcs12 | pem}
```

STEP 3 | Utilice TFTP o SCP para importar el par de claves que contiene el certificado del servidor y la clave privada para el dispositivo PAN-DB M-600.

```
admin@M-600# {tftp | scp} import keypair from <value> file <value> remote-
port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase
 <value> format {pkcs12 | pem}
```

STEP 4 | Configure un perfil de certificados que incluya la CA de raíz y la CA intermedia. Este perfil de certificado define la autenticación del dispositivo entre el servidor PAN-DB y el cortafuegos.

1. En la CLI del servidor PAN-DB, ingrese al modo de configuración.

```
admin@M-600> configure
```

2. Asigne un nombre al perfil de certificado.

```
admin@M-600# set shared certificate-profile <name>
```

3. (Opcional) Configure el dominio del usuario.

```
admin@M-600# set shared certificate-profile <name> dominio <value>
```

4. Configure la CA.

   Default-ocsp-url *y* ***ocsp-verify-cert*** *son parámetros opcionales.*

   admin@M-600# **set shared certificate-profile <name> CA <name>**

```
admin@M-600# set shared certificate-profile <name> CA <name> [default-
ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name> [ocsp-verify-
cert <value>]
```

STEP 5 | Configure un perfil SSL/TLS para el dispositivo PAN-DB M-600. Este perfil define el certificado y el alcance del protocolo que utilizan PAN-DB y los dispositivos cliente para los servicios SSL/TLS.

1. Identifique el perfil SSL/TLS.

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. Seleccione el certificado.

```
admin@M-600# set shared ssl-tls-service-profile <name> certificado <value>
```


© 2020 Palo Alto Networks, Inc.

3. Defina el alcance de SSL/TLS.

   PAN-OS 8.0 y las versiones posteriores admiten únicamente TLS 1.2 y las versiones posteriores. Debe establecer la versión máxima en TLS 1.2 o max (máximo).

```
admin@M-600# set shared ssl-tls-service-profile <name> protocol-settings
 min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name> protocol-settings
 max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | Configure la comunicación segura del servidor en PAN-DB.

1. Establezca el perfil SSL/TLS. Este perfil de servicio SSL/TLS se aplica a todas las conexiones SSL entre PAN-DB y los cortafuegos.

```
admin@M-600# set deviceconfig setting management secure-conn-server ssl-
tls-service-profile <ssltls-profile>
```

2. Establezca el perfil de certificado.

```
admin@M-600# set deviceconfig setting management secure-conn-server
 certificate-profile <certificate-profile>
```

3. Establezca el tiempo de espera de desconexión en el número de minutos que PAN-DB debe esperar antes de interrumpir y restablecer la conexión con el cortafuegos (el intervalo es de 0 a 44 640).

```
admin@M-600# set deviceconfig setting management secure-conn-server
 disconnect-wait-time <0-44640
```

STEP 7 | Importe el certificado de CA para validar el certificado en el dispositivo PAN-DB M-600.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Importe el certificado de CA.

STEP 8 | Configure un certificado local o de SCEP para el cortafuegos.

1. Si está utilizando un certificado local, realice la Importación de un par de claves al cortafuegos.
2. Si está utilizando un certificado de SCEP para el cortafuegos, realice la Configuración de un perfil SCEP.

STEP 9 | Configure el perfil de certificado para el cortafuegos. Puede configurar esto en cada cortafuegos individualmente o puede enviar esta configuración desde Panorama a los cortafuegos como parte de una plantilla.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)** para los cortafuegos o **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** para Panorama.
2. Configuración de un perfil de certificado.

STEP 10 | Implemente certificados personalizados en cada cortafuegos. Puede implementar los certificados centralmente desde Panorama o configurarlos manualmente en cada cortafuegos.

1. Inicie sesión en la interfaz web del cortafuegos.

© 2020 Palo Alto Networks, Inc.

2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** para un cortafuegos o **Panorama** > **Setup (Configuración)** > **Management (Gestión)** para Panorama y haga clic en **Edit (Editar)** para editar Secure Communication (Comunicación segura).
3. Seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)** del menú desplegable correspondiente.
4. En los ajustes Customize Communication (Personalizar comunicación), seleccione **PAN-DB Communication (Comunicación con PAN-DB)**.
5. Haga clic en **OK (Aceptar)**.
6. **Commit (Confirmar)** los cambios.

Tras confirmar los cambios, el cortafuegos no finaliza las sesiones actuales con el servidor PAN-DB hasta después del **Disconnect Wait Time (Tiempo de espera de desconexión)**. El tiempo de espera de desconexión comienza la cuenta atrás después de que aplique la utilización de certificados personalizados en el próximo paso.

STEP 11 | Después de implementar certificados personalizados en todos los cortafuegos, aplique la autenticación de certificados personalizados.

1. Inicie sesión en la CLI en el servidor PAN-DB e ingrese al modo de configuración.

```
admin@M-600> configure
```

2. Aplique la utilización de certificados personalizados.

```
admin@M-600# set deviceconfig setting management secure-conn-server
 disable-pre-defined-cert yes
```

Después de confirmar este cambio, el tiempo de espera de desconexión comienza la cuenta atrás (si configuró los ajustes en PAN-DB). Cuando el tiempo de espera finaliza, PAN-DB y su cortafuegos se conectan utilizando únicamente los certificados configurados.

STEP 12 | Existen dos opciones cuando añade nuevos cortafuegos o Panorama a su implementación de nube privada de PAN-DB.

- Si no habilitó **Custom Certificates Only (Solo certificados personalizados)**, puede añadir un nuevo cortafuegos a la nube privada de PAN-DB e implementar el certificado personalizado como se describe previamente.
- Si habilitó la opción **Custom Certificates Only (Solo certificados personalizados)** en la nube privada de PAN-DB, debe implementar los certificados personalizados en los cortafuegos antes de conectarlos a la nube privada de PAN-DB.

Calidad de servicio

La calidad de servicio (QoS) es un conjunto de tecnologías que se utilizan en una red para garantizar su capacidad de ejecutar de manera fiable aplicaciones de alta prioridad y tráfico bajo una capacidad de red limitada. Para lograr su cometido, las tecnologías de QoS ofrecen gestión diferenciada y asignación de capacidad a flujos específicos del tráfico de red. Esto permite que el administrador de red asigne el orden en que se gestiona el tráfico y la cantidad de ancho de banda permitida para el tráfico.

La calidad de servicio (QoS) de aplicaciones de Palo Alto Networks ofrece un QoS básica aplicada a redes y la amplía para proporcionar QoS a aplicaciones y usuarios.

Utilice los siguientes temas para obtener información sobre el QoS basado en aplicaciones de Palo Alto Networks y configurarlo:

- Descripción general del QoS
- Conceptos de QoS
- Configuración de QoS
- Configuración de QoS para un sistema virtual
- Aplicación forzada de QoS basada en la clasificación DSCP
- Casos de uso de QoS

Utilice la herramienta de comparación de productos de Palo Alto Networks para ver las funciones de QoS que admite su modelo de cortafuegos. Seleccione dos o más modelos de productos y haga clic en **Compare Now (Comparar ahora)** para ver la compatibilidad de las funciones de QoS para cada modelo (por ejemplo, puede comprobar si su modelo de cortafuegos admite QoS en subinterfaces y, de ser así, la cantidad máxima de subinterfaces en las que se puede habilitar QoS).

Se admite el uso de QoS con las interfaces de Ethernet de agregación (Aggregate Ethernet, AE) en los cortafuegos PA-7000 Series, PA-5200 Series y PA-3200 Series que ejecuten PAN-OS 7.0 o versiones posteriores.

© 2020 Palo Alto Networks, Inc.

Descripción general del QoS

Utilice el QoS para establecer la prioridad y ajustar los aspectos de calidad del tráfico de red. Puede asignar el orden en el que se gestionan los paquetes y adjudicar el ancho de banda, garantizando la aplicación del tratamiento preferido y los niveles óptimos de rendimiento al tráfico, aplicaciones y usuarios seleccionados.

Las medidas de calidad de servicio sujetas a una implementación de QoS son el ancho de banda (tasa de transferencia máxima), el rendimiento (tasa de transferencia real), la latencia (retraso) y la vibración (varianza en latencia). La capacidad de moldear o controlar estas medidas de calidad de servicio hace que el QoS sea de especial importancia para el ancho de banda alto, el tráfico en tiempo real como la voz sobre IP (VoIP), las videoconferencias y el vídeo bajo demanda con una alta sensibilidad a la latencia y la vibración. Asimismo, utilice QoS para lograr resultados como los siguientes:

- Establezca la prioridad del tráfico de red y aplicaciones, garantizando una alta prioridad para el tráfico importante o limitando el tráfico no esencial.
- Logre un ancho de banda equivalente compartiendo diferentes subredes, clases o usuarios en una red.
- Asigne el ancho de banda externa o internamente o de ambas formas, aplicando QoS tanto al tráfico de carga como al de descarga o solamente al tráfico de carga o al de descarga.
- Garantice una baja latencia para el tráfico generador de ingresos y de clientes en un entorno empresarial.
- Realice la generación de perfiles de tráfico de aplicaciones para garantizar el uso del ancho de banda.

La implementación de QoS en un cortafuegos de Palo Alto Networks comienza con tres componentes de configuración principales que admiten una solución completa de QoS: un perfil de QoS, una política de QoS y la configuración de la interfaz de salida de QoS. Cada una de estas opciones de la tarea de configuración de QoS facilita un proceso más amplio que optimiza y establece la prioridad del flujo de tráfico y asigna y garantiza el ancho de banda de acuerdo con los parámetros configurables.

La figura QoS Traffic Flow (Flujo de tráfico de QoS) muestra el tráfico a medida que se desplaza desde el origen, el cortafuegos con el QoS habilitada lo moldea y, por último, recibe una prioridad y se entrega en su destino.

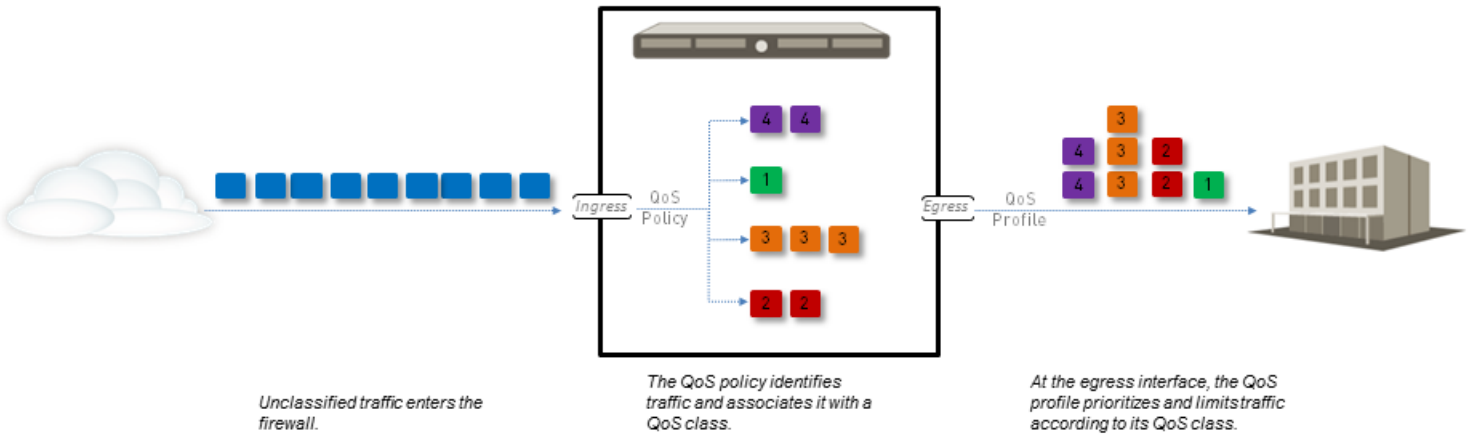


Figure 7: flujo de tráfico de QoS

Las opciones de configuración de QoS le permiten controlar el flujo de tráfico y definirlo en puntos diferentes del flujo. La figura QoS Traffic Flow (Flujo de tráfico de QoS) indica en qué lugar las opciones configurables definen el flujo de tráfico. Una regla de política QoS le permite definir el tráfico que desea que reciba tratamiento QoS y asignar a ese tráfico una clase QoS. Entonces, el tráfico coincidente se modela en función de los ajustes de la clase de perfil QoS a medida que sale de la interfaz física.

© 2020 Palo Alto Networks, Inc.

Los componentes de configuración de QoS influyen unos en otros y las opciones de configuración de QoS se pueden utilizar para crear una implementación de QoS completa y detallada, o se pueden utilizar con moderación con un mínimo de acciones del administrador.

Cada modelo de cortafuegos admite un número máximo de puertos que se puede configurar con QoS. Consulte la hoja de especificaciones de su modelo de cortafuegos o utilice la herramienta de comparación de productos para ver la compatibilidad de las funciones de QoS de dos o más cortafuegos en una única página.

© 2020 Palo Alto Networks, Inc.

Conceptos de QoS

Utilice los siguientes temas para obtener información sobre los diferentes componentes y mecanismos de una configuración de QoS en un cortafuegos de Palo Alto Networks:

- QoS para aplicaciones y usuarios
- Política de QoS
- Perfil de QoS
- Clases de QoS
- Establecimiento de colas de prioridad de QoS
- Gestión del ancho de banda de QoS
- Interfaz de salida de QoS
- QoS para texto no cifrado y tráfico de túnel

QoS para aplicaciones y usuarios

Un cortafuegos de Palo Alto Networks proporciona una QoS básica, que controla el tráfico saliente del cortafuegos de acuerdo con la red o la subred y amplía la capacidad de la QoS para también clasificar y moldear el tráfico de acuerdo con la aplicación y el usuario. El cortafuegos de Palo Alto Networks ofrece esta capacidad integrando las funciones App-ID y User-ID con la configuración de QoS. Las entradas de App-ID y User-ID que existen para identificar aplicaciones y usuarios específicos de su red están disponibles en la configuración de QoS para que pueda especificar fácilmente aplicaciones y usuarios para los cuales desea gestionar o garantizar el ancho de banda.

Política de QoS

Use una regla de políticas de QoS para definir si el tráfico recibe tratamiento QoS (ya sea preferente o de limitación de ancho de banda) y si se le asigna a dicho tráfico una clase de servicio de QoS.

Defina una regla de políticas de QoS que coincida con el tráfico basándose en:

- Aplicaciones y grupos de aplicaciones.
- Zonas de origen, direcciones de origen y usuarios de origen.
- Zonas de destino y direcciones de destino.
- Servicios y grupos de servicios limitados a números de puertos TCP o UDP concretos.
- Categorías de URL, incluidas categorías de URL personalizadas.
- Los valores de Punto de código de servicios diferenciados (DSCP) y Tipo de servicio (ToS) se utilizan para indicar el nivel de servicio solicitado para el tráfico, como la prioridad alta o la entrega de la mejor opción.

Configure varias reglas de políticas de QoS (**Policies [Políticas]** > **QoS**) para asociar diferentes tipos de tráfico a diferentes Clases de QoS de servicio.

Puesto que QoS se aplica al tráfico cuando sale del cortafuegos, su regla de políticas de QoS se aplica al tráfico después de que el cortafuegos haya aplicado todas las demás reglas de la política de seguridad, incluidas las reglas de traducción de direcciones de red (Network Address Translation, NAT). Si desea aplicar el tratamiento de QoS al tráfico basado en el origen, asegúrese de especificar la dirección de origen posterior a NAT en una regla de políticas de QoS (no utilice la dirección de origen anterior a NAT).

Perfil de QoS

Utilice una regla de perfil QoS para definir valores de hasta ocho clases de QoS incluidos en esa regla de perfil.

© 2020 Palo Alto Networks, Inc.

Con una regla de perfil QoS, puede definir el Establecimiento de colas de prioridad de QoS y la Gestión del ancho de banda de QoS para las clases de QoS. Cada regla de perfil QoS le permite configurar el ancho de banda y los ajustes de prioridad individuales para hasta ocho clases de QoS, además del ancho de banda total asignado para las ocho clases combinadas. Asocie la regla de perfil QoS (o las múltiples reglas de perfil QoS) a una interfaz física para aplicar la prioridad y los ajustes del ancho de banda definidos al tráfico saliente de la interfaz.

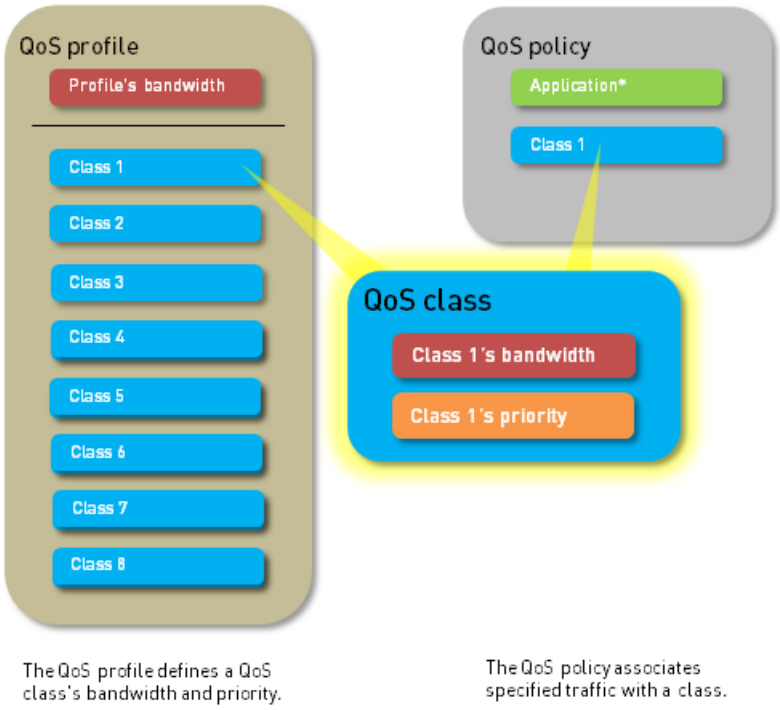
Hay una regla de perfil de QoS por defecto disponible en el cortafuegos. La regla de perfil por defecto y las clases definidas en el perfil no tienen máximo predefinido ni límites de ancho de banda garantizados.

Para definir la configuración de prioridad y ancho de banda de las clases de QoS, consulte el paso Añadir una regla del perfil de QoS.

Clases de QoS

Una clase de QoS determina la prioridad y el ancho de banda del tráfico que coincide con una regla de la política de QoS. Puede utilizar una regla de la política de QoS para definir las clases de QoS. Hay hasta ocho clases de QoS definibles en un único perfil de QoS. A menos que esté configurado de otra forma, al tráfico que no coincida con una clase de QoS se le asignará la clase 4.

El establecimiento de colas de prioridad y la gestión del ancho de banda de QoS, los mecanismos fundamentales de una configuración de QoS, se configuran dentro de la definición de la clase de QoS (consulte el paso Añada una regla del perfil de QoS). Para cada clase de QoS, puede establecer una prioridad (tiempo real, alta, media y baja) y el máximo y el ancho de banda garantizado para el tráfico coincidente. El establecimiento de colas de prioridad de QoS y la gestión del ancho de banda determinan el orden y el modo en el que se gestiona el tráfico al entrar o al salir de una red:



Establecimiento de colas de prioridad de QoS

Se puede aplicar una de las cuatro prioridades en una clase de QoS: tiempo real, alta, media y baja. Al tráfico que coincide con una regla de política de QoS se le asigna la clase de QoS asociada con esa regla

© 2020 Palo Alto Networks, Inc.

y el cortafuegos trata el tráfico coincidente en función de la prioridad de clase de QoS. Los paquetes del flujo de tráfico saliente se colocan en cola según su prioridad hasta que la red esté lista para procesarlos. El establecimiento de colas de prioridad le permite garantizar que el tráfico, las aplicaciones o los usuarios importantes tengan prioridad. La prioridad en tiempo real suele utilizarse para aplicaciones que son especialmente sensibles a la latencia, como las aplicaciones de voz y vídeo.

Gestión del ancho de banda de QoS

La gestión del ancho de banda de QoS le permite controlar los flujos de tráfico para que este no supere la capacidad de la red (lo que provocaría la congestión de la red) y también le permite asignar un ancho de banda para ciertos tipos de tráfico, aplicaciones y usuarios. Con QoS, puede aplicar un ancho de banda al tráfico en una escala reducida o amplia. Una regla de perfil QoS le permite establecer límites de ancho de banda para clases de QoS individuales y el ancho de banda total combinado para las ocho clases de QoS. Como parte de los pasos para la Configuración de QoS, puede adjuntar la regla de perfil QoS a una interfaz física para aplicar la configuración del ancho de banda en el tráfico que sale de la interfaz; la configuración de clase de QoS individual se aplica al tráfico que coincide con esa clase de QoS (las clases de QoS se asignan al tráfico que coincide con las reglas de la política de QoS). Además, el límite de ancho de banda general para el perfil se puede aplicar a todo el tráfico de texto normal (tráfico de texto normal específico que se origina en las interfaces de origen y subredes de origen), todo el tráfico de túnel y las interfaces de túnel individuales. Puede añadir varias reglas de perfil a una sola interfaz QoS para aplicar diferentes ajustes de ancho de banda al tráfico saliente de la interfaz.

Los siguientes campos admiten ajustes de ancho de banda de QoS:

- **Egress Guaranteed**: la cantidad de ancho de banda garantizado para el tráfico coincidente. Cuando se supera el ancho de banda garantizado de salida, el cortafuegos conmuta el tráfico en base a best-effort. El ancho de banda que está garantizado pero sin usar continúa disponible para todo el tráfico. Según su configuración de QoS, puede garantizar un ancho de banda para una sola clase de QoS, para todo o parte del tráfico sin cifrar, y para todo o parte del tráfico de túnel.

  Ejemplo:

  El tráfico de clase 1 tiene 5 Gbps de ancho de banda de salida garantizado, lo que significa que hay 5 Gbps disponibles pero no reservados para el tráfico de clase 1. Si el tráfico de clase 1 no usa o solo usa parcialmente el ancho de banda garantizado, otras clases de tráfico podrán usar el ancho de banda restante. Sin embargo, durante los períodos de mucho tráfico, hay 5 Gbps de ancho de banda totalmente disponibles para el tráfico de clase 1. Durante estos períodos de congestión, cualquier tráfico de clase 1 que supere los 5 Gbps es la mejor opción.
- **Egress Max**: la asignación de ancho de banda general para el tráfico coincidente. El cortafuegos descarta el tráfico que excede el límite de salida máximo que haya configurado. Según su configuración de QoS, puede establecer un límite máximo de ancho de banda para una clase QoS, para todo o parte del tráfico de texto no cifrado, para todo o parte del tráfico de túnel, y para todo el tráfico saliente de la interfaz QoS.

  El ancho de banda garantizado acumulado para las reglas de perfil QoS asociadas a la interfaz no debe superar el ancho de banda total asignado a la interfaz.

Para definir la configuración de ancho de banda de las clases de QoS, consulte el paso Añada una regla del perfil de QoS. Para aplicar esa configuración de ancho de banda a tráfico de texto normal y de túnel, y para establecer el límite de ancho de banda general para una interfaz de QoS, consulte el paso Habilite QoS en una interfaz física.

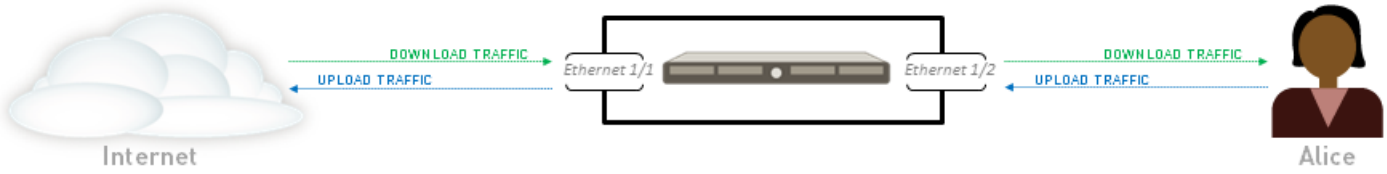
Interfaz de salida de QoS

La habilitación de una regla de perfil de QoS en la interfaz de salida del tráfico identificado para el tratamiento de QoS, completa la configuración de QoS. La interfaz de entrada del tráfico de QoS es la interfaz por la que el tráfico accede al cortafuegos. La interfaz de salida del tráfico de QoS es la interfaz

© 2020 Palo Alto Networks, Inc.

por la que el tráfico abandona el cortafuegos. QoS siempre está habilitado y aplicado en la interfaz de salida para el flujo de tráfico. La interfaz de salida de una configuración de QoS puede ser la interfaz de orientación externa o de orientación interna del cortafuegos, dependiendo del flujo de tráfico que reciba el tratamiento de QoS.

Por ejemplo, en una red empresarial, si está limitando el tráfico de descarga de los empleados en un sitio web específico, la interfaz de salida de la configuración de QoS es la interfaz interna del cortafuegos, dado que el flujo de tráfico proviene de Internet, pasa por el cortafuegos y se dirige a su red empresarial. De manera alternativa, al limitar el tráfico de carga de los empleados en el mismo sitio web, la interfaz de salida de la configuración de QoS es la interfaz externa del cortafuegos, dado que el tráfico que está limitando se desplaza desde su red empresarial, pasando por el cortafuegos, hasta Internet.



- The egress interface for Alice's download traffic is Ethernet 1/2. To prioritize or limit her download traffic, Alice enables QoS on Ethernet 1/2.
- The egress interface for Alice's upload traffic is Ethernet 1/1. To prioritize or limit her upload traffic, Alice enables QoS on Ethernet 1/1.

Puesto que QoS se aplica al tráfico cuando sale del cortafuegos, su regla de políticas de QoS se aplica al tráfico después de que el cortafuegos haya aplicado todas las demás reglas de la política de seguridad, incluidas las reglas de traducción de direcciones de red (Network Address Translation, NAT). Si desea aplicar el tratamiento de QoS al tráfico basado en el origen, debe especificar la dirección de origen posterior a NAT en una regla de políticas de QoS (no utilice la dirección de origen anterior a NAT).

Obtenga más información sobre cómo identificar la interfaz de salida para las aplicaciones que desea que reciban un tratamiento de QoS.

QoS para texto no cifrado y tráfico de túnel

Como mínimo, la habilitación de interfaces QoS requiere que seleccione una regla de perfil QoS por defecto que defina el ancho de banda y los ajustes de prioridad para todo el tráfico de texto no cifrado que sale de la interfaz. Sin embargo, al configurar o modificar una interfaz QoS, se puede aplicar una configuración de QoS detallada al tráfico saliente de texto no cifrado y de túnel. El tratamiento preferente y la limitación de ancho de banda de QoS pueden aplicarse para el tráfico de túnel, para interfaces de túnel individuales o para el tráfico de texto no cifrado procedente de otras interfaces y subredes de origen. En los cortafuegos de Palo Alto Networks, el término *tráfico de túnel* hace referencia al tráfico de interfaz de túnel, concretamente, al tráfico de IPSec en el modo de túnel.

© 2020 Palo Alto Networks, Inc.

Configuración de QoS

Siga estos pasos para configurar la calidad de servicio (QoS), que incluye cómo crear un perfil de QoS, crear una política de QoS y habilitar QoS en una interfaz.

STEP 1 | Identifique el tráfico que desea gestionar con QoS.

Este ejemplo muestra cómo utilizar el QoS para limitar la exploración web.

Seleccione **ACC** para ver la página **Application Command Center (Centro de control de aplicaciones)**. Utilice los ajustes y los gráficos de la página **ACC** para ver tendencias y el tráfico relacionado con aplicaciones, filtrado de URL, prevención de amenazas, filtrado de datos y coincidencias HIP.

Haga clic en cualquier nombre de aplicación para mostrar información de aplicación detallada.

STEP 2 | Identifique la interfaz de salida para las aplicaciones que desea que reciban un tratamiento de QoS.

La interfaz de salida del tráfico depende del flujo de tráfico. Si está moldeando el tráfico entrante, la interfaz de salida es la interfaz de orientación interna. Si está moldeando el tráfico saliente, la interfaz de salida es la interfaz de orientación externa.

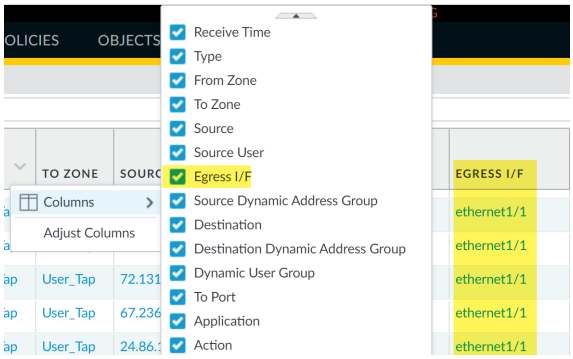
Seleccione **Monitor (Supervisar)** > **Logs [Logs]** > **Traffic (Tráfico)** para ver los logs de tráfico.

Para filtrar y mostrar únicamente los logs de una aplicación específica:

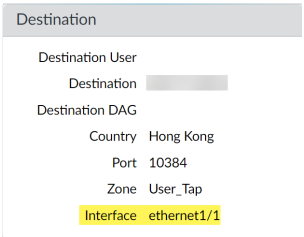
- Si se muestra una entrada para la aplicación, haga clic en el enlace subrayado de la columna Aplicación y, a continuación, haga clic en el icono de envío.
- Si una entrada no se muestra para la aplicación, haga clic en el icono Añadir log y busque la aplicación.

La **Egress I/F (Interfaz de salida)** de los logs de tráfico muestra la interfaz de salida de cada aplicación. Para mostrar la columna Interfaz de salida si no aparece de manera predeterminada:

- Haga clic en cualquier encabezado de columna para añadir una columna al log:



- Haga clic en el icono de catalejo a la izquierda de cualquier entrada para mostrar un log detallado que incluye la interfaz de salida de la aplicación indicada en la sección Destino:



© 2020 Palo Alto Networks, Inc.

STEP 3 | Añada una regla de políticas de QoS.

Las reglas de política de QoS definen el tráfico que recibirá el tratamiento de QoS. El cortafuegos asigna una clase de servicio QoS al tráfico que coincide con la regla de política.

Puesto que QoS se aplica al tráfico cuando sale del cortafuegos, su regla de políticas de QoS se aplica al tráfico después de que el cortafuegos haya aplicado todas las demás reglas de la política de seguridad, incluidas las reglas de traducción de direcciones de red (Network Address Translation, NAT). Si desea aplicar el tratamiento de QoS al tráfico basado en el origen, debe especificar la dirección de origen posterior a NAT en una regla de políticas de QoS (no utilice la dirección de origen anterior a NAT).

1. Seleccione **Policies (Políticas)** > **QoS** y seleccione **Add (Añadir)** para añadir una nueva regla de políticas.
2. En la pestaña General, otorgue a la regla de política de QoS un Nombre descriptivo.
3. Especifique el tráfico que recibirá tratamiento de QoS en función de los valores de **Source (Origen)**, **Destination (Destino)**, **Application (Aplicación)**, **Service/URL Category (Categoría de URL/servicio)** y **DSCP/ToS** (los ajustes de **DSCP/ToS** le permiten la aplicación de QoS en función de la clasificación de DSCP).

   Por ejemplo, seleccione la pestaña **Application (Aplicación)**, haga clic en **Add (Añadir)** y seleccione **web-browsing (exploración web)** para aplicar la regla de QoS al tráfico de navegación web.
4. (Opcional) Proceda con la definición de parámetros adicionales. Por ejemplo, seleccione **Source (Origen)** y **Add (Añadir)** para añadir un **Source User (Usuario de origen)** para proporcionar QoS para el tráfico web de un usuario específico.
5. Seleccione **Other Settings (Otros ajustes)** y asigne una **QoS Class (Clase de QoS)** al tráfico que coincida con la regla de política. Por ejemplo, asigne la clase 2 al tráfico web de user1:
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Añada una regla de perfil de QoS.

Una regla de perfil de QoS le permite definir las ocho clases de servicio que el tráfico puede recibir, incluida la prioridad, y habilita la gestión del ancho de banda de QoS.

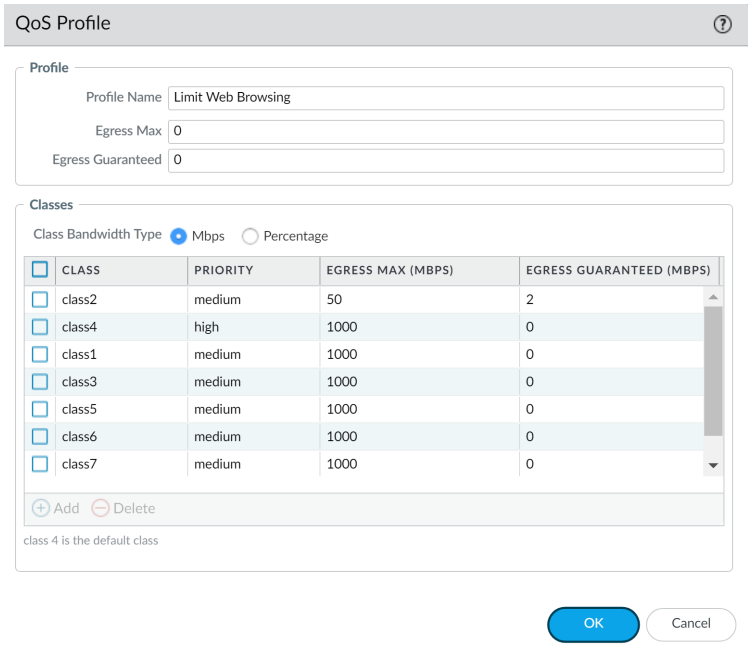
Puede editar cualquier perfil de QoS existente, incluido el valor predeterminado, haciendo clic en el nombre del perfil de QoS.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **QoS Profile (Perfil QoS)** y **Add (Añadir)** para añadir un nuevo perfil.
2. Introduzca un **Nombre de perfil** descriptivo.
3. Configure los límites de ancho de banda general para la regla del perfil de QoS:
   - Introduzca un valor de **Egress Max** para establecer la asignación del ancho de banda total para la regla de perfil de QoS.
   - Introduzca un valor de **Egress Guaranteed (Salida garantizada)** para establecer el ancho de banda garantizado para el perfil de QoS.

   Todo el tráfico que supere el valor de Egress Guaranteed será la mejor opción pero no estará garantizado. El ancho de banda que está garantizado pero sin usar continúa disponible para todo el tráfico.
4. En la sección Clases, especifique cómo tratar hasta ocho clases de QoS individuales:
   1. Haga clic en **Add (Añadir)** para añadir una clase al perfil de QoS.
   2. Seleccione la **Priority (Prioridad)** para la clase: tiempo real, alta, media o baja.
   3. Introduzca el valor de ancho de banda **Egress Max (Máximo de salida)** y **Egress Guaranteed (Salida garantizada)** para el tráfico asignado a cada clase de QoS.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

En el siguiente ejemplo, la regla de perfil de QoS denominada Limit Web Browsing limita el tráfico de clase 2 a un ancho de banda máximo de 50 Mbps y un ancho de banda garantizado de 2 Mbps.



STEP 5 | Habilite QoS en una interfaz física.

Parte de este paso involucra la opción de seleccionar texto sin cifrar y tráfico de túnel para el tratamiento de QoS único.

Compruebe si el modelo de cortafuegos que está utilizando admite la habilitación de QoS en una subinterfaz, al revisar un resumen de las especificaciones del producto.

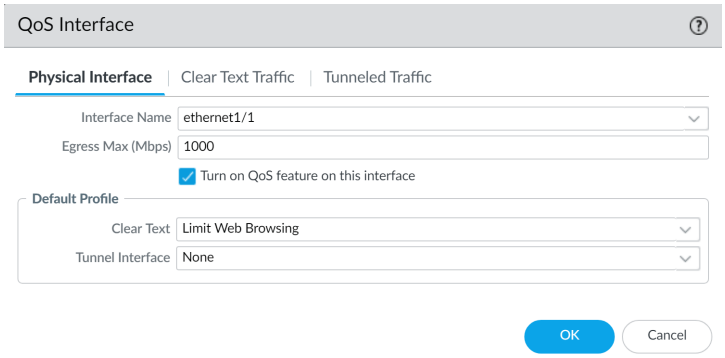
1. Seleccione **Network (Red)** > **QoS** y **Add (Añadir)** para añadir una interfaz QoS.
2. Seleccione **Physical Interface (Interfaz física)** y elija el **Interface Name (Nombre de interfaz)** de la interfaz en que desea habilitar QoS.

   En el ejemplo, Ethernet 1/1 es la interfaz de salida para el tráfico de exploración web (consulte el paso 2).
3. Configure el valor de ancho de banda **Egress Max (Máximo de salida)** para todo el tráfico que sale de esta interfaz.

   Se recomienda definir siempre el valor de Egress Max (Máximo de salida) para las interfaces de QoS. Asegúrese de que el ancho de banda garantizado acumulado para las reglas de perfil QoS que se asociaron a la interfaz no supere el ancho de banda total asignado a esta.
4. Seleccione **Activar la función QoS en esta interfaz**.
5. En la sección Default Profile (Perfil predeterminado), seleccione una regla de perfil QoS para aplicar a todo el tráfico **Clear Text (No cifrado)** saliente de la interfaz física.
6. (Opcional) Seleccione una regla de perfil QoS predeterminada para aplicar a todo el tráfico de túnel que sale de la interfaz.

Por ejemplo, habilite QoS en ethernet 1/1 y aplique el ancho de banda y los ajustes de prioridad que definió para la regla de perfil QoS Limit Web Browsing (paso 4) que deben usarse como ajustes predeterminados para el tráfico de salida no cifrado.

© 2020 Palo Alto Networks, Inc.



1. (Opcional) Prosiga con la definición de ajustes más detallados para proporcionar QoS para tráfico sin cifrar y de túnel. Los ajustes configurados en la pestaña **Clear Text Traffic** y en la pestaña **Tunneled Traffic** cancelan automáticamente los ajustes de perfil por defecto para el texto sin cifrar y el tráfico de túnel en la pestaña de interfaz física.
   - Seleccione **Clear Text Traffic (Tráfico no cifrado)** y:
     - Establezca los anchos de banda de **Salida garantizada** y **Máximo de salida** para el tráfico de texto claro.
     - Haga clic en **Add** y aplique una regla de perfil QoS para aplicar tráfico de texto sin cifrar basado en la interfaz de origen y la subred de origen.
   - Seleccione **Tunneled Traffic (Tráfico de túnel)**y:
     - Establezca los anchos de banda de **Salida garantizada** y **Máximo de salida** para el tráfico de túnel.
     - Haga clic en **Add** y asocie un perfil de QoS a una única interfaz de túnel.
2. Haga clic en **OK (Aceptar)**.

STEP 6 | Confirme los cambios.

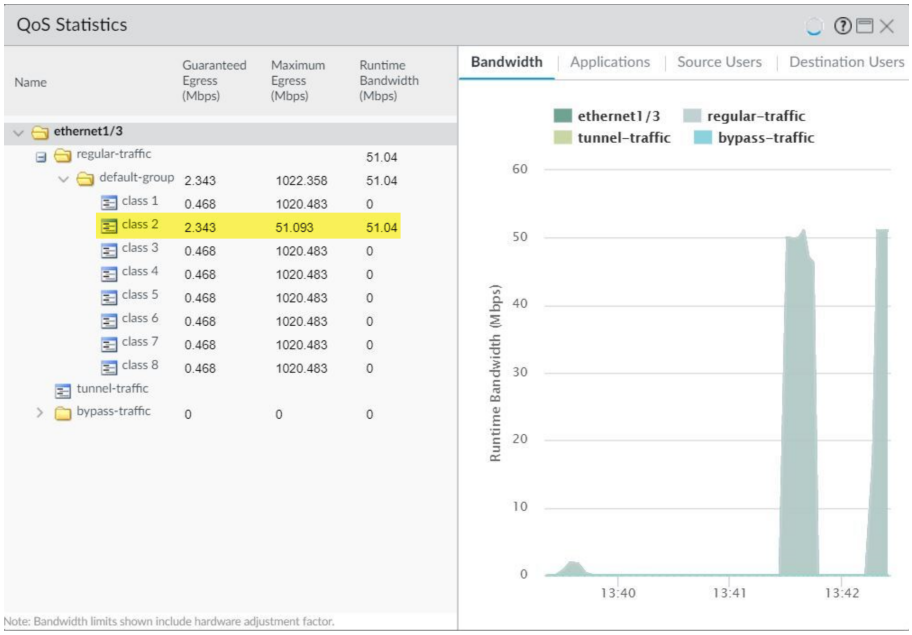
Haga clic en **Commit (Confirmar)**.

STEP 7 | Verifique la configuración de QoS.

Seleccione **Network (Red)** > **QoS** y luego **Statistics (Estadísticas)** para ver el ancho de banda de QoS, las sesiones activas de una clase de QoS seleccionada y las aplicaciones activas para la clase de QoS seleccionada.

Por ejemplo, vea las estadísticas de Ethernet 1/3 con el QoS habilitada:

© 2020 Palo Alto Networks, Inc.



Tráfico de clase 2 limitado a 2343 Mbps de ancho de banda garantizado y un ancho de banda máximo de 51 093 Mbps.

Siga haciendo clic en las pestañas para mostrar más información relativa a las aplicaciones, los usuarios de origen, los usuarios de destino, las reglas de seguridad y las reglas de QoS.

Los límites de ancho de banda que se muestran en la ventana Estadísticas de QoS incluyen un factor de ajuste de hardware.

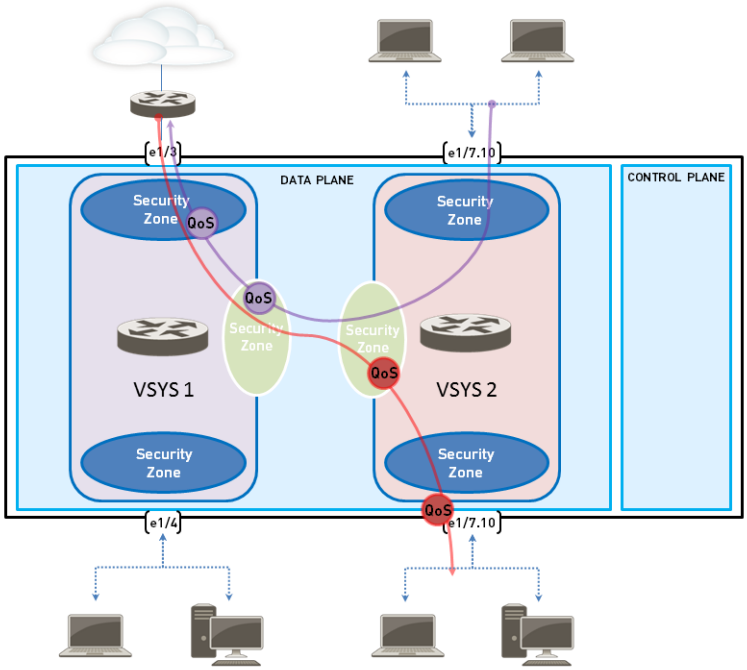
© 2020 Palo Alto Networks, Inc.

Configuración de QoS para un sistema virtual

El QoS se puede configurar para uno o varios sistemas virtuales configurados en un cortafuegos de Palo Alto Networks. Como un sistema virtual es un cortafuegos independiente, el QoS debe configurarse independientemente para un único sistema virtual.

La configuración de QoS para un sistema virtual es similar a configurar QoS en un cortafuegos físico, con la excepción de que configurar QoS para un sistema virtual requiere la especificación del origen y destino del tráfico. Dado que existe un sistema virtual sin límites físicos fijos y que el tráfico en un entorno virtual se extiende a más de un sistema virtual, es necesario especificar las zonas e interfaces de origen y destino para controlar y moldear el tráfico para un único sistema virtual.

El ejemplo siguiente muestra dos sistemas virtuales configurados en un cortafuegos. VSYS 1 (púrpura) y VSYS 2 (rojo) han configurado QoS para establecer la prioridad o limitar dos flujos de tráfico distintos, indicados por sus correspondientes líneas púrpura (VSYS 1) y roja (VSYS 2). Los nodos de QoS indican los puntos en los que el tráfico se asocia a una política QoS y se asigna a una clase de servicio QoS, y después indican el punto en el que el tráfico se moldea conforme abandona el cortafuegos



Consulte Sistemas virtuales para obtener información sobre los sistemas virtuales y cómo configurarlos.

STEP 1 | Confirme que las interfaces, los enrutadores virtuales y las zonas de seguridad adecuados están asociados a cada sistema virtual.

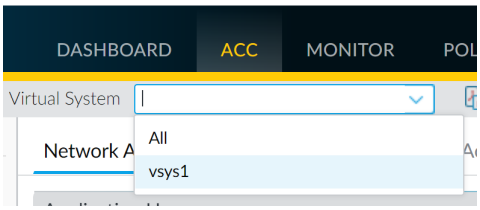
- Para ver interfaces configuradas, seleccione **Network (Red)** > **Interface (Interfaz)**.
- Para ver zonas configuradas, seleccione **Network (Red)** > **Zones (Zonas)**
- Para ver información sobre enrutadores virtuales definidos, seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.

STEP 2 | Identifique el tráfico al que aplicar el QoS.

© 2020 Palo Alto Networks, Inc.

Seleccione **ACC** para ver la página **Application Command Center (Centro de control de aplicaciones)**. Utilice los ajustes y los gráficos de la página **ACC** para ver tendencias y el tráfico relacionado con aplicaciones, filtrado de URL, prevención de amenazas, filtrado de datos y coincidencias HIP.

Para ver información de un sistema virtual específico, seleccione el sistema virtual en el menú desplegable **Sistema virtual**:



Haga clic en cualquier nombre de aplicación para mostrar información de aplicación detallada.

STEP 3 | Identifique la interfaz de salida para las aplicaciones que identifique que necesitan un tratamiento de QoS.

En un entorno de sistema virtual, el QoS se aplica al tráfico del punto de salida del tráfico en el sistema virtual. Dependiendo de la configuración de la política de QoS para un sistema virtual, el punto de salida del tráfico de QoS podría asociarse a una interfaz física o podría ser una zona.

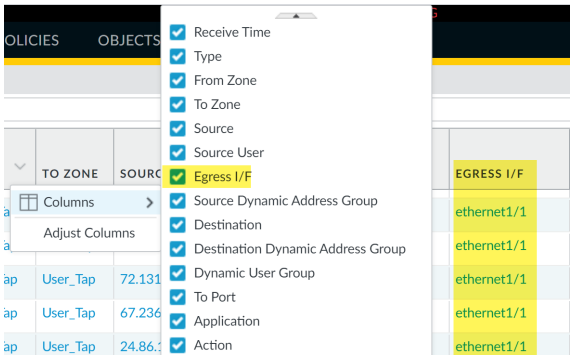
Este ejemplo muestra cómo limitar el tráfico de exploración web en VSYS 1.

Seleccione **Monitor (Supervisar)** > **Logs [Logs]** > **Traffic (Tráfico)** para ver logs de tráfico. Cada entrada tiene la opción de mostrar columnas con información necesaria para configurar QoS en un entorno de sistema virtual:

- sistema virtual
- interfaz de salida
- interfaz de entrada
- zona de origen
- zona de destino

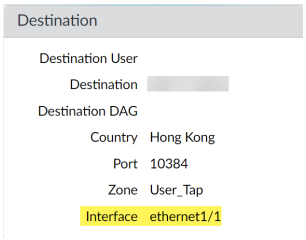
Para mostrar una columna si no aparece de manera predeterminada:

- Haga clic en cualquier encabezado de columna para añadir una columna al log:



- Haga clic en el icono de catalejo a la izquierda de cualquier entrada para mostrar un log detallado que incluye la interfaz de salida de la aplicación, así como zonas de origen y destino, en las secciones **Origen** y **Destino**:

© 2020 Palo Alto Networks, Inc.



Por ejemplo, para el tráfico de exploración web desde VSYS 1, la interfaz de entrada es Ethernet 1/2, la interfaz de salida es Ethernet 1/1, la zona de origen es fiable y la zona de destino es no fiable.

STEP 4 | Cree un perfil de QoS.

Puede editar cualquier perfil de QoS existente, incluido el valor predeterminado, haciendo clic en el nombre del perfil.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **QoS Profile (Perfil de QoS)** y haga clic en **Add (Añadir)** para abrir el cuadro de diálogo QoS Profile (Perfil de QoS).
2. Introduzca un **Nombre de perfil** descriptivo.
3. Introduzca un **Máximo de salida** para establecer la asignación del ancho de banda total para el perfil de QoS.
4. Introduzca una **Egress Guaranteed (Salida garantizada)** para establecer el ancho de banda garantizado para el perfil de QoS.

   Todo el tráfico que supere el límite garantizado de salida del perfil de QoS será la mejor opción pero no estará garantizado.
5. En la sección Clases del **Perfil de QoS**, especifique cómo tratar hasta ocho clases de QoS individuales:
   1. Haga clic en **Añadir** para añadir una clase al perfil de QoS.
   2. Seleccione la Prioridad de la clase.
   3. Introduzca un Máximo de salida para la clase para establecer el límite de ancho de banda total para esa clase individual.
   4. Introduzca una **Salida garantizada** para la clase para establecer el ancho de banda garantizado para esa clase individual.
6. Haga clic en **ACEPTAR** para guardar el perfil de QoS.

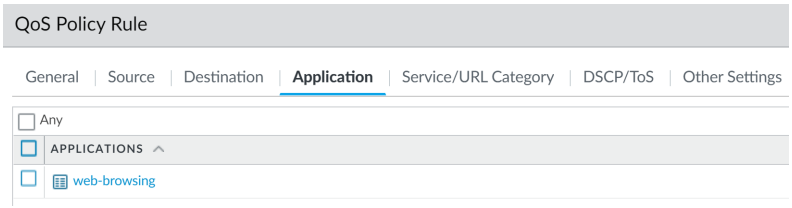
STEP 5 | Cree una política de QoS.

En un entorno con varios sistemas virtuales, el tráfico abarca más de un sistema virtual. Por este motivo, al habilitar QoS para un sistema virtual, debe definir que el tráfico reciba tratamiento QoS basado en zonas de origen y destino. De este modo se garantiza que el tráfico se prioriza y moldea solo para ese sistema virtual (y no para otros sistemas virtuales a través de los que puede fluir el tráfico).

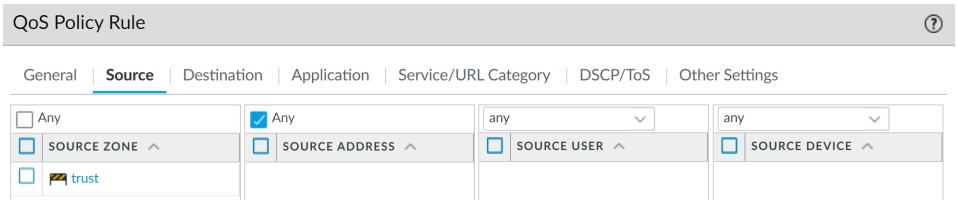
1. Seleccione **Policies (Políticas)** > **QoS** y **Add (Añadir)** para añadir una regla de políticas de QoS.
2. Seleccione **General** y asígnele un nombre descriptivo a la regla de política QoS en **Name (Nombre)**.
3. Especifique el tráfico al que se aplicará la regla de política de QoS. Utilice las pestañas **Origen**, **Destino**, **Aplicación** y **Categoría de URL/servicio** para definir los parámetros de coincidencia para identificar el tráfico.

   Por ejemplo, seleccione **Application**, haga clic en **Add** y seleccione la exploración web para aplicar la regla de política de QoS a esa aplicación:

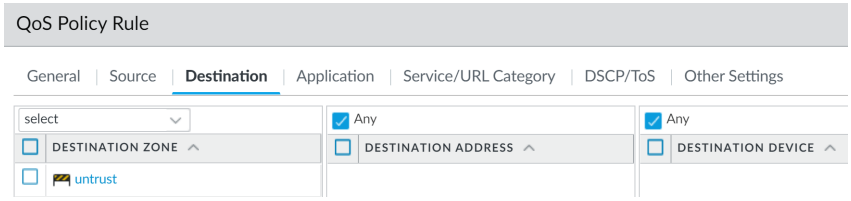
© 2020 Palo Alto Networks, Inc.



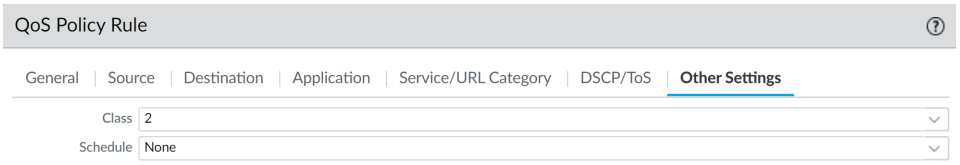
4. Seleccione **Source (Origen)** y **Add (Añadir)** para añadir la zona de origen del tráfico de exploración web de vsys 1.



5. Seleccione **Destination** y **Add** para seleccionar la zona de destino del tráfico de exploración web de vsys 1.



6. Seleccione **Other Settings** y seleccione una **QoS Class** para asignarla a la regla de política de QoS. Por ejemplo, asigne la clase 2 al tráfico de exploración web de VSYS 1:



7. Haga clic en **ACEPTAR** para guardar la regla de política de QoS.

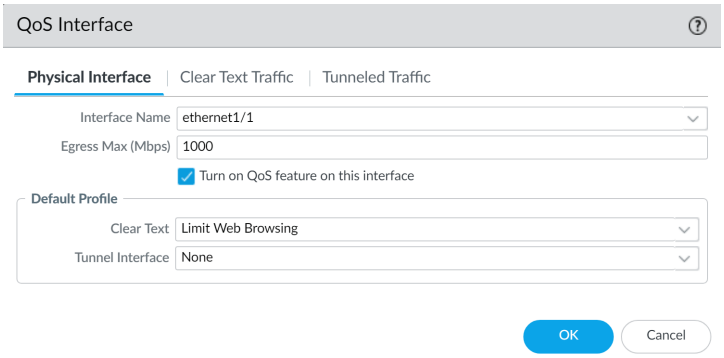
STEP 6 | Habilite el perfil de QoS en una interfaz física.

La práctica recomendada es definir siempre el valor de Máximo de salida para una interfaz de QoS.

1. Seleccione **Network (Red)** > **QoS** y haga clic en **Add (Añadir)** para abrir el cuadro de diálogo QoS Interface (Interfaz de QoS).
2. Habilite QoS en la interfaz física:
   1. En la pestaña **Interfaz física**, seleccione el **Nombre de interfaz** de la interfaz a la que se aplicará el perfil de QoS.

      En este ejemplo, Ethernet 1/1 es la interfaz de salida para el tráfico de exploración web de vsys 1 (consulte el paso 2).

© 2020 Palo Alto Networks, Inc.



2. Seleccione **Activar la función QoS en esta interfaz**.
3. En la pestaña **Interfaz física**, seleccione el perfil de QoS predeterminado que debe aplicarse a todo el tráfico de tipo **Tráfico en claro**.

   (Opcional) Utilice el campo Interfaz de túnel para aplicar un perfil de QoS predeterminado a todo el tráfico de túnel.
4. (Opcional) En la pestaña Tráfico en claro, configure ajustes de QoS adicionales para el tráfico de texto claro:
   - Establezca los anchos de banda de **Salida garantizada** y **Máximo de salida** para el tráfico de texto claro.
   - Haga clic en **Add** para aplicar un perfil de QoS al tráfico de texto no cifrado seleccionado, seleccione también el tráfico para el tratamiento de QoS de acuerdo con la interfaz de origen y la subred de origen (creando un nodo de QoS).
5. (Opcional) En la pestaña Tráfico de túnel, configure ajustes de QoS adicionales para interfaces de túnel:
   - Establezca los anchos de banda de **Salida garantizada** y **Máximo de salida** para el tráfico de túnel.
   - Haga clic en **Add** para asociar una interfaz de túnel seleccionada a un perfil de QoS.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.
7. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 7 | Verifique la configuración de QoS.

- Seleccione **Network (Red)** > **QoS** para visualizar la página de políticas de QoS. La página Políticas de QoS verifica que QoS está habilitada e incluye el enlace Estadísticas. Haga clic en el enlace Estadísticas para ver el ancho de banda de QoS, las sesiones activas de un nodo o una clase de QoS que haya seleccionado y las aplicaciones activas del nodo o la clase de QoS que haya seleccionado.
- En un entorno de VSYS múltiple, las sesiones no pueden abarcar varios sistemas. Se crean varias sesiones para un flujo de tráfico si el tráfico pasa por más de un sistema virtual. Para examinar las sesiones que se ejecuten en el cortafuegos y ver las reglas de QoS y las clases de QoS aplicadas, seleccione **Monitor (Supervisar)** > **Session Browser (Navegador de sesión)**

© 2020 Palo Alto Networks, Inc.

Aplicación forzada de QoS basada en la clasificación DSCP

Un punto de código de servicios diferenciado (Differentiated Services Code Point, DSCP) es un valor de encabezado que puede usarse para solicitar (por ejemplo) entrega de alta prioridad o la mejor opción de entrega para el tráfico. La clasificación de DSCP basada en la sesión le permite respetar los valores de DSCP para el tráfico entrante y marcar una sesión con un valor DSCP a medida que el tráfico de sesión sale del cortafuegos. Esto permite que todo el tráfico entrante y saliente de una sesión pueda recibir tratamiento QoS/DSCP continuado a medida que atraviesa su red. Por ejemplo, ahora el tráfico entrante de retorno procedente de un servidor externo se puede tratar con la misma prioridad QoS que aplicó el cortafuegos inicialmente para el flujo de salida en función del valor DSCP que el cortafuegos detectó al comienzo de la sesión. Los dispositivos de red entre el cortafuegos y el usuario final también aplicarán la misma prioridad para el tráfico de retorno (y cualquier otro tráfico entrante y saliente para la sesión).

Los diferentes tipos de marcas de DSCP indican diferentes niveles de servicio:

Al completar este paso, el cortafuegos puede marcar el tráfico con el mismo valor DSCP que se detectó al inicio de una sesión (en este ejemplo, el cortafuegos marcaría el tráfico de retorno con el valor DSCP AF11). Mientras que la configuración de QoS le permite moldear el tráfico conforme abandona el cortafuegos, habilitar esta opción en una regla de seguridad permite a los otros dispositivos de red intermedios entre el cortafuegos y el cliente seguir aplicando la prioridad para el tráfico marcado con DSCP.

- **Expedited Forwarding (EF)**: Se puede usar para solicitar pérdida baja, latencia baja y ancho de banda garantizado para el tráfico. Los paquetes con valores de puntos de código EF suelen tener garantizado el envío de máxima prioridad.
- **Assured Forwarding (AF)**: Se puede usar para ofrecer envíos fiables a las aplicaciones. Los paquetes con puntos de código AF indican una solicitud para que el tráfico reciba el tratamiento de mayor prioridad que ofrezca la mejor opción de servicio (a través de paquetes con un punto de código EF seguirá teniendo prioridad sobre aquellos con un punto de código AF).
- **Class Selector (CS)**: Se puede usar para ofrecer compatibilidad con dispositivos de red más antiguos que usan el campo Prioridad de IP para marcar el tráfico prioritario.
- **IP Precedence (ToS) (Precedencia de IP)**: Los dispositivos de red antiguos pueden usarla para marcar el tráfico prioritario (el campo de encabezado Prioridad de IP se usaba para indicar la prioridad para un paquete antes de la introducción de la clasificación DSCP).
- **Custom Codepoint**: Cree un punto de código personalizado para buscar coincidencias con el tráfico al introducir un **Codepoint Name (Nombre de punto de código)** y un **Binary Value (Valor binario)**.

Por ejemplo, seleccione **Assured Forwarding (AF)** para asegurarse de que el tráfico marcado con un valor de punto de código AF tiene mayor prioridad de entrega fiable a través de aplicaciones marcadas para recibir menor prioridad. Siga los siguientes pasos para habilitar la clasificación de DSCP basada en la sesión. En primer lugar, configure QoS basada en el marcado DSCP detectado al inicio de una sesión. Después, habilite el cortafuegos para marcar el flujo de retorno para una sesión con el mismo valor DSCP usado para aplicar QoS para el flujo de salida inicial.

STEP 1 | Realice los pasos preliminares para configurar QoS.

STEP 2 | Defina el tráfico que debe recibir tratamiento QoS en función del valor de DSCP.

1. Seleccione **Policies (Políticas)** > **QoS** y **Add (Añadir)** para añadir o modificar una regla QoS existente, y rellene los campos obligatorios.
2. Seleccione **DSCP/ToS** y seleccione **Codepoints (Puntos de código)**.

© 2020 Palo Alto Networks, Inc.

3. Seleccione **Add (Añadir)** para añadir puntos de código DSCP/ToS para los que desea aplicar QoS.
4. Seleccione el **Type** de marca DSCP/ToS para la regla QoS que coincidirá con el tráfico:

   Se recomienda usar un único tipo de DSCP para gestionar y priorizar su tráfico de red.
5. Asigne la política de QoS al tráfico en una escala más detallada al especificar el valor de **Codepoint (Punto de código)**. Por ejemplo, con reenvío garantizado (Assured Forwarding, AF) seleccionado como el **Type (Tipo)** de valor DSCP para coincidir con la política, especifique además un valor de **Codepoint (Punto de código)** AF, como por ejemplo, AF11.

   Si reenvío rápido (Expedited Forwarding, EF) está seleccionado como el Type (Tipo) de marca DSCP, no se puede especificar un valor de Codepoint (Punto de código) detallado. La política de QoS coincidirá con el tráfico marcado con cualquier valor de punto de código EF.
6. Seleccione **Other Settings** y asigne una **QoS Class** al tráfico que coincida con la regla de QoS. En este ejemplo, asigne la clase 1 a las sesiones en las que se detecte la marca DSCP de AF11 para el primer paquete de la sesión.
7. Haga clic en **OK (Aceptar)** para guardar la regla de QoS.

STEP 3 | Defina la prioridad de QoS para la recepción del tráfico cuando coincida con una regla de QoS basada en el marcado de DSCP detectado al inicio de una sesión.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **QoS Profile (Perfil QoS)** y luego haga clic en **Add (Añadir)** para añadir un perfil de QoS o modifique un perfil existente. Para obtener información sobre opciones de perfiles para establecer la prioridad y el ancho de banda del tráfico, consulte Conceptos de QoS y Configuración de QoS.
2. Seleccione **Add (Añadir)** para añadir o modificar una clase de perfil. Por ejemplo, dado que el paso 2 mostraba pasos para clasificar el tráfico AF11 como tráfico de clase 1, podría añadir o modificar una entrada de **class1**.
3. Seleccione una **Priority (Prioridad)** para la clase de tráfico, como por ejemplo, **high (alta)**.
4. Haga clic en **ACEPTAR** para guardar el perfil de QoS.

STEP 4 | Habilite el QoS en una interfaz.

Seleccione **Network (Red)** > **QoS** y **Add (Añadir)** para añadir o modifique una interfaz existente y luego seleccione **Turn on QoS feature on this interface (Activar la función QoS en esta interfaz)**.

En este ejemplo, el tráfico con un marcado AF11 DSCP se hace coincidir con la regla QoS y se asigna a la clase 1. El perfil de QoS habilitado en la interfaz aplica el tratamiento de alta prioridad para el tráfico de clase 1 a medida que sale del cortafuegos (el tráfico *saliente* de la sesión).

STEP 5 | Habilite el marcado DSCP.

Marque el tráfico de retorno con un valor DSCP, lo que permite que se marque el flujo entrante de una sesión con el mismo valor DSCP detectado para el flujo saliente.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** para añadir o modificar una política de seguridad.
2. Seleccione **Actions (Acciones)** y en el menú desplegable **QoS Marking (Marca QoS)** elija **Follow Client-to-Server-Flow (Seguir flujo de cliente a servidor)**.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

Al completar este paso, el cortafuegos puede marcar el tráfico con el mismo valor DSCP que se detectó al inicio de una sesión (en este ejemplo, el cortafuegos marcaría el tráfico de retorno con el valor DSCP AF11). Mientras que la configuración de QoS le permite moldear el tráfico conforme abandona el cortafuegos, habilitar esta opción en una regla de seguridad permite a los otros dispositivos de red

© 2020 Palo Alto Networks, Inc.

intermedios entre el cortafuegos y el cliente seguir aplicando la prioridad para el tráfico marcado con DSCP.

STEP 6 | Confirme la configuración.

Commit (Confirmar) los cambios.

© 2020 Palo Alto Networks, Inc.

Casos de uso de QoS

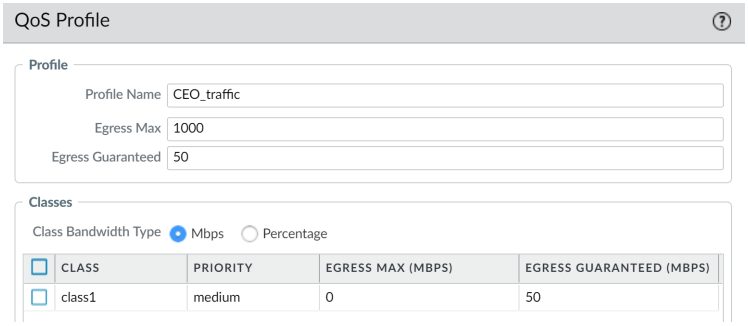
Los siguientes casos de uso demuestran cómo utilizar QoS en situaciones habituales:

- Caso de uso: QoS para un único usuario
- Caso de uso: QoS para aplicaciones de voz y vídeo

Caso de uso: QoS para un único usuario

Una directora ejecutiva observa que durante los periodos en los que la red se utiliza mucho, no puede acceder a aplicaciones empresariales para responder de manera eficaz a comunicaciones empresariales clave. El administrador de TI quiere asegurarse de que todo el tráfico hacia y desde la directora ejecutiva recibe un tratamiento preferente frente al tráfico de otros empleados, de manera que tenga garantizado, no solamente el acceso, sino un alto rendimiento de los recursos de red clave.

STEP 1 | El administrador crea el perfil de QoS ***CEO_traffic*** para definir el modo en que el tráfico originado en la directora ejecutiva se tratará y moldeará a medida que salga de la red empresarial:



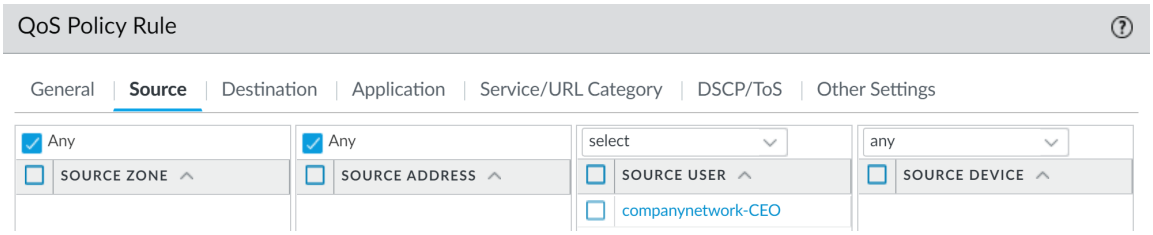
El administrador asigna un ancho de banda garantizado (**Egress Guaranteed [Salida garantizada]**) de 50 Mbps para garantizar que la directora ejecutiva disponga de esa cantidad de ancho de banda garantizado en todo momento (más de lo que necesitaría utilizar), independientemente de la congestión de la red.

El administrador sigue designando el tráfico de clase 1 como alta prioridad y establece el uso del ancho de banda máximo del perfil (**Egress Max [Máximo de salida]**) como 1000 Mbps, el mismo ancho de banda máximo para la interfaz en el que el administrador habilitará QoS. El administrador ha decidido no restringir el uso del ancho de banda de la directora ejecutiva de ningún modo.

La práctica recomendada es cumplimentar el campo Egress Max [Máximo de salida] para un perfil de QoS, aunque el ancho de banda máximo del perfil coincida con el ancho de banda máximo de la interfaz. El ancho de banda máximo del perfil de QoS nunca debería superar el ancho de banda máximo de la interfaz en la que tenga la intención de habilitar QoS.

STEP 2 | El administrador crea una política de QoS para identificar el tráfico de la directora ejecutiva (**Policies [Políticas]** > **QoS**) y asignarle la clase que definió en el perfil de QoS (consulte el paso anterior). Como se ha configurado User-ID, el administrador utiliza la pestaña **Source (Origen)**de la política de QoS para identificar de manera exclusiva el tráfico de la directora ejecutiva por su nombre de usuario de red empresarial. (Si no se ha configurado User-ID, el administrador podría **Add (Añadir)** la dirección IP de la directora ejecutiva bajo **Source Address (Dirección de origen)**. Consulte User-ID):

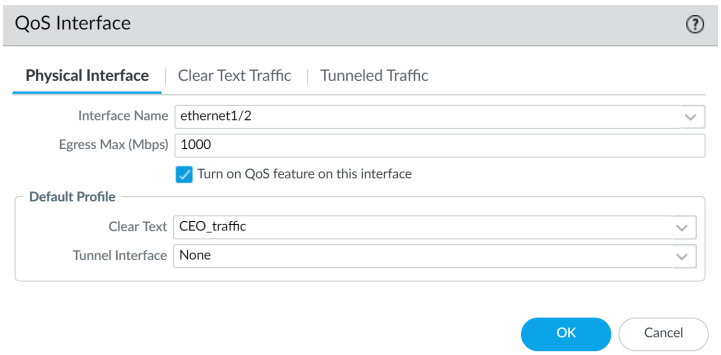
© 2020 Palo Alto Networks, Inc.



El administrador asocia el tráfico de la directora ejecutiva a la clase 1 en la pestaña **Other Settings (Otros ajustes)** y, a continuación, rellena los demás campos obligatorios de la política. El administrador asigna un nombre descriptivo a la política en el campo **Name (Nombre)** de la pestaña **General** y marca **Any (Cualquiera)** en la sección **Source Zone (Zona de origen)** de la pestaña **Source (Origen)** y en la sección **Destination Zone (Zona de destino)** de la pestaña **Destination (Destino)**:

	NAME	TAGS	Source				Destination			APPLICATION	SERVICE	DSCP/TOS	CLASS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1
3	Guarantee CEO bandwidth	none	any	any	companynet...	any	any	any	any	any	any	any	1

STEP 3 | Ahora que la clase 1 está asociada al tráfico de la directora ejecutiva, el administrador habilita QoS seleccionando **Dirección de origen (Activar la función QoS en esta interfaz)**y seleccionando la interfaz de salida del flujo de tráfico. La interfaz de salida del flujo de tráfico de la directora ejecutiva es la interfaz de orientación externa, en este caso, Ethernet 1/2:



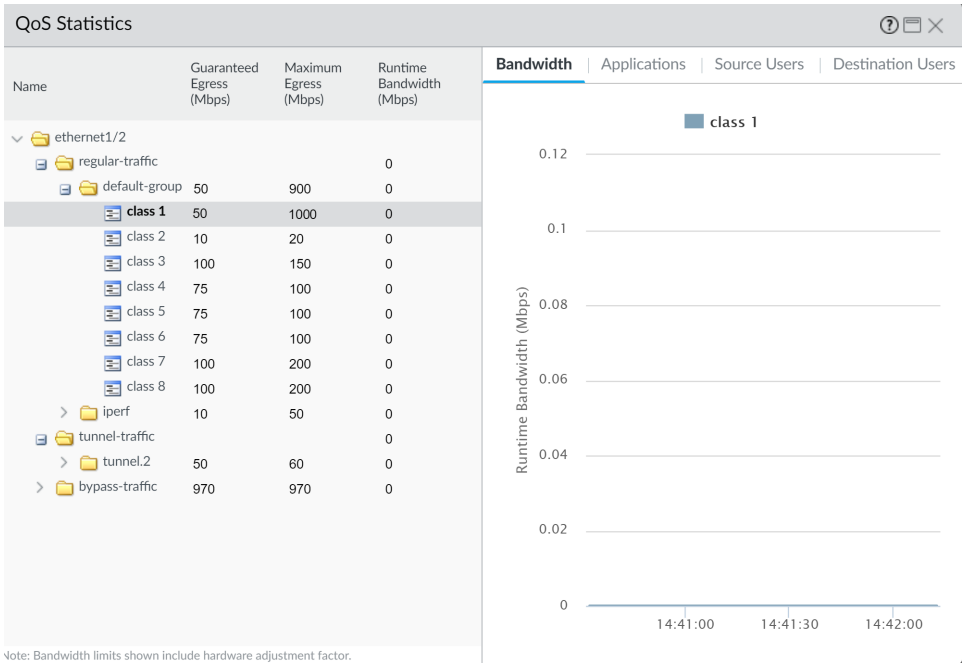
Como el administrador quiere asegurarse de que todo el tráfico originado en la directora ejecutiva está garantizado por el perfil de QoS y la política de QoS asociada que creó, selecciona *CEO_traffic* para aplicarlo al tráfico de tipo **Clear Text (No cifrado)** que se desplaza desde Ethernet 1/2.

STEP 4 | Después de confirmar la configuración de QoS, el administrador se desplaza a la página **Network (Red)** > **QoS** para confirmar que el perfil de QoS CEO_traffic está habilitado en la interfaz de orientación externa, Ethernet 1/2:

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/2		1,000.000		✓	Statistics
Tunneled Traffic					
Clear Text Traffic	50.000		CEO_traffic		

STEP 5 | Hace clic en **Statistics (Estadísticas)** para ver cómo se está moldeando el tráfico originado en la directora ejecutiva (clase 1) a medida que se desplaza desde Ethernet 1/2:

© 2020 Palo Alto Networks, Inc.



Este caso demuestra cómo aplicar QoS a tráfico originado en un único usuario de origen. Sin embargo, si también quisiera garantizar o moldear el tráfico para un usuario de destino, podría realizar una configuración de QoS similar. En lugar o además de este flujo de trabajo, cree una política de QoS que especifique la dirección IP del usuario como la Destination Address (Dirección de destino) en la página Policies (Políticas) > QoS (en lugar de especificar la información de origen del usuario) y, a continuación, habilite QoS en la interfaz de orientación interna de la red en la página Network (Red) > QoS (en lugar de la interfaz de orientación externa).

Caso de uso: QoS para aplicaciones de voz y vídeo

El tráfico de voz y vídeo es especialmente sensible a las mediciones que la función QoS moldea y controla, especialmente la latencia y la vibración. Para que las transmisiones de voz y vídeo sean audibles y claras, los paquetes de voz y vídeo no se pueden descartar, retrasar ni entregar de manera inconsistente. La práctica recomendada para aplicaciones de voz y vídeo, además de garantizar el ancho de banda, es garantizar la prioridad del tráfico de voz y vídeo.

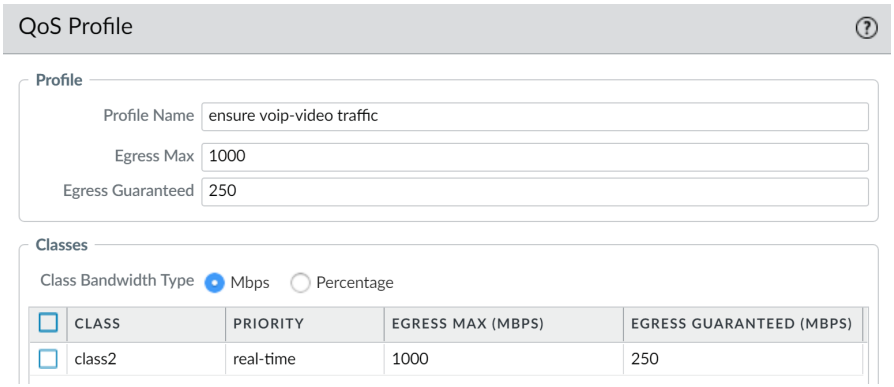
En este ejemplo, los empleados de una sucursal de la empresa están teniendo dificultades y experimentan una falta de fiabilidad al utilizar tecnologías de videoconferencia y voz sobre IP (VoIP) para realizar comunicaciones empresariales con otras sucursales, socios y clientes. Un administrador de TI tiene la intención de implementar QoS para solucionar estos problemas y garantizar una comunicación empresarial eficaz y fiable para los empleados de la sucursal. Como el administrador quiere garantizar QoS para el tráfico de red tanto entrante como saliente, habilitará QoS tanto en la interfaz de orientación interna como en la de orientación externa del cortafuegos.

STEP 1 | El administrador crea un perfil de QoS y define la clase 2 de forma que el tráfico asociado a la clase 2 reciba una prioridad en tiempo real y, en una interfaz con un ancho de banda máximo de 1000 Mbps, en todo momento, se garantizará un ancho de banda de 250 Mbps, incluyendo los períodos en los que más se utilice la red.

La prioridad en tiempo real suele recomendarse para las aplicaciones afectadas por la latencia y es de especial utilidad a la hora de garantizar el rendimiento y la calidad de aplicaciones de voz y vídeo.

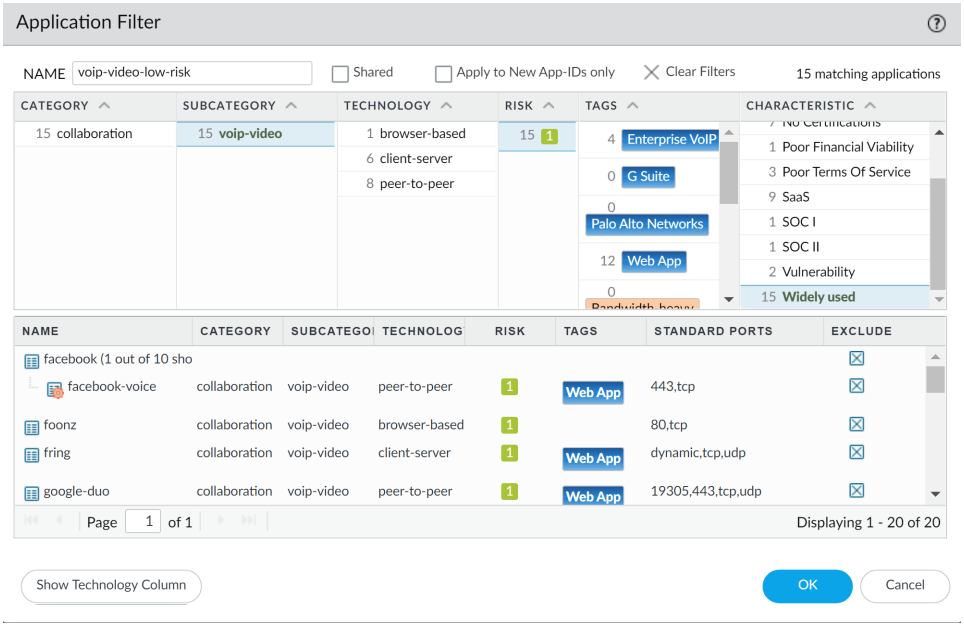
© 2020 Palo Alto Networks, Inc.

En la interfaz web del cortafuegos, el administrador selecciona **Network (Red)** > **Network Profiles (Perfiles de red)** > **Qos Profile (Perfil Qos)**, hace clic en **Add (Añadir)**, introduce el **Profile Name (Nombre del perfil)** ensure voip-video traffic y define el tráfico de clase 2.



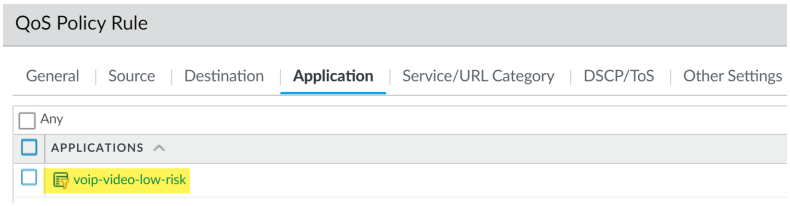
STEP 2 | El administrador crea una política de QoS para identificar el tráfico de voz y vídeo. Como la empresa no tiene una aplicación de voz y vídeo estándar, el administrador quiere asegurarse de que el QoS se aplica en un par de aplicaciones utilizadas ampliamente y con frecuencia por los empleados para comunicarse con otras oficinas, socios y clientes. En la pestaña **Policies (Políticas)** > **QoS** > **QoS Policy Rule (Regla de política de QoS)** > **Applications (Aplicaciones)**, el administrador hace clic en **Add (Añadir)** y abre la ventana **Application Filter (Filtro de aplicación)**. El administrador sigue seleccionando criterios para filtrar las aplicaciones en las que quiere aplicar el QoS, seleccionando la Subcategoría voip-video y restringiéndola al especificar únicamente aplicaciones de VoIP y vídeo que tengan un riesgo bajo y que se utilicen ampliamente.

El filtro de aplicación es una herramienta dinámica que, cuando se utiliza para filtrar aplicaciones en la política de QoS, permite aplicar QoS en todas las aplicaciones que cumplan los criterios de VoIP y vídeo, riesgo bajo y ampliamente utilizado en cualquier momento.



El administrador asigna al **Application Filter (Filtro de aplicación)** el nombre voip-video-low-risk y lo incluye en la política de QoS:

© 2020 Palo Alto Networks, Inc.

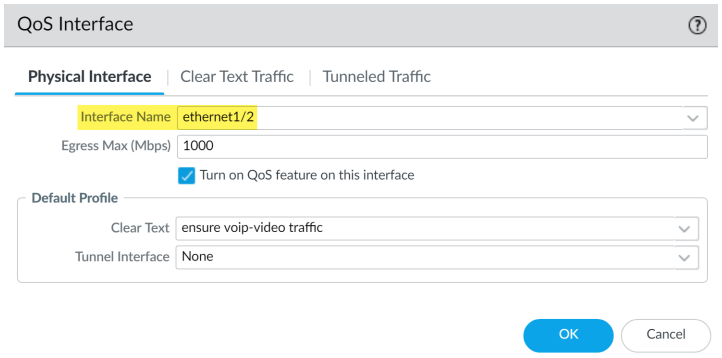


El administrador nombra la política de QoS comoVoice-Video y selecciona Other Settings para asignar el tráfico que coincide con la política de clase 2. Va a utilizar la política de QoS Voice-Video para el tráfico de QoS tanto entrante como saliente, así que establece la información de **Source (Origen)** y **Destination (Destino)** en **Any (Cualquiera)**:

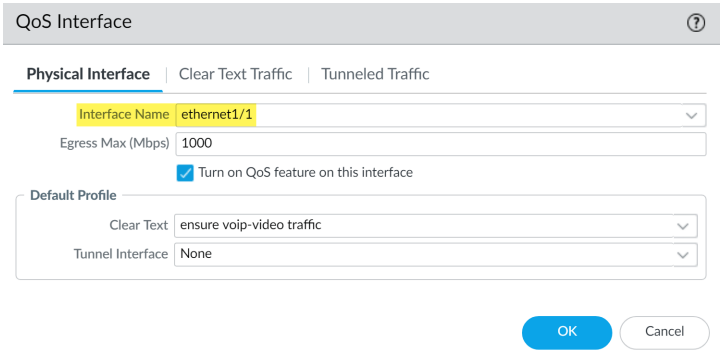
	NAME	TAGS	Source				Destination			APPLICATION	SERVICE	DSCP/TOS	CLASS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1

STEP 3 | Como el administrador quiere garantizar el QoS para comunicaciones de voz y vídeo tanto entrantes como salientes, habilita QoS en la interfaz de orientación externa de la red (para aplicar QoS a comunicaciones salientes) y en la interfaz de orientación interna (para aplicar QoS a comunicaciones entrantes).

El administrador empieza habilitando el perfil de QoS que creó, garantiza el tráfico de voz-vídeo (la clase 2 en este perfil está asociada con la política, voz-vídeo) en la interfaz de orientación externa, en este caso, Ethernet 1/2.



A continuación, habilita el mismo perfil de QoS, ensure voip-video traffic en una segunda interfaz, la interfaz de orientación interna (en este caso, Ethernet 1/1).



STEP 4 | El administrador selecciona **Network (Red)** > **QoS** para confirmar que el QoS se ha habilitado tanto para el tráfico de voz y vídeo entrante como para el saliente:

© 2020 Palo Alto Networks, Inc.

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/1		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		
ethernet1/2		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		

El administrador ha habilitado el QoS correctamente tanto en la interfaz de orientación interna de la red como en la externa. Ahora se garantiza la prioridad en tiempo real para el tráfico de aplicaciones de voz y vídeo a medida que se desplaza hacia adentro y hacia afuera de la red, garantizando que estas comunicaciones, que son especialmente sensibles a la latencia y la vibración, puedan utilizarse de manera fiable y eficaz para realizar comunicaciones empresariales tanto internas como externas.

© 2020 Palo Alto Networks, Inc.

VPN

Las redes privadas virtuales (VPN) crean túneles que permiten que los usuarios o sistemas se conecten de manera segura a través de una red pública como si se estuvieran conectando a través de una red de área local (LAN). Para configurar un túnel VPN, hacen falta dos dispositivos que puedan autenticarse mutuamente y cifrar el flujo de información entre ellos. Los dispositivos pueden ser una pareja de cortafuegos de Palo Alto Networks, o bien un cortafuegos de Palo Alto Networks y un dispositivo de otro proveedor con capacidad para VPN.

- Implementaciones de VPN
- Descripción general de VPN de sitio a sitio
- Conceptos de VPN de sitio a sitio
- Configuración de VPN de sitio a sitio
- Configuraciones rápidas de VPN de sitio a sitio

© 2020 Palo Alto Networks, Inc.

Implementaciones de VPN

El cortafuegos de Palo Alto Networks admite las siguientes implementaciones de VPN:

- **VPN de sitio a sitio**: Una VPN sencilla que se conecta a un sitio central y a un sitio remoto, o bien una VPN hub and spoke que se conecta a un sitio central con múltiples sitios remotos. El cortafuegos usa el conjunto de protocolos de Seguridad IP (IPSec) para configurar un túnel seguro entre los dos sitios. Consulte Descripción general de VPN de sitio a sitio.
- **VPN de usuario remoto a sitio**: Una solución que usa el agente GlobalProtect para permitir a un usuario remoto establecer una conexión segura a través del cortafuegos. Esta solución usa SSL e IPSec para establecer una conexión segura entre el usuario y el sitio. Consulte la GlobalProtect Administrator's Guide (Guía del administrador de GlobalProtect).
- **VPN a gran escala**: La VPN a gran escala de GlobalProtect de Palo Alto Networks (LSVPN) ofrece un mecanismo simplificado para implementar una VPN hub and spoke con un máximo de 1.024 oficinas satélite. Esta solución requiere que haya cortafuegos de Palo Alto Networks implementados en el concentrador y en todos los radios. Usa certificados para la autenticación de dispositivos, SSL para la protección entre todos los componentes e IPSec para proteger los datos. Consulte Large Scale VPN (LSVPN) (VPN a gran escala (LSVPN)).

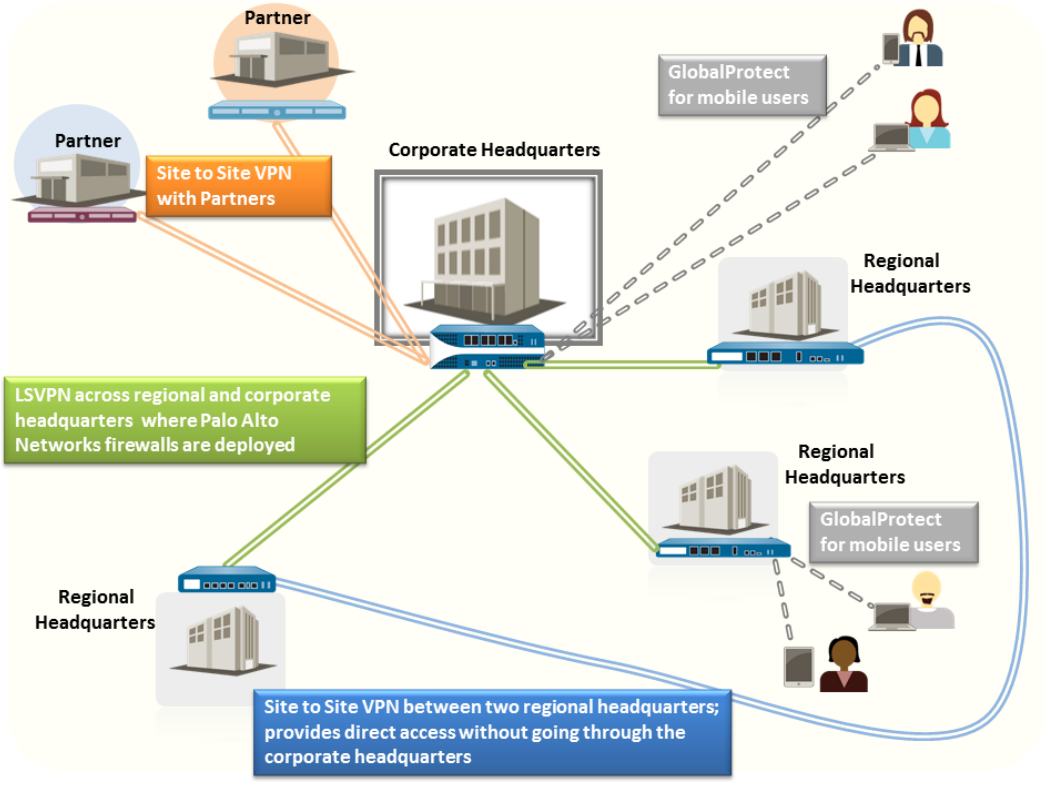


Figure 8: Implementaciones de VPN

© 2020 Palo Alto Networks, Inc.

Descripción general de VPN de sitio a sitio

Una conexión VPN que permita conectar dos redes de área local (LAN) se llama VPN de sitio a sitio. Puede configurar VPN basadas en rutas para conectar cortafuegos de Palo Alto Networks en dos ubicaciones, o bien conectar cortafuegos de Palo Alto Networks a dispositivos de seguridad de terceros en otras ubicaciones. El cortafuegos también puede interoperar con dispositivos VPN basados en políticas de terceros; el cortafuegos de Palo Alto Networks es compatible con VPN basado en rutas.

El cortafuegos de Palo Alto Networks configura una VPN basada en rutas, donde el cortafuegos toma una decisión de enrutamiento basada en la dirección IP de destino. Si el tráfico se enruta a un destino específico a través de un túnel de VPN, se cifrará como tráfico VPN.

El conjunto de protocolos de seguridad IP (IPSec) se utiliza para configurar un túnel seguro para el tráfico VPN. Asimismo, la información de los paquetes de TCP/IP está protegida (y cifrada si el tipo de túnel es ESP). El paquete IP (encabezado y carga) está incrustado en otra carga de IP, se aplica un nuevo encabezado y se envía a través del túnel IPSec. La dirección IP de origen en el nuevo encabezado es la del peer VPN local y la dirección IP de destino es la del peer VPN del otro extremo del túnel. Cuando el paquete llega al peer VPN remoto (el cortafuegos en el otro extremo del túnel), el encabezado exterior se elimina y se envía el paquete original a su destino.

Para configurar el túnel VPN, primero deben autenticarse los peers. Tras autenticarse correctamente, los peers negocian los algoritmos y el mecanismo de cifrado para proteger la comunicación. El proceso de Intercambio de claves por red (IKE) se usa para autenticar a los peers VPN, y las asociaciones de seguridad (SA) IPSec se definen en cada extremo del túnel para proteger la comunicación VPN. IKE usa certificados digitales o claves compartidas previamente, así como las claves Diffie-Hellman para configurar las SA del túnel de IPSec. Las SA especifican todos los parámetros obligatorios para el cifrado de la transmisión segura (incluyendo el índice de parámetros de seguridad [security parameter index, SPI], el protocolo de seguridad, las claves criptográficas y la dirección IP de destino), la autenticación de los datos, la integridad de los datos y la autenticación de los terminales.

La siguiente ilustración muestra un túnel de VPN entre dos sitios. Cuando un cliente que está protegido por el peer A de la VPN necesita contenido de un servidor ubicado en el otro sitio, el peer A de la VPN inicia una solicitud de conexión al peer B de la VPN. Si la política de seguridad permite la conexión, el peer A de la VPN usa los parámetros del perfil criptográfico IKE (IKE de fase 1) para establecer una conexión segura y autenticar al peer B de la VPN. A continuación, el peer A de la VPN establece el túnel VPN usando el perfil criptográfico IPSec, que define los parámetros del IKE de fase 2 para permitir la transferencia segura de datos entre los dos sitios.



Figure 9: VPN de sitio a sitio

© 2020 Palo Alto Networks, Inc.

Conceptos de VPN de sitio a sitio

Una conexión VPN ofrece acceso seguro a la información entre dos o más sitios. Para proporcionar acceso seguro a los recursos y una conectividad fiable, una conexión VPN necesita los siguientes componentes:

- Puerta de enlace de IKE
- Interfaz túnel
- Monitorización de túnel
- Intercambio de claves por red (IKE) para VPN
- IKEv2

Puerta de enlace de IKE

Los cortafuegos Palo Alto Networks o un cortafuegos y otro dispositivo de seguridad que inicien y terminen conexiones VPN entre dos redes se llaman gateways IKE. Para configurar el túnel VPN y enviar tráfico entre los gateways IKE, cada peer debe tener una dirección IP (estática o dinámica) o FQDN. Los peers VPN usan claves previamente compartidas o certificados para autenticarse mutuamente.

Los peers también deben negociar el modo (principal o agresivo) para configurar la duración del túnel VPN y la SA en IKE de fase 1. El modo principal protege la identidad de los peers y es más seguro porque se intercambian más paquetes al configurar el túnel. Si ambos peers lo admiten, el modo principal es el recomendado para la negociación IKE. El modo agresivo usa menos paquetes para configurar el túnel VPN, por lo que es una opción más rápida, aunque menos segura, de configurar el túnel VPN.

Consulte Configuración de una puerta de enlace de IKE para obtener información detallada sobre la configuración.

Interfaz túnel

Para configurar un túnel VPN, la interfaz de capa 3 en cada extremo debe tener una interfaz de *túnel* lógica para que el cortafuegos se conecte y establezca un túnel VPN. Una interfaz de túnel es una interfaz (virtual) lógica que se usa para enviar tráfico entre dos extremos. Si configura ID proxy, la ID proxy se considera en la capacidad total del túnel IPSec.

La interfaz de túnel debe pertenecer a una zona de seguridad para aplicar una política; asimismo, debe estar asignada a un enrutador virtual para usar la infraestructura de enrutamiento existente. Compruebe que la interfaz de túnel y la interfaz física estén asignadas al mismo enrutador virtual, de modo que el cortafuegos pueda realizar una búsqueda de rutas y determinar el mejor túnel que puede usar.

Normalmente, la interfaz de capa 3 a la que está vinculada la interfaz de túnel pertenece a una zona externa, por ejemplo, la zona no fiable. Aunque la interfaz de túnel puede estar en la misma zona de seguridad que la interfaz física, puede crear una zona separada para la interfaz de túnel con el fin de lograr una mayor seguridad y mejor visibilidad. Si crea una zona separada para la interfaz de túnel (p. ej., una zona VPN), necesitará crear políticas de seguridad que habiliten el flujo del tráfico entre la zona VPN y la zona fiable.

Para enrutar tráfico entre los sitios, una interfaz de túnel no necesita una dirección IP. Solo es necesaria una dirección IP si quiere habilitar la supervisión de túneles o si está usando un protocolo de enrutamiento dinámico para enrutar tráfico a través del túnel. Con enrutamiento dinámico, la dirección IP del túnel funciona como dirección IP de próximo salto para el enrutamiento de tráfico al túnel VPN.

Si está configurando el cortafuegos Palo Alto Networks con un peer VPN que utiliza una VPN basada en políticas, debe configurar un ID de proxy local y remoto cuando configure el túnel IPSec. Cada peer compara los ID de proxy que tiene configurados con lo que se recibe realmente en el paquete para permitir una negociación IKE de fase 2 correcta. Si se requieren varios túneles, configure ID de proxy exclusivos para cada interfaz de túnel; una interfaz de túnel puede tener un máximo de 250 ID de proxy. Cada ID de proxy

© 2020 Palo Alto Networks, Inc.

se tendrá en cuenta a la hora de calcular la capacidad del túnel VPN IPSec del cortafuegos, y la capacidad del túnel varía en función del modelo de cortafuegos.

Consulte Configuración de un túnel de IPSec para obtener información detallada sobre la configuración.

Monitorización de túnel

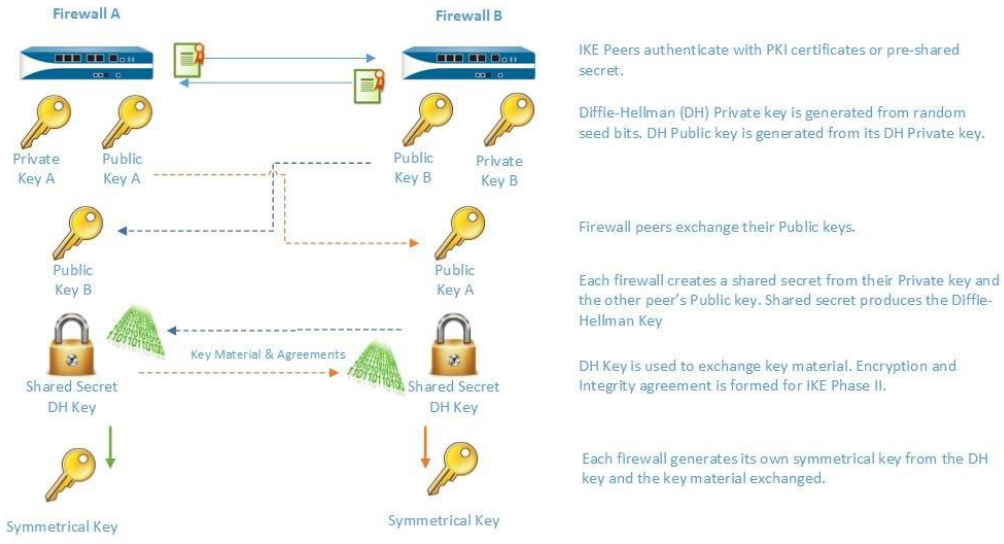
Para un túnel VPN, puede comprobar la conectividad con una dirección IP de destino a través del túnel. El perfil de supervisión de la red del cortafuegos le permite verificar la conectividad (mediante ICMP) con una dirección IP de destino o un próximo salto en el intervalo de sondeo especificado, así como especificar una acción o fallo para acceder a la dirección IP supervisada.

Si no es posible alcanzar la IP de destino, puede configurar el cortafuegos para que espere a que se recupere el túnel o configurar una conmutación por error a otro túnel. En cada caso, el cortafuegos genera un log de sistema que le alerta de un fallo del túnel y renegocia las claves IPSec para acelerar la recuperación.

Consulte Configuración de la supervisión de túnel para obtener información detallada sobre la configuración.

Intercambio de claves por red (IKE) para VPN

El proceso IKE permite a los peers VPN en ambos extremos del túnel cifrar y descifrar paquetes usando claves o certificados acordados mutuamente y un método de cifrado. El proceso IKE se realiza en dos fases: IKE de fase 1 y IKE de fase 2. Cada una de estas fases usa claves y algoritmos de cifrado que se definen usando perfiles criptográficos (perfil criptográfico IKE y perfil criptográfico IPSec), y el resultado de la negociación IKE es una asociación de seguridad (SA). Una SA es un conjunto de claves y algoritmos acordados mutuamente usados por ambos peers VPN para permitir el flujo de datos a través del túnel VPN. La siguiente ilustración muestra el proceso de intercambio de claves para configurar un túnel VPN:



IKE de fase 1

En esta fase, los cortafuegos usan los parámetros definidos en la configuración del gateway IKE y el perfil criptográfico IKE para autenticarse mutuamente y establecer un canal de control. La fase IKE es compatible con el uso de claves compartidas previamente o certificados digitales (que usan infraestructuras de claves públicas, PKI) para la autenticación mutua de los peers VPN. Las claves previamente compartidas son una solución sencilla para proteger redes pequeñas, ya que no necesitan ser compatibles con una infraestructura PKI. Los certificados digitales pueden ser más adecuados para redes o implementaciones de mayor tamaño que requieren de mayor seguridad para la autenticación.

© 2020 Palo Alto Networks, Inc.

Al usar certificados, asegúrese de que la CA que emite el certificado es de confianza para ambos peers del gateway y que la longitud máxima de la cadena de certificados es 5 o menos. Con la fragmentación IKE habilitada, el cortafuegos puede volver a juntar mensajes IKE con hasta 5 certificados en la cadena de certificados y establecer correctamente el túnel VPN.

El perfil criptográfico IKE define las siguientes opciones que se usan en la negociación de SA IKE:

- Grupo Diffie-Hellman (DH) para la generación de claves simétricas para IKE.

  El algoritmo Diffie Hellman usa la clave privada de una parte y la clave pública de la otra para crear un secreto compartido, que es una clave cifrada compartida por ambos peers del túnel VPN. Los grupos DH compatibles con el cortafuegos son: grupo 1: 768 bits; grupo 2: 1024 bits (predeterminado); grupo 5: 1536 bits; grupo 14: 2048 bits, grupo 19: grupo de curva elíptica de 256 bits y grupo 20: grupo de curva elíptica de 384 bits.
- Algoritmos de autenticación: sha1; sha 256; sha 384; sha 512 o md5
- Algoritmos de cifrado: 3des, aes-128-cbc, aes-192-cbc o aes-256-cbc o des.

IKE de fase 2

Una vez protegido y autenticado el túnel, en la fase 2 se aumenta la protección del canal para la transferencia de datos entre las redes. IKE de fase 2 usa las claves que se establecieron en la fase 1 del proceso y el perfil criptográfico IPSec, que define los protocolos y las claves IPSec usadas para la SA en el IKE de fase 2.

IPSEC usa los siguientes protocolos para habilitar una comunicación segura:

- Encapsulating Security Payload (ESP): Le permite cifrar el paquete de IP completo, así como autenticar la fuente y verificar la integridad de los datos. Mientras que ESP necesita que cifre y autentique el paquete, puede elegir solo cifrar o solo autenticar definiendo la opción de cifrado como Null; no se recomienda usar cifrado sin autenticación.
- Authentication header (AH): Autentica el origen del paquete y verifica la integridad de datos. AH no cifra la carga de datos y se desaconseja su uso en implementaciones en las que es importante la privacidad de los datos. AH se suele usar cuando el principal objetivo es verificar la legitimidad del peer y no se requiere privacidad de datos.

Table 5: Algoritmos compatibles con cifrado y autenticación IPSEC

ESP	AH
Opciones de intercambio de Diffie Hellman (DH) compatibles	
• Grupo 1: 768 bits • Grupo 2: 1024 bits (predeterminado) • Grupo 5: 1536 bits • Grupo 14: 2048 bits. • Grupo 19: grupo de curva elíptica de 256 bits • Grupo 20: grupo de curva elíptica de 384 bits • No-pfs: De manera predeterminada, perfect forward secrecy (PFS) está habilitado, lo que significa que se genera una nueva clave DH en IKE de fase 2 usando uno de los grupos enumerados arriba. Esta clave es independiente de las claves intercambiadas en IKE de fase 1 y ofrece una mejor transferencia de datos. Si selecciona no-pfs, la clave DH creada en la fase 1 no se renueva y se usa una única clave para las negociaciones con la SA IPSec. Ambos peers VPN deben estar habilitados o deshabilitados para PFS.	
Algoritmos de cifrado compatibles	

© 2020 Palo Alto Networks, Inc.

ESP	AH
• 3des	Estándar de cifrado triple de datos (3DES) con una fuerza de seguridad de 112 bits
• aes-128-cbc	Estándar de cifrado avanzado (AES) usando encadenamiento de bloques de cifras (CBC) con una fuerza de seguridad de 128 bits
• aes-192-cbc	AES usando CBC con una fuerza de seguridad de 192 bits
• aes-256-cbc	AES usando CBC con una fuerza de seguridad de 256 bits
• aes-128-ccm	AES usando Counter CBC-MAC (CCM) con una fuerza de seguridad de 128 bits
• aes-128-gcm	AES usando Modo Galois/Counter (GCM) con una fuerza de seguridad de 128 bits
• aes-256-gcm	AES usando GCM con una fuerza de seguridad de 256 bits
• des	Estándar de cifrado de datos (Data Encryption Standard, DES) con una fuerza de seguridad de 56 bits
Algoritmos de autenticación compatibles	
• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

Métodos de protección de túneles VPN IPSec (IKE de fase 2)

Los túneles VPN IPSec se pueden proteger usando claves manuales o automáticas. Asimismo, las opciones de configuración IPSec incluyen un grupo Diffie-Hellman para acordar claves o un algoritmo de cifrado y un hash para la autenticación de mensajes.

- **Clave manual**: La clave manual se suele usar si el cortafuegos Palo Alto Networks está estableciendo un túnel VPN con un dispositivo antiguo o si quiere reducir los gastos de la generación de claves de sesión. Si usa claves manuales, debe configurarse la misma en ambos peers.

  Las claves manuales no son recomendables para establecer un túnel VPN porque las claves de sesión pueden verse comprometidas cuando transmitan la información de claves entre peers; si las claves ven comprometida su seguridad, la transferencia de datos deja de ser segura.
- **Clave automática**: La clave automática le permite generar claves automáticamente para configurar y mantener el túnel IPSec basado en algoritmos definidos en el perfil criptográfico IPSec.

© 2020 Palo Alto Networks, Inc.

IKEv2

Una puerta de enlace de VPN IPSec usa IKEv1 o IKEv2 para negociar la asociación de seguridad IKE (SA) y el túnel IPSec. IKEv2 se define en RFC 5996.

A diferencia IKEv1, que usa Phase 1 SA y Phase 2 SA, IKEv2 usa una SA secundaria para Encapsulating Security Payload (ESP) o Authentication Header (AH), que se configura con una SA IKE.

Debe habilitarse NAT transversal (NAT-T) en ambos gateways si tiene NAT habilitada en un dispositivo situado entre dos gateways. Una puerta de enlace solo puede ver la dirección IP pública (enrutable globalmente) del dispositivo NAT.

IKEv2 ofrece las siguientes ventajas con respecto a IKEv1:

- Los extremos de túnel intercambian menos mensajes para establecer un túnel. IKEv2 usa cuatro mensajes; IKEv1 usa nueve mensajes (en el modo principal) o seis mensajes (en el modo agresivo).
- La funcionalidad NAT-T integrada mejora la compatibilidad entre proveedores.
- La comprobación de estado integrada se restablece automáticamente si un túnel deja de estar disponible. La comprobación de actividad sustituye la Detección de fallo del peer usada en IKEv1.
- Admite selectores de tráfico (uno por intercambio). Los selectores de tráfico se usan en las negociaciones IKE para controlar qué tráfico puede acceder al túnel.
- Admite intercambio de certificados de Hash y URL para reducir la fragmentación.
- Resiliencia ante ataques de denegación de servicio con validación de peers mejorada. Un número excesivo de SA medio abiertas puede activar la validación de cookies.

Antes de configurar IKEv2, debería estar familiarizado con los siguientes conceptos.

- Comprobación de actividad
- Umbral de activación de cookies y validación de cookies estricta
- Selectores de tráfico
- Intercambio de certificados Hash y URL
- Duración de la clave de SA e intervalo de reautenticación

Cuando haya realizado la Configuración de una puerta de enlace de IKE, si elige IKEv2, realice las siguientes tareas opcionales relacionadas con IKEv2 como se requiere en su entorno:

- Exportación de un certificado para un peer para acceder usando Hash y URL
- Importación de un certificado para Autenticación de puerta de enlace IKEv2
- Cambio de la duración de la clave o del intervalo de autenticación IKEv2
- Cambio del umbral de activación de cookies para IKEv2
- Configuración de selectores de tráfico IKEv2

Comprobación de actividad

La comprobación de actividad IKEv2 es similar a Detección de fallo del peer (DPD), que IKEv1 usa para determinar si un peer sigue disponible.

En IKEv2, la comprobación de actividad la logra cualquier transmisión de paquete IKEv2 o mensaje de información vacío que envíe el gateway al peer en un intervalo configurable (predeterminado: cinco segundos). En caso necesario, el remitente intenta la retransmisión hasta diez veces. Si no recibe respuesta, el remitente cierra y elimina la IKE_SA y las CHILD_SA correspondientes. El remitente empezará de nuevo enviando otro mensaje IKE_SA_INIT.

Umbral de activación de cookies y validación de cookies estricta

La validación de cookies siempre está habilitada para IKEv2; ayuda a proteger contra ataques DoS de media SA. Puede configurar el número de umbral global de SA a medio abrir que activará la validación de cookies.

© 2020 Palo Alto Networks, Inc.

También puede activar gateways IKE individuales para garantizar que se realiza la validación de cookies para cada SA IKEv2 nueva.

- El **Cookie Activation Threshold (Umbral de activación de cookies)** es una configuración de sesión VPN global que limita el número de SA IKE a medio abrir simultáneas (el valor predeterminado es de 500). Si el número de SA IKE a medio abrir supera el **Cookie Activation Threshold**, el respondedor solicitará una cookie y el iniciador deberá responder con una IKE_SA_INIT que contenga una cookie para validar la conexión. Si la cookie se valida correctamente, se puede iniciar otra SA. Un valor de 0 significa que la validación de cookies está siempre activa.

  El respondedor no mantiene un estado del iniciador ni realiza un intercambio de claves Diffie-Hellman hasta que el iniciador devuelva la cookie. La validación de cookies IKEv2 mitiga un ataque de denegación de servicio que podría intentar dejar numerosas conexiones a medio abrir.

  El **Cookie Activation Threshold (Umbral de activación de cookies)** debe ser inferior que el valor de **Maximum Half Opened SA (SA semiabiertas máximas)**. Si ha realizado un a un número muy alto (por ejemplo, 65534) y el ajuste **Maximum Half Opened SA (SA medio abiertas máx.)** se mantiene en el valor por defecto de 65535, la validación de cookies está esencialmente deshabilitada.
- Puede habilitar **Strict Cookie Validation** si desea que se realice la validación de cookies para cada SA IKEv2 que reciba la puerta de enlace, independientemente del umbral global. La **Strict Cookie Validation (Validación estricta de cookies)** afecta solo a la puerta de enlace que se está configurando y está deshabilitada por defecto. Si **Strict Cookie Validation (Validación estricta de cookies)** está deshabilitada, el sistema usa el **Cookie Activation Threshold (Umbral de activación de cookies)** para determinar si se necesita o no una cookie.

Selectores de tráfico

En IKEv1, un cortafuegos que tiene una VPN basada en rutas necesita usar un ID de proxy local y remoto para configurar un túnel IPSec. Cada peer compara los ID de proxy con lo que se recibe realmente en el paquete para permitir una negociación IKE de fase 2 correcta. El IKE de fase 2 consiste en negociar las SA para configurar un túnel IPSec. (Para obtener más información sobre los ID de proxy, consulte Interfaz túnel).

En IKEv2, puede realizar una Configuración de selectores de tráfico IKEv2, que son componentes de tráfico de red que se usan durante la negociación IKE. Los selectores de tráfico se usan durante la CHILD_SA (creación de túnel) de fase 2 para configurar el túnel y determinar qué tráfico está permitido a través del túnel. Los dos peers de puerta de enlace IKE deben negociar y acordar sus selectores de tráfico; de lo contrario, una parte estrecha su intervalo de direcciones para acuerdo. Una conexión IKE puede tener múltiples túneles; por ejemplo, puede asignar diferentes túneles a cada departamento para aislar su tráfico. La separación de tráfico también permite implementar funciones como QoS.

Los selectores de tráfico IPv4 e IPv6 son:

- **Dirección IP de origen**: Un prefijo de red, intervalo de dirección, host específico o un comodín.
- **Dirección IP de destino**: Un prefijo de red, intervalo de dirección, host específico o un comodín.
- **Protocolo**: un protocolo de transporte, como TCP o UDP.
- **Puerto de origen**: el puerto donde se ha originado el paquete.
- **Puerto de destino**: El puerto al que está destinado el paquete.

Durante la negociación IKE, puede haber múltiples selectores de tráfico para diferentes redes y protocolos. Por ejemplo, el Iniciador puede indicar que quiere enviar paquetes TCP desde 172.168.0.0/16 a través del túnel a su peer, destinado a 198.5.0.0/16. También quiere enviar paquetes UDP desde 172.17.0.0/16 a través del mismo túnel a la misma puerta de enlace, con destino a 0.0.0.0 (cualquier red). La puerta de enlace de peers debe coincidir con estos selectores de tráfico para que sepa qué esperar.

Es posible que una puerta de enlace empiece la negociación usando un selector de tráfico que sea una dirección IP más específica que la dirección de la otra puerta de enlace.

© 2020 Palo Alto Networks, Inc.

- Por ejemplo, la puerta de enlace A ofrece una dirección IP de origen de 172.16.0.0/16 y la dirección IP de destino 192.16.0.0/16. Pero la puerta de enlace B se configura con 0.0.0.0 (cualquier origen) como la dirección IP de origen y 0.0.0.0 (cualquier destino) como la dirección IP de destino. Por lo tanto, la puerta de enlace B restringe la dirección IP de origen a 192.16.0.0/16 y la dirección de destino 172.16.0.0/16. Así, la restricción adapta la dirección del gateway A y los selectores de tráfico de las dos gateways están de acuerdo.
- Si la puerta de enlace B (configurada con dirección IP 0.0.0.0) es el Iniciador en lugar del Respondedor, la puerta de enlace A responderá con sus direcciones IP más específicas, y la puerta de enlace B restringirá sus direcciones para llegar a un acuerdo.

Intercambio de certificados Hash y URL

IKEv2 admite Intercambio de certificados Hash y URL, que se usa durante una negociación IKEv2 de una SA. Almacene el certificado en un servidor HTTP, que se especifica mediante una URL. El peer recupera el certificado del servidor basándose en la recepción de la URL al servidor. El hash se usa para comprobar si el contenido del certificado es válido o no. Por tanto, los dos peers intercambian certificados con la CA HTTP en lugar de hacerlo entre sí.

La parte hash de Hash y URL reduce el tamaño del mensaje y de este modo Hash y URL es un modo de reducir la probabilidad de fragmentación de paquetes durante la negociación IKE. El peer recibe el certificado y el hash esperados, y por tanto la primera fase IKE ha validado el peer. La reducción de la fragmentación ayuda a proteger contra ataques de denegación de servicio.

Puede habilitar el intercambio de certificados hash y URL al configurar una puerta de enlace IKE al seleccionar **HTTP Certificate Exchange** e introducir la **Certificate URL**. El peer también debe usar el intercambio de certificados Hash y URL para que el intercambio se realice correctamente. Si el peer no puede usar Hash y URL, los certificados X.509 se intercambian de forma parecida a como lo hacen en IKEv1.

Si habilita el intercambio de certificados Hash y URL, debe exportar su certificado al servidor de certificados si aún no está allí. Al exportar el certificado, el formato de archivo debería ser **Binary Encoded Certificate (DER)**. Consulte Exportación de un certificado para un peer para acceder usando Hash y URL.

Duración de la clave de SA e intervalo de reautenticación

En IKEv2, dos valores de perfil criptográfico IKE, **Key Lifetime** y **IKEv2 Authentication Multiple**, controlan el establecimiento de SA IKE IKEv2. La duración de la clave es el tiempo de validez de una clave SA IKE negociada. Antes de que venza la clave, se deberá volver a asignar la clave de registro de SA; de no ser así, cuando llegue el vencimiento, la SA deberá comenzar una nueva asignación de claves SA IKE IKEv2. El valor predeterminado es de 8 horas.

El intervalo de reautenticación se obtiene al multiplicar la **Key Lifetime (Duración de la clave)** por **IKEv2 Authentication Multiple (Múltiplo de autenticación IKEv2)**. La autenticación múltiple es 0 de manera predeterminada, lo que deshabilita la función de reautenticación.

El intervalo del múltiplo de autenticación es 0-50. De modo que si va a configurar una autenticación múltiple de 20, por ejemplo, el sistema realizaría una reautenticación cada 20 asignaciones de clave, es decir, cada 160 horas. Eso significa que la puerta de enlace podría crear SA secundarias durante 160 horas antes de tener que reautenticarse con IKE para recrear la SA IKE desde cero.

En IKEv2, las puertas de enlace del Iniciador y el Respondedor tienen su propio valor de duración de clave, y el gateway con la duración de clave más breve es la que solicitará la reasignación de claves de SA.

© 2020 Palo Alto Networks, Inc.

Configuración de VPN de sitio a sitio

Para configurar VPN de sitio a sitio:

- Asegúrese de que sus interfaces Ethernet, enrutadores virtuales y zonas están configurados correctamente. Si desea más información, consulte Configuración de interfaces y zonas.
- Cree sus interfaces de túnel. Lo ideal sería colocar las interfaces de túnel en una zona separada para que el tráfico de túnel pueda utilizar políticas diferentes.
- Configure rutas estáticas o asigne protocolos de enrutamiento para redirigir el tráfico a los túneles VPN. Para admitir el enrutamiento dinámico (son compatibles OSPF, BGP, RIP), debe asignar una dirección IP a la interfaz del túnel.
- Defina puertas de enlace IKE para establecer comunicación entre peers a cada lado del túnel VPN; defina también el perfil criptográfico que especifica los protocolos y algoritmos para identificación, autenticación y cifrado que se usarán para configurar túneles VPN en IKEv1 de fase 1. Consulte Configuración de un puerto de enlace de IKE y Definición de perfiles criptográficos de IKE.
- Configure los parámetros necesarios para establecer la conexión IPSec para transferencia de datos a través del túnel VPN; consulte Configuración de un túnel IPSec. En IKEv1 de fase 2, consulte la Definición de perfiles criptográficos de IPSec.
- (Opcional) Especifique el modo en que el cortafuegos supervisará los túneles IPSec. Consulte la Configuración de la supervisión de túnel.
- Defina políticas de seguridad para filtrar e inspeccionar el tráfico.

Si hay una regla de denegación en el extremo de la base de reglas de seguridad, el tráfico intrazona se bloquea a menos que se permita de otro modo. Las reglas para permitir aplicaciones IKE e IPSec deben incluirse de manera explícita por encima de la regla de denegación.

Si el tráfico de su VPN atraviesa un cortafuegos serie PA-7000 o PA-5200 (no se origina ni finaliza en él), configura reglas de la política de seguridad bidireccional para permitir el tráfico de ESP o AH en ambas direcciones.

Cuando haya terminado estas tareas, el túnel estará listo para su uso. El tráfico destinado a zonas/direcciones definidas en la política se enruta automáticamente correctamente basándose en la ruta de destino de la tabla de enrutamiento y se gestiona como tráfico VPN. Para ver algunos ejemplos de VPN de sitio a sitio, consulte Configuraciones rápidas de VPN de sitio a sitio.

Para solucionar problemas, puede implementar la Habilitación/deshabilitación, actualización o reinicio de un puerto de enlace de KE o túnel IPSec.

Configuración de una puerta de enlace de IKE

Para configurar un túnel VPN, los peers o puertas de enlace VPN deben autenticarse mutuamente, utilizando claves previamente compartidas o certificados digitales, y establecer un canal seguro para negociar la asociación de seguridad (security association, SA) IPSec que se utilizará para proteger el tráfico entre los hosts en ambos lados.

STEP 1 | Defina la puerta de enlace de IKE.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)**, haga clic en **Add (Añadir)** para añadir una puerta de enlace e introduzca un **Name (Nombre)** para la puerta de enlace (pestaña **General**).
2. Establezca **Version (Versión)** en **IKEv1 only mode (Modo exclusivo IKEv1)**, **IKEv2 only mode (Modo exclusivo IKEv2)** o **IKEv2 preferred mode (Modo preferido IKEv2)**. La puerta de enlace IKE comienza

© 2020 Palo Alto Networks, Inc.

su negociación con su peer en el modo que especifica aquí. Si selecciona **IKEv2 preferred mode** los dos peers usarán IKEv2 si el peer remoto lo admite; de lo contrario, usarán IKEv1.

La selección de **Version (Versión)** también determina qué opciones están disponibles en la pestaña **Advanced Options (Opciones avanzadas)**.

STEP 2 | Establezca el endpoint local del túnel (puerta de enlace).

1. Seleccione el **Address Type (Tipo de dirección)**: **IPv4** o **IPv6**.
2. Seleccione la **Interface (Interfaz)** física de salida en el cortafuegos donde reside la puerta de enlace local.
3. En la lista **Local IP Address (Dirección IP local)**, seleccione la dirección IP que debe utilizar la conexión VPN como terminal; esta es la interfaz externa con una dirección IP del cortafuegos enrutable de forma pública.

STEP 3 | Establezca el peer en el extremo más alejado del túnel (puerta de enlace).

En **Peer IP Address Type (Tipo de dirección IP del peer)**, seleccione una de las siguientes configuraciones e introduzca la información correspondiente para el peer:

- **IP**: introduzca un valor de **Peer Address (Dirección de peer)** como una dirección IPv4 o IPv6, o un objeto de dirección que sea una dirección IPv4 o IPv6.
- **FQDN**: introduzca un valor de **Peer Address (Dirección de peer)** como un FQDN o un objeto de dirección que utilice un FQDN. Si el FQDN o el objeto de dirección de FQDN resuelve más de una dirección IP, el cortafuegos selecciona la dirección preferida del conjunto de direcciones que coinciden con el tipo de dirección (IPv4 o IPv6) de la puerta de enlace IKE de la siguiente manera:
  - Si no se negocia una asociación de seguridad (security association, SA) de IKE, la dirección preferida es la dirección IP con el valor más pequeño.
  - Si la puerta de enlace de IKE utiliza una dirección dentro de un conjunto de direcciones ofrecidas, el cortafuegos selecciona esa dirección (sea o no la dirección más pequeña en el conjunto).
  - Si la puerta de enlace de IKE utiliza una dirección que no está dentro de un conjunto de direcciones ofrecidas, el cortafuegos selecciona una nueva dirección, la dirección más pequeña en el conjunto.
- **Dynamic (Dinámico)**: seleccione **Dynamic (Dinámico)** si la dirección IP o el FQDN del peer es desconocido, de modo que el peer iniciará la negociación.



Utilizar FQDN u objetos de dirección de FQDN reduce los problemas en los entornos donde el peer está sujeto a cambios en la dirección IP dinámica (de lo contrario, requeriría que volviera a configurar esta dirección de peer de puerta de enlace de IKE).

STEP 4 | Especifique cómo autenticar el peer.

Seleccione el método de **Authentication**. **Pre-Shared Key** o **Certificate**. Si selecciona una clave precompartida, vaya al siguiente paso. Si elige un certificado, vaya a el paso 6 para configurar la autenticación basada en certificados.

STEP 5 | Configure una clave precompartida.

1. Introduzca una **Pre-shared Key (Clave precompartida)**, que es la clave de seguridad que se utilizará para autenticación a través del túnel. Introduzca de nuevo el valor en **Confirm Pre-shared Key (Confirmar clave precompartida)**. Utilice un máximo de 255 caracteres ASCII o no ASCII.



Genere una clave que sea difícil de averiguar con ataques por diccionario; use un generador de claves previamente compartidas en caso necesario.

2. En **Local Identification**, seleccione uno de los siguientes tipos e introduzca el valor que considere oportuno: **FQDN (Nombre de host)**, **dirección IP**, **KEYID (cadena de ID de formato binario en HEX)**

© 2020 Palo Alto Networks, Inc.

y **FQDN de usuario (dirección de correo electrónico)**. La identificación local define el formato y la identificación del gateway local. Si no especifica ningún valor, la dirección IP local se utilizará como el valor de identificación local.

3. En **Peer Identification (Identificación de peer)**, seleccione uno de los siguientes tipos e introduzca el valor que considere oportuno: **FQDN (Nombre de host)**, **dirección IP**, **KEYID (cadena de ID de formato binario en HEX)** y **FQDN de usuario (dirección de correo electrónico)**. La identificación del peer define el formato y la identificación del gateway local. Si no especifica ningún valor, la dirección IP de peer se utilizará como el valor de identificación de peer.
4. Vaya al paso 7 para configurar las opciones avanzadas de la puerta de enlace.

STEP 6 | Configuración de la autenticación basada en certificados.

Realice los pasos restantes de este procedimiento si ha seleccionado **Certificate (Certificado)** como el método de autenticación de la puerta de enlace del peer en el otro extremo del túnel.

1. Seleccione en **Local Certificate (Certificado local)** un certificado que ya se encuentre en el cortafuegos, haga clic en **Import (Importar)** para importar un certificado o bien haga clic en en **Generate (Generar)** para crearlo.
   - Para implementar la función **Import (Importar)** de un certificado, realice la Importación de un certificado para la autenticación de la puerta de enlace IKEv2 y regrese a esta tarea.
   - Si desea implementar la función **Generate (Generar)** para generar un nuevo certificado, Genere un certificado en el cortafuegos y regrese a esta tarea.
2. (Opcional) Marque **HTTP Certificate Exchange (Intercambio de certificados HTTP)** para configurar el hash y la URL (solo en IKE v. 2). Para un intercambio de certificados HTTP, introduzca la **Certificate URL (URL de certificado)**. Para obtener más información, consulte Intercambio de certificado de hash y URL.
3. Seleccione el tipo de **Local Identification (Identificación local)**: **Distinguished Name (Subject), FQDN (hostname) (Nombre distintivo [asunto], FQDN [nombre de host])**, **IP address (Dirección IP)** o **User FQDN (email address) (FQDN de usuario [dirección de correo electrónico])** e introduzca el valor. La identificación local define el formato y la identificación del gateway local.
4. Seleccione el tipo de **Peer Identification (Identificación de peer)**: **Distinguished Name (Subject), FQDN (hostname) (Nombre distintivo [asunto], FQDN [nombre de host])**, **IP address (Dirección IP)** o **User FQDN (email address) (FQDN de usuario [dirección de correo electrónico])** e introduzca el valor. La identificación del peer define el formato y la identificación del gateway local.
5. Seleccione el tipo de **Peer ID Check (Comprobación de ID de peer)**:
   - **Exact (Exacta)**: garantiza que el ajuste local y la carga de trabajo de la ID IKE del peer coincidan a la perfección.
   - **Wildcard (Carácter comodín)**: permite que la identificación de peer coincida siempre que coincidan todos caracteres antes del comodín (*). No es necesario que coincidan los caracteres tras el asterisco.
6. (Opcional) Seleccione **Permit peer identification and certificate payload identification mismatch (Permitir identificación de peer y falta de coincidencia de identificación de carga de certificado)** para permitir una SA IKE correcta incluso aunque la identificación del peer no coincida con la identificación del peer en el certificado.
7. En **Certificate Profile (Perfil de certificados)** seleccione un perfil. Un perfil del certificado contiene información sobre el modo de autenticar la puerta de enlace del peer.
8. (Opcional) Seleccione **Enable strict validation of peer's extended key use (Habilitar validación estricta de uso de clave extendida de peer)** para controlar estrictamente cómo se puede utilizar la clave.

STEP 7 | Configure las opciones avanzadas para la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

1. (Opcional) Seleccione **Enable Passive Mode** en las sección Common Options (Opciones comunes) (**Advanced Options (Opciones avanzadas)**) para especificar que el cortafuegos solo responda a las solicitudes de conexión IKE y que nunca las inicie.
2. Si tiene un dispositivo que realice NAT entre puertas de enlace, seleccione **Enable NAT Traversal (Habilitar NAT transversal)** para utilizar la encapsulación UDP en los protocolos IKE y UDP, y permitirles pasar a través de dispositivos de NAT intermedios.
3. Si ha configurado **IKEv1 only mode (Modo exclusivo IKE v. 1)** en el paso 1, en la pestaña IKEv1 (IKE v. 1):
   - Seleccione el **Exchange Mode (Modo de intercambio)**: **auto (automático)**, **aggressive (agresivo)** o **main (principal)**. Si el cortafuegos está configurado para utilizar el modo de intercambio **auto (automático)**, acepta solicitudes de negociación tanto del modo **main (principal)** como del modo **aggressive (agresivo)**; sin embargo, siempre que sea posible, inicia los intercambios en el modo **main (principal)**.

     Si el modo de intercambio no se ha definido como auto (automático), debe configurar ambos peers con el mismo modo de intercambio para permitir que cada peer acepte las solicitudes de negociación.
   - Seleccione un perfil existente o mantenga el perfil predeterminado en la lista **IKE Crypto Profile (Perfil criptográfico de IKE)**. De ser necesario, realice la Definición de perfiles criptográficos IKE.
   - (Únicamente cuando utiliza autenticación basada en certificados y el modo de intercambio no está definido como aggressive) Haga clic en **Enable Fragmentation (Habilitar fragmentación)** para habilitar que el cortafuegos opere con fragmentación IKE.
   - Haga clic en **Dead Peer Detection (Detección de fallo del peer)** e introduzca un **Interval (Intervalo)** (el intervalo es de 2 a 100 segundos). En **Retry (Reintento)**, defina el tiempo de espera (el intervalo es de 2 a 100 segundos) antes de intentar volver a comprobar la disponibilidad. La detección de fallo del peer identifica peers IKE inactivos o no disponibles enviando una carga de notificación IKE de fase 1 al peer y esperando a que la reconozca.
4. Si ha configurado **IKEv2 only mode (Modo exclusivo IKE v. 2)** o **IKEv2 preferred mode (Modo preferido IKE v. 2)** en el paso 1, en la pestaña IKEv2 (IKE v. 2):
   - Seleccione un perfil en **IKE Crypto Profile (Perfil criptográfico de IKE)**, que configura las opciones de la primera fase de IKE, como el grupo DH, el algoritmo de hash y la autenticación con ESP. Para obtener información sobre los perfiles criptográficos IKE, consulte IKE de fase 1.
   - (Opcional) Habilite la **Strict Cookie Validation (Validación de cookies estricta)**. ConsulteUmbral de activación de cookies y validación de cookies estricta.
   - (Opcional) Seleccione **Enable Liveness Check (Habilitar comprobación de actividad)** e introduzca un **Interval (sec) (Intervalo [s])** (el valor predeterminado es 5) si desea que la puerta de enlace envíe una solicitud de mensaje a su peer de puerta de enlace, en el que solicite una respuesta. En caso necesario, el iniciador intenta la comprobación de actividad hasta diez veces. Si no recibe respuesta, el Iniciador cierra y elimina la IKE_SA y las CHILD_SA. El Iniciador empezará de nuevo enviando otro mensaje IKE_SA_INIT.

STEP 8 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

Exportación de un certificado para un peer para acceder usando Hash y URL

IKEv2 admite Intercambio de certificados Hash y URL como método para que el peer y el extremo remoto del túnel recuperen el certificado de un servidor donde ha exportado el certificado. Realice esta tarea para exportar su certificado a ese servidor. Ya debe haber creado un certificado utilizando **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)**.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Seleccione **Device (Dispositivo)** > **Certificates (Certificados)** y, si su plataforma admite varios sistemas virtuales, en **Location (Ubicación)**, seleccione el sistema virtual adecuado.

STEP 2 | En la pestaña **Device Certificates**, seleccione el certificado para exportar al servidor mediante la opción **Export**.

El estado del certificado debe ser válido, no caducado. El cortafuegos no le impedirá exportar un certificado no válido.

STEP 3 | Para **File Format**, seleccione **Binary Encoded Certificate (DER)**.

STEP 4 | Deje **Export private key** sin marcar. No es necesario exportar la clave privada para Hash y URL

STEP 5 | Haga clic en **OK (Aceptar)**.

Importación de un certificado para Autenticación de puerta de enlace IKEv2

Realice esta tarea si está autenticando un peer para una puerta de enlace IKEv2 y no ha usado un certificado local existente en el cortafuegos, sino que quiere importar un certificado desde otra ubicación.

Para realizar esta tarea, se da por hecho que ha seleccionado **Network (Red)** > **IKE Gateways (Puertas de enlace de IKE)**, ha añadido una puerta de enlace y, en **Local Certificate (Certificado local)**, hizo clic en **Import (Importar)**.

STEP 1 | Importe un certificado.

1. Seleccione **Network (Red)** > **IKE Gateways (Puertas de enlace de IKE)**, haga clic en **Add (Añadir)** para añadir una puerta de enlace y en la pestaña **General**, en **Authentication (Autenticación)**, seleccione **Certificate (Certificado)**. En **Local Certificate (Certificado local)**, haga clic en **Import (Importar)**.
2. En la ventana Import Certificate, introduzca un nombre en **Certificate Name** para el certificado que está importando.
3. Seleccione **Shared (Compartido)** si este certificado debe compartirse entre múltiples sistemas virtuales.
4. En **Certificate File (Archivo de certificado)**, utilice **Browse (Examinar)** para buscar el archivo del certificado. Haga clic en el nombre archivo y seleccione **Open**, lo que cumplimenta el campo **Certificate File**.
5. En **File Format**, seleccione una de las opciones siguientes:
   - **Base64 Encoded Certificate (PEM)**: contiene el certificado, pero no la clave. Es texto no cifrado.
   - **Encrypted Private Key and Certificate (PKCS12)**: contiene tanto el certificado como la clave.
6. Seleccione **Import private key** si la clave está en un archivo distinto del archivo de certificados. La clave es opcional, con la siguiente excepción:
   - Debe importar una clave si establece el **File Format** en **PEM**. Introduzca un **Key file** al hacer clic en **Browse** y buscar el archivo de clave que desea importar.
   - Introduzca una **Passphrase** y seleccione **Confirm Passphrase**.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Continúe con la siguiente tarea.

Paso Configuración de la autenticación basada en certificados.

© 2020 Palo Alto Networks, Inc.

Cambio de la duración de la clave o del intervalo de autenticación IKEv2

Esta tarea es opcional; el valor predeterminado de la duración de la asignación de claves de SA IKE IKEv2 es de 8 horas. El valor predeterminado de Autenticación múltiple IKEv2 es 0, lo que significa que la función de reautenticación está deshabilitada. Para obtener más información, consulte la Duración de la clave de SA e intervalo de reautenticación.

Para cambiar los valores predeterminados, realice la siguiente tarea. Un requisito previo es que ya exista un perfil de cifrado IKE.

STEP 1 | Cambie la duración de la clave de SA o el intervalo de autenticación para un perfil criptográfico IKE

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico IKE)** y seleccione el perfil Criptográfico IKE que se aplica a la puerta de enlace local.
2. Para la **Key Lifetime (Duración de la clave)**, seleccione una unidad (**Seconds [Segundos]**, **Minutes [Minutos]**, **Hours [Horas]** o **Days [Días]**) e introduzca un valor. El mínimo es de tres minutos.
3. Para **IKE Authentication Multiple (Múltiplo de autenticación IKE)**, introduzca un valor, que se multiplica por la duración para determinar el intervalo de reautenticación.

STEP 2 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Cambio del umbral de activación de cookies para IKEv2

Realice la siguiente tarea si quiere que el cortafuegos tenga un umbral diferente del ajuste predeterminado de 500 sesiones de SA a medio abrir antes de que requiera la validación de cookies. Para obtener más información sobre la validación de cookies, consulte el Umbral de activación de cookies y validación de cookies estricta.

STEP 1 | Cambie el umbral de activación de cookies.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y edite la configuración de sesión de VPN. En **Cookie Activation Threshold (Umbral de activación de cookies)**, introduzca el número máximo de SA a medio abrir permitidas antes de que el respondedor solicite una cookie del iniciador (intervalo: 0-65.535; predeterminado: 500).
2. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de selectores de tráfico IKEv2

En IKE v. 2, puede configurar los Selectores de tráfico, que son componentes del tráfico de red que se utilizan durante la negociación de IKE. Los selectores de tráfico se usan durante la CHILD_SA (creación de túnel) de fase 2 para configurar el túnel y determinar qué tráfico está permitido a través del túnel. Los dos peers de puerta de enlace IKE deben negociar y acordar sus selectores de tráfico; de lo contrario, una parte estrecha su intervalo de direcciones para acuerdo. Una conexión IKE puede tener múltiples túneles; por ejemplo, puede asignar diferentes túneles a cada departamento para aislar su tráfico. La separación de tráfico también permite implementar funciones como QoS. Utilice el siguiente flujo de trabajo para configurar los selectores de tráfico.

STEP 1 | Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** > **Proxy IDs (ID de proxy)**.

STEP 2 | Seleccione la pestaña **IPv4** o **IPv6**.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Haga clic en **Add** e introduzca el **nombre** en el campo **Proxy ID**.

STEP 4 | En el campo **Local**, introduzca la **Source IP Address (Dirección IP de origen)**.

STEP 5 | En el campo **Remote**, introduzca **Destination IP Address**.

STEP 6 | En el campo **Protocol (Protocolo)**, seleccione el protocolo de transporte (**TCP** o **UDP**).

STEP 7 | Haga clic en **OK (Aceptar)**.

Definición de perfiles criptográficos

Un perfil criptográfico especifica los cifrados usados para autenticación o cifrado entre dos peers IKE y la duración de esta clave. El periodo entre cada renegociación se conoce como duración; cuando el tiempo especificado vence, el cortafuegos vuelve a negociar un nuevo conjunto de claves.

Para proteger las comunicaciones a través del túnel VPN, el cortafuegos requiere perfiles criptográficos IKE e IPSec para completar las negociaciones IKE de fase 1 y de fase 2, respectivamente. El cortafuegos incluye un perfil criptográfico predeterminado IKE y un perfil criptográfico predeterminado IPSec que están listos para utilizarse.

- Definición de perfiles criptográficos IKE
- Definición de perfiles criptográficos IPSec

Definición de perfiles criptográficos IKE

El perfil criptográfico IKE se utiliza para configurar algoritmos de cifrado y autenticación que sirven para el proceso de intercambio de claves en IKE de fase 1, y una duración de las claves, que especifica el tiempo que serán válidas. Para invocar el perfil, debe vincularlo a la configuración de gateway IKE.



Todas las puertas de enlace IKE configuradas en la misma interfaz o dirección IP local deben usar el mismo perfil criptográfico cuando el tipo de dirección IP de pares de la puerta de enlace IKE esté configurado como Dynamic (Dinámico) y esté aplicado el modo principal IKEv1 o IKEv2.

STEP 1 | Creación de un nuevo perfil IKE.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico de IKE)** y seleccione **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para el perfil nuevo.

STEP 2 | Especifique el Grupo DH (Diffie–Hellman) para el intercambio de claves y los algoritmos de autenticación y cifrado.

Haga clic en **Add (Añadir)** en las secciones correspondientes —DH Group (Grupo DH), Authentication (Autenticación) y Encryption (Cifrado)— y seleccione las opciones oportunas en los menús.

Si no sabe con certeza con qué son compatibles los peers VPN, añada múltiples grupos o algoritmos en orden de mayor a menor seguridad del siguiente modo; los peers negocian el grupo o algoritmo admitido más fuerte para establecer el túnel.

- DH Group (Grupo DH)
  - **group20**
  - **group19**
  - **group14**
  - **group5**

© 2020 Palo Alto Networks, Inc.

- **group2**
- **group1**

- Authentication (Autenticación)
  - **sha512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - (PAN-OS 10.0.3 y versiones 10.0 posteriores) **none**



Si selecciona un algoritmo AES-GCM para el cifrado, debe seleccionar la configuración de autenticación none (ninguna). Si no lo hace, la confirmación fallará. El hash se selecciona automáticamente en función del grupo DH seleccionado. El grupo DH 19 y las versiones inferiores usan sha256; el grupo DH 20 usa sha384.

- Encryption (Cifrado)
  - (PAN-OS 10.0.3 y versiones posteriores a 10.0) **aes-256-gcm** (requiere IKEv2; el grupo DH debe establecerse en **group20 [grupo20]**)
  - (PAN-OS 10.0.3 y versiones posteriores a 10.0) **aes-128-gcm** (requiere IKEv2 y que el grupo DH esté establecido en **group19 [grupo19]**)
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**
  - **des**



Elija los algoritmos más resistentes de autenticación y cifrado que pueda admitir el peer. En el algoritmo de autenticación, utilice SHA-256 o superior (se recomienda SHA-384 o superior para las transacciones de larga duración). No utilice SHA1 ni MD5. Para el algoritmo de cifrado, utilice AES; DES y 3DES son débiles y vulnerables. AES with Galois/Counter Mode (AES-GCM, AES con modo Galois/Counter) proporciona la seguridad más sólida y dispone de autenticación incorporada, por lo que debe establecer la autenticación en none (ninguno) si selecciona los cifrados aes-256-gcm o aes-128-gcm.

STEP 3 | Especifique la duración de la validez de la clave y el intervalo de reautenticación.

Para obtener información detallada, consulte la Duración de la clave de SA e intervalo de reautenticación.

1. En los campos **Key Lifetime (Duración de la clave)**, especifique el periodo (en segundos, minutos, horas o días) durante el cual es válida la clave (rango: 3 minutos a 365 días; valor predeterminado: 8 horas). Cuando vence la clave, el cortafuegos renegocia una nueva clave. La duración es el periodo entre cada renegociación.
2. En **IKEv2 Authentication Multiple (Autenticación IKEv2 múltiple)**, especifique un valor (rango: 0 a 50; valor predeterminado: 0) que se multiplica por la **Key Lifetime (Duración de la clave)** para determinar el conteo de autenticación. El valor predeterminado 0 deshabilita la función de reautenticación.

STEP 4 | Confirme su perfil criptográfico IKE.

Haga clic en **ACEPTAR** y en **Confirmar**.

STEP 5 | Adjunte el perfil criptográfico IKE y la configuración del gateway IKE.

© 2020 Palo Alto Networks, Inc.

Consulte Configuración de opciones avanzadas para la puerta de enlace.

Definición de perfiles criptográficos IPSec

El perfil criptográfico IPSec se invoca en IKE de fase 2. Especifica el modo en que se protegen los datos dentro del túnel cuando se usa IKE de clave automática para generar claves automáticamente para las SA del IKE.

STEP 1 | Cree un nuevo perfil IPSec.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico IPSec)** y seleccione **Add (Añadir)**.
2. Introduzca un nombre en **Name (Nombre)** para el perfil nuevo.
3. Seleccione el **IPSec Protocol (Protocolo de IPSec)** (ESP o AH) que quiere aplicar para proteger los datos cuando atraviesan el túnel.

   Se recomienda seleccionar la carga útil de seguridad encapsulada (encapsulating security payload, ESP) en lugar del encabezado de autenticación (authentication header, AH) porque ESP ofrece confidencialidad y autenticación en la conexión, pero AH solo ofrece autenticación.
4. Haga clic en **Añadir** y seleccione la **autenticación** y los algoritmos de **cifrado** para ESP, así como los algoritmos de **autenticación** para AH, de modo que los peers de IKE puedan negociar las claves para proteger la transferencia de datos a través del túnel.

   Si no sabe con certeza con qué son compatibles los peers IKE, añada múltiples algoritmos en orden de mayor a menor seguridad del siguiente modo; los peers negocian el algoritmo admitido más fuerte para establecer el túnel:

   - Cifrado: **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (el cortafuegos de la serie VM no admite esta opción), **aes-128-cbc**, **3des**, **des**.

     Se recomienda seleccionar los algoritmos más resistentes de autenticación y cifrado que pueda admitir el peer. En el algoritmo de autenticación, utilice SHA-256 o superior (se recomienda SHA-384 o superior para las transacciones de larga duración). No use SHA-1, MD5 o ninguno. Para el algoritmo de cifrado, utilice AES; DES y 3DES son débiles y vulnerables.
   - Autenticación: **sha512**, **sha384**, **sha256**, **sha1**, **md5**.

STEP 2 | Seleccione el Grupo DH para usar las negociaciones de SA IPSec en el IKE de fase 2.

En **DH Group (Grupo DH)**, seleccione la solidez de las claves que desea usar: **group1**, **group2**, **group5**, **group14**, **group19** o **group20**. Para mayor seguridad, seleccione el grupo con el número más alto.

Si no desea renovar la clave que crea el cortafuegos durante la fase 1 de IKE, seleccione **no-pfs** (sin secreto perfecto y permanente); de ese modo, el cortafuegos reutiliza la clave actual para las negociaciones de asociaciones de seguridad (security association, SA) de IPSec.

STEP 3 | Especifique la duración de la clave (tiempo y volumen del tráfico).

Usar una combinación de tiempo y volumen del tráfico le permite garantizar la seguridad de los datos.

Seleccione la **Lifetime** o el período durante el cual es válida la clave en segundos, minutos, horas o días (intervalo: 3 minutos a 365 días). Cuando vence el tiempo especificado, el cortafuegos vuelve a negociar un nuevo conjunto de claves.

Seleccione la **duración** o el volumen de datos que establecerán cuándo han de volver a negociarse las claves.

© 2020 Palo Alto Networks, Inc.

STEP 4 | Confirme su perfil IPSec.

Haga clic en **ACEPTAR** y en **Confirmar**.

STEP 5 | Adjunte el perfil IPSec a una configuración de túnel IPSec.

Consulte Configuración de intercambio de claves.

Configuración de un túnel de IPSec

La configuración de los túneles de IPSec permite autenticar o cifrar los datos (paquetes de IP) cuando los atraviesan.

Si desea configurar el cortafuegos con un peer compatible con una VPN basada en políticas, debe definir los ID del proxy. Los dispositivos compatibles con VPN basadas en políticas usan reglas/políticas o listas de acceso de seguridad específicas (direcciones de origen, direcciones de destino y puertos) para permitir el tráfico interesante a través de un túnel IPSec. Se hace referencia a estas reglas durante la negociación IKE de fase 2/modo rápido y se intercambian como ID de proxy en el primer o segundo mensaje del proceso. Por lo tanto, si configura el cortafuegos para que funcione con un peer de una VPN basada en políticas, para que la negociación de fase 2 sea correcta, debe definir el ID del proxy, de modo que ambos peers tengan la misma configuración. Si no está configurado el ID del proxy porque el cortafuegos admite VPN basadas en rutas, se utiliza como tal los valores predeterminados siguientes: IP de origen: 0.0.0.0/0, ip de destino: 0.0.0.0/0 y aplicación: cualquiera; y cuando estos valores se intercambian con el peer, se produce un fallo al configurar la conexión VPN.

STEP 1 | Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** y luego **Add (Añadir)** para añadir una configuración de túnel.

STEP 2 | En la pestaña **General**, introduzca en **Name (Nombre)** un nombre para el túnel.

STEP 3 | Seleccione en **Tunnel Interface (Interfaz de túnel)** la interfaz que se debe usar para configurar el túnel de IPSec.

Para crear una nueva interfaz de túnel:

1. Seleccione **Tunnel Interface (Interfaz de túnel)** > **New Tunnel Interface (Nueva interfaz de túnel)**. (También puede seleccionar **Network [Red]** > **Interfaces** > **Tunnel [Túnel]** y hacer clic en **Add [Añadir]**.)
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.2**.
3. En la pestaña **Config (Configuración)**, seleccione la lista **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:

Use la zona de confianza como punto de finalización del túnel: seleccione la zona. Asociar la interfaz del túnel con la misma zona (y enrutador virtual) que la interfaz externa por la que entran los paquetes al cortafuegos reduce la necesidad de crear enrutamiento entre zonas.

O bien:

Cree una zona independiente para la finalización del túnel de VPN (recomendado): seleccione **New Zone (Nueva zona)**, defina un nombre para la zona en **Name (Nombre)** (por ejemplo, vpn-corp) y haga clic en **OK (Aceptar)**.

1. En **Virtual Router (Enrutador virtual)**, seleccione **default (predeterminado)**.
2. (Opcional) Si desea asignar una dirección IPv4 a la interfaz del túnel, seleccione la pestaña **Ipv4** y haga clic en **Add (Añadir)** para añadir la dirección IP y la máscara de red, por ejemplo: 10.31.32.1/32.
3. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 4 | (Opcional) Habilite IPv6 en la interfaz de túnel.

1. Seleccione la pestaña IPv6 en **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** > **IPv6**.
2. Seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.

   Esta opción permite enrutar el tráfico IPv6 en un túnel IPv4 IPSec y ofrece confidencialidad entre redes IPv6. El tráfico IPv6 se encapsula mediante IPv4 y, a continuación, mediante ESP. Para enrutar el tráfico IPv6 al túnel, use una ruta estática al túnel, OSPF v. 3 o una regla de reenvío basado en políticas (policy-based forwarding, PBF).
3. Introduzca el **ID de interfaz** exclusivo ampliado de 64 bits en formato hexadecimal, por ejemplo, 00:26:08:FF:FE:DE:4E:29. De manera predeterminada, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física.
4. Para asignar una **dirección** IPv6 a la interfaz de túnel, haga clic en **Add (Añadir)**e ingrese la dirección IPv6 y la longitud del prefijo, por ejemplo 2001:400:f00::1/64. Si no se selecciona Prefijo, la dirección IPv6 asignada a la interfaz será la que especifique completamente en el cuadro de texto de la dirección.
   1. Seleccione **Use interface ID as host portion (Usar ID de interfaz como parte de host)** para asignar una dirección IPv6 a la interfaz que utilizará el ID de interfaz como la parte de host de la dirección.
   2. Seleccione **Anycast** para incluir el enrutamiento mediante el nodo más cercano.

STEP 5 | Configure el intercambio de clave.

En la pestaña **General**, configure uno de los siguientes tipos de intercambio de claves:

Configure el intercambio de clave automática.

1. Seleccione la puerta de enlace IKE. Para configurar una puerta de enlace IKE, consulte Configuración de una puerta de enlace IKE.
2. (Opcional) Seleccione el perfil criptográfico IPSec por defecto. Para crear un nuevo perfil de IPSec, consulte Definición de perfiles criptográficos IPSec.

Configure el intercambio de clave manual.

1. Especifique el índice de parámetros de seguridad (security parameter index, SPI) del cortafuegos local en **Local SPI (SPI local)**. SPI es un índice hexadecimal de 32 bits que se añade al encabezado de tunelización IPSec para ayudar a diferenciar los distintos flujos de tráfico IPSec; se usa para crear la SA requerida a fin de establecer un túnel de VPN.
2. Seleccione la **interfaz** que constituirá el extremo del túnel y, de manera opcional, seleccione la dirección IP para la interfaz local que es el extremo del túnel.
3. Seleccione el protocolo que se usará: **AH** o **ESP**.
4. Para AH, seleccione el método adecuado en **Authentication (Autenticación)**, introduzca la clave en **Key (Clave)** y, a continuación, haga clic en **Confirm Key (Confirmar clave)** para aceptarla.
5. Para ESP, seleccione el método adecuado en **Authentication (Autenticación)**, introduzca la clave en **Key (Clave)** y, a continuación, haga clic en **Confirm Key (Confirmar clave)** para aceptarla. A continuación, seleccione el método de **cifrado**, introduzca una **clave** y, a continuación, **confirme la clave**, en caso necesario.
6. Especifique el índice del peer remoto en **Remote SPI (SPI remoto)**.
7. Introduzca la **Remote Address (Dirección remota)**, la dirección IP y el peer remoto.

STEP 6 | Protección contra un ataque de reproducción.

Un ataque de reproducción consiste en interceptar un paquete de forma malintencionada y retransmitirlo.

En la pestaña General, haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** y marque **Enable Replay Protection (Habilitar protección contra reproducción)** para detectar y neutralizar los ataques de reproducción.

© 2020 Palo Alto Networks, Inc.

STEP 7 | (Opcional) Conserve el encabezado Type of Service para la prioridad o el tratamiento de paquetes de IP.

En la sección Show Advanced Options (Mostrar opciones avanzadas), seleccione **Copy TOS Header (Copiar encabezado de TOS)**. De este modo se copia el encabezado de TOS (Tipo de servicio) desde el encabezado IP interno en el encabezado IP externo de los paquetes resumidos con el fin de preservar la información original de TOS.

Si existen varias sesiones dentro del túnel (cada una con un valor TOS diferente), el copiar el encabezado TOS puede hacer que los paquetes IPSec lleguen desordenados.

STEP 8 | (Opcional) Haga clic en **Add GRE Encapsulation (Añadir encapsulación GRE)** para habilitar la encapsulación de enrutamiento genérico (generic routing encapsulation, GRE) por IPSec.

Añada la encapsulación GRE si el terminal remoto exige que se encapsule el tráfico del túnel de GRE antes de que IPSec lo cifre. En algunas implementaciones, por ejemplo, es obligatorio encapsular el tráfico de multidifusión para que IPSec pueda cifrarlo. Aplique la encapsulación cuando el paquete de GRE encapsulado en IPSec tiene las mismas direcciones IP de origen y de destino que el túnel de IPSec de encapsulación.

STEP 9 | Habilite la supervisión de túnel

Deberá asignar una dirección IP a la interfaz de túnel para su supervisión.

Para alertar al administrador de dispositivo de los fallos del túnel y proporcionar una conmutación por error automática a otra interfaz de túnel:

1. Seleccione **Tunnel Monitor (Supervisión de túnel)**.
2. Especifique una **IP de destino** en el otro lado del túnel que el supervisor de túnel utilizará para determinar si el túnel funciona correctamente.
3. En **Profile (Perfil)**, seleccione el perfil que determina la acción que se realiza cuando falla el túnel. Para crear un nuevo perfil, consulte Definición de perfiles supervisión de túnel.

STEP 10 | Cree un ID de proxy para identificar a los peers de VPN.

Este paso solo es obligatorio si el peer de VPN usa una VPN basada en políticas.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles de IPSec)** y haga clic en **Add (Añadir)**.
2. Seleccione la pestaña **ID de proxy**.
3. Seleccione la pestaña **IPv4** o **IPv6**.
4. Haga clic en **Add** e introduzca el nombre de **Proxy ID**.
5. Introduzca la dirección IP **Local** o subred para la puerta de enlace VPN.
6. Introduzca la dirección **Remote (Remota)** para la puerta de enlace VPN.
7. Seleccione el valor oportuno en **Protocol (Protocolo)**:
   - **Number**: especifique el número de protocolo (utilizado para la interoperabilidad con dispositivos de terceros).
   - **Any (Cualquiera)**: permita el tráfico de TCP o UDP.
   - **TCP**: especifique los números de puertos locales y remotos.
   - **UDP**: especifique los números de puertos locales y remotos.
8. Haga clic en **OK (Aceptar)**.

STEP 11 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de la supervisión de túnel

Para ofrecer un servicio VPN ininterrumpido, puede usar la capacidad Detección de fallo del peer junto con la capacidad de supervisión del túnel en el cortafuegos. También puede supervisar el estado del túnel. Estas tareas de supervisión se describen en las siguientes secciones:

- Definición de un perfil de supervisión de túnel
- Visualización del estado de los túneles

Definición de un perfil de supervisión de túnel

Un perfil de supervisión de túnel le permite verificar la conectividad entre los peers VPN; puede configurar la interfaz de túnel para hacer ping a una dirección IP de destino con un intervalo determinado y especificar la acción si la comunicación a través del túnel está cortada.

STEP 1 | Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Monitor (Supervisar)**. Hay un perfil de supervisión de túnel disponible para su uso.

STEP 2 | Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** para el perfil.

STEP 3 | Seleccione la **Action (Acción)** que se realizará si no es posible alcanzar la dirección IP de destino.

- **Esperar recuperación**: El cortafuegos espera a que el túnel se recupere. Continúa usando la interfaz del túnel para las decisiones de enrutamiento como si el túnel siguiera activo.
- **Conmutación por error**: Desvía el tráfico a una ruta alternativa si hay alguna disponible. El cortafuegos deshabilita la interfaz del túnel y, por lo tanto, deshabilita cualquier ruta en la tabla de rutas que use la interfaz.

En ambos casos, el cortafuegos intenta acelerar la recuperación negociando nuevas claves IPSec.

STEP 4 | Especifique el **Interval (sec) (Intervalo [s])** y el **Threshold (Umbral)** para iniciar la acción especificada.

- El **Threshold (Umbral)** especifica el número de latidos que se perderán antes de que el cortafuegos realice la acción especificada (rango: 2 a 100; valor predeterminado: 5).
- **Interval (sec) (Intervalo [s])** especifica el tiempo (en segundos) entre latidos (rango: 2 a 10; valor predeterminado: 3).

STEP 5 | Adjunte el perfil de supervisión a una configuración de túnel IPSec. Consulte Habilitación de la supervisión de túnel.

Visualización del estado de los túneles

El estado del túnel informa si se han establecido las SA IKE de fase 1 y de fase 2 válidas, y de si está operativa la interfaz del túnel para el paso de tráfico.

Dado que la interfaz del túnel es una interfaz lógica, no puede indicar el estado del enlace físico. Por lo tanto, debe habilitar la supervisión de túnel para que la interfaz del túnel pueda verificar la conectividad a una dirección IP y determinar si la ruta sigue siendo utilizable. Si no se puede alcanzar la dirección IP, el cortafuegos esperará a la recuperación del túnel o una conmutación por error. Cuando se produce una conmutación por error, se anula el túnel existente y se inician cambios de enrutamiento para establecer un nuevo túnel y redirigir el tráfico.

STEP 1 | Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Visualización del **Tunnel Status (Estado de túnel)**

- El color verde indica que el túnel de la SA IPSec es válido.
- El color rojo indica que la SA IPSec no está disponible o ha vencido.

STEP 3 | Vea el **IKE Gateway Status (Estado de la puerta de enlace de IKE)**.

- El color verde indica que la SA IKE de fase 1 es válida.
- El color rojo indica que la SA IKE de fase 1 no está disponible o ha vencido.

STEP 4 | Vea el **Tunnel Interface Status (Estado de la interfaz del túnel)**

- El color verde indica que la interfaz del túnel está activa.
- El color rojo indica que la interfaz de túnel no está activa porque la supervisión del túnel está habilitada y el estado es desactivado.

Para solucionar problemas de un túnel VPN que aún no esté activo, consulte Interpretación de mensajes de error de VPN.

Habilitación/deshabilitación, actualización o reinicio de un gateway IKE o túnel IPSec

Puede habilitar, deshabilitar, actualizar o reiniciar un gateway IKE o túnel de VPN para facilitar la solución de problemas.

- Habilitación o deshabilitación de una puerta de enlace de IKE o un túnel IPSec
- Comportamientos de actualización o reinicio
- Actualización o reinicio de una puerta de enlace IKE o túnel IPSec

Habilitación o deshabilitación de una puerta de enlace de IKE o un túnel IPSec

Habilite o deshabilite una puerta de enlace de IKE o túnel IPSec para facilitar la resolución de problemas.

- Habilite o deshabilite una puerta de enlace IKE.
  1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateways (Puertas de enlace de IKE)** y seleccione la puerta de enlace que desea habilitar o deshabilitar.
  2. En la parte inferior de la pantalla, haga clic en **Enable** o **Disable**.

- Habilite o deshabilite un túnel IPSec.
  1. Seleccione **Network (Red)** > **IPSec Tunnels (Tuneles IPSec)** y seleccione el túnel que desea habilitar o deshabilitar.
  2. En la parte inferior de la pantalla, haga clic en **Enable** o **Disable**.

Comportamientos de actualización o reinicio

Puede realizar la Actualización o reinicio de una puerta de enlace IKE o túnel IPSec. Los comportamientos de actualizar y reiniciar para un gateway IKE y túnel IPSec son los siguientes:

Fase	Actualizar	Reiniciar
Puerta de enlace IKE	Actualiza las estadísticas en pantalla para la puerta de enlace IKE seleccionada.	Reinicia la puerta de enlace IKE seleccionada.

© 2020 Palo Alto Networks, Inc.

Fase	Actualizar	Reiniciar
(IKE de fase 1)	Equivale a emitir un segundo comando `show` en el CLI (tras un comando `show` inicial).	**IKEv2**: También reinicia cualquier asociación de seguridad (SA) IPSec secundaria. **IKEv1**: No reinicia las SA IPSec asociadas. Un reinicio interrumpe todas las sesiones existentes. Equivale a emitir una secuencia de comandos **`clear`**, **`test`**, **`show`** en la CLI.
Túnel IPSec (IKE de fase 2)	Actualiza las estadísticas en pantalla para el túnel IPSec seleccionado. Equivale a emitir un segundo comando `show` en el CLI (tras un comando `show` inicial).	Reinicia el túnel IPSec. Un reinicio interrumpe todas las sesiones existentes. Equivale a emitir una secuencia de comandos **`clear`**, **`test`**, **`show`** en la CLI.

Actualización o reinicio de una puerta de enlace IKE o túnel IPSec

Tenga en cuenta que el resultado de reiniciar una puerta de enlace IKE depende de si se trata de IKEv1 o IKEv2. Consulte Comportamientos de actualización o reinicio para una puerta de enlace de IKE (IKEv1 e IKEv2) y para un túnel IPSec.

- Actualice o reinicie una puerta de enlace IKE.
  1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** y seleccione el túnel para la puerta de enlace que desea actualizar o reiniciar.
  2. En la fila correspondiente a ese túnel, en la columna Status, haga clic en **IKE Info**.
  3. En la parte inferior de la pantalla Info IKE, haga clic en la acción que desea:
     - **Refresh**: actualiza las estadísticas en pantalla.
     - **Restart (Reiniciar)**: borra las SA, de modo que el tráfico se descarta hasta que se inicie la negociación IKE de nuevo y se vuelva a crear el túnel.

- Actualice o reinicie un túnel IPSec.

  Puede determinar que es necesario actualizar o reiniciar el túnel porque usa la supervisión de túneles para supervisar el estado del túnel, o usa un supervisor de red externo para supervisar la conectividad de red a través del túnel IPSec.

  1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** y seleccione el túnel que desea actualizar o reiniciar.
  2. En la fila de ese túnel, en la columna Status, haga clic en **Tunnel Info**.
  3. En la parte inferior de la pantalla Información de túnel, haga clic en la acción que desea:
     - **Refresh (Actualizar)**: actualiza las estadísticas en pantalla.
     - **Restart (Reiniciar)**: borra las SA, de modo que el tráfico se descarta hasta que se inicie la negociación IKE de nuevo y se vuelva a crear el túnel.

Prueba de conectividad VPN

Realice esta tarea para probar la conectividad VPN.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Inicie el IKE de fase 1 haciendo un ping a un host a través del túnel o usando el siguiente comando del CLI:

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | Introduzca el siguiente comando para probar si el IKE de fase 1 está configurado:

```
show vpn ike-sa gateway <gateway_name>
```

En el resultado, compruebe si se muestra la asociación de seguridad. De lo contrario, revise los mensajes del log del sistema para interpretar el motivo del fallo.

STEP 3 | Inicie el IKE de fase 2 haciendo un ping a un host a través del túnel o usando el siguiente comando del CLI:

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | Introduzca el siguiente comando para probar si el IKE de fase 2 está configurado:

```
show vpn ipsec-sa tunnel <tunnel_name>
```

En el resultado, compruebe si se muestra la asociación de seguridad. De lo contrario, revise los mensajes del log del sistema para interpretar el motivo del fallo.

STEP 5 | Para ver la información del flujo de tráfico VPN, use el siguiente comando.

```
show vpn flow
total tunnels configured:               1
filter - type IPSec, state any

total IPSec tunnel configured:        1
total IPSec tunnel shown:               1

name                    id      state      local-ip       peer-ip
       tunnel-i/f
--------------------------------------------------------------------------------
vpn-to-siteB       5       active    100.1.1.1     200.1.1.1     tunnel.41
```

Interpretación de mensajes de error de VPN

La siguiente tabla enumera algunos de los mensajes de error de VPN más comunes que se registran en el log del sistema.

Table 6: Mensajes de error de Syslog para problemas de VPN

Si el error es:	Pruebe a:
`La negociación IKE de fase 1 falló como iniciador, modo principal. Falló SA: x.x.x.x(500)-y.y.y.y(500)`	• Verificar si la dirección IP pública de cada peer VPN es precisa en la configuración del gateway IKE.

© 2020 Palo Alto Networks, Inc.

Si el error es:	Pruebe a:

`cookie:84222f276c2fa2e9:0000000000000000 por agotarse el tiempo de espera.`
O
`Falló la negociación IKE de fase 1. No se pudo encontrar la configuración de solicitud IKE de fase 1 para el peer IP x.x.x.x(1929)`
	• Verificar si se puede hacer ping a las direcciones IP y que los problemas de enrutamiento no están provocando el fallo de conexión.

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x(500) to y.y.y.y(500), ignored...`
O
`Falló la negociación IKE de fase 1. No se puede procesar la SA de payload del peer.`
	Comprobar el perfil criptográfico IKE para verificar que las propuestas en ambos lados tienen un cifrado, autenticación y propuesta de grupo DH comunes.

`pfs group mismatched:my: 2peer: 0`
O
`La negociación IKE de fase 2 falló durante el proceso de la carga SA. No se encontró propuesta adecuada en la carga SA del peer.`
	Comprobar la configuración del perfil criptográfico IPSec para verificar que:
	• los dos peers VPN tienen el mismo valor de pfs: habilitado o deshabilitado
	• los grupos DH propuestos por cada peer tienen al menos un grupo DH en común

`La negociación IKE de fase 2 falló al procesar el ID de proxy. Recibió id local x.x.x.x/x tipo IPv4 dirección de protocolo 0 puerto 0, recibió id remota y.y.y.y/y tipo IPv4 dirección de protocolo 0 puerto 0.`	El peer VPN de un extremo está usando una VPN basada en políticas. Debe configurar un ID de proxy en el cortafuegos de Palo Alto Networks. Consulte Creación de una ID de proxy para identificar a los peers de VPN.

© 2020 Palo Alto Networks, Inc.

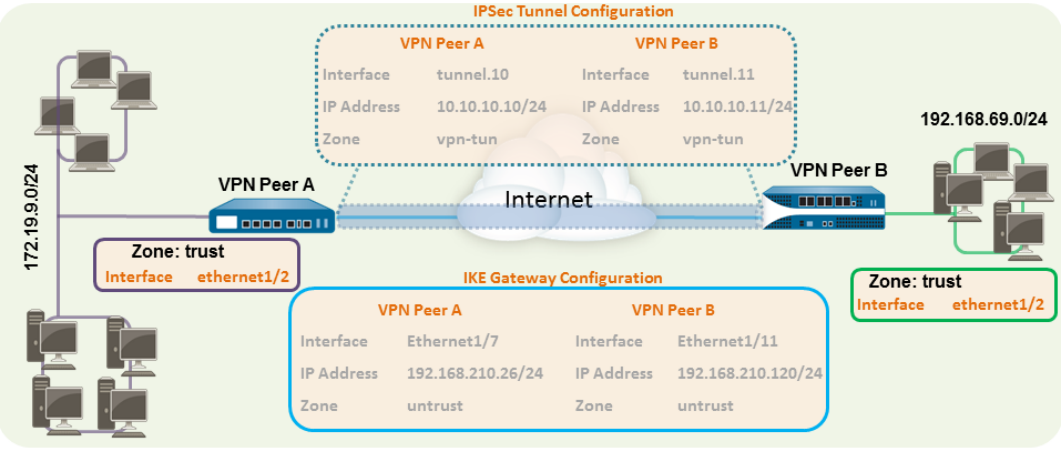
Configuraciones rápidas de VPN de sitio a sitio

En las siguientes secciones se proporcionan instrucciones detalladas para configurar algunas implementaciones globales de VPN:

- VPN de sitio a sitio con rutas estáticas
- VPN de sitio a sitio con OSPF
- VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico

VPN de sitio a sitio con rutas estáticas

Los siguientes ejemplos muestran una conexión VPN entre dos sitios que usan rutas estáticas. Sin enrutamiento dinámico, las interfaces de túnel en el peer A de VPN y el peer B de VPN no necesitan una dirección IP porque el cortafuegos usa automáticamente la interfaz del túnel como el próximo salto para el enrutamiento de tráfico a través de los sitios. Sin embargo, para habilitar la supervisión del túnel, se ha asignado una dirección IP estática a cada interfaz de túnel.



STEP 1 | Configure una interfaz de capa 3.

Esta interfaz se usa para el túnel IKE de fase 1.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
   - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
   - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en **Security Zone (Zona de seguridad)**, defina un nombre para la zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

   En este ejemplo, la configuración para el peer A de VPN es:

© 2020 Palo Alto Networks, Inc.

- **Interface (Interfaz)**: ethernet1/7
- **Security Zone (Zona de seguridad)**: untrust (no fiable)
- **Virtual Router (Enrutador virtual)**: default (predeterminado)
- **IPv4**: 192.168.210.26/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz)**: ethernet1/11
- **Security Zone (Zona de seguridad)**: untrust (no fiable)
- **Virtual Router (Enrutador virtual)**: default (predeterminado)
- **IPv4**: 192.168.210.120/24

STEP 2 | Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.1**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:
   - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
   - (Recomendado) Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Nombre** para una nueva zona, por ejemplo *vpn-tun*, y haga clic en **Aceptar**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. (Opcional) Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz.

   Con rutas estáticas, la interfaz de túnel no necesita una dirección IP. Para el tráfico destinado a una subred/dirección IP específica, la interfaz de túnel se convertirá automáticamente en el próximo salto. Plantéese añadir una dirección IP si quiere habilitar la supervisión de túnel.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: tunnel.10 (túnel.10)
   - **Zona de seguridad**: vpn_tun
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 172.19.9.2/24

   La configuración para el peer B de VPN es:

   - **Interface (Interfaz)**: tunnel.11 (túnel.11)
   - **Zona de seguridad**: vpn_tun
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 192.168.69.2/24

STEP 3 | Configure una ruta estática, en el servidor virtual, a la subred de destino.

1. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y haga clic en el enrutador que ha definido en el paso anterior.
2. Seleccione **Ruta estática**, haga clic en **Añadir** e introduzca una nueva ruta para acceder a la subred que se encuentra en el otro extremo del túnel.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Destino**: 192.168.69.0/24
   - **Interface (Interfaz)**: tunnel.10 (túnel.10)

   La configuración para el peer B de VPN es:

© 2020 Palo Alto Networks, Inc.

- **Destino**: 172.19.9.0/24
- **Interface (Interfaz)**: tunnel.11 (túnel.11)

STEP 4 | Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

STEP 5 | Configure la puerta de enlace IKE.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: ethernet1/7
   - **Dirección IP local**: 192.168.210.26/24
   - **Tipo/Dirección IP del peer**: estática/192.168.210.120
   - **Claves previamente compartidas**: introduzca un valor
   - **Local identification (Identificación local)**: None (Ninguna); significa que la dirección IP local se utilizará como el valor de identificación local.
   - La configuración para el peer B de VPN es:
   - **Interface (Interfaz)**: ethernet1/11
   - **Local IP address (Dirección IP local)**: 192.168.210.120/24
   - **Tipo/Dirección IP del peer**: estática/192.168.210.26
   - **Claves previamente compartidas**: introduzca el mismo valor que el del peer A
   - **Identificación local**: ninguna
3. Seleccione **Opciones de fase 1 avanzadas** y seleccione el perfil criptográfico de IKE que ha creado anteriormente para usar IKE de fase 1.

STEP 6 | Configure el túnel IPSec.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Tunnel Interface (Interfaz del túnel)**: tunnel.10 (túnel.10)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **IPSec Crypto Profile (Perfil criptográfico de IPSec)**: seleccione el perfil criptográfico de IPSec definido en el paso 4.

   La configuración para el peer B de VPN es:

   - **Tunnel Interface (Interfaz de túnel)**: tunnel.11 (túnel.11)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **IPSec Crypto Profile (Perfil criptográfico de IPSec)**: seleccione el perfil criptográfico de IPSec definido en el paso 4.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Seleccione **Show Advanced Options (Mostrar opciones avanzadas)**, seleccione **Tunnel Monitor (Supervisor de túnel)** y especifique una dirección IP de destino para hacer ping y verificar la conectividad. Normalmente, se usa la dirección IP de la interfaz de túnel del peer de VPN.
4. (Opcional) Para definir la acción que se realizará si no es posible establecer conectividad, consulte Definición de un perfil de supervisión de túnel.

STEP 7 | Cree políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

STEP 8 | Confirme cualquier cambio de configuración pendiente.

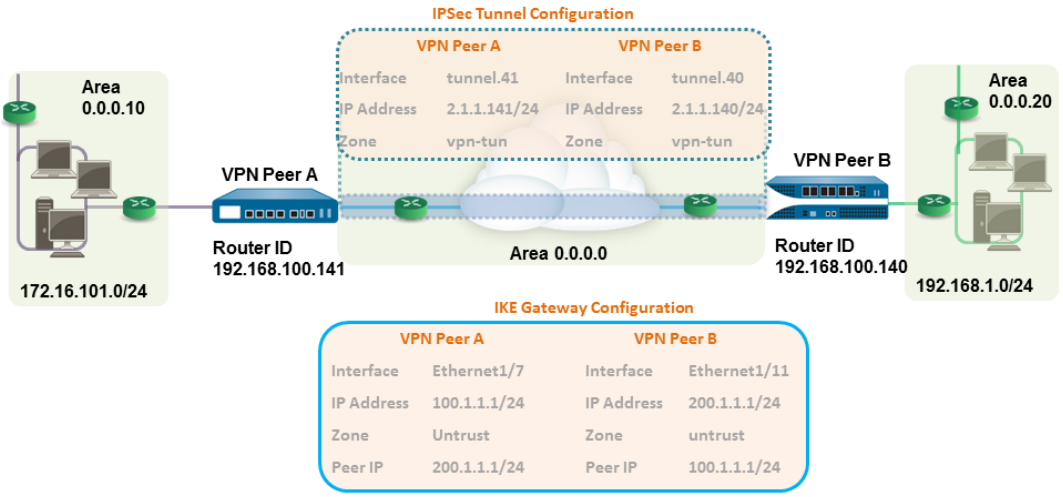
Haga clic en **Commit (Confirmar)**.

STEP 9 | Prueba de conectividad VPN.

Consulte también Visualización del estado de los túneles.

VPN de sitio a sitio con OSPF

En este ejemplo, cada sitio usa OSPF para enrutamiento o tráfico dinámicos. La dirección IP del túnel en cada peer de VPN se asigna estáticamente y sirve como el próximo salto para el enrutamiento de tráfico entre dos sitios.



STEP 1 | Configure las interfaces de capa 3 en cada cortafuegos.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en la lista **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
   - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
   - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en la lista **Security Zone (Zona de seguridad)**, defina un nombre para la zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.

© 2020 Palo Alto Networks, Inc.

5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: ethernet1/7
   - **Security Zone (Zona de seguridad)**: untrust (no fiable)
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 100.1.1.1/24

   La configuración para el peer B de VPN es:

   - **Interface (Interfaz)**: ethernet1/11
   - **Security Zone (Zona de seguridad)**: untrust (no fiable)
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 200.1.1.1/24

STEP 2 | Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.11**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:

   - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
   - (Recomendado) Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Name (Nombre)** para una nueva zona (por ejemplo, vpn-tun), y haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Add** en la sección IP e introduzca la dirección IP y la máscara de red/prefijo para asignarlos a la interfaz; por ejemplo, 172.19.9.2/24.

   Esta dirección IP se usará como dirección IP de próximo salto para enrutar el tráfico al túnel y también puede usarse para supervisar el estado del túnel.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: tunnel.41 (túnel.41)
   - **Zona de seguridad**: vpn_tun
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 2.1.1.141/24

   La configuración para el peer B de VPN es:

   - **Interface (Interfaz)**: tunnel.40 (túnel.10)
   - **Zona de seguridad**: vpn_tun
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 2.1.1.140/24

STEP 3 | Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

STEP 4 | Establezca la configuración OSPF en el enrutador virtual y adjunte las áreas OSPF con las interfaces apropiadas en el cortafuegos.

Para obtener más información sobre las opciones OSPF disponibles en el cortafuegos, consulte Configuración de OSPF.

Use Broadcast como el tipo de enlace cuando haya más de dos enrutadores OSPF que necesiten intercambiar información de enrutamiento.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador predeterminado o añada uno nuevo.
2. Seleccione **OSPF** (para IPv4) u **OSPFv3** (para IPv6) y seleccione **Enable (Habilitar)**.
3. En este ejemplo, la configuración OSPF para el peer A de VPN es:
   - **Router ID (ID de enrutador)**: 192.168.100.141
   - **Area ID (ID de área)**: 0.0.0.0 que se asigna a la interfaz del túnel.1 con el tipo de enlace: p2p
   - **Area ID (ID de área)**: 0.0.0.10 que se asigna a la interfaz Ethernet1/1 con el tipo de enlace: Broadcast

   La configuración OSPF para el peer B de VPN es:
   - **Router ID (ID de enrutador)**: 192.168.100.140
   - **Area ID (ID de área)**: 0.0.0.0 que se asigna a la interfaz del túnel.1 con el tipo de enlace: p2p
   - **Area ID (ID de área)**: 0.0.0.20 que se asigna a la interfaz Ethernet1/15 con el tipo de enlace: Broadcast

STEP 5 | Configure la puerta de enlace IKE.

Estos ejemplos usan direcciones IP estáticas para ambos peers VPN. Normalmente, la sede usa una dirección IP configurada estáticamente y la sucursal puede usar una dirección IP dinámica; las direcciones IP dinámicas no son las más indicadas para configurar servicios estables como VPN.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:
   - **Interface (Interfaz)**: ethernet1/7
   - **Local IP address (Dirección IP local)**: 100.1.1.1/24
   - **Dirección IP del peer**: 200.1.1.1/24
   - **Claves previamente compartidas**: introduzca un valor

   La configuración para el peer B de VPN es:
   - **Interface (Interfaz)**: ethernet1/11
   - **Dirección IP local**: 200.1.1.1/24
   - **Peer IP address (Dirección IP del peer)**: 100.1.1.1/24
   - **Claves previamente compartidas**: introduzca el mismo valor que el del peer A
3. Seleccione el perfil criptográfico IKE que ha creado anteriormente para usar IKE de fase 1.

STEP 6 | Configure el túnel IPSec.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)**.

© 2020 Palo Alto Networks, Inc.

2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Tunnel Interface (Interfaz de túnel)**: tunnel.41 (túnel.41)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **Perfil criptográfico de IPSec**: seleccione la puerta de enlace de IKE definida en más arriba.

   La configuración para el peer B de VPN es:

   - **Tunnel Interface (Interfaz de túnel)**: tunnel.40 (túnel.40)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **Perfil criptográfico de IPSec**: seleccione la puerta de enlace de IKE definida en más arriba.
3. Seleccione **Mostrar opciones avanzadas**, seleccione **Supervisor de túnel** y especifique una dirección IP de destino para hacer ping para verificar la conectividad.
4. Para definir la acción que se realizará si no es posible establecer conectividad, consulte Definición de perfiles supervisión de túnel.

STEP 7 | Cree políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

STEP 8 | Verifique las adyacencias OSPF y las rutas desde el CLI.

Verifique que ambos cortafuegos puedan verse entre sí con estado completo. Confirme además la dirección IP de la interfaz del túnel del peer de VPN y el ID del enrutador OSPF. Use los siguientes comandos del CLI con cada peer de VPN:

- **`show routing protocol ospf neighbor`**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```


© 2020 Palo Alto Networks, Inc.

```
admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface
2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
total routes shown: 3
```

STEP 9 | Prueba de conectividad VPN.

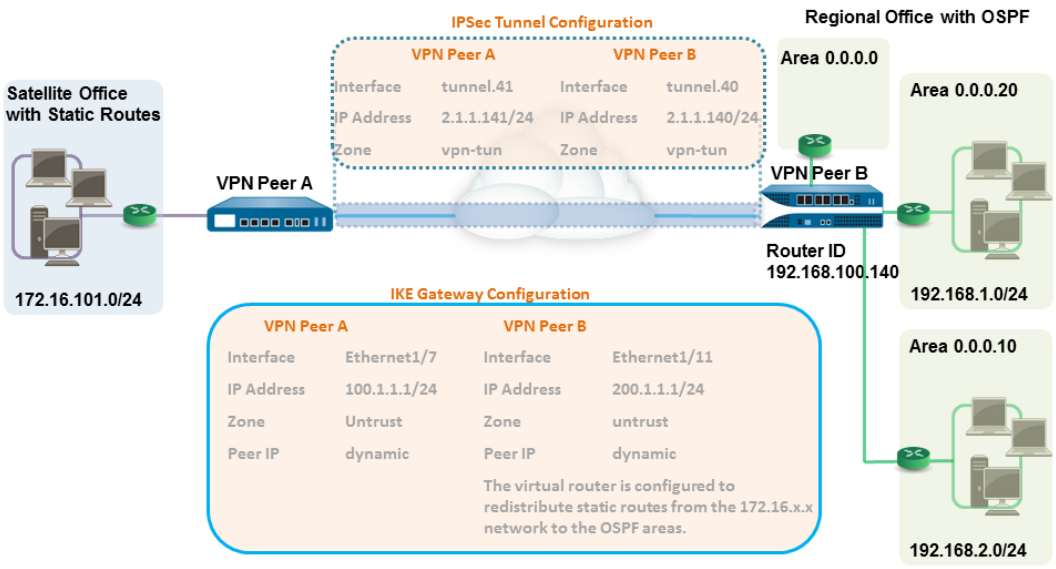
Consulte Configuración de la supervisión del túnel y Visualización del estado de los túneles.

VPN de sitio a sitio con rutas estáticas y enrutamiento dinámico

En este ejemplo, un sitio usa rutas estáticas y el otro sitio usa OSPF. Cuando el protocolo de enrutamiento no es el mismo entre ubicaciones, la interfaz del túnel en cada cortafuegos debe estar configurada con una dirección IP estática. A continuación, permita el intercambio de información de enrutamiento, el cortafuegos que participa tanto en el proceso de enrutamiento estático como el dinámico debe configurarse con un Perfil de redistribución. Configurar el perfil de redistribución habilita al enrutador virtual para redistribuir y filtrar rutas entre protocolos (rutas estáticas, rutas conectadas y hosts) desde el sistema autónomo estático al sistema autónomo OSPF. Sin este perfil de redistribución, cada protocolo funciona por su cuenta y no intercambia ninguna información de ruta con otros protocolos que se ejecutan en el mismo enrutador virtual.

En este ejemplo, la oficina satélite tiene rutas estáticas y todo el tráfico destinado a la red 192.168.x.x se enruta al túnel .41. El enrutador virtual del peer B de VPN participa tanto en el proceso de enrutamiento dinámico como el estático y está configurado como un perfil de redistribución para propagar (exportar) las rutas estáticas al sistema autónomo OSPF.

© 2020 Palo Alto Networks, Inc.



STEP 1 | Configure las interfaces de capa 3 en cada cortafuegos.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la VPN.
2. Seleccione **Layer3 (Capa 3)** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
   - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
   - Si todavía no ha creado la zona, seleccione **New Zone (Nueva zona)** en **Security Zone (Zona de seguridad)**, defina un nombre para la zona en **Name (Nombre)** y, a continuación, haga clic en **OK (Aceptar)**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Add (Añadir)** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 192.168.210.26/24.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: ethernet1/7
   - **Security Zone (Zona de seguridad)**: untrust (no fiable)
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 100.1.1.1/24

   La configuración para el peer B de VPN es:

   - **Interface (Interfaz)**: ethernet1/11
   - **Security Zone (Zona de seguridad)**: untrust (no fiable)
   - **Virtual Router (Enrutador virtual)**: default (predeterminado)
   - **IPv4**: 200.1.1.1/24

STEP 2 | Configure los perfiles criptográficos (perfil criptográfico IKE para la fase 1 y perfil criptográfico IPSec para fase 2).

Complete esta tarea en ambos peers y asegúrese de definir valores idénticos.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Crypto (Criptográfico IKE)**. En este ejemplo, hemos usado el perfil predeterminado.
2. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico IPSec)**. En este ejemplo, hemos usado el perfil predeterminado.

STEP 3 | Configure la puerta de enlace IKE.

Con claves compartidas previamente, para añadir el escrutinio de autenticación al configurar el túnel IKE de fase 1, puede configurar atributos de identificación de peer y local, y un valor correspondiente con el que coincide en el proceso de negociación.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IKE Gateway (Puerta de enlace de IKE)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Interface (Interfaz)**: ethernet1/7
   - **Local IP address (Dirección IP local)**: 100.1.1.1/24
   - **Tipo de IP de peer**: dinámica
   - **Claves previamente compartidas**: introduzca un valor
   - **Local identification (Identificación local)**: seleccione **FQDN(hostname) (FQDN [nombre de host])** e introduzca un valor para el peer A de VPN.
   - **Peer identification (Identificación del peer)**: seleccione **FQDN(hostname) (FQDN [nombre de host])** e introduzca un valor para el peer B de VPN.

   La configuración para el peer B de VPN es:

   - **Interface (Interfaz)**: ethernet1/11
   - **Dirección IP local**: 200.1.1.1/24
   - **Peer IP address (Dirección IP de peer)**: dynamic (dinámica)
   - **Claves previamente compartidas**: introduzca el mismo valor que el del peer A
   - **Identificación local**: seleccione **FQDN(nombre de host)** e introduzca un valor para el peer B de VPN.
   - **Identificación del peer**: seleccione **FQDN(nombre de host)** e introduzca un valor para el peer A de VPN.
3. Seleccione el perfil criptográfico IKE que ha creado anteriormente para usar IKE de fase 1.

STEP 4 | Cree una interfaz de túnel y vincúlela a un enrutador virtual y una zona de seguridad.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, p. ej., **.41**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:

   - Si desea usar la zona de confianza como punto de finalización del túnel, selecciónela.
   - (Recomendado) Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Nombre** para una nueva zona, por ejemplo *vpn-tun*, y haga clic en **Aceptar**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. Asigne una dirección IP a la interfaz de túnel, seleccione la pestaña **IPv4** o **IPv6**, haga clic en **Add** en la sección IP e introduzca la dirección IP y la máscara de red/prefijo para asignarlos a la interfaz; por ejemplo, 172.19.9.2/24.

   Esta dirección IP se usará para enrutar el tráfico al túnel y supervisar el estado del túnel.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

En este ejemplo, la configuración para el peer A de VPN es:

- **Interface (Interfaz)**: tunnel.41 (túnel.41)
- **Zona de seguridad**: vpn_tun
- **Virtual Router (Enrutador virtual)**: default (predeterminado)
- **IPv4**: 2.1.1.141/24

La configuración para el peer B de VPN es:

- **Interface (Interfaz)**: tunnel.42 (túnel.42)
- **Zona de seguridad**: vpn_tun
- **Virtual Router (Enrutador virtual)**: default (predeterminado)
- **IPv4**: 2.1.1.140/24

STEP 5 | Especifique la interfaz para enrutar el tráfico a un destino en la red 192.168.x.x.

1. En el peer A de VPN, seleccione el enrutador virtual.
2. Seleccione **Static Routes (Rutas estáticas)** y **Add (Añadir)** para añadir túnel.41 como la **Interface (Interfaz)** para el enrutamiento de tráfico con un **Destination (Destino)** en la red 192.168.x.x.

STEP 6 | Establezca la ruta estática y la configuración OSPF en el enrutador virtual y adjunte las áreas OSPF con las interfaces apropiadas en el cortafuegos.

1. En el peer B de VPN, seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador predeterminado o añada uno nuevo.
2. Seleccione **Static Routes (Rutas estáticas)** y **Add (Añadir)** para añadir la dirección IP del túnel como el próximo salto para el tráfico en la red 172.168.x.x.

   Asigne la métrica de ruta deseada; usando un valor bajo se aumenta la prioridad para la selección de ruta en la tabla de reenvíos.
3. Seleccione **OSPF** (para IPv4) u **OSPFv3** (para IPv6) y seleccione **Enable (Habilitar)**.
4. En este ejemplo, la configuración OSPF para el peer B de VPN es:

   - ID del enrutador: 192.168.100.140
   - ID de área: 0.0.0.0 se asigna a la interfaz Ethernet1/12 con el tipo de enlace: Broadcast
   - ID de área: 0.0.0.10 que se asigna a la interfaz Ethernet1/1 con el tipo de enlace: Broadcast
   - ID de área: 0.0.0.20 se asigna a la interfaz Ethernet1/15 con el tipo de enlace: Broadcast

STEP 7 | Cree un perfil de redistribución para inyectar las rutas estáticas en el sistema autónomo OSPF.

1. Cree un perfil de redistribución en el peer B de VPN.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador que ha usado más arriba.
   2. Seleccione **Redistribution Profiles (Perfiles de redistribución)** y haga clic en **Add (Añadir)**.
   3. Introduzca un nombre para el perfil, seleccione **Redistr.** y asigne un valor de **Prioridad**. Si ha configurado múltiples perfiles, coincidirá primero el perfil con el valor de propiedad más bajo.
   4. Defina **Source Type (Tipo de origen)** como **static (estático)** y haga clic en **OK (Aceptar)**. Se usa la ruta estática definida en el paso 6 para la redistribución.
2. Inyecte rutas estáticas en el sistema OSPF.
   1. Seleccione **OSPF** > **Export Rules (Reglas de exportación)** (para IPv4) u **OSPFv3** > **Export Rules (Reglas de exportación)** (para IPv6).
   2. Haga clic en **Add (Añadir)** y seleccione el perfil de redistribución que acaba de crear.
   3. Seleccione cómo se llevan las rutas externas al sistema OSPF. La opción predeterminada, **Ext2**, calcula el coste total de la ruta usando solo métricas externas. Para usar métricas OSPF tanto internas como externas, use **Ext1**.

© 2020 Palo Alto Networks, Inc.

4. Asigne una **Metric (Métrica)** (valor de coste) a las rutas inyectadas en el sistema OSPF. Esta opción le permite cambiar la métrica para la ruta inyectada al entrar en el sistema OSPF.
5. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure el túnel IPSec.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)**.
2. Haga clic en **Add (Añadir)** y configure las opciones en la pestaña **General**.

   En este ejemplo, la configuración para el peer A de VPN es:

   - **Tunnel Interface (Interfaz de túnel)**: tunnel.41 (túnel.41)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **Perfil criptográfico de IPSec**: seleccione la puerta de enlace de IKE definida en más arriba.

   La configuración para el peer B de VPN es:

   - **Tunnel Interface (Interfaz de túnel)**: tunnel.40 (túnel.40)
   - **Type (Tipo)**: Auto Key (Clave automática)
   - **IKE Gateway (Puerta de enlace de IKE)**: seleccione la puerta de enlace de IKE definida más arriba.
   - **Perfil criptográfico de IPSec**: seleccione la puerta de enlace de IKE definida en más arriba.
3. Seleccione **Mostrar opciones avanzadas**, seleccione **Supervisor de túnel** y especifique una dirección IP de destino para hacer ping para verificar la conectividad.
4. Para definir la acción que se realizará si no es posible establecer conectividad, consulte Definición de perfiles supervisión de túnel.

STEP 9 | Cree políticas para permitir el tráfico entre los sitios (subredes).

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Cree reglas para permitir el tráfico entre la zona no fiable y la zona vpn-tun y la zona vpn-tun y la zona no fiable para tráfico que se origine desde el origen especificado y las direcciones IP de destino.

STEP 10 | Verifique las adyacencias OSPF y las rutas desde el CLI.

Verifique que ambos cortafuegos puedan verse entre sí con estado completo. Confirme además la dirección IP de la interfaz del túnel del peer de VPN y el ID del enrutador OSPF. Use los siguientes comandos del CLI con cada peer de VPN:

- **`show routing protocol ospf neighbor`**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```


© 2020 Palo Alto Networks, Inc.

```
admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **`show routing route`**

A continuación se muestra un ejemplo de salida en cada peer de VPN.

```
VPN PeerA

destination            next hop        metric  flags   age     interface       next-AS
192.168.1.0/24         2.1.1.141       20      A S             tunnel.41
192.168.2.0/24         2.1.1.141       20      A S             tunnel.41
172.16.101.0/24        0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24           2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination            next hop        metric  flags   age     interface       next-AS
192.168.1.0/24         0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24         0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24        2.1.1.140       20      A H             tunnel.40
2.1.1.141/24           2.1.1.140       10      A C             tunnel.40
```

STEP 11 | Prueba de conectividad VPN.

Consulte Configuración de la supervisión del túnel y Visualización del estado de los túneles.

© 2020 Palo Alto Networks, Inc.

VPN a gran escala (LSVPN)

La función VPN a gran escala (LSVPN) de GlobalProtect incluida en el cortafuegos de nueva generación de Palo Alto Networks simplifica la implementación de VPN de topología en estrella tradicionales, lo que le permite implementar rápidamente redes empresariales con varias sucursales con una cantidad mínima de configuración obligatoria en los dispositivos *satélite* remotos. Esta solución utiliza certificados para la autenticación de cortafuegos e IPSec para proteger datos.

LSVPN habilita VPN de sitio a sitio entre cortafuegos de Palo Alto Networks. Para configurar una VPN de sitio a sitio entre un cortafuegos de Palo Alto Networks y otro dispositivo, consulte VPN.

Los siguientes temas describen los componentes de LSVPN y cómo configurarlos para habilitar servicios de VPN de sitio a sitio entre cortafuegos de Palo Alto Networks:

- Descripción general de LSVPN
- Creación de interfaces y zonas para la LSVPN
- Habilitación de SSL entre componentes de LSVPN de GlobalProtect
- Configuración del portal para autenticar satélites
- Configuración de puertas de enlace de GlobalProtect para LSVPN
- Configuración del portal de GlobalProtect para LSVPN
- Preparación del satélite para unirse a la LSVPN
- Verificación de la configuración de LSVPN
- Configuraciones rápidas de LSVPN

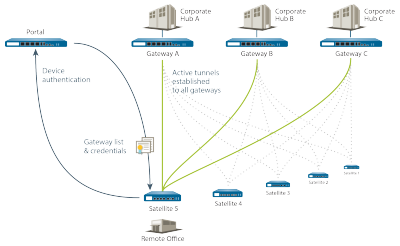
© 2020 Palo Alto Networks, Inc.

Descripción general de LSVPN

GlobalProtect proporciona una completa infraestructura para gestionar el acceso seguro a recursos corporativos desde sus ubicaciones remotas. Esta infraestructura incluye los siguientes componentes:

- Portal de GlobalProtect: Proporciona las funciones de gestión necesarias para su infraestructura de LSVPN de GlobalProtect. Cada satélite que participa en la LSVPN de GlobalProtect recibe información de configuración del portal, incluida información de configuración para permitir que los satélites (los radios) se conecten a los gateways (los concentradores). El portal se configura en una interfaz de cualquier cortafuegos de última generación de Palo Alto Networks.
- **Puertas de enlace de GlobalProtect**: cortafuegos de Palo Alto Networks que proporciona el extremo del túnel para conexiones de satélites. Los recursos a los que acceden los satélites están protegidos por la política de seguridad del gateway. No es obligatorio tener un portal y un gateway separados; un único cortafuegos puede actuar tanto de portal como de gateway.
- **Satélite de GlobalProtect**: cortafuegos de Palo Alto Networks en una ubicación remota que establece túneles de IPSec con las puertas de enlace de sus sedes para lograr un acceso seguro a recursos centralizados. La configuración del cortafuegos del satélite es mínima, lo que le permite ajustar rápida y fácilmente su VPN a medida que añada nuevas ubicaciones.

El siguiente diagrama muestra cómo funcionan los componentes de LSVPN de GlobalProtect en conjunto.



© 2020 Palo Alto Networks, Inc.

Creación de interfaces y zonas para la LSVPN

Debe configurar las siguientes interfaces y zonas para su infraestructura de LSVPN:

- **Portal de GlobalProtect**: requiere una interfaz de capa 3 para que se conecten los satélites de GlobalProtect. Si el portal y el gateway se encuentran en el mismo cortafuegos, pueden usar la misma interfaz. El portal debe estar en una zona accesible desde sus sucursales.
- **Gateways de GlobalProtect**: Requiere tres interfaces: una interfaz de capa 3 en la zona a la que pueden acceder los satélites remotos, una interfaz interna en la zona fiable que se conecta con los recursos protegidos y una interfaz de túnel lógica para finalizar los túneles de VPN desde los satélites. A diferencia de otras soluciones de VPN de sitio a sitio, el gateway de GlobalProtect solamente requiere una única interfaz de túnel, que utilizará para las conexiones de túnel con todos sus satélites remotos (punto a multipunto). Si tiene la intención de utilizar el enrutamiento dinámico, deberá asignar una dirección IP a la interfaz de túnel. GlobalProtect admite el direccionamiento IPv6 e IPv4 para la interfaz de túnel.
- **Satélite de GlobalProtect**: Requiere una única interfaz de túnel para establecer una VPN con los gateways remotos (hasta un máximo de 25 gateways). Si tiene la intención de utilizar el enrutamiento dinámico, deberá asignar una dirección IP a la interfaz de túnel. GlobalProtect admite el direccionamiento IPv6 e IPv4 para la interfaz de túnel.

Si desea más información sobre portales, puertas de enlace y satélites, consulte Descripción general de LSVPN.

STEP 1 | Configure una interfaz de capa 3.

El portal y cada gateway y cada satélite requieren una interfaz de capa 3 para permitir que el tráfico se enrute entre las distintas ubicaciones.

Si el gateway y el portal se encuentran en el mismo cortafuegos, puede utilizar una única interfaz para ambos componentes.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y, a continuación, seleccione la interfaz que desee configurar para la LSVPN de GlobalProtect.
2. Seleccione **Layer3** en el menú desplegable **Interface Type**.
3. En la pestaña **Configurar**, seleccione la **Zona de seguridad** a la que pertenezca la interfaz:
   - La interfaz debe ser accesible desde una zona fuera de su red fiable. Considere la posibilidad de crear una zona de VPN específica para lograr la visibilidad y el control necesarios del tráfico de su VPN.
   - Si todavía no ha creado la zona, seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **Nombre** para la nueva zona y, a continuación, haga clic en **ACEPTAR**.
4. Seleccione el **Virtual Router (Enrutador virtual)** que debe utilizarse.
5. Asigne una dirección IP a la interfaz:
   - Para una dirección IPv4, seleccione **IPv4** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 203.0.11.100/24.
   - Para una dirección IPv6, seleccione **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 2001:1890:12f2:11::10.1.8.160/80.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 2 | En los cortafuegos donde se alojen puertas de enlace de GlobalProtect, configure la interfaz de túnel lógica que finalizará los túneles de VPN establecidos por los satélites de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

No se requieren direcciones IP en la interfaz de túnel a menos que tenga la intención de utilizar el enrutamiento dinámico. Sin embargo, asignar una dirección IP a la interfaz de túnel puede resultar útil para solucionar problemas de conexión.

Asegúrese de habilitar User-ID en la zona donde finalizan los túneles de VPN.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.2**.
3. En la pestaña **Config (Configurar)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** para definir la zona del siguiente modo:
   - Para usar una zona fiable como punto de finalización del túnel, seleccione la zona en el menú desplegable.
   - (Recomendado) Para crear una zona separada para terminación del túnel de VPN, haga clic en **New Zone (Nueva zona)**. En el cuadro de diálogo Zona, defina un **Nombre** para la nueva zona (por ejemplo, *lsvpn-tun*), seleccione la casilla de verificación **Habilitar identificación de usuarios** y, a continuación, haga clic en **ACEPTAR**.
4. Seleccione el **Virtual Router (Enrutador virtual)**.
5. (Opcional) Para asignar una dirección IP a la interfaz de túnel:
   - Para una dirección IPv4, seleccione **IPv4** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 203.0.11.100/24.
   - Para una dirección IPv6, seleccione **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 2001:1890:12f2:11::10.1.8.160/80.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 3 | Si ha creado una zona separada para la finalización del túnel de las conexiones VPN, cree una política de seguridad para habilitar el flujo de tráfico entre la zona VPN y su zona fiable.

Por ejemplo, una regla de política habilita el tráfico entre la zona *lsvpn-tun* y la zona *L3-Trust*.

STEP 4 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Habilitación de SSL entre componentes de LSVPN de GlobalProtect

Toda la interacción entre los componentes de GlobalProtect se realiza a través de una conexión SSL/TLS. Por lo tanto, debe generar y/o instalar los certificados necesarios antes de configurar cada componente, de modo que pueda hacer referencia a los certificados y/o perfiles de certificados adecuados en las configuraciones de cada componente. En las siguientes secciones se describen los métodos compatibles de implementación de certificados, las descripciones y las directrices de recomendaciones para los diversos certificados de GlobalProtect, además de ofrecer instrucciones para la generación e implementación de los certificados necesarios:

- Acerca de la implementación de certificados
- Implementación de certificados de servidor en los componentes de LSVPN de GlobalProtect
- Implementación de certificados cliente en los satélites de GlobalProtect usando SCEP

Acerca de la implementación de certificados

Hay dos métodos básicos para implementar certificados para LSVPN de GlobalProtect:

- **Autoridad de certificación empresarial**: Si ya cuenta con su propia entidad de certificación empresarial, puede utilizar esta CA interna para emitir un certificado de CA intermedio para el portal de GlobalProtect para habilitarlo con el fin de que emita certificados para los gateways y los satélites de GlobalProtect. También puede configurar el portal de GlobalProtect para que funcione como cliente de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) para emitir certificados cliente a satélites de GobalProtect.
- **Certificados autofirmados**: Puede generar un certificado de CA raíz autofirmado en el cortafuegos y usarlo para emitir certificados de servidor para el portal, los gateways y los satélites. Si emplea certificados de CA de raíz autofirmados, es recomendable que cree un certificado de CA de raíz autofirmado en el portal y lo utilice para emitir los certificados de servidor para las puertas de enlace y los satélites. De este modo, la clave privada utilizada para la firma del certificado permanece en el portal.

Implementación de certificados de servidor en los componentes de LSVPN de GlobalProtect

Los componentes de LSVPN de GlobalProtect utilizan SSL/TLS para autenticarse mutuamente. Antes de implementar el LSVPN, debe asignar un perfil de servicio SSL/TLS a cada portal y gateway. El perfil especifica el certificado del servidor y versiones de TLS permitidas para la comunicación con dispositivos satélite. No necesita crear perfiles de servicio SSL/TLS para los dispositivos satélite debido a que el portal emitirá un certificado de servidor para cada satélite durante la primera conexión como parte del proceso de registro del dispositivo satélite.

Además, debe importar el certificado de entidad de certificación (CA) raíz utilizado para emitir los certificados de servidor en cada cortafuegos que tenga la intención de alojar como puerta de enlace o satélite. Por último, en cada puerta de enlace y satélite que participe en la LSVPN, deberá configurar un perfil de certificado que los habilitará para establecer una conexión SSL/TLS mediante la autenticación mutua.

El siguiente flujo de trabajo muestra los pasos recomendados para implementar certificados SSL en los componentes de LSVPN de GlobalProtect:

© 2020 Palo Alto Networks, Inc.

STEP 1 | En el cortafuegos que aloja el portal GlobalProtect, cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect.

Creación de un certificado de CA raíz autofirmado:

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)** y haga clic en **Generate (Generar)**.
2. Introduzca un **Certificate Name (Nombre de certificado)**, como **`LSVPN_CA`**.
3. No seleccione ningún valor en el campo **Firmado por** (esto es lo que indica que está autofirmado).
4. Seleccione la casilla de verificación **Certificate Authority (Autoridad del certificado)** y, a continuación, haga clic en **OK (Aceptar)** para generar el certificado.

STEP 2 | Cree perfiles de servicio SSL/TLS para el portal y los gateways GlobalProtect.

Para el portal y cada gateway, debe asignar un perfil de servicio SSL/TLS que haga referencia a un único certificado de servidor autofirmado.

La práctica recomendada es emitir todos los certificados necesarios en el portal, para que el certificado de firma (con la clave privada) no tenga que exportarse.

Si el portal y gateway GlobalProtect se encuentran en la misma interfaz del cortafuegos, puede utilizar el mismo certificado de servidor para ambos componentes.

1. Utilice la CA raíz en el portal para la generación de un certificado para cada puerta de enlace que implemente:
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)** y haga clic en **Generate (Generar)**.
   2. Introduzca un **Certificate Name (Nombre de certificado)**.
   3. Introduzca el FQDN (recomendado) o la dirección IP de la interfaz donde pretende configurar la puerta de enlace en el campo **Common Name (Nombre común)**.
   4. En el campo **Signed By (Firmado por)**, seleccione el certificado **`LSVPN_CA`** que acaba de crear.
   5. En la sección Atributos del certificado, haga clic en **Añadir** y defina los atributos para identificar de forma exclusiva la puerta de enlace. Tenga en cuenta que si añade un atributo **Host Name (Nombre de host)** (que cumplimenta el campo SAN del certificado), debe coincidir exactamente con el valor que haya definido en el campo **Common Name (Nombre común)**.
   6. Seleccione **Generar** el certificado.
2. Configure un perfil de servicio SSL/TLS para el portal y cada puerta de enlace:
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** y haga clic en **Add (Añadir)**.
   2. Introduzca un nombre en **Name** para identificar el perfil y seleccione el **Certificate** de servidor que acaba de crear para el portal o puerta de enlace.
   3. Defina el intervalo de versiones TLS (**Min Version**) a **Max Version**) permitido para comunicarse con dispositivos satélite y haga clic en **OK**.

STEP 3 | Implemente los certificados de servidor autofirmados en los gateways.

Recomendaciones:

- Exporte los certificados de servidor autofirmados emitidos por la CA raíz desde el portal e impórtelos en los gateways.

© 2020 Palo Alto Networks, Inc.

- Asegúrese de emitir un único certificado de servidor para cada gateway.
- El campo de nombre común (CN) y, si es aplicable, de nombre alternativo del asunto (SAN) del certificado deben coincidir con la dirección IP o con el nombre de dominio completo (FQDN) de la interfaz donde configure el gateway.

1. En el portal, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**, seleccione el certificado de puerta de enlace que desea implementar y haga clic en **Export (Exportar)**.
2. Seleccione **Clave privada cifrada y certificado (PKCS12)** en el menú desplegable **Formato de archivo**.
3. Introduzca dos veces una **Frase de contraseña** para cifrar la clave privada asociada al certificado y, a continuación, haga clic en **ACEPTAR** para descargar el archivo PKCS12 en su ordenador.
4. En la puerta de enlace, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)** y haga clic en **Import (Importar)**.
5. Introduzca un **Certificate Name (Nombre de certificado)**.
6. Introduzca la ruta y el nombre en el **archivo de certificado** que acaba de descargar del portal o seleccione **Examinar** para buscar el archivo.
7. Seleccione **Encrypted Private Key and Certificate (PKCS12) (Clave privada cifrada y certificado [PKCS12])** como el **File Format (Formato de archivo)**.
8. Introduzca la ruta y nombre en el archivo PKCS#12 en el campo **Archivo de clave** o seleccione **Examinar** para encontrarla.
9. Vuelva a introducir la **Passphrase** que usó para cifrar la clave privada cuando la exportó desde el portal y después haga clic en **OK** para importar el certificado y la clave.

STEP 4 | Importe el certificado de CA raíz utilizado para la emisión de certificados de servidor para los componentes de LSVPN.

Debe importar el certificado de CA raíz en todas los gateways y los satélites. Por motivos de seguridad, asegúrese de exportar únicamente el certificado, no la clave privada asociada.

1. Descargue el certificado de CA raíz del portal.
    1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.
    2. Seleccione el certificado de CA raíz utilizado para la emisión de certificados para los componentes de LSVPN y haga clic en **Export (Exportar)**.
    3. Seleccione **Certificado codificado en Base64 (PEM)** en la lista desplegable **Formato de archivo** y haga clic en **ACEPTAR** para descargar el certificado. (No exporte la clave privada).
2. En los cortafuegos que alojan los gateways y los satélites, importe el certificado de CA raíz.
    1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)**.
    2. Introduzca un **Certificate Name (Nombre de certificado)** que identifique al certificado como su certificado de CA de cliente.
    3. Seleccione **Browse (Examinar)** para buscar el **Certificate File (Archivo de certificado)** que ha descargado desde la CA.
    4. Seleccione **Base64 Encoded Certificate (PEM) [Certificado codificado en Base64 (PEM)]** como **File Format (Formato de archivo)** y, a continuación, haga clic en **OK (Aceptar)**.
    5. Seleccione el certificado que acaba de importar en la pestaña **Device Certificates (Certificados de dispositivos)** para abrirlo.
    6. Seleccione **Trusted Root CA (CA raíz de confianza)** y, a continuación, haga clic en **OK (Aceptar)**.
    7. Haga clic en **Commit (Confirmar)** para confirmar los cambios.

STEP 5 | Cree un perfil de certificado.

© 2020 Palo Alto Networks, Inc.

El portal y cada puerta de enlace de LSVPN de GlobalProtect requieren un perfil de certificado que especifique qué certificado utilizar para autenticar los satélites.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)** y haga clic en **Add (Añadir)** e introduzca un nombre de perfil en **Name (Nombre)**.
2. Asegúrese de establecer **Campo de nombre de usuario** como **Ninguno**.
3. En el campo **CA Certificates (Certificados de CA)**, haga clic en **Add (Añadir)** y seleccione el certificado de CA raíz de confianza que importó en el paso anterior.
4. (Recomendado) Habilite el uso de CRL y/o OCSP para habilitar la verificación del estado de certificado.
5. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 6 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Implementación de certificados cliente en los satélites de GlobalProtect usando SCEP

Como método alternativo para la implementación de certificados cliente a dispositivos satélite, puede configurar su portal de GlobalProtect para que actúe como cliente de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) en un servidor SCEP de la PKI empresarial. La operación de SCEP es dinámica ya que la PKI empresarial genera un certificado cuando el portal lo solicita y envía el certificado al portal.

Cuando el dispositivo satélite solicita una conexión al portal o puerta de enlace, también incluye su número de serie con la solicitud de conexión. El portal envía una CSR al servidor SCEP usando los ajustes del perfil SCEP y automáticamente incluye el número de serie del dispositivo en el asunto del certificado cliente. Después de recibir el certificado ciente de la PKI empresarial, el portal implementa de modo transparente el certificado cliente en el dispositivo satélite. El dispositivo satélite luego presenta el certificado cliente al portal o puerta de enlace para su autenticación.

STEP 1 | Cree un perfil de SCEP.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **SCEP** y luego **Add (Añadir)** para añadir un nuevo perfil.
2. Introduzca un nombre en **Name (Nombre)** para identificar el perfil de SCEP.
3. Si este perfil es para un cortafuegos con capacidad de sistemas virtuales múltiples, seleccione un sistema virtual o **Shared (Compartido)** como la **Location (Ubicación)** donde está disponible el perfil.

STEP 2 | (Opcional) Para que la generación de certificados basada en SCEP sea más segura, configure un mecanismo de respuesta de comprobación de SCEP entre la PKI y el portal de cada solicitud de certificado.

Después de configurar este mecanismo, su operación es invisible, y no requerirá que realice otras acciones.

Para cumplir con los estándares federales Para cumplir con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) de los Estados Unidos, use una comprobación SCEP dinámica. Para ello, haga clic en **Dynamic (Dinámica)** SCEP Challenge (Comprobación SCEP) y especifique una **Server URL (URL de servidor)** que use HTTPS (consulte el paso 7).

Seleccione una de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

- **None (Ninguna)** (valor predeterminado): el servidor SCEP no comprueba el portal antes de emitir un certificado.
- **Fixed (Fijo)**: obtenga la contraseña de comprobación de inscripción del servidor SCEP (por ejemplo, **`http://10.200.101.1/CertSrv/mscep_admin/`**) en la infraestructura PKI y luego copie o introduzca la contraseña en el campo Password (Contraseña).
- **Dynamic**: introduzca la **Server URL** de SCEP a la que el portal-cliente envía estas credenciales (por ejemplo, **`http://10.200.101.1/CertSrv/mscep_admin/`**) y un nombre de usuario y OTP que desee. El nombre de usuario y la contraseña pueden ser las credenciales del administrador de PKI.

STEP 3 | Especifique los ajustes para la conexión entre el servidor SCEP y el portal para habilitar el portal para que solicite y reciba certificados cliente.

Para identificar el satélite, el portal incluye automáticamente el número de serie del dispositivo en la solicitud CSR para el servidor SCEP. Debido a que el perfil SCEP requiere un valor en el campo **Subject**, puede dejar el símbolo **`$USERNAME`** por defecto aunque el valor no se use en los certificados cliente para LSVPN.

1. Configure la **Server URL (URL de servidor)** que usa el portal para conectarse con el servidor SCEP en la PKI (por ejemplo, **`http://10.200.101.1/certsrv/mscep/`**).
2. Introduzca una cadena (hasta 255 caracteres de extensión) en el campo **CA-IDENT Name (Nombre CA-IDENT)** para identificar el servidor SCEP.
3. Seleccione **Subject Alternative Name Type (Tipo de nombre de asunto alternativo)**:
   - **RFC 822 Name (Nombre RFC 822)**: introduzca el nombre del correo electrónico en el asunto o la extensión de nombre alternativo de asunto del certificado.
   - **DNS Name (Nombre de DNS)**: ingrese el nombre de DNS usado para evaluar los certificados.
   - **Uniform Resource Identifier (Identificador uniforme de recursos)**: introduzca el nombre del recurso desde el cual el cliente obtendrá el certificado.
   - **None (Ninguno)**: no especifique atributos para el certificado.

STEP 4 | (Opcional) Configure ajustes criptográficos para el certificado.

- Seleccione la extensión de la clave (**Number of Bits**) del certificado. Si el cortafuegos está en modo FIPS-CC y el algoritmo de generación de claves es RSA. Las claves RSA deben ser de 2048 bits o más.
- Seleccione la opción **Digest for CSR (Resumen para CSR)** que indica el algoritmo de resumen para la solicitud de firma de certificados (certificate signing request, CSR): SHA1, SHA256, SHA384 o SHA512.

STEP 5 | (Opcional) Configure los usos permitidos del certificado, ya sea para firma o cifrado.

- Para usar este certificado para la firma, seleccione la casilla de verificación **Use as digital signature**. Esto habilita el extremo para usar la clave privada en el certificado a fin de validar una firma digital.
- Para usar este certificado para cifrado, seleccione la casilla de verificación **Use for key encipherment (Usar para cifrado de clave)**. Esto habilita al cliente para usar la clave privada en el certificado para cifrar los datos intercambiados en la conexión HTTPS establecida con los certificados emitidos por el servidor SCEP.

STEP 6 | (Opcional) Para garantizar que el portal se conecte al servidor SCEP correcto, introduzca la huella digital de certificado CA en **CA Certificate Fingerprint (Huella de certificado de CA)**. Obtenga esta huella en el campo Thumbprint (Huella digital) de la interfaz del servidor SCEP.

1. Introduzca la URL para la IU administrativa del servidor SCEP (por ejemplo, **`http://<hostname or IP>/CertSrv/mscep_admin/`**).
2. Copie la huella e introdúzcala en el campo **CA Certificate Fingerprint (Huella de certificado de CA)**.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Habilite la autenticación SSL mutua entre el servidor SCEP y el portal GlobalProtect. Esto es necesario para cumplir con los estándares federales de EE. UU. de procesamiento de la información (U.S. Federal Information Processing Standard, FIPS).



La operación de FIPS-CC se indica en la página de inicio de sesión del cortafuegos y en la barra de estado del cortafuegos.

Seleccione el **CA Certificate (Certificado de CA)** raíz del servidor SCEP. De manera opcional, puede habilitar la autenticación SSL mutua entre el servidor SCEP y el portal de GlobalProtect seleccionado un **Client Certificate (Certificado de cliente)**.

STEP 8 | Guarde y confirme la configuración.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes y cierre la configuración de SCEP.
2. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

El portal intenta solicitar un certificado de CA usando los ajustes del perfil SCEP y lo guarda en el cortafuegos que aloja al portal. Si se obtiene correctamente, el certificado de CA se muestra en **Device (Dispositivo)** > **Certificate Management (Gestión de certificado)** > **Certificates (Certificados)**.

STEP 9 | (Opcional) Si después de guardar el perfil SCEP, el portal no puede obtener el certificado, usted puede generar manualmente una solicitud de firma de certificado (CSR) del portal.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y, luego, haga clic en **Generate (Generar)**.
2. Introduzca un **Certificate Name (Nombre de certificado)**. Este nombre no puede contener espacios.
3. Seleccione el **SCEP Profile (Perfil SCEP)** para usar para enviar una CSR a la PKI de su empresa.
4. Haga clic en **OK** para enviar la solicitud y generar el certificado.

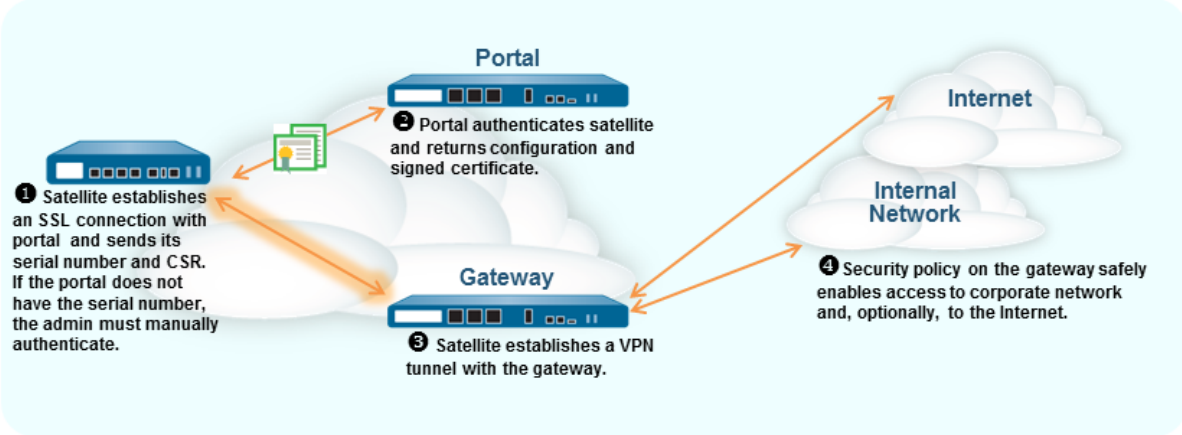
© 2020 Palo Alto Networks, Inc.

Configuración del portal para autenticar satélites

Para registrarse en la LSVPN, cada satélite debe establecer una conexión SSL/TLS con el portal. Tras establecer la conexión, el portal autentica el dispositivo satélite para asegurarse de que está autorizado para unirse a la LSVPN. Después de autenticar correctamente el satélite, el portal emitirá un certificado de servidor para el satélite y enviará la configuración de LSVPN que especifica los gateways a los que puede conectarse el satélite y el certificado de CA raíz necesario para establecer una conexión SSL con los gateways.

Hay dos formas en las que el satélite puede autenticar en el portal durante su conexión inicial:

- **Número de serie**: Puede configurar el portal con el número de serie de los cortafuegos satélite autorizados para unirse a la LSVPN. Durante la conexión inicial del satélite al portal, el satélite presenta su número de serie al portal y, si el portal tiene el número de serie en su configuración, el satélite se autenticará correctamente. Los números de serie de los satélites autorizados se añaden al configurar el portal. Consulte la Configuración del portal.
- **Nombre de usuario y contraseña**: si prefiere proporcionar sus dispositivos satélite sin introducir manualmente los números de serie de los dispositivos satélite en la configuración del portal, puede solicitar al administrador de los dispositivos satélite que los autentique al establecer la conexión inicial con el portal. Aunque el portal siempre buscará el número de serie en la solicitud inicial del satélite, si no puede identificar el número de serie, el administrador de satélites deberá proporcionar un nombre de usuario y una contraseña para autenticarlo en el portal. Debido a que el portal siempre retrocederá a esta forma de autenticación, debe crear un perfil de autenticación para confirmar la configuración del portal. Esto requiere que configure un perfil de autenticación para la configuración de LSVPN del portal, aunque tenga la intención de autenticar los satélites mediante el número de serie.



El siguiente flujo de trabajo describe el modo de configurar el portal para la autenticación de satélites mediante un servicio de autenticación existente. LSVPN de GlobalProtect admite la autenticación externa mediante una base de datos local, LDAP (incluido Active Directory), Kerberos o TACACS+ o RADIUS.

STEP 1 | (Autenticación externa únicamente) Cree un perfil de servidor en el portal.

El perfil de servidor define de qué manera el cortafuegos se conecta con un servicio de autenticación externo para validar las credenciales de autenticación proporcionadas por el administrador de dispositivos satélite.

© 2020 Palo Alto Networks, Inc.



Si utiliza la autenticación local, omita este paso y añada un usuario local para el administrador de dispositivos satélite; consulte Añada la cuenta de usuario a la base de datos local*.*

Configure un perfil de servidor para el tipo de servicio de autenticación:

- Añada un perfil de servidor RADIUS.



Puede utilizar RADIUS para integrarlo en un servicio de autenticación multifactor*.*

- Añada un perfil de servidor TACACS+.
- Añada un perfil de servidor SAML IdP.
- Añada un perfil de servidor Kerberos.
- Añada un perfil de servidor LDAP. Si está usando LDAP para conectarse a Active Directory (AD), debe crear un perfil de servidor LDAP diferente para cada dominio de AD.

STEP 2 | Configure un perfil de autenticación.

El perfil de autenticación especifica qué perfil de servidor debe utilizarse para autenticar dispositivos satélite.

1. Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name** para el perfil y, a continuación, seleccione el tipo de autenticación en **Type**. Si el **Type (Tipo)** es un servicio externo, seleccione el **Server Profile (Perfil de servidor)** que creó en el paso anterior. Si en su lugar ha añadido un usuario local, defina el **Type (Tipo)** como **Local Database (Base de datos local)**.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de puertas de enlace de GlobalProtect para LSVPN

Puesto que la configuración de GlobalProtect que el portal entrega a los satélites incluye la lista de puertas de enlace a los que puede conectarse el satélite, es recomendable configurar las puertas de enlace antes de configurar el portal.

Antes de poder configurar la puerta de enlace de GlobalProtect, debe haber realizado las tareas siguientes:

- Creación de interfaces y zonas para la LSVPNen la interfaz donde pretende configurar cada puerta de enlace. Debe configurar tanto la interfaz física como la interfaz de túnel virtual.
- Habilitación de SSL entre componentes de LSVPN de GlobalProtect al configurar los certificados de servidor de puerta de enlace, los perfiles de servicio SSL/TLS y el perfil de certificado necesario para establecer una conexión SSL/TLS mutua desde los dispositivos satélite GlobalProtect con la puerta de enlace.

Configure cada puerta de enlace de GlobalProtect para que participe en la LSVPN de la manera siguiente:

STEP 1 | Añada un gateway.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un nombre para la puerta de enlace en **Name (Nombre)**. El nombre de la puerta de enlace no puede contener espacios y se recomienda que incluya la ubicación u otra información descriptiva que ayude a los usuarios y a otros administradores a identificar la puerta de enlace.
3. (Opcional) Seleccione el sistema virtual al que pertenece esta puerta de enlace en el campo **Location (Ubicación)**.

STEP 2 | Especifique la información de red que permita a los satélites conectarse a la puerta de enlace.

Si aún no ha creado la interfaz de red para la puerta de enlace, consulte las instrucciones de Creación de interfaces y zonas para la LSVPN.

1. Seleccione la **Interfaz** que utilizarán los satélites para acceder a la puerta de enlace.
2. Especifique el **IP Address Type (Tipo de dirección IP)** y la **IP address (Dirección IP)** para el acceso a la puerta de enlace:
   - El tipo de dirección IP puede ser **IPv4** (únicamente), **IPv6** (únicamente) o **IPv4 e IPv6**. Utilice **IPv4 and IPv6 (IPv4 e IPv6)** si su red admite dos configuraciones de pila, donde IPv4 e IPv6 se ejecutan al mismo tiempo.
   - La dirección IP debe ser compatible con el tipo de dirección IP. Por ejemplo, `172.16.1/0` para las direcciones IPv4 o `21DA:D3:0:2F3B` para las direcciones IPv6. Para las configuraciones de pila doble, introduzca una dirección IPv4 e IPv6.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 3 | Especifique de qué manera la puerta de enlace autentica los dispositivos satélite al intentar establecer túneles. Si aún no ha creado un certificado de servicio SSL/TLS para la puerta de enlace, consulte Implementación de certificados de servidor en los componentes de LSVPN de GlobalProtect.

Si aún no ha configurado los perfiles de autenticación o del certificado, consulte las instrucciones de Configuración del portal para autenticar satélites.

© 2020 Palo Alto Networks, Inc.

Si aún no ha configurado el perfil de certificado, consulte las instrucciones de Habilitación de SSL entre componentes de LSVPN de GlobalProtect.

En el cuadro de diálogo de configuración de la puerta de enlace de GlobalProtect, seleccione Authentication y luego configure cualquiera de las siguientes opciones:

- Para proteger la comunicación entre la puerta de enlace y los dispositivos satélite, seleccione **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)** para la puerta de enlace.
- Para especificar el perfil de autenticación para usar en la autenticación de dispositivos satélite, seleccione **Add** para añadir una autenticación de cliente. Luego, introduzca un nombre en **Name** para identificar configuración y seleccione **OS**: **Satellite (Satélite)** para aplicar la configuración a todos los dispositivos satélite y especifique el **Authentication Profile (Perfil de autenticación)** para usar al autenticar el dispositivo satélite. También puede seleccionar un **Certificate Profile** que debe utilizar la puerta de enlace para autenticar dispositivos satélite que intenten establecer túneles.

STEP 4 | Configure los parámetros del túnel y habilite la tunelización.

1. En el cuadro de diálogo de configuración de puerta de enlace de GlobalProtect, seleccione **Satellite (Satélite)** > **Tunnel Settings (Configuraciones de túnel)**.
2. Seleccione la casilla de verificación **Configuración de túnel** para habilitar la tunelización.
3. Seleccione la **Tunnel Interface (Interfaz de túnel)** que definió para finalizar los túneles VPN establecidos por los satélites de GlobalProtect cuando realizó la tarea para Creación de interfaces y zonas para la LSVPN.
4. (Opcional) Si desea conservar la información de tipo de servicio (ToS) en los paquetes resumidos, seleccione **Copy TOS**.



Si existen varias sesiones dentro del túnel (cada una con un valor TOS diferente), el copiar el encabezado TOS puede hacer que los paquetes IPSec lleguen desordenados.

STEP 5 | (Opcional) Habilite la supervisión de túnel.

La supervisión de túnel habilita los dispositivos satélite para que supervisen su conexión de túnel de puerta de enlace, lo que permite realizar una conmutación por error a una puerta de enlace de reserva si falla la conexión. La conmutación a otra puerta de enlace es el único tipo de perfil de supervisión de túnel permitido con LSVPN.

1. Seleccione la casilla de verificación **Supervisión de túnel**.
2. Especifique la **Destination IP Address (Dirección IP de destino)** que los satélites deberían utilizar para determinar si la puerta de enlace está activa. Puede especificar una dirección **IPv4** e **IPv6**, o ambas. De forma alternativa, si ha configurado una dirección IP para la interfaz de túnel, puede dejar este campo en blanco y, en su lugar, el monitor de túnel utilizará la interfaz de túnel para determinar si la conexión está activa.
3. Seleccione **Failover (Conmutación por error)** en el menú desplegable **Tunnel Monitor Profile (Perfil de monitor de túnel)** (este es el único perfil de monitor de túnel admitido para LSVPN).

STEP 6 | Seleccione el perfil criptográfico IPSec que debe utilizarse al establecer conexiones de túnel.

El perfil especifica el tipo de cifrado de IPSec y/o el método de autenticación para proteger los datos que atraviesen el túnel. Dado que ambos extremos del túnel de una LSVPN son cortafuegos fiables de su organización, por lo general puede utilizar el perfil predeterminado, que utiliza el protocolo ESP como protocolo IPSec, el grupo DH 2, el cifrado AES-128-CBC y la autenticación SHA-1.

Seleccione **default** en el menú desplegable **IPSec Crypto Profile** para usar el perfil por defecto o seleccione **New IPSec Crypto Profile** para definir un nuevo perfil. Si desea información detallada sobre las opciones de autenticación y cifrado, consulte Definición de perfiles criptográficos IPSec.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Configure los ajustes de red para asignar los satélites durante el establecimiento del túnel de IPSec.

También puede configurar el dispositivo satélite para que envíe la configuración DNS a sus clientes locales al configurar un servidor DHCP en el cortafuegos que aloja al dispositivo satélite. En esta configuración, el satélite enviará la configuración DNS que obtenga del gateway a los clientes DHCP.

1. En el cuadro de diálogo Gateway Configuration (Configuración de puerta de enlace) de GlobalProtect, seleccione **Satellite (Satélite)** > **Network Settings (Configuración de red)**.
2. (Opcional) Si los clientes locales del dispositivo satélite necesitan resolver FQDN en la red corporativa, configure la puerta de enlace para que envíe la configuración DNS a los dispositivos satélite de una de las maneras siguientes:
   - Si la puerta de enlace tiene una interfaz configurada como cliente DHCP, puede establecer el **Inheritance Source** en esa interfaz y asignar a los dispositivos satélite de GlobalProtect los mismos ajustes recibidos por el cliente DHCP. También puede heredar los sufijos de DNS del mismo origen.
   - Defina manualmente los ajustes **DNS principal**, **DNS secundario** y **Sufijo DNS** para enviarlos a los satélites.
3. Para especificar el grupo de direcciones en **IP Pool (Grupo de IP)** para asignar la interfaz de túnel en los dispositivos satélite cuando se establezca la VPN, haga clic en **Add (Añadir)** y, a continuación, especifique los intervalos de direcciones IP que deben utilizarse.
4. Para definir a qué subredes de destino enrutar a través del túnel, haga clic en **Add (Añadir)** en el área de **Access Route (Ruta de acceso)** y, a continuación, introduzca las rutas del siguiente modo:
   - Si desea enrutar todo el tráfico desde los satélites a través del túnel, deje este campo en blanco.

     Tenga en cuenta que, en este caso, todo el tráfico excepto el destinado a la subred local se enviará a la puerta de enlace a través de túnel.

   - Para enrutar únicamente parte del tráfico a través de la puerta de enlace (lo que se denomina túneles divididos), especifique las subredes de destino que deberán tunelizarse. En este caso, el satélite enrutará el tráfico no destinado a una ruta de acceso especificada mediante su propia tabla de rutas. Por ejemplo, puede decidir tunelizar únicamente el tráfico destinado a su red corporativa y utilizar el satélite local para permitir el acceso a Internet de forma segura.
   - Si desea habilitar el enrutamiento entre satélites, introduzca la ruta de resumen para la red protegida por cada satélite.

STEP 8 | (Opcional) Defina qué rutas, si las hubiera, aceptará la puerta de enlace de los satélites.

De manera predeterminada, el gateway no añadirá ninguna ruta que los satélites anuncien en su tabla de rutas. Si no desea que la puerta de enlace acepte rutas de puerta de enlace, no necesita realizar este paso.

1. Para habilitar la puerta de enlace para que acepte rutas anunciadas por dispositivos satélite, seleccione **Satellite (Satélite)** > **Route Filter (Filtro de ruta)**.
2. Seleccione la casilla de verificación **Aceptar rutas publicadas**.
3. Para filtrar cuáles de las rutas anunciadas por los satélites deben añadirse a la tabla de rutas de la puerta de enlace, haga clic en **Añadir** y, a continuación, defina las subredes que hay que incluir. Por ejemplo, si todos los satélites están configurados con la subred 192.168.x.0/24 en el extremo de la LAN, configurando una ruta permitida de 192.168.0.0/16 para habilitar el gateway con el fin de que solamente acepte rutas del satélite si está en la subred 192.168.0.0/16.

STEP 9 | Guarde la configuración de la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes y cerrar el cuadro de diálogo de configuración de puerta de enlace de GlobalProtect.
2. Haga clic en **Commit (Confirmar)** para confirmar la configuración.

© 2020 Palo Alto Networks, Inc.

Configuración del portal de GlobalProtect para LSVPN

El portal de GlobalProtect proporciona las funciones de gestión para su LSVPN de GlobalProtect. Todos los sistemas satélite que participan en la LSVPN reciben información de configuración desde el portal, incluida información sobre los gateways disponibles, así como el certificado que necesitan para conectarse a los gateways.

Las siguientes secciones describen los procedimientos para configurar el portal:

- Tareas previas del portal de GlobalProtect para LSVPN
- Configuración del portal
- Definición de las configuraciones de satélites

Tareas previas del portal de GlobalProtect para LSVPN

Antes de poder configurar el portal de GlobalProtect, debe haber realizado las tareas siguientes:

- ❑ Creación de interfaces y zonas para la LSVPN en la interfaz donde va a configurar el portal.
- ❑ Habilitación de SSL entre componentes de LSVPN de GlobalProtect creando un perfil de servicio SSL/TLS para el certificado de servidor de portal, emitiendo certificados de servidor de puerta de enlace y configurando el portal para emitir certificados de servidor para los dispositivos satélite de GlobalProtect.
- ❑ Configuración del portal para autenticar satélites definiendo el perfil de autenticación que utilizará el portal para autenticar dispositivos satélite si el número de serie no está disponible.
- ❑ Configuración de puertas de enlace de GlobalProtect para LSVPN.

Configuración del portal

Tras completar las Tareas previas del portal de GlobalProtect para LSVPN, configure el portal de GlobalProtect del siguiente modo:

STEP 1 | Añada el portal.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un nombre en **Name (Nombre)** para el portal. El nombre del portal no debe contener espacios.
3. (Opcional) Seleccione el sistema virtual al que pertenece este portal en el campo **Location**.

STEP 2 | Especifique la información de red que permita a los satélites conectarse al portal.

Si no ha creado la interfaz de red para el portal, consulte la Creación de interfaces y zonas para LSVPN para obtener instrucciones.

1. Seleccione la **Interfaz** que utilizarán los satélites para acceder al portal.
2. Especifique el **IP Address Type (Tipo de dirección IP)** y la **IP address (Dirección IP)** para acceder por satélite al portal:
   - El tipo de dirección IP puede ser **IPv4** (solo para tráfico IPv4), **IPv6** (solo para tráfico IPv6, o **IPv4 and IPv6 (IPv4 y IPv6)**. Utilice **IPv4 and IPv6 (IPv4 e IPv6)** si su red admite dos configuraciones de pila, donde IPv4 e IPv6 se ejecutan al mismo tiempo.
   - La dirección IP debe ser compatible con el tipo de dirección IP. Por ejemplo, `172.16.1/0` para las direcciones IPv4 o `21DA:D3:0:2F3B` para las direcciones IPv6. Para las configuraciones de pila doble, introduzca una dirección IPv4 e IPv6.
3. Haga clic en **OK (Aceptar)** para guardar los cambios.

© 2020 Palo Alto Networks, Inc.

STEP 3 | Seleccione el perfil de servicio SSL/TLS que se debe usar para permitir que el dispositivo satélite establezca una conexión SSL/TLS con el portal.

Si todavía no ha creado un perfil de servicio SSL/TLS para el portal y emitió certificados de puerta de enlace, consulte la Implementación de certificados de servidores en los componentes de LSVPN de GlobalProtect.

1. En el cuadro de diálogo de configuración del portal de GlobalProtect, seleccione **Authentication**.
2. Seleccione el **SSL/TLS Service Profile**.

STEP 4 | Especifique un perfil de autenticación y perfil de certificado opcional para la autenticación de dispositivos satélite.

Si el portal no puede validar los números de serie de los dispositivos satélite en conexión, volverá al perfil de autenticación. Por lo tanto, antes de guardar la configuración del portal (al hacer clic en OK [Aceptar]), debe realizar la Configuración de un perfil de autenticación.

Seleccione **Add (Añadir)** para añadir una autenticación de cliente y luego introduzca un nombre en **Name** para identificar la configuración y seleccione **OS**: **Satellite** para aplicar la configuración a todos los dispositivos satélite y especifique el **Authentication Profile (Perfil de autenticación)** para usar al autenticar los dispositivos satélite. También puede especificar un **Certificate Profile** que debe utilizar el portal para autenticar dispositivos satélite.

STEP 5 | Proceda a definir las configuraciones que deben enviarse a los dispositivos satélite o, si ya ha creado las configuraciones de los dispositivos satélite, guarde la configuración del portal.

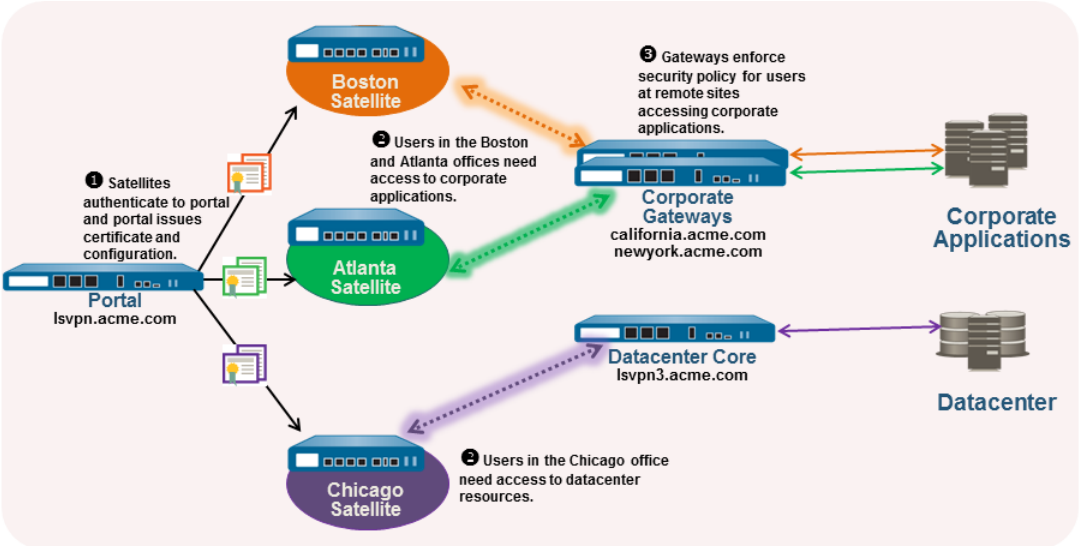
Haga clic en **OK (Aceptar)** para guardar la configuración del portal o continúe para llevar a cabo la Definición de las configuraciones de satélites.

Definición de las configuraciones de satélites

Cuando un satélite de GlobalProtect se conecta y autentica correctamente en el portal de GlobalProtect, el portal proporciona una configuración de satélite, que especifica a qué gateways puede conectarse el satélite. Si todos sus satélites van a utilizar las mismas configuraciones de gateway y certificado, puede crear una única configuración de satélite para proporcionarla a todos los satélites tras una autenticación correcta. Sin embargo, si requiere diferentes configuraciones de satélites (por ejemplo, si desea que un grupo de satélites se conecte a ungateway y otro grupo de satélite se conecte a un gateway diferente), puede crear una configuración de satélite separada para cada uno. El portal utilizará entonces el nombre de usuario/nombre de grupo de inscripción o el número de serie del dispositivo satélite para determinar qué configuración de satélite debe implementarse. Como con la evaluación de reglas de seguridad, el portal busca una coincidencia empezando por la parte superior de la lista. Cuando encuentra una coincidencia, proporciona la configuración correspondiente al satélite.

Por ejemplo, la siguiente ilustración muestra una red en la que determinadas sucursales requieren un acceso de tipo VPN a las aplicaciones corporativas protegidas por sus cortafuegos de perímetro y otra ubicación necesita un acceso de tipo VPN al centro de datos.

© 2020 Palo Alto Networks, Inc.



Utilice el siguiente procedimiento para crear una o más configuraciones de satélites.

STEP 1 | Añada una configuración de satélite.

La configuración de satélite especifica los ajustes de configuración de LSVPN de GlobalProtect que deberán implementarse en los satélites que se conecten. Debe definir al menos una configuración de satélite.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y seleccione la configuración de portal para la que desee añadir una configuración de satélite y, a continuación, seleccione la pestaña **Satellite (Satélite)**.
2. En la sección Satellite, haga clic en **Add (Añadir)**.
3. Introduzca un **Name (Nombre)** para la configuración.

   Si pretende crear múltiples configuraciones, asegúrese de que el nombre que defina para cada una sea suficientemente descriptivo para distinguirlas.
4. Para cambiar la frecuencia con la que un dispositivo satélite debería comprobar el portal para obtener actualizaciones de configuración, especifique un valor en el campo **Configuration Refresh Interval (hours)** (el intervalo es 1-48; por defecto es 24).

STEP 2 | Especifique los dispositivos satélite en los cuales implementar esta configuración.

El portal utiliza los ajustes **Usuario de inscripción/Grupo de usuarios** y/o los números de serie de **Dispositivos** para hacer coincidir un satélite con una configuración. Por lo tanto, si tiene múltiples configuraciones, asegúrese de ordenarlas correctamente. En cuanto el portal encuentre una coincidencia, distribuirá la configuración. Así, las configuraciones más específicas deberán preceder a las más generales. Consulte en el paso 5 para conocer las instrucciones sobre cómo ordenar la lista de configuraciones de satélites.

Especifique los criterios de coincidencia para la configuración de satélite de la manera siguiente:

- Para restringir esta configuración a dispositivos satélite con números de serie específicos, seleccione la pestaña **Devices (Dispositivos)**, haga clic en **Add (Añadir)**, e introduzca un número de serie (no necesita introducir el nombre de host del dispositivo satélite; se añadirá automáticamente cuando el satélite se conecte). Repita este paso para cada satélite que quiera que reciba esta configuración.
- Seleccione la pestaña **Usuario de inscripción/Grupo de usuarios**, haga clic en **Añadir** y, a continuación, seleccione el usuario o grupo que quiera que reciba esta configuración. Los satélites que no coinciden en el número de serie deberán autenticarse como un usuario especificado aquí (bien como un usuario individual, bien como un miembro de grupo).

© 2020 Palo Alto Networks, Inc.

Para poder restringir la configuración a grupos específicos, debe asignar usuarios a grupos*.*

STEP 3 | Especifique los gateways con los que los satélites con esta configuración podrán establecer túneles de VPN.

Las rutas publicadas por el gateway se instalan en el satélite como rutas estáticas. La medida para la ruta estática es 10 veces la prioridad de enrutamiento. Si tiene más de un gateway, asegúrese también de establecer la prioridad de enrutamiento para garantizar que las rutas anunciadas por gateways de reserva tienen medidas más altas en comparación con las mismas rutas anunciadas por gateways principales. Por ejemplo, si establece la prioridad de enrutamiento para el gateway principal y el gateway de reserva como 1 y 10 respectivamente, el satélite utilizará 10 como medida para el gateway principal y 100 como medida para el gateway de reserva.

1. En la pestaña **Puertas de enlace**, haga clic en **Añadir**.
2. Introduzca un **Name (Nombre)** descriptivo para la puerta de enlace. El nombre que introduzca aquí debería coincidir con el nombre que definió al configurar el gateway y debería ser lo suficientemente descriptivo para identificar la ubicación del gateway.
3. Introduzca el FQDN o la dirección IP de la interfaz donde está configurada la puerta de enlace en el campo **Gateways (Puertas de enlace)**. La dirección que especifique debe coincidir exactamente con el nombre común (common name, CN) en el certificado del servidor de la puerta de enlace.
4. (Opcional) Si está añadiendo dos o más puertas de enlace a la configuración, la **Routing Priority** ayuda al dispositivo satélite a seleccionar la puerta de enlace preferida. Introduzca un valor de entre 1 y 25; cuanto menor sea el número, mayor será la prioridad (es decir, el gateway al que se conectará el satélite si todos los gateways están disponibles). El satélite multiplicará la prioridad de enrutamiento por 10 para determinar la medida de enrutamiento.

STEP 4 | Guarde la configuración de satélite.

1. Haga clic en **OK (Aceptar)** para guardar la configuración de satélite.
2. Si desea añadir otra configuración de satélite, repita los pasos anteriores.

STEP 5 | Prepare las configuraciones de satélites para que se implemente la configuración correcta en cada satélite.

- Para subir una configuración de satélite en la lista de configuraciones, selecciónela y haga clic en **Move Up (Mover hacia arriba)**.
- Para bajar una configuración de satélite en la lista de configuraciones, selecciónela y haga clic en **Mover hacia abajo**.

STEP 6 | Especifique los certificados necesarios para permitir a los satélites participar en la LSVPN.

1. En el campo **CA raíz de confianza**, haga clic en **Añadir** y, a continuación, seleccione el certificado de CA utilizado para emitir los certificados de servidor de la puerta de enlace. El portal implementará los certificados de CA raíz que añada aquí a todos los satélites como parte de la configuración para habilitar el satélite con el fin de que pueda establecer una conexión SSL con los gateways. Se recomienda usar el mismo emisor para todos los gateways.
2. Seleccione el método de distribución de **Client Certificate**:
   - **To store the client certificates on the portal**: seleccione **Local** y seleccione el certificado de CA raíz que el portal utilizará para emitir certificados cliente para satélites tras autenticarlos correctamente desde el menú desplegable **Issuing Certificate**.

© 2020 Palo Alto Networks, Inc.



Si el certificado de CA raíz utilizado para emitir sus certificados de servidor de la puerta de enlace no está en el portal, haga clic en Import (Importar) para importarlo ahora. Consulte Habilitación de SSL entre componentes de LSVPN de GlobalProtect *para obtener información detallada sobre cómo importar un certificado de CA raíz.*

- **Para habilitar el portal para que actúe como cliente SCEP para solicitar y emitir certificados de cliente de forma dinámica**: seleccione **SCEP** y luego seleccione el perfil **SCEP** utilizado para generar CSR para su servidor SCEP.



Si aún no ha configurado el portal para que funcione como cliente SCEP, puede añadir un nuevo perfil SCEP ahora haciendo clic en New. Consulte Implementación de certificados de cliente en los satélites de GlobalProtect usando SCEP *para obtener detalles.*

STEP 7 | Guarde la configuración del portal.

1. Haga clic en **OK (Aceptar)** para guardar los ajustes y cerrar el cuadro de diálogo de configuración de puerta de portal de GlobalProtect.
2. **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Preparación del satélite para unirse a la LSVPN

Para participar en la LSVPN, los dispositivos satélite necesitan una cantidad mínima de configuración. Debido a que la configuración exigida es mínima, puede preconfigurar los dispositivos satélite antes de enviarlos a sus sucursales para su instalación.

STEP 1 | Configure una interfaz de capa 3 (consulte Configuración de interfaces de capa 3).

Esta es la interfaz física que el satélite utilizará para conectarse al portal y al gateway. Esta interfaz debe estar en una zona que permita el acceso fuera de la red fiable local. La práctica recomendada es crear una zona específica para conexiones de VPN con el fin de lograr visibilidad y control sobre el tráfico destinado a los gateways corporativos.

STEP 2 | Configure la interfaz de túnel lógica para el túnel que deberá utilizarse para establecer túneles de VPN con los gateways de GlobalProtect.



No se requieren direcciones IP en la interfaz de túnel a menos que tenga la intención de utilizar el enrutamiento dinámico. Sin embargo, asignar una dirección IP a la interfaz de túnel puede resultar útil para solucionar problemas de conexión.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)**.
2. En el campo **Interface Name (Nombre de interfaz)**, especifique un sufijo numérico, como **.2**.
3. En la pestaña **Config (Configuración)**, amplíe el menú desplegable **Security Zone (Zona de seguridad)** y seleccione una zona existente o cree una zona separada para el tráfico de túnel de VPN haciendo clic en **New Zone (Nueva zona)** y definiendo un **Name (Nombre)** para la nueva zona (por ejemplo, *lsvpnsat*).
4. En el menú desplegable **Virtual Router (Enrutador virtual)**, seleccione **default (predeterminado)**.
5. (Opcional) Para asignar una dirección IP a la interfaz de túnel:
   - Para una dirección IPv4, seleccione **IPv4** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 203.0.11.100/24.
   - Para una dirección IPv6, seleccione **IPv6**, **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** y **Add (Añadir)** para añadir la dirección IP y la máscara de red para asignar a la interfaz; por ejemplo, 2001:1890:12f2:11::10.1.8.160/80.
6. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 3 | Si generó el certificado de servidor del portal mediante una CA raíz que no es de confianza para los satélites (por ejemplo, si utilizó certificados autofirmados), importe el certificado de CA raíz utilizado para emitir el certificado de servidor del portal.

El certificado de CA raíz es obligatorio para habilitar el dispositivo satélite con el fin de que establezca la conexión inicial con el portal para obtener la configuración de LSVPN.

1. Descargue el certificado de CA que se utilizó para generar los certificados de servidor del portal. Si está utilizando certificados autofirmados, exporte el certificado de CA raíz desde el portal de la manera siguiente:
   1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivo)**.
   2. Seleccione el certificado de CA y haga clic en **Export (Exportar)**.
   3. Seleccione **Certificado codificado en Base64 (PEM)** en la lista desplegable **Formato de archivo** y haga clic en **ACEPTAR** para descargar el certificado. (No necesita exportar la clave privada.)
2. Importe el certificado de CA raíz que acaba de exportar en cada satélite de la manera siguiente.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y haga clic en **Import (Importar)**.
2. Introduzca un **Certificate Name (Nombre de certificado)** que identifique al certificado como su certificado de CA de cliente.
3. Seleccione **Browse (Examinar)** para buscar el **Certificate File (Archivo de certificado)** que ha descargado desde la CA.
4. Seleccione **Base64 Encoded Certificate (PEM) [Certificado codificado en Base64 (PEM)]** como **File Format (Formato de archivo)** y, a continuación, haga clic en **OK (Aceptar)**.
5. Seleccione el certificado que acaba de importar en la pestaña **Device Certificates (Certificados de dispositivos)** para abrirlo.
6. Seleccione **Trusted Root CA (CA raíz de confianza)** y, a continuación, haga clic en **OK (Aceptar)**.

STEP 4 | Realice la configuración de túnel de IPSec.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles de IPSec)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la configuración de IPSec.
3. Seleccione la **Tunnel Interface (Interfaz de túnel)** que creó para el satélite.
4. Seleccione **GlobalProtect Satellite (Satélite de GlobalProtect)** como el **Type (Tipo)**.
5. Introduzca la dirección IP o el FQDN del portal como la **Dirección IP del portal**.
6. Seleccione la **Interfaz** de capa 3 que configuró para el satélite.
7. Seleccione la **IP Address (Dirección IP)** que debe utilizarse en la interfaz seleccionada. Puede seleccionar una dirección **IPv4** o **IPv6**, o ambas. Especifique si desea **IPv6 preferred for portal registration (IPv6 preferida para el registro del portal)**.

STEP 5 | (Opcional) Configure el dispositivo satélite para publicar rutas locales en la puerta de enlace.

Enviar rutas al gateway permite el tráfico de las subredes locales al satélite a través del gateway. Sin embargo, también debe configurar la puerta de enlace para aceptar las rutas como se detalla en Configuración de puertas de enlace de GlobalProtect para LSVPN

1. Para permitir que el satélite envíe rutas a la puerta de enlace, en la pestaña **Avanzado**, seleccione **Publicar todas las rutas estáticas y conectadas a la puerta de enlace**.

   Si selecciona esta casilla de verificación, el cortafuegos reenviará todas las rutas estáticas y conectadas desde el satélite al gateway. Sin embargo, para evitar la creación de bucles de enrutamiento, el cortafuegos aplicará algunos filtros de ruta como los siguientes:

   - Rutas predeterminadas
   - Las rutas de un enrutador virtual distinto de los enrutadores virtuales asociados con la interfaz de túnel.
   - Rutas que usan la interfaz de túnel
   - Rutas que usan la interfaz física asociada con la interfaz de túnel
2. (Opcional) Si solamente desea enviar rutas para subredes específicas en lugar de a todas las rutas, haga clic en **Add (Añadir)** en la sección Subred y especifique qué rutas de subredes deben publicarse.

STEP 6 | Guarde la configuración de satélite.

1. Haga clic en **OK (Aceptar)** para guardar la configuración de túneles de IPSec.
2. Haga clic en **Commit (Confirmar)**.

STEP 7 | Si se le pide, proporcione las credenciales para permitir que el satélite se autentique en el portal.

Este paso solamente es obligatorio si el portal no ha podido encontrar un número de serie coincidente en su configuración o si el número de serie no ha funcionado. En este caso, el satélite no podrá establecer el túnel con los gateways.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **IPSec Tunnels (Túneles de IPSec)** y haga clic en el enlace **Gateway Info (Información de puerta de enlace)** en la columna Status (Estado) de la configuración de túnel que creó para la LSVPN.
2. Haga clic en el enlace **enter credentials (introducir credenciales)** del campo **Portal Status (Estado del portal)** e introduzca el nombre de usuario y la contraseña necesarios para autenticar el satélite en el portal.

   Después de que el satélite se autentique correctamente en el portal, recibirá su certificado firmado y su configuración, que deberá utilizar para conectarse a los gateways. Debería ver cómo se establece el túnel y cómo cambia el **Estado** a **Activo**.

© 2020 Palo Alto Networks, Inc.

Verificación de la configuración de LSVPN

Después de configurar el portal, las puertas de enlace y los dispositivos satélite, verifique que los dispositivos satélite puedan conectarse al portal y a la puerta de enlace, y establecer túneles de VPN con las puertas de enlace.

STEP 1 | Verifique la conectividad del satélite con el portal.

En el cortafuegos que aloja el portal, verifique que los satélites se conecten correctamente seleccionando **Network (Red)** > **GlobalProtect** > **Portal** y haciendo clic en **Satellite Info (Información de satélite)** en la columna Info (Información) de la entrada de configuración del portal.

STEP 2 | Verifique la conectividad del satélite con los gateways.

En cada cortafuegos que aloja una puerta de enlace, verifique que los satélites puedan establecer túneles de VPN seleccionando **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y haciendo clic en **Satellite Info (Información de satélite)** en la columna Info (Información) de la entrada de configuración de la puerta de enlace. Los satélites que hayan establecido túneles correctamente con la puerta de enlace aparecerán en la pestaña **Active Satellites (Satélites activos)**.

STEP 3 | Verifique el estado del túnel de LSVPN en el satélite.

En cada cortafuegos que aloja un satélite, verifique el estado del túnel seleccionando **Network (Red)** > **IPSec Tunnels (Túneles de IPsec)** y verifique que tiene un estado activo, lo que se indica con un icono verde.

© 2020 Palo Alto Networks, Inc.

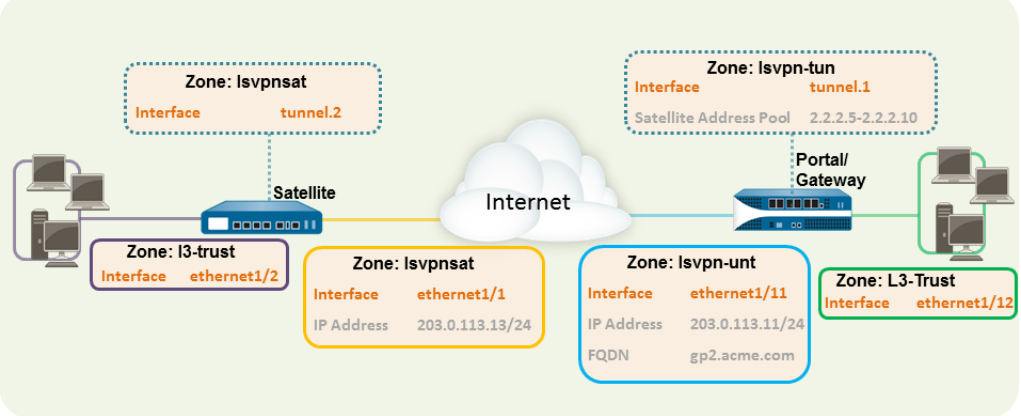
Configuraciones rápidas de LSVPN

Las siguientes secciones proporcionan instrucciones detalladas para configurar algunas implementaciones comunes de LSVPN de GlobalProtect:

- Configuración básica de LSVPN con rutas estáticas
- Configuración avanzada de LSVPN con enrutamiento dinámico
- Configuración avanzada de LSVPN con iBGP

Configuración básica de LSVPN con rutas estáticas

Esta configuración rápida muestra la forma más rápida de empezar a utilizar la LSVPN. En este ejemplo, un único cortafuegos de la ubicación de la sede de la empresa se configura como portal y como gateway. Los dispositivos satélite pueden implementarse rápida y fácilmente con una configuración mínima para garantizar una escalabilidad optimizada.



El siguiente flujo de trabajo muestra los pasos para establecer esta configuración básica:

STEP 1 | Configure una interfaz de capa 3.

En este ejemplo, la interfaz de capa 3 del portal/gateway requiere la siguiente configuración:

- **Interface (Interfaz)**: ethernet1/11
- **Zona de seguridad**: lsvpn-tun
- **IPv4**: 203.0.113.11/24

STEP 2 | En los cortafuegos donde se alojen puertas de enlace de GlobalProtect, configure la interfaz de túnel lógica que finalizará los túneles de VPN establecidos por los satélites de GlobalProtect.

Para permitir la visibilidad de los usuarios y grupos que se conecten a través de la VPN, habilite User-ID en la zona donde finalicen los túneles de VPN.

En este ejemplo, la interfaz de túnel del portal/gateway requiere la siguiente configuración:

- **Interfaz**: túnel.1
- **Zona de seguridad**: lsvpn-tun

© 2020 Palo Alto Networks, Inc.

STEP 3 | Cree la regla de la política de seguridad para habilitar el flujo de tráfico entre la zona de la VPN donde finaliza el túnel (lsvpn-tun) y la zona fiable donde residen las aplicaciones corporativas (L3-Trust).

Consulte Creación de una regla de política de seguridad.

STEP 4 | Asigne un perfil de servicio SSL/TLS al portal/puerta de enlace. El perfil debe hacer referencia a un certificado de servidor autofirmado.

El nombre de asunto del certificado debe coincidir con el FQDN o la dirección IP de la interfaz de capa 3 que cree para el portal/gateway.

1. En el cortafuegos que aloja el portal GlobalProtect, cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect. En este ejemplo, el certificado de CA raíz, **`lsvpn-CA`**, se utilizará para emitir el certificado de servidor para el portal/puerta de enlace. Además, el portal utilizará este certificado de CA raíz para firmar las CSR de los dispositivos satélite.
2. Cree perfiles de servicio SSL/TLS para el portal y los gateways GlobalProtect.

   Como el portal y la puerta de enlace estarán en la misma interfaz en este ejemplo, pueden compartir un perfil de servicio SSL/TLS que usa el mismo certificado de servidor. En este ejemplo, el perfil se denomina **`lsvpnserver`**.

STEP 5 | Cree un perfil de certificado.

En este ejemplo, el perfil del certificado **`lsvpn-profile`** hace referencia al certificado de CA raíz **`lsvpn-CA`**. La puerta de enlace utilizará este perfil de certificado para autenticar satélites que intenten establecer túneles de VPN.

STEP 6 | Configure un perfil de autenticación para que lo utilice el portal si el número de serie del satélite no está disponible.

1. Cree un tipo de perfil de servidor en el portal:
   - Añada un perfil de servidor RADIUS.

     Puede utilizar RADIUS para integrarlo en un servicio de autenticación multifactor.
   - Añada un perfil de servidor TACACS+.
   - Añada un perfil de servidor SAML IdP.
   - Añada un perfil de servidor Kerberos.
   - Añada un perfil de servidor LDAP. Si está usando LDAP para conectarse a Active Directory (AD), debe crear un perfil de servidor LDAP diferente para cada dominio de AD.
2. Configure un perfil de autenticación. En este ejemplo, el perfil **`lsvpn-sat`** se utiliza para autenticar satélites.

STEP 7 | Configuración de puertas de enlace de GlobalProtect para LSVPN.

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y haga clic en **Add (Añadir)** para añadir una configuración. Este ejemplo requiere la siguiente configuración de gateway:

- **Interface (Interfaz)**: ethernet1/11
- **Dirección IP**: 203.0.113.11/24
- **SSL/TLS Server Profile (Perfil de servidor SSL/TLS)**: lsvpnserver
- **Certificate Profile (Perfil del certificado)**: lsvpn-profile
- **Tunnel Interface (Interfaz del túnel)**: tunnel.1 (túnel.10)
- **DNS principal/DNS secundario**: 4.2.2.1/4.2.2.2

© 2020 Palo Alto Networks, Inc.

- **Grupo de IP**: 2.2.2.111-2.2.2.120
- **Access Route (Ruta de acceso)**: 10.2.10.0/24

STEP 8 | Configuración del portal.

Seleccione **Network (Red)** > **GlobalProtect** > **Portal** y **Add (Añadir)** para añadir una configuración. Este ejemplo requiere la siguiente configuración de portal:

- **Interface (Interfaz)**: ethernet1/11
- **Dirección IP**: 203.0.113.11/24
- **SSL/TLS Server Profile (Perfil de servidor SSL/TLS)**: lsvpnserver
- **Authentication Profile (Perfil de autenticación)**: lsvpn-sat

STEP 9 | Definición de las configuraciones de satélites.

En la pestaña **Satellite (Satélite)** de la configuración del portal, haga clic en **Add (Añadir)** para añadir una configuración de satélite y una CA raíz de confianza y especifique la CA que utilizará el portal para emitir certificados para los satélites. En este ejemplo, los ajustes obligatorios son los siguientes:

- **Puerta de enlace**: 203.0.113.11
- **Emisor del certificado**: lsvpn-CA
- **CA raíz de confianza**: lsvpn-CA

STEP 10 | Prepare el satélite para unirse a la LSVPN

La configuración de satélite de este ejemplo requiere los siguientes ajustes:

Configuración de interfaz

- Interfaz de capa 3: ethernet1/1, 203.0.113.13/24
- Interfaz de túnel: túnel.2
- Zona: lsvpnsat

Certificado de CA raíz del portal

- lsvpn-CA

Configuración de túnel de IPSec

- **Tunnel Interface (Interfaz del túnel)**: tunnel.2 (túnel.10)
- **Portal Address (Dirección IP del portal)**: 203.0.113.11
- **Interface (Interfaz)**: ethernet1/1
- **Dirección IP local**: 203.0.113.13/24
- **Publish all static and connected routes to Gateway (Publicar todas las rutas estáticas y conectadas a puerta de enlace)**: habilitado

Configuración avanzada de LSVPN con enrutamiento dinámico

En implementaciones de LSVPN de mayor tamaño con varios gateways y varios satélites, invertir algo más de tiempo en la configuración inicial para establecer el enrutamiento dinámico simplificará el mantenimiento de las configuraciones de gateways, ya que las rutas de acceso se actualizarán dinámicamente. La siguiente configuración de ejemplo muestra cómo ampliar la configuración básica de LSVPN para configurar OSPF como el protocolo de enrutamiento dinámico.

El establecimiento de una LSVPN para utilizar OSPF para el enrutamiento dinámico requiere los siguientes pasos adicionales en los gateways y los satélites:

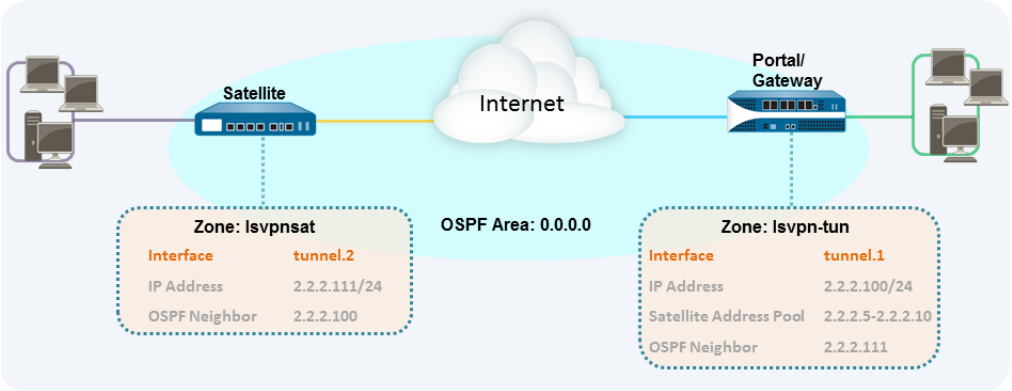
- Asignación manual de direcciones IP a interfaces de túnel en todos los gateways y todos los satélites.

© 2020 Palo Alto Networks, Inc.

- Configuración de OSPF de punto a multipunto (P2MP) en el enrutador virtual en todos los gateways y todos los satélites. Además, como parte de la configuración de OSPF de cada gateway, debe definir manualmente la dirección IP de túnel de cada satélite como un vecino OSPF. Del mismo modo, en cada satélite, debe definir manualmente la dirección IP de túnel de cada gateway como un vecino OSPF.

Aunque el enrutamiento dinámico requiere una configuración adicional durante la configuración inicial de la LSVPN, reduce las tareas de mantenimiento asociadas a la actualización de las rutas a medida que se producen cambios de topología en su red.

La siguiente ilustración muestra una configuración de enrutamiento dinámico de LSVPN. Este ejemplo muestra cómo configurar OSPF como el protocolo de enrutamiento dinámico para la VPN.



Para realizar una configuración básica de una LSVPN, siga los pasos de Configuración básica de LSVPN con enrutamiento estático. A continuación, podrá realizar los pasos del siguiente flujo de trabajo para ampliar la configuración con el fin de utilizar el enrutamiento dinámico en lugar de rutas estáticas.

STEP 1 | Añada una dirección IP a la configuración de interfaz de túnel en cada gateway y cada satélite.

Realice los siguientes pasos en cada gateway y cada satélite:

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y seleccione la configuración de túnel que creó para la LSVPN, para abrir el cuadro de diálogo Tunnel Interface (Interfaz de túnel).

   Si aún no ha creado la interfaz de túnel, consulte el paso 2 en Creación de interfaces y zonas para la LSVPN.
2. En la pestaña **IPv4**, haga clic en **Añadir** y, a continuación, introduzca una dirección IP y una máscara de subred. Por ejemplo, para añadir una dirección IP para la interfaz de túnel de gateway, debería introducir 2.2.2.100/24.
3. Haga clic en **OK (Aceptar)** para guardar la configuración.

STEP 2 | Configure el protocolo de enrutamiento dinámico en el gateway.

Para configurar OSPF en el gateway:

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual asociado a sus interfaces de VPN.
2. En la pestaña **Áreas**, haga clic en **Añadir** para crear el área troncal, o bien, si ya está configurada, haga clic en el ID de área para editarlo.
3. Si está creando una nueva área, introduzca un **Area ID (ID de área)** en la pestaña **Type (Tipo)**.
4. En la pestaña **Interfaz**, haga clic en **Añadir** y seleccione la **Interfaz** de túnel que creó para la LSVPN.
5. Seleccione **p2mp** como **Tipo de enlace**.
6. Haga clic en **Add** en la sección Neighbors e introduzca la dirección IP de la interfaz de túnel de cada dispositivo satélite; por ejemplo, 2.2.2.111.

© 2020 Palo Alto Networks, Inc.

7. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración del enrutador virtual y, a continuación, haga clic en **Commit (Confirmar)** para confirmar los cambios en la puerta de enlace.
8. Repita este paso cada vez que añada un nuevo satélite a la LSVPN.

STEP 3 | Configure el protocolo de enrutamiento dinámico en el satélite.

Para configurar OSPF en el satélite:

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual asociado a sus interfaces de VPN.
2. En la pestaña **Áreas**, haga clic en **Añadir** para crear el área troncal, o bien, si ya está configurada, haga clic en el ID de área para editarlo.
3. Si está creando una nueva área, introduzca un **Area ID (ID de área)** en la pestaña **Type (Tipo)**.
4. En la pestaña **Interfaz**, haga clic en **Añadir** y seleccione la **Interfaz** de túnel que creó para la LSVPN.
5. Seleccione **p2mp** como **Tipo de enlace**.
6. Haga clic en **Añadir** en la sección Vecinos e introduzca la dirección IP de la interfaz de túnel de cada puerta de enlace de GlobalProtect, por ejemplo, 2.2.2.100.
7. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración del enrutador virtual y, a continuación, haga clic en **Commit (Confirmar)** para confirmar los cambios en la puerta de enlace.
8. Repita este paso cada vez que añada un nuevo gateway.

STEP 4 | Verifique que los gateways y los satélites pueden formar adyacencias de enrutador.

- En cada satélite y cada gateway, confirme que se han formado adyacencias de peer y que se han creado entradas de tabla de rutas para los peers (es decir, que los satélites tienen rutas hacia los gateways y los gateways tienen rutas hacia los satélites). Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y luego haga clic en el enlace **More Runtime Stats (Más estadísticas de tiempo de ejecución)** para el enrutador virtual que está utilizando para la LSVPN. En la pestaña Enrutamiento, verifique que el peer de la LSVPN tiene una ruta.
- En la pestaña **OSPF** > **Interface (Interfaz)**, verifique que el **Type (Tipo)** sea **p2mp**.
- En la pestaña **OSPF** > **Neighbor (Vecino)**, verifique que los cortafuegos que alojan a sus puertas de enlace hayan establecido adyacencias de enrutador con los cortafuegos que alojan a sus satélites y viceversa. Verifique también que el **Estado** es **Completo**, lo que indica que se han establecido adyacencias completas.

Configuración avanzada de LSVPN con iBGP

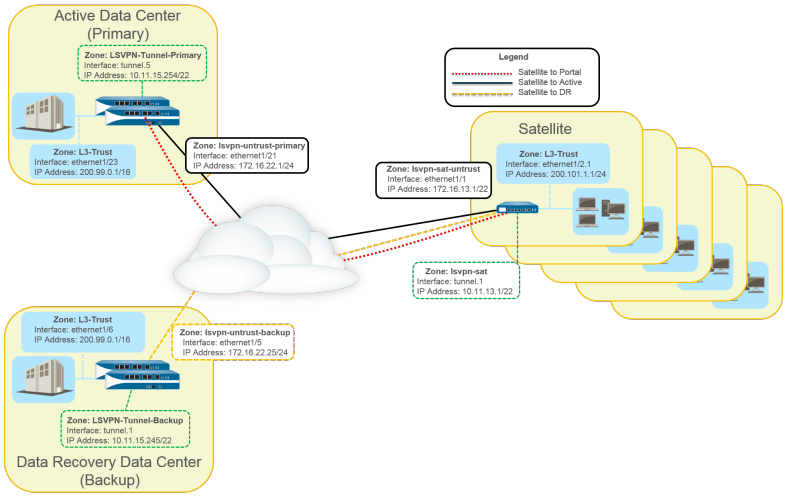
Este caso de uso ilustra de qué manera la LSVPN de GlobalProtect conecta de manera segura las ubicaciones de oficina distribuidas con centros de datos primarios y de recuperación ante desastres que alojan aplicaciones críticas para los usuarios, y de qué manera el protocolo de puerta de enlace de límite interno (iBGP) facilita la implementación y el mantenimiento. Usando este método, puede extender hasta 500 oficinas satélites mediante la conexión a una sola puerta de enlace.

BGP es un protocolo de enrutamiento dinámico altamente escalable que es ideal para implementaciones en forma de estrella, tales como LSVPN. Como protocolo de enrutamiento dinámico, elimina gran parte de la sobrecarga asociada con las rutas de acceso (rutas estáticas), al permitir una implementación relativamente fácil de cortafuegos satélites adicionales. Debido a sus prestaciones y características de filtro, tales como varios temporizadores ajustables, amortiguación de ruta y actualización de ruta, escalas de BGP a una cantidad mucho más grande de prefijos de enrutamiento con mayor estabilidad que otros protocolos de enrutamiento, como RIP y OSPF. En el caso de iBGP, un grupo de peer que incluye todos los satélites y puertas de enlace de la implementación LSVPN, establece adyacencias en los endpoints del túnel. Entonces, el protocolo implícitamente toma el control de los anuncios, actualizaciones y convergencias de la ruta.

© 2020 Palo Alto Networks, Inc.

En este ejemplo de configuración, un par HA activo/pasivo de cortafuegos PA-5200 se implementa en el centro de datos primarios (activo) y actúa como el portal y puerta de enlace primaria. El centro de datos de recuperación ante desastres también posee dos PA-5200 en un par de HA activo/pasivo, que actúa como puerta de enlace de LSVPN de copia de seguridad. El portal y las puertas de enlace actúan como 500 PA-220 implementados como satélites de LSVPN en las sucursales.

Ambos centros de datos anuncian las rutas, pero con diferentes métricas. Como resultado, los satélites prefieren e instalan las rutas de centros de datos activos. Sin embargo, las rutas de respaldo también existen en la base de información de enrutamiento (routing information base, RIB). Si el centro de datos activo falla, las rutas anunciadas por el centro de datos se eliminan y reemplazan por rutas del centro de datos de recuperación ante desastres. El tiempo de conmutación por error depende de la selección de los tiempos de iBGP y la convergencia de enrutamiento asociada con iBGP.



El siguiente flujo de trabajo muestra los pasos para configurar esta implementación:

STEP 1 | Creación de interfaces y zonas para la LSVPN.

Portal y puerta de enlace primaria:

- **Zone (Zona)**: LSVPN-Untrust-Primary
- Interface (Interfaz): ethernet1/21
- IPv4: 172.16.22.1/24
- **Zone (Zona)**: L3-Fiable
- **Inteface (Interfaz)**: ethernet1/23
- **IPv4**: 200.99.0.1/16

Backup gateway (Puerta de enlace de copia de seguridad):

- **Zone (Zona)**: LSVPN-Untrust-Primary
- **Interface (Interfaz)**: ethernet1/5
- **IPv4**: 172.16.22.25/24
- **Zone (Zona)**: L3-Fiable
- **Interface (Interfaz)**: ethernet1/6
- **IPv4**: 200.99.0.1/16

Satélite:

- **Zone (Zona)**: LSVPN-Sat-Untrust

© 2020 Palo Alto Networks, Inc.

- **Interface (Interfaz)**: ethernet1/1
- **IPv4**: 172.16.13.1/22
- **Zone (Zona)**: L3-Fiable
- **Interface (Interfaz)**: ethernet1/2.1
- **IPv4**: 200.101.1.1/24



Configure las zonas, interfaces y direcciones IP en cada satélite. La interfaz y dirección IP local serán diferentes para cada satélite. Esta interfaz se utiliza para la conexión VON al portal y la puerta de enlace.

STEP 2 | En los cortafuegos donde se alojen puertas de enlace de GlobalProtect, configure la interfaz de túnel lógica que finalizará los túneles de VPN establecidos por los satélites de GlobalProtect.

Puerta de enlace primaria:

- **Interfaz**: tunnel.5
- **IPv4**: 10.11.15.254/22
- **Zone (Zona)**: LSVPN-Tunnel-Primary

Puerta de enlace de respaldo:

- **Interface (Interfaz)**: tunnel.1
- **IPv4**: 10.11.15.245/22
- **Zone (Zona)**: LSVPN-Tunnel-Backup

STEP 3 | Habilitación de SSL entre componentes de LSVPN de GlobalProtect.

La puerta de enlace utiliza la autoridad de certificado (certificate authority, CA) de raíz autofirmado para emitir certificados para los satélites en una LSVPN de GlobalProtect. Debido a que un cortafuegos aloja el portal y la puerta de enlace primaria, se utiliza un mismo certificado para autenticar en los satélites. El mismo CA se utiliza para generar un certificado para la puerta de enlace de respaldo. El CA genera certificados que se envían a los satélites desde el portal y luego son utilizados por los satélites para la autenticación en las puertas de enlace.

Usted debe generar también un certificado del mismo CA para la puerta de enlace de respaldo, que permite autenticarse con los satélites.

1. En el cortafuegos que aloja el portal GlobalProtect, cree el certificado de CA raíz para la emisión de certificados autofirmados para los componentes de GlobalProtect. En este ejemplo, el certificado CA raíz se denomina CA-cert.
2. Cree perfiles de servicio SSL/TLS para el portal y los gateways GlobalProtect. Si el portal y la puerta de enlace primaria de GlobalProtect se encuentran en la misma interfaz del cortafuegos, puede utilizar el mismo certificado de servidor para ambos componentes.
   - **Certificado CA raíz:** CA-Cert
   - **Nombre del certificado**: Escala LSVPN
3. Implemente los certificados de servidor autofirmados en los gateways.
4. Importe el certificado de CA raíz utilizado para la emisión de certificados de servidor para los componentes de LSVPN.
5. Cree un perfil de certificado.
6. Repita los pasos del 2 al 5 en la puerta de enlace de respaldo con los siguientes ajustes:
   - **Certificado CA raíz:** CA-cert
   - **Nombre del certificado**: LSVPN-back-GW-cert

STEP 4 | Configuración de puertas de enlace de GlobalProtect para LSVPN.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, nombre la puerta de enlace primaria como **`LSVPN-Scale`**.
3. En **Network Settings (Configuración de red)**, seleccione **`ethernet1/21`** como la puerta de enlace primaria e introduzca **`172.16.22.1/24`** como la dirección IP.
4. En la pestaña **Authentication (Autenticación)**, seleccione el certificado de LSVPN creado en el paso 3.
5. Seleccione **Satellite (Satélite)** > **Tunnel Settings (Ajustes de túnel)** y seleccione **Tunnel Configuration (Configuración de túnel)**. Configure la **Tunnel Interface (Interfaz de túnel)** en tunnel.5. Todos los satélites en este caso de uso se conectan con una misma puerta de enlace, por lo que se necesita una sola configuración de satélite. Los satélites son cotejados según el número de serie, por lo que no se necesitarán satélites para autenticarse como usuario.
6. En **Satellite (Satélite)** > **Network Settings (Configuración de red)**, defina el grupo de direcciones IP para asignar a la interfaz de túnel en el satélite una vez que se establece la conexión VPN. Debido a que este caso de uso utiliza un enrutamiento dinámico, el ajuste de las rutas de acceso permanece en blanco.
7. Repita los pasos del 1 al 5 en la puerta de enlace de respaldo con los siguientes ajustes:
   - **Name (Nombre)**: LSVPN de respaldo
   - **Interfaz de puerta de enlace**: ethernet1/5
   - **IP de puerta de enlace**: 172.16.22.25/24
   - **Certificado de servidor**: LSVPN-backup-GW-cert
   - **Interfaz de túnel**: tunnel.1

STEP 5 | Configure iBGP en las puertas de enlace primaria y de respaldo, y añada un perfil de redistribución para permitir que los satélites introduzcan rutas locales nuevamente en las puertas de enlace.

Cada oficina satélite gestiona su propia red y cortafuegos, por lo que el perfil de redistribución denominado ToAllSat se configura para redistribuir las rutas locales nuevamente a la puerta de enlace de GlobalProtect.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y **Add (Añadir)** para añadir un enrutador virtual.
2. En **Router Settings (Configuración de enrutador)**, añada el **Name (Nombre)** y la **Interface (Interfaz)** para el enrutador virtual.
3. En **Redistribution Profile (Perfil de redistribución)** y seleccione **Add (Añadir)**.
   1. Nombre el perfil de redistribución **`ToAllSat`** y configure la **Priority (Prioridad)** en 1.
   2. Configure Redistribute (Redistribuir) en **Redist (Redistribución)**.
   3. Seleccione **Add (Añadir)** **`ethernet1/23`** en la lista desplegable de la interfaz.
   4. Haga clic en **OK (Aceptar)**.
4. Seleccione **BGP** en el enrutador virtual para configurar BGP.
   1. En **BGP** > **General**, seleccione **Enable (Habilitar)**.
   2. Ingrese la dirección IP de la puerta de enlace como la **Router ID (ID de enrutador)** (**`172.16.22.1`**) y **`1000`** como el **AS Number (Número AS)**.
   3. En la sección Options (Opciones), seleccione **Install Route (Instalar ruta)**.
   4. En **BGP** > **Peer Group (Grupo de peer)**, haga clic en **Add (Añadir)** para añadir un grupo de peer con todos los satélites que se conectarán a la puerta de enlace.
   5. En **BGP** > **Redist Rules (Reglas de distribución)**, seleccione **Add (Añadir)** para añadir el perfil de distribución **`ToAllSat`** que creó anteriormente.
5. Haga clic en **OK (Aceptar)**.
6. Repita los pasos del 1 al 5 en la puerta de enlace de respaldo usando **`ethernet1/6`** para el perfil de distribución.

© 2020 Palo Alto Networks, Inc.

STEP 6 | Prepare el satélite para unirse a la LSVPN

La configuración que se muestra es un ejemplo de un solo satélite.

Repita esta configuración cada vez que añada un nuevo satélite a la implementación de LSVPN.

1. Configure una interfaz de túnel como el endpoint de túnel para la conexión VPN a las puertas de enlace.
2. Configure el tipo de túnel IPSec en GlobalProtect Satellite (Satélite de GlobalProtect) e introduzca la dirección IP del portal de GlobalProtect.
3. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y **Add (Añadir)** para añadir un enrutador virtual.
4. En **Router Settings (Configuración de enrutador)**, añada el **Name (Nombre)** y la **Interface (Interfaz)** para el enrutador virtual.
5. Seleccione **Virtual Router (Enrutador virtual)** > **Redistribution Profile (Perfil de redistribución)** y seleccione **Add (Añadir)** para añadir un perfil con los siguientes ajustes.
    1. Nombre el perfil de redistribución **`ToLSVPNGW`** y configure la **Priority (Prioridad)** en 1.
    2. Seleccione **Add (Añadir)** para añadir una **Interface (Interfaz)** **`ethernet1/2.1`**.
    3. Haga clic en **OK (Aceptar)**.
6. Seleccione **BGP** > **General**, **Enable (Habilitar)** BGP y configure el protocolo de la siguiente manera:
    1. Ingrese la dirección IP de la puerta de enlace como la **Router ID (ID de enrutador)** (**`172.16.22.1`**) y **`1000`** como el **AS Number (Número AS)**.
    2. En la sección Options (Opciones), seleccione **Install Route (Instalar ruta)**.
    3. En **BGP** > **Peer Group (Grupo de peer)**, haga clic en **Add (Añadir)** para añadir un grupo de peer con todos los satélites que se conectarán a la puerta de enlace.
    4. En **BGP** > **Redist Rules (Reglas de distribución)**, seleccione **Add (Añadir)** para añadir el perfil de distribución **`ToLSVPNGW`** que creó anteriormente.
7. Haga clic en **OK (Aceptar)**.

STEP 7 | Configure el portal de GlobalProtect para LSVPN.

Ambos centros de datos anuncian sus rutas, pero con diferentes prioridades de enrutamiento para garantizar que el centro de datos activos sea la puerta de enlace preferida.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** y haga clic en **Add (Añadir)**.
2. En **General**, introduzca **`LSVPN-Portal`** como el nombre del portal.
3. En **Network Settings (Configuración de red)**, seleccione **`ethernet1/21`** como la **Interface (Interfaz)** y seleccione **`172.16.22.1/24`** como la **IP Address (Dirección IP)**.
4. En la pestaña **Authentication (Autenticación)**, seleccione el perfil SSL/TLS de la puerta de enlace creada anteriormente **`LSVPN-Scale`** en el menú desplegable **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.
5. En la pestaña **Satellite (Satélite)**, seleccione **Add (Añadir)** para añadir un satélite y en **Name (Nombre)** ingrese **`sat-config-1`**.
6. Configure el **Configuration Refresh Interval (Intervalo de actualización de configuración)** en **`12`**.
7. En **GlobalProtect Satellite (Satélite de GlobalProtect)** > **Devices (Dispositivos)**, añada el número de serie y nombre de host de cada dispositivo satélite en la LSVPN.
8. En **GlobalProtect Satellite (Satélite de GlobalProtect)** > **Gateways (Puertas de enlace)**, añada el nombre y la dirección IP de cada puerta de enlace. Configure la prioridad de enrutamiento de la puerta de enlace primaria en 1 y la puerta de enlace de respaldo en 10 para garantizar que el centro de datos activo sea la puerta de enlace preferida.

STEP 8 | Verifique la configuración de LSVPN.

STEP 9 | (Opcional) Añada una nueva ubicación a la implementación LSVPN.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **GlobalProtect Portal (Portal de GlobalProtect)** > **Satellite Configuration (Configuración del satélite)** > **GlobalProtect Satellite (Satélite de GlobalProtect)** > **Devices (Dispositivos)** para añadir el número de serie del nuevo satélite al portal de GlobalProtect.
2. Configure el túnel IPSec en el satélite con la dirección IP el portal de GlobalProtect.
3. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** > **BGP** > **Peer Group (Grupo de peer)** para añadir el satélite a la configuración de grupo de peer BGP en cada puerta de enlace.
4. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** > **BGP** > **Peer Group (Grupo de peer)** para añadir las puertas de enlace a la configuración de grupo de peer BGP en el nuevo satélite.

Networking

Todos los cortafuegos de próxima generación de Palo Alto Networks® proporcionan una arquitectura de red flexible que incluye la compatibilidad con el enrutamiento dinámico, la conmutación y la conectividad de VPN, lo que le permite implementar el cortafuegos en prácticamente cualquier entorno de red. Al configurar los puertos Ethernet en su cortafuegos, podrá elegir entre una implementación de interfaz de Virtual Wire, capa 2 o capa 3. Además, para permitirle integrar una variedad de segmentos de red, podrá configurar diferentes tipos de interfaces en diferentes puertos. Tras configurar las interfaces de red, puede realizar la Exportación de los datos de la tabla de configuración como PDF o CSV para una revisión o auditoría interna.

Los siguientes temas describen conceptos de redes y cómo integrar cortafuegos de próxima generación de Palo Alto Networks en su red.

- Configuración de interfaces
- Enrutadores virtuales
- Rutas de servicio
- Rutas estáticas
- RIP
- OSPF
- BGP
- IP de multidifusión
- Redistribución de ruta
- Túneles GRE
- DHCP
- DNS:
- Descripción general del DNS dinámico
- Configuración del DNS dinámico en las interfaces de cortafuegos
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD
- Configuración de sesión y tiempos de espera de sesión
- Inspección del contenido del túnel

© 2020 Palo Alto Networks, Inc.

Configuración de interfaces

Un cortafuegos de última generación Palo Alto Networks puede funcionar en múltiples implementaciones a la vez porque las implementaciones se producen en el nivel de la interfaz. Por ejemplo, puede configurar algunas interfaces para que las interfaces de capa 3 integren el cortafuegos a su entorno de enrutamiento dinámico y configurar otras interfaces de modo que se integren en su red de conmutación de capa 2. Los siguientes temas describen cada tipo de implementación de interfaz y cómo configurar los tipos de interfaces correspondientes:

- Interfaces de modo tap
- Interfaces de cable virtual
- Interfaces de capa 2
- Interfaces de capa 3
- Configuración de los grupos de interfaces de agregación
- Uso de los perfiles de gestión de interfaz para restringir el acceso

Interfaces de modo tap

Un tap de red es un dispositivo que proporciona acceso a los datos que atraviesan una red de equipos. La implementación del modo tap permite supervisar de forma pasiva los flujos de tráfico a través de una red mediante un conmutador SPAN o un puerto espejo.

El puerto SPAN o de espejo permite copiar el tráfico de otros puertos en el conmutador. Al configurar una interfaz del cortafuegos como interfaz de modo tap y conectarla con un puerto SPAN de conmutación, este puerto proporciona al cortafuegos un reflejo del tráfico. De esta forma es posible visualizar la aplicación en la red sin necesidad de estar en el flujo del tráfico de red.

Al implementar el cortafuegos en modo tap, obtiene visibilidad sobre las aplicaciones que están ejecutando en la red sin tener que realizar ningún cambio en su diseño. En este modo, el cortafuegos también puede identificar las amenazas que se ciernen sobre la red. No obstante, tenga en cuenta que no hay tráfico en el cortafuegos en este modo, por lo que no puede realizar ninguna acción sobre él, como bloquear el tráfico con amenazas o aplicar el control del tráfico con QoS.

Para configurar una interfaz de modo tap y empezar a supervisar las aplicaciones de la red y las amenazas que se ciernen sobre ella:

STEP 1 | Decida el puerto que desea utilizar como interfaz de modo tap y conéctelo a un conmutador configurado con SPAN, RSPAN o reflejo de puertos.

El tráfico de la red se envía desde el puerto SPAN de destino por el cortafuegos, de modo que obtenga visibilidad sobre las aplicaciones de la red y las amenazas que se ciernen sobre ella.

STEP 2 | En la interfaz web del cortafuegos, configure la interfaz que desea utilizar en el modo tap de la red.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz que corresponde al puerto que acaba de cablear.
2. Seleccione **Tap** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**.
4. En el cuadro de diálogo Zone (Zona), introduzca el nombre de la zona en **Name (Nombre)** (por ejemplo, TapZone [ZonaTap]) y haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Cree los perfiles de reenvío que desea utilizar.

© 2020 Palo Alto Networks, Inc.

- Configuración de perfiles de reenvío de logs
- Configuración de la monitorización de syslog

STEP 4 | Cree Perfiles de seguridad para analizar el tráfico de la red en busca de amenazas:

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)**.
2. En cada uno de los tipos de perfiles de seguridad, haga clic en **Add (Añadir)** para añadir un perfil nuevo y configure la acción en **alert (alertar)**.

   Como el cortafuegos no está en línea con el tráfico, no se pueden especificar las acciones de bloqueo ni de restablecimiento. Al configurar la alerta como acción, ve todas las amenazas que detecta el cortafuegos en los logs y en el centro de control de aplicaciones (application command center, ACC).

STEP 5 | Cree una regla de la política de seguridad para permitir el tráfico en la interfaz de modo tap.

Cuando cree una regla de la política de seguridad para el modo tap, las zonas de origen y de destino deben ser la misma.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en la zona TapZone (ZonaTap) que acaba de crear.
3. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** también en la zona TapZone (ZonaTap).
4. Configure todos los criterios de coincidencia con la regla, **Applications (Aplicaciones)**, **User (Usuario)**, **Service (Servicio)** y **Address Dirección)**, en **any (cualquiera)**.
5. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
6. Configure **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione todos los perfiles de seguridad que ha creado para alertar sobre las amenazas.
7. Verifique que **Log at Session End** esté habilitado.
8. Haga clic en **OK (Aceptar)**.
9. Coloque la regla al principio de la base de reglas.

STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 7 | Supervise los logs del cortafuegos con **Monitor (Supervisar)** > **Logs (Logs)** y el **ACC** para obtener información sobre las aplicaciones de la red y las amenazas que se ciernen sobre ella.

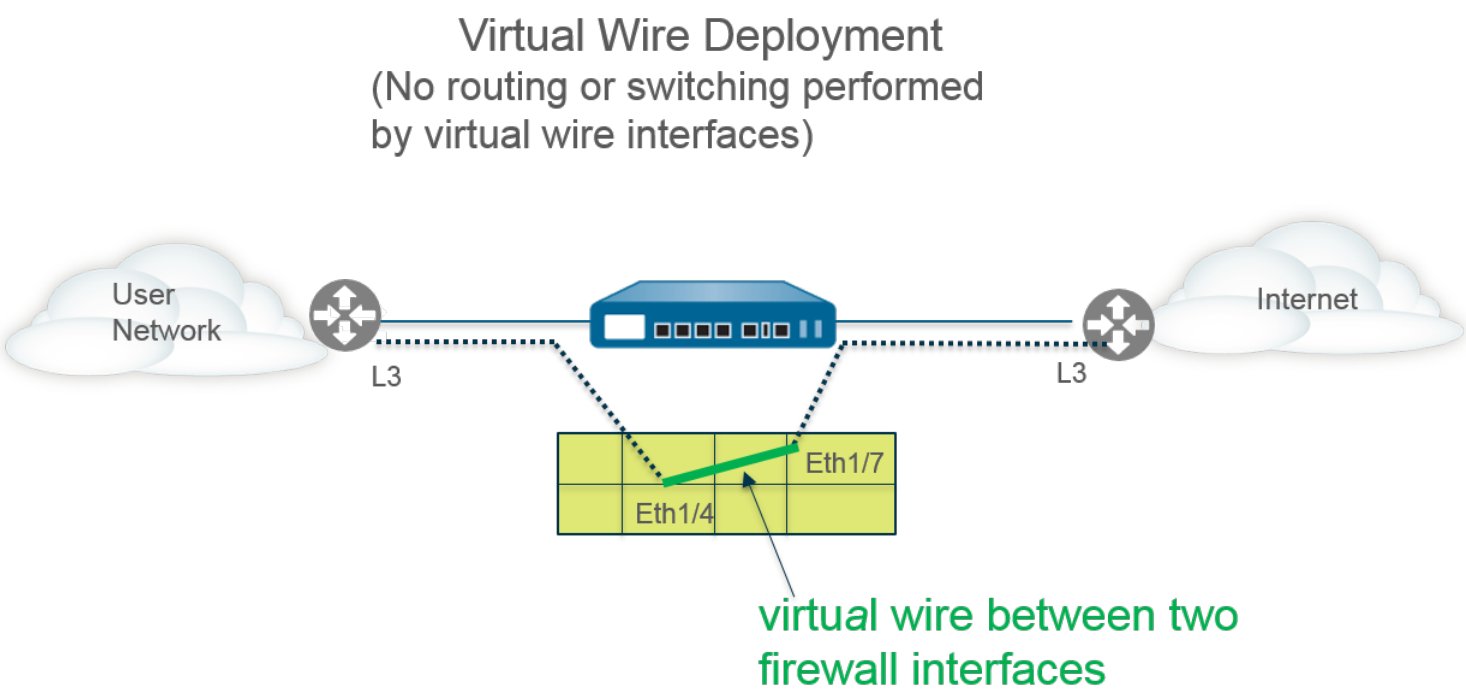
Interfaces de cable virtual

En una implementación de cable virtual, debe instalar un cortafuegos de forma transparente en un segmento de red uniendo dos puertos (interfaces) del cortafuegos. Evidentemente, el cable virtual conecta dos interfaces; por lo tanto, el cable virtual es un componente interno del cortafuegos.

Utilice una implementación de cable virtual solo cuando desee integrar sin inconvenientes un cortafuegos en una topología y las dos interfaces conectadas en el cortafuegos no deben llevar a cabo conmutación o enrutamiento. En el caso de estas dos interfaces, el cortafuegos se considera como *puesto en el cable (bump-in-the-wire)*.

Una implementación de cable virtual simplifica la instalación y la configuración del cortafuegos debido a que puede insertar el cortafuegos en una topología existente sin asignar direcciones MAC o IP a las interfaces, rediseñar la red o reconfigurar los dispositivos de red alrededor. El cable virtual admite el bloqueo o el permiso de tráfico en función de etiquetas de la LAN virtual (VLAN), además de admitir reglas de la política de seguridad, App-ID, Content-ID, User-ID, cifrado, LLDP, HA activa/pasiva y activa/activa, QoS, protección de zona (con algunas excepciones), protección de protocolo no IP, protección contra DoS, protección del búfer de paquetes, inspección del contenido del túnel y NAT.

© 2020 Palo Alto Networks, Inc.



Cada interfaz de cable virtual está conectada directamente a un dispositivo o host de red de capa 2 o capa 3. Las interfaces de cable virtual no tienen direcciones de capa 2 o capa 3. Cuando una de las interfaces de cable virtual recibe una trama o paquete, ignora cualquier dirección de capa 2 o de capa 3 con fines de conmutación o enrutamiento, pero se aplica a sus reglas de la política de seguridad o de NAT antes de pasar una trama o paquete permitida en el cable virtual a la segunda interfaz y hacia el dispositivo de red conectado a ella.

No debe utilizar una implementación de cable virtual para las interfaces que deben admitir conmutación, túneles VPN o enrutamiento debido a que requieren una dirección de capa 2 o capa 3. Una interfaz de cable virtual no utiliza un perfil de gestión de interfaces, que controla servicios como HTTP y ping, y, por lo tanto, requiere que la interfaz cuente con una dirección IP.

Todos los cortafuegos que se envían desde la fábrica cuentan con dos puertos Ethernet (puerto 1 y 2) preconfigurados como interfaces de cable virtual, y estas interfaces permiten todo el tráfico sin etiquetas.

Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Si el cortafuegos está en alguno de esos modos, puede inspeccionar el tráfico etiquetado y ofrecer prevención contra amenazas.

Si no desea utilizar el cable virtual preconfigurado, debe eliminar esta configuración para evitar que interfiera con otra configuración del cortafuegos. Consulte Establecimiento de acceso a la red para servicios externos*.*

- Paquetes de capa 2 y capa 3 en un cable virtual
- Velocidad de puertos en las interfaces de cable virtual
- LLDP en un cable virtual
- Interfaces agregadas para un cable virtual
- Compatibilidad del cable virtual con la alta disponibilidad
- Protección de zona para una interfaz de cable virtual
- Tráfico con etiqueta de VLAN

© 2020 Palo Alto Networks, Inc.

- Subinterfaces de Virtual Wire
- Configuración de cables virtuales

Paquetes de capa 2 y capa 3 en un cable virtual

Una interfaz de cable virtual permitirá que los paquetes de capa 2 y capa 3 procedentes de dispositivos conectados pasen de manera transparente siempre que las políticas que se aplican a la zona o a la interfaz permitan el tráfico. Las interfaces de cable virtual no participan en el enrutamiento o la conmutación.

Por ejemplo, el cortafuegos no reduce el TTL en un paquete de traceroute hacia el enlace virtual debido a que el enlace es transparente y no cuenta como un salto. Los paquetes como las unidades de datos de protocolo (PDU) de operaciones, administración y mantenimiento (OAM), por ejemplo, no finalizan en el cortafuegos. Por lo tanto, el cable virtual permite que el cortafuegos mantenga una presencia transparente actuando como un enlace de paso, mientras que proporciona servicios de seguridad, NAT y QoS.

Con el fin de que las unidades de datos para protocolo puente (BPDU) y otros paquetes de control de capa 2 (que, por lo general, no se etiquetan) pasen por un cable virtual, las interfaces deben adjuntarse a un objeto de cable virtual que permita el tráfico no etiquetado. Esta es la configuración predeterminada. Si el campo **Tag Allowed (Etiqueta permitida)** del objeto de cable virtual está vacío, el cable virtual permite tráfico no etiquetado. (Las reglas de la política de seguridad no se aplican a los paquetes de capa 2).

Para que los paquetes de control (de capa 3) de enrutamiento pasen por un cable virtual, debe aplicar una regla de la política de seguridad que permita el paso de tráfico. Por ejemplo, aplique una regla de la política de seguridad que permita una aplicación como BGP o OSPF.

Si desea poder aplicar reglas de la política de seguridad a una zona para el tráfico IPv6 que llega a una interfaz de cable virtual en el cortafuegos, habilite el cortafuegos IPv6. De lo contrario, el tráfico IPv6 se reenviará de manera transparente por el cable.

Si habilita el cortafuegos de multidifusión para un objeto de cable virtual y lo aplica a una interfaz de cable virtual, el cortafuegos inspecciona el tráfico multidifusión y lo reenvía o no, en función de las reglas de la política de seguridad. Si no habilita el cortafuegos de multidifusión, el cortafuegos reenviará el tráfico de multidifusión de manera transparente.

La fragmentación en un cable virtual se produce de igual manera que en otros modos de implementación de la interfaz.

Velocidad de puertos en las interfaces de cable virtual

Los diferentes modelos de cortafuegos proporcionan varios puertos de cobre y de fibra óptica, que funcionan a diferente velocidad. Un cable virtual puede unir dos puertos Ethernet del mismo tipo (ambos de cobre o ambos de fibra óptica) o unir un puerto de cobre con un puerto de fibra óptica. De manera predeterminada, la **Link Speed (Velocidad del enlace)** de los puertos de cobre en el cortafuegos se establece en **auto (automático)**, lo que significa que el cortafuegos negocia automáticamente su velocidad y modo de transmisión (**Link Duplex [Dúplex de enlace]**). Cuando realiza la Configuración de cables virtuales, también puede seleccionar una **Link Speed (Velocidad del enlace)** y un **Link Duplex (Dúplex de enlace)** específicos, pero los valores de estos ajustes deben ser iguales en ambos puertos de cualquier cable virtual.

LLDP en un cable virtual

Las interfaces de cable virtual pueden utilizar LLDP para encontrar dispositivos vecinos y sus capacidades, y el LLDP permite a los dispositivos vecinos detectar la presencia del cortafuegos en la red. LLDP facilita la resolución de problemas, especialmente en el caso de implementaciones de cable virtual donde el cortafuegos suele pasar desapercibido debido a un ping o traceroute que pasa por un cable virtual. LLDP proporciona un método para que los dispositivos detecten el cortafuegos en la red. Sin el LLDP, es prácticamente imposible que los sistemas de gestión de redes detecten la presencia de un cortafuegos mediante el enlace virtual.

© 2020 Palo Alto Networks, Inc.

Interfaces agregadas para un cable virtual

Puede Configurar un grupo de interfaces agregadas de interfaces de cable virtual, pero los cables virtuales no utilizan el LACP. Si configura el LACP en dispositivos que se conectan el cortafuegos a otras redes, el cable virtual pasará paquetes del LACP de manera transparente sin realizar las funciones del LACP.



Para que los grupos de interfaces agregados funcionen correctamente, asegúrese de que todos los enlaces del mismo grupo de LACP en el mismo lado del cable virtual se asignen a la misma zona.

Compatibilidad del cable virtual con la alta disponibilidad

Si configura el cortafuegos para realizar la supervisión de rutas para la alta disponibilidad utilizando un grupo de rutas de cable virtual, el cortafuegos intenta resolver el ARP de la dirección IP de destino configurada enviando paquetes de ARP de ambas interfaces de cable virtual. La dirección IP de destino que supervisa debe permanecer en la misma subred que uno de los dispositivos alrededor del cable virtual.

Las interfaces de cable virtual admiten HA activa/pasiva y activa/activa. En implementaciones de HA activa/activa con un cable virtual, los paquetes examinados deben devolverse al cortafuegos de destino para conservar la ruta de reenvío. Por lo tanto, si un cortafuegos recibe un paquete que pertenece a la sesión que el cortafuegos de HA del peer posee, lo devuelve mediante el enlace HA3 al peer.

En PAN-OS 7.1 y versiones posteriores, puede configurar el cortafuegos pasivo en un par de HA para permitir que los dispositivos del peer en ambos lados del cortafuegos negocien previamente los paquetes LLDP y LACP mediante un cable virtual antes de que se produzca una conmutación de error de HA. Una configuración que garantice la Negociación previa de LACP y LLDP para HA activa/pasiva acelera las conmutaciones por error de HA.

Protección de zona para una interfaz de cable virtual

Puede aplicar una protección de zona a una interfaz de cable virtual pero, dado que las interfaces de cable virtual no realizan el enrutamiento, no puede aplicar protección de ataques basados en paquetes a los paquetes provenientes de una dirección IP falsa, ni suprimir los paquetes de error vencidos de TTL ICMP o los paquetes que requieren fragmentación de ICMP.

De manera predeterminada, una interfaz de cable virtual reenvía todo el tráfico no IP que recibe. Sin embargo, puede aplicar un perfil de protección de zona con protección de protocolos para bloquear o permitir determinados paquetes de protocolo no IP entre las zonas de seguridad en un cable virtual.

Tráfico con etiqueta de VLAN

Las interfaces de cable virtual predeterminadas permiten todo el tráfico sin etiquetas. No obstante, puede utilizar un cable virtual para conectar dos interfaces y configurarlas para que bloqueen o permitan el tráfico basándose en las etiquetas de LAN virtual (VLAN). La etiqueta VLAN 0 indica el tráfico sin etiquetar.

También puede crear varias subinterfaces, añadirlas a diferentes zonas y, a continuación, clasificar el tráfico de acuerdo con una etiqueta VLAN, o una combinación de una etiqueta VLAN con clasificadores IP (dirección, intervalo o subred) para aplicar un control detallado de las políticas para etiquetas VLAN específicas o para etiquetas VLAN de una dirección IP de origen, intervalo o subred en concreto.

Subinterfaces de Virtual Wire

Las implementaciones de cable virtual pueden usar subinterfaces de cable virtual para separar el tráfico en zonas. Las subinterfaces de Virtual Wire ofrecen flexibilidad a la hora de aplicar distintas políticas cuando necesita gestionar el tráfico de varias redes de clientes. Las subinterfaces le permiten separar y clasificar el tráfico en diferentes zonas (las zonas pueden pertenecer a sistemas virtuales separados, si es necesario) utilizando los siguientes criterios:

© 2020 Palo Alto Networks, Inc.

- **Etiquetas de la VLAN**: el ejemplo de Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN) muestra un ISP que utiliza subinterfaces de Virtual Wire con etiquetas VLAN para separar el tráfico para dos clientes diferentes.
- **Etiquetas VLAN junto con clasificadores IP (dirección, intervalo o subred)**: el siguiente ejemplo muestra un ISP con dos sistemas virtuales separados en un cortafuegos que gestiona el tráfico de dos clientes diferentes. En cada sistema virtual, el ejemplo ilustra cómo se utilizan las subinterfaces de Virtual Wire con etiquetas VLAN y clasificadores IP para clasificar el tráfico en zonas separadas y aplicar la política relevante para los clientes de cada red.

Flujo de trabajo de subinterfaces de Virtual Wire

- Configure dos interfaces Ethernet con el tipo Virtual Wire y asigne estas interfaces a un Virtual Wire.

- Cree subinterfaces en el Virtual Wire principal para separar el tráfico del cliente A del cliente B. Asegúrese de que las etiquetas VLAN definidas en cada par de subinterfaces configuradas como Virtual Wire sean idénticas. Esto es esencial, porque un Virtual Wire no conmuta etiquetas VLAN.

- Cree nuevas subinterfaces y defina clasificadores IP. Esta tarea es opcional y solamente es necesaria si desea añadir subinterfaces adicionales con clasificadores IP para gestionar de manera más exhaustiva el tráfico de un cliente basándose en la combinación de etiquetas VLAN y una dirección IP de origen, intervalo o subred en concreto.

También puede utilizar clasificadores IP para gestionar el tráfico sin etiquetar. Para ello, debe crear una subinterfaz con la etiqueta VLAN “0” y definir subinterfaces con clasificadores IP para gestionar el tráfico sin etiquetar mediante clasificadores IP.

La clasificación de IP solamente puede utilizarse en las subinterfaces asociadas con un lado del Virtual Wire. Las subinterfaces definidas en el lado correspondiente del Virtual Wire deben utilizar la misma etiqueta VLAN, pero no deben incluir un clasificador IP.

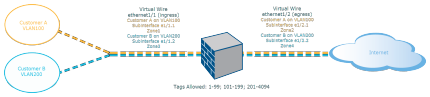


Figure 10: Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN)

Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN) muestra al cliente A y al cliente B conectados al cortafuegos mediante una interfaz física, Ethernet 1/1, configurada como Virtual Wire, que es la interfaz de entrada. Una segunda interfaz física, Ethernet1/2, también forma parte del Virtual Wire y se utiliza como la interfaz de salida que proporciona acceso a internet.

Para el cliente A, también tiene las subinterfaces Ethernet 1/1.1 (entrada) y Ethernet 1/2.1 (salida). Para el cliente B, tiene las subinterfaces Ethernet 1/1.2 (entrada) y Ethernet 1/2.2 (salida). Cuando configure las subinterfaces, debe asignar la etiqueta VLAN y la zona correctas para aplicar las políticas a cada uno de los clientes. En este ejemplo, las políticas del cliente A se crean entre la zona 1 y la zona 2, y las políticas del cliente B se crean entre la zona 3 y la zona 4.

Cuando el tráfico entre en el cortafuegos desde el cliente A o el cliente B, la etiqueta VLAN del paquete entrante primero deberá coincidir con la etiqueta VLAN definida en las subinterfaces de entrada. En este ejemplo, solo una subinterfaz coincide con la etiqueta VLAN en el paquete entrante, por lo que se seleccionará esa subinterfaz. Las políticas definidas para la zona se evalúan y aplican antes de que el paquete salga de la subinterfaz correspondiente.

No debe definirse la misma etiqueta VLAN en la interfaz del Virtual Wire principal y la subinterfaz. Verifique que las etiquetas VLAN definidas en la lista Tag Allowed (Etiquetas

© 2020 Palo Alto Networks, Inc.

permitidas) de la interfaz de Virtual Wire principal (Network [Red] > Virtual Wires [Cables virtuales]) no se incluyan en una subinterfaz.

Implementación de Virtual Wire con subinterfaces (etiquetas VLAN y clasificadores IP) muestra al cliente A y al cliente B conectados a un cortafuegos físico que tiene dos sistemas virtuales (vsys), además del sistema virtual predeterminado (vsys1). Cada sistema virtual es un cortafuegos virtual independiente que se gestiona por separado para cada cliente. Cada vsys tiene adjuntadas interfaces/subinterfaces y zonas de seguridad que se gestionan de manera independiente.

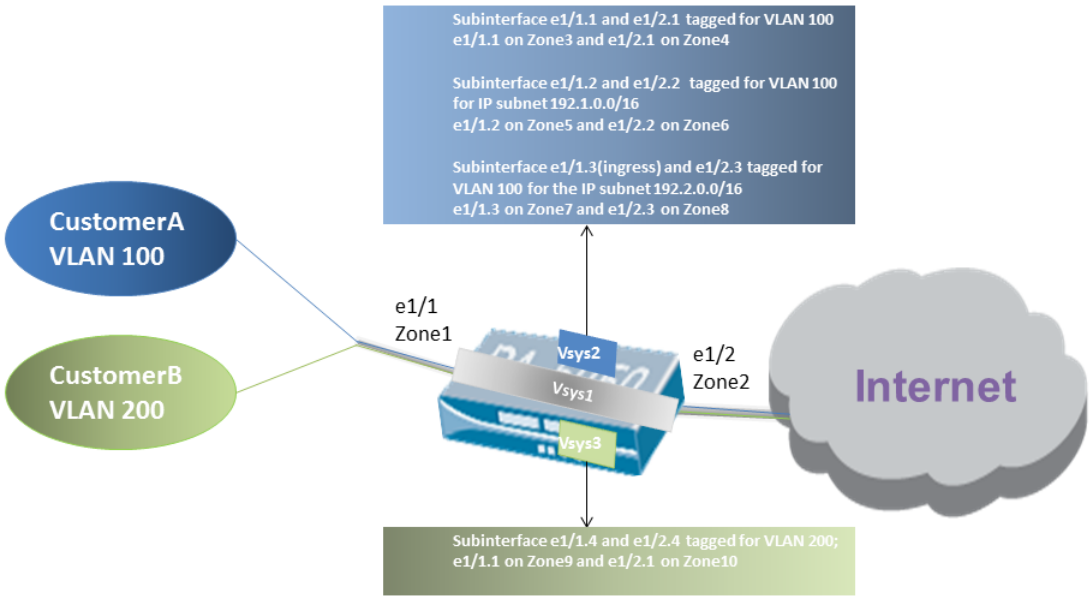


Figure 11: Implementación de Virtual Wire con subinterfaces (etiquetas VLAN y clasificadores IP)

Vsys1 está configurado para utilizar las interfaces físicas Ethernet 1/1 y Ethernet 1/2 como Virtual Wire; Ethernet 1/1 es la interfaz de entrada y Ethernet 1/2 es la interfaz de salida que proporciona el acceso a Internet. Este Virtual Wire está configurado para aceptar todo el tráfico etiquetado y sin etiquetar a excepción de las etiquetas VLAN 100 y 200, que están asignadas a las subinterfaces.

El cliente A se gestiona en vsys2 y el cliente B se gestiona en vsys3. En vsys2 y vsys3, se crean las siguientes subinterfaces de Virtual Wire con las etiquetas VLAN y las zonas adecuadas para aplicar las medidas incluidas en las políticas.

Cliente	Vsys	Subinterfaces de Vwire	Zona	Etiqueta VLAN	Clasificador IP
A	2	e1/1.1 (entrada) e1/2.1 (salida)	Zone3 Zone4	100 100	ninguno
	2	e1/1.2 (entrada)	Zone5	100	Subred IP

© 2020 Palo Alto Networks, Inc.

Cliente	Vsys	Subinterfaces de Vwire	Zona	Etiqueta VLAN	Clasificador IP
		e1/2.2 (salida)	Zone6	100	192.1.0.0/16
	2	e1/1.3 (entrada) e1/2.3 (salida)	Zone7 Zone8	100 100	Subred IP 192.2.0.0/16
B	3	e1/1.4 (entrada) e1/2.4 (salida)	Zone9 Zone10	200 200	ninguno

Cuando el tráfico entre en el cortafuegos desde el cliente A o el cliente B, la etiqueta VLAN del paquete entrante primero deberá coincidir con la etiqueta VLAN definida en las subinterfaces de entrada. En este caso, para el cliente A, hay varias subinterfaces que utilizan la misma etiqueta VLAN. De este modo, el cortafuegos primero acota la clasificación a una subinterfaz basándose en la dirección IP de origen del paquete. Las políticas definidas para la zona se evalúan y aplican antes de que el paquete salga de la subinterfaz correspondiente.

Para el tráfico de ruta de retorno, el cortafuegos compara la dirección IP de destino del modo definido en el clasificador IP en la subinterfaz del cliente y selecciona el Virtual Wire adecuado para enrutar el tráfico a través de la subinterfaz precisa.

No debe definirse la misma etiqueta VLAN en la interfaz del Virtual Wire principal y la subinterfaz. Verifique que las etiquetas VLAN definidas en la lista Tag Allowed (Etiquetas permitidas) de la interfaz de Virtual Wire principal (Network [Red] > Virtual Wires [Cables virtuales]) no se incluyan en una subinterfaz.

Configuración de cables virtuales

La siguiente tarea muestra cómo configurar dos Interfaces de cable virtual (Ethernet 1/3 y Ethernet 1/4 en este ejemplo) para crear un cable virtual. Las dos interfaces deben tener la misma **Link Speed (Velocidad de enlace)** y el mismo modo de transmisión (**Link Duplex [Dúplex de enlace]**). Por ejemplo, un puerto de cobre de 1000 Mbps de dúplex completo se corresponde con un puerto de fibra óptica de 1 Gbps de dúplex completo.

STEP 1 | Cree la primera interfaz de cable virtual.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz que haya conectado por cable (**ethernet1/3** en este ejemplo).
2. Establezca el **Interface Type (Tipo de interfaz)** en **Virtual Wire (Cable virtual)**.

STEP 2 | Conecte la interfaz a un objeto de cable virtual.

1. En la misma interfaz de Ethernet, seleccione **Virtual Wire (Cable virtual)** en la pestaña **Config (Configuración)** y haga clic en **New Virtual Wire (Nuevo cable virtual)**.
2. Introduzca un **Name (Nombre)** para el cable virtual.
3. Para **Interface1**, seleccione la interfaz que acaba de configurar (**ethernet1/3**). En la lista solo aparecen las interfaces configuradas como interfaces de cable virtual.
4. Para **Tag Allowed (Etiqueta permitida)**, introduzca **0** para indicar que el tráfico sin etiquetar (como BPDU y otro tráfico de control de capa 2) está permitido. La ausencia de una etiqueta implica una etiqueta de 0. Ingrese números enteros de etiquetas permitidas adicionales o intervalos de etiquetas, separados por coma (el valor predeterminado es 0; el intervalo es de 0 a 4094).
5. Seleccione **Multicast Firewalling (Cortafuegos de multidifusión)** si desea poder aplicar reglas de política de seguridad al tráfico de multidifusión que atraviesa el cable virtual. De lo contrario, el tráfico de multidifusión se envía de manera transparente por el cable virtual.

© 2020 Palo Alto Networks, Inc.

6. Seleccione **Link State Pass Through (Paso del estado del enlace)**, para que el cortafuegos pueda funcionar de manera transparente. Cuando el cortafuegos detecta un estado inactivo para un enlace de cable virtual, desactiva la otra interfaz en el par de cable virtual. Por lo tanto, los dispositivos en ambos lados del cortafuegos ven un estado de enlace constante, como si no hubiera un cortafuegos entre ellos. Si no selecciona esta opción, el estado del enlace no se propaga por el cable virtual.
7. Haga clic en **OK (Aceptar)** para guardar el objeto de cable.

STEP 3 | Determine la velocidad del enlace de la interfaz de cable virtual.

1. Mientras esté en la misma interfaz Ethernet, seleccione **Advanced (Avanzado)** y registre o cambie la **Link Speed (Velocidad de enlace)**. El tipo de puerto condiciona los ajustes de velocidad disponibles en la lista. De manera predeterminada, los puertos de cobre se configuran en **auto (automático)** para negociar la velocidad del enlace. Ambas interfaces de cable virtual deben tener la misma velocidad de enlace.
2. Haga clic en **OK (Aceptar)** para guardar la interfaz de Ethernet.

STEP 4 | Configure la segunda interfaz de cable virtual (**ethernet1/4** en este ejemplo) repitiendo los pasos anteriores.

Cuando selecciona el objeto de **Virtual Wire (Cable virtual)** que creó, el cortafuegos añade automáticamente la segunda interfaz de cable virtual como **Interface2**.

STEP 5 | Cree una zona de seguridad diferente para cada una de las interfaces de cable virtual.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una zona.
2. Introduzca un nombre para la zona en **Name (Nombre)**, (como `internet`).
3. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
4. Para **Type (Tipo)**, seleccione **Virtual Wire (Cable virtual)**.
5. Haga clic en **Add (Añadir)** para añadir la **Interface (Interfaz)** que pertenezca a la zona.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | (Opcional) Cree reglas de política de seguridad para permitir el paso del tráfico de capa 3.

Para permitir el tráfico de capa 3 en el cable virtual, Creación de una regla de política de seguridad para permitir el tráfico desde la zona de usuario a la zona de Internet, y otra para permitir el tráfico desde la zona de Internet a la zona de usuario, al seleccionar las aplicaciones que desea permitir, tal como BGP u OSPF.

STEP 7 | (Opcional) Habilite los cortafuegos IPv6.

Si desea poder aplicar reglas de política de seguridad al tráfico IPv6 que llega a la interfaz de cable virtual, habilite los cortafuegos IPv6. De lo contrario, el tráfico IPv6 se enviará de manera transparente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 8 | **Commit (Confirmar)** los cambios.

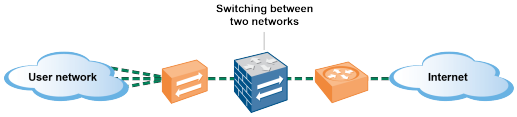
STEP 9 | (Opcional) Configure un perfil LLDP y aplíquelo a las interfaces de cable virtual (consulte Configuración de LLDP).

STEP 10 | (Opcional) Aplique el control de protocolo no IP a las zonas de cable virtual (consulte Configuración de la protección de protocolos). De lo contrario, todo el tráfico no IP se reenviará por el cable virtual.

© 2020 Palo Alto Networks, Inc.

Interfaces de capa 2

En una implementación de capa 2, el cortafuegos permite cambiar entre dos o más redes. Los dispositivos se conectan a una trama de capa 2; el cortafuegos reenvía las tramas al puerto adecuado, que se asocia a la dirección MAC que se identifica en la trama. Realice la Configuración de una interfaz de capa 2 cuando se requiera la conmutación.



Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Si el cortafuegos está en alguno de esos modos, puede inspeccionar el tráfico etiquetado y ofrecer prevención contra amenazas.

Los siguientes temas describen los diferentes tipos de interfaces de capa 2 que puede configurar para cada tipo de implementación que necesita, lo que incluye los detalles sobre la utilización de LAN virtuales (VLAN) para la separación del tráfico y la política en los grupos. En otro tema se describe cómo el cortafuegos reescribe el número de ID de VLAN del puerto entrante en un árbol de conmutación por VLAN (PVST+) de Cisco o una unidad de datos para protocolo puente (BPDU) de PVST+ rápido.

- Interfaces de capa 2 sin LAN
- Interfaces de capa 2 con LAN
- Configure la interfaz de capa 2
- Configuración de una interfaz de capa 2, una subinterfaz y una VLAN
- Gestión de la reescritura de BPDU del árbol de conmutación por VLAN (Per-VLAN Spanning Tree, PVST+)

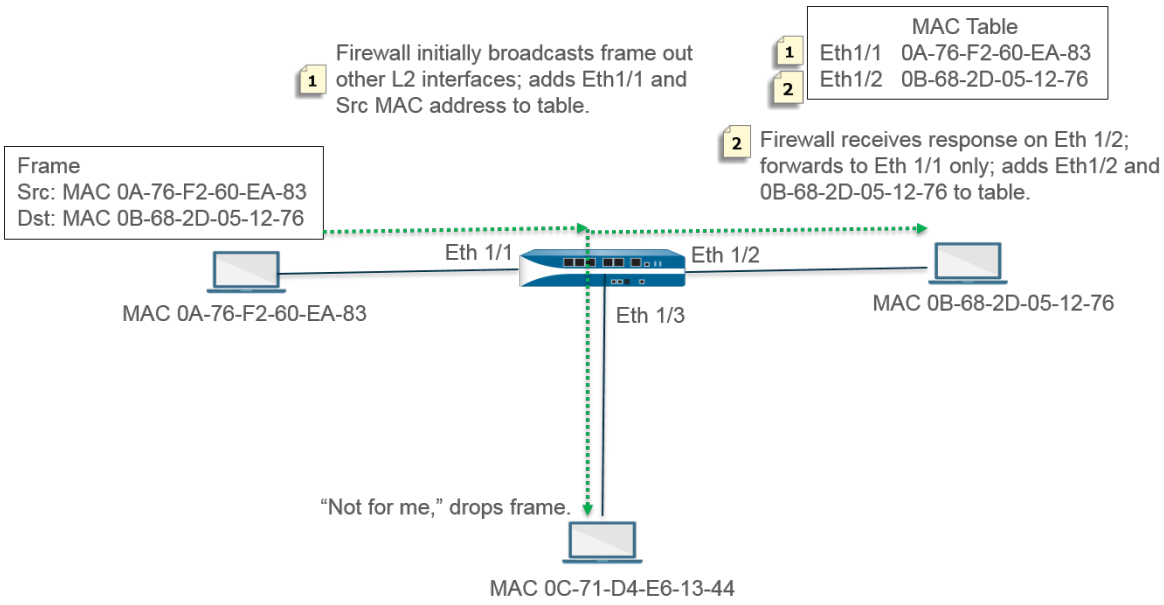
Interfaces de capa 2 sin LAN

Realice la Configuración de una interfaz de capa 2 en el cortafuegos, de modo que pueda actuar como un conmutador en su red de capa 2 (no en el borde de la red). Probablemente, los hosts de capa 2 se encuentran cercanos geográficamente y pertenecen a un dominio de difusión único. El cortafuegos proporciona seguridad entre los hosts de capa 2 cuando asigna las interfaces a las zonas de seguridad y aplica las reglas de seguridad a las zonas.

Los hosts se comunican con el cortafuegos y entre sí en la capa 2 del modelo OSI intercambiando tramas. Una trama contiene un encabezado Ethernet que incluye una dirección de control de acceso a los medios (MAC), que es una dirección de hardware físico. Las direcciones MAC son números hexadecimales de 48 bits con formato de seis octetos separados por dos puntos o guiones (por ejemplo, 00-85-7E-46-F1-B2).

La siguiente figura tiene un cortafuegos con interfaces de capa 2 que se conectan a un host de capa 2 en una asignación de uno a uno.

© 2020 Palo Alto Networks, Inc.



El cortafuegos comienza con una tabla MAC vacía. Cuando el host con dirección de origen 0A-76-F2-60-EA-83 envía una trama al cortafuegos, el cortafuegos no cuenta con una dirección de destino 0B-68-2D-05-12-76 en su tabla MAC, de modo que no sabe a qué interfaz reenviar la trama y difunde la trama a todas sus interfaces de capa 2. El cortafuegos introduce la dirección de origen 0A-76-F2-60-EA-83 y la dirección Eth1/1 asociada en su tabla MAC.

El host en 0C-71-D4-E6-13-44 recibe la difusión, pero la dirección MAC de destino no es su propia dirección MAC y, por lo tanto, descarta la trama.

La interfaz de destino Ethernet 1/2 reenvía la trama a su host. Cuando el host 0B-68-2D-05-12-76 responde, utiliza la dirección de destino 0A-76-F2-60-EA-83 y el cortafuegos añade Ethernet 1/2 como la interfaz en su tabla MAC para alcanzar la dirección 0B-68-2D-05-12-76.

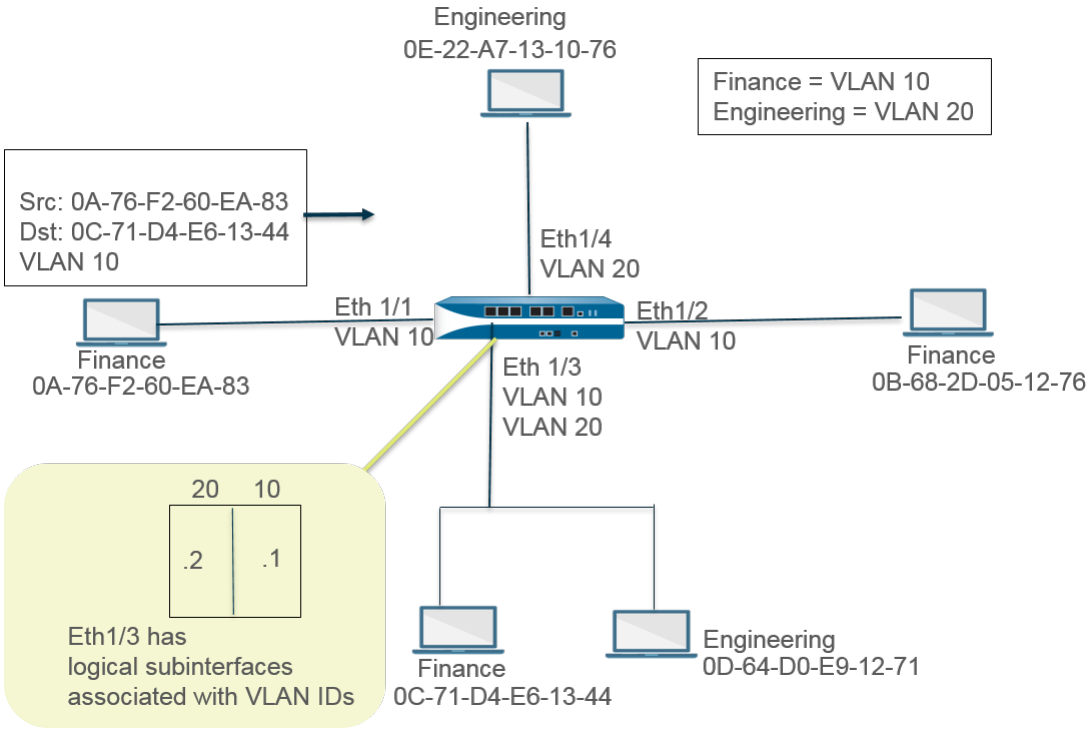
Interfaces de capa 2 con LAN

Cuando su organización desea dividir una LAN en LAN virtuales (VLAN) separadas para que el tráfico y las políticas de los diferentes departamentos permanezcan separados, puede agrupar los hosts de capa 2 en VLAN y, por lo tanto, dividir un segmento de red de capa 2 en dominios de difusión. Por ejemplo, puede crear VLAN para los departamentos de finanzas e ingeniería. Para ello, realice la Configuración de una interfaz de capa 2, una subinterfaz y una VLAN.

El cortafuegos actúa como conmutador para reenviar una trama con un encabezado Ethernet que contiene una ID de VLAN, y la interfaz de destino debe tener una subinterfaz con la ID de VLAN con el fin de recibir la trama y reenviarla al host. Puede configurar una interfaz de capa 2 en el cortafuegos y configurar una o más subinterfaces lógicas para el interfaz, cada una con una etiqueta (ID) de VLAN.

En la siguiente figura, el cortafuegos tiene cuatro interfaces de capa 2 que se conectan a hosts de capa 2 pertenecientes a diferentes departamentos dentro de una organización. La interfaz Ethernet 1/3 se configura con subinterfaz .1 (etiquetada con VLAN 10) y subinterfaz .2 (etiquetada con VLAN 20); por lo tanto, existen dos dominios de difusión en ese segmento. Los hosts en VLAN 10 pertenecen al departamento de finanzas; los hosts en VLAN 20 pertenecen al departamento de ingeniería.

© 2020 Palo Alto Networks, Inc.



En este ejemplo, el host en la dirección MAC 0A-76-F2-60-EA-83 envía una trama con VLAN ID 10 al cortafuegos y el cortafuegos lo difunde a sus otras interfaces de capa 2. La interfaz Ethernet 1/3 acepta la trama debido a que está conectada al host con la dirección de destino 0C-71-D4-E6-13-44 y se asigna la VLAN 10 a su subinterfaz .1. La interfaz Ethernet 1/3 reenvía la trama a su host de finanzas.

Configure la interfaz de capa 2

Configure las interfaces de capa 2 sin VLAN cuando desee una conmutación de capa 2 y no necesite un tráfico independiente en las VLAN.

STEP 1 | Configure la interfaz de capa 2.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz. El **Interface Name (Nombre de la interfaz)** es fijo, como ethernet1/1.
2. En **NAT Type (Tipo de NAT)**, seleccione **Layer2**.
3. Seleccione la pestaña **Config (Configuración)** y asigne la interfaz a una **Security Zone (Zona de seguridad)** o cree una **New Zone (Nueva zona)**.
4. Configure interfaces de capa 2 adicionales en el cortafuegos que se conecten a otros hosts de capa 2.

STEP 2 | Seleccione Confirmar.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de una interfaz de capa 2, una subinterfaz y una VLAN

Configure interfaces de capa 2 con VLAN cuando desee una conmutación de capa 2 y un tráfico independiente en las VLAN. De manera opcional, puede controlar protocolos no IP entre zonas de seguridad en una interfaz de capa 2 o entre interfaces dentro de una misma zona en una VLAN de capa 2.

STEP 1 | Configure una interfaz de capa 2 y una subinterfaz, y asigne una ID de VLAN.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz. El **Interface Name (Nombre de la interfaz)** es fijo, como ethernet1/1.

© 2020 Palo Alto Networks, Inc.

2. En **NAT Type (Tipo de NAT)**, seleccione **Layer2**.
3. Seleccione la pestaña **Config (Configuración)**.
4. En **VLAN**, conserve la configuración **None (Ninguno)**.
5. Asigne la interfaz a una **Security Zone (Zona de seguridad)** o cree una **New Zone (Nueva zona)**.
6. Haga clic en **OK (Aceptar)**.
7. Cuando la interfaz Ethernet esté resaltada, haga clic en **Add Subinterface (Añadir subinterfaz)**.
8. El campo **Interface Name (Nombre de interfaz)** permanece fijo. Tras el punto, introduzca el número de subinterfaz en el rango de 1 a 9999.
9. Introduzca una ID con una **Tag (Etiqueta)** de VLAN en el rango de 1 a 4094.
10. Asigne la interfaz a una **Security Zone (Zona de seguridad)**.
11. Haga clic en **OK (Aceptar)**.

STEP 2 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

STEP 3 | (Opcional) Aplique un perfil de protección de zona con protección de protocolo para controlar paquetes de protocolo no IP entre zonas de capa 2 (o entre interfaces dentro de una zona de capa 2).

Configure la protección de protocolo.

Gestión de la reescritura de BPDU del árbol de conmutación por VLAN (Per-VLAN Spanning Tree, PVST+)

Cuando una interfaz del cortafuegos está configurada para una implementación de capa 2, el cortafuegos reescribe el número de ID de VLAN del puerto entrante (PVID) en un árbol de conmutación por VLAN (PVST+) Cisco o una unidad de datos para protocolo puente (BPDU) de PVST+ rápido con el número de ID de VLAN entrante adecuado y reenvía BPDU. Este comportamiento predeterminado a partir de PAN-OS 7.1 permite que el cortafuegos etiquete correctamente las tramas de PVST+ y PVST+ rápido de Cisco entre los conmutadores de Cisco en las VLAN a cada lado del cortafuegos para que la detección de bucle de árbol de expansión que utiliza Cisco PVST+ y PVST+ rápido pueda funcionar correctamente. El cortafuegos no participa en el proceso de elección del protocolo de árbol de expansión (Spanning Tree Protocol, STP) y no hay ningún cambio de comportamiento para otros tipos de árbol de expansión.

El conmutador Cisco debe tener el loopguard deshabilitado para que PVST+ o la BPDU de PVST+ rápido reescriba la función correctamente en el cortafuegos.

Esta función solo es compatible con las interfaces Ethernet de capa 2 y de Ethernet de agregación (Aggregate Ethernet, AE). El cortafuegos admite un intervalo de PVID de 1 a 4094 con un ID de VLAN nativa de 1 para que sea compatible con la implementación de VLAN nativa de Cisco.

Para admitir la función de reescritura de BPDU de PVST+, PAN-OS admite el concepto de una VLAN nativa de PVST+. Las tramas enviadas a una VLAN nativa o enviadas desde ella no están etiquetadas con un PVID igual que la VLAN nativa. Todos los conmutadores y cortafuegos en la misma implementación de capa 2 deben tener la misma VLAN nativa para que PVST+ funcione correctamente. Aunque la VLAN nativa de Cisco se configura de forma predeterminada en vlan1, la ID de VLAN puede ser un número distinto de 1.

Por ejemplo, el cortafuegos está configurado con un objeto VLAN (denominado VLAN_BRIDGE), que describe las interfaces y subinterfaces que pertenecen a un conmutador o dominio de difusión. En este ejemplo, la VLAN incluye tres subinterfaces: ethernet1/21.100 con la etiqueta 100, ethernet1/22.1000 con la etiqueta 1000 y ethernet1/23.1500 con la etiqueta 1500.

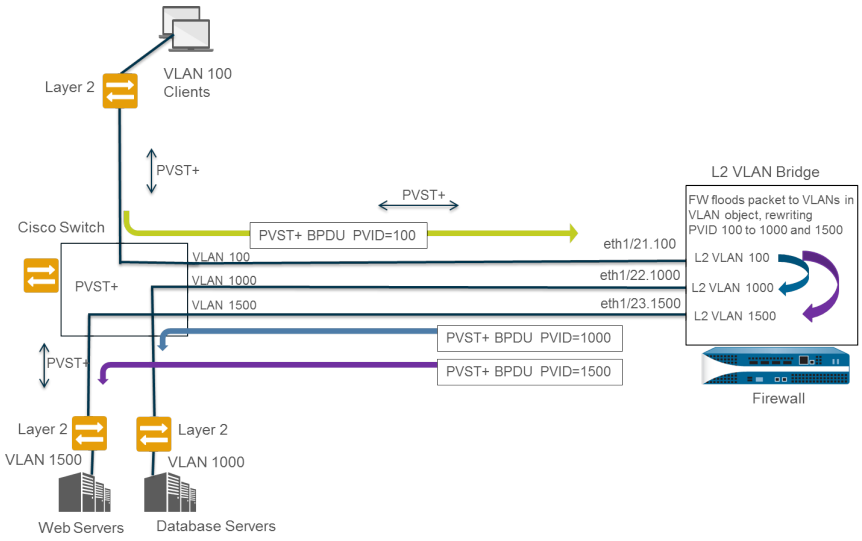
© 2020 Palo Alto Networks, Inc.

Las subinterfaces que pertenecen a VLAN_BRIDGE tienen el siguiente aspecto:

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

En el siguiente gráfico y explicación se muestra la secuencia en la que el cortafuegos reescribe automáticamente la BPDU de PVST+:



1. El puerto del conmutador de Cisco que pertenece a la VLAN 100 envía una BPDUP de PVST+, con el PVID y la etiqueta VLAN 802.1Q establecida en 100, al cortafuegos.
2. Las interfaces y subinterfaces de cortafuegos están configuradas como un tipo de interfaz de capa 2. La subinterfaz de entrada en el cortafuegos tiene la etiqueta VLAN 100, que coincide con la etiqueta PVID y VLAN de la BPDU entrante, por lo que el cortafuegos acepta la BPDU. El cortafuegos inunda la BPDU de PVST+ en todas las demás interfaces que pertenecen al mismo objeto VLAN (en este ejemplo, ethernet1/22.1000 y ethernet1/23.1500). Si las etiquetas VLAN no coinciden, el cortafuegos descartará la BPDU.
3. Cuando el cortafuegos inunda la BPDU a través de otras interfaces (que pertenecen al mismo objeto VLAN), reescribe el PVID y cualquier etiqueta VLAN 802.1Q para que coincida con la etiqueta VLAN de la interfaz de salida. En este ejemplo, el cortafuegos reescribe el PVID de la BPDU de 100 a 1000 para una subinterfaz y de 100 a 1500 para la segunda subinterfaz cuando la BPDU atraviesa el puente de capa 2 en el cortafuegos.
4. Cada conmutador Cisco recibe la etiqueta PVID y VLAN correcta en la BPDU entrante y procesa el paquete PVST+ para detectar posibles bucles en la red.

Los siguientes comandos operativos de la CLI le permiten gestionar BPDU de PVST+ y PVST+ rápido.

© 2020 Palo Alto Networks, Inc.

- Deshabilite o vuelva a habilitar globalmente la reescritura de la BPDU de PVST+ y PVST+ rápido del PVID (el valor predeterminado es habilitado).

  set session rewrite-pvst-pvid <yes|no>

- Establezca la ID de VLAN nativa para el cortafuegos (el intervalo es de 1 a 4094; el valor predeterminado es 1).

  Si la ID de VLAN nativa en su conmutador es un valor distinto de 1, debe establecer la ID de VLAN nativa del cortafuegos en ese mismo número; de lo contrario, el cortafuegos eliminará los paquetes con esa ID de VLAN. Esto se aplica a las interfaces troncalizadas y no troncalizadas.

  set session pvst-native-vlan-id <*vid*>

- Descarte todos los paquetes de BPDU STP.

  set session drop-stp-packet <yes|no>

  Ejemplos de por qué es posible que quiera descartar todos los paquetes de BPDU STP:

  - Si solo hay un conmutador a cada lado del cortafuegos y no hay otras conexiones entre los conmutadores que puedan causar un bucle, no es necesario STP y puede desactivarse en el conmutador o que el cortafuegos lo bloquee.
  - Si hay un interruptor STP con un comportamiento erróneo que inunda de manera inapropiada las BPDU, puede detener los paquetes STP en el cortafuegos para detener la inundación de BPDU.

- Compruebe si la reescritura de BPDU de PVST+ está habilitada, vea el ID de VLAN nativa de PVST y determine si el cortafuegos está descartando todos los paquetes de BPDU STP.

  show vlan all

  ```
  pvst+ tag rewrite: disabled
  pvst native vlan id:     5
  drop stp:                disabled
  total vlans shown:       1
  name     interface           virtual interface
  bridge   ethernet1/1
           ethernet1/2
           ethernet1/1.1
           ethernet1/2.1
  ```

- Solucione los errores de la BPDU de PVST+.

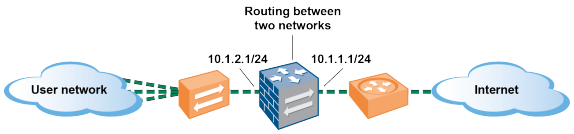
  show counter global

  Observe contador `flow_pvid_inconsistent`, que registra la cantidad de veces que no coinciden los campos de etiqueta 802.1Q y PVID dentro de un paquete de BPDU de PVST+.

© 2020 Palo Alto Networks, Inc.

Interfaces de capa 3

En una implementación de capa 3, el cortafuegos enruta el tráfico entre múltiples puertos. Antes de que pueda realizar la Configuración de interfaces de capa 3, debe configurar los enrutadores virtuales que desea que el cortafuegos utilice para enrutar el tráfico para cada interfaz de capa 3.



Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Ahora bien, si debe utilizar un cortafuegos de capa 3 en una red Cisco TrustSec, tiene que implementarlo entre dos peers del protocolo de intercambio de SGT (SXP, SGT Exchange Protocol) y configurarlo de modo que permita el tráfico entre ellos.

Los siguientes temas describen cómo configurar interfaces de capa 3, y cómo utilizar el protocolo de detección de vecinos (NDP) para suministrar hosts IPv6 y visualizar las direcciones IPv6 de los dispositivos en la red local del enlace para ubicar dispositivos con rapidez.

- Configuración de interfaces de capa 3
- Gestión de hosts IPv6 con NDP

Configuración de interfaces de capa 3

El siguiente procedimiento es necesario para configurar interfaces de capa 3 (Ethernet, VLAN, bucle invertido e interfaces de túnel) con direcciones IPv4 o IPv6, de manera que el cortafuegos pueda realizar el enrutamiento en estas interfaces. Si un túnel se utiliza para el enrutamiento o si la supervisión de túnel está activada, el túnel necesita una dirección IP. Antes de realizar la siguiente tarea, defina uno o más enrutadores virtuales.

Habitualmente usaría el siguiente procedimiento para configurar una interfaz externa que se conecte con Internet y una interfaz para su red interna. Puede configurar ambas direcciones tanto IPv4 como IPv6 en una misma interfaz.

Los modelos de cortafuegos PAN-OS admiten un máximo de 16.000 direcciones IP asignadas a interfaces de capa 3 físicas o virtuales; este máximo incluye direcciones IPv4 e IPv6.

Si está utilizando rutas IPv6, puede configurar el cortafuegos para que proporcione anuncios de enrutador IPv6 para la configuración DNS. El cortafuegos proporciona a los clientes DNS IPv6 direcciones de servidor DNS recursivas (RDNS) y una lista de búsqueda DNS para que el cliente pueda resolver sus solicitudes DNS IPv6. Por lo tanto, el cortafuegos actúa como un servidor DHCPv6 para usted.

STEP 1 | Seleccione una interfaz y configúrela con una zona de seguridad.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**, según el tipo de interfaz que desee.
2. Seleccione la interfaz que desea configurar.
3. Seleccione **Interface Type**—**Layer3 (Tipo de interfaz: capa 3)**.
4. En la pestaña **Config**, para **Virtual Router (Enrutador virtual)**, seleccione el enrutador virtual que está configurando, tal como **default (predeterminado)**.
5. Para **Virtual System (Sistema virtual)**, seleccione el sistema virtual que está configurando, en el caso de un cortafuegos de sistema virtual múltiple.

© 2020 Palo Alto Networks, Inc.

6. Para **Security Zone (Zona de seguridad)**, seleccione la zona a la cual pertenece la interfaz o cree una **New Zone (Zona nueva)**.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure la interfaz con una dirección IPv4.

Para asignar la dirección IPv4 a una interfaz de capa 3, dispone de tres opciones:

- Estático
- Cliente DHCP: la interfaz del cortafuegos funciona como un cliente DHCP y recibe una dirección IP asignada dinámicamente. El cortafuegos también permite propagar los ajustes recibidos mediante la interfaz del cliente DHCP a un servidor DHCP activo en el cortafuegos. Esta opción se suele utilizar para propagar los ajustes del servidor DNS desde un proveedor de servicios de Internet a las máquinas cliente de la red que están protegidas por el cortafuegos.
- PPPoE: configure la interfaz como un punto de finalización del protocolo punto a punto sobre Ethernet (Point-to-Point Protocol over Ethernet, PPPoE) con el fin de permitir la conectividad en un entorno de línea de suscripción digital (DSL) en el que existe un módem DSL, pero ningún otro dispositivo PPPoE que finalice la conexión.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**, según el tipo de interfaz que desee.
2. Seleccione la interfaz que desea configurar.
3. Para configurar la interfaz con una dirección IPv4 estática, en la pestaña **IPv4**, configure **Type (Tipo)** en **Static (Estático)**.
4. Seleccione **Add (Añadir)** para añadir un nombre en **Name** y opcionalmente una descripción de la dirección en **Description**.
5. Para **Type (Tipo)**, seleccione una de las siguientes opciones:
   - **IP Netmask (Máscara de red IP)**: introduzca la dirección IP y la máscara de red para asignarla a la interfaz; por ejemplo, 208.80.56.100/24.

     Si utiliza una máscara de subred /31 para la dirección de interfaz de capa 3, la interfaz debe configurarse con la dirección .1/31, de modo que las utilidades, como ping, funcionen correctamente.

     Si está configurando una interfaz de bucle invertido con una dirección IPv4, debe tener una máscara de subred /32; por ejemplo, 192.168.2.1/32.
   - **IP Range (Intervalo IP)**: introduzca un intervalo de dirección IP, tal como 192.168.2.1-192.168.2.4.
   - **FQDN**: introduzca un nombre de dominio completo.
6. Seleccione **Tags (Etiquetas)** para aplicarlas a la dirección.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure una interfaz con el protocolo punto a punto sobre Ethernet (PPPoE). Consulte Interfaces de capa 3.

PPPoE no es compatible en modo HA activo/activo.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv4**, configure el **Type (Tipo)** en **PPPoE**.
4. En la pestaña **General**, seleccione **Enable (Habilitar)** para activar la interfaz para la finalización de PPPoE.

© 2020 Palo Alto Networks, Inc.

5. Introduzca el **Username (Nombre de usuario)** de la conexión de punto a punto.
6. Introduzca la **Password (Contraseña)** para el nombre de usuario y seleccione **Confirm Password (Confirmar contraseña)**.
7. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure una interfaz como cliente DHCP para que reciba la dirección IPv4 asignada de forma dinámica.

El cliente DHCP no es compatible en modo HA activo/activo.

STEP 5 | Configure una interfaz con una dirección IPv6 estática.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** para permitir el direccionamiento de IPv6 en la interfaz.
4. Para **Interface ID (ID de interfaz)**, introduzca el identificador único ampliado de 64 bits (EUI-64) en formato hexadecimal (por ejemplo, 00:26:08:FF:FE:DE:4E:29). Si deja este campo en blanco, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física. Si activa la opción **Use interface ID as host portion (Usar la ID de interfaz como parte de host)** cuando se añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.
5. Seleccione **Add (Añadir)** para añadir la **Address (Dirección)** IPv6 o seleccione un grupo de direcciones.
6. Seleccione **Enable address on interface (Habilitar dirección en interfaz)** para habilitar la dirección IPv6 en la interfaz.
7. Seleccione **Use interface ID as host portion (Usar ID de interfaz como parte de host)** para utilizar el ID de interfaz como la parte de host de la dirección IPv6.
8. (Opcional) Seleccione **Anycast (Difusión por proximidad)** para que la dirección (ruta) IPv6 sea una dirección (ruta) de difusión por proximidad, lo que significa que varias ubicaciones pueden anunciar el mismo prefijo, e IPv6 envía el tráfico de difusión por proximidad al nodo que considera más cercano, según los costes del protocolo de enrutamiento y otros factores.
9. (Solo interfaz Ethernet) Seleccione **Send Router Advertisement (Enviar anuncio de enrutador,** RA) para habilitar el cortafuegos para que envíe esta dirección en anuncios de enrutador, en cuyo caso también debe habilitar la opción global **Enable Router Advertisement (Habilitar anuncio de enrutador)** en la interfaz (paso siguiente).
10. (Solo interfaz Ethernet) Introduzca la **Valid Lifetime (sec) (Duración válida [s])**, en segundos, por la que el cortafuegos considera la dirección como válida. La duración válida debe ser igual o superar la **Preferred Lifetime (sec) (Duración preferida [s])** (el valor predeterminado es 2 592 000).
11. (Solo interfaz Ethernet) Introduzca la **Preferred Lifetime (sec) (Duración preferida [s])** por la que se prefiere la dirección válida, lo que significa que el cortafuegos la puede utilizar para enviar y recibir tráfico. Cuando caduca la duración preferida, el cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que caduque la **Valid Lifetime (Duración válida)** (el valor predeterminado es 604 800).
12. (Solo interfaz Ethernet) Seleccione **On-link (Enlace activo)** si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador.
13. (Solo interfaz Ethernet) Seleccione **Autonomous (Autónomo)** si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
14. Haga clic en **OK (Aceptar)**.

STEP 6 | (Interfaz Ethernet o VLAN usando una dirección IPv6 únicamente) Habilite el cortafuegos para que envíe los anuncios de enrutador IPv6 (RA) desde una interfaz y, opcionalmente, para que ajuste los parámetros RA.

© 2020 Palo Alto Networks, Inc.

Ajuste los parámetros RA por cualquiera de estos motivos: Para interoperar con un enrutador/host que utilice diferentes valores. Para lograr una convergencia más rápida cuando haya varias puertas de enlace presentes. Por ejemplo, configure valores de Min Interval (Intervalo mínimo), Max Interval (Intervalo máximo) y Router Lifetime (Duración del enrutador) más bajos para que el cliente/host IPv6 pueda cambiar rápidamente la puerta de enlace predeterminada después de que haya fallado la puerta de enlace principal, e iniciar el envío a otra puerta de enlace predeterminada en la red.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que desee configurar.
3. Seleccione **IPv6**.
4. Seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
5. En la pestaña **Router Advertisement (Anuncio de enrutador)**, seleccione **Enable Router Advertisement (Habilitar anuncio de enrutador)** (por defecto está deshabilitado).
6. (Opcional) Especifique el **Min Interval (sec) (Intervalo mínimo [s])**; es decir, el intervalo mínimo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 3 a 1350; el valor predeterminado es 200). El cortafuegos envía los RA en intervalos aleatorios entre los valores mínimo y máximo que usted configure.
7. (Opcional) Especifique el **Max Interval (sec) (Intervalo máximo [s])**; es decir, el intervalo máximo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 4 a 1800; el valor predeterminado es 600). El cortafuegos envía los RA en intervalos aleatorios entre los valores mínimo y máximo que usted configure.
8. (Opcional) Configure el **Hop Limit (Límite de salto)** que se debe aplicar a los clientes en los paquetes salientes (el intervalo es de 1 a 255; el valor predeterminado es 64). Introduzca 0 si no desea ningún límite de salto.
9. (Opcional) Configure **Link MTU (Unidad de transmisión máxima de enlace)**, la unidad de transmisión máxima (maximum transmission unit, MTU) de enlace para aplicar a los clientes (el intervalo es de 1280 a 9192; el valor predeterminado es **unspecified [no especificado]**). Seleccione **unspecified (no especificado)** para que no haya un MTU de enlace.
10. (Opcional) Configure el **Reachable Time (ms) (Tiempo alcanzable [s])**; es decir, el tiempo alcanzable (en milisegundos) que el cliente utilizará para asumir que un vecino es alcanzable después de recibir un mensaje de confirmación de esta condición. Seleccione **unspecified (no especificado)** si no desea establecer ningún valor de tiempo alcanzable (el intervalo es de 0 a 3 600 000; el valor predeterminado es **unspecified [no especificado]**).
11. (Opcional) Configure el **Retrans Time (ms) (Tiempo de retransmisión [ms])**; el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente, en milisegundos, antes de retransmitir los mensajes de convocatoria de vecinos. Seleccione **unspecified (no especificado)** si no desea ningún tiempo de retransmisión (el intervalo es de 0 a 4 294 967 295; el valor predeterminado es **unspecified [no especificado]**).
12. (Opcional) Configure la **Router Lifetime (sec) (Duración de enrutador [s])** para especificar cuánto tiempo, en segundos, el cliente utilizará el cortafuegos como puerta de enlace predeterminada (el intervalo es de 0 a 9000; el valor predeterminado es 1800). Un valor cero especifica que el cortafuegos no es la puerta de enlace predeterminada. Cuando acaba la duración, el cliente elimina la entrada del cortafuegos de la lista de ruta predeterminada y utiliza otro enrutador como puerta de enlace predeterminada.
13. Configure la **Router Preference (Preferencia de enrutador)** que el cliente utiliza para seleccionar un enrutador preferido si el segmento de red tiene varios enrutadores IPv6. **High (Alta)**, **Medium (Intermedia)** (valor predeterminado) o **Low (Baja)** es la prioridad que el RA anuncia para indicar la prioridad relativa del enrutador virtual del cortafuegos en relación con otros enrutadores del segmento.
14. Seleccione **Managed Configuration (Configuración gestionada)** para indicar al cliente que las direcciones están disponibles a través de DHCPv6.

© 2020 Palo Alto Networks, Inc.

15. Seleccione **Other Configuration (Otra configuración)** para indicar al cliente que hay disponible otra información de dirección (por ejemplo, ajustes relacionados con DNS) a través de DHCPv6.
16. Seleccione **Consistency Check (Comprobación de consistencia)** si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos envía logs sobre cualquier incoherencia.
17. Haga clic en **OK (Aceptar)**.

STEP 7 | (Interfaz Ethernet o VLAN usando una dirección IPv6 únicamente) Especifique las direcciones del servidor DNS recursivo y la lista de búsqueda de DNS que el cortafuegos anunciará en los anuncios de enrutador ND desde esta interfaz.

Los servidores RDNS y la lista de búsqueda DNS son parte de la configuración DNS para el cliente DNS, de manera que el cliente pueda resolver las solicitudes DNS IPv6.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6** > **DNS Support (Soporte DNS)**.
4. Seleccione **Include DNS information in Router Advertisement (Incluir información DNS en el anuncio de enrutador)** para habilitar el cortafuegos para que envíe información DNS IPv6.
5. Para el **Server (Servidor)** DNS, seleccione **Add (Añadir)** para añadir la dirección IPv6 de un servidor DNS recursivo. Seleccione **Add (Añadir)** para añadir hasta ocho servidores DNS recursivos. El cortafuegos envía direcciones de servidor en un anuncio de enrutador ICMPv6 en orden descendente.
6. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el servidor RDNS específico para resolver nombres de dominio.
   - El intervalo de la **Lifetime (Duración)** es cualquier valor igual o entre el **Max Interval (Intervalo máximo)** (que configuró en la pestaña **Router Advertisement [Anuncio de enrutador]**) y dos veces ese **Max Interval (Intervalo máximo)**. Por ejemplo, si su intervalo máximo es de 600 segundos, el intervalo de duración es de 600 a 1200 segundos.
   - La **Lifetime (Duración)** predeterminada es de 1200 segundos.
7. Para el sufijo DNS, seleccione **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** (nombre de dominio de un máximo de 255 bytes). Seleccione **Add (Añadir)** para añadir hasta ocho sufijos DNS. El cortafuegos envía sufijos en un anuncio de enrutador ICMPv6 en orden descendente.
8. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el sufijo. La duración posee el mismo intervalo y valor predeterminado que el **servidor**.
9. Haga clic en **OK (Aceptar)**.

STEP 8 | (Ethernet o interfaz de VLAN) Especifique las entradas de ARP. Las entradas de ARP estáticas reducen el procesamiento de ARP.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **ARP Entries (Entradas de ARP)**.
4. Haga clic en **Add (Añadir)** para añadir una **IP Address (Dirección IP)** y la **MAC Address (Dirección MAC)** correspondiente (dirección de control de acceso a medios o hardware). Para una interfaz de VLAN, también debe seleccionar la **Interface (Interfaz)**.

   Las entradas de ARP estáticas no agotan su tiempo de espera. Las entradas de ARP que se obtienen automáticamente en caché se agotan en 1800 segundos de manera predeterminada; debe personalizar el tiempo de espera de caché del ARP; consulte Configuración de los tiempos de espera de sesión.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 9 | (Ethernet o interfaz de VLAN) Especifique las entradas estáticas del Protocolo de detección de vecinos (Neighbor Discovery Protocol, NDP). NDP para IPv6 realiza funciones similares a las que ofrece ARP para IPv4.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **ND Entries (Entradas del ND)**.
4. Haga clic en **Add (Agregar)** para agregar una **IPv6 Address (Dirección IPv6)** y la **MAC Address (Dirección MAC)** correspondiente.
5. Haga clic en **OK (Aceptar)**.

STEP 10 | (Opcional) Habilite los servicios en la interfaz.

1. Para habilitar los servicios en la interfaz, seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**.
4. Expanda la lista **Management Profile (Perfil de gestión)** y seleccione un perfil o **New Management Profile (Nuevo perfil de gestión)**.
5. Introduzca un **Name (Nombre)** para el perfil.
6. Para **Permitted Services (Servicios permitidos)**, seleccione servicios, tales como **Ping**, y haga clic en **OK (Aceptar)**.

STEP 11 | **Commit (Confirmar)** los cambios.

STEP 12 | Conecte el cable de Internet.

Conecte cables directos desde las interfaces que ha configurado al conmutador o enrutador correspondiente de cada segmento de red.

STEP 13 | Verifique que la interfaz esté activa.

Desde la interfaz web, seleccione **Network (Red)** > **Interfaces** y verifique que el icono de la columna Link State (Estado de enlace) esté de color verde. También puede supervisar el estado de enlace desde el widget **Interfaces** en el **Dashboard (Panel)**.

STEP 14 | Configure rutas estáticas o un protocolo de enrutamiento dinámico (RIP, OSPF o BGP), para que el enrutador virtual pueda enrutar el tráfico.

- Configuración de una ruta estática
- RIP
- OSPF
- BGP

STEP 15 | Configuración de una ruta predeterminada.

Configure una ruta estática y establézcala como predeterminada.

Gestión de hosts IPv6 con NDP

Este tema describe cómo puede utilizar NDP para suministrar hosts IPv6; por lo tanto, no necesita un servidor DHCPv6 separado para este fin. Esto también explica cómo utilizar el NDP para supervisar direcciones IPv6, lo que le permite rastrear con rapidez la dirección IPv6 y la dirección MAC de un dispositivo y el usuario asociado que ha violado una regla de seguridad.

- Anuncios de enrutador IPv6 para la configuración del DNS
- Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6

© 2020 Palo Alto Networks, Inc.

- Monitorización NDP
- Habilitar supervisión NDP

Anuncios de enrutador IPv6 para la configuración del DNS

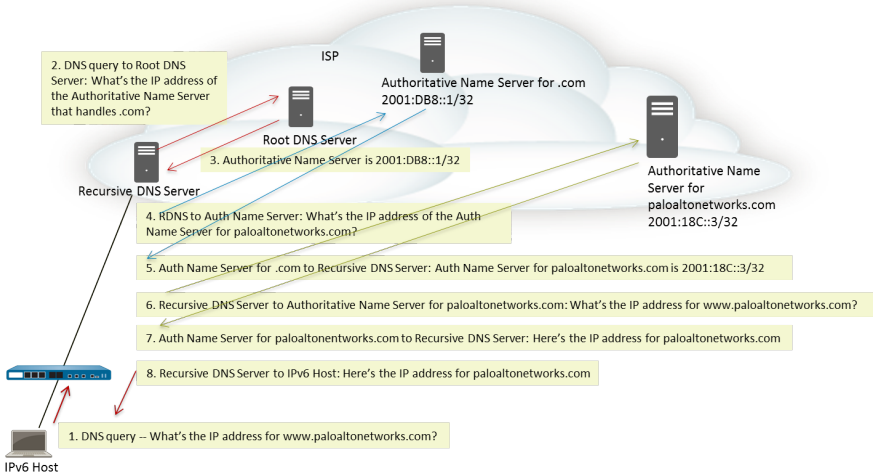
Se mejora la implementación del cortafuegos de la detección de vecinos (ND) de modo que pueda ofrecerle a los hosts IPv6 la opción de servidor DNS recursivo (RDNSS) y la opción de lista de búsqueda de DNS (DNSSL) según RFC 6106, Opciones de anuncios de enrutador IPv6 para la configuración del DNS. Cuando realiza la Configuración de interfaces de capa 3, configura estas opciones de DNS en el cortafuegos y el cortafuegos puede suministrar a los hosts IPv6; por lo tanto, no es necesario que un servidor DHCPv6 independiente para suministrar a los hosts. El cortafuegos envía anuncios de enrutador (RA) IPv6 con estas opciones a hosts IPv6 como parte de su configuración de DNS para suministrarlos completamente con el fin de alcanzar los servicios de internet. Por lo tanto, sus hosts IPv6 se configuran con las siguientes variables:

- Las direcciones de los servidores RDNS que pueden resolver consultas de DNS.
- Una lista de nombres de dominio (sufijos) que el cliente DNS agrega (una a la vez) a un nombre de dominio no calificado antes de introducir el nombre de dominio en una consulta DNS.

Los anuncios de enrutador IPv6 para la configuración del DNS son compatibles con los interfaces Ethernet, los subinterfaces, los interfaces Ethernet agregados y los interfaces VLAN de capa 3 en todas las plataformas PAN-OS.

La capacidad del cortafuegos de enviar RA IPv6 para la configuración del DNS le permite al cortafuegos realizar una función similar al DHCP y no se relaciona con el cortafuegos como proxy DNS, cliente DNS o servidor DNS.

Después de configurar el cortafuegos con las direcciones de los servidores RDNS, el cortafuegos suministra un host IPv6 (el cliente DNS) con esas direcciones. El host IPv6 utiliza una o más de estas direcciones para alcanzar un servidor RDNS. El DNS recursivo corresponde a una serie de solicitudes DNS de un servidor RDNS, como se muestra con tres pares de consultas y respuestas en la siguiente figura. Por ejemplo, cuando un usuario intenta acceder a www.paloaltonetworks.com, el explorador local detecta que esa dirección IP para ese nombre de dominio no se encuentra en su almacenamiento en caché ni en el sistema operativo del cliente. El sistema operativo del cliente inicia una consulta DNS para un servidor DNS recursivo perteneciente al ISP local.



Un anuncio de enrutador IPv6 puede incluir varias opciones de dirección de servidor DNS recursivo y cada opción posee una duración similar o diferente. Una opción única de dirección de servidor DNS recursivo puede incluir varias direcciones de servidor DNS recursivo siempre que las direcciones compartan la misma duración.

© 2020 Palo Alto Networks, Inc.

Una lista de búsqueda de DNS es una lista de los nombres de dominio (sufijos) que el cortafuegos anuncia a un cliente DNS. Por lo tanto, el cortafuego suministra al cliente DNS para que utilice los sufijos en sus consultas de DNS no calificadas. El cliente DNS agrega los sufijos, uno a uno, a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, y utilizar, de ese modo, un nombre de dominio completo (FQDN) en la consulta DNS. Por ejemplo, si un usuario (del cliente DNS que se configura) intenta enviar una consulta DNS con el nombre "calidad" sin un sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda de DNS al nombre y transmite una consulta DNS. Si el primer sufijo DNS de la lista es "empresa.com", la consulta DNS resultante del enrutador se realizará con el FQDN "calidad.empresa.com".

Si la consulta DNS falla, el cliente agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El cliente utiliza los sufijos DNS en orden hasta que una búsqueda de DNS sea correcta (se omiten los sufijos restantes) o hasta que el enrutador haya intentado todos los sufijos de la lista.

Configure el cortafuegos con los sufijos que desea facilitar al enrutador de cliente DNS en una opción DNSSL de ND; el cliente DNS que recibe la lista de búsqueda de DNS utiliza los sufijos en sus consultas DNS no calificadas.

Para especificar los servidores RDNS y una lista de búsqueda de DNS, realice la Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6.

Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6

Realice esta tarea para llevar a cabo los Anuncios de enrutadores IPv6 para la configuración de DNS de hosts IPv6.

STEP 1 | Permita que el cortafuegos envíe anuncios de enrutadores IPv6 desde una interfaz.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
4. En la pestaña **Router Advertisement (Anuncios de enrutadores)**, seleccione **Enable Router Advertisement (Habilitar anuncios de enrutadores)**.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Especifique las direcciones del servidor DNS recursivo y la lista de búsqueda de DNS que el cortafuegos anunciará en los anuncios de enrutadores de ND de esta interfaz.

Los servidores RDNS y la lista de búsqueda DNS son parte de la configuración DNS para el cliente DNS, de manera que el cliente pueda resolver las solicitudes DNS IPv6.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6** > **DNS Support (Soporte DNS)**.
4. Seleccione **Include DNS information in Router Advertisement (Incluir información DNS en el anuncio de enrutador)** para habilitar el cortafuegos para que envíe información DNS IPv6.
5. Para el **Server (Servidor)** DNS, seleccione **Add (Añadir)** para añadir la dirección IPv6 de un servidor DNS recursivo. Seleccione **Add (Añadir)** para añadir hasta ocho servidores DNS recursivos. El cortafuegos envía direcciones de servidor en un anuncio de enrutador ICMPv6 en orden descendente.
6. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el servidor RDNS específico para resolver nombres de dominio.
   - El intervalo de la **Lifetime (Duración)** es cualquier valor igual o entre el **Max Interval (Intervalo máximo)** (que configuró en la pestaña **Router Advertisement [Anuncio de enrutador]**) y dos veces

© 2020 Palo Alto Networks, Inc.

ese **Max Interval (Intervalo máximo)**. Por ejemplo, si su intervalo máximo es de 600 segundos, el intervalo de duración es de 600 a 1200 segundos.
- La **Lifetime (Duración)** predeterminada es de 1200 segundos.

7. Para el sufijo DNS, seleccione **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** (nombre de dominio de un máximo de 255 bytes). Seleccione **Add (Añadir)** para añadir hasta ocho sufijos DNS. El cortafuegos envía sufijos en un anuncio de enrutador ICMPv6 en orden descendente.
8. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el sufijo. La duración posee el mismo intervalo y valor predeterminado que el **servidor**.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Monitorización NDP

El protocolo de detección de vecinos (NDP) para la dirección IPv6 (RFC 4861) lleva a cabo funciones similares a las funciones de ARP para IPv4. El cortafuegos predeterminado ejecuta el NDP, que utiliza paquetes ICMPv6 para encontrar y rastrear las direcciones de capa de enlace y el estado de los vecinos en los enlaces conectados.

Habilitar supervisión NDP de modo que pueda visualizar las direcciones IPv6 de los dispositivos en la red local del enlace, sus direcciones MAC, el nombre de usuario asociado de User-ID (si el usuario de ese dispositivo utilizó un servicio de directorio para iniciar sesión), el estado de alcance de la dirección, y la última fecha y hora informada en la que el supervisor NDP recibió un anuncio de enrutador de esta dirección IPv6. El nombre de usuario depende del mejor caso; pueden existir varios dispositivos IPv6 en una red sin nombre de usuario, como las impresoras, los equipos de fax, los servidores, etc.

Si desea rastrear con rapidez un dispositivo y un usuario que violó una regla de seguridad, es útil que la dirección IPv6, la dirección MAC y el nombre de usuario se muestren en un lugar. Necesita la dirección MAC que corresponde a la dirección IPv6 para rastrear la dirección MAC de vuelta a un conmutador físico o punto de acceso.

No se garantiza que la supervisión de NDP descubra todos los dispositivos debido a que podría haber otros dispositivos de red entre el cortafuegos y el cliente que filtra mensajes de NDP o detección de direcciones duplicadas (DAD). El cortafuegos solo puede supervisar los dispositivos que encuentra en la interfaz.

La supervisión de NDP también supervisa los paquetes de detección de direcciones duplicadas (DAD) de clientes y vecinos. También puede supervisar los logs de ND IPv6 para facilitar la resolución de problemas.

La supervisión de NDP admite interfaces Ethernet, subinterfaces, interfaces Ethernet de agregación e interfaces VLAN en todos los modelos PAN-OS.

Habilitar supervisión NDP

Realice esta tarea para habilitar la supervisión NDP en una interfaz.

STEP 1 | Habilite la supervisión NDP.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6**.
4. Seleccione **Address Resolution (Resolución de dirección)**.
5. Seleccione **Enable NDP Monitoring (Habilitar supervisión NDP)**.

© 2020 Palo Alto Networks, Inc.

Tras habilitar o deshabilitar la supervisión NDP, debe hacer clic en Commit (Confirmar) para confirmar el cambio antes de que la supervisión NDP se inicie o se detenga.

6. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

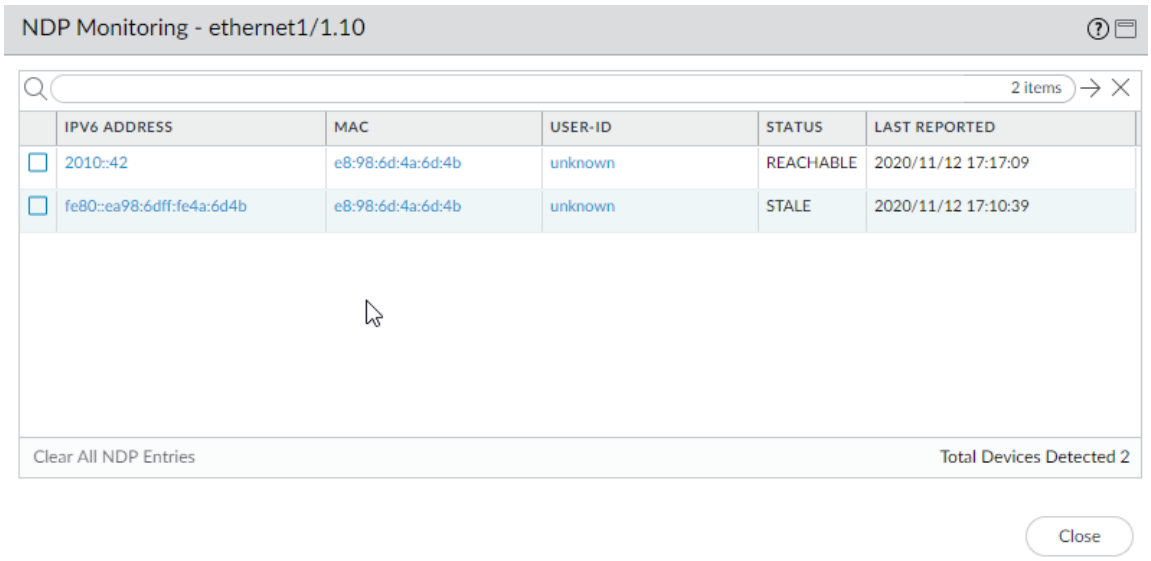
Haga clic en **Commit (Confirmar)**.

STEP 3 | Supervise paquetes NDP y DAD de clientes y vecinos.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. En la interfaz donde habilitó la supervisión NDP, en la columna Features (Funciones), mueva el puntero sobre el icono de supervisión NDP .

   El resumen de supervisión NDP de la interfaz muestra la lista de **prefijos** IPv6 que la interfaz enviará en el anuncio de enrutador (RA) si se encuentra habilitada esta opción (se trata de los prefijos IPv6 de la interfaz misma).

   Además, el resumen indica si las opciones DAD, anuncio de enrutador o asistencia de DNS están habilitadas; si las direcciones IP de los servidores DNS recursivos están configurados y los sufijos DNS configurados en la lista de búsqueda de DNS.
3. Haga clic en el icono de supervisión NDP para mostrar información detallada.



   Cada fila de la tabla detallada de supervisión NDP de la interfaz muestra la dirección IPv6 de un vecino que descubrió el cortafuegos, la dirección MAC correspondiente, la ID de usuario correspondiente (basada en el mejor caso), estado de alcance de la dirección, y última fecha y hora informada en la que este supervisor NDP recibió un RA de esta dirección IP. Una ID de usuario no se mostrará en las impresoras u otros hosts no basados en un usuario. Si el estado de la dirección IP es antiguo, se desconoce si el vecino es alcanzable, según RFC 4861.

   En la esquina inferior derecha, se encuentra el contador de **Total Devices Detected (Dispositivos totales detectados)** en la red local del enlace.

   - Introduzca una dirección IPv6 en el campo de filtro para buscar la dirección que desea mostrar.
   - Seleccione las casillas de verificación para mostrar o no mostrar las direcciones IPv6.
   - Haga clic en los números, la flecha derecha o izquierda, o la barra de desplazamiento vertical para avanzar a través de las entradas.

© 2020 Palo Alto Networks, Inc.

- Haga clic en **Clear All NDP Entries (Borrar todas las entradas de NDP)** para borrar toda la tabla.

STEP 4 | Supervise los logs de ND para crear informes.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **System (Sistema)**.
2. En la columna Type (Tipo), visualice los logs **ipv6nd** y las descripciones correspondientes.

   Por ejemplo, `inconsistent router advertisementreceived`(anuncio de enrutador incoherente recibido) indica que el cortafuegos recibió un RA diferente al RA que enviará.

Configuración de los grupos de interfaces de agregación

Un grupo de interfaz de agregación utiliza la agregación de enlaces IEEE 802.1AX para combinar varias interfaces de Ethernet en una sola interfaz virtual que conecta el cortafuegos a otro dispositivo de red o cortafuegos. Un grupo de agregación aumenta el ancho de banda entre peers al equilibrar la carga de tráfico en las interfaces combinadas. También proporciona redundancia; cuando una interfaz falla, las interfaces restantes continúan manteniendo el tráfico.

Por defecto, la detección de fallos de interfaz es automática solo en la capa física, entre peers conectados directamente. Sin embargo, si habilita el protocolo de control de adición de enlaces (Link Aggregation Control Protocol, LACP), la detección de fallos es automática en la capa física y de enlace de datos, independientemente de si los peers están conectados directamente. LACP también permite la conmutación por error automática a interfaces en espera si configura reservas activas. Todos los cortafuegos de Palo Alto Networks admiten los grupos de agregación, excepto los modelos VM-Series. La herramienta de selección de productos indica la cantidad de grupos de agregación que admite cada cortafuegos. Cada grupo de agregación puede tener hasta ocho interfaces.

Los modelos de cortafuegos PAN-OS admiten un máximo de 16.000 direcciones IP asignadas a interfaces de capa 3 físicas o virtuales; este máximo incluye direcciones IPv4 e IPv6.

QoS solo es compatible con los primeros ocho grupos de agregación.

Antes de configurar un grupo de agregación, debe configurar sus interfaces. Entre las interfaces asignadas a cualquier grupo de agregación particular, el soporte físico del hardware puede ser diferente (por ejemplo, puede mezclar fibra óptica y cobre), pero el ancho de banda y el tipo de interfaz deben ser los mismos. Las opciones de ancho de banda y tipo de interfaz son las siguientes:

- **Ancho de banda**: 1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps
- **Interface type**: HA3, Virtual Wire, capa 2 o capa 3.

Este procedimiento describe los pasos de configuración únicamente para el cortafuegos de Palo Alto Networks. También debe configurar el grupo de agregación en el dispositivo peer. Consulte la documentación de dicho dispositivo para obtener instrucciones.

STEP 1 | Configure los parámetros de grupo de interfaz generales.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y **Add Aggregate Group (Añadir grupo de agregación)**.
2. En el campo adyacente a **Interface Name (Nombre de interfaz)** de solo lectura, introduzca un número (1-8) para identificar el grupo de agregación.
3. Para el **Interface Type**, seleccione **HA**, **Virtual Wire**, **Layer2** o **Layer3**.
4. Configure los parámetros restantes para el **Interface Type** que seleccionó.

STEP 2 | Configure los ajustes de LACP.

© 2020 Palo Alto Networks, Inc.

Realice este paso únicamente si desea habilitar LACP para el grupo de agregación.

No puede habilitar LACP para interfaces de cable virtual.

1. Seleccione la pestaña **LACP** y luego **Enable LACP (Habilitar LACP)**.
2. Configure el **Mode** para las consultas de estado de LACP en **Passive** (el valor por defecto es que el cortafuegos solo responde) o **Active** (el cortafuegos consulta a dispositivos peer).

   Se recomienda configurar un peer LACP como activo y el otro como pasivo. LACP no puede funcionar si los dos peers son pasivos. El cortafuegos no puede detectar el modo de su dispositivo peer.
3. Configure el **Transmission Rate** para la consulta LACP e intercambios de respuesta en **Slow** (cada 30 segundos, el valor por defecto) o **Fast** (cada segundo). Base su selección en el nivel de procesamiento LACP que admite la red y con qué velocidad los peers LACP deben detectar y resolver fallos de interfaz.
4. Seleccione **Fast Failover** si desea habilitar la conmutación por error a una interfaz en espera en menos de un segundo. Por defecto, la opción está deshabilitada y el cortafuegos utiliza el estándar IEEE 802.1ax para el procesamiento de conmutación por error, que demora al menos tres segundos.

   La práctica recomendada es usar Fast Failover en implementaciones en las que pueda perder datos críticos durante el intervalo de conmutación por error estándar.
5. Introduzca el **máximo de puertos** (cantidad de interfaces) que están activas (de 1 a 8) en el grupo de agregación. Si el número de interfaces que asigna al grupo supera el **máximo de puertos**, el resto de las interfaces están en modo de espera. El cortafuegos usa la **LACP Port Priority (Prioridad de puerto LACP)** de cada interfaz que usted asigna (paso 3) para determinar qué interfaces están activas inicialmente y el orden en que se activan las interfaces en espera tras la conmutación por error. Si los peers de LACP no tienen valores de prioridad de puerto coincidentes, los valores del peer con el número de **prioridad del sistema** más bajo (el valor predeterminado es 32 768; el intervalo es de 1a 65 535), cancelará el otro peer.
6. (Opcional) Para los cortafuegos activos/pasivos únicamente, seleccione **Enable in HA Passive State** si desea habilitar la negociación previa de LACP para el cortafuegos pasivo. La negociación previa de LACP permite una conmutación por error más rápida al cortafuegos pasivo (para obtener detalles, consulte Negociación previa de LACP y LLDP para la HA activa/pasiva)

   Si selecciona esta opción, no puede seleccionar Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para HA activo-pasivo); la negociación previa requiere direcciones MAC de interfaz únicas en cada cortafuegos HA.
7. (Opcional) Para los cortafuegos activos/pasivos únicamente, seleccione **Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para HA activo-pasivo)** y especifique una sola **MAC Address (Dirección MAC)** para ambos cortafuegos HA. Esta opción minimiza la latencia de conmutación por error si los peers LACP están virtualizados (aparecen en la red como un solo dispositivo). Por defecto, esta opción está deshabilitada: cada cortafuegos de un par en HA tiene una única dirección MAC.

   Cuando los peers del LACP no se virtualizan, utilizar las direcciones MAC únicas minimiza la latencia de la conmutación por error.

STEP 3 | Asignación de interfaces al grupo de agregación

Realice los siguientes pasos para cada interfaz (1-8) que pertenecerá al grupo de agregación.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en el nombre de la interfaz para editarla.
2. Cambie el **Tipo de interfaz** a **Ethernet de agregación**.
3. Seleccione el **Grupo de agregación** que acaba de definir.
4. Seleccione **Link Speed (Velocidad de enlace)**, **Link Duplex (Dúplex de enlace)** y **Link State (Estado de enlace)**.

   Se recomienda establecer la misma velocidad de enlace y valores duplicados para cada interfaz del grupo. Para los valores que no coinciden, el cortafuegos activa por defecto la velocidad más alta y dúplex completo.
5. (Opcional) Introduzca una **prioridad del puerto LACP** (el valor predeterminado es 32 768; el intervalo es de 1 a 65 535) si habilitó LACP para el grupo de agregación. Si el número de interfaces que asigna excede el valor de **Max Ports** del grupo, las prioridades de puerto determinan qué interfaces están activas o en espera. Se activarán las interfaces con los valores numéricos más bajos (prioridades más altas).
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Si los cortafuegos tienen una configuración activa/activa y usted está agregando interfaces HA3, habilite el reenvío de paquetes para el grupo de agregación.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)**, y edite la sección Packet Forwarding (Reenvío de paquetes).
2. Seleccione el grupo de agregación que configuró para **HA3 Interface** y haga clic en **OK**.

STEP 5 | Confirme los cambios y verifique el estado del grupo de agregación.

1. Haga clic en **Commit (Confirmar)**.
2. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
3. Compruebe que la columna Estado de enlace muestra un icono verde para el grupo de agregación, indicando que todas las interfaces miembro están funcionando. Si el icono es amarillo, al menos un miembro falla, pero no todos. Si el icono está en rojo, todos los miembros han fallado.
4. Si configuró LACP, compruebe que la columna Features muestre el icono de LACP habilitado para el grupo de agregación.

Reflector de Bonjour para la segmentación de red

Apple Bonjour (también conocida como red de configuración cero) permite la detección automática de dispositivos y servicios en una red local. Por ejemplo, Bonjour le permite conectarse a una impresora sin configurar manualmente su dirección IP. Para traducir nombres a direcciones en una red local, Bonjour usa DNS de multidifusión (mDNS, Multicast DNS). Bonjour utiliza un intervalo de multidifusión privado para su tráfico, que no permite el enrutamiento del tráfico. Esto evita el uso en un entorno que utilice la segmentación de red con fines administrativos o de seguridad (por ejemplo, cuando los servidores y los clientes se encuentren en subredes diferentes).

Para admitir Apple Bonjour en entornos de red que utilicen segmentación para enrutar el tráfico, puede reenviar el tráfico IPv4 de Bonjour entre interfaces o subinterfaces de Ethernet de capa 3 (L3, Layer 3) o de Ethernet de agregación (AE, Aggregated Ethernet). La opción de reflector de Bonjour le permite reenviar anuncios y consultas de Bonjour de multidifusión a interfaces o subinterfaces Ethernet de L3 y AE, lo que garantiza el acceso del usuario a los servicios y la detección del dispositivo independientemente de los valores de tiempo de vida (TTL, Time To Live) o las limitaciones de salto.

El reenvío de tráfico de Bonjour es compatible con PA-220, PA-800 y PA-3200 Series.

© 2020 Palo Alto Networks, Inc.

Cuando habilite esta opción, el cortafuegos redirigirá el tráfico de Bonjour a las interfaces y subinterfaces de L3 y AE donde habilite esta opción. Debe habilitar esta opción en todas las interfaces compatibles en las que desee gestionar el tráfico de Bonjour; por ejemplo, si desea que una interfaz de L3 específica reenvíe el tráfico de Bonjour a una interfaz de AE, debe habilitar esta opción en ambas interfaces. Puede habilitar esta opción en hasta 16 interfaces.

Para evitar bucles, el cortafuegos modifica la dirección MAC de origen a la dirección MAC de la interfaz de salida del cortafuegos. Para ayudar a prevenir ataques de inundación, si el cortafuegos recibe más paquetes por segundo que el número especificado en la siguiente tabla, el cortafuegos descarta los paquetes para proteger el cortafuegos y la red.

Límite de frecuencia de la	*serie (por segundo)*
PA-220	*100*
PA-800	*200*
PA-3200	*500*

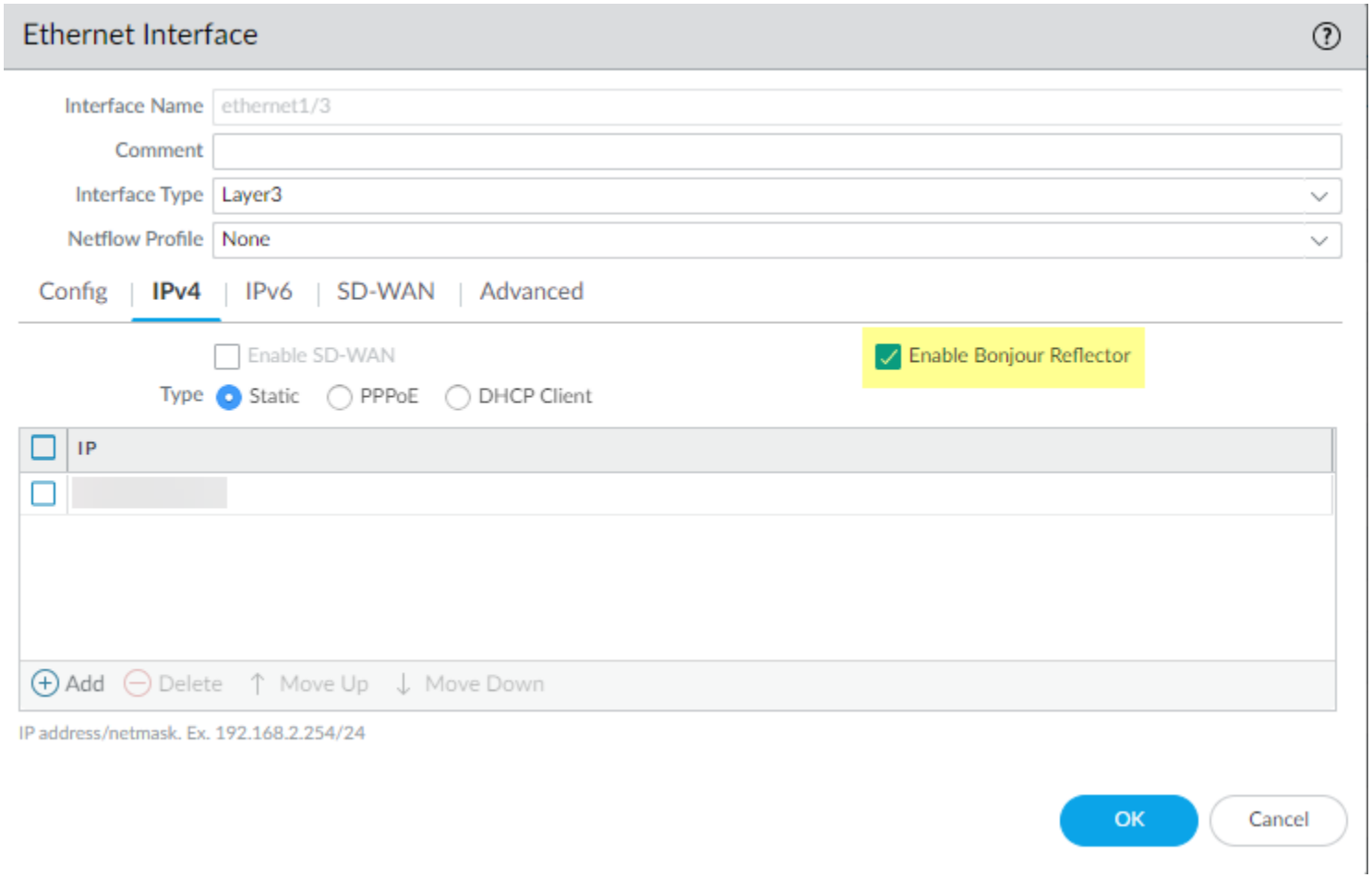
STEP 1 | Seleccone **Network (Red)** > **Interfaces**.

STEP 2 | Seleccione o **añada** una Ethernet o subinterfaz de L3 o interfaz de AE.

Si añade una subinterfaz, debe usar una etiqueta distinta de 0.

STEP 3 | Seleccione **IPv4** y, a continuación, seleccione la opción **Enable Bonjour Reflector (Habilitar reflector de Bonjour)**.

© 2020 Palo Alto Networks, Inc.



STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Repita los pasos del 1 al 4 para todas las interfaces y subinterfaces de L3 o AE a las que desee reenviar el tráfico de Bonjour.

Puede habilitar esta opción en hasta 16 interfaces o subinterfaces diferentes.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Confirme que la columna **Features (Funciones)** para la interfaz o interfaces donde habilita la opción de reflector de Bonjour muestre **`Bonjour Reflector:yes`** ( ).

STEP 8 | Utilice el comando de la CLI **`show bonjour interface (mostrar interfaz de bonjour)`** para mostrar todas las interfaces a las que el cortafuegos reenvía el tráfico de Bonjour y una lista de contadores. **`rx`** representa el número total de paquetes de Bonjour que recibe la interfaz, **`tx`** representa el número total de paquetes de Bonjour que transmite la interfaz y **`drop (descartar)`** representa el número de paquetes que descarta la interfaz.

```
admin> show bonjour interface

name                    rx          tx          drop
```


© 2020 Palo Alto Networks, Inc.

```
-------------------------------------------------------------
ethernet1/4              1            1            0
ethernet1/7              0            0            0
ethernet1/7.10           0            0            0
ethernet1/7.20           4            4            0
ae15                     0            0            0
ae16                     0            0            0
ae16.30                  0            2            0
ae16.40                  0            0            0
```

Uso de los perfiles de gestión de interfaz para restringir el acceso

Un perfil de gestión de interfaz protege al cortafuegos contra el acceso no autorizado mediante la definición de los protocolos, servicios y direcciones IP que una interfaz de cortafuegos permite para el tráfico de gestión. Por ejemplo, puede impedir que los usuarios accedan a la interfaz web del cortafuegos en la interfaz Ethernet1/1, pero permitir que la interfaz reciba consultas SNMP de su sistema de supervisión de red. En este caso, usted habilitaría SNMP y deshabilitaría HTTP/HTTPS en un perfil de gestión de interfaz y asignaría el perfil a Ethernet1/1.

Puede asignar un perfil de gestión de interfaz a interfaces Ethernet capa 3 (incluidas las subinterfaces) y a interfaces lógicas (interfaces de grupo de agregación, VLAN, loopback y de túnel) Si no asigna un perfil de gestión de interfaz a una interfaz, esta denegará por defecto el acceso a todas las direcciones IP, protocolos y servicios.

La interfaz de gestión (MGT) no requiere un perfil de gestión de interfaz. Usted restringe los protocolos, servicios y direcciones IP para la interfaz MGT cuando lleva a cabo la Realización de la configuración inicial *del cortafuegos. En caso de que la interfaz MGT deje de funcionar, permitir el acceso de gestión por otra interfaz le da la posibilidad de seguir gestionando el cortafuegos.*

Si permite el acceso a la interfaz del cortafuegos con un perfil de gestión de interfaces, no habilite el acceso de gestión (HTTP, HTTPS, SSH ni Telnet) desde internet ni desde zonas no fiables que estén dentro de los límites de seguridad de su empresa. No habilite nunca el acceso por HTTP ni Telnet porque esos protocolos realizan transmisiones de texto sin cifrar. Respete las Prácticas recomendadas para proteger el acceso administrativo *para garantizar que protege adecuadamente el acceso de gestión al cortafuegos.*

STEP 1 | Configure el perfil de gestión de interfaz.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
2. Seleccione los protocolos que la interfaz permitirá para el tráfico de gestión: **Ping**, **Telnet**, **SSH**, **HTTP**, **HTTP OCSP**, **HTTPS** o **SNMP**.

   No habilite HTTP ni Telnet porque esos protocolos realizan transmisiones de texto sin cifrar y, por lo tanto, no son seguros.
3. Seleccione los servicios que la interfaz permitirá para el tráfico de gestión:
   - **Response Pages (Páginas de respuesta)**: utilícela para habilitar páginas de respuesta para lo siguiente:
     - **Authentication Portal (Portal de autenticación)**: para ofrecer las páginas de respuesta del portal de autenticación, el cortafuegos deja los puertos abiertos en las interfaces de capa 3: 6081 para el portal de autenticación en modo transparente y 6082 para el portal de

© 2020 Palo Alto Networks, Inc.

autenticación en modo de redireccionamiento. Para obtener más información, consulte Configuración del portal de autenticación.
    - **Anulación de administrador de URL:** para obtener información detallada, consulte Permiso de acceso con contraseña a ciertos sitios.
  - **User-ID**: utilícelo para Redistribución de las marcas de tiempo de autenticación y datos.
  - **User-ID Syslog Listener-SSL (SSL de escucha de Syslog de User-ID)** o **User-ID Syslog Listener-UDP (UDP de escucha de Syslog de User-ID)**: utilice esta opción para la Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios en SSL o UDP.
4. (Opcional) Seleccione **Add (Añadir)** para añadir las direcciones IP permitidas que pueden acceder a la interfaz. Si no añade entradas a la lista, la interfaz no tendrá restricciones de direcciones IP.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Asigne el perfil de gestión de interfaz a una interfaz.

1. Seleccione **Network (Red)** > **Interfaces**, seleccione el tipo de interfaz (**Ethernet**, **VLAN**, **Loopback [Bucle invertido]** o **Tunnel [Túnel]**) y seleccione la interfaz.
2. Seleccione **Advanced (Avanzado)** > **Other info (Otra información)** y seleccione la interfaz **Management Profile (Perfil de gestión)** que acaba de añadir.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Enrutadores virtuales

Un enrutador virtual es una función del cortafuegos que participa en el enrutamiento de capa 3. El cortafuegos utiliza enrutadores virtuales para obtener rutas a otras subredes definiendo manualmente rutas estáticas o mediante la participación en uno o más protocolos de enrutamiento de capa 3 (rutas dinámicas). Las rutas que obtiene el cortafuegos mediante estos métodos completan la base de información de enrutamiento (routing information base, RIB) IP del cortafuegos. Cuando un paquete esté destinado a una subred diferente, el enrutador virtual obtendrá la mejor ruta de la RIB, la ubicará en la base de información de reenvío (FIB) y reenviará el paquete al siguiente enrutador de salto definido en la FIB. El cortafuegos utiliza la conmutación de Ethernet para llegar a otros dispositivos de la misma subred IP. (Una excepción para una mejor ruta en la FIB se produce si utiliza ECMP, en cuyo caso todas las rutas a igual coste se encuentran en la FIB.)

Las interfaces Ethernet, VLAN y del túnel definidas en el cortafuegos reciben y reenvían paquetes de capa 3. La zona de destino se deriva de la interfaz de salida basada en los criterios de reenvío y el cortafuegos consulta las reglas de la política para identificar las políticas de seguridad que se aplican a cada paquete. Además de enrutar a otros dispositivos de red, los enrutadores virtuales pueden enrutar a otros enrutadores virtuales en el mismo cortafuegos si se especifica un siguiente salto que señale a otro enrutador virtual.

Puede configurar interfaces de capa 3 en un enrutador virtual para participar con protocolos de enrutamiento dinámico (BGP, OSPF, OSPFv3 o RIP), así como añadir rutas estáticas. También puede crear varios enrutadores virtuales, cada uno de los cuales mantendrá un conjunto separado de rutas que no se comparten entre enrutadores virtuales, lo que le permitirá configurar diferentes comportamientos de enrutamiento para diferentes interfaces.

Todas las interfaces de capa 3, de bucle invertido, de VLAN y de túnel definidas en el cortafuegos se deben asociar con un enrutador virtual. Si bien cada interfaz puede pertenecer a un único enrutador virtual, puede configurar varios protocolos de enrutamiento y rutas estáticas para un enrutador virtual. Independientemente de las rutas estáticas y los protocolos de enrutamiento dinámico que se configuran para un enrutador virtual, es necesario contar con una configuración general:

STEP 1 | Obtenga la información necesaria de su administrador de red.

- Interfaces en el cortafuegos que desea para realizar el enrutamiento.
- Distancias administrativas para rutas estáticas, internas de OSFP, externas de OSPF, IBGP, EBGP y RIP.

STEP 2 | Cree un enrutador virtual y aplique interfaces a él.

El cortafuegos incluye un enrutador virtual denominado **default (predeterminado)**. Puede editar el enrutador virtual **default (predeterminado)** o añadir un nuevo enrutador virtual.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. Seleccione un enrutador virtual (**default [predeterminado]** o un enrutador virtual diferente) o haga clic en **Add (Añadir)** para añadir un nombre en **Name (Nombre)** para un nuevo enrutador virtual.
3. Seleccione **Router Settings (Configuración de enrutador)** > **General**.
4. En el cuadro **Interfaces**, haga clic en **Add (Añadir)** y seleccione una interfaz que ya esté definida.

   Repita este paso para todas las interfaces que desee añadir al enrutador virtual.
5. Haga clic en **OK (Aceptar)**.

STEP 3 | Establezca las distancias administrativas para las rutas estáticas y el enrutamiento dinámico.

© 2020 Palo Alto Networks, Inc.

Establezca las distancias administrativas para los tipos de rutas como sea necesario para su red. Cuando el enrutador virtual tiene dos o más rutas diferentes hacia el mismo destino, utiliza la distancia administrativa para seleccionar la mejor ruta de diferentes protocolos de enrutamiento y rutas estáticas, y prefiere una distancia menor.

- **Static (Estático)**: el intervalo es 10-240 y el valor por defecto es 10.
- **OSPF Internal (OSPF interno)**: el intervalo es 10-240 y el valor por defecto es 30.
- **OSPF External (OSPF externo)**: el intervalo es 10-240 y el valor por defecto es 110.
- **IBGP**: intervalo 10-240; predeterminado 200.
- **EBGP**: intervalo 10-240; predeterminado 20.
- **RIP**: intervalo 10-240; predeterminado 120.



Consulte ECMP si desea aprovechar varias rutas a igual coste para el reenvío.

STEP 4 | Confirme la configuración general del enrutador virtual.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 5 | Configure las interfaces Ethernet, VLAN, de bucle invertido y de túnel como sea necesario.

Configuración de interfaces de capa 3.

© 2020 Palo Alto Networks, Inc.

Rutas de servicio

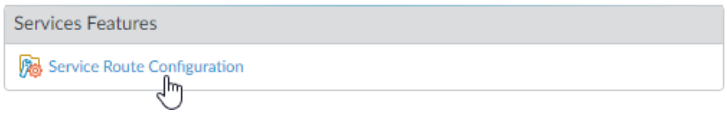
El cortafuegos utiliza la interfaz de gestión (MGT) de manera predeterminada para acceder a servicios externos, como los servidores DNS, los servidores de autenticación externa, los servicios de Palo Alto Networks como software, URL actualizaciones, licencias y AutoFocus. Una alternativa al uso de la interfaz MGT es la configuración de un puerto de datos (una interfaz regular) para acceder a estos servicios. La ruta desde la interfaz al servicio en un servidor se conoce como *ruta de servicio*. Los paquetes de servicio abandonan el cortafuegos en un puerto asignado al servicio externo y el servidor envía su respuesta a la interfaz de origen configurada y a la dirección IP de origen.

Puede configurar las rutas de servicio de manera global para el cortafuegos (se muestra en la siguiente tarea) o realizar la Personalización de rutas de servicio para un sistema virtual en un cortafuegos habilitado para varios sistemas virtuales, de modo que pueda tener la flexibilidad para utilizar interfaces asociados a un sistema virtual. Cualquier sistema virtual que no tenga una ruta de servicio configurada para un servicio particular hereda una interfaz y dirección IP establecidas globalmente para ese servicio.

El siguiente procedimiento le permite cambiar la interfaz que utiliza el cortafuegos para enviar solicitudes a los servicios externos.

STEP 1 | Personalice las rutas de servicio.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global** (omita la opción Global en un cortafuegos sin capacidad para varios sistemas virtuales), y en la sección Services Features (Funciones de servicio), haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.



2. Seleccione **Customize (Personalizar)** y realice una de las siguientes tareas para crear una ruta de servicio:
   - Para un servicio predefinido:
     - Seleccione **IPv4** o **IPv6** y haga clic en el enlace del servicio cuya ruta de servicio desea personalizar.

       Para utilizar la misma dirección de origen en varios servicios, seleccione la casilla de verificación de los servicios, haga clic en Set Selected Routes (Establecer rutas seleccionadas) y pase al siguiente paso.
     - Para limitar la lista de direcciones de origen, seleccione una interfaz en **Source Interface (Interfaz de origen)** y, luego, una dirección de esa interfaz en **Source Address (Dirección de origen)** como ruta de servicio. Si selecciona **Any (Cualquiera)** en Source Interface (Interfaz de origen), están disponibles todas las direcciones IP de todas las interfaces en la lista Source Address (Dirección de origen) en la que debe seleccionar una dirección. Si selecciona **Use default (Utilizar predeterminado)**, el cortafuegos utilizará la interfaz de gestión para la ruta de servicio, a menos que la dirección IP de destino del paquete coincida con la dirección IP de destino configurada, en cuyo caso, la dirección IP de origen se establece como la **Source Address (Dirección de origen)** configurada para la dirección de **Destination (Destino)**. Si selecciona **MGT (Gestión)**, el cortafuegos utilizará la interfaz MGT (Gestión) en la ruta de servicio independientemente de la ruta de servicio de destino.
     - Haga clic en **OK (Aceptar)** para guardar la configuración.
     - Repita este paso si desea especificar las direcciones IPv4 e IPv6 de un servicio.
   - Para una ruta de servicio de destino:

© 2020 Palo Alto Networks, Inc.

- Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una dirección IP de **Destination (Destino)**. En este caso, si el paquete llega con una dirección IP de destino que coincide con esta dirección de **Destination (Destino)** configurada, la dirección IP de origen del paquete se establecerá como la **Source Address (Dirección de origen)** configurada en el siguiente paso.
- Para limitar la lista de direcciones de origen, seleccione una interfaz en **Source Interface (Interfaz de origen)** y, luego, una dirección de esa interfaz en **Source Address (Dirección de origen)** como ruta de servicio. Si selecciona **Any (Cualquiera)** en Source Interface (Interfaz de origen), están disponibles todas las direcciones IP de todas las interfaces en la lista Source Address (Dirección de origen) en la que debe seleccionar una dirección. Si selecciona **MGT (Gestión)**, el cortafuegos utilizará la interfaz MGT (Gestión) en la ruta de servicio.
- Haga clic en **OK (Aceptar)** para guardar la configuración.

3. Repita los pasos indicados anteriormente para cada ruta de servicio que desea personalizar.
4. Haga clic en **OK (Aceptar)** para guardar la configuración de la ruta de servicio.

STEP 2 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Rutas estáticas

Por lo general, las rutas estáticas se utilizan junto con protocolos de enrutamiento dinámico. Puede configurar una ruta estática para una ubicación que un protocolo de enrutamiento dinámico no puede alcanzar. Las rutas estáticas requieren una configuración manual en cada enrutador de la red, en lugar del cortafuegos que ingresa a las rutas dinámicas en sus tablas de rutas. A pesar de que las rutas estáticas requieren esa configuración en todos los enrutadores, es posible que se la recomiende para redes pequeñas en lugar de utilizarla para protocolo de enrutamiento.

- Descripción general de la ruta estática
- Eliminación de ruta estática basada en el control de ruta
- Configuración de una ruta estática
- Configuración del control de ruta para una ruta estática

Descripción general de la ruta estática

Si desea que el tráfico específico de la capa 3 tome una ruta determinada sin participar en los protocolos de enrutamiento IP, puede realizar el procedimiento Configuración de una ruta estática utilizando rutas IPv4 e IPv6.

Una ruta predeterminada es una ruta estática específica. Si no utiliza el enrutamiento dinámico para obtener una ruta predeterminada para su enrutador virtual, debe configurar una ruta estática predeterminada. Cuando el enrutador virtual posee un paquete entrante y no encuentra coincidencias para el destino del paquete en su tabla de rutas, el enrutador virtual envía el paquete a la ruta predeterminada. La ruta IPv4 predeterminada es 0.0.0.0/0; la ruta IPv6 predeterminada es ::/0. Puede configurar rutas predeterminadas para IPv4 y para IPv6.

Las rutas estáticas no cambian ni se ajustan a los cambios en los entornos de red, de modo que por lo general, el tráfico no se redirige si se produce una falla en la ruta hacia un extremo definido como estático. Sin embargo, cuenta con opciones para respaldar las rutas estáticas si se produce un problema:

- Puede configurar una ruta estática con un perfil de detección de reenvío bidireccional (bidirectional forwarding detection, BFD). Así, si falla la sesión de BFD entre el cortafuegos y el peer de BFD, el cortafuegos elimina la ruta estática fallida de las tablas de las bases de información de enrutamiento (routing information base, RIB) y de reenvío (forwarding information base, FIB) y utiliza una ruta alternativa de menor prioridad.
- Realice el procedimiento Configuración del control de ruta para una ruta estática para que el cortafuegos pueda utilizar una ruta alternativa.

De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 10. Cuando el cortafuegos tiene dos o más rutas hacia el mismo destino, utiliza la ruta con la menor distancia administrativa. Si se aumenta la distancia administrativa de una ruta estática a un valor mayor que el de una ruta dinámica, puede utilizar la ruta estática como una ruta de respaldo si la ruta dinámica no se encuentra disponible.

Cuando configura una ruta estática, puede especificar si el cortafuegos instala una ruta estática IPv4 en la tabla de rutas (RIB) de unidifusión o multidifusión, o en ambas tablas, o si no la instala. Por ejemplo, solo puede instalar una ruta estática IPv4 en la tabla de rutas de multidifusión debido a que solo desea que el tráfico multidifusión utilice esta ruta. Esta opción le proporciona más control sobre la ruta que toma el tráfico. Puede especificar si el cortafuegos instala una ruta estática IPv6 en la tabla de rutas de unidifusión o no.

© 2020 Palo Alto Networks, Inc.

Eliminación de ruta estática basada en el control de ruta

Cuando configura el control de red para una ruta estática, el cortafuegos utiliza el control de red para detectar cuando una ruta a uno o más destinos se ha caído. Así puede redirigir el tráfico por rutas alternativas. El cortafuegos utiliza el control de rutas para las rutas estáticas de manera similar al control de rutas para el reenvío HA o basado en políticas (policy-based forwarding, PBF), de la siguiente manera:

- El cortafuegos envía mensajes de ping ICMP (mensajes de heartbeat) a uno o más destinos controlados que usted determine que son robustos y que reflejan la disponibilidad de la ruta estática.
- Si los pings a cualquiera de los destinos, o a todos los destinos, fallan, el cortafuegos considera la ruta estática como inactiva también y la elimina de la base de información de enrutamiento (Routing Information Base, RIB) y la base de información de reenvío (Forwarding Information Base, FIB). La RIB es la tabla de rutas estáticas con las que el cortafuegos está configurado y las rutas dinámicas que detectó en los protocolos de enrutamiento. La FIB es la tabla de reenvío de rutas que el cortafuegos utiliza para el reenvío de paquetes. El cortafuegos selecciona una ruta estática alternativa hacia el mismo destino (según la ruta con la métrica más baja) desde la RIB y la coloca en la FIB.
- El cortafuegos continúa controlando la ruta que falló. Cuando la ruta se reactiva (según la condición de fallo **Any [Cualquiera]** o **All [Todos]**) y el control de ruta regresa al estado activo, se inicia el temporizador de tiempo de espera preferente. El control de ruta debe permanecer activo por la duración del temporizador de tiempo de espera; luego el cortafuegos considera la ruta estática como estable y la restablece en la RIB. El cortafuegos luego compara las métricas de las rutas hacia el mismo destino para decidir qué rutas corresponden a la FIB.

La supervisión de rutas es un mecanismo deseable para evitar el descarte de tráfico silenciosamente para los siguientes elementos:

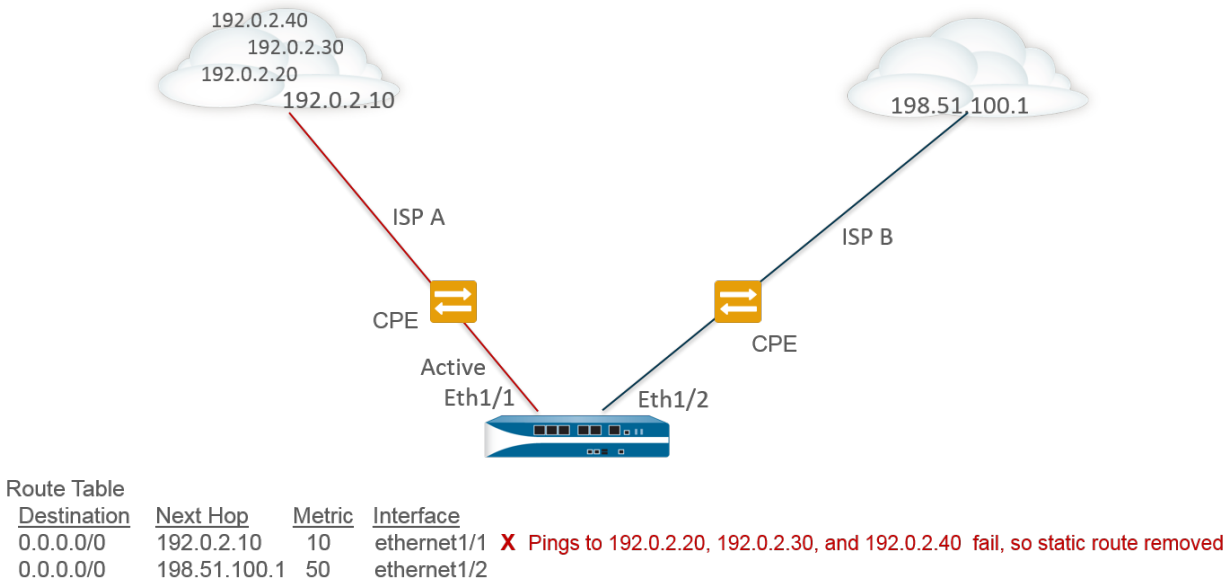
- Una ruta estática o predeterminada.
- Una ruta estática o predeterminada redistribuida a un protocolo de enrutamiento.
- Una ruta estática o predeterminada cuando un peer no admite BFD. (La práctica recomendada es no habilitar tanto BFD como el control de ruta en una misma interfaz).
- Una ruta estática o predeterminada en lugar de usar el control de ruta PBF, que no elimina una ruta estática que falló de la RIB, FIB o política de redistribución.

El control de ruta no se aplica a las rutas estáticas configuradas entre enrutadores virtuales.

En la siguiente figura, el cortafuegos está conectado a dos ISP para la redundancia de ruta a Internet. La ruta predeterminada principal 0.0.0.0 (métrica 10) utiliza el próximo salto 192.0.2.10; la ruta predeterminada secundaria 0.0.0.0 (métrica 50) utiliza el próximo salto 198.51.100.1. El equipo del cliente en las instalaciones (customer premises equipment, CPE) para ISP A mantiene el enlace físico principal activo, incluso después de que la conexión a Internet cae. Cuando el enlace está artificialmente activo, el cortafuegos no puede detectar que el enlace está inactivo y que debe reemplazar la ruta que falló por la ruta secundaria de la RIB.

Para evitar el descarte silenciosos del tráfico hacia un enlace erróneo, configure el control de ruta de 192.0.2.20, 192.0.2.30 y 192.0.2.40 y si todas las rutas (o algunas de las rutas) a estos destinos fallan, el cortafuegos asume que la ruta al próximo salto 192.0.2.10 también está inactiva, elimina la ruta estática 0.0.0.0 (que utiliza el próximo salto 192.0.2.10) de su RIB y la reemplaza por la ruta secundaria al mismo destino 0.0.0.0 (que utiliza el próximo salto 198.51.100.1), que también accede a Internet.

© 2020 Palo Alto Networks, Inc.



Cuando Configura una ruta estática, uno de los siguientes campos es el próximo salto hacia ese destino. El tipo de próximo salto que configure determinará la medida que tomará el cortafuegos durante el control de ruta, de la siguiente manera:

Si Next Hop Type (Tipo de próximo salto) en Static Route (Ruta estática) es:	Acción del cortafuegos para el ping ICMP
Dirección IP	El cortafuegos utiliza la dirección IP de origen y la interfaz de salida de la ruta estática como la dirección de origen e interfaz de salida en el ping ICMP. Utiliza la dirección IP de destino configurada del destino controlado como la dirección de destino del ping. Utiliza la dirección de próximo salto de la ruta como la dirección de próximo salto del ping.
Next VR (Siguiente VR)	El cortafuegos utiliza la dirección IP de origen de la ruta estática como la dirección de origen en el ping ICMP. La interfaz de salida se basa en el resultado de búsqueda del enrutador virtual de próximo salto. La dirección IP de destino configurada del destino controlado como es la dirección de destino del ping.
ninguno	El cortafuegos utiliza la dirección IP de destino del control de ruta como el próximo salto y envía el ping de ICMP a la interfaz especificada en la ruta estática.

Cuando el control de ruta para una ruta estática o predeterminada falla, el cortafuegos registra un evento crítico (ruta-control-fallo). Cuando la ruta estática o predeterminada se recupera, el cortafuegos registra otro evento crítico (ruta-contro-recuperación).

El cortafuegos sincroniza las configuraciones de control de ruta para una implementación HA activa/pasiva, pero el cortafuegos bloquea los paquetes de ping ICMP de salida en un peer HA pasivo, debido a que no procesa activamente el tráfico. El cortafuegos no sincroniza las configuraciones de control de ruta para las implementaciones HA activas/activas.

© 2020 Palo Alto Networks, Inc.

Configuración de una ruta estática

Realice la siguiente tarea para configurar las Rutas estáticas o una ruta predeterminada para un enrutador virtual en el cortafuegos.

STEP 1 | Configure una ruta estática.

1. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y seleccione el enrutador virtual que desea configurar, como **default (predeterminado)**.
2. Seleccione la pestaña **Static Routes**.
3. Seleccione **IPv4** o **IPv6**, según el tipo de ruta estática que desee configurar.
4. **Add (Añada)** un **Name (Nombre)** para la ruta.
5. En **Destination (Destino)**, introduzca la ruta y la máscara de red (por ejemplo, 192.168.2.2/24 como dirección IPv4 o 2001:db8:123:1::1/64 como dirección IPv6). Si crea una ruta predeterminada, introduzca la ruta predeterminada (0.0.0.0/0 como dirección IPv4 o ::/0 como dirección IPv6). O bien, puede crear un objeto de dirección de tipo máscara de red IP.
6. (Opcional) En **Interface (Interfaz)**, especifique la interfaz saliente que utilizarán los paquetes para ir al próximo salto. Utilice este control más estricto en la interfaz que el cortafuegos utiliza en lugar de la interfaz en la tabla de rutas para el próximo salto de esta ruta.
7. En **Next Hop (Próximo salto)**, seleccione una de las siguientes opciones:
   - **IP Address (Dirección IP):** introduzca la dirección IP (por ejemplo, 192.168.56.1 o 2001:db8:49e:1::1) cuando desee enrutarla a un próximo salto específico. Debe **habilitar direcciones IPv6 en la interfaz** (cuando Configuración de interfaces de capa 3) para utilizar una dirección IPv6 de próximo salto. Si crea una ruta predeterminada, en **Next Hop (Próximo salto)**, debe seleccionar **IP Address (Dirección IP)** e introducir la dirección IP de su puerta de enlace de internet (por ejemplo, 192.168.56.1 o 2001:db8:49e:1::1). O bien, puede crear un objeto de dirección de tipo máscara de red IP. El objeto de dirección debe tener la máscara de red /32 para IPv4 o /128 para IPv6.
   - **Next VR (Próximo VR):** seleccione esta opción y seleccione un enrutador virtual si desea enrutarlo internamente a un enrutador virtual diferente en el cortafuegos.
   - **FQDN**: introduzca un nombre de dominio completo (Fully Qualified Domain Name, FQDN), seleccione un objeto de dirección que utilice un FQDN o cree un objeto de dirección del tipo FQDN.

     Si utiliza un FQDN como siguiente salto de la ruta estática, se debe resolver en una dirección IP que pertenezca a la misma subred que la interfaz configurada para dicha ruta; de lo contrario, el cortafuegos rechaza la resolución y el FQDN se queda sin resolver.

     El cortafuegos solo emplea una dirección IP (de cada tipo de familia, esto es, IPv4 o IPv6) de la resolución de DNS del FQDN. Si se devuelven varias direcciones, el cortafuegos utiliza la dirección IP preferida que coincida con el tipo de familia de IP (IPv4 o IPv6) configurado para el siguiente salto. La dirección IP preferida es la primera dirección que devuelve el servidor DNS en su respuesta inicial. El cortafuegos la mantiene como preferida mientras siga apareciendo en las respuestas posteriores, aunque el orden sea distinto.
   - **Discard (Descartar):** seleccione esta opción para descartar los paquetes que se dirigen a este destino.
   - **None (Ninguno)**: seleccione esta opción si no existe el siguiente salto en la ruta. Por ejemplo, una conexión punto a punto no requiere un próximo salto debido a que solo existe una dirección de destino para los paquetes.
8. Introduzca una **Admin Distance (Distancia administrativa)** para que la ruta anule la distancia administrativa predeterminada establecida para las rutas estáticas en este enrutador virtual (intervalo de 10 a 240; valor predeterminado: 10).

© 2020 Palo Alto Networks, Inc.

9. Introduzca una **Metric (Métrica)** para la ruta (el intervalo es de 1 a 65 535).

STEP 2 | Seleccione la ubicación donde se instalará la ruta.

Seleccione la **Route Table (Tabla de rutas)** (RIB) en la que desea que el cortafuegos instale la ruta estática:

- **Unicast (Unidifusión):** instale la ruta en la tabla de rutas de unidifusión. Seleccione esta opción si desea que la ruta se utilice únicamente para el tráfico de rutas de unidifusión.
- **Multicast (Multidifusión):** instale la ruta en la tabla de rutas de multidifusión (disponible solo en el caso de las rutas IPv4). Seleccione esta opción si desea que la ruta se utilice únicamente para el tráfico de rutas de multidifusión.
- **Both (Ambas):** instale la ruta en la tabla de rutas de unidifusión y multidifusión (disponible solo en el caso de las rutas IPv4). Seleccione esta opción si desea que el tráfico de unidifusión o de multidifusión utilice esta ruta.
- **No Install (Sin instalación):** no instale la ruta en ninguna de las tablas de rutas.

STEP 3 | (Opcional) Si su modelo de cortafuegos admite BFD, puede aplicar un **perfil de BFD** a la ruta estática, de modo que si la ruta estática falla, el cortafuegos elimine la ruta de la RIB y la FIB, y utilice una ruta alternativa. El valor predeterminado es **None (Ninguna)**.

STEP 4 | Haga clic en **OK** dos veces.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Configuración del control de ruta para una ruta estática

Utilice el siguiente procedimiento para configurar la Eliminación de ruta estática basada en el control de ruta.

STEP 1 | Habilite el control de ruta para una ruta estática.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Static Routes (Rutas estáticas)**, **IPv4** o **IPv6**, y la ruta estática que desea controlar. Puede controlar hasta 128 rutas estáticas.
3. Seleccione **Path Monitoring (Control de ruta)** para habilitar el control para la ruta.

STEP 2 | Configure los destinos controlados para la ruta estática.

1. Seleccione **Add (Añadir)** para añadir un destino controlado por **Name (Nombre)**. Puede añadir hasta ocho destinos controlados por ruta estática.
2. Seleccione **Enable (Habilitar)** para controlar el destino.
3. Para **Source IP (IP de origen)**, seleccione la dirección IP que el cortafuegos utiliza en el ping ICMP para el destino controlado:
   - Si la interfaz tiene varias direcciones IP, seleccione una.
   - Si selecciona una interfaz, el cortafuegos utilizará la primera dirección IP asignada a la interfaz de forma predeterminada.
   - Si selecciona **DHCP (Use DHCP Client address) (DHCP (Usar la dirección del cliente DHCP))**, el cortafuegos utilizará la dirección que DHCP asignó a la interfaz. Para ver la dirección DHCP, seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en la fila de la interfaz Ethernet, haga clic en **Dynamic DHCP Client (Cliente DHCP dinámico)**. La dirección IP aparecerá en la ventana Estado de la interfaz IP dinámica.
4. Para **Destination IP (IP de destino)**, ingrese una dirección IP o un objeto de dirección para el cual el cortafuegos supervisará la ruta. El destino controlado y el destino de ruta estática deben usar la misma familia de direcciones (IPv4 o IPv6).

© 2020 Palo Alto Networks, Inc.



La dirección IP de destino debe pertenecer a un endpoint confiable; no debería basar el control de ruta en un dispostivio que es inestable o no confiable.

5. (Opcional) Especifique el **Ping Interval (sec) (Intervalo de ping [s])** ICMP en segundos para determinar con qué frecuencia el cortafuegos supervisará la ruta (el intervalo es de 1 a 60 y el valor predeterminado es 3).
6. (Opcional) Especifique el **Ping Count (Recuento de pings)** ICMP de paquetes que no regresan del destino para que el cortafuegos considere la ruta estática como inactiva y la elimine de RIB y FIB (el intervalo es de 3 a 10; el valor predeterminado es 5).
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Determine si el control de ruta para la ruta estática se basa en uno o todos los destinos controlados, y configure el tiempo de retención preferente.

1. Seleccione una **Failure Condition (Condición de fallo)**, **Any (Cualquiera)** o **All (Todas)** de los destinos controlados para la ruta estática deben estar al alcance del ICMP para que el cortafuegos elimine la ruta estática de RIB y FIB, y añada la ruta estática que contenga la siguiente métrica más baja al mismo destino en FIB.



Seleccione All (Todos) para evitar la posibilidad de que un solo destino controlado designe un fallo de ruta cuando, por ejemplo, el destino esté simplemente fuera de línea para el mantenimiento.

2. (Opcional) Especifique el **Preemptive Hold Time (min) (Tiempo de espera preferente [s])**, que es la cantidad de minutos que un monitor de ruta inactivo debe permanecer en estado activo para que el cortafuegos vuelva a instalar la ruta estática en RIB. El monitor de ruta evalúa todos sus destinos controlados para la ruta estática y aparece según la condición de fallo de **Any (Cualquiera)** o **All (Todos)**. Si el enlace se desactiva o fluctúa durante el tiempo de espera, cuando el enlace vuelve a estar activo, el monitor de ruta puede volver a activarse; el temporizador se reinicia cuando el monitor de ruta regresa al estado activo.

   Un **Preemptive Hold Time (Tiempo de espera preferente)** de cero hace que el cortafuegos vuelva a instalar la ruta en el RIB inmediatamente después de que el monitor de ruta se activa. El intervalo es de 0 a 1,440; el valor predeterminado es 2.
3. Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

STEP 5 | Verifique el control de ruta en rutas estáticas.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual en el que está interesado, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. En la pestaña **Routing (Enrutamiento)**, seleccione **Static Route Monitoring (Control de ruta estática)**.
3. Para una ruta estática (Destino), visualice si el control de ruta está habilitado o inhabilitado. La columna Status (Estado) indica si la ruta está activa, inactiva o inhabilitada. Las marcas para la ruta estática son las siguientes: A: activa, S: estática; E: ECMP.
4. Seleccione **Refresh (Actualizar)** periódicamente para ver el estado más reciente del control de ruta (comprobación de estado).
5. Pase el ratón sobre el estado de una ruta para ver las direcciones IP controladas y los resultados de los pings enviados a los destinos controlados para esa ruta. Por ejemplo, 3/5 significa que un intervalo de ping de 3 segundos y un recuento de pings de 5 pings omitidos consecutivos (el cortafuegos no recibe ningún ping en los últimos 15 segundos) indica que el control de rutas detecta un fallo de enlace. Según la condición de fallo **Any (Cualquiera)** o **All (Todos)**, si el control de ruta está

© 2020 Palo Alto Networks, Inc.

en modo de fallo y el cortafuegos recibe un ping después de 15 segundos, la ruta puede considerarse activa y se inicia el **Preemptive Hold Time (Tiempo de espera preferente)**.

El estado indica los resultados del último ping controlado: correcto o fallido. El fallo indica que la serie de paquetes de ping (intervalo de pings multiplicado por el recuento de pings) no fue correcta. Un solo fallo de paquete de ping no refleja un estado de fallo de ping.

STEP 6 | Visualice el RIB y FIB para verificar que la ruta estática se haya eliminado.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual en el que está interesado, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. En la pestaña **Routing (Enrutamiento)**, seleccione **Route Table (Tabla de rutas)** (RIB) y luego la **Forwarding Table (Tabla de reenvío)** (FIB) para visualizar cada una, respectivamente.
3. Seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para visualizar la tabla de rutas correspondiente.
4. Para **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 and IPv6 (IPv4 e IPv6)**, **IPv4 Only (IPv4 únicamente)** o **IPv6 Only (IPv6 únicamente)**.
5. (Opcional) En el campo de filtros, ingrese la ruta que está buscando y seleccione la flecha o use la barra de desplazamiento para moverse por las páginas de rutas.
6. Determine si la ruta se eliminó o está presente.
7. Seleccione **Refresh (Actualizar)** periódicamente para ver el estado más reciente del control de ruta (comprobación de estado).



Para visualizar los eventos registrados para el control de ruta, seleccione Monitor (Supervisar) > Logs [Logs] > System (Sistema). Verifique la entrada para path-monitor-failure (ruta-control-fallo), que indica el control de ruta para un destino de ruta estática fallido, de tal forma que la ruta se eliminó. Verifique la entrada para path-monitor-recovery (ruta-control-recuperación), que indica el control de ruta para un destino de ruta estática recuperado, de tal forma que la ruta se restauró.

© 2020 Palo Alto Networks, Inc.

RIP

El protocolo de información de enrutamiento (RIP, Routing Information Protocol) es un protocolo de gateway interior (IGP, interior gateway protocol) diseñado para redes IP pequeñas. RIP se basa en el recuento de saltos para determinar las rutas; las mejores rutas tienen el menor número de saltos. RIP se basa en UDP y utiliza el puerto 520 para las actualizaciones de rutas. Al limitar las rutas a un máximo de 15 saltos, el protocolo ayuda a evitar el desarrollo de bucles de enrutamiento, pero también limita el tamaño de red admitido. Si se requieren más de 15 saltos, el tráfico no se enruta. RIP también puede tardar más en converger que OSPF y otros protocolos de enrutamiento. El cortafuegos admite RIP v2.

Realice el siguiente procedimiento para configurar RIP:

STEP 1 | Configure los ajustes de configuración general de enrutador virtual.

Consulte Enrutadores virtuales para obtener más información.

STEP 2 | Configure los ajustes de configuración general de RIP.

1. Seleccione la pestaña RIP.
2. Seleccione **Enable (Habilitar)** para habilitar el protocolo RIP.
3. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta predeterminada a través de RIP. Este es el ajuste predeterminado recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas predeterminadas mediante RIP.

STEP 3 | Configure interfaces para RIP.

1. En la sección de configuración de la interfaz de la pestaña **Interfaces**, seleccione una interfaz.
2. Seleccione una interfaz ya definida.
3. Seleccione **Enabled (Habilitado)**.
4. Seleccione **Advertise** si desea anunciar una ruta por defecto a peers RIP con el valor métrico especificado.
5. (Opcional) Seleccione un perfil en la lista **Auth Profile (Perfil de autenticación)**.
6. En la lista **Mode (Modo)**, seleccione normal (normal), passive (pasivo) o send-only (solo envío).
7. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure los temporizadores de RIP.

1. En la pestaña **Timers**, introduzca un valor para **Interval Seconds (sec)**. Este ajuste define la duración de los siguientes intervalos del temporizador en segundos (el intervalo es 1-60; el valor por defecto es 1).
2. Especifique los **Update Intervals** para definir el número de intervalos entre los anuncios de actualización de ruta (el intervalo es 1-3.600; el valor por defecto es 30).
3. Especifique los **Delete Intervals** para definir el número de intervalos entre el momento en el que caduca la ruta y su eliminación (el intervalo es 1-3.600; el valor por defecto es 180).
4. Especifique los intervalos de vencimiento en **Expire Intervals (Intervalos de vencimiento)** para definir la cantidad de intervalos entre la última vez que se actualizó la ruta y su vencimiento (rango: 1 a 3600; valor predeterminado: 120).

STEP 5 | (Opcional) Configure perfiles de autenticación.

De manera predeterminada, el cortafuegos no utiliza autenticación de RIP para el intercambio entre vecinos de RIP. Opcionalmente, puede configurar una autenticación de RIP entre vecinos de RIP con una

© 2020 Palo Alto Networks, Inc.

contraseña simple o la autenticación MD5. Se recomienda la autenticación MD5; es más segura que una contraseña simple.

Autenticación de contraseña simple de RIP

1. Seleccione **Auth Profiles (Perfiles de autenticación)** y haga clic en **Add (Añadir)** para añadir un nombre para el perfil de autenticación para autenticar los mensajes RIP.
2. Seleccione Contraseña simple como Tipo de contraseña.
3. Introduzca una contraseña simple y, a continuación, confírmela.

Autenticación MD5 de RIP

1. Seleccione **Auth Profiles (Perfiles de autenticación)** y haga clic en **Add (Añadir)** para añadir un nombre para el perfil de autenticación para autenticar los mensajes RIP.
2. Seleccione **MD5** como el **Password Type (Tipo de contraseña)**.
3. Haga clic en **Add (Añadir)** para añadir una o más entradas de contraseña, que incluyan las siguientes:
   - ID de clave (intervalo: 0-255)
   - Clave
4. (Opcional) Seleccione el estado **Preferred (Preferido)**.
5. Haga clic en **ACEPTAR** para especificar la clave que deberá utilizarse para autenticar el mensaje saliente.
6. Vuelva a hacer clic en **ACEPTAR** en el cuadro de diálogo Enrutador virtual - RIP - Perfil de autenticación.

STEP 6 | **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

OSPF

Open Shortest Path First (OSPF) es un protocolo de gateway interior (IGP) que suele utilizarse la mayoría de las veces para gestionar dinámicamente rutas de red en redes de empresas de gran tamaño. Determina las rutas de forma dinámica obteniendo la información de otros enrutadores y anunciando las rutas a otros enrutadores mediante anuncios de estado de enlaces (LSA, Link State Advertisements). La información recopilada de los LSA se utiliza para construir un mapa de topología de la red. Este mapa de topología se comparte entre los enrutadores de la red y se utiliza para cumplimentar la tabla de enrutamiento IP con rutas disponibles.

Los cambios en la topología de la red se detectan dinámicamente y se utilizan para generar un nuevo mapa de topología en cuestión de segundos. Se calcula un árbol con la ruta más corta de cada ruta. Se utilizan las medidas asociadas a cada interfaz de enrutamiento para calcular la mejor ruta. Pueden incluir distancia, rendimiento de red, disponibilidad de enlaces, etc. Además, estas medidas pueden configurarse de manera estática para dirigir el resultado del mapa de topología de OSPF.

La implementación de Palo Alto Networks de OSPF admite por completo los siguientes RFC:

- RFC 2328 (para IPv4)
- RFC 5340 (para IPv6)

Los siguientes temas ofrecen más información sobre el OSPF y los procedimientos para configurar OSPF en el cortafuegos:

- Conceptos de OSPF
- Configuración de OSPF
- Configuración de OSPFv3
- Configuración del reinicio correcto de OSPF
- Confirmación del funcionamiento de OSPF

Conceptos de OSPF

Los siguientes temas presentan los conceptos de OSPF que debe comprender para configurar el cortafuegos con el fin de que participe en una red OSPF:

- OSPFv3
- Vecinos OSPF
- Áreas OSPF
- Tipos de enrutadores OSPF

OSPFv3

OSPFv3 permite la compatibilidad con el protocolo de enrutamiento OSPF dentro de una red IPv6. Como tal, permite la compatibilidad con direcciones y prefijos IPv6. Conserva la mayor parte de la estructura y las funciones de OSPFv2 (para IPv4) con algunos cambios menores. A continuación se indican algunas de las adiciones y los cambios en OSPFv3:

- **Compatibilidad con varias instancias por enlace**: Con OSPFv3, puede ejecutar varias instancias del protocolo OSPF a través de un único enlace. Esto se consigue al asignar un número de ID de instancia de OSPFv3. Una interfaz que esté asignada a un ID de instancia descartará paquetes que contengan un ID diferente.
- **Procesamiento de protocolos por enlace**: OSPFv3 funciona según enlace en lugar de hacerlo según subred IP como en OSPFv2.

© 2020 Palo Alto Networks, Inc.

- **Cambios en las direcciones**: Las direcciones IPv6 no están presentes en paquetes OSPFv3, excepto en el caso de cargas de LSA en paquetes de actualización de estado de enlace. Los enrutadores vecinos se identifican mediante el ID de enrutador.
- **Cambios de autenticación**: OSPFv3 no incluye ninguna capacidad de autenticación. Para configurar OSPFv3 en un cortafuegos, es necesario un perfil de autenticación que especifique una carga de seguridad encapsulada (ESP) o un encabezado de autenticación (AH) de IPv6. El procedimiento de nueva asignación de claves especificado en el RFC 4552 no se admite en esta versión.
- **Compatibilidad con varias instancias por enlace**: Cada instancia se corresponde con un ID de instancia incluido en el encabezado de paquete OSPFv3.
- **Nuevos tipos de LSA**: OSPFv3 admite dos nuevos tipos de LSA: LSA de enlace y LSA de prefijo intraárea.

Todos los cambios adicionales se describen de manera detallada en el RFC 5340.

Vecinos OSPF

Dos enrutadores con OSPF conectados por una red común y en la misma área OSPF que forman una relación son vecinos OSPF. La conexión entre estos enrutadores puede ser a través de un dominio de difusión común o mediante una conexión de punto a punto. Esta conexión se realiza a través del intercambio de paquetes de saludo del protocolo OSPF. Estas relaciones de vecinos se utilizan para intercambiar actualizaciones de enrutamiento entre enrutadores.

Áreas OSPF

OSPF funciona en un único sistema autónomo (AS). No obstante, las redes de dentro de este AS único pueden dividirse en distintas áreas. De manera predeterminada, se crea el área 0. El área 0 puede funcionar por sí sola o actuar como la red troncal de OSPF para un mayor número de áreas. Cada área OSPF recibe un nombre que es un identificador de 32 bits, el cual, en la mayoría de los casos, se escribe en la misma notación decimal con puntos que una dirección IP4. Por ejemplo, el área 0 suele escribirse como 0.0.0.0.

La topología de un área se mantiene en su propia base de datos de estados de enlaces y se oculta de otras áreas, lo que reduce la cantidad de tráfico de enrutamiento que necesita OSPF. A continuación, la topología se comparte de manera resumida entre áreas mediante un enrutador de conexión.

Tipos de áreas OSPF	Description (Descripción)
Área troncal	El área troncal (Área 0) es el núcleo de una red OSPF. El resto de las áreas se conectan a ella y todo el tráfico entre las áreas debe atravesarla. Todo el enrutamiento entre las áreas se distribuye a través del área troncal. Si bien el resto de las áreas OSPF deben conectarse al área troncal, esta conexión no tiene que ser directa y puede realizarse a través de un enlace virtual.
Área OSPF normal	En un área OSPF normal no hay restricciones; el área puede aceptar todo tipo de rutas.
Área OSPF de código auxiliar	Un área de código auxiliar no recibe rutas de otros sistemas autónomos. El enrutamiento desde el área de código auxiliar se realiza a través de la ruta predeterminada hasta el área troncal.
Área de NSSA	El área de NSSA (Not So Stubby Area) es un tipo de área de código auxiliar que puede importar rutas externas con algunas excepciones limitadas.

© 2020 Palo Alto Networks, Inc.

Tipos de enrutadores OSPF

Dentro de un área OSPF, los enrutadores se dividen en las siguientes categorías.

- **Enrutador interno**: Enrutador que solamente tiene relaciones de vecino OSPF con los dispositivos de la misma área.
- **Enrutador de borde de área (ABR)**: un enrutador que tiene relaciones de vecino OSPF con los dispositivos de varias áreas OSPF. Los ABR recogen información de topología de sus áreas conectadas y la distribuyen al área troncal.
- **Enrutador de área troncal:** un enrutador de área troncal es un enrutador que ejecuta OSPF y cuenta con, al menos, una interfaz conectada al área troncal OSPF. Como los ABR siempre están conectados a la red troncal, siempre se clasifican como enrutadores troncales.
- **Enrutador de límite de sistema autónomo (ASBR)**: Enrutador que se conecta a más de un protocolo de enrutamiento e intercambia información de enrutamiento entre ellos.

Configuración de OSPF

OSPF determina las rutas de forma dinámica obteniendo la información de otros enrutadores y anunciando las rutas a otros enrutadores mediante anuncios de estado de enlaces (LSA). El enrutador mantiene la información sobre los enlaces entre él y el destino y puede realizar decisiones de enrutamiento con gran eficiencia. Se asigna un coste a cada interfaz de enrutador y las mejores rutas son aquellas con menor coste, después de sumar todas las interfaces de enrutador saliente detectadas y la interfaz que recibe los LSA.

Las técnicas jerárquicas se utilizan para limitar el número de rutas que se deben anunciar y los LSA asociados. Como OSPF procesa dinámicamente una cantidad considerable de información de enrutamiento, tiene mayores requisitos de procesador y memoria que RIP.

STEP 1 | Configure los ajustes de configuración general de enrutador virtual.

Consulte Enrutadores virtuales para obtener más información.

STEP 2 | Habilite OSPF.

1. Seleccione la pestaña OSPF.
2. Seleccione **Enable** para habilitar el protocolo OSPF.
3. Introduzca el **Router ID (Identificador de enrutador)**.
4. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta predeterminada a través de OSPF. Este es el ajuste predeterminado recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas por defecto a través de OSPF.

STEP 3 | Configure el tipo de áreas para el protocolo OSPF.

1. En la pestaña **Areas (Áreas)**, seleccione **Add (Añadir)** para añadir un **Area ID (Identificador de área)** para el área, con formato *x.x.x.x*. Es el identificador que cada vecino debe aceptar para formar parte de la misma área.
2. En la pestaña **Type (Tipo)**, seleccione una de las siguientes opciones de la lista **Type (Tipo)** del área:
   - **Normal**: no hay restricciones; el área puede aceptar todos los tipos de rutas.
   - **Stub (Código auxiliar)**: no hay salida desde el área. Para acceder a un destino fuera del área, es necesario atravesar el límite, que conecta con el resto de áreas. Si selecciona esta opción, configure lo siguiente:
     - **Aceptar resumen**: Los anuncios de estado de enlaces (LSA) se aceptan desde otras áreas. Si esta opción de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está deshabilitada, el área OSPF se comportará como un área totalmente de código auxiliar (TSA) y ABR no propagará ninguno de los LSA de resumen.

© 2020 Palo Alto Networks, Inc.

- **Advertise Default Route (Anunciar ruta predeterminada)**: los LSA de ruta por defecto se incluirán en los anuncios al área de código auxiliar junto con un valor de medida configurado dentro del intervalo configurado 1-255.

- **NSSA**: el cortafuegos solamente puede salir del área por rutas que no sean rutas de OSPF. Si selecciona NSSA, seleccione **Accept Summary (Aceptar resumen)** y **Advertise Default Route (Anunciar ruta predeterminada)** como se describió para el **Stub (Código auxiliar)**. Si selecciona esta opción, configure lo siguiente:
  - **Type (Tipo)**: Seleccione el tipo de ruta **Ext 1** o **Ext 2** para anunciar el LSA predeterminado.
  - **Ext Ranges (Intervalos externos)**: seleccione **Add (Añadir)** para añadir intervalos de rutas externas que desee en **Advertise (Anunciar)** o para los que desee **Suppress (Suprimir)** el anuncio.

3. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure el intervalo de áreas para el protocolo OSPF.

1. En la pestaña **Range (Intervalo)**, haga clic en **Add (Añadir)** para añadir direcciones de destino LSA agrupadas en el área en subredes.
2. Seleccione **Anunciar** o **Suprimir** los anuncios de LSA que coincidan con la subred y haga clic en **ACEPTAR**. Repita esta acción para añadir intervalos adicionales.

STEP 5 | Configure las interfaces de áreas para el protocolo OSPF.

1. En la pestaña **Interface (Interfaz)**, haga clic en **Add (Añadir)** e ingrese la siguiente información para cada interfaz que se incluirá en el área:
   - **Interface (Interfaz)**: seleccione una interfaz.
   - **Enable (Habilitar)**: al seleccionar esta opción, la configuración de la interfaz OSPF surte efecto.
   - **Passive**: seleccione esta opción si no desea que la interfaz OSPF envíe o reciba paquetes OSPF. Aunque los paquetes OSPF no se envían ni reciben, si selecciona esta opción, la interfaz se incluirá en la base de datos de LSA.
   - **Link type**: seleccione **Broadcast** si desea poder acceder a todos los vecinos mediante la interfaz y poder detectarlos automáticamente por mensajes de saludo OSPF de multidifusión, como una interfaz Ethernet. Seleccione **p2p** (punto a punto) para descubrir al vecino automáticamente. Elija **p2mp** (punto a multipunto) cuando los vecinos deban definirse manualmente y seleccione **Add (Añadir)** para añadir las direcciones IP vecinas para todos los vecinos cercanos a través de esta interfaz.
   - **Metric**: introduzca una métrica OSPF para esta interfaz (el intervalo es 0-65.535; el valor por defecto es 10).
   - **Prioridad**: Introduzca una prioridad de OSPF para esta interfaz. Esta es la prioridad del enrutador para ser el enrutador designado (DR) o de reserva (BDR) según el protocolo OSPF (intervalo: 0-255; predeterminado: 1). Si el valor se configura como cero, el enrutador no se designará como DR ni BDR.
   - **Auth Profile**: seleccione un perfil de autenticación definido previamente.
   - **Timing (Sincronización)**: modifique los ajustes de sincronización si lo desea (no recomendado). Si desea obtener información detallada sobre estos ajustes, consulte la ayuda en línea.
2. Haga clic en **OK (Aceptar)**.

STEP 6 | Configure enlaces virtuales de áreas.

1. En la pestaña **Virtual Link (Enlace virtual)**, haga clic en **Add (Añadir)** e ingrese la siguiente información para cada enlace virtual que se incluirá en el área troncal:
   - **Name**: introduzca un nombre para el enlace virtual.
   - **Enable**: seleccione para habilitar el enlace virtual.
   - **Neighbor ID**: introduzca el ID del enrutador (vecino) del otro lado del enlace virtual.
   - **Transit Area**: introduzca el ID del área de tránsito que contiene físicamente al enlace virtual.

© 2020 Palo Alto Networks, Inc.

- **Timing**: es recomendable que mantenga su configuración temporal por defecto.
- **Auth Profile**: seleccione un perfil de autenticación definido previamente.

2. Haga clic en **OK (Aceptar)** para guardar los enlaces virtuales.
3. Haga clic en **OK (Aceptar)** para guardar el área.

STEP 7 | (Opcional) Configure perfiles de autenticación.

De manera predeterminada, el cortafuegos no utiliza autenticación de OSPF para el intercambio entre vecinos OSPF. Opcionalmente, puede configurar una autenticación de OSPF entre vecinos OSPF mediante una contraseña simple o mediante la autenticación MD5. Se recomienda la autenticación MD5; es más segura que una contraseña simple.

Autenticación de contraseña simple de OSPF

1. Seleccione la pestaña **Auth Profiles (Perfiles de autenticación)** y luego **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPF.
2. Seleccione Contraseña simple como Tipo de contraseña.
3. Introduzca una contraseña simple y, a continuación, confírmela.

Autenticación MD5 de OSPF

1. Seleccione la pestaña **Auth Profiles (Perfiles de autenticación)** y luego **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPF.
2. Seleccione **MD5** como el **Password Type (Tipo de contraseña)** y luego **Add (Añadir)** para añadir una o más entradas de contraseña, incluidas las siguientes:
   - ID de clave (intervalo: 0-255)
   - Clave
   - Seleccione la opción Preferido para especificar que la clave debe utilizarse para autenticar mensajes salientes.
3. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure las opciones avanzadas de OSPF.

1. En la pestaña **Advanced (Avanzado)**, seleccione **RFC 1583 Compatibility (Compatibilidad con RFC 1583)** para garantizar la compatibilidad con RFC 1583.
2. Especifique un valor para el temporizador **SPF Calculation Delay (sec) (Retardo de cálculo SPF [s])**, que le permite definir el retraso de tiempo (en segundos) entre la recepción de nueva información de topología y la ejecución de un cálculo SPF. Los valores menores permiten una reconvergencia OSPF más rápida. Los enrutadores que se emparejan con el cortafuegos deben usar el mismo valor de retardo para optimizar los tiempos de convergencia.
3. Especifique un valor para el temporizador **LSA Interval (sec) (Intervalo LSA [s])**, que es el tiempo mínimo entre las transmisiones de dos instancias del mismo LSA (mismo enrutador, mismo tipo, mismo ID de LSA). Es un equivalente de MinLSInterval en RFC 2328. Los valores más bajos se pueden utilizar para reducir los tiempos de reconvergencia cuando se producen cambios en la tipología.
4. Haga clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios.

Configuración de OSPFv3

OSPF admite IPv4 e IPv6. Usted debe usar OSPFv3 si está utilizando IPv6.

STEP 1 | Configure los ajustes de configuración general de enrutador virtual.

Consulte Enrutadores virtuales para obtener más información.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Configure los ajustes de configuración general de OSPFv3.

1. Seleccione la pestaña **OSPFv3**.
2. Seleccione **Enable** para habilitar el protocolo OSPF.
3. Introduzca el **Router ID (Identificador de enrutador)**.
4. Seleccione la casilla **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta por defecto a través de OSPFv3. Este es el ajuste por defecto recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas predeterminadas a través de OSPFv3.

STEP 3 | Configure el perfil de autenticación para el protocolo OSPFv3.

OSPFv3 no incluye ninguna capacidad de autenticación propia; se basa completamente en IPSec para proteger las comunicaciones entre vecinos.

Al configurar un perfil de autenticación, debe utilizar una carga de seguridad encapsulada (Encapsulating Security Payload, ESP) o un encabezado de autenticación (Authentication Header, AH) de IPv6.

Autenticación de ESP OSPFv3

1. En la pestaña **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPFv3.
2. Especifique un índice de política de seguridad (**SPI**) (valor hexadecimal en el intervalo de 00000000 a FFFFFFFF). Los dos extremos de la adyacencia OSPFv3 debe incluir valores SPI coincidentes.
3. Seleccione **ESP** como **Protocol (Protocolo)**.
4. Seleccione el valor adecuado en **Crypto Algorithm (Algoritmo criptográfico)**.

   Puede seleccionar **None (Ninguno)** o alguno de los siguientes algoritmos: SHA1, SHA256, SHA384, SHA512 o MD5.
5. Si se seleccionó un **Crypto Algorithm (Algoritmo criptográfico)** en lugar de no seleccionar ningún valor, ingrese un valor para **Key (Clave)** y, a continuación, confírmelo.

Autenticación de AH OSPFv3

1. En la pestaña **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPFv3.
2. Especifique un índice de política de seguridad (**SPI**). El SPI debe coincidir entre ambos extremos de la adyacencia de OSPFv3. El número del SPI debe ser un valor hexadecimal entre 00000000 y FFFFFFFF.
3. Seleccione **AH** como **Protocolo**.
4. Seleccione el valor adecuado en **Crypto Algorithm (Algoritmo criptográfico)**.

   Debe introducir uno de los siguientes algoritmos: SHA1, SHA256, SHA384, SHA512 o MD5.
5. Introduzca un valor para **Clave** y, a continuación, confírmelo.
6. Haga clic en **OK (Aceptar)**.
7. Vuelva a hacer clic en **OK (Aceptar)** en el cuadro de diálogo Enrutador virtual - OSPF - Perfil de autenticación.

STEP 4 | Configure Areas - Type (Áreas - Tipo) para el protocolo OSPFv3.

1. En la pestaña **Areas (Áreas)**, seleccione **Add (Añadir)** para añadir un **Area ID (Identificador de área)**. Es el identificador que cada vecino debe aceptar para formar parte de la misma área.
2. En la pestaña **General**, seleccione una de las siguientes opciones de la lista **Type (Tipo)** del área:

   - **Normal**: no hay restricciones; el área puede aceptar todos los tipos de rutas.
   - **Stub (Código auxiliar)**: no hay salida desde el área. Para acceder a un destino fuera del área, es necesario atravesar el límite, que conecta con el resto de áreas. Si selecciona esta opción, configure lo siguiente:

© 2020 Palo Alto Networks, Inc.

- **Aceptar resumen**: Los anuncios de estado de enlaces (LSA) se aceptan desde otras áreas. Si esta opción de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está deshabilitada, el área OSPF se comportará como un área totalmente de código auxiliar (TSA) y ABR no propagará ninguno de los LSA de resumen.
- **Advertise Default Route (Anunciar ruta predeterminada)**: los LSA de ruta por defecto se incluirán en los anuncios al área de código auxiliar junto con un valor de medida configurado dentro del intervalo configurado 1-255.

- **NSSA**: el cortafuegos solamente puede salir del área por rutas que no sean rutas de OSPF. Si está seleccionado, configure Aceptar resumen y Anunciar ruta predeterminada como se describe para Código auxiliar. Si selecciona esta opción, configure lo siguiente:
  - **Type (Tipo)**: Seleccione el tipo de ruta **Ext 1** o **Ext 2** para anunciar el LSA predeterminado.
  - **Ext Ranges (Intervalos extendidos)**: haga clic en **Add (Añadir)** para añadir intervalos de rutas externas para los que desee habilitar o suprimir los anuncios.

STEP 5 | Asocie un perfil de autenticación OSPFv3 a un área o una interfaz.

Para un área

1. En la pestaña **Areas (Áreas)**, seleccione un área existente de la tabla.
2. En la pestaña **General**, seleccione un perfil definido previamente con la opción **Authentication Profile (Perfil de autenticación)** de la lista **Authentication (Autenticación)**.
3. Haga clic en **OK (Aceptar)**.

Para una interfaz

1. En la pestaña **Areas (Áreas)**, seleccione un área existente de la tabla.
2. Seleccione la pestaña **Interface (Interfaz)** y haga clic en **Add (Añadir)** para añadir el perfil de autenticación que desea asociar a la interfaz de OSPF de la lista **Auth Profile (Perfil de autenticación)**.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar la configuración del área.

STEP 7 | (Opcional) Configure reglas de exportación.

1. En la pestaña **Export Rules (Reglas de exportación)**, seleccione **Allow Redistribute Default Route (Permitir redistribución de ruta predeterminada)** para permitir la redistribución de rutas predeterminadas a través de OSPFv3.
2. Haga clic en **Add (Añadir)**.
3. Ingrese un nombre en **Name**: el valor debe ser una subred IPv6 válida o un nombre de perfil de redistribución válido.
4. Seleccione **New Path Type (Nuevo tipo de ruta)**, **Ext 1** o **Ext 2**.
5. Especifique una **New Tag (Nueva etiqueta)** para la ruta coincidente que tenga un valor de 32 bits en notación decimal con punto.
6. Asigne una **Metric (Métrica)** para la nueva regla (el intervalo es 1 a 16,777,215).
7. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure las opciones avanzadas de OSPFv3.

1. En la pestaña **Advanced (Avanzado)** seleccione la casilla de verificación **Disable Transit Routing for SPF Calculation (Deshabilitar el enrutamiento de tránsito para el cálculo de SPF)** si desea que el cortafuegos participe en la distribución de la topología de OSPF sin ser utilizado para reenviar tráfico de tránsito.
2. Especifique un valor para el temporizador **SPF Calculation Delay (sec) (Retardo de cálculo SPF [s])**, que le permite definir el retraso de tiempo (en segundos) entre la recepción de nueva información de topología y la ejecución de un cálculo SPF. Los valores menores permiten una reconvergencia

© 2020 Palo Alto Networks, Inc.

OSPF más rápida. Los enrutadores que se emparejan con el cortafuegos deben usar el mismo valor de retardo para optimizar los tiempos de convergencia.

3. Especifique un valor para el temporizador **LSA Interval (sec) (Intervalo LSA [s])**, que es el tiempo mínimo (en segundos) entre las transmisiones de dos instancias del mismo LSA (mismo enrutador, mismo tipo, mismo ID de LSA). Es un equivalente de MinLSInterval en RFC 2328. Los valores más bajos se pueden utilizar para reducir los tiempos de reconvergencia cuando se producen cambios en la tipología.
4. (Opcional) Configuración del reinicio correcto de OSPF.
5. Haga clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios.

Configuración del reinicio correcto de OSPF

El reinicio correcto de OSPF dirige a los vecinos OSPF para que sigan utilizando rutas mediante un cortafuegos durante una breve transición cuando esté fuera de servicio. Este comportamiento aumenta la estabilidad de red reduciendo la frecuencia de reconfiguración de la tabla de enrutamiento y los flaps de ruta relacionados que pueden producirse durante breves tiempos de inactividad periódicos.

Para un cortafuegos de Palo Alto Networks, el reinicio correcto de OSPF implica las siguientes operaciones:

- **Cortafuegos como dispositivo de reinicio**: si el cortafuegos estará inactivo durante un breve periodo de tiempo o no estará disponible durante intervalos breves, enviará LSA de gracia a sus vecinos OSPF. Los vecinos deben configurarse para ejecutarse en modo auxiliar de reinicio correcto. En el modo auxiliar, los vecinos reciben los LSA de gracia que le informan de que el cortafuegos realizará un reinicio correcto en un periodo de tiempo especificado definido como el **Periodo de gracia**. Durante el periodo de gracia, el vecino sigue reenviando rutas a través del cortafuegos y enviando LSA que anuncian rutas a través del cortafuegos. Si el cortafuegos reanuda su funcionamiento antes de que venza el periodo de gracia, el reenvío de tráfico seguirá como antes sin ninguna interrupción de la red. Si el cortafuegos no reanuda su funcionamiento después de que venza el periodo de gracia, los vecinos saldrán del modo auxiliar y reanudarán el funcionamiento normal, lo que implicará la reconfiguración de la tabla de enrutamiento para eludir el cortafuegos.
- **Cortafuegos como auxiliar de reinicio correcto:** si es posible que los enrutadores vecinos estén inactivos durante breves períodos de tiempo, se puede configurar el cortafuegos para que funcione en el modo auxiliar de reinicio correcto, en cuyo caso, el cortafuego emplea un **Max Neighbor Restart Time (Tiempo de reinicio máximo de vecinos)**. Cuando el cortafuegos reciba los LSA de gracia de su vecino OSPF, seguirá enrutando tráfico hacia el vecino y anunciando rutas a través del vecino hasta que venza el periodo de gracia o hasta alcanzar el tiempo máximo de reinicio del mismo nivel. Si ninguno de los dos vence antes de que el vecino vuelva a estar en funcionamiento, el reenvío de tráfico continuará como antes sin ninguna interrupción de la red. Si ninguno de los dos periodos vence antes de que el vecino vuelva a estar en funcionamiento, el cortafuegos saldrá del modo auxiliar y reanudará el funcionamiento normal, lo que implicará la reconfiguración de la tabla de enrutamiento para eludir el vecino.

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que desea configurar.

STEP 2 | Seleccione **OSPF** > **Advanced (Avanzado)** o **OSPFv3** > **Advanced (Avanzado)**.

STEP 3 | Verifique que las siguientes casillas de verificación están seleccionadas (están habilitadas por defecto):

- **Habilitar reinicio correcto**
- **Habilitar modo auxiliar**

© 2020 Palo Alto Networks, Inc.

- **Habilitar comprobación de LSA estricta**

Las tres opciones deberían permanecer seleccionadas a menos que su topología requiera lo contrario.

STEP 4 | Configure un **Período de gracia** en segundos.

STEP 5 | Configure un **Max Neighbor Restart Time (Tiempo máx. de reinicio del mismo nivel)** en segundos.

Confirmación del funcionamiento de OSPF

Una vez se haya compilado una configuración de OSPF, podrá utilizar cualquiera de las operaciones siguientes para confirmar que OSPF está funcionando:

- Visualización de la tabla de enrutamiento
- Confirmación de adyacencias OSPF
- Confirmación de que se han establecido conexiones OSPF

Visualización de la tabla de enrutamiento

Al visualizar la tabla de enrutamiento, puede ver si se han establecido rutas OSPF. Se puede acceder a la tabla de enrutamiento desde la interfaz web o la CLI. Si está utilizando la CLI, utilice los siguientes comandos:

- `show routing route`
- `show routing fib`

Si utiliza la interfaz web para ver la tabla de enrutamiento, utilice el siguiente flujo de trabajo:

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la misma fila del enrutador virtual en el que está interesado, haga clic en el enlace **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 2 | Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de rutas)** y examine la columna **Flags (Marcas)** de la tabla de enrutamiento para determinar qué rutas ha obtenido OSPF.

Confirmación de adyacencias OSPF

Utilice el siguiente flujo de trabajo para confirmar que se establezcan las adyacencias OSPF:

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la misma fila del enrutador virtual en el que está interesado, haga clic en el enlace **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 2 | Seleccione **OSPF** > **Neighbor (Vecino)** y examine la columna **Status (Estado)** para determinar si se establecieron adyacencias OSPF.

Confirmación de que se han establecido conexiones OSPF

Visualice el log del sistema para confirmar que el cortafuegos haya establecido conexiones OSPF.

STEP 1 | Seleccione **Monitor (Supervisar)** > **System (Sistema)** y observe los mensajes para confirmar que se establecieron adyacencias OSPF.

STEP 2 | Seleccione **OSPF** > **Neighbor (Vecino)** y examine la columna **Status (Estado)** para determinar si se establecieron adyacencias OSPF (completas).

© 2020 Palo Alto Networks, Inc.

BGP

El protocolo de gateway de borde (BGP) es el principal protocolo de enrutamiento de Internet. BGP determina el alcance de la red en función de los prefijos IP que están disponibles en sistemas autónomos (AS), donde un sistema autónomo es un conjunto de prefijos IP que un proveedor de red ha designado para formar parte de una política de enrutamiento simple.

- Descripción general del BGP
- MP-BGP
- Configuración de BGP
- Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6
- Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4
- Confederaciones BGP

Descripción general del BGP

El BGP funciona entre sistemas autónomos (BGP externo o eBGP) o dentro de un AS (BGP interno o iBGP) para intercambiar información de enrutamiento y alcance con los emisores del BGP. El cortafuegos proporciona una implementación completa de BGP que incluye las siguientes funciones:

- Especificación de una instancia de enrutamiento BGP por enrutador virtual.
- Configuración de BGP por enrutador virtual, que incluye parámetros básicos como ID de ruta local y AS local, y opciones avanzadas como selección de ruta, reflector de ruta, confederaciones BGP, amortiguación de flap de ruta y reinicio correcto.
- Configuración de vecino y grupos de peers, que incluye direcciones de vecino y AS remotos, y opciones avanzadas como atributos y conexiones de vecino.
- Políticas de enrutamiento para controlar los procesos de importación, exportación y anuncios de rutas; filtrado basado en prefijos; y agregación de direcciones.
- Interacción IGP-BGP para introducir rutas en BGP utilizando perfiles de redistribución.
- Perfiles de autenticación que especifican la clave de autenticación MD5 para conexiones BGP. La autenticación permite prevenir fugas de rutas y ataques exitosos al DoS.
- El BGP multiprotocolo (MP-BGP), que permite a los peers de BGP transportar rutas de unidifusión IPv6 y rutas de multidifusión IPv4 en paquetes de actualización, y permite al cortafuegos y a un peer de BGP comunicarse entre sí mediante direcciones IPv6.

MP-BGP

BGP admite prefijos de unidifusión IPv4, pero una red BGP que utiliza rutas multidifusión IPv4 o prefijos de unidifusión IPv6 necesita BGP multiptotocolo (MP-BGP) a fin de intercambiar rutas de tipos de direcciones que no sean unidifusión IPv4. MP-BGP permite a los peers BGP que transporten rutas multidifusión IPv4 y rutas unidifusión IPv6 en paquetes de actualización, además de las rutas unidifusión IPv4 que los peers BGP pueden transportar sin habilitar MP-BGP.

De esta manera, MP-BGP proporciona conectividad IPv6 para sus redes BGP que utilizan IPv6 nativa o IPv4 e IPv6 de pila doble. Los proveedores de servicio pueden ofrecer servicio IPv6 a sus clientes y las empresas pueden usar servicio IPv6 de los proveedores de servicio. El cortafuegos y un peer BGP pueden comunicarse entre sí usando direcciones IPv6.

A fin de que BGP admita protocolos de capa de red múltiples (que no sea BGP para IPv4), extensiones multiprotocolo para BGP-4 (RFC 4760), utilice la información de disponibilidad de capa de red (Network Layer Reachability Information, NLRI) en un atributo NLRI alcanzable multiprotocolo que el cortafuegos envía y recibe en paquetes de actualización BGP. El atributo contiene información sobre el prefijo de destino, incluidos estos dos identificadores:

© 2020 Palo Alto Networks, Inc.

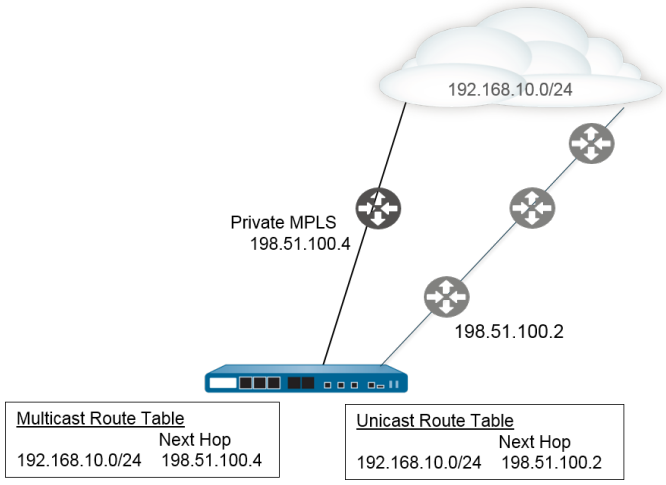
- El identificador de familia de direcciones (Address Family Identifier, AFI), según se define en IANA en Números de familia de direcciones, indica que el prefijo de destino es una dirección IPv4 o IPv6. (PAN-OS admite AFI IPv4 e IPv6).
- El identificador de familia de direcciones posterior (SAFI) en PAN-OS indica que el prefijo de destino es una dirección de unidifusión o multidifusión (si AI es IPv4) o que el prefijo de destino es una dirección de unidifusión (si el AFI es IPv6). PAN-OS no admite multidifusión IPv6.

Si usted habilita MP-BGP para la multidifusión IPV4 o si configura una ruta est´tica de multidifusión, el cortafuegos admite tablas de ruta de unidifusión y multidifusión separadas para las rutas estáticas. Es posible que desee separar el tráfico de unidifusión y multidifusión que va al mismo destino. El tráfico de multidifusión puede tomar una ruta diferente del tráfico de unidifusión ya que, por ejemplo, su tráfico de multidifusión es crítico, por lo que debe ser más eficiente, con menos saltos, o someterse a una menor latencia.

También puede ejercer más control sobre el funcionamiento de BGP al configurar BGP para que utilice rutas solo de la tabla de rutas de unidifusión o multidifusión (o ambas) cuando BGP importa o exporta rutas, envía anuncios condicionales o realiza la redistribución o agregación de rutas.

Usted puede decidir usar un RIB de multidifusión (tabla de rutas) al habilitar MP-BGP y seleccionar la familia de direcciones de IPv4 y la familia de direcciones posteriores de multidifusión, o al instalar una ruta estática IPv4 en la tabla de rutas de multidifusión. Después de aplicar cualquiera de los métodos para usar el RIB de multidifusión, el cortafuegos usa el RIB de multidifusión para todo el enrutamiento de multidifusión y envío de rutas inverso (RPF). Si prefiere usar el RIB de unidifusión para todo el enrutamiento (unidifusión y multidifusión) no debe habilitar el RIB de multidifusión por ninguno de los métodos.

En la siguiente figura, una ruta estática a 192.168.10.0/24 está instalada en la tabla de ruta de unidifusión, y el siguiente salto es 198.51.100.2. Sin embargo, el tráfico de multidifusión puede tomar una ruta diferente a una nube MPLS privada; la misma ruta estática está instalada en la tabla de rutas de multidifusión con un salto siguiente diferente (198.51.100.4), por lo que la ruta es diferente.



El uso de tablas de rutas de unidifusión y multidifusión separadas le brinda mayor flexibilidad y control cuando configura estas funciones BGP:

- Instale una ruta estática IPv4 en la tabla de rutas de unidifusión o multidifusión, o ambas, según se describió en el ejemplo anterior. (Puede instalar una ruta estática IPv6 en la tabla de ruta de unidifusión únicamente).
- Cree una regla de importación para que cualquier prefijo que coincida con los criterios se importen en la tabla de rutas de unidifusión o multidifusión, o ambas.
- Cree una regla de exportación para que cualquier prefijo que coincida con los criterios se exporten (envíen al peer) desde la tabla de rutas de unidifusión o multidifusión, o ambas.

© 2020 Palo Alto Networks, Inc.

- Configure un anuncio condicional con un filtro no existente, para que el cortafuegos busque la tabla de ruta de unidifusión o multidifusión (o ambas) para garantizar que la ruta no exista en la tabla y el cortafuegos anuncie una ruta diferente.
- Configure un anuncio condicional con un filtro de anuncio, de manera que el cortafuegos anuncie rutas que coincidan con los criterios de la tabla de rutas de unidifusión o multidifusión, o ambas.
- Redistribuya una ruta que aparezca en la tabla de rutas de unidifusión o multidifusión, o ambas.
- Configure la agregación de rutas con un filtro de anuncio, de manera que las rutas agregadas que deben anunciarse provengan de la tabla de rutas de unidifusión o multidifusión, o ambas.
- A la inversa, configure la agregación de rutas con un filtro de supresión, de manera que las rutas agregadas que deben suprimirse (no anunciarse) provengan de la tabla de rutas de unidifusión o multidifusión, o ambas.

Cuando configura un peer con MP_BGP utilizando una familia de direcciones de IPv6, puede usar direcciones IPv6 en los campos de prefijo de dirección y próximo salto de una regla de importación, regla de exportación, anuncio condicional (filtro de anuncio y filtro no existente), y regla de agregación (filtro de anuncio, filtro de supresión y atributo de ruta de agregación).

Configuración de BGP

Realice la siguiente tarea para configurar BGP.

STEP 1 | Configure los ajustes de configuración general de enrutador virtual.

Consulte Enrutadores virtuales para obtener información detallada.

STEP 2 | Habilite BGP para el enrutador virtual, asigne una ID de enrutador y asigne el enrutador virtual a un AS.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP**.
3. **Habilite** BGP para este enrutador virtual.
4. Asigne un **Router ID (ID de enrutador)** a BGP para el enrutador virtual, que generalmente es una dirección IPv4, para garantizar que el ID de enrutador sea único.
5. Asigne el **AS Number**, el número AS al que pertenece el enrutador virtual, en función del ID del enrutador (el intervalo es de 1 a 4 294 967 295).
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure los ajustes de configuración general de BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **General**.
3. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** para ignorar todas las rutas por defecto anunciadas por peers BGP.
4. Seleccione **Install Route (Instalar ruta)** para instalar rutas BGP en la tabla de enrutamiento global.
5. Seleccione **Aggregate MED (Agrupar MED)** para activar la agregación de rutas incluso si las rutas tienen valores diferentes valores de discriminador de salida múltiple (Multi-Exit Discriminator, MED).
6. Especifique la **Default Local Preference (Preferencia local predeterminada)** que se puede utilizar para determinar preferencias entre las diferentes rutas.
7. Seleccione el **AS Format (Formato AS)** para fines de interoperabilidad:
   - **2 bytes** (predeterminado)
   - **4 bytes**

   Las estadísticas de tiempo de ejecución muestran números AS de 4 bytes de BGP con una notación simple de acuerdo con RFC 5396.

© 2020 Palo Alto Networks, Inc.

8. Habilite o deshabilite cada uno de los siguientes ajustes de **Path Selection (Selección de rutas)**:
   - **Always Compare MED (Comparar siempre MED)**: habilite esta comparación para elegir rutas de vecinos en diferentes sistemas autónomos.
   - **Comparación determinista de MED**: Habilite esta comparación para elegir entre rutas anunciadas por peers IBGP (peers BGP en el mismo sistema autónomo).
9. Para los **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un perfil de autenticación:
   - **Profile Name**: introduzca un nombre para identificar el perfil.
   - **Secret/Confirm Secret (Secreto/Confirmar secreto)**: Introduzca y confirme la contraseña para comunicaciones de peer BGP. El secreto se utiliza como clave en una autenticación MD5.
10. Haga clic en **OK** dos veces.

STEP 4 | (Opcional) Configure los ajustes de BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Advanced (Avanzado)**.
3. Seleccione **ECMP Multiple AS Support (Compatibilidad AS múltiple de ECMP)** si configuró ECMP y desea ejecutar ECMP en varios sistemas BGP autónomos.
4. Seleccione **Enforce First AS for EBGP (Aplicar primero AS para EBGP)** (habilitado de forma predeterminada) para que el cortafuegos descarte un paquete de actualización entrante de un peer de eBGP que no enumera el propio número AS del peer de eBGP como el primer número de AS en el atributo AS_PATH.
5. Seleccione **Graceful Restart (Reinicio correcto)** y configure los siguientes temporizadores:
   - **Stale Route Time (sec) (Tiempo de ruta obsoleto (s))**: especifica la cantidad de tiempo en segundos que una ruta puede permanecer en el estado obsoleto (el intervalo es de 1 a 3600; el valor predeterminado es 120).
   - **Local Restart Time (sec) (Hora de reinicio local (s))**: especifica la cantidad de tiempo en segundos que el dispositivo local tarda en reiniciar. Este valor se les comunica a los peers (el intervalo es de 1 a 3600; el valor predeterminado es 120).
   - **Max Peer Restart Time (sec) (Máx. de hora de reinicio del peer (s))**: especifica el tiempo máximo en segundos que el dispositivo local acepta como periodo de gracia para reiniciar los dispositivos peer (el intervalo es 1 de 3600; el valor predeterminado es 120).
6. Para **Reflector Cluster ID (ID de clúster reflector)**, especifique un identificador IPv4 para representar el clúster reflector.
7. Para **Confederation Member AS (AS de miembro de confederación)**, especifique el identificador de número de sistema autónomo (también se denomina número de sistema subautónomo), visible únicamente en la confederación BGP. Para obtener más información, consulte Confederaciones BGP.
8. Haga clic en **Add (Añadir)**para introducir la siguiente información para cada perfil de amortiguación que quiera configurar, seleccione **Enable (Habilitar)** y haga clic en **OK (Aceptar)**:
   - **Profile Name**: introduzca un nombre para identificar el perfil.
   - **Cutoff (Corte)**: especifique un umbral retirada de ruta por encima del que se suprime un anuncio de ruta (el intervalo es de 0,0 a 1000; el valor predeterminado es 1,25).
   - **Reuse (Reutilizar)**: especifique un umbral de retirada de ruta por debajo del cual una ruta suprimida se vuelve a utilizar (el intervalo es de 0,0 a 1000; el valor predeterminado es 5).
   - **Max Hold Time (sec) (Máx. de tiempo de espera (s))**: especifique el tiempo máximo en segundos durante el que una ruta se puede suprimir, independientemente de su inestabilidad (el intervalo es de 0 a 3600; el valor predeterminado es 900).
   - **Decay Half Life Reachable (sec) (Media vida de disminución alcanzable (s))**: especifique el tiempo en segundos después del cual la métrica de estabilidad de una ruta se divide entre dos si la ruta se considera alcanzable (el intervalo es de 0 a 3600; el valor predeterminado es 300).

© 2020 Palo Alto Networks, Inc.

- **Decay Half Life Reachable (sec) (Media vida de disminución no alcanzable (s))**: especifique el tiempo después del cual la métrica de estabilidad de una ruta se divide entre dos si la ruta se considera inalcanzable (el intervalo es de 0 a 3600; el valor predeterminado es 300).

9. Haga clic en **OK** dos veces.

STEP 5 | Configure el grupo del peer BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y **Add (Añadir)** para añadir un **nombre** para el grupo de peers y **habilítelo**.
3. Seleccione **Aggregated Confed AS Path** para incluir una ruta a la AS de confederación agregada configurada.
4. Seleccione **Soft Reset with Stored Info (Restablecimiento parcial con información almacenada)** para ejecutar un restablecimiento parcial del cortafuegos después de actualizar los ajustes de peer.
5. Seleccione el **Type (Tipo)** de grupo de peers.
   - IBGP: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP confederado: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP confederado: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP: Importar siguiente salto: Seleccione **Original** o **Use self**; y **Export Next Hop (Exportar siguiente salto)**: Especifique **Resolve (Resolver)** o **Use self (Utilizar automático)**. Seleccione **Remove Private AS (Eliminar AS privado)** si desea forzar que BGP elimine números AS privados del atributo AS_PATH en las actualizaciones que el cortafuegos envía a un peer en otro AS.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | Configure un peer BGP que pertenezca al grupo de peers y especifique su direccionamiento.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Para el peer, seleccione **Add (Añadir)** para añadir un peer por **Name (Nombre)**.
4. **Habilite** el peer.
5. Introduzca el **Peer AS** al cual pertenece el peer.
6. Seleccione **Addressing (Direccionamiento)**.
7. Para **Local Address (Dirección local)**, seleccione la **Interface (Interfaz)** para la cual está configurando BGP. Si la interfaz tiene más de una dirección **IP**, introduzca la dirección IP para que esa interfaz sea el peer BGP.
8. En **Peer Address (Dirección de peer)**, tiene dos opciones: seleccione **IP** e introduzca la dirección IP, seleccione un objeto de dirección o cree un objeto de dirección, o bien seleccione **FQDN** e introduzca el nombre de dominio completo (fully qualified domain name, FQDN) o un objeto de dirección del tipo FQDN.

   El cortafuegos solo emplea una dirección IP (de cada tipo de familia, esto es, IPv4 o IPv6) de la resolución de DNS del FQDN. Si se devuelven varias direcciones, el cortafuegos utiliza la dirección IP preferida que coincida con el tipo de familia de IP (IPv4 o IPv6) configurado para el peer de BGP. La dirección IP preferida es la primera dirección que devuelve el servidor DNS en su respuesta inicial. El cortafuegos la mantiene como preferida mientras siga apareciendo en las respuestas posteriores, aunque el orden sea distinto.

9. Haga clic en **OK (Aceptar)**.

STEP 7 | Configure los ajustes de conexión para el peer BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Seleccione el **Peer** que configuró.

© 2020 Palo Alto Networks, Inc.

4. Seleccione las **Connection Options (Opciones de conexión)**.
5. Seleccione un **Auth Profile (Perfil de autenticación)** para el peer.
6. **Keep Alive Interval (sec) (Mantener el intervalo activo (s))**: el intervalo (en segundos) después del cual las rutas de un peer se suprimen según el parámetro de tiempo de espera (el intervalo es de 0 a 1200; el valor predeterminado es 30).
7. Configure **Multi Hop (Salto múltiple)**, el valor del tiempo de vida (Time-To-Live, TTL) en el encabezado IP (el intervalo es de 0 a 255; el valor predeterminado es 0). El valor predeterminado de 0 significa 1 para iBGP. El valor predeterminado de 0 significa 255 para iBGP.
8. Configure **Open Delay Time (sec) (Tiempo de retardo de apertura (s))**, el retardo, en segundos, entre un protocolo TCP y el envío del cortafuegos del primer mensaje de apertura de BGP para establecer una conexión BGP (el intervalo es de 0 a 240; el valor predeterminado es 0).
9. Configure el **Hold Time (sec) (Tiempo de espera (s))**, el período, en segundos, que puede transcurrir entre mensajes Keepalive o de actualización sucesivos de un peer antes de cerrar la conexión del peer (el intervalo es de 3 a 3600; el valor predeterminado es 90).
10. Configure **Idle Hold Time (sec) (Tiempo de espera inactivo [s])**, el período de espera (en segundos) antes de reintentar conectarse al peer (el intervalo es de 1 a 3600; el valor predeterminado es 15).
11. En **Min Route Advertisement Interval (sec) (Intervalo mínimo entre anuncios de rutas (s))**, establezca el número mínimo de segundos que debe transcurrir entre dos mensajes de actualización (Update) sucesivos que envíe el emisor de BGP (esto es, el cortafuegos) a un peer de BGP para anunciar que se han establecido o retirado rutas; el intervalo es de 1 a 600 y el valor predeterminado es 30.
12. Para **Incoming Connections (Conexiones entrantes)**, introduzca un **Remote Port (Puerto remoto)** y seleccione **Allow (Permitir)** para permitir el tráfico entrante a este puerto.
13. Para **Outgoing Connections (Conexiones salientes)**, introduzca un **Local Port (Puerto local)** y seleccione **Allow (Permitir)** para permitir el tráfico saliente de este puerto.
14. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure el peer BGP con los ajustes para el cliente reflector de ruta, tipo de emparejamiento, prefijos máximos y detección de reenvío bidireccional (BFD).

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Seleccione el **Peer** que configuró.
4. Seleccione **Advanced (Avanzado)**.
5. En **Reflector Client (Cliente reflector)**, seleccione una de las opciones siguientes:
   - **non-client (no cliente)** (predeterminado): el peer no es un cliente reflector de ruta.
   - **client (cliente)**: el peer es un cliente reflector de ruta.
   - **meshed-client (cliente en malla)**
6. Para **Peering Type (Tipo de emparejamiento)**, seleccione una de las siguientes opciones:
   - **Bilateral**: los dos peers BGP establecen una conexión de peer.
   - **Unspecified (No especificado)**: (predeterminado).
7. Para los **Max Prefixes (Prefijos máximos)**, introduzca la cantidad máxima de prefijos IP admitidos (el intervalo es de 1 a 100 000) o seleccione **unlimited (ilimitado)**.
8. Para habilitar **BFD** para el peer (y por lo tanto, cancelar la configuración BFD por BGP, siempre que BFD no esté deshabilitado para BGP a nivel del enrutador virtual), seleccione una de las siguientes opciones:
   - **default (predeterminado)**: usa únicamente los ajustes BFD por defecto.
   - **Inherit-vr-global-setting (Heredar ajuste global para el enrutador virtual)** (valor predeterminado): el peer hereda el perfil BFD que usted seleccionó globalmente para BGP para el enrutador virtual.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

© 2020 Palo Alto Networks, Inc.



Seleccione Disable BFD (Deshabilitar BFD) para deshabilitar el peer de BGP.

9. Haga clic en **OK (Aceptar)**.

STEP 9 | Configure reglas de importación y exportación.

Las reglas de importación y exportación se utilizan para importar y exportar rutas desde otros enrutadores y hacia otros enrutadores (por ejemplo, mediante la importación la ruta predeterminada desde su proveedor de servicios de Internet).

1. Seleccione **Import (Importar)** y **añada** un nombre en el campo **Rules (Reglas)**, y **habilite** la regla de importación.
2. Haga clic en **Add (Añadir)** y seleccione el **Peer Group (Grupo del peer)** desde el que se importarán las rutas.
3. Seleccione **Match (Coincidencia)** y defina las opciones utilizadas para filtrar la información de enrutamiento. También puede definir el valor de discriminador de salida múltiple (MED) y un valor de siguiente salto como enrutadores o subredes para el filtrado de rutas. La opción MED es una medida externa que permite que los vecinos sepan cuál es la ruta preferida de un AS. Se prefiere un valor más bajo antes que un valor más alto.
4. Seleccione **Action (Acción)** y defina la acción que debería producirse (permitir o denegar) basándose en las opciones de filtrado definidas en la pestaña **Coincidencia**. Si selecciona **Deny (Denegar)**, no tendrá que definir ninguna opción adicional. Si selecciona **Allow (Permitir)**, tendrá que definir otros atributos.
5. Seleccione **Export (Exportar)** y defina atributos de exportación, que son similares a los ajustes de **Importar**, pero que se utilizan para controlar la información de rutas que se exporta desde el cortafuegos a los vecinos.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Configure los anuncios condicionales, que le permiten controlar la ruta que se anunciará en caso de que no exista ninguna ruta diferente en la tabla de enrutamiento BGP local (LocRIB), indicando un fallo de emparejamiento o alcance.

Esta función es útil si desea intentar forzar rutas de un AS a otro, por ejemplo, si tiene enlaces a Internet a través de varios ISP y desea enrutar el tráfico a un único proveedor, en lugar de a los otros, salvo que se produzca una pérdida de conectividad con el proveedor preferido.

1. Seleccione **Conditional Adv (Anuncio condicional)** y **añada** un nombre de **política**.
2. **Habilite** el anuncio condicional.
3. En la sección **Used By (Utilizado por)**, **añada** los grupos de peers que utilizarán la política de anuncios condicionales.
4. Seleccione **Non Exist Filter (Filtro no existente)** y defina los prefijos de red de la ruta preferida. De esta forma, se especifica la ruta que desea anunciar, si está disponible en la tabla de ruta de BGP local. Si un prefijo se va a anunciar y coincide con un filtro no existente, el anuncio se suprimirá.
5. Seleccione **Advertise Filters (Anunciar filtros)** y defina los prefijos de la ruta de la tabla de enrutamiento Local-RIB que se debería anunciar en caso de que la ruta del filtro no existente no esté disponible en la tabla de enrutamiento local. Si un prefijo se va a anunciar y no coincide con un filtro no existente, el anuncio se producirá.
6. Haga clic en **OK (Aceptar)**.

STEP 11 | Configure opciones agregadas para resumir rutas en la configuración de BGP.

La agregación de rutas de BGP se utiliza para controlar el modo en que BGP agrega direcciones. Cada entrada de la tabla da como resultado la creación de una dirección de agregación. El resultado será una entrada agregada en la tabla de enrutamiento cuando se obtiene al menos una ruta específica que coincide con la dirección especificada.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Aggregate (Agregación)** y **añada** un nombre para la dirección de agregación.
2. Especifique el **prefijo** de la red, que será el prefijo principal de los prefijos agregados.
3. Seleccione **Suppress Filters (Suprimir filtros)** y defina los atributos que harán que las rutas coincidentes se supriman.
4. Seleccione **Advertise Filters (Anunciar filtros)** y defina los atributos que harán que las rutas coincidentes se anuncien siempre a los peers.
5. Haga clic en **OK (Aceptar)**.

STEP 12 | Configure las reglas de redistribución.

Esta regla se utiliza para redistribuir las rutas de host y las rutas desconocidas que no se encuentran en la RIB local de los enrutadores de peers.

1. Seleccione **Redist Rules (Reglas de redistribución)** y **añada** una nueva regla de redistribución.
2. Especifique el **nombre** de una subred IP o seleccione un perfil de redistribución. Si es necesario, también puede configurar un perfil de redistribución nuevo.
3. Seleccione **Enable (Habilitar)** para habilitar la regla.
4. Especifique la **métrica** de ruta que se utilizará para la regla.
5. En la lista **Set Origin (Configurar origen)**, seleccione **incomplete (incompleto)**, **igp** o **egp**.
6. (Opcional) Establezca MED, la preferencia local, el límite de ruta AS y los valores de comunidad.
7. Haga clic en **OK (Aceptar)**.

STEP 13 | **Commit (Confirmar)** los cambios.

Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6

Después de configurar BGP, configure un peer BGP con MP-BGP para unidifusión IPv4 o IPv6 por cualquiera de los siguientes motivos:

- Para que su peer BGP transporte rutas de unidifusión IPv6, configure MP-BGP con el tipo de familia de dirección **IPv6** y la familia de direccion posterior **Unicast**, de manera que el peer pueda enviar actualizaciones BGP que incluyan rutas de unidifusión IPv6. Los peer BGP (dirección local y dirección de peer) pueden ser las direcciones IPv4 o las direcciones IPv6.
- Para realizar el emparejamiento de BGP en direcciones IPv6 (**Local Address [Dirección local]** y **Peer Address [Dirección de peer]** utilizan direcciones IPv6).

La siguiente tarea muestra cómo habilitar un peer BGP con MP-BGP para poder transportar rutas de unidifusión IPv6, y así poder emparejarlo usando direcciones IPv6.

La tarea también muestra cómo ver las tablas de ruta unidifusión o multidifusión, y cómo ver la tabla de reenvío, la RIB local de BGP y salida RIB de BGP (rutas enviada a vecinos) para ver las rutas de la tabla de rutas de unidifusión o multidifusión, o una familia de direcciones específica (IPv4 o IPv6).

STEP 1 | Habilite la extensiones MP-BGP para un peer.

Configure lo siguiente para que un peer de BGP pueda transportar rutas unidifusión IPv4 o IPv6 en paquetes de actualización y el cortafuegos pueda usar direcciones IPv4 o IPv6 para comunicarse con su peer.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **BGP**.
3. Seleccione **Peer Group (Grupo de peers)** y seleccione un grupo de peers.

© 2020 Palo Alto Networks, Inc.

4. Seleccione un peer BGP (enrutador).
5. Seleccione **Addressing (Direccionamiento)**.
6. Seleccione **Enable MP-BGP Extensions (Habilitar las extensiones MP-BGP)** para el peer.
7. En **Address Family Type (Tipo de familia de direcciones)**, haga clic en **IPv4** o **IPv6**. Por ejemplo, seleccione IPv6.
8. En **Subsequent Address Family (Familia de direcciones posteriores)**, se selecciona **Unicast (Unidifusión)**. Si elige **IPv4** para la familia de direcciones, puede seleccionar también **Multicast (Multidifusión)**.
9. En **Local Address (Dirección local)**, seleccione una **Interface (Interfaz)** y, opcionalmente, seleccione una dirección **IP**; por ejemplo, 2001:DB8:55::/32
10. En **Peer Address (Dirección de peer)**, introduzca la dirección **IP**, utilizando la misma familia de direcciones (IPv4 o IPv6) como la dirección local; por ejemplo, 2001:DB8:58::/32.
11. Seleccione **Advanced (Avanzado)**.
12. (Opcional) **Enable Sender Side Loop Detection (Habilitar detección de bucle en el lado del remitente)**. Cuando habilita la detección de bucle en el lado del remitente, el cortafuegos comprobará el atributo AS_PATH de una ruta en su FIB antes de enviar la ruta en una actualización, para asegurarse de que el número de AS del peer no esté en la lista AS_PATH. Si está, el cortafuegos lo elimina para evitar un bucle.
13. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cree una ruta estática e instálela en la tabla de rutas de unidifusión, ya que desea que la ruta se utilice solo para fines de unidifusión.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **Static Routes (Rutas estáticas)**, seleccione **IPv4** o **IPv6**, y luego **Add (Añadir)** para añadir una ruta.
3. Introduzca un nombre en **Name (Nombre)** para la ruta estática.
4. Introduzca el prefijo y la máscara de red de **Destination (Destino)** IPv4 o IPv6, según si elige IPv4 o IPv6.
5. Seleccione la salida **Interface (Interfaz)**.
6. Seleccione **Next Hop (Próximo salto)** como **IPv6 Address (Dirección IPv6)** (o **IP Address [Dirección IP]** si elige IPv4) e introduzca la dirección del siguiente salto al cual desea dirigir el tráfico de unidifusión para esta ruta estática.
7. Ingrese una **Admin Distance (Distancia de administrador)**.
8. Ingrese una **Metric (Métrica)**.
9. Para la **Route Table (Tabla de ruta)**, seleccione **Unicast (Unidifusión)**.
10. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

STEP 4 | Visualice la tabla de ruta de unidifusión o multidifusión.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de enrutamiento)**.
4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

© 2020 Palo Alto Networks, Inc.

La selección de Multicast (Multidifusión) con IPv6 Only (IPv6 únicamente) no es compatible.

STEP 5 | Visualice la tabla de reenvío.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Forwarding Table (Tabla de desvío)**.
4. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

STEP 6 | Visualice las tablas RIB de BGP.

1. Visualice la RIB local de BGP, que muestra las rutas BGP que el cortafuegos utiliza para enrutar paquetes BGP.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
   2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
   3. Seleccione **BGP** > **Local RIB**.
   4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
   5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

   La selección de Multicast (Multidifusión) con IPv6 Only (IPv6 únicamente) no es compatible.
2. Visualice la tabla de salida RIB de BGP, que muestra las rutas que el cortafuegos envía a los vecinos BGP.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
   2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
   3. Seleccione **BGP** > **RIB Out (Salida RIB)**.
   4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
   5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

   La selección de Multicast (Multidifusión) con IPv6 Only (IPv6 únicamente) no es compatible.

Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4

Tras la Configuración del BGP, configure un peer de BGP con MP-BGP para la ruta de multidifusión IPv4 si desea que su peer de BGP pueda aprender y pasar rutas de multidifusión IPv4 en las actualizaciones de BGP. Podrá separar el tráfico de rutas de unidifusión del de rutas de multidifusión, o emplear las funciones

© 2020 Palo Alto Networks, Inc.

enumeradas en el MP-BGP para utilizar solo rutas de la tabla de rutas de unidifusión o de multidifusión, o rutas de ambas tablas.

Si desea admitir solo tráfico de rutas de multidifusión, debe utilizar un filtro para eliminar el tráfico de rutas de unidifusión.

El cortafuegos no es compatible con el ECMP de tráfico de rutas de multidifusión.

STEP 1 | Habilite las extensiones del MP-BGP para que un peer de BGP puede intercambiar rutas de multidifusión IPv4.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **BGP**.
3. Seleccione **Peer Group (Grupo de peers)**, seleccione un grupo de peers y un peer de BGP.
4. Seleccione **Addressing (Direccionamiento)**.
5. Seleccione **Enable MP-BGP Extensions (Habilitación de las extensiones del MP-BGP)**.
6. En el campo **Address Family Type (Tipo de familia de dirección)**, seleccione **IPv4**.
7. En el campo **Subsequent Address Family (Familia de la dirección siguiente)**, seleccione **Unicast (Unidifusión)** y **Multicast (Multidifusión)**.
8. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cree una ruta estática IPv4 e instálela en la tabla de rutas de multidifusión únicamente.

Estos pasos se realizan para dirigir el tráfico de rutas de multidifusión de un peer de BGP a un siguiente salto específico, como se muestra en la topología en el MP-BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **Static Routes (Rutas estáticas)** > **IPv4** y **Add (Añadir)** para añadir un nombre en el campo **Name (Nombre)** para la ruta.
3. Introduzca el prefijo de **Destination (Destino)** IPv4 y la máscara de red.
4. Seleccione la salida **Interface (Interfaz)**.
5. Seleccione el **Next Hop (Siguiente salto)** como la **IP Address (Dirección IP)** e introduzca la dirección IP del siguiente salto al que desea dirigir el tráfico de rutas de multidifusión para esta ruta estática.
6. Ingrese una **Admin Distance (Distancia de administrador)**.
7. Ingrese una **Metric (Métrica)**.
8. En **Route Table (Tabla de rutas)**, seleccione **Multicast (Multidifusión)**.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

STEP 4 | Vea la tabla de rutas.

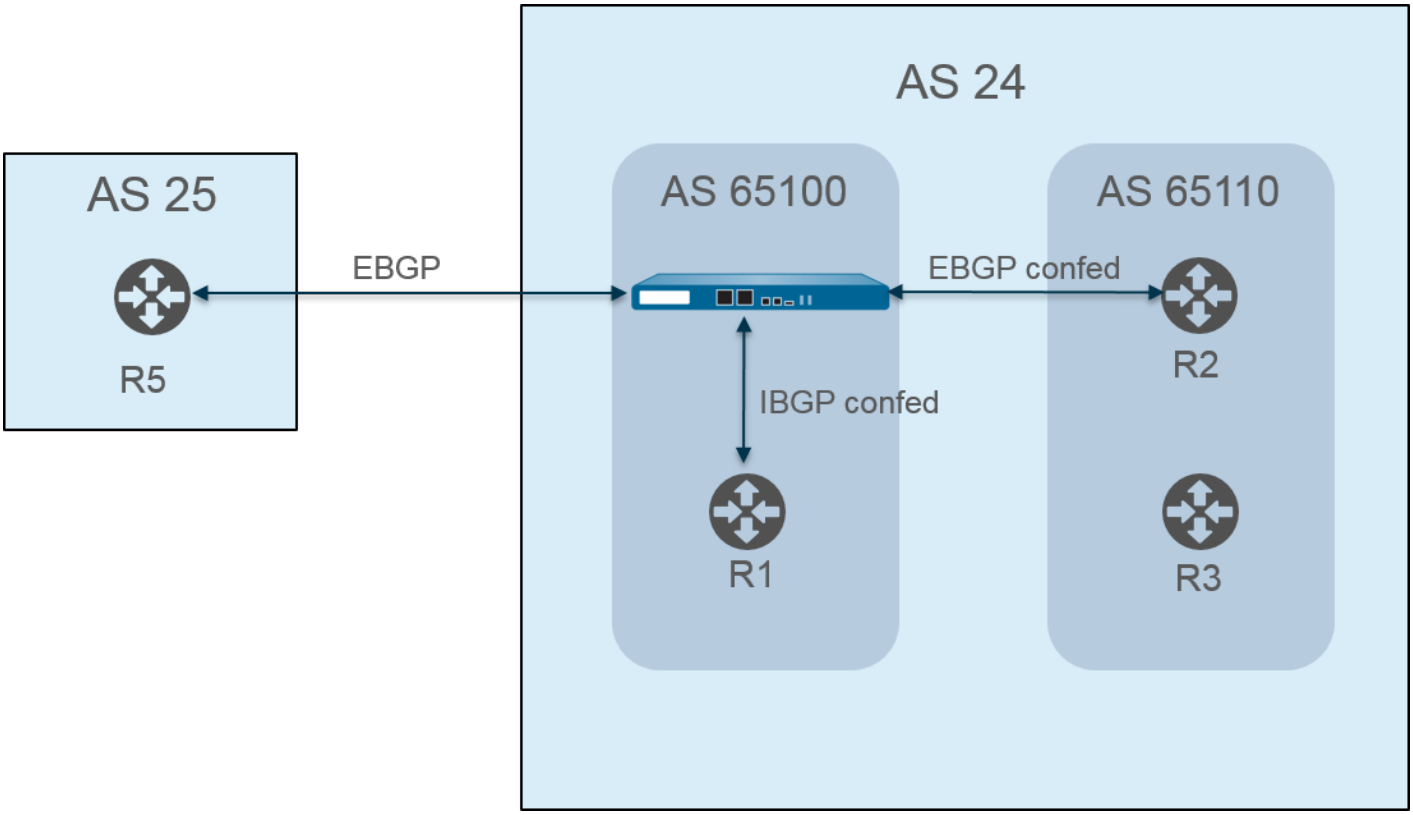
1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de enrutamiento)**.
4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Para ver la tabla de reenvío, la tabla de la RIB local del BGP o la tabla de salida de la RIB del BGP, consulte la Configuración de un peer de BGP con MP-BGP para rutas de unidifusión IPv4 o IPv6.

Confederaciones BGP

Las confederaciones BGP proporcionan una manera de dividir un sistema autónomo (autonomous system, AS) en dos o más sistemas subautónomos (sub-AS) para reducir la carga que provoca el requisito de malla completa de IBGP. Los cortafuegos (u otros dispositivos de enrutamiento) en un sistema subautónomo deben poseer una malla completa de iBGP con otros cortafuegos en el mismo sistema subautónomo. Es necesario el emparejamiento de BGP entre sistemas subautónomos para garantizar una conectividad completa en el sistema subautónomo principal. Los cortafuegos que se emparejan entre sí en un sistema subautónomo forman un emparejamiento de confederación IBGP. El cortafuegos en un sistema subautónomo que se empareja con un cortafuegos en un sistema subautónomo diferente forma un emparejamiento de confederación EBGP. Dos cortafuegos de diferentes sistemas autónomos que se conectan son peers de EBGP.



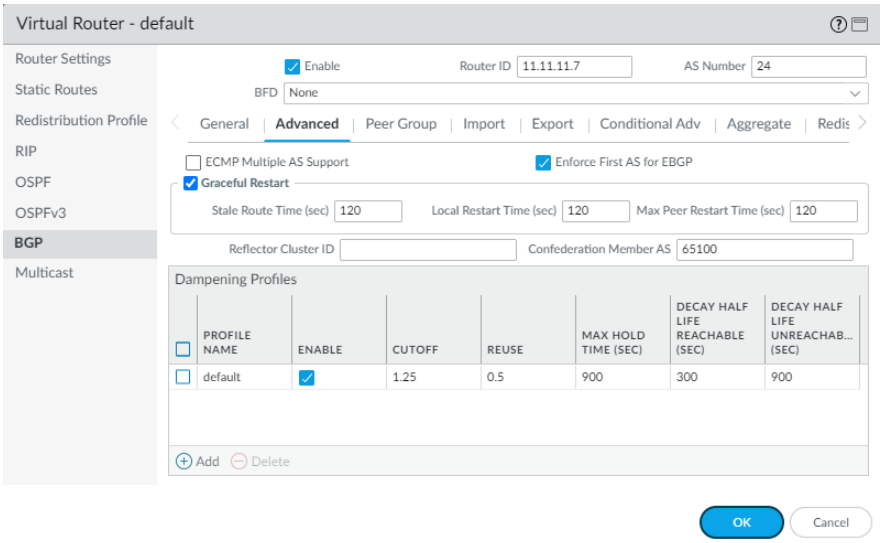
Los sistemas autónomos se identifican con un número de AS (asignado globalmente) público como AS 24 y AS 25 en la figura previa. En un entorno PAN-OS, asigne a cada sistema subautónomo un número de AS de miembro de la confederación único, que es un número privado que solo se ve dentro del sistema subautónomo. En esta figura, las confederaciones son AS 65100 y AS 65110. (RFC6996, reserva de sistema subautónomo [AS] para uso privado; indica que la IANA reserva los números del AS 64512 a 65534 para uso privado).

Las confederaciones de sistemas subautónomos parecen sistemas autónomos completos entre sí dentro del sistema subautónomo. Sin embargo, cuando el cortafuegos envía una ruta de AS a un peer de EBGP, únicamente el número público de AS aparece en la ruta de AS; no se incluyen números privados de sistema subautónomo (AS miembro de la confederación).

© 2020 Palo Alto Networks, Inc.

Se produce el emparejamiento de BGP entre el cortafuegos y R2; el cortafuegos en la figura posee los siguientes ajustes relevantes:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP confederado
- AS del peer: 65110



El enrutador 2 (R2) en AS 65110 se configura de la siguiente manera:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP confederado
- AS del peer: 65110

El emparejamiento de BGP también se produce entre el cortafuegos y R1. El cortafuegos posee la siguiente configuración adicional:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: IBGP confederado
- AS del peer: 65110

R1 se configura de la siguiente manera:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: IBGP confederado
- AS del peer: 65110

El emparejamiento de BGP se produce entre el cortafuegos y R5. El cortafuegos posee la siguiente configuración adicional:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP
- AS del peer: 25

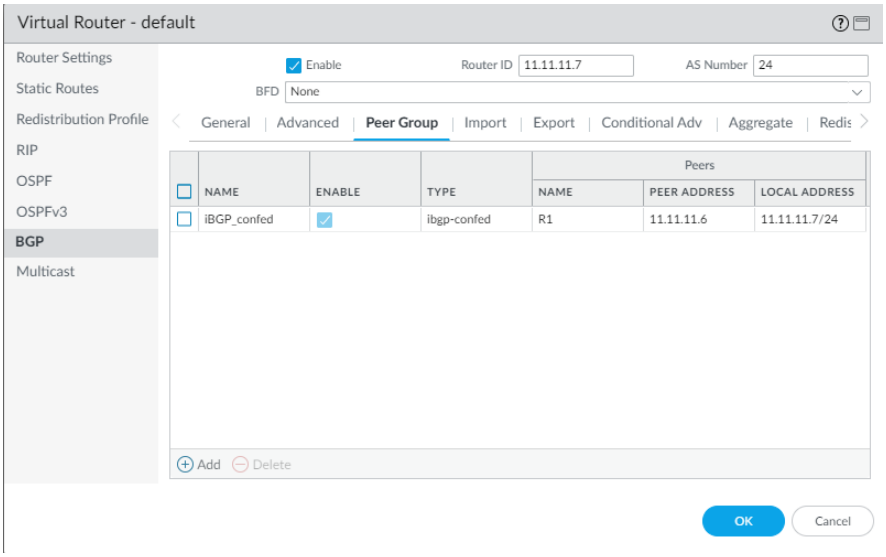
R5 se configura de la siguiente manera:

- AS—25

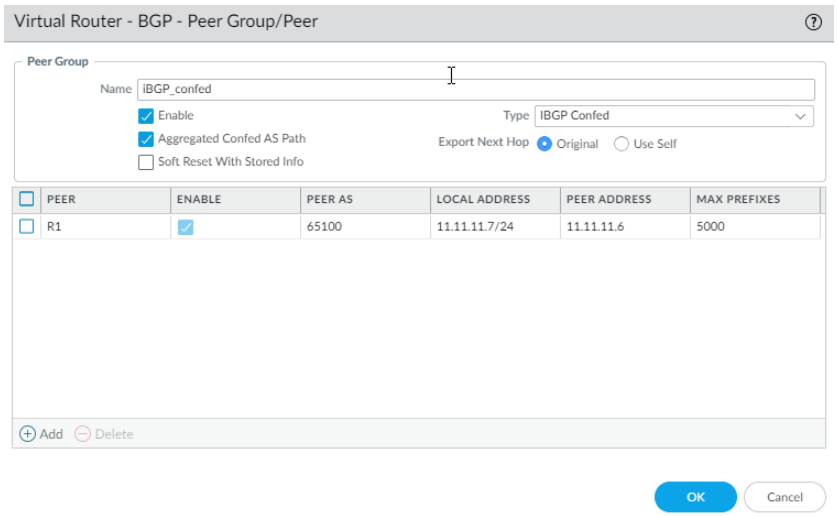
© 2020 Palo Alto Networks, Inc.

- Tipo del peer: EBGP
- AS del peer: 24

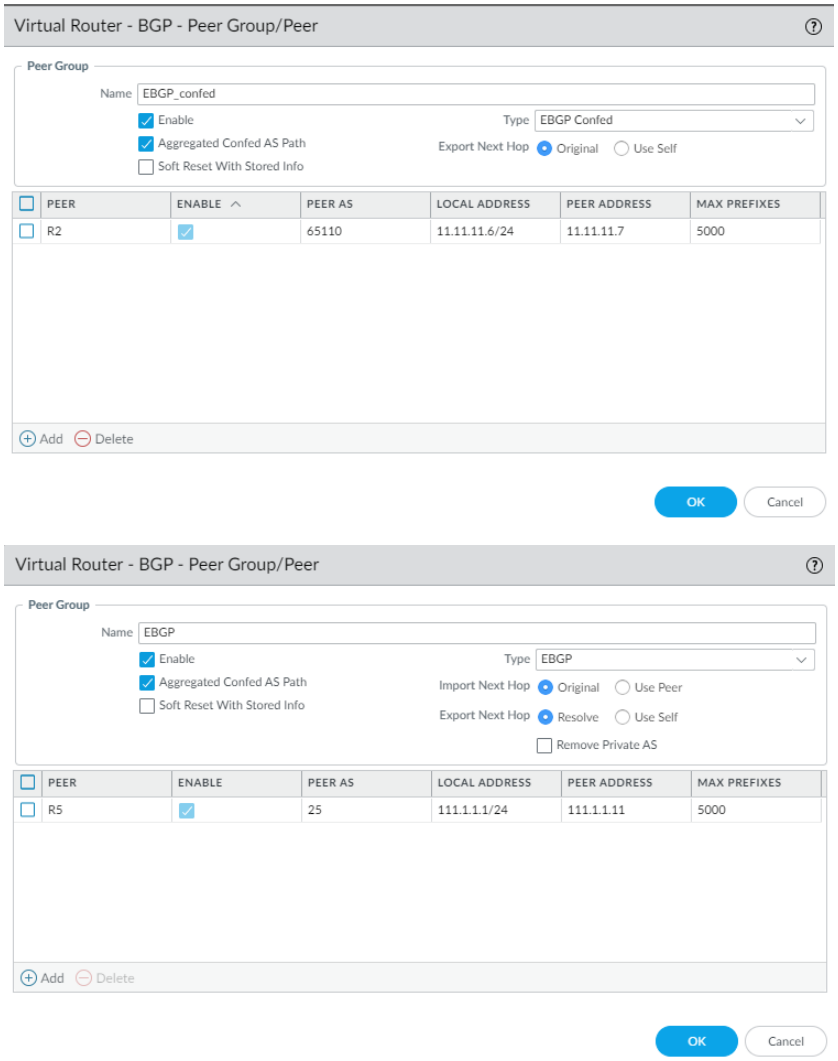
Después de que el cortafuegos se configure para emparejarse con R1, R2 y R5, sus peers se ven en la pestaña **Peer Group (Grupo de peers)**:



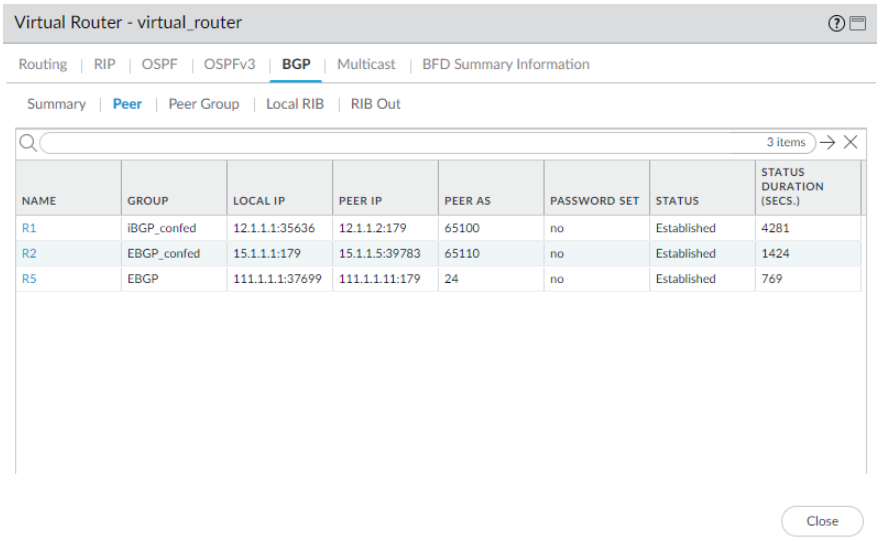
El cortafuegos muestra los peers R1, R2, and R5:



© 2020 Palo Alto Networks, Inc.

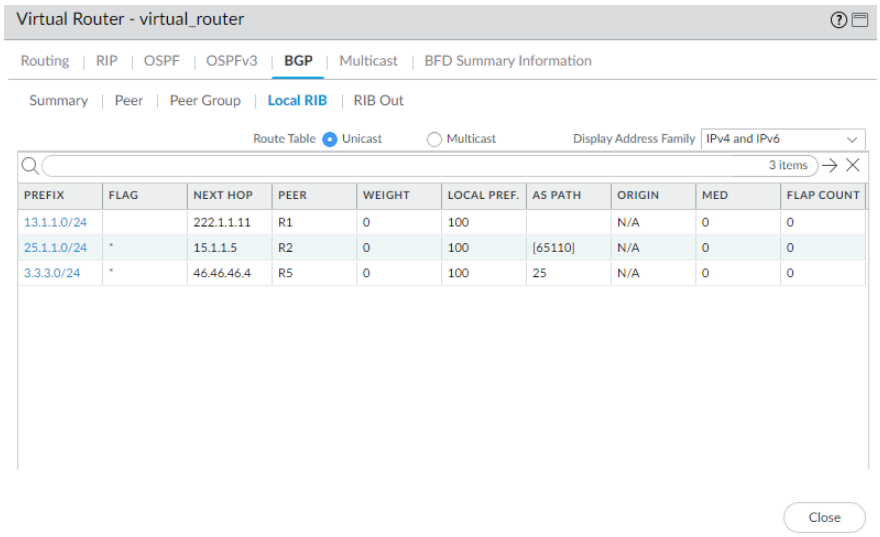


Para verificar que se establezcan las rutas desde el cortafuegos a los peers, en la pantalla del enrutador virtual, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)** y seleccione la pestaña **Peer**.

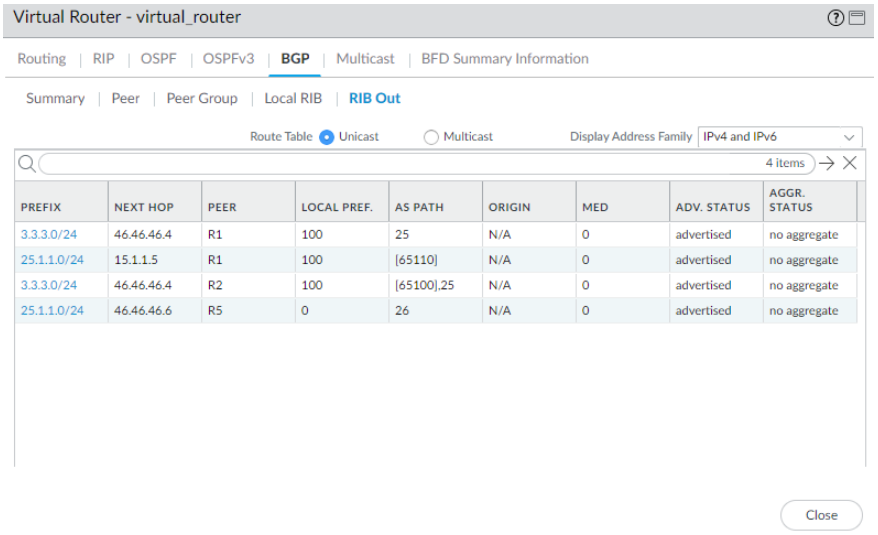


© 2020 Palo Alto Networks, Inc.

Seleccione la pestaña **Local RIB (RIB local)** para ver la información sobre las rutas almacenadas en la base de información de enrutamiento (Routing Information Base, RIB).



Luego, seleccione la pestaña **RIB Out (Salida RIB)**.



© 2020 Palo Alto Networks, Inc.

IP de multidifusión

La multidifusión de IP es un conjunto de protocolos que los dispositivos de red usan para enviar datagramas de IP de multidifusión a un grupo de receptores interesados mediante una trasmisión en lugar de una realizar una unidifusión del tráfico a varios receptores, lo que ahorra ancho de banda. La multidifusión de IP es adecuada para la comunicación desde una fuente (o varias) a muchos receptores, como la transmisión de audio o vídeo, IPTV, videoconferencias y distribución de otras comunicaciones, como noticias y datos financieros.

Una dirección de multidifusión identifica un grupo de receptores que desea recibir tráfico que se dirige a esa dirección. No debe utilizar las direcciones de multidifusión reservadas para casos especiales, como el rango de 224.0.0.0 a 224.0.0.255 o de 239.0.0.0 a 239.255.255.255. El tráfico de multidifusión usa UDP, que no vuelve a enviar los paquetes que faltan.

Los cortafuegos de Palo Alto Networks® admiten la multidifusión de IP y la Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) en una interfaz de capa 3 que configura para un enrutador virtual en el cortafuegos.

Para el enrutamiento de multidifusión, el tipo de interfaz de capa 3 puede ser Ethernet, Ethernet agregada (Aggregate Ethernet, AE), VLAN, bucle invertido o túnel. Los grupos de interfaces le permiten configurar más de una interfaz de cortafuegos a la vez con el mismo Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) y parámetros PIM, y con los mismos permisos de grupo (grupos de multidifusión que tienen permitido aceptar tráfico de cualquier fuente o de una única fuente específica). Una interfaz puede pertenecer a solo un grupo de interfaces.

El cortafuegos admite la multidifusión de IPv4, no admite la de IPv6. El cortafuegos no admite el Modo denso de PIM (PIM Dense Mode, PIM-DM), proxy IGMP, uniones estáticas de IGMP, RP de difusión limitada, GRE o configuraciones de multidifusión en un tipo de interfaz de cable virtual o capa 2. Sin embargo, una interfaz de cable virtual puede pasar paquetes de multidifusión. Además, una interfaz de capa 2 puede cambiar paquetes de multidifusión IPv4 de capa 3 entre diferentes VLAN y el cortafuegos volverá a etiquetar el ID de VLAN con el ID de VLAN de la interfaz de salida.

Debe habilitar la multidifusión para un enrutador virtual y habilitar PIM para una interfaz de entrada y salida para que las interfaces reciban o reenvíen paquetes de multidifusión. Además de PIM, también debe habilitar IGMP en las interfaces de salida que se orientan a los receptores. Debe configurar una regla de política de seguridad para permitir el tráfico de multidifusión de IP en una zona de destino de capa 3 predefinida con el nombre **multicast (multidifusión)** o a cualquier zona de destino cuando se configura como **any (cualquiera)**.

- IGMP
- PIM
- Configuración de IP de multidifusión
- Visualización de información de IP de multidifusión

IGMP

El Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) es un protocolo IPv4 que un receptor de multidifusión usa para comunicarse con una interfaz de un cortafuegos de Palo Alto Networks® y que el cortafuegos usa para registrar la pertenencia de los grupos de multidifusión. Cuando un host desea recibir tráfico de multidifusión, su implementación de IGMP envía un mensaje de informe de pertenencia de IGMP y el enrutador receptor envía un mensaje de unión de PIM a la dirección del grupo de multidifusión del grupo al cual el host desea unirse. Un enrutador habilitado para IGMP en la misma red física (como un segmento de Ethernet) usa PIM para comunicarse con otros enrutadores habilitados para PIM y determinar una ruta desde la fuente a los receptores interesados.

© 2020 Palo Alto Networks, Inc.

Habilite IGMP solo en interfaces que se orientan al receptor de multidifusión. Los receptores pueden estar a solo un salto de capa 3 de distancia del enrutador virtual. Los mensajes de IGMP son mensajes de capa 2 que tienen un valor TTL de uno y, por lo tanto, no pueden salir de la red LAN.

Cuando configure la multidifusión de IP, especifique si una interfaz usa IGMP Versión 1, IGMP Versión 2 o IGMP Versión 3. Puede aplicar la opción de alerta de enrutador de IP, RFC 2113, de modo que los paquetes entrantes de IGMP que use IGMPv2 o IGMPv3 tengan la opción de alerta de enrutador de IP.

De manera predeterminada, una interfaz acepta los informes de pertenencia de IGMP para todos los grupos de multidifusión. Puede configurar permisos del grupo de multidifusión para controlar los grupos en los que el enrutador virtual acepta informes de pertenencia de cualquier fuente (Multidifusión de cualquier fuente [Any-Source Multicast, ASM]), que en esencia es el Modo disperso de PIM (PIM Sparse Mode, PIM-SM). También puede especificar los grupos en los que el enrutador virtual acepta los informes de pertenencia de una fuente específica Multidifusión de fuente específica [Source-Specific Multicast, SSM] de PIM). Si especifica permisos para los grupos ASM o SSM, el enrutador virtual rechaza los informes de pertenencia de otros grupos. La interfaz debe usar IGMPv3 para pasar el tráfico de PIM-SSM.

Puede especificar la cantidad máxima de fuentes y el número máximo de grupos de multidifusión que IGMP puede procesar simultáneamente para una interfaz.

El enrutador virtual realiza la multidifusión de una consulta de IGMP en intervalos regulares a todos los receptores de un grupo de multidifusión. Un receptor responde a una consulta de IGMP con un informe de pertenencia de IGMP que confirma que el receptor todavía desea recibir tráfico de multidifusión de ese grupo. El enrutador virtual conserva una tabla de los grupos de multidifusión que tienen receptores; el enrutador virtual reenvía un paquete de multidifusión fuera de la interfaz al siguiente salto solo si todavía hay un receptor en ese árbol de distribución de multidifusión que esté unido al grupo. El enrutador virtual no registra exactamente qué receptores se unieron a un grupo. Solo un enrutador en una subred responde a las consultas de IGMP y es el solicitante de IGMP, el enrutador con la dirección IP más baja.

Puede configurar una interfaz con el intervalo de consulta de IGMP y la cantidad de tiempo permitido para que un receptor responda a una consulta (la opción Max Query Response Time [(Máx. de tiempo de respuesta de consulta]). Cuando un enrutador virtual recibe un mensaje de salida de IGMP de un receptor para abandonar un grupo, el enrutador virtual comprueba que la interfaz que recibió este mensaje no esté configurada con la opción Immediate Leave (Salida inmediata). Si no está la opción Immediate Leave (Salida inmediata), el enrutador virtual envía una consulta para determinar si todavía existen miembros del receptor en el grupo. La opción Last Member Query Interval (Último intervalo de consulta del miembro) especifica cuántos segundos se proporcionan para que los receptores restantes de ese grupo respondan y confirmen que todavía desea el tráfico de multidifusión de ese grupo.

Una interfaz admite la variable de potencia de IGMP, que puede ajustar para que el cortafuegos ajuste las opciones Group Membership Interval (Intervalo de pertenencia del grupo), Other Querier Present Interval (Otro intervalo presente del solicitante), Startup Query Count (Recuento de consultas de inicio) y Last Member Query Count (Último recuento de consulta del miembro). Una variable de mayor potencia puede tener una subred que probablemente descarte paquetes.

Visualice la información de multidifusión de IP para ver las interfaces habilitadas para IGMP, la versión de IGMP, la dirección del solicitante, la configuración de potencia, los límites en la cantidad de fuentes y grupos de multidifusión, y si la interfaz está confirmada para la salida inmediata. También puede ver los grupos de multidifusión a los cuales pertenecen las interfaces y otra información de pertenencia de IGMP.

PIM

La multidifusión de IP usa el protocolo de enrutamiento de Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) entre enrutadores para determinar la ruta del árbol de distribución que los paquetes de multidifusión toman desde el origen hasta los receptores (miembros del grupo de multidifusión). Un cortafuegos de Palo Alto Networks® admite el Modo disperso de PIM (PIM-SM) (RFC 4601), la Multidifusión de cualquier origen (Any-Source Multicast, ASM) de PIM (a veces denominada como el Modo disperso de PIM) y la Multidifusión de origen específico (Source-Specific Multicast, SSM) de PIM.

© 2020 Palo Alto Networks, Inc.

En PIM-SM, el origen no reenvía tráfico de multidifusión hasta que un receptor (usuario) que pertenece a un grupo de multidifusión solicita que el origen envíe el tráfico. Cuando un host desea recibir tráfico de multidifusión, su implementación de IGMP envía un mensaje de informe de pertenencia de IGMP y el enrutador receptor envía un mensaje de unión de PIM a la dirección del grupo de multidifusión del grupo al que desea unirse.

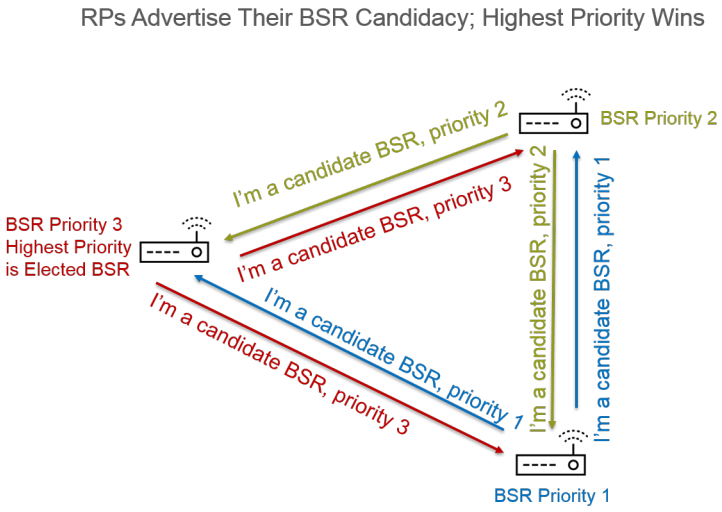
- En **ASM**, el receptor usa IGMP para solicitar tráfico de una dirección de grupo de multidifusión; cualquier origen podría haber originado ese tráfico. Por consecuencia, el receptor no conoce necesariamente a los emisores, y el receptor podría recibir tráfico de multidifusión en el que no tiene interés.
- En **SSM** (RFC 4607), el receptor usa IGMP para solicitar tráfico desde uno o más orígenes específicos hacia una dirección de grupo de multidifusión. El receptor conoce la dirección IP de los emisores y recibe solo el tráfico de multidifusión que desea. SSM requiere IGMPv3. Puede anular el espacio de direcciones SSM predeterminado, que es 232.0.0.0/8.

Cuando configura la multidifusión de IP en un cortafuegos de Palo Alto Networks®, debe habilitar PIM para que una interfaz reenvíe el tráfico de multidifusión, incluso en interfaces accesibles desde un receptor. Esto es diferente a IGMP, que habilita solo en interfaces accesibles desde un receptor.

ASM requiere un *punto de encuentro* (rendezvous point, RP), que es un enrutador localizado en la unión o raíz de un árbol de distribución compartida. El RP de un dominio de multidifusión sirve como un único punto al cual todos los miembros del grupo de multidifusión envían sus mensajes de unión. Este comportamiento reduce la probabilidad de un bucle de enrutamiento que, de lo contrario, ocurriría si los miembros del grupo enviaran sus mensajes de unión a varios enrutadores. (SSM no necesita un RP porque la multidifusión específica de origen usa un árbol con la ruta más corta y, por lo tanto, no necesita un RP).

En un entorno de ASM, existen dos maneras de que el enrutador virtual determine qué enrutador es el RP de un grupo de multidifusión:

- **Asignación estática de RP a grupo:** configura el enrutador virtual en el cortafuegos para que actúe como RP de grupos de multidifusión. Puede configurar un RP local configurando una dirección RP estática o especificando que el RP local sea un RP candidato y el RP se elija dinámicamente (sobre la base del menor valor de prioridad). También puede configurar estáticamente uno o más RP externos para diferentes rangos de direcciones de grupo que no están cubiertos por el RP local, lo que ayuda a equilibrar la carga del tráfico de multidifusión para que un RP no se sobrecargue.
- **Enrutador de arranque (bootstrap router, BSR)**: (RFC 5059); define la función de un BSR. Primero, los candidatos para BSR anuncian su prioridad entre ellos y, luego, el candidato con la prioridad más alta es elegido BSR, como se muestra en la siguiente figura:

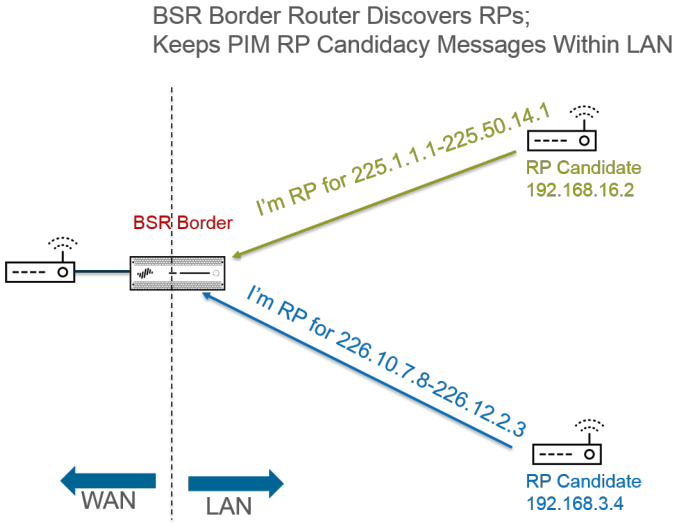


A continuación, el BSR descubre RP cuando los RP candidatos realizan la unidifusión periódica de un mensaje de BSR al BSR que contiene su dirección IP y el rango de grupo de multidifusión para el cual actuarán como RP. Puede configurar el enrutador virtual local para que sea un RP candidato, en

© 2020 Palo Alto Networks, Inc.

este caso el enrutador virtual anuncia su candidatura de RP para grupos o un grupo de multidifusión específico. El BSR envía la información de RP a los demás RP del dominio de PIM.

Cuando configure PIM para una interfaz, puede seleccionar el borde de BSR cuando la interfaz en el cortafuegos esté en un límite empresarial que se sale de la red empresarial. La configuración de borde de BSR evita que el cortafuegos envíe los mensajes de BSR de la candidatura de RP fuera de la red LAN. En la siguiente ilustración, el borde de BSR está habilitado para la interfaz que está frente a la red LAN y esa interfaz tiene la prioridad más alta. Si el enrutador virtual tiene un RP estático y uno dinámico (obtenido del BSR), puede especificar si el RP estático debe anular el RP obtenido de un grupo cuando configure el RP estático local.



Para que el Modo disperso de PIM notifique al RP que tiene tráfico para enviar al árbol compartido, el RP debe conocer el origen. El host notifica al RP que está enviando tráfico a una dirección del grupo de multidifusión cuando el *enrutador designado* (designated router, DR) encapsula el primer paquete del host en un mensaje de registro de PIM y realiza la unidifusión del paquete al RP en su red local. El DR también reenvía mensajes de eliminación desde un receptor al RP. El RP mantiene la lista de direcciones IP de orígenes que se envían a un grupo de multidifusión y el RP puede reenviar paquetes de multidifusión desde los orígenes.

¿Por qué los enrutadores de un dominio de PIM necesitan un DR? Cuando el enrutador envía un mensaje de unión de PIM a un conmutador, dos enrutadores podrían recibirlo y reenviarlo al mismo RP, lo que provoca tráfico redundante y desperdicio de ancho de banda. Para evitar el tráfico innecesario, los enrutadores de PIM eligen un DR (el enrutador con la dirección IP más alta) y solo el DR reenvía el mensaje de unión al RP. De manera alternativa, puede asignar una prioridad de DR a un grupo de interfaces, que tiene precedencia sobre las comparaciones de direcciones IP. Como recordatorio, el DR reenvía (o realiza la unidifusión) mensajes de PIM; no realiza la multidifusión de paquetes de multidifusión de IP.

Puede especificar las direcciones IP de los vecinos de PIM (enrutadores) que el grupo de interfaces permitirá intercambiar con el enrutador virtual. De forma predeterminada, todos los enrutadores habilitados para PIM pueden ser vecinos de PIM, pero la opción para limitar vecinos proporciona un paso hacia la protección del enrutador virtual en su entorno de PIM.

- Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido
- Mecanismo de imposición de PIM
- Reenvío de ruta inversa

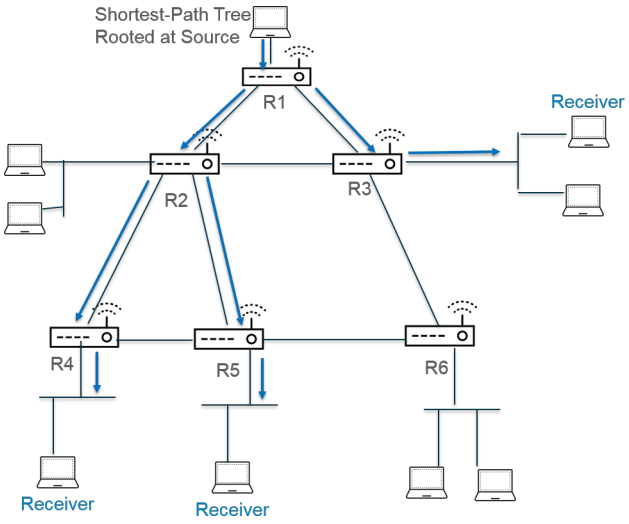
Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido

Después de que un receptor se una a un grupo de multidifusión, los enrutadores en la red de acceso múltiple crean las rutas necesarias para enviar datos a cada receptor del grupo. Cada datagrama de IP

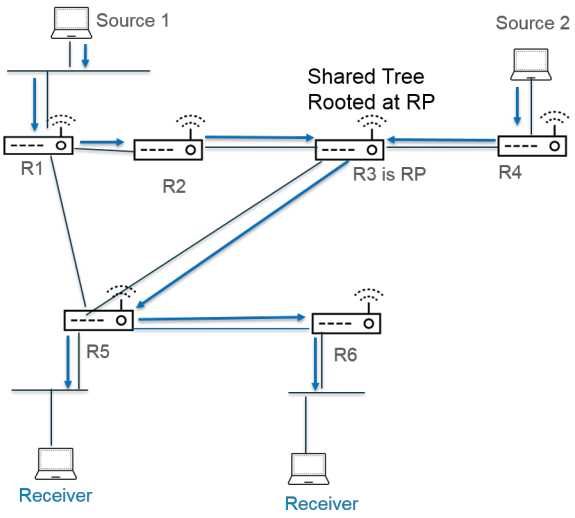
© 2020 Palo Alto Networks, Inc.

enviado a un grupo de multidifusión se distribuye (reenvía) a todos los miembros. Las rutas constituyen un tipo de árbol de distribución para un paquete de multidifusión. El objetivo de un árbol de distribución de multidifusión es que el enrutador duplique un paquete de multidifusión cuando este llegue a una divergencia de rutas y el enrutador debe enviarlo a varias rutas para llegar a todos los miembros del grupo, pero el árbol de distribución debe abstenerse de enviar paquetes por una ruta en la que no existen receptores interesados. El árbol de distribución es uno de los siguientes:

- Un **árbol fuente:** una ruta de una fuente de multidifusión (la raíz del árbol) a través de la red a los receptores en el grupo de multidifusión. El árbol fuente es la ruta más corta que un paquete de multidifusión puede tomar desde la fuente al receptor, por lo que también se le conoce como el **árbol con la ruta más corta (shortest-path tree, SPT)**. El emisor y receptor se anotan como un par del grupo multidifusión y fuente, abreviado a (S, G); por ejemplo, (192.168.1.1, 225.9.2.6). La siguiente figura muestra tres árboles con la ruta más corta desde la fuente hasta los tres receptores.



- Un **árbol compartido:** una ruta con la raíz en el RP, no en la fuente de multidifusión. Al árbol compartido también se le conoce como árbol RP o RPT. Los enrutadores reenvían paquetes de multidifusión de varias fuentes al RP y el RP reenvía los paquetes al árbol compartido. Un árbol compartido se anota como (*,G) con un asterisco como la fuente porque todas las fuentes que pertenecen al grupo de multidifusión comparten el mismo árbol de distribución del RP. Un ejemplo de anotación de árbol compartido es (*, 226.3.1.5). La siguiente figura muestra un árbol compartido desde la raíz en el RP a los receptores.



© 2020 Palo Alto Networks, Inc.

La Multidifusión de fuente específica (Source-Specific Multicast, SSM) usa la distribución del árbol fuente. Cuando configura la multidifusión de IP para que use la Multidifusión de cualquier fuente (Any Source Multicast, ASM), puede especificar qué árbol de distribución usa el enrutador virtual en su cortafuegos de Palo Alto Networks® para entregar paquetes de multidifusión a un grupo mediante la configuración de un umbral de SPT para el grupo:

- De manera predeterminada, el enrutador virtual cambia el enrutamiento de multidifusión del árbol compartido a SPT cuando recibe el primer paquete de multidifusión para un grupo o prefijo (el **SPT Threshold [Umbral de SPT]** se configura en 0).
- Puede configurar que el enrutador virtual cambie a SPT cuando el número total de kilobits de los paquetes que llegan al grupo o prefijo de multidifusión especificado en cualquier interfaz durante cualquier período de tiempo alcance un número configurado.
- Puede configurar que el enrutador virtual nunca cambie a SPT para el grupo o prefijo (continúa usando el árbol compartido).

SPT requiere más memoria, por lo que debe elegir su configuración en función de su nivel de tráfico de multidifusión en el grupo. Si el enrutador virtual cambia a SPT, los paquetes llegarán desde la fuente (en lugar del RP) y el enrutador virtual envía un mensaje de eliminación al RP. La fuente envía paquetes de multidifusión subsiguientes para ese grupo por el árbol con la ruta más corta.

Mecanismo de imposición de PIM

Para evitar que los enrutadores de una red de acceso múltiple reenvíen el mismo tráfico de multidifusión al mismo salto siguiente (lo que provocaría tráfico redundante y un desperdicio de ancho de banda), PIM usa el mecanismo de imposición para elegir un solo reenviador de PIM para la red de acceso múltiple.

Si el enrutador virtual recibe un paquete multidifusión de una fuente en una interfaz que el enrutador virtual ya asocia como la interfaz de salida para el mismo par (S, G) identificado en el paquete, esto significa que es un paquete duplicado. Por tanto, el enrutador virtual envía un mensaje de imposición que contiene sus métricas a los demás enrutadores de la red de acceso múltiple. Luego, los enrutadores eligen un reenviador de PIM de esta manera:

1. El reenviador de PIM es el enrutador con la menor distancia administrativa a la fuente de multidifusión.
2. En el caso de un empate en la menor distancia administrativa, el reenviador de PIM es el enrutador con la mejor métrica de enrutamiento de unidifusión a la fuente.
3. En el caso de un empate en la mejor métrica, el reenviador de PIM es el enrutador con la dirección IP más alta.

Los enrutadores que se eligen como reenviador de PIM detendrán el reenvío de tráfico al grupo de multidifusión identificado en el par (S, G).

Cuando configure una multidifusión de IP, puede configurar el intervalo en cual el enrutador virtual envía mensajes de imposición de PIM a la interfaz (el intervalo de imposición). Cuando visualiza la información de la multidifusión de IP, la pestaña **PIM Interface (Interfaz de PIM)** muestra el intervalo de imposición de una interfaz.

Reenvío de ruta inversa

PIM usa el Reenvío de ruta inversa (reverse-path forwarding, RPF) para evitar bucles de enrutamiento de la multidifusión mediante el aprovechamiento de la tabla de enrutamiento de unidifusión en el enrutador virtual. Cuando el enrutador virtual recibe un paquete de multidifusión, busca la fuente en su tabla de enrutamiento de unidifusión para verificar si la interfaz de salida asociada con esa dirección IP de origen es la interfaz a la que llegó el paquete. Si las interfaces coinciden, el enrutador virtual duplica el paquete y lo reenvía desde las interfaces hacia los receptores de multidifusión del grupo. Si las interfaces no coinciden, el enrutador virtual descarta el paquete. La tabla de enrutamiento de unidifusión se basa en las rutas estáticas subyacentes o el protocolo de puerta de enlace interno (interior gateway protocol, IGP) que usa su red, como OSPF.

© 2020 Palo Alto Networks, Inc.

PIM también usa RPF para crear un árbol con la ruta más corta a una fuente, un salto de enrutador de PIM a la vez. El enrutador virtual tiene la dirección de la fuente de multidifusión, de modo que el enrutador virtual seleccione como su siguiente salto hacia la fuente el PIM vecino más próximo que el enrutador virtual usaría para reenviar paquetes de unidifusión a la fuente. El enrutador del siguiente salto realiza la misma acción.

Después de que el RPF se realice correctamente y el enrutador virtual tenga una entrada de ruta en su Base de información de enrutamiento multidifusión (multicast routing information base, mRIB), el enrutador virtual conserva las entradas del árbol basadas en la fuente (S,G) y las entradas de árbol compartido (*,G) en su base de información de reenvío de multidifusión (la tabla de reenvío de multidifusión [multicast forwarding table, mFIB]). Cada entrada incluye la dirección IP de origen, el grupo de multidifusión, la interfaz de entrada (interfaz de RPF) y la lista de interfaces de salida. Pueden existir varias interfaces de salida para una entrada porque el árbol con la ruta más corta puede bifurcarse en el enrutador, y el enrutador debe reenviar el paquete a varias interfaces para llegar a los receptores del grupo que están ubicados en diferentes rutas. Cuando el enrutador virtual usa mFIB para reenviar un paquete de multidifusión, coincide con una entrada (S,G) antes de intentar coincidir con una entrada (*,G).

Si anuncia prefijos de fuente de multidifusión en BGP (configuró MP-BGP con la familia de direcciones IPv4 y la familia de direcciones subsiguiente de multidifusión), el cortafuegos siempre realiza la comprobación de RPF en las rutas de BGP que el cortafuegos recibió conforme a la familia de direcciones subsiguiente de multidifusión.

Visualice la información de multidifusión de IP para verificar cómo ver las entradas mFIB y mRIB. Tenga en cuenta que la tabla de ruta de multidifusión (multicast route table, mRIB) es una tabla separada de la tabla de ruta de unidifusión (unicast route table, RIB)

Configuración de IP de multidifusión

Configure interfaces en un enrutador virtual de un cortafuegos de Palo Alto Networks® para recibir y reenviar paquetes de IP de multidifusión. Debe habilitar la multidifusión de IP para el enrutador virtual, configurar la Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) en las interfaces de entrada y salida, y configurar el Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) en las interfaces que acceden los receptores.

STEP 1 | Habilite la multidifusión de IP para un enrutador virtual.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Multicast (Multidifusión)** y **Enable (Habilitar)** para habilitar la multidifusión de IP.

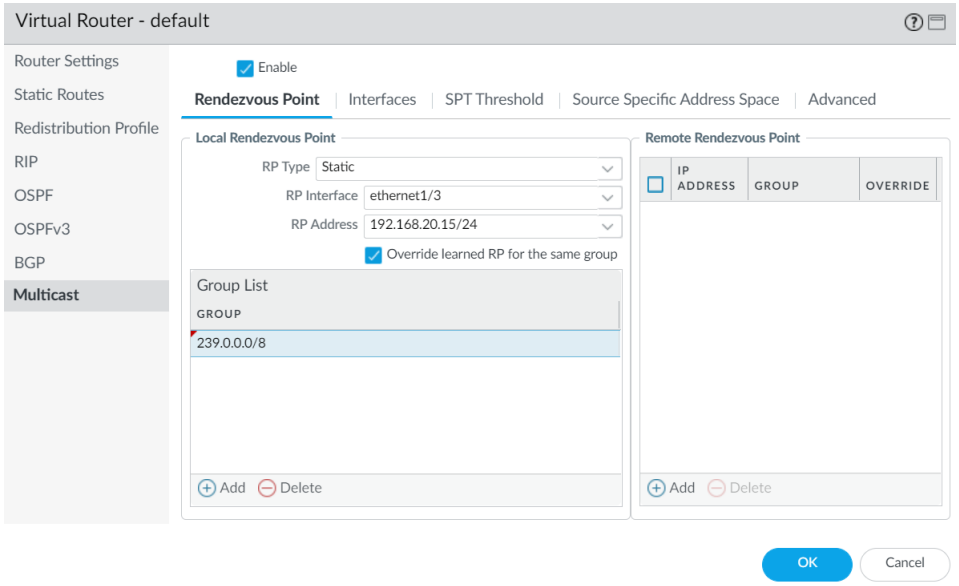
STEP 2 | (Únicamente en ASM) Si el dominio de multidifusión en el que el enrutador virtual está localizado usa Multidifusión de cualquier origen (Any-Source Multicast, ASM), identifique y configure los Puntos de encuentro (rendezvous points, RP) locales y remotos para los grupos de multidifusión.

1. Seleccione **Rendezvous Point (Punto de encuentro)**.
2. Seleccione un **RP Type (Tipo de RP)** local, que determine cómo se elige el RP (las opciones son **Static [Estático]**, **Candidate [Candidato]** o **None [Ninguno]**):

   - **Static (Estático)**: establece una asignación estática de un RP para grupos de multidifusión. Si configura un RP estático, se requiere que configure explícitamente el mismo RP en otros enrutadores de PIM en el dominio de PIM.
     - Seleccione **RP Interface (Interfaz de RP)**. Los tipos de interfaz válidos son Capa 3, cable virtual, bucle invertido, VLAN, Ethernet agregada (Aggregate Ethernet, AE) y túnel.
     - Seleccione **RP Address (Dirección de RP)**. La lista se llena con las direcciones IP de la interfaz de RP seleccionada.
     - Seleccione **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)** de modo que este RP estático sirva como RP en lugar del RP elegido para los grupos en la lista de grupos.

© 2020 Palo Alto Networks, Inc.

- Seleccione **Add (Añadir)** para añadir uno o más **Groups (Grupos)** de multidifusión para que el RP actúe como RP.



- **Candidate (Candidato)**: establece una asignación dinámica de un RP a grupos de multidifusión según la prioridad, de modo que cada enrutador en un dominio de PIM elija automáticamente el mismo RP.
  - Seleccione **RP Interface (Interfaz de RP)** del RP candidato. Los tipos de interfaz válidos son Capa 3, bucle invertido, VLAN, Ethernet agregada (Aggregate Ethernet, AE) y túnel.
  - Seleccione la **RP Address (Dirección de RP)** del RP candidato. La lista se llena con las direcciones IP de la interfaz de RP seleccionada.
  - (Opcional) Cambie la **Priority (Prioridad)** para el RP candidato. El cortafuegos compara la prioridad del RP candidato con la prioridad de otros RP candidatos para determinar cuál actúa como RP para los grupos especificados; el cortafuegos selecciona el RP candidato con el valor de prioridad más bajo (el rango es de 0 a 255; el valor predeterminado es 192).
  - (Opcional) Cambie el **Advertisement Interval (sec) (Intervalo de anuncios [segundos])** (el rango es de 1 a 26 214; el valor predeterminado es 60).
  - Introduzca una **Group List (Lista de grupos)** de grupos de multidifusión que se comunique con el RP.
- **None (Ninguno)**: seleccione esta opción si este enrutador virtual no es un RP.

3. Seleccione **Add (Añadir)** para añadir un Punto de encuentro remoto e introduzca la **IP Address (Dirección IP)** de ese RP remoto (externo).
4. Seleccione **Add (Añadir)** para añadir las **Group Addresses (Direcciones del grupo)** de multidifusión para las cuales la dirección de RP remoto especificado actúa como RP.
5. Seleccione **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)** de modo que el RP externo que configuró estáticamente sirva como RP en lugar de un RP que se obtenga (elija) de manera dinámica para los grupos en la lista de direcciones de grupos.
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Especifique un grupo de interfaces que comparta una configuración de multidifusión (IGMP, PIM y permisos de grupo).

1. En la pestaña **Interfaces (Interfaces)**, seleccione **Add (Añadir)** para añadir un nombre en **Name (Name)** para el grupo de interfaces.
2. Introduzca una **Description (Descripción)**.

© 2020 Palo Alto Networks, Inc.

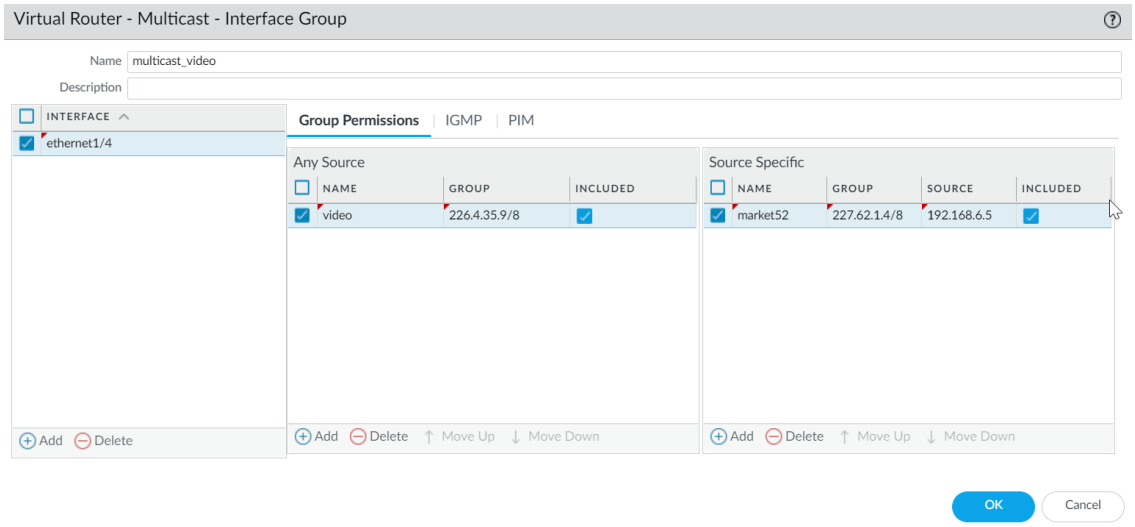
3. Seleccione **Add (Añadir)** para añadir una interfaz en **Interface (interfaz)** y seleccione una o más interfaces de Capa 3 que pertenezcan al grupo de interfaces.

STEP 4 | (Opcional) Configure permisos de grupo de multidifusión para el grupo de interfaces. De manera predeterminada, el grupo de interfaces acepta informes de pertenencia de IGMP y mensajes de unión de PIM de todos los grupos.

1. Seleccione **Group Permissions (Permisos del grupo)**.
2. Para configurar grupos de Multidifusión de cualquier origen (Any-Source Multicast, ASM) para este grupo de interfaces, en la ventana Any Source (Cualquier origen), seleccione **Add (Añadir)** para añadir un nombre en **Name (Nombre)** e identificar un grupo de multidifusión que acepte informes de pertenencia de IGMP y mensajes de unión de PIM de cualquier origen.
3. Introduzca una dirección de grupo o dirección de grupo de multidifusión en **Group (Grupo)** y el / prefijo que pueda recibir paquetes de multidifusión de cualquier origen en estas interfaces.
4. Seleccione **Included (Incluido)** para incluir la dirección del grupo de ASM en **Group (Grupo)** en el grupo de interfaces (predeterminado). Cancele la selección de **Included (Incluido)** para excluir con facilidad un grupo de ASM del grupo de interfaces, por ejemplo, durante una prueba.
5. Seleccione **Add (Añadir)** para añadir grupos de multidifusión adicionales en **Groups (Grupos)** (para el grupo de interfaces) que desean recibir paquetes de multidifusión de cualquier origen.
6. Para configurar los grupos de Multidifusión de origen específico (Source-Specific Multicast, SSM) en este grupo de interfaces, en la ventana Source Specific (Origen específico), seleccione **Add (Añadir)** para añadir un nombre en **Name (Nombre)** a fin de identificar el par de direcciones de origen y grupo de multidifusión. No utilice un nombre que use para la multidifusión de cualquier origen. (Debe usar IGMPv3 para configurar SSM).
7. Introduzca la dirección de grupo o una dirección de grupo de multidifusión en **Group (Grupo)** y el / prefijo del grupo que desea recibir paquetes de multidifusión del origen especificado solamente (y que puede recibir los paquetes en estas interfaces).

   Un grupo de un origen específico para el cual especifica permisos es un grupo que el enrutador virtual debe tratar como específico del origen. Configure Source Specific Address Space (Espacio de dirección de origen específico) (Paso 9) que incluye los grupos específicos de origen para los cuales configuró el permiso.
8. Introduzca la dirección IP de origen en **Source (Origen)** desde la cual este grupo de multidifusión puede recibir paquetes de multidifusión.
9. Seleccione **Included (Incluido)** para incluir el par de direcciones de origen y grupo SSM en el grupo de interfaces (predeterminado). Cancele la selección de **Included (Incluido)** para excluir con facilidad el par del grupo de interfaces, por ejemplo, durante una prueba.
10. Seleccione **Add (Añadir)** para añadir grupos de multidifusión adicionales en **Groups (Grupos)** (para el grupo de interfaces) que reciban paquetes de multidifusión de un único origen específico.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Configure IGMP para el grupo de interfaces si una interfaz afronta receptores de multidifusión, que deben usar IGMP para unirse a un grupo.

1. En la pestaña **IGMP**, seleccione **Enable (Habilitar)** para habilitar IGMP (predeterminado).
2. Especifique los parámetros de IGMP para las interfaces del grupo de interfaces:

- **IGMP Version (Versión de IGMP)**: **1**, **2** o **3** (predeterminada).
- **Enforce Router-Alert IP Option (Aplicar opción de IP de enrutador-alerta)** (deshabilitada de forma predeterminada): seleccione esta opción si requiere paquetes de IGMP que usen IGMPv2 o IGMPv3 para tener la opción de alerta de enrutador de IP, RFC 2113.
- **Robustness (Potencia)**: una variable que el cortafuegos usa para ajustar las opciones Group Membership Interval (Intervalo de pertenencia del grupo), Other Querier Present Interval (Otro intervalo presente del solicitante), Startup Query Count (Recuento de consultas de inicio) y Last Member Query Count (Último recuento de consulta del miembro) (el rango es de 1 a 7; el valor predeterminado es 2). Aumente el valor si la subred en la cual está ubicado este cortafuegos es propensa a perder paquetes.
- **Max Sources (Máx. de fuentes)**: la cantidad máxima de fuentes que IGMP puede procesar de manera simultánea para una interfaz (el rango es de 1 a 65 535; el valor predeterminado es **unlimited [ilimitado]**).
- **Max Groups (Máx. de grupos)**: la cantidad máxima de grupos que IGMP puede procesar de manera simultánea para una interfaz (el rango es de 1 a 65 535; el valor predeterminado es **unlimited [ilimitado]**).
- **Query Interval (Intervalo de consulta)**: la cantidad de segundos entre mensajes de consulta de pertenencia de IGMP que el enrutador virtual envía a un receptor para determinar si el receptor aún desea recibir los paquetes de multidifusión para un grupo (el rango es de 1 a 31 744; el valor predeterminado es 125).
- **Max Query Response Time (sec) (Máx. de tiempo de respuesta de consulta [segundos])**: la cantidad máxima de segundos permitidos para que un receptor responda a un mensaje de consulta de pertenencia de IGMP antes de que el enrutador virtual determine que el receptor ya no desea recibir paquetes de multidifusión para el grupo (el rango es de 0 a 3174,4; el valor predeterminado es 10).
- **Last Member Query Interval (sec) (Último intervalo de consulta del miembro [segundos])**: la cantidad de segundos permitidos para que un receptor responda a una consulta específica del grupo que el enrutador virtual envía después de que un receptor envía un mensaje para abandonar el grupo (el rango es de 0,1 a 3174,4; el valor predeterminado es 1).
- **Immediate Leave (Salida inmediata)** (deshabilitado de forma predeterminada): cuando existe solo un miembro en un grupo de multidifusión y el enrutador virtual recibe un mensaje de salida de

© 2020 Palo Alto Networks, Inc.

IGMP para ese grupo, la configuración de Immediate Leave (Salida inmediata) provoca que el enrutador virtual elimine de inmediato ese grupo y la interfaz de salida de la Base de información del enrutador de multidifusión (multicast routing information base, mRIB) y la Base de información de reenvío de multidifusión, mFIB), en lugar de esperar que caduque el Último intervalo de consulta del miembro. La opción Immediate Leave (Salida inmediata) ahorra recursos de red. No puede seleccionar Immediate Leave (Salida inmediata) si el grupo de interfaces usa IGMPv1.

STEP 6 | Configure el Modo disperso de PIM (PIM Sparse Mode, PIM-SM) para el grupo de interfaces.

1. En la pestaña **PIM**, seleccione **Enable (Habilitar)** para habilitar PIM (habilitado de manera predeterminada).
2. Especifique los parámetros de PIM del grupo de interfaces:
   - **Assert Interval (Intervalo de imposición)**: la cantidad de segundos entre los mensajes de imposición de PIM que el enrutador virtual envía a otros enrutadores de PIM en la red de multiacceso cuando eligen un reenvío de PIM (el rango es de 0 a 65 534; el valor predeterminado es 177).
   - **Hello Interval (Intervalo de saludo)**: la cantidad de segundos entre los mensajes de saludo de PIM que el enrutador virtual envía a sus vecinos de PIM de cada interfaz en el grupo de interfaces (el rango es de 0 a 18 000; el valor predeterminado es 30).
   - **Join Prune Interval (Intervalo de unión/eliminación)**: la cantidad de segundos entre mensajes de unión de PIM (y entre mensajes de eliminación de PIM) que el enrutador virtual envía hacia un origen de multidifusión (el rango es de 0 a 18 000; el valor predeterminado es 60).
   - **DR Priority (Prioridad de DR)**: la prioridad de Enrutador designado (Designated Router, DR) que controla qué enrutador de una red de multiacceso reenvía mensajes de unión y eliminación de PIM al RP (el rango es de 0 a 429 467 295; el valor predeterminado es 1). La prioridad de DR tiene precedencia sobre las comparaciones de direcciones IP para elegir el DR.
   - **BSR Border (Borde de BSR)**: seleccione esta opción si las interfaces del grupo de interfaces se encuentran en un enrutador virtual que es el BSR localizado en el borde de una red LAN empresarial. Esto evitará que los mensajes del BSR de candidatura de RP salgan de la red LAN.
3. Seleccione **Add (Añadir)** para añadir uno o más **Permitted PIM Neighbors (Vecinos de PIM permitidos)** y especifique la **IP Address (Dirección IP)** de cada enrutador desde el cual el enrutador virtual acepta paquetes de multidifusión.

STEP 7 | Haga clic en **OK (Aceptar)** para guardar la configuración del grupo de interfaces.

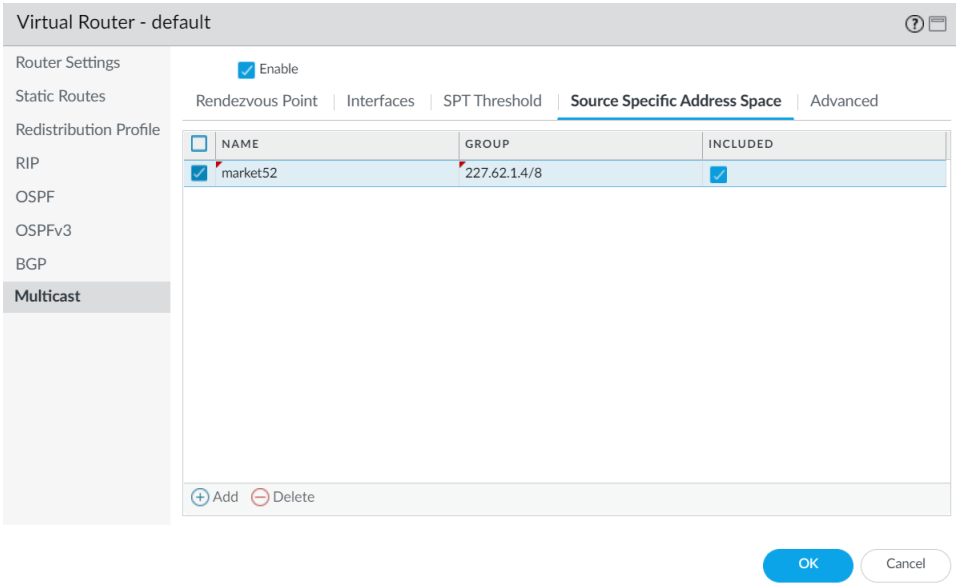
STEP 8 | (Opcional) Cambie el umbral del Árbol con la ruta más corta (Shortest-Path Tree, SPT), como se describe en Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido.

1. Seleccione **SPT Threshold (Umbral de SPT)** y **Add (Añadir)** para añadir un **Multicast Group/Prefix (Prefijo/grupo de mulidifusión)**, el grupo de multidifusión o prefijo para el cual especifica el árbol de distribución.
2. Especifique el **Threshold (kb) (Umbral [kb])**: el punto en el que el enrutamiento al prefijo o grupo de multidifusión especificado cambia del árbol compartido (con origen desde el RP) a una distribución de SPT:
   - **0 (switch on first data packet) (0 [cambiar en el primer paquete de datos])** (predeterminado): el enrutador virtual cambia del árbol compartido al SPT para el grupo o prefijo cuando el enrutador virtual recibe el primer paquete de datos del grupo o prefijo.
   - **never (do not switch to spt) (Nunca [no cambia a spt])**: el enrutador virtual continúa usando el árbol compartido para reenviar paquetes al grupo o prefijo.
   - Introduzca el número total de kilobits de los paquetes de multidifusión que pueden llegar para el grupo de multidifusión o prefijo en cualquier interfaz y durante cualquier período de tiempo, en el que el enrutador virtual cambia a la distribución de SPT para ese prefijo o grupo de multidifusión.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Identifique los grupos de multidifusión o grupos y prefijos que acepten paquetes de multidifusión solo desde una fuente específica.

1. Seleccione **Source Specific Address Space (Espacio de dirección de origen específico)** y **Add (Añadir)** para añadir un **Name (Nombre)** para el espacio.
2. Introduzca una dirección de grupo de multidifusión en **Group (Grupo)** con la longitud de prefijo para identificar el espacio de direcciones que recibe paquetes de multidifusión de una fuente específica. Si el enrutador virtual recibe un paquete de multidifusión para un grupo de SSM pero el grupo está cubierto por un **Source Specific Address Space (Espacio de dirección de origen específico)**, el enrutador virtual descarta el paquete.
3. Seleccione **Included (Incluido)** para incluir espacio de dirección de origen específico como un rango de direcciones del grupo de multidifusión desde el cual el enrutador virtual aceptará los paquetes de multidifusión que se originaron desde una fuente específica permitida. Cancele la selección de **Included (Incluido)** para excluir fácilmente un espacio de direcciones de grupo de la prueba.
4. Añada otros espacios de direcciones de origen específico para incluir todos estos grupos para los cuales especificó el permiso de grupo de SSM.



STEP 10 | (Opcional) Cambie la cantidad de tiempo que una ruta de multidifusión permanece en mRIB después de que finalice la sesión entre un grupo de multidifusión y una fuente.

1. Seleccione la pestaña **Advanced (Avanzado)**.
2. Especifique el **Multicast Route Age Out Time (sec) (Tiempo de vencimiento de ruta de multidifusión [segundos])** (el intervalo es de 210 a 7200; el valor predeterminado es 210).

STEP 11 | Haga clic en **OK (Aceptar)** para guardar la configuración de multidifusión.

STEP 12 | Cree una regla de política de seguridad para permitir el tráfico de multidifusión a la zona de destino.

1. Cree una regla de política de seguridad y en la pestaña **Destination (Destino)**, seleccione **multicast (Multidifusión)** o **any (Cualquiera)** para la **Destination Zone (Zona de destino)**. La zona **multicast (Multidifusión)** es una zona de Capa 3 predefinida que coincide con todo el tráfico de multidifusión. La **Destination Address (Dirección de destino)** puede ser una dirección del grupo de multidifusión.
2. Configure el resto de la regla de política de seguridad.

STEP 13 | (Opcional) Habilite el almacenamiento en búfer de los paquetes de multidifusión antes de configurar una ruta.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Habilite el **Multicast Route Setup Buffering (Configuración del almacenamiento en búfer de la ruta de multidifusión)** (deshabilitado de forma predeterminada). El cortafuegos puede preservar los primeros paquetes desde un flujo de multidifusión si una entrada del grupo de multidifusión correspondiente todavía no existe en la tabla de reenvío de multidifusión (mFIB) El **Buffer Size (Tamaño del búfer)** controla cuántos paquetes almacena el cortafuegos en el búfer desde un flujo. Después de instalar la ruta en mFIB, el cortafuegos reenvía automáticamente los primeros paquetes almacenados en el búfer al receptor. (Solo debe habilitar la configuración de almacenamiento en el búfer de la ruta de multidifusión si los servidores de contenido están directamente conectados al cortafuegos y su aplicación de multidifusión no puede resistir que el primer paquete del flujo se omita).
3. (Opcional) Cambie el **Buffer Size (Tamaño del búfer)**. El tamaño del búfer es el número de paquetes por flujo de multidifusión que el cortafuegos puede almacenar en el búfer hasta que se configura la entrada de mFIB (el intervalo es de 1 a 2000; el valor predeterminado es 1000). El cortafuegos puede almacenar en el búfer un máximo de 5000 paquetes en total (para todos los flujos).
4. Haga clic en **OK (Aceptar)**.

STEP 14 | **Commit (Confirmar)** los cambios.

STEP 15 | Visualice la información de multidifusión de IP para ver las entradas de mRIB y mFIB, configuración de interfaz de IGMP, pertenencias de grupo de IGMP, modos de ASM SSM de PIM, asignaciones de grupo a los RP, direcciones de DR, configuración de PIM, vecinos de PIM y mucho más.

STEP 16 | Si configura una ruta estática para el tráfico de multidifusión, puede instalar la ruta solamente en la tabla de enrutamiento de multidifusión (no en la tabla de enrutamiento de unidifusión) de modo que la ruta se utilice solo para el tráfico de multidifusión.

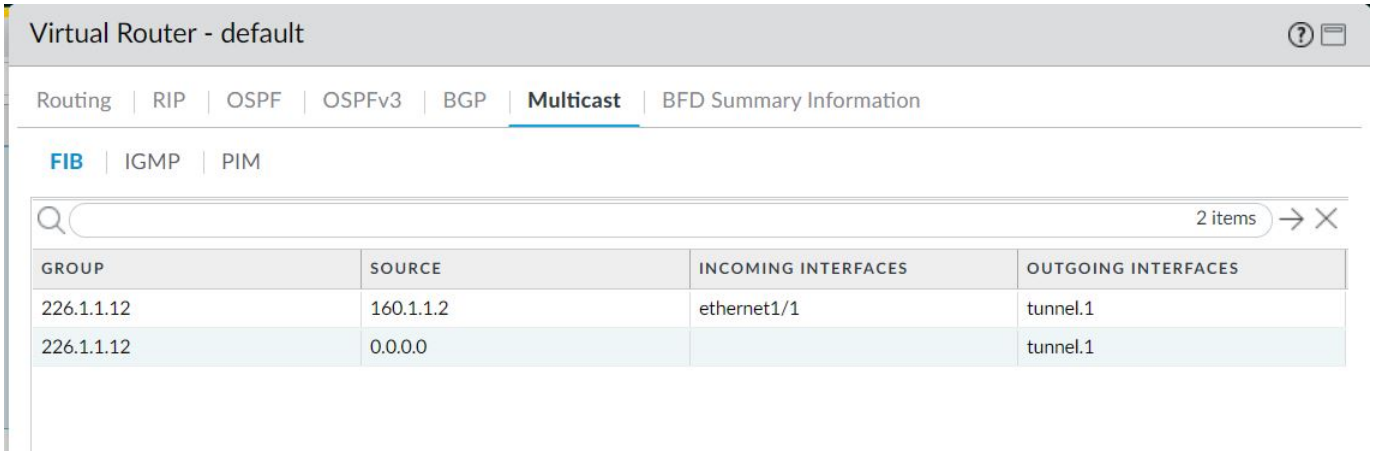
STEP 17 | Si habilita la multidifusión de IP, no es necesario configurar BGP con MP-BGP para la multidifusión de IPv4 salvo que tenga una topología de multidifusión lógica separada de una topología de unidifusión lógica. Configure extensiones MP-BGP con la familia de direcciones IPv4 y la familia de direcciones subsiguientes de multidifusión solo cuando desee anunciar prefijos de origen de multidifusión en BGP bajo la familia de direcciones subsiguientes de multidifusión.

Visualización de información de IP de multidifusión

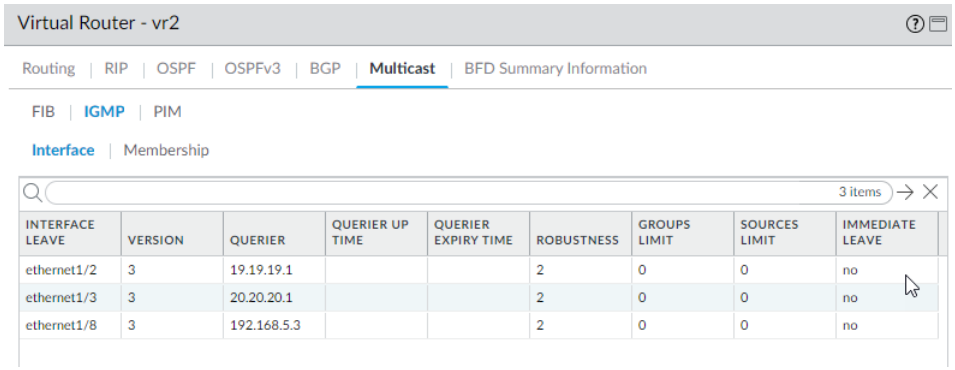
Luego de configurar el enrutamiento de la multidifusión de IP, visualice las rutas de multidifusión, las entradas de reenvío y la información sobre sus interfaces IGMP y PIM.

- Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual que configuró, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
  1. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de rutas)** y luego el botón de opción **Multicast (Multidifusión)** para mostrar solo las rutas de multidifusión (grupo de multidifusión de IP de destino, el siguiente salto a ese grupo y la interfaz de salida). Esta información proviene de la mRIB.
  2. Seleccione **Multicast (Multidifusión)** > **FIB** para ver la información de la ruta de multidifusión de la mFIB: grupos de multidifusión a los que pertenece el enrutador virtual, la fuente correspondiente, las interfaces de entrada y las interfaces de salida hacia los receptores.

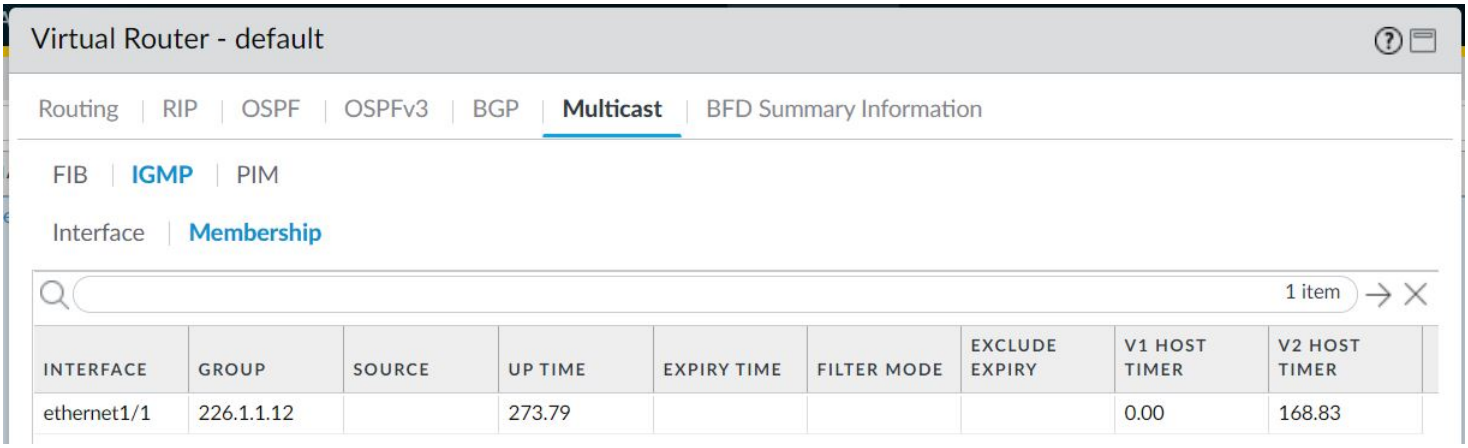
© 2020 Palo Alto Networks, Inc.



3. Seleccione **Multicast (Multidifusión)** > **IGMP** > **Interface (Interfaz)** para ver las interfaces habilitadas para IGMP, la versión de IGMP asociada, la dirección IP del solicitante de IGMP, el tiempo en actividad y la fecha de validez del solicitante, la configuración de potencia, los límites en la cantidad de fuentes y grupos de multidifusión, y si la interfaz está configurada para la salida inmediata.

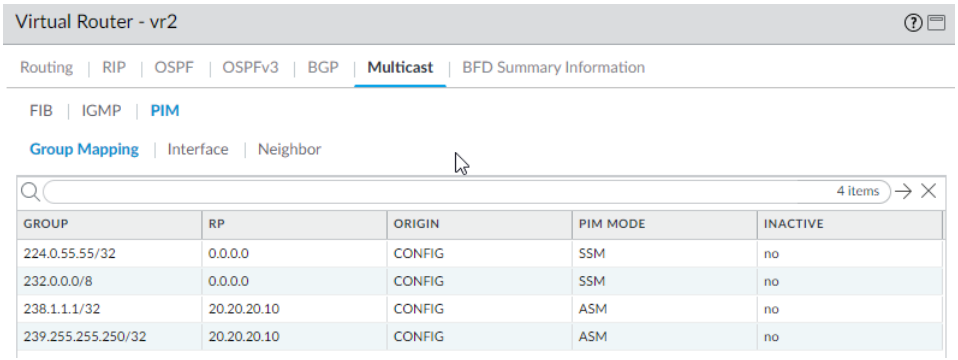


4. Seleccione **Multicast (Multidifusión)** > **IGMP** > **Membership (Pertenencia)** para ver las interfaces habilitadas para IGMP y los grupos de multidifusión a los cuales pertenecen, la fuente y otra información de IGMP.

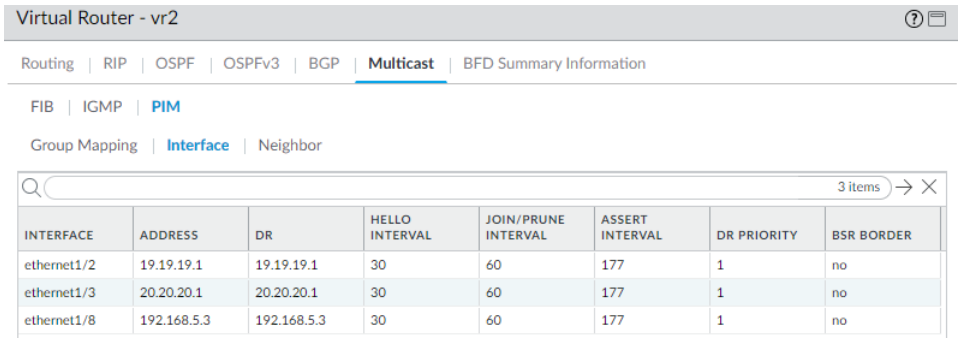


5. Seleccione **Multicast (Multidifusión)** > **PIM** > **Group Mapping (Asignación de grupos)** para ver los grupos de multidifusión asignados a un RP, el origen de la asignación de RP, el modo de PIM del grupo (ASM o SSM) y si el grupo está inactivo. Los grupos en modo SSM no usan un RP, de modo que la dirección de RP que se muestra es 0.0.0.0. El grupo SSM predeterminado es 232.0.0.0/8.

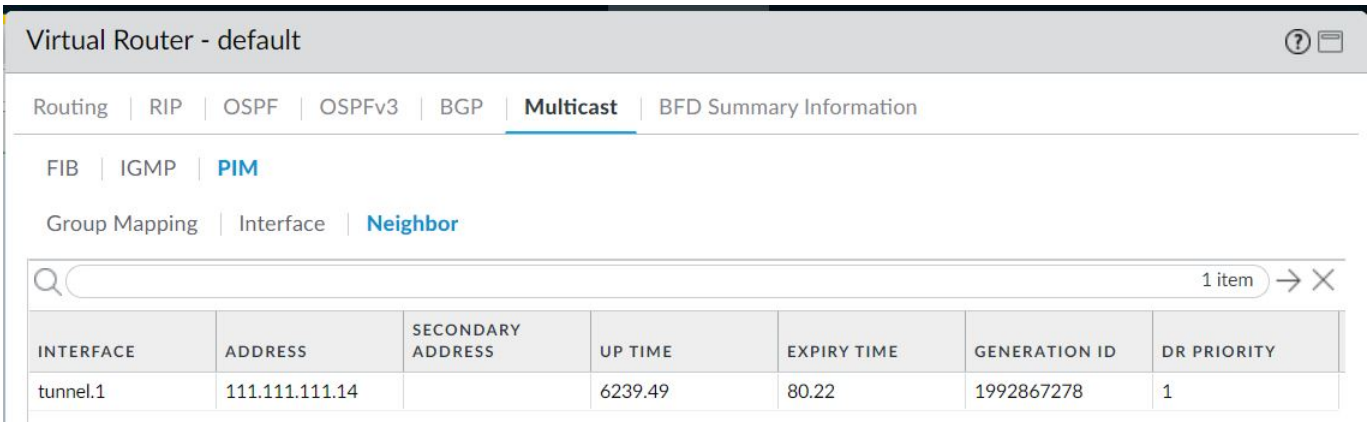
© 2020 Palo Alto Networks, Inc.



6. Seleccione **Multicast (Multidifusión)** > **PIM** > **Interface (Interfaz)** para ver la dirección IP del DR de una interfaz; la prioridad de DR; los intervalos de saludo, unión/eliminación e imposición; y si la interfaz es un enrutador de arranque (bootstrap router, BSR).



7. Seleccione **Multicast (Multidifusión)** > **PIM** > **Neighbor (Vecino)** para ver la información sobre enrutadores que son vecinos PIM del enrutador virtual.



© 2020 Palo Alto Networks, Inc.

Redistribución de ruta

La redistribución de rutas en el cortafuegos es el proceso de crear rutas que el cortafuegos obtuvo de un protocolo de enrutamiento (o una ruta estática o conectada) disponible para un protocolo de enrutamiento diferente, con lo cual se aumenta la accesibilidad del tráfico de red. Sin la redistribución de rutas, un enrutador o enrutador virtual anuncia y comparte rutas solo con otros enrutadores que se ejecutan en el mismo protocolo de enrutamiento. Puede redistribuir rutas BGP Ipv6 o IPv4, conectadas o estáticas en RIB OSPF y redistribuir rutas OSPFv3, conectadas o estáticas en RIB BGP.

Esto significa, por ejemplo, que puede crear redes específicas que una vez estuvieron disponibles solo mediante una configuración de ruta estática manual en enrutadores específicos para sistemas BGP autónomos o áreas OSPF. También puede anunciar rutas conectadas a nivel local, tal como rutas a una red de laboratorio privada, en sistemas BGP autónomos o en áreas OSPF.

Podría proporcionar a los usuarios de su red OSPFv3 interna acceso a BGP, para que puedan acceder a los dispositivos en Internet. En este caso, puede redistribuir las rutas BGP en el RIB OPSFv3.

Por el contrario, puede brindar a sus usuarios externos acceso a algunas partes de su red interna, de modo que puede poner sus redes OSPFv3 internas a disposición a través de BGP mediante la redistribución de las rutas OSPFv3 en el RIB de BGP.

STEP 1 | Cree un perfil de redistribución.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y, luego, **Add (Añadir)** para añadir un perfil.
3. Introduzca un **Name (Nombre)** para el perfil, que debe comenzar con un carácter alfanumérico y puede contener cero o más guiones bajos (_), guiones (-), puntos (.) o espacios (hasta 16 caracteres).
4. Introduzca una **Priority (Prioridad)** para el perfil en el intervalo de 1 a 255. El cortafuegos compara las rutas a los perfiles en orden y utiliza el perfil con la prioridad más alta (valor de prioridad más bajo) en primer lugar. Las reglas de prioridad más altas tienen preferencia sobre las reglas con prioridades más bajas.
5. Para **Redistribute (Redistribuir)**, seleccione una de las siguientes opciones:
   - **Redist (Redistribuir)**: seleccione esta opción para la redistribución de las rutas que coincidan con este filtro.
   - **No Redist (No redistribuir)**: seleccione las rutas de redistribución que coincidan con los perfiles de redistribución, excepto las rutas que coincidan con este filtro. Esta selección trata el perfil como una lista de bloqueo que especifica qué rutas no se deben seleccionar para la redistribución. Por ejemplo, si tiene varios perfiles de redistribución para BGP, puede crear un perfil **No Redist (No redistribuir)** para excluir varios prefijos y luego un perfil de redistribución general con una prioridad más baja (valor de prioridad más alto) posterior a aquel. Los dos perfiles se combinan y el perfil de prioridad más alta tiene preferencia. No puede tener solo perfiles **No Redist (No redistribuir)**; siempre necesita al menos un perfil **Redist (Redistribuir)** para redistribuir rutas.
6. En la pestaña **General Filter (Filtro general)**, para Source Type (Tipo de origen), seleccione uno o más tipos de rutas para redistribuir:
   - **bgp**: redistribuya rutas BGP que coincidan con el perfil.
   - **connect**: redistribuya rutas conectadas que coincidan con el perfil.
   - **ospf** (solo IPv4): redistribuya rutas OSPF que coincidan con el perfil.
   - **rip** (solo IPv4): redistribuya rutas RIP que coincidan con el perfil.
   - **ospfv3** (solo IPv6): redistribuya rutas OSPFv3 que coincidan con el perfil.
   - **static**: redistribuya rutas estáticas que coincidan con el perfil.

© 2020 Palo Alto Networks, Inc.

7. (Opcional) Para **Interface (Interfaz)**, seleccione **Add (Añadir)** y añada una o más interfaces de salida de las rutas asociadas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
8. (Opcional) Para **Destination (Destino)**, seleccione **Add (Añadir)** y añada uno o más destinos IPv4 o IPv6 de las rutas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
9. (Opcional) Para **Next Hop (Próximo salto)**, seleccione **Add (Añadir)** y añada una o más direcciones IPv4 o IPv6 de próximo salto de las rutas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional: cuando el filtrado general incluye ospf u ospfv3) Cree un filtro OSPF para especificar en detalle qué rutas OSPF u OSPFv3 redistribuir.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y seleccione el perfil que creó.
3. Seleccione **OSPF Filter (Filtro OSPF)**.
4. Para Path Type (Tipo de ruta), seleccione uno o más de los siguientes tipos de ruta OSPF para redistribuir: **ext-1**, **ext-2**, **inter-area**, or **intra-area**.
5. Para especificar un **Area (Área)** desde la cual redistribuir las rutas OSPF u OSPFv3, seleccione **Add (Añadir)** y añada un área en formato de dirección IP.
6. Para especificar una **Tag (Etiqueta)**, seleccione **Add (Añadir)** para añadir una etiqueta en formato de dirección IP.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional: cuando el filtrado general incluye bgp) Cree un filtro BGP para especificar en detalle qué rutas BGP redistribuir.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y seleccione el perfil que creó.
3. Seleccione **BGP Filter (Filtro BGP)**.
4. Para **Community (Comunidad)**, seleccione **Add (Añadir)** para seleccionar de la lista de comunidades, tal como las comunidades reconocidas: **local-as**, **no-advertise**, **no-export**, or **nopeer**. También puede introducir un valor de 32 bits en formato decimal o hexadecimal o formato AS:VAL en el que AS y VAL estén dentro del intervalo de 0 a 65 535. Introduzca un máximo de 10 entradas.
5. Para **Extended Community (Comunidad extendida)**, seleccione **Add (Añadir)** para añadir una comunidad extendida como un valor de 64 bits en formato hexadecimal o en formato TYPE:AS:VAL o TYPE:IP:VAL. TYPE es de 16 bits; AS o IP es de 16 bits; VAL es de 32 bits. Introduzca un máximo de cinco entradas.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione el protocolo en el cual está redistribuyendo las rutas, y establezca los atributos para esas rutas.

Esta tarea ilustra las rutas de redistribución en BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **BGP** > **Redist Rules (Reglas de redistribución)**.
3. Seleccione **Allow Redistribute Default Route (Permitir ruta predeterminada de redistribución)** para permitir que el cortafuegos redistribuya la ruta predeterminada.
4. Haga clic en **Add (Añadir)**.
5. Seleccione **Address Family Type (Tipo de familia de direcciones)**: **IPv4** o **IPv6** para especificar en qué tabla de rutas se colocarán las rutas redistribuidas.

© 2020 Palo Alto Networks, Inc.

6. En **Name (Nombre)**, seleccione el nombre del perfil de redistribución que creó, que selecciona las rutas para redistribuir.
7. Seleccione **Enable (Habilitar)** para habilitar la regla de redistribución.
8. (Opcional) Ingrese cualquiera de los siguientes valores, que el cortafuegos aplica a las rutas que se están redistribuyendo:
   - **Metric (Métrica)** en el intervalo de 1 a 65 535.
   - **Set Origin (Establecer origen)**; el origen de la ruta: **igp**, **egp**, or **incomplete**.
   - **Set MED (Configurar MED)**: valor MED en el intervalo de 0 a 4 294 967 295.
   - **Set Local Preference (Establecer preferencia local)**: valor de preferencia local en el intervalo de 0 a 4 294 967 295.
   - **Set AS Path Limit (Establecer límite de ruta AS)**: cantidad máxima de sistemas autónomos en AS_PATH en el intervalo de 1 a 255.
   - **Set Community (Establecer comunidad)**: seleccione o introduzca un valor de 32 bits en formato decimal o hexadecimal, o introduzca un valor en formato AS:VAL en el que AS y VAL estén dentro del intervalo de 0 a 65 525. Introduzca un máximo de 10 entradas.
   - **Set Extended Community (Establecer comunidad extendida)**: seleccione o introduzca una comunidad extendida como un valor de 64 bits en formato hexadecimal o en formato TYPE:AS:VAL o TYPE:IP:VAL. TYPE es de 16 bits; AS o IP es de 16 bits; VAL es de 32 bits. Introduzca un máximo de cinco entradas.
9. Haga clic en **OK (Aceptar)**.

STEP 5 | **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Túneles GRE

El protocolo de túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) es un protocolo de operador que encapsula un protocolo de carga. El paquete de GRE se encapsula en un protocolo de transporte (IPv4 o IPv6).

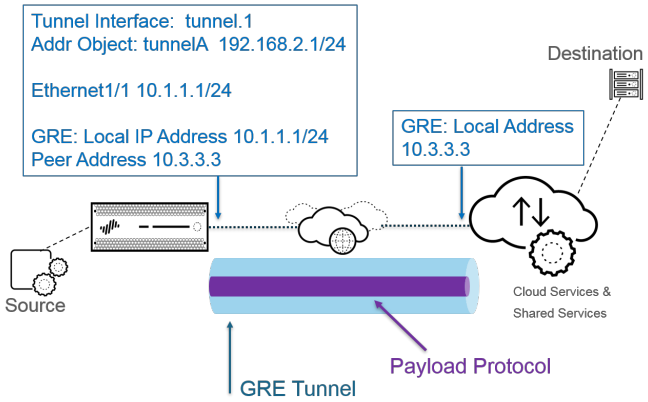
- Descripción general de los túneles de GRE
- Creación de túneles de GRE

Descripción general de los túneles de GRE

Un túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) se conecta a dos endpoints (un cortafuegos y otro dispositivo) con un enlace lógico punto a punto. El cortafuegos puede finalizarlos, y el usuario puede enrutar o reenviar paquetes a los túneles de GRE. Son tan fáciles de usar que se suelen elegir como protocolo de tunelización para ofrecer conectividad de punto a punto, sobre todo a los servicios en la nube o a las redes de socios.

Cree un túnel de GRE para que los paquetes destinados a cierta dirección IP sigan una ruta de punto a punto concreta, por ejemplo, a un proxy basado en la nube o a la red de un socio. Los paquetes atraviesan el túnel de GRE (por una red de tránsito como Internet) hasta servicio en la nube en su camino hacia la dirección de destino. De ese modo, el servicio en la nube puede aplicarles sus servicios o políticas.

En la figura siguiente se muestra un ejemplo de túnel de GRE que conecta el cortafuegos con un servicio en la nube a través de internet.



Para mejorar el rendimiento y para evitar fallos en puntos únicos, reparta las conexiones al cortafuegos entre varios túneles de GRE en vez de usar uno. Cada túnel de GRE necesita una interfaz de túnel.

Cuando el cortafuegos permite que un paquete pase (basándose en una coincidencia con la política) y el paquete sale a una interfaz de túnel de GRE, el cortafuegos añade encapsulación GRE, pero no genera ninguna sesión. El cortafuegos no realiza una búsqueda de las reglas de la política de seguridad para el tráfico encapsulado con GRE, por lo que no hacen falta en este caso. Ahora bien, cuando el cortafuegos recibe tráfico de GRE, genera una sesión y aplica todas las políticas al encabezado IP de GRE, además de al tráfico encapsulado. El cortafuegos trata el paquete de GRE recibido como cualquier otro paquete. Por lo tanto:

- Si el cortafuegos recibe el paquete de GRE en una interfaz que tiene la misma zona que la interfaz asociada al túnel de GRE (por ejemplo, tunnel.1 [túnel.1]), la zona de origen es la misma que la zona de destino. Como el tráfico se permite dentro de una zona concreta de manera predeterminada (tráfico intrazona), el tráfico de GRE de entrada también está permitido por defecto.

© 2020 Palo Alto Networks, Inc.

- No obstante, si configura una regla de la política de seguridad propia sobre intrazonas en la política de seguridad para denegar dicho tráfico, debe permitir de forma explícita el tráfico de GRE.
- De igual modo, si la zona de la interfaz asociada al túnel de GRE (por ejemplo, tunnel.1 [túnel.1]) es distinta de la zona de la interfaz de entrada, debe configurar una regla de la política de seguridad para permitir el tráfico de GRE.

Como el cortafuegos encapsula el paquete tunelizado en un paquete de GRE, los 24 bytes adicionales del encabezado de GRE tienen de forma automática un Tamaño de segmento máximo (MSS) más reducido en la unidad máxima de transmisión (Maximum Transmission Unit, MTU). Si no modifica el tamaño de ajuste del tamaño máximo de segmento (Maximum Segment Size, MSS) de IPv4 correspondiente a la interfaz, el cortafuegos reduce la MTU en 64 bytes (40 bytes del encabezado de IP más 24 bytes del encabezado de GRE) de forma predeterminada. Eso significa que, si la MTU predeterminada es de 1500 bytes, el MSS es de 1436 bytes (1500 - 40 - 24 = 1436). Si configura un tamaño de ajuste de MSS de 300 bytes, por ejemplo, el MSS es de solo 1,176 bytes (1500 - 300 - 24 = 1176).

El cortafuegos no admite el enrutamiento de un túnel de GRE o IPSec a un túnel de GRE, pero puede enrutar un túnel de GRE a un túnel de IPSec. Adicionalmente:

- Los túneles de GRE no admiten la calidad de servicio (quality of service, QoS).
- El cortafuegos no admite que una sola interfaz funcione a la vez como terminal de túneles de GRE y como agente de descifrado.
- La tunelización de GRE no admite la traducción de direcciones de red (network address translation, NAT) entre los terminales de los túneles de GRE.



Si necesita conectarse a la red de otro proveedor, le recomendamos Configuración de un túnel de IPSec, no un túnel de GRE; debe usar un túnel de GRE solo si es el único mecanismo de túnel punto a punto que admite el proveedor. Además, si el endpoint remoto exige GRE por IPSec, puede habilitar esta opción en Add GRE Encapsulation (Añadir encapsulación GRE). Añada la encapsulación GRE si el terminal remoto exige que se encapsule el tráfico del túnel de GRE antes de que IPSec lo cifre. En algunas implementaciones, por ejemplo, es obligatorio encapsular el tráfico de multidifusión para que IPSec pueda cifrarlo. Si es un requisito de su entorno y si los túneles de GRE y de IPSec comparten la dirección IP, seleccione Add GRE Encapsulation (Añadir encapsulación GRE) cuando configure el túnel de IPSec.



Si desea inspeccionar y controlar el tráfico que atraviesa el cortafuegos por un túnel de GRE, pero no tiene intención de finalizar este, no lo cree; en su lugar, realice el procedimiento Inspección del contenido del túnel para inspeccionar el tráfico de GRE. Aparte de tener esa finalidad, la inspección del contenido permite aplicar la política al tráfico de GRE que pasa a través del cortafuegos sin crear un enlace lógico punto a punto para dirigir el tráfico.

Creación de túneles de GRE

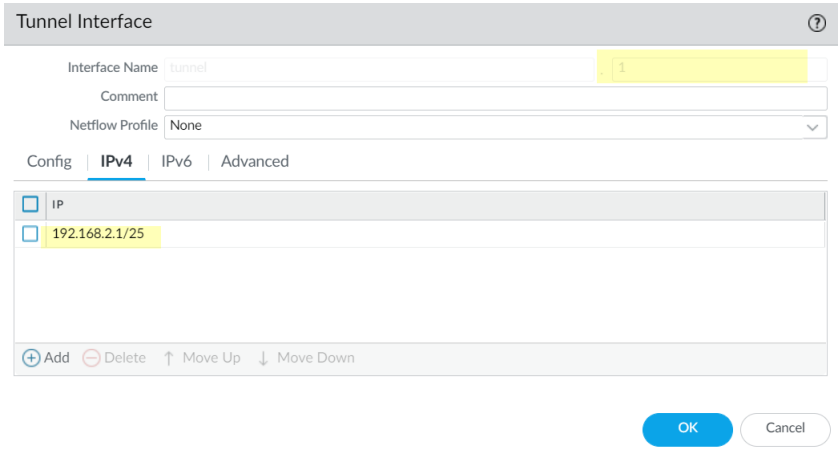
Cree un túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) para conectar dos endpoints con un enlace lógico punto a punto.

STEP 1 | Cree una interfaz de túnel.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)**.
2. **Añada** un túnel y especifique el **nombre de interfaz**seguido por un punto y un número (el intervalo es de 1 a 9999). Por ejemplo, `tunnel.1`.
3. En la pestaña **Config (Configuración)**, asigne la interfaz de túnel a un enrutador en **Virtual Router (Enrutador virtual)**.
4. Si el cortafuegos admite varios sistemas virtuales, asigne la interfaz de túnel a uno concreto en **Virtual System (Sistema virtual)**.

© 2020 Palo Alto Networks, Inc.

5. Asigne la interfaz de túnel a una zona segura en **Security Zone (Zona de seguridad)**.



6. Asigne una dirección IP a la interfaz de túnel. Es obligatorio asignarla si desea realizar el enrutamiento a este túnel o supervisar su terminal. Seleccione **IPv4** o **IPv6** o bien configure ambas opciones.

   Tanto esta dirección como la dirección correspondiente de la interfaz de túnel del peer deben estar en la misma subred, ya que es un enlace lógico de punto a punto.

   - (Solo IPv4) En la pestaña **IPv4**, haga clic en **Add (Añadir)** para agregar una dirección IPv4 o seleccionar un objeto de dirección o bien haga clic en **New Address (Nueva dirección)**, especifique el **tipo** de dirección e introdúzcala. Por ejemplo, especifique `192.168.2.1/25`.
   - (Solo IPv6) En la pestaña **IPv6**, **habilite IPv6 en la interfaz**.
     1. En **Interface ID (ID de interfaz)**, seleccione **EUI-64 (default 64-bit Extended Unique Identifier) (EUI-64 [identificador único ampliado de 64 bits predeterminado])**.
     2. **Añada** una nueva **dirección**, seleccione un objeto de dirección IPv6 o haga clic en **New Address (Nueva dirección)** y especifique un **nombre** de dirección. **Habilite la dirección en la interfaz** y haga clic en **OK (Aceptar)**.
     3. Seleccione el **tipo** de dirección y especifique la dirección IPv6 o FQDN y haga clic en**OK (Aceptar)** para guardar la nueva dirección.
     4. Seleccione **Enable address on interface (Habilitar la dirección en la interfaz)** y haga clic en **OK (Aceptar)**.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree un túnel de GRE para forzar que los paquetes atraviesen una ruta de punto a punto concreta.

1. Seleccione **Network (Red)** > **GRE Tunnels (Túneles de GRE)** y haga clic en **Add (Añadir)** para añadir un túnel según el valor de **Name (Nombre)**.
2. Seleccione la **interfaz** que se usará como en endpoint de túnel GRE (interfaz de túnel), que es una interfaz o subinterfaz Ethernet, una interfaz Ethernet de agregación (Aggregate Ethernet, AE), una interfaz de bucle invertido o una interfaz VLAN.
3. En **Local Address (Dirección local)**, seleccione la dirección que se debe introducir en **IP** y, luego, seleccione la dirección IP de la interfaz que acaba de seleccionar.
4. En **Peer Address (Dirección de peer)**, introduzca la dirección IP del terminal opuesto del túnel de GRE.
5. En **Tunnel Interface (Interfaz de túnel)**, seleccione la interfaz creada en el paso 1. Este valor identifica el túnel cuando actúa como interfaz de salida del enrutamiento.
6. Introduzca el **TTL** para el paquete IP encapsulado en el paquete GRE (el intervalo es de 1 a 255, el valor predeterminado es 64).

© 2020 Palo Alto Networks, Inc.

7. Marque **Copy ToS Header (Copiar encabezado de ToS)** para copiar el campo del tipo de servicio (type of service, ToS) del encabezado de la IP interna en el encabezado de la IP externa de los paquetes encapsulados a fin de conservar la información original del ToS. Seleccione esta opción si la red utiliza la calidad de servicio (quality of service, QoS) y depende de los bits del ToS para aplicar las políticas de QoS.



STEP 3 | (Práctica recomendada) Habilite la función de conexión persistente en el túnel de GRE.

Si habilita la opción de conexión persistente, de manera predeterminada, toma tres paquetes keepalive no devueltos (reintentos) a intervalos de 10 segundos para que el túnel de GRE se desactive y toma cinco intervalos del temporizador de espera a intervalos de 10 segundos para que el túnel de GRE se reactive.

1. Haga clic en **Keep Alive (Conexión permanente)** para habilitar esta función en el túnel de GRE (no está activada de manera predeterminada).
2. (Opcional) En **Interval (sec) (Intervalo [s])**, configure los segundos que deben transcurrir entre los paquetes keepalive (conexión permanente) que envía el extremo local del túnel de GRE a su peer. Al multiplicar este intervalo por el valor de **Hold Timer (Temporizador de espera)**, se obtiene el tiempo durante el que el cortafuegos debe detectar paquetes keepalive (conexión permanente) correctos para que se vuelva a activar el túnel de GRE (el intervalo es de 1 a 50; el valor predeterminado es 10). Si configura un intervalo demasiado breve, pueden aparecer muchos paquetes keepalive (conexión permanente) innecesarios en el entorno, que exigen ancho de banda y procesamiento adicionales. Si configura un intervalo demasiado prolongado, se puede retrasar la conmutación por error porque no se identifican de inmediato las condiciones de error.
3. (Opcional) Introduzca el ajuste **Retry (Reintentar)**, que indica cuántos intervalos sin devolución de paquetes keepalive (conexión permanente) deben pasar para que el cortafuegos considere que el peer del túnel está inactivo (el intervalo es de 1 a 255; el valor predeterminado es 3). Si el túnel está inactivo, el cortafuegos elimina las rutas asociadas de la tabla de reenvío. Configure esta opción para evitar que se tomen medidas en túneles que no están desactivados.
4. (Opcional) En **Hold Timer (Temporizador de espera)**, configure cuántos intervalos con paquetes keepalive (conexión permanente) correctos deben pasar para que el cortafuegos restablezca la comunicación con el peer del túnel (el intervalo es de 1 a 64; el valor predeterminado es 5).

STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Configure un protocolo de enrutamiento o una ruta estática para enrutar el tráfico al destino por medio del túnel de GRE. Por ejemplo, realice el procedimiento Configuración de una ruta estática para configurar la ruta a la red del servidor de destino y especifique la interfaz de

© 2020 Palo Alto Networks, Inc.

salida que funciona como endpoint local del túnel (tunnel.1). Configure como siguiente salto la dirección IP del extremo opuesto del túnel. Por ejemplo, 192.168.2.3.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Configure el extremo opuesto del túnel con su dirección IP pública, con las direcciones IP local y del peer (que se corresponden, respectivamente, con las direcciones IP del peer y local del túnel de GRE del cortafuegos) y con su protocolo de enrutamiento o ruta estática.

STEP 8 | Verifique que el cortafuegos se comunica con su peer por el túnel de GRE.

1. Acceso a la CLI.
2. `> ping source 192.168.2.1 host 192.168.2.3`

© 2020 Palo Alto Networks, Inc.

DHCP

Esta sección describe el protocolo de configuración de host dinámico (DHCP) y las tareas necesarias para configurar una interfaz en un cortafuegos de Palo Alto Networks para actuar como servidor, cliente o agente de relé de DHCP. Al asignar esas funciones a distintas interfaces, el cortafuegos puede desempeñar múltiples funciones.

- Descripción general de DHCP
- Cortafuegos como servidor y cliente DHCP
- Mensajes DHCP
- Direccionamiento DHCP
- Opciones de DHCP
- Configure una interfaz como servidor DHCP
- Configure una interfaz como cliente DHCP
- Configuración de la interfaz de gestión como cliente DHCP
- Configure una interfaz como agente de relé DHCP
- Supervisión y resolución de problemas de DHCP

Descripción general de DHCP

DHCP es un protocolo estandarizado definido en RFC 2131, Protocolo de configuración de host dinámico. DHCP tiene dos objetivos principales: Proporcionar los parámetros de configuración de capa de enlace y TCP/IP y proporcionar direcciones de red con hosts configurados dinámicamente en la red TCP/IP.

DHCP usa un modelo cliente-servidor de comunicación. Este modelo consta de tres funciones que puede desempeñar el dispositivo: Cliente DHCP, servidor DHCP y agente de relé DHCP.

- Un dispositivo que funcione como cliente DHCP (host) puede solicitar una dirección IP y otros ajustes de configuración al servidor DHCP. Los usuarios de los dispositivos cliente ahorran el tiempo y esfuerzo de configuración, y no necesitan conocer el plan de direcciones de red y otros recursos y opciones que heredan del servidor DHCP.
- Un dispositivo que actúa como un servidor DHCP puede atender a los clientes. Si se usa alguno de esos tres mecanismos de Direccionamiento DHCP, el administrador de red ahorra tiempo y tiene la ventaja de reutilizar un número limitado de direcciones IP cuando un cliente ya no necesita una conectividad de red. El servidor puede ofrecer direcciones IP y muchas opciones DHCP a muchos clientes.
- Un dispositivo que actúa como un agente de relé DHCP transmite mensajes DHCP entre los clientes y los servidores DHCP.

DHCP usa el protocolo de datagramas de usuario (UDP), RFC 768, como su protocolo de transporte. Los mensajes DHCP que un cliente envía a un servidor se envían al puerto conocido 67 (UDP, protocolo de arranque y DHCP). Mensajes DHCP que un servidor envía a un cliente se envían al puerto 68.

Una interfaz de un cortafuegos de Palo Alto Networks puede realizar la función de un servidor, un cliente o un agente de relé DHCP. La interfaz de un servidor o agente de relé DHCP debe ser una interfaz VLAN de capa 3, Ethernet agregado o Ethernet de capa 3. Puede configurar las interfaces del cortafuegos con la configuración adecuada para cualquier combinación de funciones. El comportamiento de cada función se resume en Cortafuegos como servidor y cliente DHCP.

El cortafuegos admite el servidor DHCPv4 y el relé DHCPv6. Sin embargo, una única interfaz no admite el servidor DHCPv4 y el relé DHCPv6.

Las implementaciones de Palo Alto Networks del servidor DHCP y el cliente DHCP solo admiten direcciones IPv4. Su implementación del relé DHCP admite IPv4 e IPv6. El cliente DHCP no es compatible en el modo HA activo/activo.

© 2020 Palo Alto Networks, Inc.

Cortafuegos como servidor y cliente DHCP

El cortafuegos puede funcionar como servidor DHCP y como cliente DHCP. El protocolo de configuración de host dinámico, Dynamic Host Configuration Protocol, RFC 2131, se ha diseñado para admitir direcciones IPv4 e IPv6. La implementaciones de Palo Alto Networks del servidor DHCP admite solo direcciones IPv4.

El servidor DHCP funciona del siguiente modo:

- Cuando el servidor DHCP recibe un mensaje DHCPDISCOVER de un cliente, responde con un mensaje DHCPOFFER que contiene todas las opciones predefinidas y las opciones definidas por el usuario en el orden que aparecen en la configuración. El cliente selecciona las opciones que necesita y responde con un mensaje DHCPREQUEST.
- Cuando el servidor recibe un mensaje DHCPREQUEST de un cliente, el servidor responde con su mensaje DHCPACK, que contiene solo las opciones especificadas en la solicitud.

El cliente DHCP del cortafuegos funciona del siguiente modo:

- Cuando el cliente DHCP recibe una DHCPOFFER del servidor, el cliente automáticamente almacena en caché todas las opciones ofrecidas para futuros usos, independientemente de las opciones que enviara en su DHCPREQUEST.
- De manera predeterminada, y para ocupar menos memoria, el cliente almacena en caché solo el primer valor de cada código de opción si recibe varios valores para un código.
- No hay una longitud máxima para mensajes DHCP a menos que el cliente DHCP especifique un máximo en la opción 57 en sus mensajes DHCPDISCOVER o DHCPREQUEST.

Mensajes DHCP

DHCP usa ocho tipos de mensajes estándar, que se identifican mediante un número de tipo de opción en el mensaje DHCP. Por ejemplo, cuando un cliente quiere encontrar un servidor DHCP, difunde un mensaje DHCPDISCOVER en su subred física local. Si no hay ningún servidor DHCP en su subred y si DHCP auxiliar o un relé DHCP se configura adecuadamente, el mensaje se reenvía a los servidores DHCP en una subred física diferente. De lo contrario, el mensaje no avanzará más allá de la subred en la que se origina. Uno o más servidores DHCP responderán al mensaje DHCPOFFER que contienen una dirección de red disponible y otros parámetros de configuración.

Cuando el cliente necesita una dirección IP, envía un DHCPREQUEST a uno o más servidores. Por supuesto, si el cliente solicita una dirección IP, aún no tiene una, por lo que RFC 2131 requiere que el mensaje de difusión que envía el cliente tenga una dirección de origen de 0 en su encabezado IP.

Cuando un cliente solicita parámetros de configuración desde un servidor, puede recibir respuestas de más de un servidor. Cuando un cliente ha recibido su dirección IP, se dice que el cliente tiene al menos una dirección IP y posiblemente otros parámetros de configuración *vinculados* a ella. Los servidores DHCP gestionan esa vinculación de parámetros de configuración con los clientes.

La siguiente tabla enumera los mensajes de DHCP.

Mensaje DHCP	Description (Descripción)
DHCPDISCOVER	El cliente realiza una difusión para buscar los servidores DHCP disponibles.
DHCPOFFER	La respuesta del servidor al DHCPDISCOVER del cliente, ofreciendo parámetros de configuración.
DHCPREQUEST	Mensaje del cliente dirigido a uno o más servidores para hacer algo de lo siguiente:

© 2020 Palo Alto Networks, Inc.

Mensaje DHCP	Description (Descripción)
	• Solicitar los parámetros a un servidor y rechazar implícitamente ofertas de otros servidores. • Confirmar que una dirección antes asignada es correcta, por ejemplo, un reinicio del sistema. • Extender la concesión de una dirección de red.
DHCPACK	El mensaje de reconocimiento del servidor al cliente, que contiene los parámetros de configuración, incluida una dirección de red confirmada.
DHCPNAK	Reconocimiento negativo del servidor al cliente, que indica que el cliente comprende que la dirección de red es incorrecta (por ejemplo, si el cliente se mueve a una subred nueva) o que la concesión del cliente ha vencido.
DHCPDECLINE	Mensaje de cliente a servidor que indica que la dirección de red ya se está usando.
DHCPRELEASE	Mensaje de cliente a servidor que da al usuario la dirección de red y cancela el tiempo restante de la concesión.
DHCPINFORM	Mensaje de cliente a servidor que solicita únicamente los parámetros de configuración local; el cliente tiene una dirección de red configurada externamente.

Direccionamiento DHCP

- Métodos de asignación de direcciones DHCP
- Concesiones DHCP

Métodos de asignación de direcciones DHCP

El servidor DHCP asigna o envía una dirección IP a un cliente de tres formas:

- **Ubicación automática**: El servidor DHCP asigna una dirección IP permanente a un cliente desde sus **IP Pools (Grupos de IP)**. En el cortafuegos, una **Lease (Concesión)** que se especifique como **Unlimited (Ilimitada)** significa que la ubicación es permanente.
- **Ubicación dinámica**: El servidor DHCP asigna una dirección IP reutilizable desde **IP Pools (Grupos de IP)** de direcciones a un cliente para un periodo máximo de tiempo, conocido como *Concesión*. Este método de asignación de la dirección es útil cuando el cliente tiene un número limitado de direcciones IP; pueden asignarse a los clientes que necesitan solo un acceso temporal a la red. Consulte la sección DHCP Leases (Concesiones DHCP)
- **Asignación estática**: El administrador de red selecciona la dirección IP para asignarla al cliente y el servidor DHCP se la envía. La asignación DHCP estática es permanente; se realiza configurando un servidor DHCP y seleccionando una **Reserved Address (Dirección reservada)** para que corresponda con la **MAC Address (Dirección MAC)** del dispositivo cliente. La asignación DHCP continúa en su lugar aunque el cliente cierre sesión, reinicie, sufra un corte de alimentación, etc.

  La asignación estática de una dirección IP es útil, por ejemplo, si tiene una impresora en una LAN y no desea que su dirección IP siga cambiando porque se asocia con un nombre de impresora a través de DNS. Otro ejemplo es si el dispositivo cliente se usa para una función crucial y debe mantener la misma dirección IP aunque el dispositivo se apague, desconecte, reinicie o sufra un corte de alimentación, etc.

  Tenga lo siguiente en cuenta cuando configure una **Reserved Address (Dirección reservada)**:

© 2020 Palo Alto Networks, Inc.

- Es una dirección de **IP Pools (Grupos de IP)**. Puede configurar múltiples direcciones reservadas.
- Si no configura ninguna **Reserved Address (Dirección reservada)**, los clientes del servidor recibirán nuevas asignaciones de DHCP del grupo cuando sus concesiones venzan o si se reinician, etc. (a no ser que haya especificado que una **Lease (Concesión)** sea **Unlimited (Ilimitada)**).
- Si asigna todas las direcciones de **IP Pools (Grupos IP)** como una **Reserved Address (Dirección reservada)**, no hay direcciones dinámicas libres para asignar al siguiente cliente DHCP que solicite una dirección.
- Puede configurar una **Dirección reservada (Dirección reservada)** sin configurar una **Dirección MAC (Dirección MAC)**. En este caso, el servidor DHCP no asignará la **Reserved Address (Dirección reservada)** a ningún dispositivo. Puede reservar unas direcciones del grupo y asignarlas estáticamente a un fax e impresora, por ejemplo, sin usar DHCP.

Concesiones DHCP

Una concesión se define como la duración durante la que el servidor DHCP asigna a una dirección IP para un cliente. La concesión puede extenderse (renovarse) en las solicitudes posteriores. Si el cliente ya no necesita la dirección, puede liberarla en el servidor antes de que la concesión termine. El servidor es entonces libre de asignar esa dirección a un cliente distinto, si ya se le han agotado las direcciones sin asignar.

El periodo de concesión configurado para un servidor DHCP se aplica a todas las direcciones que un servidor DHCP único (interfaz) asigna dinámicamente a sus clientes. Es decir, todas las direcciones de interfaz asignadas dinámicamente tienen una duración **Ilimitada** o el mismo valor de **Tiempo de espera**. Un servidor DHCP diferente configurado en el cortafuegos puede tener un plazo de concesión distinto para sus clientes. Una **Reserved Address (Dirección reservada)** es una asignación de dirección estática y no está sometida a esas condiciones de concesión.

Según el estándar DHCP, RFC 2131, un cliente DHCP no espera a que la concesión venza, ya que se arriesga a que se le asigne una nueva dirección. En su lugar, cuando un cliente DHCP alcanza el punto medio de su periodo de concesión, intenta extenderla para conservar la misma dirección IP. Así, la duración de la concesión es como una ventana corredera.

Por lo general, si se ha asignado una dirección IP a un dispositivo, y este se saca de la red sin prolongar su concesión, el servidor DHCP dejará que esa concesión se agote. Como el cliente ha salido de la red y ya no necesita la dirección, se alcanza la duración de la concesión del servidor y la concesión pasa al estado "Expirado".

El cortafuegos tiene un temporizador de espera que evita que la dirección IP expirada se reasigne inmediatamente. Este sistema reserva temporalmente la dirección para el dispositivo en caso de que vuelva a la red. Pero si el grupo de direcciones se queda sin direcciones, el servidor reubicará esta dirección expirada antes de que se termine el temporizador de espera. Las direcciones expiradas se borran automáticamente a medida que los sistemas necesitan más direcciones o cuando el temporizador de espera las libera.

En la CLI, use el comando operativo **`show dhcp server lease`** para ver la información de concesión de las direcciones IP asignadas. Si no desea esperar a que las concesiones vencidas se liberen automáticamente, puede utilizar el comando **`clear dhcp lease interface <interface> expired-only`** para borrar las concesiones vencidas y permitir que vuelvan a estar disponibles en el grupo. Puede utilizar el comando **`clear dhcp lease interface <interface> ip <ip_address>`** para liberar una dirección IP concreta. Puede utilizar el comando **`clear dhcp lease interface <interface> mac <mac_address>`** para liberar una dirección MAC concreta.

Opciones de DHCP

La historia del DHCP y sus opciones DHCP se remonta al protocolo de arranque (BOOTP). Un host usó BOOTP para configurarse dinámicamente durante su procedimiento de arranque. El host recibía una

© 2020 Palo Alto Networks, Inc.

dirección IP y un archivo desde el que descargaba un programa de arranque desde un servidor, junto con la dirección del servidor y la dirección de la gateway de Internet.

En el BOOTP incluía un campo de información del proveedor, que contenía un número de campos etiquetados con distintos tipos de información como la máscara de subred, el tamaño del archivo BOOTP y muchos otros valores. RFC 1497 describe las extensiones de información de proveedor BOOTP. El DHCP sustituye a BOOTP; no se admite BOOTP en el cortafuegos.

Estas extensiones llegan a expandirse con el uso de los parámetros de configuración de host DHCP y DHCP, conocidos como opciones. Al igual que las extensiones de proveedor, las opciones de DHCP son elementos de datos etiquetados que proporcionan información a un cliente DHCP. La opciones se envían en un campo de longitud variable al final de un mensaje DHCP. Por ejemplo, el tipo de mensaje DHCP es la opción 53, y un valor de 1 indica un mensaje DHCPDISCOVER. Las opciones DHCP se definen en RFC 2132, Opciones DHCP y extensiones de proveedores de BOOTP.

Un cliente DHCP puede negociar con el servidor, limitándolo a enviar solo esas opciones que solicita el cliente.

- Opciones de DHCP predefinidas
- Múltiples valores para una opción de DHCP
- Opciones de DHCP 43, 55 y 60 y otras opciones personalizadas

Opciones de DHCP predefinidas

Los cortafuegos de Palo Alto Networks admiten opciones de DHCP predefinidas y definidas por los usuarios en la implementación del servidor DHCP. Dichas opciones se configuran en el servidor DHCP y se envían a los clientes que envían una DHCPREQUEST al servidor. Se dice que los clientes *heredan* e implementan las opciones que están programados para aceptar.

El cortafuegos admite las siguientes opciones predefinidas en sus servidores DHCP, que se muestran en el orden en que aparecen en la pantalla de configuración del **servidor DHCP**:

Opción de DHCP	Nombre de opción de DHCP
51	Duración de la concesión
3	Gateway
1	Subred de grupo de IP (máscara)
6	Dirección de servidor del sistema de nombres de dominio (DNS:) (principal y secundaria)
44	Dirección de servidor del Servicio de nombres Internet de Windows (WINS) (primaria y secundaria)
41	Dirección de servidor del Servicio de información de la red (NIS) (primaria y secundaria)
42	Dirección de servidor del protocolo de tiempo de redes(NTP) (primaria y secundaria)
70	Dirección de servidor del Protocolo de oficina de correo Versión 3 (POP3)
69	Dirección de servidor del Protocolo simple de transferencia de correo (SMTP)

© 2020 Palo Alto Networks, Inc.

Opción de DHCP	Nombre de opción de DHCP
15	Sufijos DNS

Como se menciona, también puede configurar opciones específicas del proveedor y personalizadas, compatibles con una gran variedad de equipos de oficina, tales como teléfonos IP y dispositivos de infraestructura inalámbrica. Cada código de opción admite múltiples valores, que pueden ser direcciones IP o formato hexadecimal ASCII. Gracias a la compatibilidad con la opción de DCHP mejorada, las sucursales no necesitan comprar y gestionar sus propios servidores de DHCP para ofrecer opciones personalizadas y específicas de proveedores a los clientes de DHCP.

Múltiples valores para una opción de DHCP

Puede introducir varios valores de opciones para un **Option Code** con el mismo **Option Name**, pero todos los valores para un código particular y una combinación de nombre deben ser del mismo tipo (dirección IP, ASCII o hexadecimal). Si se hereda o introduce un tipo, y después se introduce un segundo tipo para la misma combinación de código y nombre, el segundo tipo sobrescribirá el primero.

Puede introducir un **Option Code** más de una vez usando un **Option Name** diferente. En este caso, el **Option Type** del Código de opción puede variar entre los múltiples nombres de opción. Por ejemplo, si la opción Coastal Server (código de opción 6) está configurada con el tipo de dirección IP, también se admite la opción Server XYZ (código de opción 6) con ASCII.

El cortafuegos envía múltiples valores para una opción (vinculados) a un cliente en orden descendente (de arriba abajo). Por lo tanto, al introducir múltiples valores para una opción, introduzca los valores en el orden de preferencia, o si no, mueva las opciones para establecer el orden que prefiera en la lista. El orden de las opciones en la configuración del cortafuegos determina el orden en que aparecen las opciones en los mensajes DHCPOFFER y DHCPACK.

Puede introducir un código de opción que ya existe como código de opción predefinida, y el código de opción personalizado sobrescribirá la opción de DHCP predefinida; el cortafuegos emitirá una advertencia.

Opciones de DHCP 43, 55 y 60 y otras opciones personalizadas

La siguiente tabla describe el comportamiento de las opciones para varias opciones descritas en RFC 2132.

Código de opción	Nombre de opción	Descripción/Comportamiento de la opción
43	Información específica del proveedor	Enviada desde el servidor al cliente. Información específica del proveedor que el servidor de DHCP ha configurado para ofrecerla al cliente. La información se envía al cliente solo si el servidor tiene un Identificador de clase de proveedor (VCI) en la tabla que coincide con el VCO en la DHCPREQUEST del cliente. Un paquete de opción 43 puede contener múltiples informaciones específicas del proveedor. También puede incluir extensiones de datos encapsuladas específicas del proveedor.
55	Lista de requisitos de parámetros	Enviado desde el cliente al servidor. Lista de parámetros de configuración (códigos de opción) que está solicitando un cliente DHCP, probablemente en el orden de preferencia del cliente. El servidor intenta responder con opciones en el mismo orden.

© 2020 Palo Alto Networks, Inc.

Código de opción	Nombre de opción	Descripción/Comportamiento de la opción
60	Identificador de clase de proveedor (VCI)	Enviado desde el cliente al servidor. Configuración y tipo de proveedor de un cliente DHCP. El cliente DHCP envía un código de opción 60 en una DHCPREQUEST al servidor de DHCP. Cuando el servidor recibe la opción 60, ve el VCI, busca el VCI correspondiente en su propia tabla y regresa con una opción 43 con el valor (que se corresponde con el VCI), por lo tanto, retransmitiendo información específica del proveedor al cliente correcto. Tanto el cliente como el servidor tienen conocimiento del VCI.

Puede enviar códigos específicos del proveedor personalizados que no están definidos en RFC 2132. Estos códigos de opción pueden estar dentro del intervalo 1-254 y tener una longitud fija o variable.

El servidor DHCP no valida las opciones de DHCP personalizadas; debe asegurarse de introducir los valores correctos para las opciones que cree.

Para tipos de opciones ASCII DHCP hexadecimal, el valor de opción puede ser de 255 octetos como máximo.

Configure una interfaz como servidor DHCP

Los requisitos previos de esta tarea son:

- Configure una interfaz Ethernet de capa 3 o VLAN de capa 3.
- Asigne la interfaz a un enrutador virtual y a una zona.
- Determine un grupo válido de direcciones IP de su plan de red que pueda designar para que su servidor DHCP las asigne a los clientes.
- Recopile los valores, identificadores de clase de proveedor y opciones de DHCP que tiene previsto configurar.

Estas son las funciones:

- Para ver modelos de cortafuegos distintos de PA-5200 Series y PA-7000 Series, consulte la Herramienta de selección de productos.
- En los cortafuegos PA-5220, puede configurar un máximo de 500 servidores DHCP y un máximo de 2048 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 1548 agentes de transmisión DHCP.
- En los cortafuegos PA-5250, PA-5260 y PA-7000 Series, puede configurar un máximo de 500 servidores DHCP y un máximo de 4096 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 3596 agentes de transmisión DHCP.

Realice la siguiente tarea para configurar una interfaz en el cortafuegos para que actúe como servidor DHCP.

STEP 1 | Seleccione una interfaz para que sea un servidor DHCP.

1. Seleccione **Network (Red)** > **DHCP** > **DHCP Server (Servidor DHCP)** y, luego, haga clic en **Add (Añadir)** para añadir o seleccionar el nombre de la interfaz en **Interface (Interfaz)**.

© 2020 Palo Alto Networks, Inc.

2. En **Mode (Modo)**, seleccione **enabled (habilitado)** o modo **auto (automático)**. El modo automático habilita el servidor y lo deshabilita si se detecta otro servidor DHCP en la red. El ajuste **disabled (deshabilitar)** desactiva el servidor.
3. (Opcional) Seleccione **Ping IP when allocating new IP (Hacer ping a la IP al asignar IP nuevas)** si desea que el servidor haga ping a la dirección IP antes de asignarla a su cliente.



Si el ping recibe una respuesta, significará que ya hay un dispositivo diferente con esa dirección, por lo que no está disponible para su asignación. El servidor asigna la siguiente dirección desde el grupo. Este comportamiento es similar a Duplicar detección de dirección (DAD) para IPv6, RFC 4429*.*



Tras definir las opciones y volver a la pestaña del servidor DHCP, la columna Probe IP de la interfaz indicará si Ping IP when allocating new IP estaba seleccionada.

STEP 2 | Configure las Opciones DHCP predefinidas que el servidor envía a sus clientes.

- En la sección Opciones, seleccione un tipo de **Concesión**.
- **Unlimited (Ilimitada)** provoca que el servidor seleccione dinámicamente direcciones IP desde los Grupos IP y los asigne de forma permanente a los clientes.
- **Timeout (Tiempo de espera)** determina cuánto durará esa concesión. Introduzca el número de **Días** y **Horas** y, opcionalmente, el número de **Minutos**.
- **Origen de herencia**: Deje **Ninguno** o seleccione una interfaz de cliente DHCP de origen o una interfaz de cliente PPPoE para propagar distintos ajustes de servidor en el servidor de DHCP. Si especifica un **Inheritance Source (Origen de herencia)**, seleccione una o varias opciones que desee como **inherited (heredadas)** desde este origen.

Especificar un origen de herencia permite al cortafuegos añadir rápidamente opciones de DHCP desde el servidor previo recibidas por el cliente DHCP. También mantiene actualizadas las opciones de cliente si el origen cambia una opción. Por ejemplo, si el origen sustituye a su servidor NTP (que se ha identificado como el servidor **NTP principal**), el cliente heredará automáticamente la nueva dirección como su nuevo servidor **NTP principal**.



Al heredar opciones de DHCP que contienen múltiples direcciones IP, el cortafuegos usa solo la primera dirección IP contenida en la opción para ocupar menos memoria caché. Si necesita múltiples direcciones IP para una única opción, configure las opciones DHCP directamente en el cortafuegos en lugar de configurar la herencia.

- **Check inheritance source status (Verificar estado del origen de herencia)**: si ha seleccionado **Inheritance Source (Origen de herencia)**, al hacer clic en este enlace se abrirá la ventana **Dynamic IP Interface Status (Estado de interfaz de IP dinámica)**, que muestra las opciones que se han heredado del cliente DHCP.
- **Gateway (Puerta de enlace)**: la dirección IP de la puerta de enlace de la red (una interfaz en el cortafuegos) que se usa para llegar a cualquier dispositivo que no esté en la misma LAN que este servidor DHCP.
- **Subnet Mask**: máscara de red con las direcciones del campo **IP Pools**.

En los siguientes campos, haga clic en la flecha hacia abajo y seleccione **None (Ninguno)** o **inherited (heredado)**, o introduzca una dirección IP de servidor remoto que su servidor DHCP enviará a los clientes para acceder a ese servicio. Si ha seleccionado **inherited (heredado)**, el servidor DHCP hereda los valores desde el cliente DHCP de origen, especificado como **Inheritance Source (Origen de herencia)**.

- **Primary DNS (DNS primario)**, **Secondary DNS (DNS secundario)**: dirección IP de los servidores del sistema de nombres de dominio (DNS) preferidos y alternativos.
- **Primary WINS (WINS primario)**, **Secondary WINS (WINS secundario)**: dirección IP de los servidores Windows Internet Naming Service (WINS) preferidos y alternativos.

© 2020 Palo Alto Networks, Inc.

- **Primary NIS (NIS primario)**, **Secondary NIS (NIS secundario)**: introduzca la dirección IP de los servidores del Servicio de información de la red (NIS) preferidos y alternativos.
- **Primary NTP (NTP primario)**, **Secondary NTP (NTP secundario)**: dirección IP de los servidores del protocolo de tiempo de redes disponibles.
- **POP3 Server (Servidor POP3)**: dirección IP del servidor Post Office Protocol (POP3).
- **SMTP Server**: introduzca la dirección IP del servidor del protocolo simple de transferencia de correo (Simple Mail Transfer Protocol, SMTP).
- **DNS Suffix (Sufijo DNS)**: sufijo para que el cliente lo use localmente cuando se introduce un nombre de host sin cualificar que no puede resolverse.

STEP 3 | (Opcional) Configure una opción DHCP personalizada o específica del proveedor que el servidor DHCP enviará a los clientes.

1. En la sección opciones de DHCP personalizadas, haga clic en **Add (Añadir)** e introduzca un nombre descriptivo en **Name (Nombre)** para identificar la opción DHCP.
2. Introduzca el **Option Code (Código de opción)** que desea configurar para ofrezca el servidor (el intervalo es 1-254). (Consulte RFC 2132 para conocer códigos de opción).
3. Si el **Option Code** es **43**, aparecerá el campo **Vendor Class Identifier**. Introduzca un VCI, que es una cadena o valor hexadecimal (con prefijo 0x) usado como coincidencia frente a un valor procedente de la solicitud del cliente que contiene una opción 60. El servidor busca el VCI entrante en esta tabla, lo encuentra, y devuelve la opción 43 y el valor de opción correspondiente.
4. **Inherit from DHCP server inheritance source (Heredar del origen de herencia del servidor DHCP)**: seleccione esta opción si ha especificado un **Inheritance Source (Origen de herencia)** para las opciones predeterminadas del servidor DHCP y desea **heredar** también de este origen.
5. **Check inheritance source status (Verificar estado del origen de herencia)**: si ha seleccionado **Inheritance Source (Origen de herencia)**, al hacer clic en este enlace se abrirá la ventana **Dynamic IP Interface Status (Estado de interfaz de IP dinámica)**, que muestra las opciones que se han heredado del cliente DHCP.
6. Si no ha seleccionado la casilla de verificación **Inherit from DHCP server inheritance source**, seleccione un **Option Type**: **IP Address**, **ASCII** o **Hexadecimal**. Los valores hexadecimales deben empezar por el prefijo 0x.
7. Introduzca el **Option Value (Valor de opción)** que el servidor DHCP debe ofrecer para ese **Option Code (Código de opción)**. Puede introducir múltiples valores en líneas separadas.
8. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Añada otra opción DHCP personalizada o específica del proveedor.

1. Repita el paso anterior para introducir otra opción DHCP personalizada.
   - Puede introducir múltiples valores de opciones para un **Option Code** con el mismo **Option Name**, pero todos los valores para un **Option Code** deben ser del mismo tipo (**IP Address**, **ASCII** o **Hexadecimal**). Si se hereda o introduce un tipo y se introduce un segundo tipo para el mismo **Option Code** y **Option Name**, el segundo tipo sobrescribirá al primero.

     Al introducir múltiples valores para una opción, introduzca los valores en el orden de preferencia, o si no, mueva las opciones de DHCP personalizadas para establecer el orden que prefiera en la lista. Seleccione una opción y haga clic en **Move Up (Mover arriba)** o **Move Down (Mover abajo)**.
   - Puede introducir un **Option Code** más de una vez usando un **Option Name** diferente. En este caso, el **Option Type** del Código de opción puede variar entre los múltiples nombres de opción.
2. Haga clic en **OK (Aceptar)**.

STEP 5 | Identifique el grupo de direcciones IP de estado desde el que el servidor DHCP selecciona una dirección y la asigna a un cliente DHCP.

© 2020 Palo Alto Networks, Inc.

Si no es el administrador de su red, pídale a él un grupo válido de direcciones IP de su plan de red que puede designarse para que su servidor DHCP lo asigne.

1. En el campo **IP pools (Grupos IP)**, haga clic en **Add (Añadir)** e introduzca el intervalo de direcciones IP desde el cual este servidor asigna una dirección a un cliente. Introduzca una subred IP y una máscara de subred (por ejemplo, 192.168.1.0/24) o un intervalo de direcciones IP (por ejemplo, 192.168.1.10-192.168.1.20).
   - El grupo de IP o la **dirección reservada** son obligatorios para la asignación de dirección IP dinámica.
   - El grupo IP es opcional para la asignación de dirección IP, siempre y cuando las direcciones IP estáticas que asigne vayan a la subred que asiste la interfaz del cortafuegos.
2. (Opcional) Repita este paso para especificar otro grupo de direcciones IP.

STEP 6 | (Opcional) Especifique una dirección IP de los grupos IP que no se asignarán dinámicamente. Si especifica también una **Dirección MAC**, la **Dirección reservada** se asigna a ese dispositivo cuando el dispositivo solicita una dirección IP a través de DHCP.

Consulte la sección DHCP Addressing (Direccionamiento DHCP) si desea una explicación de la asignación de una Reserved Address (Dirección reservada).

1. En el campo **Reserved Address (Dirección reservada)**, haga clic en **Add (Añadir)**.
2. Introduzca una dirección IP desde **Grupos IP** (formato *x.x.x.x*) que no desea que se asigne dinámicamente al servidor DHCP.
3. (Opcional) Especifique la **MAC Adress (Dirección MAC)** (formato *xx:xx:xx:xx:xx:xx*) del dispositivo al que desea asignar de forma permanente la dirección IP que acaba de especificar.
4. (Opcional) Repita los dos pasos anteriores para reservar otra dirección.

STEP 7 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configure una interfaz como cliente DHCP

Antes de configurar una interfaz de cortafuegos como cliente DHCP, tiene que haber configurado una interfaz de capa 3 (Ethernet, subinterfaz de Ethernet, VLAN, subinterfaz de VLAN, agregación o subinterfaz de agregación) y haberla asignado a una zona y a un enrutador virtual. Configure una interfaz como cliente DHCP si necesita usar DHCP para solicitar una dirección IPv4 para la interfaz.

También puede realizar la Configuración de la interfaz de gestión como cliente DHCP.

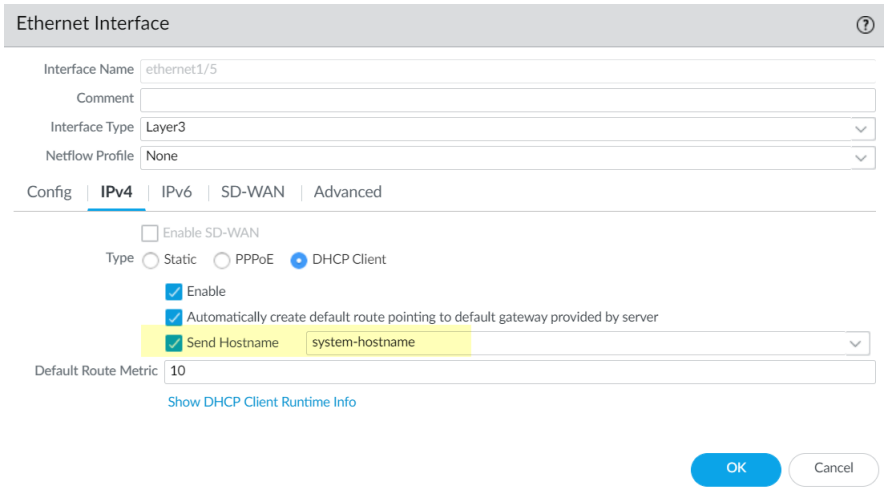
STEP 1 | Configure una interfaz como cliente DHCP.

1. Seleccone **Network (Red)** > **Interfaces**.
2. En las pestañas **Ethernet** o **VLAN**, **añada** una interfaz de capa 3 o seleccione una ya configurada que quiera que sea cliente DHCP.
3. Seleccione la pestaña **IPv4** y ,en **Type (Tipo)**, seleccione **DHCP Client (Cliente DHCP)**.
4. Seleccione **Enabled (Habilitado)**.
5. (Opcional) Habilite la opción para **crear una ruta predeterminada automáticamente que apunte a la puerta de enlace predeterminada proporcionada por el servidor** habilitada de forma predeterminada. Si activa esta opción, el cortafuegos creará una ruta estática a una puerta de enlace predeterminada

© 2020 Palo Alto Networks, Inc.

que será útil cuando los clientes intenten acceder a muchos destinos que no necesitan mantener rutas en una tabla de enrutamiento en el cortafuegos.

6. (Opcional) Habilite la opción**Send Hostname (Enviar nombre de host)** para asignar un nombre de host a la interfaz del cliente DHCP y enviar dicho nombre (opción 12) a un servidor DHCP. Este lo registra en el servidor DNS, que puede gestionar automáticamente la resolución de nombres de host en direcciones IP dinámicas. Los hosts externos pueden identificar la interfaz por su nombre de host. El valor predeterminado es **system-hostname (nombre-host-sistema)**, que se corresponde con el nombre de host del cortafuegos definido en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**. Si lo prefiere, introduzca un nombre de host para la interfaz con 64 caracteres como máximo, que pueden incluir letras mayúsculas y minúsculas, números, puntos (.), guiones (-) y guiones bajos (_).



7. (Opcional) Introduzca una **Default Route Metric** (nivel de prioridad) para la ruta entre el cortafuegos y el servidor DHCP (el intervalo es de 1 a 65 535; el valor predeterminado es 10). Un ruta con un número más bajo tiene una prioridad alta durante la selección de la ruta. Por ejemplo, una ruta con una métrica de 10 se usa antes que una ruta con una métrica de 100.

   La métrica de ruta predeterminada para la ruta entre el cortafuegos y el servidor DHCP es 10 de forma predeterminada. Si la ruta estática predeterminada 0.0.0.0/0 utiliza la interfaz DHCP como su interfaz de salida, la métrica predeterminada de esa ruta es también 10. Por lo tanto, hay dos rutas con una métrica de 10 y el cortafuegos puede elegir aleatoriamente una de las rutas una vez y la otra ruta en otro momento.

   Suponga que habilita la opción para crear automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor, selecciona un enrutador virtual, añade una ruta estática para la interfaz de capa 3, cambia la métrica (cuyo valor predeterminado es 10) a un valor superior a 10 (en este ejemplo, 100) y confirma los cambios. En la tabla de rutas, la métrica de la ruta no indicará 100. En su lugar, indicará el valor predeterminado de 10, como se esperaba, porque 10 tiene prioridad sobre el valor configurado de 100. Sin embargo, si cambia la métrica de la ruta estática a un valor inferior a 10 (como 6), se actualizará la ruta de la tabla de rutas para indicar la métrica configurada de 6.

8. (Opcional) Habilite la opción **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)** para ver todos los ajustes que el cliente ha heredado del servidor DHCP.

STEP 2 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

La interfaz Ethernet debe ahora indicar **Dynamic-DHCP Client (Cliente DHCP dinámico)** como **dirección IP** en la pestaña **Ethernet**.

STEP 3 | (Opcional) Vea qué interfaces del cortafuegos se han configurado como clientes DHCP.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y compruebe **IP Address (Dirección IP)** para verificar las interfaces que se indican como cliente DHCP.
2. Seleccione **Network (Red)** > **Interfaces** > **VLAN** y observe el campo **IP Address (Dirección IP)** para verificar las interfaces que se indican como cliente DHCP.

Configuración de la interfaz de gestión como cliente DHCP

La interfaz de gestión en el cortafuegos admite el cliente DHCP para IPv4 que permite que la interfaz de gestión reciba su dirección IPv4 de un servidor DHCP. La interfaz de gestión también admite la opción 12 y la opción 61 de DHCP, que permite que el cortafuegos envíe su nombre de host e identificador de cliente, respectivamente, a los servidores DHCP.

Por defecto, los cortafuegos de la serie VM implementados en AWS y Azure™ usan la interfaz de gestión como cliente DHCP para obtener su dirección IP, en lugar de una dirección IP estática, debido a que las implementaciones en la nube requieren la automatización que ofrece esta característica. DHCP en la interfaz de gestión está desactivada por defecto para el cortafuegos de la serie VM, excepto para el cortafuegos de la serie VM en AWS y Azure. Las interfaces de gestión en los modelos de WildFire y Panorama no admiten esta funcionalidad DHCP.

- *Para los modelos de cortafuegos basados en hardware (no la serie de VM), configure la interfaz de gestión con una dirección IP estática cuando fuera posible.*
- *Si el cortafuegos adquiere una dirección de interfaz de gestión a través de DHCP, asigne una reserva de dirección MAC en el servidor DHCP que se encarga de ese cortafuegos. La reserva garantiza que el cortafuegos conserve su dirección IP de gestión después de un reinicio. Si el servidor DHCP es un cortafuegos de Palo Alto Networks, consulte el paso 6 de* Configuración de una interfaz como servidor DHC *para reservar una dirección.*

Si configura la interfaz de gestión como un cliente DHCP, se aplican las siguientes restricciones:

- No puede usar la interfaz de gestión en una configuración HA para el enlace de control (copia de seguridad de HA1 o HA1), enlace de datos (copia de seguridad de HA2 o HA2 o la comunicación de reenvío de paquete (HA3).
- No puede seleccionar **MGT** como la interfaz de origen al personalizar las rutas de servicio (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Service Route Configuration [Configuración de ruta de servicio]** > **Customize [Personalizar]**). Sin embargo, puede seleccionar **Use default (Usar predeterminado)** para enrutar los paquetes a través de la interfaz de gestión.
- No puede usar la dirección IP dinámica de la interfaz de gestión para conectarse con un módulo de seguridad de hardware (Hardware Security Module, HSM). La dirección IP en el cortafuegos del cliente HSM debe ser una dirección IP estática debido a que HSM autentica el cortafuegos usando la dirección IP y las operaciones en HSM dejarían de funcionar si la dirección IP cambiara durante el tiempo de ejecución.

Un requisito previo para esta tarea es que la interfaz de gestión debe ser capaz de conectarse a un servidor DHCP.

STEP 1 | Configure la interfaz de gestión como cliente DHCP ara que pueda recibir su dirección IP (IPv4), máscara de red (IPv4) y puerta de enlace por defecto de un servidor DHCP.

© 2020 Palo Alto Networks, Inc.

O bien, también puede enviar el nombre de host e identificador de cliente de la interfaz de gestión al servidor DHCP si el sistema de orquestación que utiliza acepta esta información.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de interfaz de gestión.
2. Para **IP Type (Tipo de IP)**, seleccione **DHCP Client (Cliente DHCP)**.
3. (Opcional) Seleccione una de las opciones, o ambas, para que el cortafuegos envíe al servidor DHCP en los mensajes de detección o solicitud de DHCP:
   - **Send Hostname (Enviar nombre de host)**: envía el **Hostname (Nombre de host)** (como se definió en **Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]**) como parte de la opción 12 de DHCP.
   - **Send Client ID**: envía su identificador de cliente como parte de la opción 61 de DHCP. Un identificador de cliente identifica de manera única un cliente DHCP, y el servidor DHCP lo utiliza para indexar su base de datos de parámetro de configuración.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Configure el cortafuegos para que acepte el nombre de host y dominio del servidor DHCP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes generales.
2. Seleccione una opción o ambas:
   - **Accept DHCP server provided Hostname**: permite que el cortafuegos acepte el nombre de host del servidor DHCP (si es válido). Cuando está habilitada, el nombre de host del servidor DHCP sobrescribe cualquier **Hostname (Nombre de host)** existente especificado en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**. No seleccione esta opción si desea configurar manualmente un nombre de host.
   - **Accept DHCP server provided Domain**: permite que el cortafuegos acepte el dominio del servidor DHCP. El dominio (sufijo DNS) del servidor DHCP sobrescribe cualquier **dominio** existente especificado en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión).** No seleccione esta opción si desea configurar manualmente un dominio.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

STEP 4 | Visualice información del cliente DHCP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y Management Interface Settings (Ajustes de la interfaz de gestión).
2. Haga clic en **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)**.

STEP 5 | (Opcional) Renueve la DHCP lease (Concesión DHCP) con el servidor DHCP, independientemente del plazo de concesión.

Esta opción es práctica si está comprobando o resolviendo problemas de red.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de interfaz de gestión.
2. Haga clic en **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)**.
3. Haga clic en **Renew**.

© 2020 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Libere las siguientes opciones de DHCP provenientes del servidor DHCP:

- Dirección IP
- Máscara de red
- Gateway predeterminada
- Servidor DNS (primario y secundario)
- Servidor NTP (primario y secundario)
- Dominio (sufijo DNS)

Una liberación desbloquea la dirección IP, que desactiva la conexión de su red y hace que el cortafuegos no pueda gestionarse si no hay otra interfaz configurada para el acceso de gestión.

Use el comando operativo de CLI **`request dhcp client management-interface release`**.

Configure una interfaz como agente de relé DHCP

Para habilitar una interfaz de cortafuegos para que transmita mensajes DHCP entre clientes y servidores, debe configurar el cortafuegos como agente de transmisión DHCP. La interfaz puede reenviar mensajes a un máximo de ocho servidores DHCP IPv4 externos y ocho servidores DHCP IPv6 externos. Un mensaje de DHCPDISCOVER del cliente se envía a todos los servidores configurados, y el mensaje DHCPOFFER del primer servidor que responde se retransmite al cliente que originó la petición.

Estas son las funciones:

- Puede configurar un número total combinado de 500 servidores DHCP (IPv4) y agentes de retransmisión DHCP (IPv4 y IPv6) en todos los modelos de cortafuegos, excepto los cortafuegos PA-5200 Series y PA-7000 Series.
- En los cortafuegos PA-5220, puede configurar un máximo de 500 servidores DHCP y un máximo de 2048 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 1548 agentes de transmisión DHCP.
- En los cortafuegos PA-5250, PA-5260 y PA-7000 Series, puede configurar un máximo de 500 servidores DHCP y un máximo de 4096 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 3596 agentes de transmisión DHCP.

Antes de configurar un agente de retransmisión DHCP, asegúrese de que ha configurado una interfaz Ethernet de capa 3 o VLAN de capa 3, y de que la interfaz se ha asignado a una zona y un enrutador virtual.

STEP 1 | Seleccione Retransmisión DHCP.

Seleccione **Network (Red)** > **DHCP** > **DHCP Relay (Transmisión DHCP)**.

STEP 2 | Especifique la dirección IP del servidor DHCP con el que se comunicará el agente del relé DHCP.

1. En el campo **Interface (Interfaz)**, seleccione la interfaz que debe funcionar como agente de retransmisión DHCP.
2. Seleccione **IPv4** o **IPv6**, lo que indica el tipo de dirección del servidor DHCP que va a especificar.
3. Si seleccionó **IPv4**, en el campo **DHCP Server IP Address (Dirección IP del servidor DHCP)**, haga clic en **Add (Añadir)** e introduzca la dirección del servidor DHCP de origen y destino para la transmisión de mensajes DHCP.
4. Si seleccionó **IPv6**, en el campo **DHCP Server IPv6 Address (Dirección IPv6 del servidor DHCP)**, haga clic en **Add (Añadir)** e introduzca la dirección del servidor DHCP de origen y destino para la

© 2020 Palo Alto Networks, Inc.

transmisión de mensajes DHCP. Si especifica una dirección *multidifusión*, especifique también una **Interfaz** saliente.

5. (Opcional) Repita los tres pasos anteriores para introducir un máximo de ocho direcciones de servidor DHCP por cada familia de dirección IP.

STEP 3 | Confirme la configuración.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Supervisión y resolución de problemas de DHCP

Puede visualizar el estado de las concesiones de dirección dinámica asignadas por su servidor DHCP o a su cliente DHCP enviando comandos desde la CLI. También puede eliminar concesiones antes de que caduquen y se liberen automáticamente.

- Ver información de servidor DHCP principal
- Borrado de concesiones DHCP
- Ver información de cliente DHCP
- Recopilación de resultados de depuración sobre DHCP

Ver información de servidor DHCP principal

Realice esta tarea para ver las estadísticas del grupo DHCP, las direcciones IP que ha asignado el servidor DHCP, la dirección MAC correspondiente, el estado y la duración de la concesión, y la hora de inicio de la concesión. Si la dirección se ha configurado como **Reserved Address (Dirección reservada)**, la columna `state (estado)` indica `reserved (reservado)` y no se indican `duration (duración)` ni `lease_time (tiempo de concesión)`. Si la concesión se configuró como **Unlimited (Ilimitada)**, la columna `duration (duración)` se mostrará con un valor de `0`.

- Vea las estadísticas de grupo DHCP, la dirección IP que ha asignado el servidor DHCP, la dirección MAC, el estado y la duración de la concesión, y la hora de inicio de la concesión.

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip              mac                state      duration    lease_time
192.168.3.11    f0:2f:af:42:70:cf  committed  0           Wed Jul  2
 08:10:56 2014
admin@PA-220>
```

- Vea las opciones que un servidor DHCP ha asignado a los clientes.

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit source
------------------------------------------------------------------------------
ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10             ethernet1/3
admin@PA-220>
```


© 2020 Palo Alto Networks, Inc.

Borrado de concesiones DHCP

Cuenta con varias opciones para borrar las concesiones DHCP.

- Libere las concesiones DHCP vencidas de una interfaz (servidor), como ethernet1/2, antes de que el temporizador de espera las libere automáticamente. Estas direcciones volverán a estar disponibles en el grupo IP.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

- Libere una concesión de una dirección IP particular, por ejemplo, 192.168.3.1.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

- Libere una concesión de una dirección MAC particular, por ejemplo, f0:2c:ae:29:71:34.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac f0:2c:ae:29:71:34
```

Ver información de cliente DHCP

Para visualizar el estado de las concesiones de dirección IP enviadas al cortafuegos cuando actúa como cliente DHCP, utilice cualquiera de estos comandos de la CLI.

- **admin@PA-220>show dhcp client state *<interface_name>***

- **admin@PA-220> show dhcp client state all**

```
Interface       State        IP              Gateway          Leased-until
-------------------------------------------------------------------------
ethernet1/1     Bound        10.43.14.80     10.43.14.1       70315
admin@PA-220>
```

Recopilación de resultados de depuración sobre DHCP

Para reunir los resultados de la depuración sobre DHCP, utilice uno de los siguientes comandos:

- **admin@PA-220> debug dhcpd**

- **admin@PA-220> debug management-server dhcpd**

© 2020 Palo Alto Networks, Inc.

DNS:

El sistema de nombres de dominio (Domain Name System, DNS) es un protocolo que traduce (resuelve) un nombre de dominio sencillo, como www.paloaltonetworks.com, en una dirección IP, de modo que los usuarios puedan acceder a ordenadores, sitios web, servicios u otros recursos en internet o en redes privadas.

- Descripción general del DNS
- Objeto proxy DNS
- Perfil de servidor DNS
- Implementaciones de DNS multiusuario
- Configuración de un objeto proxy DNS
- Configuración de un perfil de servidor DNS
- Caso de uso 1: el cortafuegos exige la resolución de DNS
- Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual.
- Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor
- Regla de proxy DNS y coincidencia FQDN

Descripción general del DNS

DNS realiza una función crucial en la habilitación del acceso de usuarios a los recursos de red, de modo que los usuarios no deban recordar las direcciones IP y los ordenadores individuales no deban almacenar un gran volumen de nombres de dominios asignados a las direcciones IP. DNS emplea un modelo de cliente/servidor; un servidor DNS resuelve una consulta de un cliente DNS buscando el dominio en su caché y, de ser necesario, enviando consultas a otros servidores hasta que puede responder al cliente con la dirección IP correspondiente.

La estructura de DNS de los nombres de dominio es jerárquica; el dominio de nivel superior (TLD) en un nombre de dominio puede ser un TLD genérico (gTLD): com, edu, gov, int, mil, net u org (gov y mil corresponden solo a Estados Unidos) o un código de país (ccTLD), como au (Australia) o us (Estados Unidos). Por lo general, los ccTLD se reservan para países y territorios independientes.

Un nombre de dominio completo (FQDN) incluye, como mínimo, un nombre de host, un dominio de segundo nivel y un TLD para especificar completamente la ubicación del host en la estructura del DNS. Por ejemplo, www.paloaltonetworks.com es un FQDN.

Siempre que un cortafuegos de Palo Alto Networks utiliza un FQDN en la interfaz de usuario o CLI, el cortafuegos debe resolver el FQDN que utiliza DNS. En función de dónde se origina la consulta del FQDN, el cortafuegos determina la configuración que se utilizará para resolver la consulta.

Los registros de DNS de los FQDN incluyen un valor de tiempo de vida (time-to-live, TTL). El cortafuegos actualiza de manera predeterminada cada uno de los FQDN que tiene almacenados en su caché en función del TTL que proporciona el servidor DNS, siempre que dicho valor sea igual o superior al tiempo mínimo de actualización de los FQDN que configure en el cortafuegos o, si no lo especifica, al ajuste predeterminado de 30 segundos. La actualización de los FQDN basada en el valor del TTL resulta de especial utilidad para proteger el acceso a los servicios de las plataformas en la nube, que suelen exigir una actualización frecuente para garantizar la alta disponibilidad. Por ejemplo, los entornos de nube con escalabilidad automática dependen de la resolución de los FQDN para ampliar o reducir los servicios de forma dinámica; en esos entornos donde el tiempo es un factor tan importante, es fundamental la rapidez en la resolución de los FQDN.

Si configura el tiempo mínimo de actualización de los FQDN, limita el valor mínimo de TTL que respeta el cortafuegos. Si sus direcciones IP no varían a menudo, defina un tiempo de actualización mayor para que el

© 2020 Palo Alto Networks, Inc.

cortafuegos no actualice las entradas innecesariamente. El cortafuegos usa el valor que sea más alto: el TTL de DNS o el tiempo mínimo de actualización de los FQDN configurado.

Por ejemplo, dos FQDN tienen los siguientes valores de TTL. El tiempo mínimo de actualización de los FQDN los sustituye, ya que estos son más bajos, es decir, más breves.

	TTL	Tiempo mínimo de actualización de FQDN = 26	Tiempo real de actualización
FQDN A	20		26
FQDN B	30		30

El temporizador de actualización de un FQDN se pone en marcha cuando el cortafuegos recibe una respuesta de DNS del servidor DNS o del objeto de proxy DNS que resuelve el FQDN.

Además, puede configurar un tiempo de espera de obsolescencia, que determina cuánto tiempo debe seguir usando el cortafuegos las resoluciones de FQDN obsoletas (vencidas) si no se puede acceder al servidor DNS. Si termina el tiempo de espera de obsolescencia y aún no se puede acceder al servidor DNS, las entradas de FQDN obsoletas se quedan sin resolver, y el cortafuegos las elimina.

Las siguientes tareas del cortafuegos están relacionadas con el DNS:

- Configure su cortafuegos con, al menos, un servidor DNS para que resuelva los nombres de host. Configure los servidores DNS principal y secundario o un objeto de proxy DNS que especifique esos servidores como se explica en Caso de uso 1: el cortafuegos exige la resolución de DNS.
- Personalice cómo el cortafuegos gestiona la resolución de DNS iniciada por las reglas de la política de seguridad, la creación de informes y los servicios de gestión (como correo electrónico, Kerberos, SNMP, Syslog, etc.) de cada sistema virtual, como se muestra en Caso de uso 2: el usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, creación de informes y servicios dentro de su sistema virtual.
- Configure el cortafuegos para que actúe como un servidor DNS para un cliente, como se muestra en Caso de uso 3: el cortafuegos actúa como proxy DNS entre cliente y servidor.
- Configure un perfil antispyware para garantizar el Uso de consultas de DNS para identificar hosts infectados en la red.
- Realice la Habilitación de firmas de evasión y habilite las firmas de evasión para la prevención de amenazas.
- Realice la Configuración de una interfaz como servidor DHCP. Esto permite que el cortafuegos actúe como un servidor DHCP y envíe información de DNS a sus clientes DHCP, de modo que los clientes DHCP asignados puedan alcanzar los servidores DNS correspondientes.

Objeto proxy DNS

Cuando se configura como proxy DNS, el cortafuegos actúa como intermediario entre los clientes y servidores de DNS; actúa como un servidor DNS en sí mismo resolviendo consultas desde su caché de proxy DNS. Si no encuentra el nombre de dominio en la caché de proxy DNS, el cortafuegos busca una coincidencia del nombre de dominio entre las entradas en el objeto proxy DNS específico (en la interfaz en la que se recibe la consulta DNS). El cortafuegos reenvía la consulta a un servidor DNS en función de los resultados. Si no se encuentra una coincidencia, el cortafuegos utiliza los servidores DNS predeterminados.

Un objeto de proxy DNS es donde se configuran los ajustes que determinan el funcionamiento del cortafuegos como proxy DNS. Puede asignar un objeto de proxy DNS a un único sistema virtual o compartirlo entre todos los sistemas virtuales.

© 2020 Palo Alto Networks, Inc.

- Si el objeto de proxy DNS es para un sistema virtual, puede especificar un Perfil de servidor DNS, que especifica las direcciones de servidores de DNS principales y secundarias, junto con otra información. El perfil de servidor DNS simplifica la configuración.
- Si el objeto proxy de DNS es compartido, debe especificar al menos la dirección principal de un servidor DNS.



Al configurar múltiples usuarios (abonados del ISP) con servicios DNS, se debe definir el proxy DNS de cada usuario, lo que mantiene el servicio DNS separado de los servicios de otros usuarios.

En el objeto de proxy, se especifican las interfaces en las que el cortafuegos actúa como proxy DNS. El proxy DNS para la interfaz no usa la ruta de servicio; las respuestas a las solicitudes DNS se envían siempre a la interfaz asignada al enrutador virtual donde se recibió la solicitud de DNS.

Cuando realiza la Configuración de un objeto proxy DNS, puede introducir en el proxy DNS asignaciones estáticas de FQDN a dirección. Además, puede crear reglas de proxy DNS que controlen a qué servidor DNS se dirigen las consultas de nombres de dominio especificado (que coinciden con las reglas de proxy). Puede configurar un máximo de 256 objetos de proxy DNS en un cortafuegos. Debe habilitar la **caché** y **las respuestas de EDNS de la caché** (en **Network (Red)** > **DNS Proxy (Proxy DNS)** > **Advanced (Avanzado)**) si el objeto proxy DNS se asigna a **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **DNS** o **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** > **vsys** > **General** > **DNS Proxy (Proxy DNS)**. Además, si este objeto proxy DNS tiene configuradas **reglas de proxy DNS**, esas reglas también deben tener la caché habilitada (**Turn on caching of domains resolved by this mapping (Activar el almacenamiento en caché de dominios resueltos por esta asignación)**).

Cuando un cortafuegos recibe una consulta de FQDN (y el nombre del dominio no se encuentra en el caché de proxy DNS), el cortafuegos compara el nombre de dominio de la consulta de FQDN con los nombres de dominio en las reglas de proxy DNS del objeto de proxy DNS. Si especifica múltiples nombres de dominio en una regla de proxy DNS, una consulta que coincida con alguno de los nombres de dominio en la regla indicará que la consulta coincide con la regla. Regla de proxy DNS y coincidencia FQDN describe cómo el cortafuegos determina si un FQDN coincide con un nombre de dominio en una regla de proxy DNS. Una consulta de DNS que coincide con una regla se envía al servidor DNS principal configurado para el objeto de proxy que debe resolverse.

Perfil de servidor DNS

Para simplificar la configuración de un sistema virtual, un perfil de servidor DNS le permite especificar el sistema virtual que se está configurando, un origen de herencia o las direcciones IP principales y secundarias para los servidores de DNS, así como una interfaz y la dirección de origen (ruta de servicio) que se usará en los paquetes enviados al servidor DNS. La interfaz de origen determina el enrutador virtual, que tiene una tabla de enrutamiento. Se busca la dirección IP de destino en la tabla de rutas del enrutador virtual donde está asignada la interfaz de origen. Es posible que el resultado de la interfaz de salida de IP de destino difiera de la interfaz de origen. El paquete saldría de la interfaz de salida de IP de destino determinada por la búsqueda de la tabla de enrutamiento, pero la dirección IP de origen sería la dirección configurada. La dirección de origen se usa como la dirección de destino en la respuesta del servidor DNS.

El informe del sistema virtual y el perfil del servidor del sistema virtual envían sus consultas al servidor DNS especificado en el sistema virtual, de haberlo. (El servidor DNS utilizado se define en **Device [Dispositivo]** > **Virtual Systems [Sistemas virtuales]** > **General** > **DNS Proxy [Proxy DNS]**.) Si no hay ningún servidor DNS especificado para el sistema virtual, se consulta al servidor DNS especificado para el cortafuegos.

La Configuración de un perfil de servidor DNS se realiza solo para un sistema virtual; no sirve para la ubicación compartida global.

© 2020 Palo Alto Networks, Inc.

Implementaciones de DNS multiusuario

El cortafuegos determina cómo gestionar solicitudes DNS basadas en el origen de la solicitud. Un entorno donde un ISP tiene varios usuarios en un cortafuegos se conoce como multiusuario. Hay tres casos de uso para implementaciones de DNS multiusuario:

- **Resolución DNS de gestión global**: el cortafuegos necesita resolución DNS para sus propios fines; por ejemplo, la solicitud procede del plano de gestión para resolver un FQDN de un evento de gestión como en un servicio de actualización de software. El cortafuegos utiliza la ruta de servicio para llegar a un servidor DNS debido a que la solicitud DNS no proviene de un enrutador virtual específico.
- **Resolución FQDN de políticas e informes para un sistema virtual**: en el caso de las consultas DNS de una política de seguridad, un informe o un servicio, puede especificar un conjunto de servidores DNS específicos para el sistema virtual (usuario) o utilizar la opción predeterminada para los servidores DNS globales. Si su caso de uso requiere un conjunto diferente de servidores DNS por sistema virtual, debe configurar un objeto proxy DNS. La resolución es específica del sistema virtual al que se ha asignado el proxy DNS. Si no tiene servidores DNS específicos que puedan aplicarse a este sistema virtual, el cortafuegos utiliza la configuración de DNS global.
- **Resolución DNS en el plano de datos para un sistema virtual**: este método también se conoce como solicitud de red para resolución DNS. El sistema virtual del usuario se puede configurar de modo que los nombres de dominio especificados se resuelvan en el servidor DNS del usuario en su red. Este método es compatible con *DNS dividido*, lo que significa que el usuario también puede usar sus propios servidores DNS del ISP para las consultas de DNS restantes no resueltas en su propio servidor. Las reglas de objeto proxy DNS controlan el DNS dividido; el dominio del usuario redirige las solicitudes DNS a sus servidores DNS, que están configurados con un perfil de servidor DNS. El perfil de servidor DNS tiene servidores DNS principales y secundarios designados, así como rutas de servicio DNS para IPv4 e IPv6, que anulan la configuración DNS predeterminada.

La siguiente tabla resume los tipos de resolución de DNS. La ubicación de enlace determina qué objeto de proxy DNS se usa para la resolución. Los casos de uso muestran, a modo de ejemplo, cómo un proveedor de servicios puede configurar los ajustes DNS con el fin de ofrecer servicios de DNS para resolver consultas de DNS requeridas en el cortafuegos y para los sistemas virtuales del usuario (abonado).

Tipo de resolución del	compartido: Lugar	compartido: Vsys específico
Resolución de DNS del cortafuegos: realizada por el plano de datos	Enlace: Global Ilustrado en el Caso de uso 1	n/c
Perfil de seguridad, informes y resolución de perfiles de servidor: realizado por el plano de gestión	Enlace: Global El mismo comportamiento que en caso de uso 1	Enlace: Vsys específico Ilustrado en el Caso de uso 2
Resolución de proxy DNS para hosts de clientes DNS conectados a la interfaz en el cortafuegos, que atraviesan el cortafuegos hacia un servidor DNS: realizado por el plano de datos.	Enlace: Interface (Interfaz) Ruta de servicio: Interfaz y dirección IP en las que se recibió la solicitud DNS. Ilustrado en el Caso de uso 3	

- Caso de uso 1: el cortafuegos exige la resolución de DNS
- Caso de uso 2: el usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, creación de informes y servicios dentro de su sistema virtual
- Caso de uso 3: el cortafuegos actúa como proxy DNS entre cliente y servidor

© 2020 Palo Alto Networks, Inc.

Configuración de un objeto proxy DNS

Si su cortafuegos va a funcionar como un proxy DNS, realice esta tarea para configurar un objeto proxy DNS. El objeto de proxy puede ser tanto compartido entre todos los sistemas virtuales como aplicado a un sistema virtual específico.

Cuando el cortafuegos está habilitado para funcionar como proxy DNS, las firmas de evasión que detectan solicitudes HTTP o TLS manipuladas pueden alertar en instancias en las que un cliente se conecta a un dominio que no sea el dominio especificado en la solicitud DNS original. Se recomienda habilitar las firmas de evasión tras configurar el proxy DNS para que se active una alerta si se detectan solicitudes manipuladas.

STEP 1 | Configure los ajustes básicos para un objeto de proxy DNS.

1. Seleccione **Network (Red)** > **DNS Proxy** y luego **Add (Añadir)** para añadir un nuevo objeto.
2. Verifique que **Enable** esté seleccionado.
3. Introduzca un nombre para el objeto en **Name**.
4. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica el objeto. Si selecciona **Shared (Compartido)**, debe especificar al menos una dirección **Primary (Primaria)** de servidor DNS y, de manera opcional, una dirección **Secondary (Secundaria)**.
5. Si ha seleccionado un sistema virtual, para **Server Profile (Perfil de servidor)**, seleccione un perfil de servidor DNS o haga clic en **DNS Server Profile (Perfil de servidor DNS)** para configurar un nuevo perfil. Consulte Configuración de un perfil de servidor DNS.
6. Para Inheritance Source (Origen de herencia), seleccione un origen del cual heredar las configuraciones del servidor DNS predeterminadas. El valor predeterminado es **None (Ninguno)**.
7. Para **Interface**, haga clic en **Add** y especifique las interfaces a las que se aplica el objeto de proxy DNS.
   - Si usa el objeto de proxy DNS para realizar búsquedas de DNS, necesita una interfaz. El cortafuegos escuchará las solicitudes de DNS en esta interfaz, y después las transmitirá.
   - Si usa el objeto de proxy DNS para una ruta de servicio, la interfaz es opcional.

STEP 2 | (Opcional) Especifique reglas de proxy DNS

1. En la pestaña **DNS Proxy Rules (Reglas de proxy DNS)**, haga clic en **Add (Añadir)** e introduzca un nombre para la regla en **Name (Nombre)**.
2. Seleccione **Turn on caching of domains resolved by this mapping**, si desea que el cortafuegos almacene en caché los dominios resueltos.
3. En **Domain Name (Nombre de dominio)**, seleccione **Add (Añadir)** para añadir una o más entradas por fila, con las cuales el cortafuegos comparará las consultas FQDN. Si una consulta coincide con uno de los dominios de la regla, la consulta se envía a uno de los siguientes servidores para resolverse (según lo que configuró en el paso anterior):
   - El servidor DNS **Primary (Primario)** o **Secondary (Secundario)** especificado directamente para este objeto proxy.
   - El servidor DNS **Primary (Primario)** o **Secondary (Secundario)** especificado directamente para este objeto proxy.

   DNS Proxy Rule and FQDN Matching (Regla de proxy DNS y coincidencia FQDN) describe de qué manera el cortafuegos coteja los nombres de dominio en un FQDN con una regla proxy DNS. Si no se encuentra coincidencia, los servidores DNS predeterminados resuelven la consulta.
4. Realice una de las siguientes acciones, según lo que configure en **Location (Ubicación)**:
   - Si ha elegido un sistema virtual, seleccione aquí un **DNS Server profile (Perfil de servidor DNS)**.
   - Si ha elegido **Shared (Compartido)**, introduzca una dirección **Primary (Primaria)** y, opcionalmente, una dirección **Secondary (Secundaria)**.

© 2020 Palo Alto Networks, Inc.

5. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Indique las entradas estáticas FQDN a dirección en el proxy DNS. Las entradas DNS estáticas permiten al cortafuegos resolver el FQDN a una dirección IP sin enviar una consulta al servidor DNS.

1. En la pestaña **Static Entries (Entradas estáticas)**, haga clic en **Add (Añadir)** e introduzca un nombre en **Name (Nombre)**.
2. Introduzca el nombre de dominio completo (**FQDN**).
3. Para **Address (Dirección)**, haga clic en **Add (Añadir)** e introduzca la dirección IP a la que se debería asignar el FQDN.

   Puede proporcionar direcciones IP adicionales para una entrada. El cortafuegos proporcionará todas las direcciones IP en su respuesta DNS y el cliente elige qué dirección usar.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Habilite el almacenamiento en caché y configure otros ajustes avanzados para el proxy DNS.

1. En la pestaña **Advanced (Avanzada)**, seleccione **TCP Queries (Consultas TCP)** para habilitar las consultas DNS mediante TCP.
   - **Max Pending Requests**: introduzca el número máximo de solicitudes DNS TCP pendientes simultáneas que admitirá el cortafuegos (intervalo 64-256, por defecto: 64).
2. Para **UDP Queries Retries (Reintentos de consultas UDP)**, introduzca lo siguiente:
   - **Interval (Intervalo)**: el tiempo (en segundos) después del cual se enviará otra solicitud si no se ha recibido respuesta (el intervalo es de 1 a 30, el valor predeterminado es 2).
   - **Attempts (Intentos)**: el número máximo de intentos de consulta UDP (sin incluir el primer intento) después de los cuales se intentará el siguiente servidor DNS (el intervalo es de 1 a 5; el valor predeterminado es 30).
3. Seleccione **Cache (Caché)** para habilitar al cortafuegos para que almacene en caché las asignaciones de FQDN a dirección que detecte. Debe habilitar la **caché** (habilitada de forma predeterminada) si este objeto proxy DNS se utiliza para consultas que genera el cortafuegos (es decir, en **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **DNS** o en **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** y seleccione un sistema virtual y **General** > **DNS Proxy (Proxy DNS)**.
   - **Enable TTL (Habilitar TTL)**: limite el tiempo que el cortafuegos almacena en caché las entradas DNS del objeto proxy. De forma predeterminada, esta opción está deshabilitada.
     - Introduzca **Time to Live (sec) (Periodo de vida [s])**, la cantidad de segundos después de los cuales se eliminan todas las entradas de la memoria caché para el objeto proxy. Después de eliminar las entradas, las nuevas solicitudes de DNS deben volver a resolverse y almacenarse en caché. El intervalo es de 60-86.400. No hay TTL por defecto; las entradas permanecen hasta que el cortafuegos se queda sin memoria caché.
   - **Cache EDNS Responses (Respuestas de EDNS de caché)**: debe habilitar esta configuración si se utiliza este objeto proxy DNS para consultas que genera el cortafuegos (es decir, en **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **DNS** o en **Device** > **Virtual Systems (Sistemas virtuales)** y selecciona un sistema virtual y **General** > **DNS Proxy (Proxy DNS)**.

STEP 5 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de un perfil de servidor DNS

Configure un perfil de servidor DNS, lo que simplifica la configuración de un sistema virtual. La dirección **Primary DNS (DNS primaria)** o **Secondary DNS (DNS secundaria)** se usa para crear la solicitud DNS que el sistema virtual envía al servidor DNS.

© 2020 Palo Alto Networks, Inc.

STEP 1 | Nombre el perfil de servidor DNS, seleccione el sistema virtual al que se aplica y especifica las direcciones de servidor DNS principal y secundaria.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **DNS** y **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil de servidor DNS.
2. Para **Location**, seleccione el sistema virtual al que se aplica el perfil.
3. En **Inheritance Source (Origen de herencia)**, seleccione **None (Ninguno)** si las direcciones del servidor DNS no se heredan. De lo contrario, especifique el servidor de DNS desde el que el perfil debería heredar la configuración. Si ha elegido un servidor DNS, haga clic en **Check inheritance source status** para ver esa información.
4. Especifique la dirección IP del servidor **Primary DNS** o déjelo como **inherited** si ha elegido un **Inheritance Source**.

   Tenga en cuenta que si especifica un FQDN en lugar de una dirección IP, el DNS para ese FQDN se resuelve en Device (Dispositivo) > Virtual Systems (Sistema virtual) > DNS Proxy (Proxy DNS).
5. Especifique la dirección IP del servidor **Secondary DNS**, o déjelo como **inherited** si ha elegido un **Inheritance Source**.

STEP 2 | Configure la ruta de servicio que usa el cortafuegos automáticamente, basada en si el servidor DNS de destino tiene un tipo de familia de dirección IP IPv4 o IPv6.

1. Haga clic en **Service Route IPv4** para habilitar la siguiente interfaz y la dirección IPv4 que se usará como ruta de servicio, si la dirección DNS de destino es una dirección IPv4.
2. Especifique la **Source Interface (Interfaz de origen)** para seleccionar la dirección IP de origen del servidor DNS que usará la ruta de servicio. El cortafuegos determina qué enrutador virtual se asigna a esa interfaz, y después realiza una búsqueda de rutas en la tabla de enrutamiento del enrutador virtual para llegar a la red de destino (en función de la dirección **Primary DNS**).
3. Especifique la **dirección de origen** IPv4 desde la que se originan los paquetes dirigidos al servidor de DNS.
4. Haga clic en **Service Route IPv6 (Ruta de servicio IPv6)** para habilitar la siguiente interfaz y la dirección IPv6 que se usará como ruta de servicio, si la dirección DNS de destino es una dirección IPv6.
5. Especifique la **Source Interface (Interfaz de origen)** para seleccionar la dirección IP de origen del servidor DNS que usará la ruta de servicio. El cortafuegos determina qué enrutador virtual se asigna a esa interfaz, y después realiza una búsqueda de rutas en la tabla de enrutamiento del enrutador virtual para llegar a la red de destino (en función de la dirección **Primary DNS**).
6. Especifique la **Source Address (Dirección de origen)** IPv6 desde la que se originan los paquetes dirigidos al servidor de DNS.
7. Haga clic en **OK (Aceptar)**.

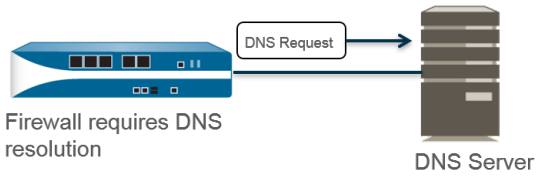
STEP 3 | Confirme la configuración.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Caso de uso 1: el cortafuegos exige la resolución de DNS

En este caso de uso, el cortafuegos es el cliente que solicita la resolución de DNS de los FQDN para las reglas de la política de seguridad, la creación de informes, los servicios de gestión (como correo electrónico, Kerberos, SNMP o syslog, entre otros) y los eventos de gestión (como servicios de actualización de software, actualizaciones dinámicas de software y WildFire). En los entornos dinámicos, los FQDN cambian con más frecuencia; por eso, una resolución de DNS precisa permite que el cortafuegos aplique las políticas con rigurosidad, preste servicios de gestión y elaboración de informes y maneje los eventos de gestión. Los servicios DNS globales y compartidos realizan la resolución DNS para las funciones del plano de gestión.

© 2020 Palo Alto Networks, Inc.



STEP 1 | Configure los servidores DNS principal y secundario que debe usar el cortafuegos para la resolución de DNS.

Debe configurar manualmente al menos un servidor DNS en el cortafuegos o no podrá resolver los nombres de host; el cortafuegos no utilizará los ajustes de servidor DNS de otra fuente, como un ISP.

1. Edite los ajustes de los servicios (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Global** en los cortafuegos que admiten varios sistemas virtuales; **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** en los que no los admiten).
2. En la pestaña **Services (Servicios)**, en **DNS**, seleccione **Servers (Servidores)** e introduzca la dirección del **Primary DNS Server (Servidor DNS principal)** y la dirección del **Secondary DNS Server (Servidor DNS secundario)**.
3. Continúe al paso 3.

STEP 2 | De manera alternativa, puede configurar un objeto Proxy DNS si desea configurar funciones DNS avanzadas como DNS dividido, anulaciones de proxy DNS, reglas de proxy DNS, entradas estáticas o herencia DNS.

1. Edite los ajustes de los servicios (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Global** en los cortafuegos que admiten varios sistemas virtuales; **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** en los que no los admiten).
2. En la pestaña **Services (Servicios)**, en **DNS**, seleccione **DNS Proxy Object (Objeto Proxy DNS)**.
3. En la lista **DNS Proxy (Proxy DNS)**, seleccione el proxy DNS que desea utilizar para configurar los servicios de DNS globales o bien seleccione **DNS Proxy (Proxy DNS)** para configurar un objeto de proxy DNS nuevo del modo siguiente:
   1. Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el objeto proxy DNS.
   2. En los cortafuegos que admiten varios sistemas virtuales, en **Location (Ubicación)**, seleccione **Shared (Compartido)** para los servicios proxy DNS globales en todo el cortafuegos.

      Los objetos proxy DNS compartidos no utilizan perfiles de servidor DNS porque no requieren una ruta de servicio específica que pertenezca a un sistema virtual del usuario.
   3. Introduzca la dirección IP del servidor DNS principal en **Primary (Principal)**. También puede introducir una dirección IP del servidor DNS **Secondary (Secundario)**.
4. Seleccione la pestaña **Advanced (Avanzado)**. Asegúrese de que la **caché** se habilite y se activen las **respuestas EDNS de la caché** (ambas habilitadas de forma predeterminada).
5. Haga clic en **OK (Aceptar)** para guardar el objeto proxy DNS.

STEP 3 | (Opcional) Configure el valor oportuno en **Minimum FQDN Refresh Time (sec) (Tiempo mínimo de actualización de FQDN [s])** para limitar la frecuencia con la que el cortafuegos actualiza las entradas de FQDN de la caché.

El cortafuegos actualiza de manera predeterminada cada uno de los FQDN que tiene almacenados en su caché en función del tiempo de vida (time-to-live, TTL) del FQDN incluido en un registro de DNS,

© 2020 Palo Alto Networks, Inc.

siempre que dicho valor sea igual o superior a este tiempo mínimo de actualización de los FQDN o, si no lo configura, al ajuste predeterminado de 30 segundos. Si desea especificar un tiempo mínimo de actualización de los FQDN, introduzca el valor oportuno en segundos entre 0 y 14 400; el valor predeterminado es 30. El valor 0 significa que el cortafuegos actualiza los FQDN en función del valor de TTL que figura en los registros de DNS, ya que el cortafuegos no aplica ningún tiempo mínimo de actualización de los FQDN. El cortafuegos usa el valor que sea más alto: el TTL de DNS o el tiempo mínimo de actualización de los FQDN.

Si el TTL del FQDN de DNS es breve, pero las resoluciones de FQDN no cambian con tanta frecuencia y no hacen falta actualizaciones tan repetidas, debe configurar un tiempo mínimo de actualización de los FQDN para que no se produzcan más intentos de actualización de los FQDN de los necesarios.

STEP 4 | (Opcional) En **FQDN Stale Entry Timeout (min) (Tiempo de espera de entradas obsoletas de FQDN [min])**, especifique cuántos minutos debe seguir usando el cortafuegos las resoluciones de FQDN obsoletas si no se puede acceder al servidor DNS; el intervalo admitido va de 0 a 10 080 y el valor predeterminado es 1440.

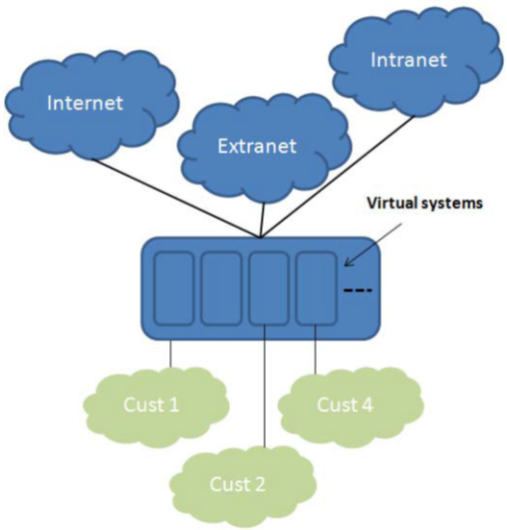
El valor 0 significa que el cortafuegos no sigue usando las entradas de FQDN obsoletas.

Asegúrese de que el tiempo de espera de las entradas de FQDN obsoletas sea lo suficientemente breve como para impedir el reenvío de tráfico incorrecto, que supone un riesgo para la seguridad, pero lo bastante prolongado para permitir la continuidad del tráfico sin causar interrupciones inesperadas en la red.

STEP 5 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual.

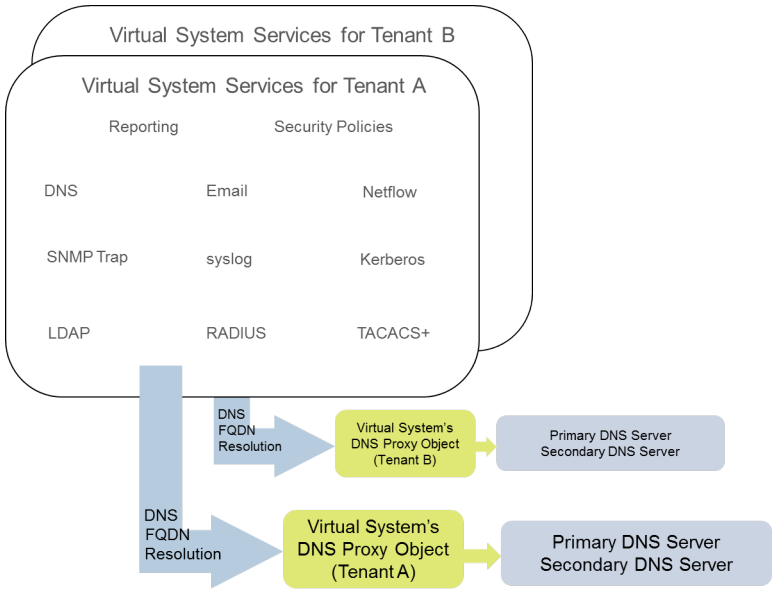
En este caso de uso, se definen varios usuarios (abonados del ISP) en el cortafuegos y a cada usuario se le asigna un sistema virtual (vsys) y un enrutador virtual diferentes para segmentar sus servicios y dominios administrativos. La siguiente figura ilustra varios sistemas virtuales dentro de un cortafuegos.



© 2020 Palo Alto Networks, Inc.

Cada usuario tiene sus propios perfiles de servidor para sus reglas de política de seguridad, informes y servicios de gestión (como correo electrónico, Kerberos, SNMP, syslog, etc.) definidos en sus propias redes.

Para las resoluciones DNS iniciadas por estos servicios, cada sistema virtual está configurado con su propio Objeto proxy DNS para permitir que cada usuario personalice la gestión de la resolución DNS dentro de su sistema virtual. Cualquier servicio con una **Location (Ubicación)** usará el objeto Proxy DNS configurado para el sistema virtual para determinar el servidor DNS principal (o secundario) para resolver FQDN, como se ilustra en la siguiente figura.



STEP 1 | Especifique el proxy DNS que se usará en cada sistema virtual.

1. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** y **Add (Añadir)** para añadir el **ID** del sistema virtual (el intervalo es de 1 a 255), y luego un nombre opcional en **Name (Nombre)**; en este ejemplo, Corp1 Corporation.
2. En la pestaña **General**, seleccione un **DNS Proxy (Proxy DNS)** o cree uno nuevo. En este ejemplo, se selecciona Corp1 DNS Proxy como el proxy para el sistema virtual de Corp1 Corporation.
3. En **Interfaces**, haga clic en **Add (Añadir)**. En este ejemplo, Ethernet 1/20 se dedica a este usuario.
4. En **Virtual Routers (Enrutadores virtuales)**, haga clic en **Add (Añadir)**. Se asigna al sistema virtual un enrutador virtual llamado Corp1 VR para separar las funciones de enrutamiento.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure un proxy DNS y un perfil de servidor para permitir la resolución DNS para un sistema virtual.

1. Seleccione **Network (Red)** > **DNS Proxy** y haga clic en **Add (Añadir)**.
2. Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el proxy DNS.
3. En **Location (Ubicación)**, seleccione el sistema virtual del usuario, en este ejemplo, Corp1 Corporation (vsys6). (Puede elegir el recurso proxy DNS **Shared (Compartido)** en su lugar).
4. En **Server Profile (Perfil de servidor)**, seleccione o cree un perfil con el fin de personalizar servidores DNS para usar resoluciones DNS para esta política de seguridad de usuarios, informe y servicios de perfil de servidor.

   Si el perfil aún no está configurado, en el campo **Server Profile (Perfil de servidor)**, haga clic en **DNS Server Profile (Perfil de servidor DNS)** para Configuración de un perfil de servidor DNS.

   El perfil de servidor DNS identifica las direcciones IP del servidor DNS principal y secundario para usar las resoluciones de DNS de gestión para este sistema virtual.

© 2020 Palo Alto Networks, Inc.

5. También para este perfil de servidor, tiene la opción de configurar una **Service Route IPv4 (IPv4 de ruta de servicio)** o una **Service Route IPv6 (IPv6 de ruta de servicio)** para indicar al cortafuegos qué **Source Interface (Interfaz de origen)** usar en sus solicitudes DNS. Si esta interfaz tiene más de una dirección IP, configure también la **Source Address (Dirección de origen)**.
6. Seleccione la pestaña **Advanced (Avanzado)**. Asegúrese de que la **caché** se habilite y se activen las **respuestas EDNS de la caché** (ambas habilitadas de forma predeterminada). Esto es obligatorio si se utiliza el objeto proxy DNS en **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** > **vsys** > **General** > **DNS Proxy (Proxy DNS)**.
7. Haga clic en **OK (Aceptar)**.
8. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Se pueden configurar funciones avanzadas opcionales como DNS dividido usando DNS Proxy Rules (Reglas de proxy DNS). Si es necesario, se puede usar un perfil de servidor DNS separado para redirigir las resoluciones DNS que coinciden con el Domain Name (Nombre de dominio) en una DNS Proxy Rule (Regla de proxy DNS) para otro conjunto de servidores DNS. El Caso de uso 3 ilustra el DNS dividido.

Si usa dos perfiles de servidor DNS separados en el mismo objeto Proxy DNS, uno para el proxy DNS y otro para la regla de proxy DNS, se produce lo siguiente:

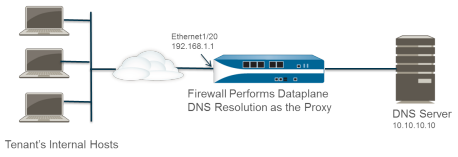
- Si se define una ruta de servicio en el perfil de servidor DNS usado por el proxy DNS, tiene prioridad y se usa.
- Si se define una ruta de servicio en el perfil de servidor DNS usado en las reglas del proxy DNS, no se usa. Si la ruta de servicio difiere de la definida en el perfil de servidor DNS usado en el proxy DNS, se muestra el siguiente mensaje de advertencia durante el proceso **Commit (Confirmar)**:

```
Warning: The DNS service route defined in the DNS proxy object is
 different from the DNS proxy rule's service route. Using the DNS proxy
 object's service route.
```

- Si no se define ninguna ruta de servicio en ningún perfil de servidor DNS, se usa la ruta de servicio global en caso necesario.

Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor

En este caso de uso, el cortafuegos se encuentra entre el cliente DNS y el servidor DNS. Se configura un cortafuegos en el proxy DNS para que actúe como servidor DNS de los hosts que residen en la red del usuario conectada a la interfaz del cortafuegos. En dicho escenario, el cortafuegos realiza una resolución DNS en su plano de datos.



El escenario utiliza *DNS dividido*, una configuración donde las reglas de proxy DNS se configuran para redirigir las solicitudes DNS a un conjunto de servidores DNS basados en una coincidencia de nombres de dominio. Si no hay coincidencia, el perfil del servidor determina los servidores DNS a los que se envía la solicitud; por eso, hay dos métodos de resolución de DNS dividido.

© 2020 Palo Alto Networks, Inc.

Para las resoluciones DNS de plano de datos, la dirección IP de origen desde el proxy DNS en PAN-OS al servidor DNS externo sería la dirección del proxy (la IP de destino de la solicitud original). No se usa ninguna ruta de servicio definida en el perfil de servidor DNS. Por ejemplo, si la consulta se realiza desde el host 172.16.1.1 al proxy DNS 192.168.1.1, la solicitud al servidor DNS (en 10.10.10.10) usaría un origen 192.168.1.1 y un destino 10.10.10.10.

STEP 1 | Seleccione **Network (Red)** > **DNS Proxy** y haga clic en **Add (Añadir)**.

STEP 2 | Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el proxy DNS.

STEP 3 | En **Location (Ubicación)**, seleccione el sistema virtual del usuario, en este ejemplo, Corp1 Corporation (vsys6).

STEP 4 | En **Interface (Interfaz)**, seleccione la interfaz que recibirá las solicitudes DNS de los hosts del usuario, en este ejemplo, Ethernet 1/20.

STEP 5 | Seleccione o cree un **Server Profile (Perfil de servidor)** para personalizar servidores DNS para que resuelvan solicitudes DNS para este usuario.

STEP 6 | En la pestaña **DNS Proxy Rules (Reglas de proxy DNS)**, haga clic en **Add (Añadir)** e introduzca un nombre para la regla en **Name (Nombre)**.

STEP 7 | (Opcional) Seleccione **Turn on caching of domains resolved by this mapping (Activar el almacenamiento en caché de dominios resueltos por esta asignación)**.

STEP 8 | Haga clic en **Add (Añadir)** para añadir uno o más nombres de dominio en **Domain Name (Nombre de dominio)**, uno por fila. En Búsqueda de coincidencias de FQDN en la regla de proxy DNS, se describe cómo el cortafuegos encuentra coincidencias entre los FQDN y los nombres de dominio en una regla de proxy DNS.

STEP 9 | En **DNS Server profile (Perfil de servidor DNS)**, seleccione un perfil. El cortafuegos compara el nombre de dominio en la solicitud DNS con el nombre de dominio definido en **DNS Proxy Rules (Reglas de proxy DNS)**. Si hay coincidencia, se usa el **DNS Server profile (Perfil de servidor DNS)** definido en la regla para determinar el servidor DNS.

STEP 10 | En este ejemplo, si el dominio en la solicitud coincide con myweb.corp1.com, se usa el servidor DNS definido en perfil de servidor myweb DNS Server Profile. Si no hay coincidencia, se usa el servidor DNS definido en **Server profile (Perfil de servidor)** (perfil de servidor DNS Corp1).

STEP 11 | Haga clic en **OK** dos veces.

Regla de proxy DNS y coincidencia FQDN

Cuando configura el cortafuegos con un objeto proxy DNS que utiliza reglas de proxy DNS, el cortafuegos compara un FQDN de una consulta DNS con el nombre de dominio de una regla de proxy DNS. La comparación del cortafuegos funciona de la siguiente manera:

© 2020 Palo Alto Networks, Inc.

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
El cortafuegos primero divide en tokens los FQDN y los nombres de dominio de las reglas de proxy DNS. En un nombre de dominio, un token es una cadena delimitada por un punto (.).	**`*.boat.fish.com`** se compone de cuatro tokens tokens: **`[*][boat][fish][com]`**
El proceso de cotejo es una coincidencia de token exacta entre el FQDN y el nombre de dominio en la regla, las cadenas parciales no se cotejan.	Regla: **`fishing`** FQDN: **`fish`** — **no hay coincidencia**
Una excepción al requisito de coincidencia exacta es el uso del carácter comodín: un asterisco (*). El * coincide con uno o más tokens. Esto significa que una regla que consta únicamente de un carácter comodín (*) compara cualquier FQDN con uno o más tokens.	Regla: **`*.boat.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.blue.boat.com`** — coincidencia FQDN: **`boat.com`** — **no hay coincidencia**
	Regla: **`*`** FQDN: **`boat`** — coincidencia FQDN: **`boat.com`**: coincidencia FQDN: **`www.boat.com`** — coincidencia
Puede usar el * en cualquier posición: antes del token, entre tokens o al final de un token (pero no con otros caracteres, como un único token).	Regla: **`www.*.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.blue.boat.com`** — coincidencia
	Regla: **`www.*.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.boat.fish.com`**: coincidencia
	Regla: **`www.boat*.com`**: **no válida**
Pueden aparecer varios caracteres comodines (*) en cualquier posición del nombre de dominio: antes del token, entre tokens o al final del token. Cada * no consecutivo coincide con uno o más tokens.	Regla: **`a.*.d.*.com`** FQDN: **`a.b.d.e.com`**: coincidencia FQDN: **`a.b.c.d.e.f.com`**: coincidencia FQDN: **`a.d.d.e.f.com`**: coincidencia (el primer **`*`** coincide con **`d`**; el segundo **`*`** coincide con **`e`** y **`f`**). FQDN: **`a.d.e.f.com`**: **no hay coincidencia** (el primer **`*`** coincide con **`d`**; las **`d`** posteriores de la regla no se cotejan).
Cuando se utilizan caracteres comodín en tokens consecutivos, el primer * coincide con uno o más tokens; el segundo * coincide con un token.	Caracteres comodín consecutivos antes de los tokens: Regla: **`*.*.boat.com`** FQDN: **`www.blue.boat.com`** — coincidencia

© 2020 Palo Alto Networks, Inc.

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
Esto significa que una regla que consta únicamente de *.* compara cualquier FQDN con dos o más tokens.	FQDN: **www.blue.sail.boat.com**: coincidencia
	Caracteres comodín consecutivos entre tokens: Regla: **www.*.*.boat.com** FQDN: **www.blue.sail.boat.com**: coincidencia FQDN: **www.big.blue.sail.boat.com**: coincidencia
	Caracteres comodín consecutivos al final de los tokens: Regla: **www.boat.*.*** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia
	Caracteres comodín consecutivos únicamente: Rule: *.* FQDN: **boat: no hay coincidencia** FQDN: **boat.com**: coincidencia FQDN: **www.boat.com** — coincidencia
Los caracteres comodín consecutivos y no consecutivos pueden aparecer en la misma regla.	Regla: **a.*.d.*.*.com** FQDN: **a.b.c.d.e.f.com**: coincidencia (el primer ***** coincide con **b** y **c**; el segundo ***** coincide con **e**; el tercer ***** coincide con **f**). FQDN: **a.b.c.d.e.com**: **no hay coincidencia** (el primer ***** coincide con **b** y **c**; el segundo ***** coincide con **e**; el tercer ***** no se coteja).
El comportamiento de coincidencia final implícita ofrece una taquigrafía adicional: Mientras el último token de la regla no sea un *, la comparación cotejará si todos los tokens de la regla coinciden con el FQDN, incluso si el FQDN posee tokens finales adicionales que la regla no tiene.	Regla: **www.boat.fish** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia FQDN: **www.boat.fish**: coincidencia
Esta regla finaliza con *, por lo que la regla de coincidencia final implícita no se aplica. El * actúa como se indica; coincide con uno o más tokens.	Regla: **www.boat.fish.*** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia FQDN: **www.boat.fish: no hay coincidencia** (este FQDN no posee un token para coincidir con el * en la regla).

© 2020 Palo Alto Networks, Inc.

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
En el caso en que un FQDN coincida con más de una regla, un algoritmo de separación selecciona la regla más específica (extensa); es decir, el algoritmo favorece la regla con más tokens y menos caracteres comodines (*).	Regla 1: **`*.fish.com`**: coincidencia Regla 2: **`*.com`**: coincidencia Regla 3: **`boat.fish.com`**: coincidencia y división FQDN: **`boat.fish.com`** El FQDN coincide con las tres reglas; el cortafuegos utiliza la regla 3 debido a que es la más específica.
	Regla 1: **`*.fish.com`: no hay coincidencia** Regla 2: **`*.com`**: coincidencia Regla 3: **`boat.fish.com`: no hay coincidencia** FQDN: **`fish.com`** El FQDN no coincide con la Regla 1 debido a que el * no tiene un token con el cual coincidir.
	Regla 1: **`*.fish.com`**: coincidencia y división Regla 2: **`*.com`**: coincidencia Regla 3: **`boat.fish.com`: no hay coincidencia** FQDN: **`blue.boat.fish.com`** El FQDN coincide con la Regla 1 y la Regla 2 (debido a que el * coincide con uno o más tokens). El cortafuegos utiliza la regla 1 debido a que es la más específica.
Al trabajar con caracteres comodín (*) y reglas de coincidencia final implícita, puede haber casos en los que el FQDN coincide con más de una regla y el algoritmo de separación pondera las reglas por igual. Para evitar ambigüedades, si las reglas con coincidencia final implícita o un carácter comodín (*) pueden superponerse, reemplace una regla de coincidencia final implícita al especificar el token final.	Reemplace lo siguiente: Regla: **`www.boat`** por lo siguiente: Regla: **`www.boat.com`**
Prácticas recomendadas para crear reglas de proxy DNS a fin de evitar ambigüedad y resultados inesperados	
Incluya un dominio de nivel superior en el nombre de dominio para que no se invoque una coincidencia final implícita, que podría hacer coincidir el FQDN con más de una regla.	**`boat.com`**

© 2020 Palo Alto Networks, Inc.

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
Si utiliza un carácter comodín (*), utilícelo únicamente como el token del extremo izquierdo. Esta práctica permite la comprensión común de los registros DNS con caracteres comodín y la naturaleza jerárquica del DNS.	**`*.boat.com`**
No use más de un* en una regla.	
Use el * para establecer una regla de base asociada con un servidor DNS, y utilice reglas con más tokens para crear excepciones a la regla, la cual asocia con diferentes servidores. El algoritmo de división seleccionará la coincidencia más específica, en función de la cantidad de tokens coincidentes.	Regla: **`*.corporation.com`**: servidor DNS A Regla: **`www.corporation.com`**: servidor DNS B Regla: **`*.internal.corporation.com`**: servidor DNS C Regla: **`www.internal.corporation.com`**: servidor DNS D FQDN: **`mail.internal.corporation.com`**: coincide con el servidor DNS C FQDN: **`mail.corporation.com`**: coincide con el servidor DNS A

© 2020 Palo Alto Networks, Inc.

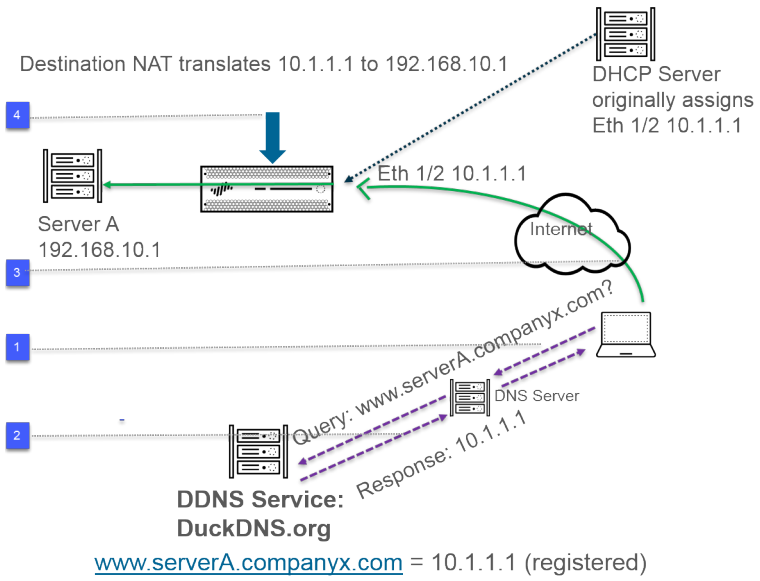
Descripción general del DNS dinámico

Si hay servicios alojados tras el cortafuegos y se emplean políticas de traducción de direcciones de red (network address translation, NAT) de destino para acceder al cortafuegos o si es preciso franquear el acceso remoto al cortafuegos, registre los cambios en las direcciones IPv4 (si la interfaz es un cliente DHCP que recibe una dirección dinámica o tiene una dirección estática) o las direcciones IPv6 (solo estáticas) de la interfaz con un proveedor de servicios de sistemas de nombres de dominio dinámicos (dynamic domain name system, DDNS). El servicio DDNS actualiza automáticamente las asignaciones de nombres de dominio a direcciones IP con el fin de proporcionar direcciones IP precisas a los clientes DNS para que puedan acceder al cortafuegos y a los servicios que protege. Este servicio se suele utilizar en las implementaciones de sucursales que alojan servicios. Si las interfaces de cortafuegos no admiten DDNS, hacen falta componentes externos para proporcionar direcciones IP precisas a los clientes.

Los cortafuegos admiten estos proveedores de servicios de DDNS: Duck DNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org y No-IP. Cada proveedor ofrece unos servicios distintos, por ejemplo, el número de direcciones IP que admite para cada nombre de host o la compatibilidad con direcciones IPv6. Palo Alto Networks aprovecha las actualizaciones de contenido para añadir más proveedores de DDNS y para facilitar las actualizaciones en sus servicios.

En las configuraciones de alta disponibilidad (high availability, HA), compruebe que las versiones de contenido de los peers del cortafuegos de HA (activo/pasivo o activo/activo) estén sincronizadas, ya que el cortafuegos basa el mantenimiento de la configuración de DDNS en la versión de contenido vigente de Palo Alto Networks. Palo Alto Networks puede modificar o dejar de usar servicios de DDNS disponibles mediante versiones de contenido. Además, los proveedores de DDNS pueden alterar sus servicios. Si no coinciden las versiones de contenido de los peers de HA, pueden tener problemas para utilizar el servicio DDNS.

En el ejemplo siguiente, el cortafuegos es un cliente DDNS de un proveedor de servicios de DDNS. Al principio, el servidor DHCP asigna la dirección IP 10.1.1.1 a la interfaz Ethernet 1/2. La política de NAT de destino traduce la dirección pública 10.1.1.1 a la auténtica dirección del servidor A (192.168.10.1), situado tras el cortafuegos.



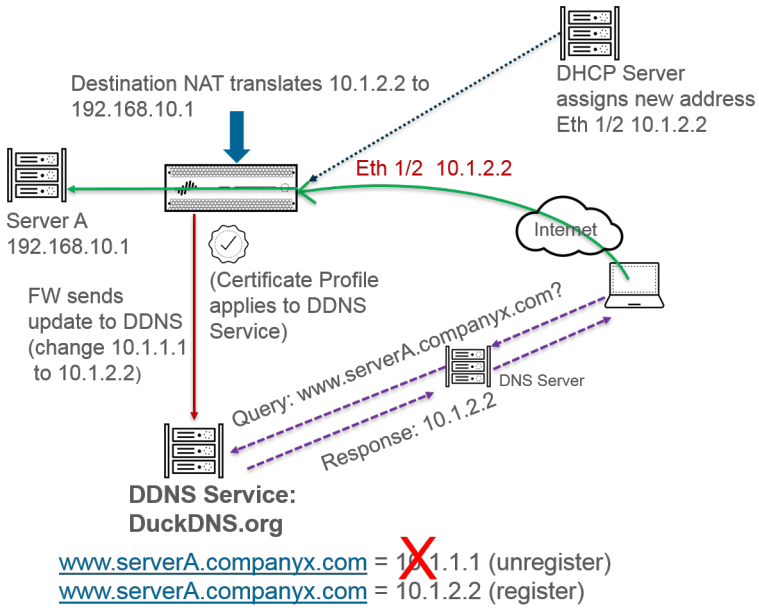
1. Cuando el usuario se intenta poner en contacto con www.serverA.companyx.com, consulta la dirección IP en el servidor DNS local. En este ejemplo, www.serverA.companyx.com (configurado como

© 2020 Palo Alto Networks, Inc.

CNAME en el registro de duckdns.org: serverA.companyx.duckdns.org) es un dominio que pertenece al proveedor de DDNS (Duck DNS). El servidor DNS comprueba el registro con el proveedor de DDNS para resolver la consulta.

2. El servidor DNS responde al usuario con 10.1.1.1, que es la dirección IP de www.serverA.companyx.com.
3. El paquete del usuario cuyo destino es 10.1.1.1 va a la interfaz del cortafuegos Ethernet 1/2.
4. En este ejemplo, el cortafuegos ejecuta la NAT de destino y traduce 10.1.1.1 a 192.168.10.1 antes de enviar el paquete al destino.

Algún tiempo después, DHCP asigna una dirección IP nueva a la interfaz del cortafuegos, lo cual provoca la siguiente actualización de DDNS:



1. El servidor DHCP asigna una dirección IP nueva (10.1.2.2) a Ethernet 1/2.
2. Cuando el cortafuegos recibe esta información, envía una actualización al servicio DDNS con la nueva dirección de www.serverA.companyx.com para que la registre. El cortafuegos también envía actualizaciones periódicas según los intervalos configurados. La actualizaciones de DDNS las envía por el puerto HTTPS 443.

La siguiente vez que el cliente consulta la dirección IP de www.serverA.companyx.com en el servidor DNS, que consulta el servicio DDNS, este envía la dirección actualizada (10.1.2.2). El usuario emplea esa dirección actualizada y logra acceder al servicio o a la aplicación que le interesa por medio de la interfaz del cortafuegos.

Si ha configurado el modo activo/pasivo de HA, el cortafuegos envía las actualizaciones de DDNS al servicio DDNS mientras convergen los estados de ambos cortafuegos. Cuando se alcanza la convergencia, se deshabilita DDNS en el cortafuegos pasivo. Por ejemplo, la primera vez que arrancan dos cortafuegos de HA, ambos envían actualizaciones de DDNS hasta que dilucidan si están en modo activo o pasivo. Mientras tanto, aparecen actualizaciones de DDNS en los logs del sistema. Cuando convergen los estados de HA y cada uno de los cortafuegos notifica a sus clientes si es activo o pasivo, el cortafuegos pasivo deja de enviar actualizaciones de DDNS. En el modo de HA con peers activo/activo, no se sincroniza la configuración de DDNS porque cada cortafuegos tiene la suya propia.

© 2020 Palo Alto Networks, Inc.

Configuración del DNS dinámico en las interfaces de cortafuegos

Antes de configurar sistemas de nombres de dominio dinámicos (dynamic domain name system, DDNS) en las interfaces de cortafuegos:

- Averigüe el nombre de host registrado en el proveedor de DDNS.
- Obtenga el certificado SSL público del servicio DDNS e impórtelo al cortafuegos.
- (Con FreeDNS Afraid.org v. 1 o FreeDNS Afraid.org Dynamic API v. 1) En el servidor DDNS, la pestaña de este servicio incluye la opción **Link updates of the same IP together? (Actualizar la misma IP a la vez).** Si la marca, el servicio DDNS actualiza el nombre de host en todos los registros de DNS que contengan la dirección IP antigua que ha cambiado, no solo en el registro de DNS de un nombre de host y una dirección IP únicos. Para evitarlo, quite la marca de la opción **Link updates of the same IP together? (Actualizar la misma IP a la vez)**. De ese modo, el servidor DDNS solo actualiza el registro de DNS que contiene el nombre de host concreto con la nueva dirección IP incluida en la actualización de DDNS.

STEP 1 | Configure DDNS.

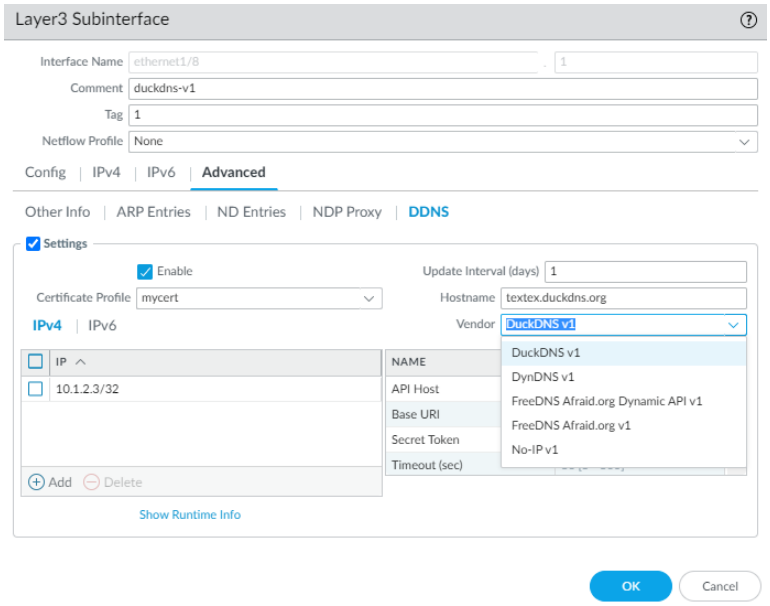
1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz de capa 3, una subinterfaz o una interfaz Ethernet de agregación (AE) o bien seleccione **Network (Red)** > **Interfaces** > **VLAN** y seleccione una interfaz o una subinterfaz.
2. Seleccione **Advanced (Opciones avanzadas)** > **DDNS** y seleccione **Settings (Configuración)**.
3. Marque **Enable (Habilitar)** para habilitar DDNS. Debe habilitar inicialmente DDNS para configurarlo. Si la configuración de su DDNS no está terminada, guárdela sin habilitarla para no perder los cambios realizados hasta el momento.
4. En **Update Interval (days) (Intervalo entre actualizaciones [días])**, introduzca el número de días que debe transcurrir entre los envíos del cortafuegos al servicio DDNS para actualizar las direcciones IP asignadas a los FQDN; el valor predeterminado es 1 y el intervalo, de 1 a 30. Base este intervalo en la frecuencia con la que cambian las direcciones IP. Además de estas actualizaciones, el cortafuegos también envía otras a intervalos periódicos que, por ejemplo, garantizan que no se pierdan las relativas a cambios en las direcciones.
5. En **Hostname (Nombre de host)**, introduzca el nombre de host de la interfaz registrada en el servicio DDNS (por ejemplo, www.serverA.companyx.com o serverA).

   Cerciórese de que es el nombre de host registrado en el servicio DDNS. Debe introducir un FQDN como nombre de host. El cortafuegos no lo valida salvo para confirmar que la sintaxis solo utiliza los caracteres válidos que admite DNS para los nombres de dominio.
6. Seleccione **IPv4** y seleccione una dirección IPv4 o varias que estén asignadas a la interfaz o bien haga clic en **Add (Añadir)** para añadir la dirección IPv4 que desea asociar al nombre de host (por ejemplo, 10.1.1.1). Puede seleccionar tantas direcciones IPv4 como permita el servicio DDNS. Todas las direcciones IPv4 seleccionadas se registran en el servicio DDNS. Seleccione al menos una dirección IPv4 o IPv6.
7. Seleccione **IPv6** y seleccione una dirección IPv6 o varias que estén asignadas a la interfaz o bien haga clic en **Add (Añadir)** para añadir la dirección IPv6 que desea asociar al nombre de host. Puede seleccionar tantas direcciones IPv6 como permita el servicio DDNS. Todas las direcciones IPv6 seleccionadas se registran en el servicio DDNS. Seleccione al menos una dirección IPv4 o IPv6.
8. En **Certificate Profile (Perfil de certificados)**, seleccione o cree un perfil de certificados usando el certificado SSL importado del servicio DDNS para verificarlo cuando el cortafuegos se conecta por primera vez a dicho servicio para registrar alguna dirección IP y en cada actualización. Cuando el cortafuegos se conecta al servicio DDNS para enviar actualizaciones, este le otorga un certificado SSL

© 2020 Palo Alto Networks, Inc.

firmado por la entidad de certificación (certificate authority, CA) con el que se puede autenticar en el servicio.

9. En **Vendor (Proveedor)**, seleccione el proveedor y el número de versión que utiliza para el servicio DDNS.



Palo Alto Networks puede cambiar los proveedores de servicios de DDNS admitidos mediante una actualización de contenido.

10. La opción seleccionada en Vendor (Proveedor) condiciona los valores que se muestran debajo en los campos **Name (Nombre)** y **Value (Valor)**. Algunos campos de valor son de solo lectura e indican los parámetros que utiliza el cortafuegos para conectarse al servicio DDNS. Configure los demás campos de valores, como la contraseña que proporciona el servicio DDNS y el tiempo de espera que aplica el cortafuegos si no recibe ninguna actualización del servicio DDNS.
11. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Si desea que el cortafuegos se comunique con el servicio DDNS con otra interfaz que no sea la de gestión, configure una ruta de servicio para DDNS; consulte Establecimiento de acceso a la red para servicios externos.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | Consulte la información de DDNS de la interfaz.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** o **Network (Red)** > **Interfaces** > **VLAN** y seleccione la interfaz que ha configurado. Las interfaces que tienen configurado DDNS muestran el icono en el campo Features (Funciones).
2. Seleccione **Advanced (Opciones avanzadas)** > **DDNS** y marque **Settings (Configuración)**.
3. Haga clic en **Show Runtime Info (Mostrar información de tiempo de ejecución)** para ver los datos de DDNS de la interfaz, entre otros, el código generado con la última actualización de los FQDN o la fecha y la hora cuando el servicio DDNS la ha recibido.

© 2020 Palo Alto Networks, Inc.

NAT

Esta sección describe la traducción de direcciones de red (Network Address Translation, NAT) y cómo configurar el cortafuegos para NAT. El NAT le permite traducir la direcciones IPv4 privadas y no enrutables a una o más direcciones IPv4 globalmente enrutables, con lo cual se conservan las direcciones IP enrutables de la organización. El NAT le permite no tener que divulgar las direcciones IP reales de los hosts que deben acceder a direcciones públicas y gestionar el tráfico al realizar el reenvío de puertos. Puede usar NAT para resolver dificultades de diseño de la red y permitir que las redes con subredes IP idénticas se comuniquen entre sí. El cortafuegos admite NAT en capa 3 e interfaces de Virtual Wire.

La opción NAT64 traduce entre direcciones IPv4 e IPv6, por lo que ofrece conectividad entre las redes con esquemas de direcciones IP distintas y una ruta de migración hacia las direcciones IPv6. La traducción de prefijo de red IPv6 a IPv6 (NPTv6) traduce un prefijo IPv6 a otro prefijo IPv6. PAN-OS es compatible con todas estas funciones.

Cuando utilice direcciones IP privadas en sus redes internas, deberá utilizar NAT para traducir las direcciones privadas en direcciones públicas que puedan enrutarse a redes externas. En PAN-OS, usted crea reglas de políticas de NAT que indican al cortafuegos qué direcciones de paquetes y puertos necesitan traducción y cuáles son las direcciones y puertos traducidos.

- Reglas de políticas NAT
- NAT de origen y destino
- Casos de uso de NAT de destino con reescritura de DNS
- Capacidades de regla NAT
- Sobresuscripción de NAT de IP dinámica y puerto
- Estadísticas de memoria NAT de plano de datos
- Configuración de NAT
- Ejemplos de configuración de NAT

Reglas de políticas NAT

- Descripción general de la política de NAT
- Grupos de direcciones NAT identificados como objetos de direcciones
- ARP proxy para grupos de direcciones NAT

Descripción general de la política de NAT

Puede configurar una regla NAT que coincida con una zona de origen del paquete y una zona de destino, como mínimo. Además de las zonas, puede configurar criterios equivalentes basados en la interfaz de destino del paquete, la dirección de origen y destino y servicio. Puede configurar múltiples reglas NAT. El cortafuegos evalúa las reglas en orden descendente. Cuando un paquete compara los criterios de una única regla NAT, el paquete no está sujeto a reglas NAT adicionales. Por ello, su lista de reglas NAT debe estar en orden de más a menos específico, de modo que los paquetes estén sujetos a la regla más específica que haya creado para ellos.

Las reglas NAT estáticas no tienen prioridad sobre otras formas de NAT. Por lo tanto, para que la NAT estática funcione, las reglas NAT estática deben estar por encima del resto de reglas NAT en la lista del cortafuegos.

Las reglas NAT ofrecen traducción de direcciones, y son distintas de las reglas de políticas de seguridad, que permiten o deniegan paquetes. Es importante comprender la lógica del flujo del cortafuegos cuando aplica las reglas NAT y las reglas de política de seguridad, de modo que pueda determinar qué reglas necesita en función de las zonas que ha definido. Debe configurar reglas de política de seguridad para permitir el tráfico de NAT.

© 2020 Palo Alto Networks, Inc.

En la entrada, el cortafuegos examina el paquete y enruta la búsqueda para determinar la interfaz de salida y la zona. Entonces el cortafuegos determina si el paquete coincide con alguna de las reglas NAT que se han definido, basándose en la zona de origen o destino. A continuación, evalúa y aplica las políticas de seguridad que coincidan con el paquete basándose en las direcciones de origen y destino originales (anteriores a NAT), pero en las zonas posteriores a NAT. Por último, en la salida cuando una de las reglas NAT coincide, el cortafuegos traduce las direcciones y números de puerto de origen y de destino.

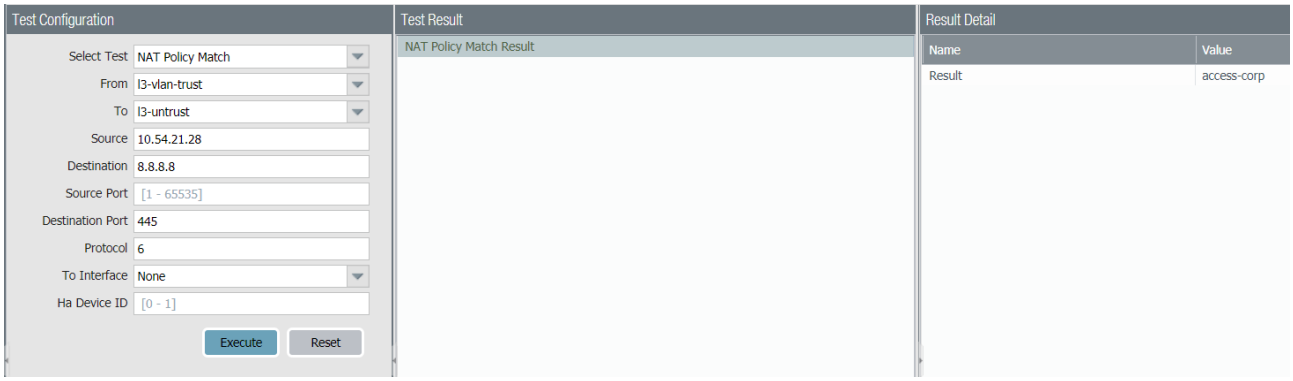
Tenga en cuenta que la traducción de la dirección IP y el puerto no se produce hasta que el paquete sale del cortafuegos. Las reglas y políticas de seguridad NAT se aplican a la dirección IP original (la dirección anterior a NAT). Una regla NAT se configura en función de la zona asociada con una dirección IP anterior a NAT.

Las políticas de seguridad difieren de las reglas NAT en que examinan las zonas anteriores a NAT para determinar si se permite o no el paquete. Como la naturaleza de NAT es modificar las direcciones IP de origen o destino, lo que puede provocar que se modifique la zona y la interfaz saliente del paquete, las políticas de seguridad se aplican en la zona posterior a NAT.

Una llamada SIP en ocasiones experimenta un audio unidireccional cuando atraviesa el cortafuegos, debido a que el administrador de llamadas envía un mensaje de SIP en reemplazo del teléfono para establecer la conexión. Cuando el mensaje del administrador de llamadas llega al cortafuegos, el SIP ALG debe colocar la dirección IP del teléfono a través de NAT. Si el administrador de llamadas y los teléfonos no están en la misma zona de seguridad, la búsqueda de NAT de la dirección IP del teléfono se realiza usando la zona del administrador de llamadas. La política de NAT debe tener esto en cuenta.

Las reglas no NAT están configuradas para permitir la exclusión de direcciones IP definidas en el intervalo de las reglas NAT definidas posteriormente en la política NAT. Para definir una política no NAT, especifique todos los criterios coincidentes y seleccione Sin traducción de origen en la columna de traducción de origen.

Si desea verificar las reglas de NAT procesadas, seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y compruebe las coincidencias del tráfico con ellas. Por ejemplo:



Grupos de direcciones NAT identificados como objetos de direcciones

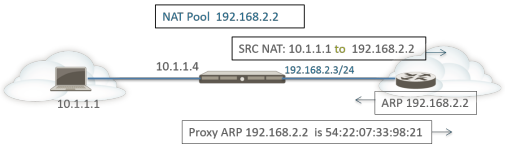
Al configurar un grupo de direcciones NAT de **Dynamic IP** o **Dynamic IP and Port** en una regla de políticas NAT, lo habitual es configurar el grupo de direcciones traducidas con un objeto de dirección. Cada objeto de dirección puede ser una dirección IP de host, un intervalo de direcciones IP o una subred de IP.

Debido a que tanto las reglas NAT como las reglas de política de seguridad usan objetos de dirección, lo mejor es distinguirlas nombrando al objeto de dirección que se usa para NAT con un prefijo, como por ejemplo "nombre NAT".

© 2020 Palo Alto Networks, Inc.

ARP proxy para grupos de direcciones NAT

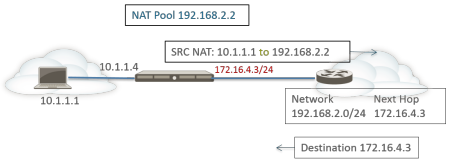
Los grupos de direcciones NAT no están vinculados a ninguna interfaz. La figura siguiente ilustra el comportamiento del cortafuegos cuando realiza ARP proxy para una dirección en un grupo de direcciones NAT.



El cortafuegos realiza NAT de origen para un cliente, traduciendo la dirección de origen 10.1.1.1 a la dirección en el grupo NAT, 192.168.2.2. El paquete traducido se envía a un enrutador.

Para el tráfico de retorno, el enrutador no sabe cómo llegar a 192.168.2.2 (porque la dirección IP solo es una dirección en el grupo de direcciones NAT), de modo que envía un paquete de solicitud de ARP al cortafuegos.

- Si el grupo de direcciones (192.168.2.2) está en la misma subred que la dirección IP de interfaz de entrada/salida (192.168.2.3/24), el cortafuegos puede enviar una respuesta de ARP proxy al enrutador, que indica la dirección MAC de capa 2 de la dirección IP, como muestra la figura anterior.
- Si el grupo de direcciones (192.168.2.2) no es una subred de una interfaz en el cortafuegos, el cortafuegos no enviará una respuesta ARP proxy al enrutador. Esto significa que el enrutador debe estar configurado con la ruta necesaria para saber a dónde enviar los paquetes destinados a 192.168.2.2, con el fin de garantizar que el tráfico de retorno se enruta de regreso al cortafuegos, como se muestra en la figura siguiente.



NAT de origen y destino

El cortafuegos admite tanto la traducción de puerto y/o dirección de origen como la traducción de puerto y/o dirección de destino.

- NAT de origen
- NAT de destino

NAT de origen

Los usuarios internos suelen usar el NAT de origen para acceder a Internet; la dirección de origen de traduce y se mantienen en privado. Hay tres tipos de NAT de origen:

- **IP y puerto dinámico (DIPP)**: Permite que múltiples hosts traduzcan sus direcciones IP de origen a la misma dirección IP pública con distintos números de puerto. La traducción dinámica es a la siguiente dirección disponible en el grupo de direcciones NAT, que configura como un grupo de **Dirección traducida** para dirección IP, intervalo de direcciones, subred o combinación de todas.

  Como alternativa al uso de la siguiente dirección en el grupo de direcciones NAT, el DIPP le permite especificar la dirección de la propia **interfaz**. La ventaja de especificar la interfaz de la regla NAT es que la regla NAT se actualizará automáticamente para utilizar cualquier dirección que adquiera la interfaz a continuación. DIPP también se conoce como NAT basada en interfaz o traducción de puertos de direcciones de red (NAPT).

© 2020 Palo Alto Networks, Inc.

DIPP tiene una ratio predeterminada de sobresuscripción NAT, es decir, el número de ocasiones en las que el mismo par de dirección IP y puerto traducido se pueden usar de forma simultánea. Para obtener más información, consulte Sobresuscripción de NAT de IP dinámica y puerto y Modificación de la ratio de sobresuscripción para NAT DIPP.



(Afecta solo a los cortafuegos PA-7000 Series que no usan tarjetas de gestión de conmutadores PA-7050-SMC-B o PA-7080-SMC-B de segunda generación) Cuando use el protocolo de túnel punto a punto (Point-to-Point Tunnel Protocol, PPTP) con NAT DIPP, el cortafuegos se limitará a usar un par de puerto y dirección IP traducidos para una sola conexión; el cortafuegos no es compatible con NAT DIPP. La solución alternativa es actualizar el cortafuegos de PA-7000 Series a una tarjeta SMC-B de segunda generación.

- **IP dinámica**: Permite una traducción dinámica 1 a 1 de una dirección IP de origen únicamente (sin número de puerto) a la siguiente traducción disponible en el grupo de direcciones NAT. El tamaño del grupo de NAT debe ser igual al número de hosts internos que requieren traducciones de red. Por defecto, si el grupo de direcciones de origen es mayor que el de direcciones NAT y en un momento dado se asignan todas las direcciones NAT, se descartan las nuevas conexiones que necesiten una traducción de la dirección. Para anular este comportamiento por defecto, use **Advanced (Dynamic IP/Port Fallback)** para habilitar el uso de direcciones DIPP cuando sea necesario. En cualquiera de los dos casos, a medida que las sesiones terminan y las direcciones en el grupo están disponibles, pueden asignarse para traducir nuevas conexiones.

  NAT de IP dinámica admite la opción de realizar una Reserva de direcciones NAT de IP dinámicas.
- **IP estática**: Permite la traducción estática 1 a 1 de una dirección IP de origen, pero deja el puerto de origen sin modificar. Una situación común en la que se traduce una IP estática es un servidor interno que debe estar disponible en Internet.

NAT de destino

La traducción de direcciones de red (network address translation, NAT) de destino se ejecuta en los paquetes entrantes cuando el cortafuegos traduce una dirección de destino a otra distinta; por ejemplo, traduce una dirección de destino pública a una privada. El NAT de destino también ofrece la opción para realizar reenvío o traducción de puertos.

El NAT de destino permite la traducción estática y dinámica:

- **Static IP (IP estática)**: puede configurar una traducción estática de uno a uno en varios formatos. Puede especificar que el paquete original tenga una dirección IP de destino única, un intervalo de direcciones IP o una máscara de red IP, siempre que el paquete traducido esté en el mismo formato y especifique la misma cantidad de direcciones IP. El cortafuegos traduce estáticamente una dirección de destino original a la misma dirección de destino traducida cada vez. Es decir, si hay más de una dirección de destino, el cortafuegos traduce la primera dirección de destino configurada para el paquete original a la primera dirección de destino configurada para el paquete traducido, y traduce la segunda dirección de destino original configurada a la segunda dirección de destino traducida configurada, y así sucesivamente, y siempre utiliza la misma traducción.

  Si utiliza la NAT de destino para traducir direcciones IPv4 estáticas, también puede recurrir a los servicios de DNS de un lado del cortafuegos para resolver los FQDN de clientes del otro lado. Cuando la respuesta de DNS que contiene la dirección IPv4 atraviesa el cortafuegos, el servidor DNS proporciona una dirección IP interna a un dispositivo externo, o al contrario. Desde PAN-OS 9.0.2 (y en las versiones 9.0 posteriores), puede configurar el cortafuegos para que reescriba la dirección IP de la respuesta de DNS (que coincide con la regla). De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino. El caso de uso de reescritura de DNS aplicable determina cómo se configura.
- **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])**: la NAT de destino permite traducir la dirección de destino original a un host o servidor de destino que tiene una

© 2020 Palo Alto Networks, Inc.

dirección IP dinámica, como un grupo de direcciones o un objeto de dirección que utiliza una máscara de red de IP, un intervalo de IP o un FQDN; cualquiera de ellos puede devolver varias direcciones de DNS. La IP dinámica con distribución de sesiones solo admite direcciones IPv4. La NAT de destino con una dirección IP dinámica resulta de especial utilidad en implementaciones en la nube que utilizan direcciones IP dinámicas.

Si la dirección de destino traducida se resuelve en más de una dirección, el cortafuegos distribuye las sesiones de NAT entrantes entre todas a fin de mejorar el rendimiento. La distribución se basa en alguno de estos métodos: turnos (predeterminado), hash de IP de origen, módulo de IP, hash de IP o menos sesiones. Si el servidor DNS devuelve más de 32 direcciones IPv4 para un FQDN, el cortafuegos utiliza las 32 primeras del paquete.

Si la dirección traducida es un objeto de dirección del tipo FQDN que solo se resuelve en direcciones IPv6, la regla de la política de NAT de destino considera que no se ha resuelto el FQDN.

Utilizar la opción de **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])** le permite traducir varias direcciones IP de destino previas a la NAT *M* a varias direcciones IP de destino posteriores a la NAT *N*. Una traducción de varios a varios implica que puede haber *M* x *N* traducciones de NAT de destino utilizando una regla de NAT.

Para el destino NAT, se recomienda lo siguiente:

- *Utilice la traducción de direcciones IP estáticas para las direcciones IP estáticas. De esa forma, el cortafuegos comprobará que el número de direcciones IP de destino originales sea igual al número de direcciones IP de destino traducidas y se asegurará de ello.*
- *Utilice la traducción de direcciones de IP dinámicas (con distribución de sesiones) solo para direcciones dinámicas basadas en FQDN (el cortafuegos no realiza una comprobación del número de direcciones IP).*

A continuación, se muestran ejemplos comunes de traducciones de NAT de destino que permite el cortafuegos:

Tipo de traducción	Dirección de destino del paquete original	Se asigna a la dirección de destino del paquete traducido	Notas
IP estática	192.168.1.1	2.2.2.2	El paquete original y el paquete traducido tienen una dirección de destino posible.
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	El paquete original y el paquete traducido tienen cuatro direcciones de destino posibles: 192.168.1.1 siempre se asigna a 2.2.2.1 192.168.1.2 siempre se asigna a 2.2.2.2 192.168.1.3 siempre se asigna a 2.2.2.3 192.168.1.4 siempre se asigna a 2.2.2.4

© 2020 Palo Alto Networks, Inc.

Tipo de traducción	Dirección de destino del paquete original	Se asigna a la dirección de destino del paquete traducido	Notas
	192.168.1.1/30	2.2.2.1/30	El paquete original y el paquete traducido tienen cuatro direcciones de destino posibles: 192.168.1.1 siempre se asigna a 2.2.2.1 192.168.1.2 siempre se asigna a 2.2.2.2 192.168.1.3 siempre se asigna a 2.2.2.3 192.168.1.4 siempre se asigna a 2.2.2.4
IP dinámica (con distribución de sesiones)	192.168.1.1/30	domainname.com	El paquete original posee cuatro direcciones de destino y si, por ejemplo, el FQDN en la dirección de destino traducida dirige a cinco direcciones IP, existen 20 posibles traducciones de NAT de destino en una regla de NAT.

Un uso común de la NAT de destino es configurar varias reglas NAT que asignen una dirección de destino pública única a varias direcciones de host de destino privadas a servidores o servicios. En este caso, los números de puerto de destino se usan para identificar a los hosts de destino. Por ejemplo:

- **Reenvío de puertos**: Puede traducir una dirección de destino pública y un número de puerto a una dirección de destino privada, pero mantener el mismo número de puerto.
- **Traducción de puertos**: Puede traducir una dirección de destino pública y un número de puerto a una dirección de destino privada y un número de puerto distinto, con lo que el número de puerto real es privado. La traducción de puertos se configura introduciendo un **Translated Port (Puerto traducido)** en la pestaña **Translated Packet (Paquete traducido)** de la regla de política de NAT. Consulte NAT de destino con ejemplo de traducción de puerto.

Casos de uso de NAT de destino con reescritura de DNS

Cuando utiliza la traducción de direcciones de red (network address translation, NAT) de destino para ejecutar la traducción estática de direcciones IPv4 a otras del mismo tipo, es posible que también esté usando servicios de DNS de un lado del cortafuegos para resolver los FQDN de los clientes. Cuando la respuesta de DNS que contiene la dirección IP atraviesa el cortafuegos para dirigirse al cliente, el cortafuegos no realiza la NAT en esa dirección IP. Por eso, el servidor DNS proporciona una dirección IP interna a un dispositivo externo, o al contrario. En ese caso, el cliente DNS no logra conectar al servicio de destino.

Para evitar ese problema, puede configurar el cortafuegos para que reescriba la dirección IP de la respuesta de DNS (del registro A) basándose en la dirección IP traducida que haya configurado en la regla de la política de NAT. El cortafuegos ejecuta la NAT de la dirección IPv4 (es decir, la resolución del FQDN) incluida en la respuesta de DNS antes de reenviar esta al cliente. De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino. Basta una sola regla de la política de NAT para que el cortafuegos ejecute la NAT en los paquetes que coincidan con ella, así como en las direcciones IP incluidas en las

© 2020 Palo Alto Networks, Inc.

respuestas de DNS que coincidan con la dirección de destino original o la dirección de destino traducida de la regla.

La reescritura de DNS se produce a nivel global; el cortafuegos asigna la dirección de destino en la pestaña Original Packet (Paquete original) a la dirección de destino en la pestaña Translated Packet (Paquete traducido). Todos los demás campos de la pestaña Original Packet (Paquete original) se ignoran. Cuando llega un paquete de respuesta de DNS, el cortafuegos verifica si la respuesta contiene algún registro A que coincida con una de las direcciones de destino asignadas, según la dirección, de la siguiente manera.

Debe especificar cómo el cortafuegos ejecuta NAT en la dirección IP en la respuesta de DNS relacionada con la regla de NAT: **reverse (inverso)** o **forward (directo)**:

- **reverse (inverso)**: si la respuesta de DNS coincide con la dirección de destino **traducida** en la regla, traduzca la respuesta de DNS mediante la traducción inversa que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP **1.1.1.10 a 192.168.1.10**, el cortafuegos reescribe una respuesta de DNS de **192.168.1.10 a 1.1.1.10**.
- **forward (directo)**: si el paquete es una respuesta de DNS que coincide con la dirección de destino **original** en la regla, traduzca la respuesta de DNS mediante la misma traducción que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP **1.1.1.10 a 192.168.1.10**, el cortafuegos reescribe una respuesta de DNS de **1.1.1.10 a 192.168.1.10**.



Si una regla de NAT está superpuesta y tiene deshabilitada la reescritura de DNS y una regla de NAT inferior incluida en la superposición sí la tiene habilitada, el cortafuegos reescribe la respuesta de DNS conforme a la regla de NAT inferior en sentido inverso o directo, según se especifique. Tiene prioridad la reescritura, así que se ignora el orden de las reglas de NAT.

Cuando configure la reescritura de DNS, tenga en cuenta estos casos de uso:

- Casos de uso de NAT de destino con reescritura inversa de DNS
- Casos de uso de NAT de destino con reescritura directa de DNS

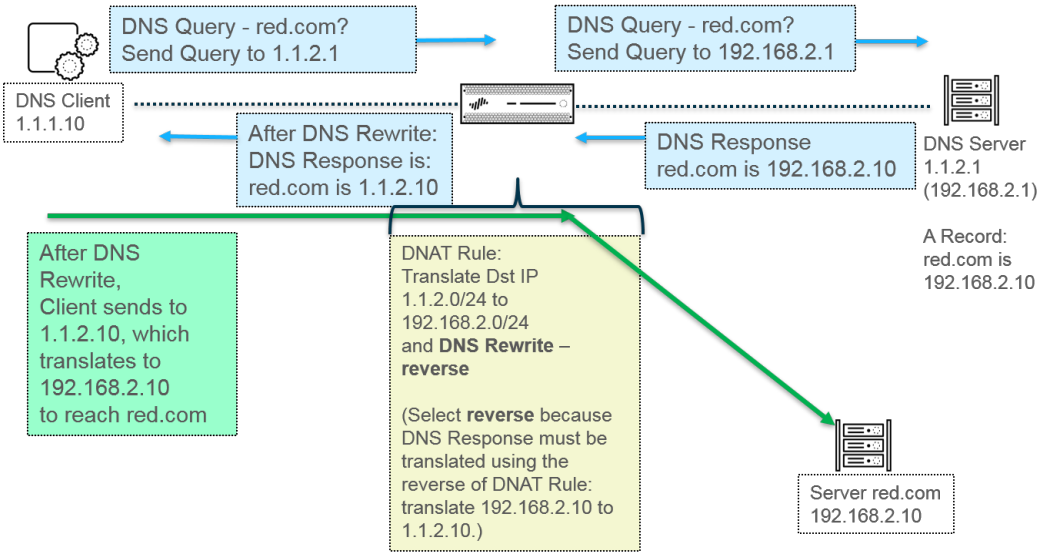
Casos de uso de NAT de destino con reescritura inversa de DNS

En los siguientes casos de uso se ilustra la traducción de direcciones de red (network address translation, NAT) de destino con reescritura de DNS habilitada en sentido **inverso**. La única diferencia entre ambos estriba en si el cliente DNS, el servidor DNS y el servidor de destino están en el lado público o el interno del cortafuegos. La similitud en ambos es que el cliente DNS se encuentra en el lado del cortafuegos opuesto al del servidor de destino último. Si el cliente y ese servidor están en el mismo lado, consulte los casos 3 y 4 de Casos de uso de NAT de destino con reescritura directa de DNS.

En este primer caso de uso, el cliente DNS está en el lado público del cortafuegos, en tanto que el servidor DNS y el servidor de destino último se encuentran en el lado interno. En este caso se necesita la reescritura de DNS en sentido inverso. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla de NAT para traducir la consulta (que se dirigía originalmente a la dirección pública 1.1.2.1) a la dirección interna 192.168.2.1. El servidor DNS responde que red.com tiene la dirección IP 192.168.2.10. Como la regla incluye **Enable DNS Rewrite - reverse (Habilitar reescritura de DNS: [Sentido] inverso)** y la respuesta de DNS 192.168.2.10 coincide con la dirección traducida de destino 192.168.2.0/24 de la regla, el cortafuegos traduce la respuesta de DNS con la traducción **inversa** que emplea la regla. La regla indica que se traduzca 1.1.2.0/24 a 192.168.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 192.168.2.10 a 1.1.2.10. El cliente DNS recibe la respuesta y realiza el envío a 1.1.2.10, que la regla traduce a 192.168.2.10 para acceder al servidor de red.com.

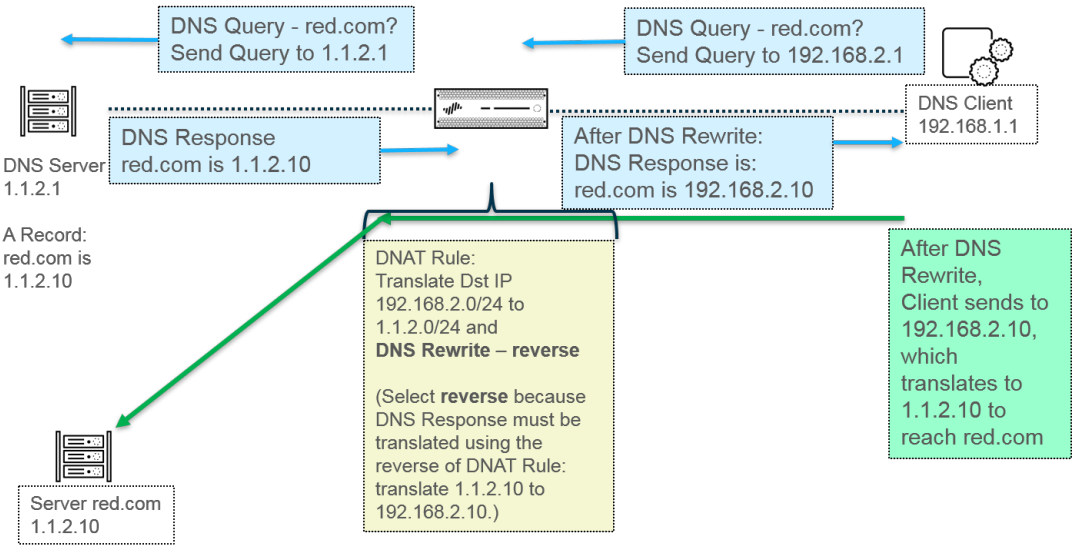
Resumen del caso de uso 1: el cliente DNS y el servidor de destino están en lados opuestos del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino traducida de la regla de NAT, es decir, convierte la respuesta de DNS usando la traducción **inversa** de dicha regla.

© 2020 Palo Alto Networks, Inc.



En este segundo caso de uso, el cliente DNS está en el lado interno del cortafuegos, en tanto que el servidor DNS y el servidor de destino último se encuentran en el lado público. En este caso se necesita la reescritura de DNS en sentido inverso. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla de NAT para traducir la consulta (que se dirigía originalmente a la dirección interna 192.168.2.1) a la dirección pública 1.1.2.1. El servidor DNS responde que red.com tiene la dirección IP 1.1.2.10. Como la regla incluye **Enable DNS Rewrite - reverse (Habilitar reescritura de DNS: [Sentido] inverso)** y la respuesta de DNS 1.1.2.10 coincide con la dirección traducida de destino 1.1.2.0/24 de la regla, el cortafuegos traduce la respuesta de DNS con la traducción **inversa** que emplea la regla. La regla indica que se traduzca 192.168.2.0/24 a 1.1.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 1.1.2.10 a 192.168.2.10. El cliente DNS recibe la respuesta y realiza el envío a 192.168.2.10, que la regla traduce a 1.1.2.10 para acceder al servidor de red.com.

El resumen del caso de uso 2 es idéntico al del caso 1: el cliente DNS y el servidor de destino están en lados opuestos del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino traducida de la regla de NAT, es decir, convierte la respuesta de DNS usando la traducción **inversa** de dicha regla.



Para implementar la reescritura de DNS, realice el procedimiento Configuración de la NAT de destino con reescritura de DNS.

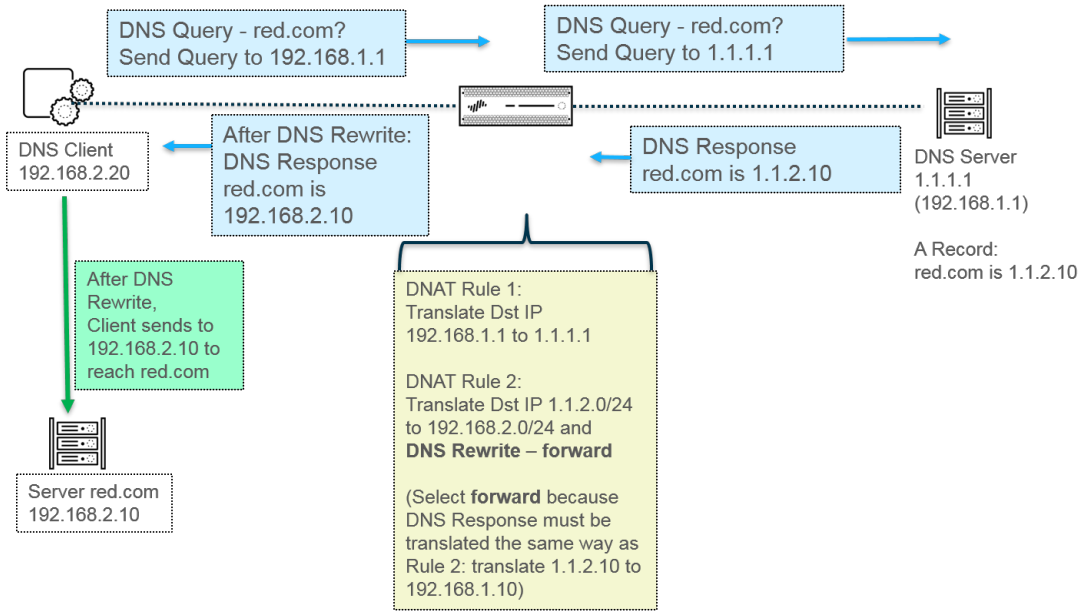
© 2020 Palo Alto Networks, Inc.

Casos de uso de NAT de destino con reescritura directa de DNS

En los siguientes casos de uso se ilustra la traducción de direcciones de red (network address translation, NAT) de destino con reescritura de DNS habilitada en sentido **directo**. La única diferencia entre ambos estriba en si el cliente DNS, el servidor DNS y el servidor de destino están en el lado público o el interno del cortafuegos. La similitud en ambos es que el cliente DNS se encuentra en el mismo lado del cortafuegos que el servidor de destino último. Si el cliente y ese servidor están en lados opuestos, consulte los casos 1 y 2 de Casos de uso de NAT de destino con reescritura inversa de DNS.

En este tercer caso de uso, el cliente DNS y el servidor de destino último están en el lado interno del cortafuegos, en tanto que el servidor DNS se encuentra en el lado público. En este caso se necesita la reescritura de DNS en sentido directo. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla 1 para traducir la consulta (que se dirigía originalmente a la dirección interna 192.168.1.1) a 1.1.1.1. El servidor DNS responde que red.com tiene la dirección IP 1.1.2.10. Como la regla 2 incluye **Enable DNS Rewrite - forward (Habilitar reescritura de DNS: [Sentido] directo)** y la respuesta de DNS 1.1.2.10 coincide con la dirección de destino original 1.1.2.0/24 de la regla 2, el cortafuegos traduce la respuesta de DNS con la **misma** traducción que emplea la regla. La regla 2 indica que se traduzca 1.1.2.0/24 a 192.168.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 1.1.2.10 a 192.168.2.10. El cliente DNS recibe la respuesta y realiza el envío a 192.168.2.10 para acceder al servidor de red.com.

Resumen del caso de uso 3: el cliente DNS y el servidor de destino están en el mismo lado del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino original de la regla de NAT, es decir, convierte la respuesta de DNS usando la misma traducción (**directa**) de dicha regla.

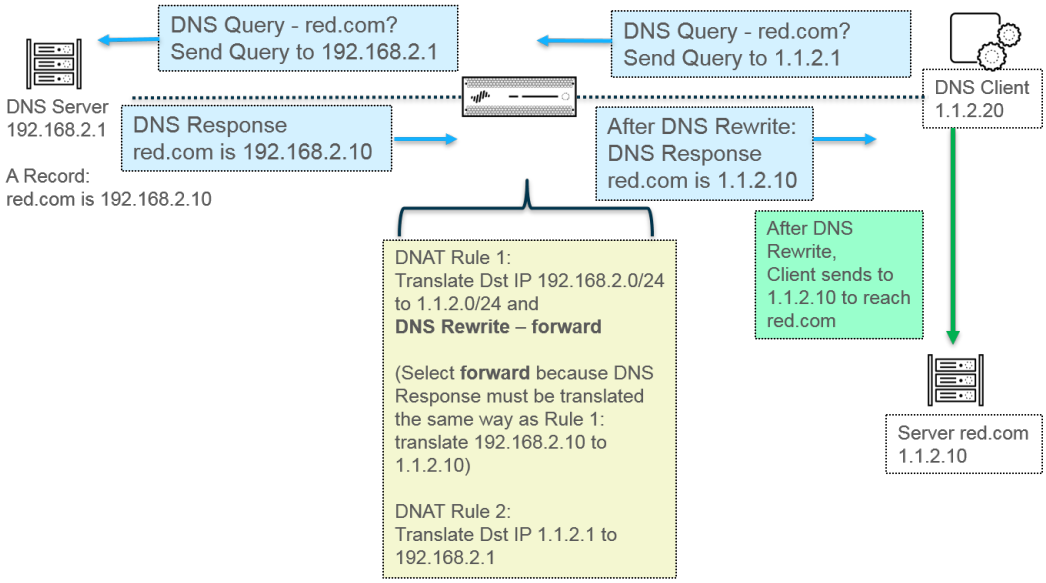


En este cuarto caso de uso, el cliente DNS y el servidor de destino último están en el lado público del cortafuegos, en tanto que el servidor DNS se encuentra en el lado interno. En este caso se necesita la reescritura de DNS en sentido directo. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla 2 para traducir la consulta (que se dirigía originalmente al destino público 1.1.2.1) a 192.168.2.1. El servidor DNS responde que red.com tiene la dirección IP 192.168.2.10. Como la regla 1 incluye **Enable DNS Rewrite - forward (Habilitar reescritura de DNS: [Sentido] directo)** y la respuesta de DNS 192.168.2.10 coincide con la dirección de destino original 192.168.2.0/24 de la regla 1, el cortafuegos traduce la respuesta de DNS con la **misma** traducción que emplea la regla. La regla 1 indica que se traduzca 192.168.2.0/24 a 1.1.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 192.168.2.10 a 1.1.2.10. El cliente DNS recibe la respuesta y realiza el envío a 1.1.2.10 para acceder al servidor de red.com.

El resumen del caso de uso 4 es idéntico al del caso 3: el cliente DNS y el servidor de destino están en el mismo lado del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de

© 2020 Palo Alto Networks, Inc.

destino original de la regla de NAT, es decir, convierte la respuesta de DNS usando la misma traducción (**directa**) de dicha regla.



Para implementar la reescritura de DNS, realice el procedimiento Configuración de la NAT de destino con reescritura de DNS.

Capacidades de regla NAT

La cantidad de reglas NAT permitidas se basan en el modelo del cortafuegos. Los límites de reglas individuales se definen para la NAT de IP dinámica (DIP) e IP dinámica y puerto (DIPP). La suma del número de reglas usadas para estos tipos de NAT no puede superar la capacidad total de reglas NAT. Para DIPP, el límite de reglas se basa en el ajuste de sobresuscripción (8, 4, 2 o 1) del cortafuegos y la suposición de una dirección IP traducida por regla. Para ver los límites de las reglas NAT y los límites de direcciones IP traducidas específicos de cada modelo, utilice la herramienta de Comparación de cortafuegos.

Considere lo siguiente cuando trabaje con reglas NAT:

- Si se queda sin recursos de grupo, no podrá crear más reglas NAT, aunque no se haya alcanzado el recuento máximo de reglas del modelo.
- Si consolida las reglas NAT, el logging e informes se consolidarán también. Las estadísticas se proporcionan por regla, no para todas las direcciones de la regla. Si necesita logging e informes granulares, no combine las reglas.

Sobresuscripción de NAT de IP dinámica y puerto

El NAT de IP dinámica y puerto (DIPP) le permite usar cada par de dirección IP y puerto traducidos varias veces (8, 4 o 2 veces) en sesiones simultáneas. Esta capacidad de reutilización de una dirección IP y puerto (conocida como sobresuscripción) ofrece escalabilidad a los clientes que tengan muy pocas direcciones IP públicas. El diseño se basa en el supuesto de que los hosts se conectan a distintos destinos, por lo que las sesiones pueden identificarse de forma única, con pocas posibilidades de colisiones. En efecto, la ratio de sobresuscripción multiplica el tamaño original del grupo de direcciones/puertos por 8, por 4 o por 2. Por ejemplo, el límite predeterminado de 64 000 sesiones simultáneas, si se multiplica por una ratio de sobresuscripción de 8, da lugar a 512 000 sesiones simultáneas.

Las tasas de sobresuscripción permitidas varían según el modelo. La tasa de sobresuscripción es global y se aplica al cortafuegos. Esta ratio de sobresuscripción se define por defecto y consume memoria, aunque tenga disponibles suficientes direcciones IP públicas para que la sobresuscripción sea innecesaria. Puede reducir la ratio del ajuste predeterminado a uno inferior, o incluso a 1 (que significa sin sobresuscripción). Al

© 2020 Palo Alto Networks, Inc.

configurar una ratio reducida, está reduciendo el número de traducciones de dispositivo de origen posibles, pero aumentando la capacidad de reglas NAT DIP y DIPP. Para cambiar la ratio predeterminada, consulte Modificación de la ratio de sobresuscripción para NAT DIPP.

Si selecciona **Platform Default (Valor predeterminado de plataforma)**, se desactivará su configuración explícita de sobresuscripción y se aplicará el valor predeterminado para el modelo, tal y como se muestra en la siguiente tabla. El ajuste **Valor predeterminado de plataforma** le permite actualizar la licencia de software o cambiar a una menor.

La siguiente tabla muestra la tasa predeterminada (más alta) de sobresuscripción para cada modelo.

Modelo	Ratio de sobresuscripción predeterminada
PA-220	2
PA-820	2
PA-850	2
PA-3220	4
PA-3250	4
PA-3260	4
PA-5220	4
PA-5250	8
PA-5260	8
PA-5280	8
PA-7050	8
PA-7080	8
VM-50	2
VM-100	1
VM-200	1
VM-300	2
VM-500	8
VM-700	8
VM-1000-HV	2

El cortafuegos admite un máximo de 256 direcciones IP traducidas por regla NAT y cada modelo admite una cantidad máxima de direcciones IP traducidas (para todas las reglas NAT combinadas). Si la sobresuscripción provoca que se supere el máximo de direcciones traducidas por regla (256), el cortafuegos reducirá

© 2020 Palo Alto Networks, Inc.

automáticamente la tasa de sobresuscripción en un intento de que funcione la compilación. Sin embargo, si sus reglas NAT generan traducciones que superan el máximo de direcciones traducidas para el modelo, la confirmación fallará.

Estadísticas de memoria NAT de plano de datos

El comando **`show running global-ippool`** muestra estadísticas relacionadas con el consumo de memoria NAT de un grupo. La columna Tamaño muestra el número de bytes de memoria que está usando el grupo de recursos. La columna Tasa muestra la tasa de sobresuscripción (solo para grupos DIPP). Las líneas de grupos y estadísticas de memoria se explican en los siguientes resultados de muestras:

```
admin@PA-7050-HA-0 (active-primary)> show running global-ippool

Idx  Type            From                  To          Num   Ref.Cnt  Size      Ratio
1    Dynamic IP      201.0.0.0-201.0.255.255  210.0.0.0   4096  2        657072    N/A
2    Dynamic IP      202.0.0.0-202.0.0.255    220.0.0.0   256   1        41232     N/A
3    Dynamic IP/Port 200.0.2.100-200.0.2.100  200.0.3.11  1     1        68720       8

Usable NAT DIP/DIPP shared memory size:  58490064      ← Total physical NAT memory (bytes)
Used NAT DIP/DIPP shared memory size:  767024  (1.3%)  ← Bytes and % of usable NAT memory
Dynamic IP NAT Pool:  2 (1.19%)          ← Number of DIP pools in use and % of total usable memory that all  DIP pools use
Dynamic IP/Port NAT Pool:  1 (0.12%)     ← Number of DIPP pools in use and % of total usable memory that all DIPP pools use
```

Para las estadísticas de grupo NAT de un sistema virtual, el comando **`show running ippool`** tiene comandos que indican el tamaño de memoria usado por la regla NAT y la tasa de sobresuscripción usada (para reglas DIPP). La siguiente es una muestra de resultados del comando.

```
admin@PA-7050-HA-0 vsys1 (active-primary)>  show running ippool

VSYS 1 has 4 NAT rules, DIP and DIPP rules:
Rule          Type            Used      Available     Mem Size      Ratio
------------  --------------  -------   ------------  -------------  -------
nat1          Dynamic IP      0         4096            788144         0
nat2          Dynamic IP      0         256              49424         0
nat3          Dynamic IP/Port 0         638976          100976         4
nat11         Dynamic IP      0         4096            788144         0
```

Un campo del resultado del comando **`show running nat-rule-ippool rule`** muestra la memoria (bytes) usada por regla NAT. El siguiente es una ejemplo de resultados del comando con el uso de memoria de la regla rodeado.

```
admin@PA-7050-HA-0 (active-primary)> show running nat-rule-ippool rule nat1

VSYS 1 Rule nat1:
Rule: nat1, Pool index: 1,  memory usage: 788144
-----------------------------------------------------------
Reserve IP: no
201.0.0.0-201.0.255.255  =>
          210.0.0.0-210.0.15.255

Source          Xlat-Source     Ref.Cnt (F)     TTL(s)

Total IPs in use:  0
Total entries in time-reserve cache:  0
Total freelist left:  4096
```

Configuración de NAT

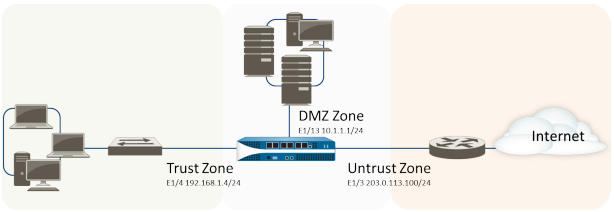
Realice las siguientes tareas para configurar varios aspectos del NAT. Además de los ejemplos siguientes, hay otros en la sección Ejemplos de configuración de NAT.

- Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen)

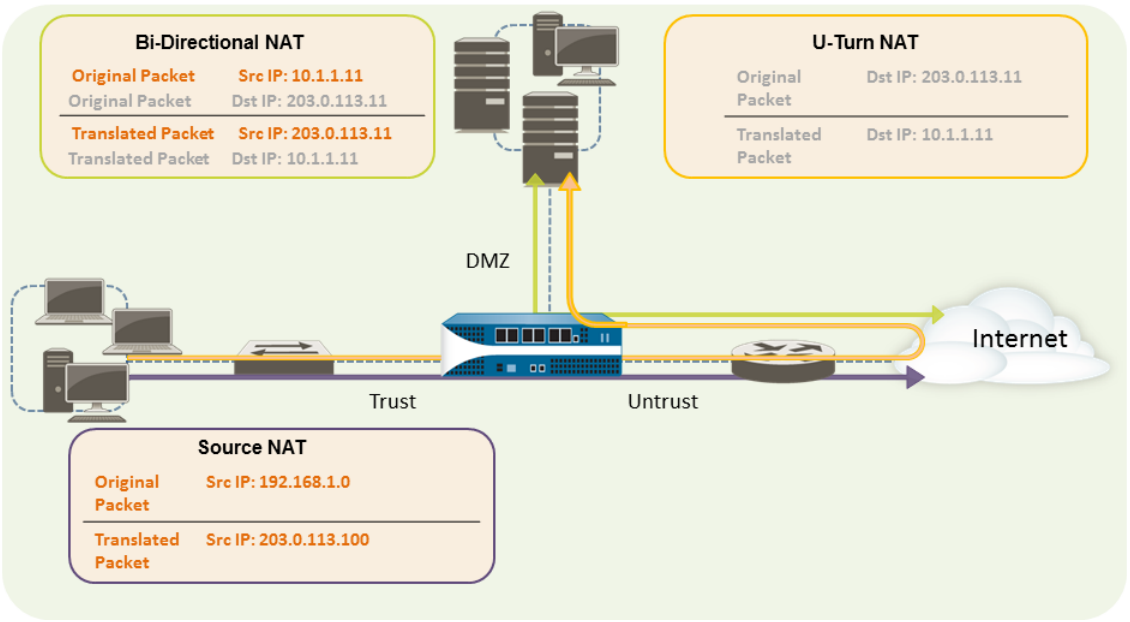
© 2020 Palo Alto Networks, Inc.

- Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino)
- Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática)
- Configuración de la NAT de destino con reescritura de DNS
- Configuración de NAT de destino utilizando direcciones IP dinámicas
- Modificación de la ratio de sobresuscripción para NAT DIPP
- Reserva de direcciones NAT de IP dinámicas
- Deshabilitación de NAT para un host o interfaz específico

Los primeros tres ejemplos de NAT en esta sección se basan en la siguiente topología:



En función de esta topología, se deben crear tres políticas de NAT de la siguiente manera:



- Para permitir que los clientes de la red interna accedan a recursos en Internet, las direcciones 192.168.1.0 internas deberán traducirse a direcciones enrutables públicamente. En este caso, configuraremos NAT de origen (el cuadro y la fecha púrpuras en la imagen anterior) utilizando la dirección de interfaz de salida, 203.0.113.100, como la dirección de origen en todos los paquetes que salgan del cortafuegos desde la zona interna. Consulte Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen) para obtener las instrucciones.
- Para permitir que los clientes de la red interna accedan al servidor web público en la zona DMZ, debemos configurar una regla NAT que redirija el paquete desde la red externa, donde la búsqueda de tabla de enrutamiento original determinará que debe ir, basándose en la dirección de destino de 203.0.113.11 dentro del paquete, a la dirección real del servidor web de la red DMZ de 10.1.1.11. Para ello, deberá crear una regla NAT desde la zona fiable (donde se encuentra la dirección de origen del paquete) hasta la zona no fiable (donde se encuentra la dirección de destino) para traducir la dirección de destino a una dirección de la zona DMZ. Este tipo de NAT de destino se denomina *NAT de ida y vuelta*

© 2020 Palo Alto Networks, Inc.

(el cuadro y la flecha amarillos en la imagen anterior). Consulte Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino) para obtener las instrucciones.

- Para permitir que el servidor web (que tiene tanto una dirección IP privada en la red DMZ como una dirección pública para que accedan usuarios externos) envíe y reciba solicitudes, el cortafuegos debe traducir los paquetes entrantes desde la dirección IP pública hacia la dirección IP privada y los paquetes salientes desde la dirección IP privada hacia la dirección IP pública. En el cortafuegos, puede lograr esto con una única política NAT de origen estática bidireccional (el cuadro y la flecha verdes de la imagen anterior). Consulte Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática).

Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen)

Cuando un cliente de su red interna envía una solicitud, la dirección de origen del paquete contiene la dirección IP del cliente de su red interna. Si utiliza intervalos de direcciones IP privadas, los paquetes del cliente no se podrán enrutar en Internet a menos que traduzca la dirección IP de origen de los paquetes que salen de la red a una dirección enrutable públicamente.

En el cortafuegos, puede realizar esta acción configurando una política NAT de origen que traduzca la dirección de origen (y opcionalmente el puerto) a una dirección pública. Un modo de hacerlo es traducir la dirección de origen de todos los paquetes a la interfaz de salida de su cortafuegos, como se muestra en el procedimiento siguiente.

STEP 1 | Cree un objeto de dirección para la dirección IP externa que tenga la intención de utilizar.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y **Add (Añadir)** para añadir un nombre en **Name (Nombre)** y una descripción opcional en **Description (Descripción)** para el objeto.
2. Seleccione **IP Netmask (Máscara de red de IP)** en **Type (Tipo)** y, a continuación, introduzca la dirección IP de la interfaz externa del cortafuegos (203.0.113.100 en este ejemplo).
3. Haga clic en **OK (Aceptar)**.



Aunque no tiene que utilizar objetos de dirección en sus políticas, es una práctica recomendada porque simplifica la administración al permitirle realizar actualizaciones en un lugar en vez de tener que actualizar cada política donde se hace referencia a la dirección.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la política.
3. (Opcional) Introduzca una etiqueta, que es una palabra clave o frase que le permite ordenar o filtrar políticas.
4. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
5. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
6. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **Dynamic IP And Port (IP y puerto dinámicos)** en la lista **Translation Type (Tipo de traducción)** de la sección Source Address Translation (Traducción de dirección de origen).
7. Para **Address Type**, hay dos opciones. Puede seleccionar **Translated Address** y luego hacer clic en **Add**. Seleccione el objeto de dirección que acaba de crear.

   Un **Address Type (Tipo de dirección)** alternativo es una **Interface Address (Dirección de interfaz)** en la que la dirección traducida será la dirección IP de la interfaz. Para esta opción, debe seleccionar **Interface** y opcionalmente una **IP Address** si la interfaz tiene más de una dirección IP.

© 2020 Palo Alto Networks, Inc.

8. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

STEP 4 | (Opcional) Acceda a la CLI para verificar la traducción.

1. Use el comando **`show session all`** para ver la tabla de sesión, donde puede comprobar el puerto y la dirección IP y el puerto y dirección IP traducidos correspondientes.
2. Use *show session id <id_number>* para ver más detalles acerca de una sesión.
3. Si ha configurado una NAT de IP dinámica, use el comando **`show counter global filter aspect session severity drop | match nat`** para ver si falló alguna sesión debido a la asignación IP NAT. Si todas las direcciones en el grupo NAT de IP dinámica están asignadas cuando debería traducirse una conexión, el paquete será descartado.

Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino)

Cuando un usuario de la red interna envíe una solicitud para acceder al servidor web corporativo en DMZ, el servidor DNS se resolverá en la dirección IP pública. Al procesar la solicitud, el cortafuegos utilizará el destino original del paquete (la dirección IP pública) y enrutará el paquete a la interfaz de salida para la zona no fiable. Para que el cortafuegos sepa que debe traducir la dirección IP pública del servidor web a una dirección de la red DMZ cuando reciba solicitudes de usuarios en la zona fiable, deberá crear una regla NAT de destino que permita al cortafuegos enviar la solicitud a la interfaz de salida para la zona DMZ de la manera siguiente.

STEP 1 | Cree un objeto de dirección para el servidor web.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)** para añadir un **Name (Nombre)** y una **Description (Descripción)** opcional para el objeto.
2. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e introduzca la dirección IP del servidor web, 203.0.113.11 en este ejemplo.

   Puede cambiar el tipo de objeto de dirección de **IP Netmask (Máscara de red IP)** a **FQDN** haciendo clic en **Resolve (Resolver)**, y cuando aparezca el FQDN, haga clic en **Use this FQDN (Utilizar este FQDN)**. De manera alternativa, para **Type (Tipo)**, seleccione **FQDN** e introduzca el FQDN que se utilizará para el objeto de dirección. Si introduce un FQDN y hace clic en **Resolve (Resolver)**, la dirección IP a la que dirige el FQDN aparece en el campo. Para cambiar el **Type (Tipo)** de objeto de dirección de un FQDN a una máscara de red IP utilizando esta dirección IP, haga clic en **Use this address (Utilizar esta dirección)** y el **Type (Tipo)** cambiará a **IP Netmask (Máscara de red IP)** con la dirección IP que aparece en el campo.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la regla NAT.
3. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
4. En la sección **Destination Address (Dirección de destino)**, haga clic en **Add (Añadir)** y seleccione el objeto de dirección que creó para su servidor web público.
5. En la pestaña **Translated Packet (Paquete traducido)**, para Destination Address Translation (Traducción de la dirección de destino), en **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)** e introduzca la dirección IP asignada a la interfaz del servidor web de la red DMZ,

© 2020 Palo Alto Networks, Inc.

10.1.1.11 en este ejemplo. Como alternativa, seleccione **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])** en **Translation Type (Tipo de traducción)** e introduzca en **Translated Address (Dirección traducida)** un objeto de dirección o un grupo de direcciones que utilicen una máscara de red de IP, un intervalo de IP o un FQDN; cualquiera de ellos puede devolver varias direcciones de DNS. Si la dirección de destino traducida se resuelve en más de una dirección, el cortafuegos distribuye las sesiones de NAT entrantes entre todas basándose en uno de los métodos que puede seleccionar: **Round Robin (Turnos)** (predeterminado), **Source IP Hash (Hash de IP de origen)**, **IP Modulo (Módulo de IP)**, **IP Hash (Hash de IP)** o **Least Sessions (Menos sesiones)**.

6. Haga clic en **OK (Aceptar)**.

STEP 3 | Haga clic en **Commit (Confirmar)**.

Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática)

Cuando sus servidores públicos tengan direcciones IP privadas asignadas en el segmento de red en el que se encuentran físicamente, necesitará una regla NAT de origen para traducir la dirección de origen del servidor a la dirección externa en el momento de la salida. Puede crear una regla NAT estática para traducir la dirección de origen interna, 10.1.1.11, a la dirección del servidor web externa, 203.0.113.11 en nuestro ejemplo.

Sin embargo, un servidor orientado al público debe ser capaz de enviar y recibir paquetes. Necesita una política recíproca que traduzca la dirección pública (la dirección IP de destino en paquetes entrantes de usuarios de Internet) a la dirección privada para permitir que el cortafuegos enrute el paquete a su red DMZ. Puede realizar una regla NAT estática bidireccional como se describe en el procedimiento siguiente. La traducción bidireccional es una opción solo para NAT estática.

STEP 1 | Cree un objeto de dirección para la dirección IP interna del servidor web.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y **Add (Añadir)** para añadir un nombre en **Name (Nombre)** y una descripción opcional en **Description (Descripción)** para el objeto.
2. Seleccione **IP Netmask (Máscara de red de IP)** en la lista **Type (Tipo)** e introduzca la dirección IP del servidor web de la red DMZ (10.1.1.11 en este ejemplo).
3. Haga clic en **OK (Aceptar)**.



Si todavía no ha creado un objeto de dirección para la dirección pública de su servidor web, también debería crear ese objeto ahora.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la regla NAT.
3. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la DMZ en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
4. En la sección **Source Address (Dirección de origen)**, haga clic en **Add (Añadir)** y seleccione el objeto de dirección que creó para su dirección de servidor web interno.
5. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **Static IP (IP estática)** en la lista **Translation Type (Tipo de traducción)** de la sección **Source Address Translation (Traducción de dirección de origen)** y, a continuación, seleccione el objeto de dirección que ha creado para la dirección del servidor web externo en la lista **Translated Address (Dirección traducida)**.
6. En el campo **Bi-directional (Bidireccional)**, seleccione **Yes (Sí)**.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Seleccione Confirmar.

© 2020 Palo Alto Networks, Inc.

Haga clic en **Commit (Confirmar)**.

Configuración de la NAT de destino con reescritura de DNS

Cuando configure una regla de política de NAT de destino que realce una traducción estática de direcciones IPv4, también podrá habilitar la reescritura DNS para que el cortafuegos reescriba la dirección IPv4 en una respuesta DNS basada en la dirección IP de destino original y la dirección IP de destino traducida configurada para la regla. El cortafuegos ejecuta la NAT de la dirección IPv4 (es decir, la resolución del FQDN) incluida en la respuesta de DNS (que coincide con la regla) antes de reenviar esta al cliente. De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino.

Consulte los casos de uso de reescritura de DNS para comprender la reescritura DNS y determinar si se debe realizar la reescritura **inversa** o **directa**.

No puede habilitar la traducción de direcciones de origen de tipo Bi-directional (Bidireccional) en la misma regla de NAT en la que haya habilitado la reescritura de DNS.

STEP 1 | Cree una regla de la política de NAT de destino en la que se especifique que el cortafuegos ejecute la traducción estática de las direcciones IPv4 que coincidan con ella y que, además, reescriba las direcciones IP de las respuestas de DNS cuando las direcciones IPv4 (del registro A) coincidan con la dirección de destino original de la regla de NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir una regla de la política de NAT.
2. (Opcional) En la pestaña **General**, introduzca un nombre descriptivo para la regla en **Name (Nombre)**.
3. Para **NAT Type (Tipo de NAT)**, seleccione **ipv4**.
4. En la pestaña **Original Packet (Paquete original)**, **añada** una **dirección de destino**.

   También tendrá que seleccionar una zona de origen o cualquier zona de origen, pero la reescritura de DNS se produce a nivel global; solo coincide la dirección de destino en la pestaña Original Packet (Paquete original). La rescritura DNS ignora todos los demás campos de la pestaña Original Packet (Paquete original).
5. En la sección Destination Address Translation (Traducción de dirección de destino) de la pestaña **Translated Packet (Paquete traducido)**, seleccione **Static IP (IP estática)** en **Translation Type (Tipo de traducción)**.
6. Seleccione una **dirección traducida** o especifique una nueva dirección.
7. Haga clic en **Enable DNS Rewrite (Habilitar reescritura de DNS)** y seleccione uno de estos valores en **Direction (Sentido)**:
   - Seleccione **reverse (inverso)**, que es el valor predeterminado, si la dirección IP de la respuesta de DNS exige la traducción opuesta que se especifica en la regla de NAT. Si la respuesta de DNS coincide con la dirección de destino **traducida** en la regla, traduzca la respuesta de DNS mediante la traducción inversa que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP 1.1.1.10 a 192.168.1.10, el cortafuegos reescribe una respuesta de DNS de 192.168.1.10 a 1.1.1.10.
   - Seleccione **forward (directo)** si la dirección IP de la respuesta de DNS exige la misma traducción que se especifica en la regla de NAT. Si el paquete es una respuesta de DNS que coincide con la dirección de destino **original** en la regla, traduzca la respuesta de DNS mediante la misma traducción que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP 1.1.1.10 a 192.168.1.10, el cortafuegos reescribe una respuesta de DNS de 1.1.1.10 a 192.168.1.10.
8. Haga clic en **OK (Aceptar)**.

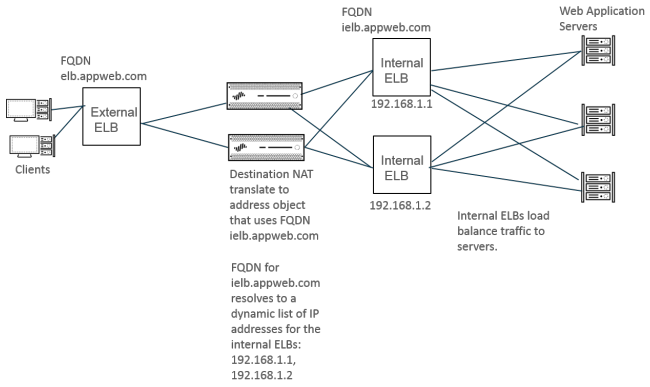
STEP 2 | **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Configuración de NAT de destino utilizando direcciones IP dinámicas

Utilice la NAT de destino para traducir la dirección de destino original a un host o servidor de destino que tiene una dirección IP dinámica y que utiliza un FQDN. Una NAT de destino con una dirección IP dinámica es especialmente útil en implementaciones en la nube que, por lo general, utilizan direcciones IP dinámicas. Cuando el host o el servidor en la nube posee nuevas direcciones IP (dinámico), no debe actualizar manualmente la regla de políticas de NAT realizando consultas continuamente al servidor DNS, ni debe utilizar un componente externo diferente para actualizar el servidor DNS con la asignación de FQDN a la dirección IP más reciente.

En el siguiente ejemplo de topología, los clientes desean comunicarse con los servidores que alojan aplicaciones web en la nube. Un equilibrador de carga elástico (Elastic Load Balancer, ELB) externo se conecta al cortafuegos, que se conecta a los ELB internos que se conectan a los servidores. Con el tiempo, Amazon Web Services (AWS), por ejemplo, añade (y elimina) direcciones IP del FQDN asignado a los ELB internos en función de la demanda de servicio. La flexibilidad utilizar un FQDN para la NAT del ELB interno ayuda a la política a dirigir a direcciones IP diferentes en momentos diferentes, lo que facilita la utilización de NAT de destino debido a que las actualizaciones son dinámicas.



STEP 1 | Cree un objeto de dirección utilizando el FQDN del servidor al que desea traducir la dirección. El objeto de dirección también puede ser una máscara de red de IP o un intervalo de IP.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)** para añadir un objeto de dirección por **Name (Nombre)**, como **`post-NAT-Internal-ELB`**.
2. Seleccione **FQDN** como el **Type (Tipo)** e introduzca el FQDN. En este ejemplo, el FQDN es **`ielb.appweb.com`**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree la política NAT de destino.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir una regla de la política de NAT por **Name (Nombre)** en la pestaña **General**.
2. Seleccione **ipv4** en **NAT Type (Tipo de NAT)**.
3. En la pestaña **Original Packet (Paquete original)**, haga clic en **Add (Añadir)** para añadir la **Source Zone (Zona de origen)** y la **Destination Zone (Zona de destino)**.
4. En la pestaña **Translated Packet (Paquete traducido)**, en la sección Destination Address Translation (Traducción de la dirección de destino), seleccione la **Dynamic IP (with session distribution) (Dirección IP [con distribución de sesiones])** como el **Translation Type (Tipo de traducción)**.
5. En **Translated Address (Dirección traducida)**, seleccione el objeto de dirección que ha creado para el FQDN, la máscara de red de IP o el intervalo de IP. En este ejemplo, el FQDN es **`post-NAT-Internal-ELB`**.
6. En **Session Distribution Method (Método de distribución de sesiones)**, seleccione una de estas opciones:

© 2020 Palo Alto Networks, Inc.

- **Round Robin (Operación por turnos)**: (valor predeterminado) asigna nuevas sesiones a las direcciones IP de forma rotativa. Este método suele ser el adecuado, a menos que exista algún motivo para cambiarlo.
- **Source IP Hash (Hash de IP de origen)**: asigna las sesiones nuevas en función del hash de la dirección IP de origen. Si tiene tráfico proveniente de una única dirección IP de origen, no seleccione Source IP Hash (Hash IP de origen); seleccione un método diferente.
- **IP Modulo (Módulo IP)**: el cortafuegos considera la dirección IP de origen y destino del paquete entrante, realiza una operación XOR y una operación de módulo y el resultado determina a qué dirección IP el cortafuegos asignará las nuevas sesiones.
- **IP Hash (Hash de IP)**: asigna las sesiones nuevas basándose en el hash de las direcciones IP de origen y de destino.
- **Least Sessions (Menos sesiones)**: asigna las sesiones nuevas a la dirección IP que tiene menos sesiones simultáneas. Si tiene numerosas sesiones de corta duración, **Least Sessions (Últimas sesiones)** le proporcionará una distribución más equilibrada de las sesiones.



El cortafuegos no elimina las entradas duplicadas de la lista de direcciones IP de destino antes de distribuir las sesiones entre varias, de modo que las distribuye entre las direcciones duplicadas igual que lo hace entre las únicas. Pueden aparecer direcciones duplicadas en el grupo de traducción si, por ejemplo, la dirección traducida es un grupo de direcciones de objetos de dirección, uno de los cuales es un FQDN que se resuelve en una dirección IP y otro, un intervalo que incluye esa misma dirección.

7. Haga clic en **OK (Aceptar)**.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | (Opcional) Configure la frecuencia con la que el cortafuegos actualiza un FQDN. Consulte Caso de uso 1: el cortafuegos exige la resolución de DNS.

Modificación de la ratio de sobresuscripción para NAT DIPP

Si tiene suficientes direcciones IP públicas y no necesita usar una sobresuscripción de NAT DIPP, puede reducir la ratio de sobresuscripción, consiguiendo así que se permitan más reglas NAT de DIP y DIPP.

STEP 1 | Consulte la ratio de sobresuscripción NAT DIPP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)**. Consulte el ajuste **Ratio de sobresuscripción NAT**.

STEP 2 | Defina la ratio de sobresuscripción NAT DIPP.

1. Modifique la sección Session Settings.
2. En la lista **NAT Oversubscription Rate (Ratio de sobresuscripción a NAT)**, seleccione **1x (1)**, **2x (2)**, **4x (4)** u **8x (8)**, en función de la proporción que le interese.



La configuración Platform Default (Valor predeterminado de plataforma) se aplica a la configuración de sobresuscripción predeterminada para el modelo. Si no desea ninguna sobresuscripción, seleccione 1x.

3. Haga clic en **ACEPTAR** y seleccione **Confirmar** el cambio.

Reserva de direcciones NAT de IP dinámicas

Puede reservar direcciones NAT IP dinámicas (durante un período configurable) para evitar que se asignen como direcciones traducidas a una dirección IP de origen diferente que necesita traducción. Cuando

© 2020 Palo Alto Networks, Inc.

se configura, la reserva se aplica a todas las direcciones IP dinámicas traducidas en curso y a cualquier traducción nueva.

Tanto para traducciones en curso como para nuevas, cuando se traduce una dirección IP de origen a una dirección IP traducida disponible, ese emparejamiento se conserva incluso después de que hayan caducado todas las sesiones relacionadas con esa IP de origen específica. El temporizador de reservas para cada dirección IP de origen se inicia una vez que han caducado todas las sesiones que usen esa traducción de dirección IP de origen. La NAT de IP dinámica es una traducción de uno a uno; una dirección IP de origen se traduce a una dirección IP traducida que se elige dinámicamente entre aquellas direcciones disponibles en el grupo configurado. Por tanto, una dirección IP traducida que esté reservada no estará disponible para ninguna otra dirección IP de origen hasta que caduque la reserva al no haber iniciado una nueva sesión. El temporizador se reinicia cada vez que se inicia una nueva sesión para una asignación de IP de origen/IP traducida, tras un periodo sin sesiones activas.

De manera predeterminada, no hay ninguna dirección reservada. Puede reservar direcciones NAT de IP dinámicas para el cortafuegos o para un sistema virtual.

- Reserve direcciones NAT IP dinámicas para un cortafuegos.

  Introduzca los siguientes comandos:

  ```
  admin@PA-3250# set setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set setting nat reserve-time <1-604800 secs>
  ```

- Reserve direcciones NAT IP dinámicas para un sistema virtual.

  Introduzca los siguientes comandos:

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
  ```

  ```
  admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800 secs>
  ```

  Por ejemplo, supongamos que hay un grupo NAT de IP dinámicas de 30 direcciones y que hay 20 traducciones en curso cuando **nat reserve-time** se establece en 28800 segundos (8 horas). Estas 20 traducciones ahora están reservadas, de modo que cuando expire la última sesión (de cualquier aplicación) que use cada asignación de IP de origen /IP traducida, la dirección IP traducida estará reservada solo para aquella dirección IP de origen durante 8 horas en caso de que la dirección IP de origen necesite de nuevo una traducción. Asimismo, dado que las 10 direcciones traducidas restantes están asignadas, cada una está reservada para su dirección IP de origen, cada una con un temporizador que se inicia cuando expire la última sesión de esa dirección IP de origen.

  De este modo, cada dirección IP de origen puede traducirse repetidas veces en la misma dirección NAT del grupo; no se asignará la dirección IP traducida reservada del grupo a ningún otro host, incluso aunque no haya sesiones activas para esa dirección traducida.

  Supongamos que han caducado todas las sesiones de una asignación IP de origen/IP traducida y que se pone en marcha su temporizador de 8 horas. Si se inicia una nueva sesión, el temporizador se detiene y las sesiones continúan hasta su finalización, momento en el cual el temporizador de reservas se inicia de nuevo para reservar las direcciones traducidas.

  El temporizador de reservas permanece activo en el grupo NAT de IP dinámicas hasta que lo desactive al introducir el comando **set setting nat reserve-ip no** o al cambiar el valor de **nat reserve-time** por un valor diferente.

© 2020 Palo Alto Networks, Inc.

Los comandos de la CLI para reservas no afectan a los grupos de IP y puertos dinámicos (DIPP) o NAT de IP estáticas.

Deshabilitación de NAT para un host o interfaz específico

Tanto las reglas NAT de origen como las NAT de destino se pueden configurar para deshabilitar la traducción de direcciones. Puede haber excepciones en las que no desee que se produzca el NAT para un host una subred o para el tráfico que sale de una interfaz específica. El siguiente procedimiento muestra cómo deshabilitar el NAT para un host.

STEP 1 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir un nombre descriptivo en **Name (Nombre)** para la política.
2. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
3. En **Dirección de origen**, haga clic en **Añadir** e introduzca la dirección del host. Haga clic en **OK (Aceptar)**.
4. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **None (Ninguno)** en la lista **Translation Type (Tipo de traducción)** de la sección Source Address Translation (Traducción de dirección de origen).
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Las reglas de NAT se procesan en orden descendente; ponga la política de excepción antes de otras políticas NAT para garantizar que se procesa antes de que se realice una traducción de dirección de los orígenes que quiere excluir.

Ejemplos de configuración de NAT

- Ejemplos de NAT de destino: asignación de uno a uno
- NAT de destino con ejemplo de traducción de puerto
- Ejemplo de NAT de destino: asignación de uno a uno
- Ejemplo de NAT de origen y destino
- Ejemplo de NAT de origen de Virtual Wire
- Ejemplo de NAT estática de Virtual Wire
- Ejemplo de NAT de destino de Virtual Wire

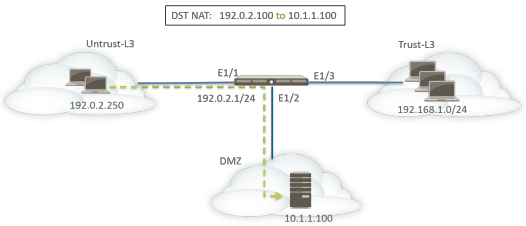
Ejemplos de NAT de destino: asignación de uno a uno

Los errores más frecuentes en la configuración de NAT y de reglas de seguridad se cometen en las referencias a los objetos de direcciones y zonas. Las direcciones usadas en las reglas NAT de destino se refieren siempre a la dirección IP original del paquete (es decir, la dirección pretraducida). La zona de destino de la regla NAT se determina después de la búsqueda de rutas de la dirección IP de destino en el paquete original (es decir, la dirección IP de destino pre-NAT).

Las direcciones en la política de seguridad también hacen referencia a las direcciones IP del paquete origina (es decir, la dirección pre-NAT). Sin embargo, la zona de destino es la zona donde está conectado físicamente el host de destino. Dicho de otro modo, la zona de destino en la regla de seguridad se determina tras la búsqueda de ruta de la dirección IP de destino post-NAT.

© 2020 Palo Alto Networks, Inc.

En el siguiente ejemplo de una asignación uno a uno de NAT de destino, los usuarios de la zona denominada Untrust-L3 acceden al servidor 10.1.1.100 en la zona denominada DMZ usando la dirección IP 192.0.2.100.



Antes de configurar las reglas NAT, tenga en cuenta la secuencia de eventos de esta situación.

- El host 192.0.2.250 envía una solicitud de ARP para la dirección 192.0.2.100 (la dirección pública del servidor de destino).
- El cortafuegos recibe el paquete de solicitud de ARP para el destino 192.0.2.100 en la interfaz Ethernet 1/1 y procesa la solicitud. El cortafuegos responde a la solicitud de ARP con su propia dirección MAC debido a la regla NAT de destino configurada.
- Se evalúan las reglas NAT para buscar coincidencias. Para traducir la dirección IP de destino, debe crearse una regla NAT de destino desde la zona Untrust-L3 a la zona Untrust-L3 para traducir la dirección IP de destino de 192.0.2.100 a 10.1.1.100.
- Tras determinar la dirección traducida, el cortafuegos realiza una búsqueda de ruta para el destino 10.1.1.100 con el fin de determinar la interfaz de salida. En este ejemplo, la interfaz de salida es Ethernet 1/2 en la zona DMZ.
- El cortafuegos realiza una búsqueda de políticas de seguridad para comprobar si se permite el tráfico desde la zona Untrust-L3 a DMZ.

La dirección de la política coincide con la zona de entrada y la zona donde está ubicado físicamente el servidor.

La política de seguridad hace referencia a la dirección IP en el paquete original, que tiene una dirección de destino de 192.0.2.100.

- El cortafuegos reenvía el paquete al servidor que está fuera de la interfaz de salida Ethernet1/2. La dirección de destino se cambia a 10.1.1.100 cuando el paquete abandona el cortafuegos.

Para este ejemplo, los objetos de dirección están configurados para servidor web-privado (10.1.1.100) y servidor web-público (192.0.2.100). La regla NAT configurada sería como esta:

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

La dirección de las reglas NAT se basa en el resultado de la búsqueda de ruta.

La política de seguridad configurada para ofrecer acceso al servidor desde la zona untrust-l3 sería parecida a esta:

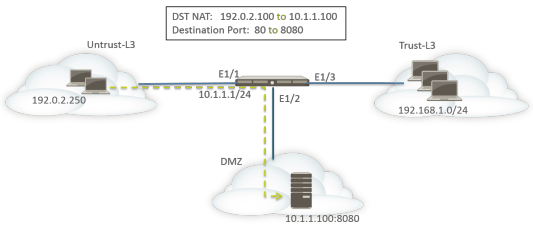
	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

NAT de destino con ejemplo de traducción de puerto

En este ejemplo, el servidor web está configurado para escuchar el tráfico HTTP en el puerto 8080. Los clientes acceden al servidor web usando la dirección IP 192.0.2.100 y el puerto TCP 80. La regla NAT de

© 2020 Palo Alto Networks, Inc.

destino está configurada para traducir tanto la dirección IP como el puerto a 10.1.1.100 y el puerto TCP 8080. Los objetos de dirección están configurados para servidor web-privado (10.1.1.100) y servidor web-público (192.0.2.100).



Deben configurarse en el cortafuegos las siguientes reglas de seguridad y NAT:

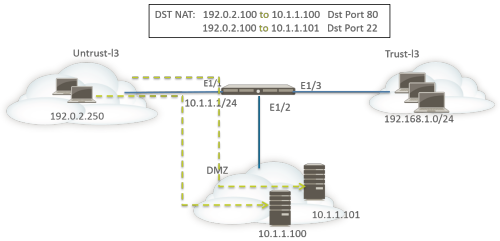
		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

Use el comando de la CLI **`show session all`** para verificar la traducción.

Ejemplo de NAT de destino: asignación de uno a uno

En este ejemplo, la dirección IP se asigna a dos hosts internos distintos. El cortafuegos usa la aplicación para identificar el host interno al que el cortafuegos reenvía el tráfico.



Todo el tráfico HTTP se envía al host 10.1.1.100 y el tráfico SSH se envía al servidor 10.1.1.101. Se requieren los siguientes tipos de perfil:

- Objeto de dirección para una dirección IP pretraducida del servidor
- Objeto de dirección para la dirección IP real del servidor SSH
- Objeto de dirección para la dirección IP real del servidor web

Se crean los objetos de dirección correspondientes:

- Servidores-públicos: 192.0.2.100
- Servidor-SSH: 10.1.1.101
- Servidor web-privado: 10.1.1.100

Las reglas NAT configuradas serían parecidas a esta:

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

© 2020 Palo Alto Networks, Inc.

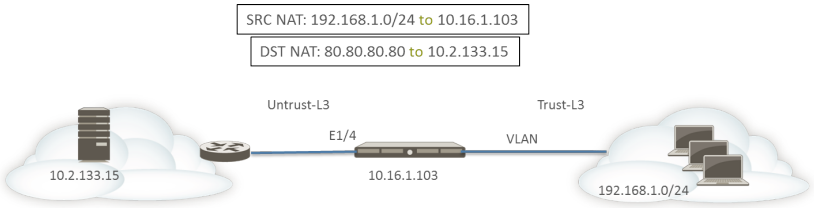
Las reglas de seguridad serían parecidas a esta:

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

Ejemplo de NAT de origen y destino

En este ejemplo, las reglas NAT traducen la dirección IP tanto de origen como de destino de paquetes entre los clientes y el servidor.

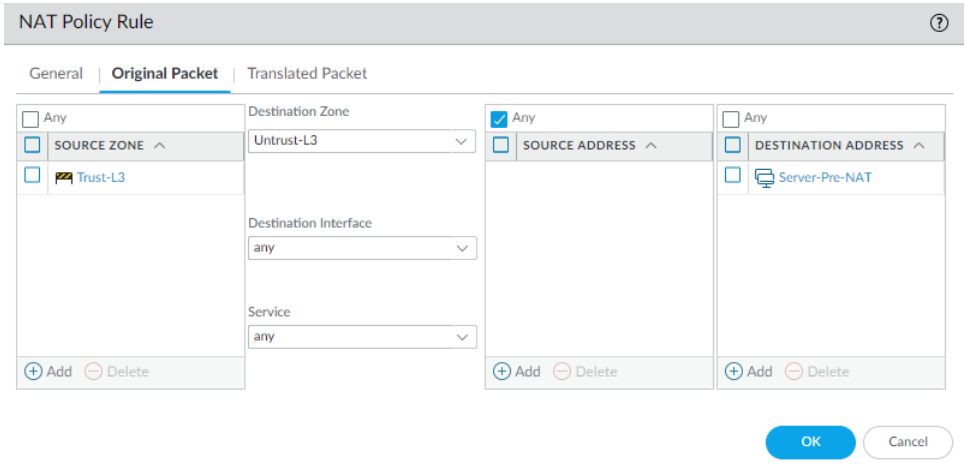
- NAT de origen: las direcciones de origen en los paquetes de los clientes en la zona Trust-L3 hacia el servidor en la zona Untrust-L3 se traducen desde las direcciones privadas de la red 192.168.1.0/24 a la dirección IP de la interfaz de salida en el cortafuegos (10.16.1.103). La traducción de puertos e IP dinámicas hace que los números de puerto también se traduzcan.
- NAT de destino: Las direcciones de destino en los paquetes procedentes de los clientes y dirigidos al servidor se traducen desde la dirección pública del servidor (80.80.80.80) a la dirección privada del servidor (10.2.133.15).



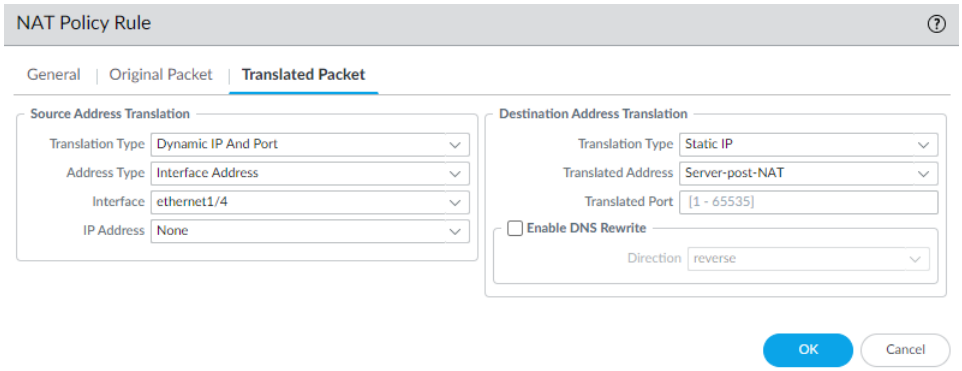
Se crean los siguientes objetos de dirección para la NAT de destino.

- Server-Pre-NAT: 80.80.80.80
- Server-post-NAT: 10.2.133.15

Las capturas de pantalla siguientes ilustran el modo de configurar las políticas NAT de origen y destino del ejemplo.



© 2020 Palo Alto Networks, Inc.



Para verificar las traducciones, use el comando de la CLI **`show session all filter destination 80.80.80.80`**. Una dirección de cliente 192.168.1.11 y su número de puerto se ha traducido a 10.16.1.103 y un número de puerto. La dirección de destino 80.80.80.80 se ha traducido a 10.2.133.15.

Ejemplo de NAT de origen de Virtual Wire

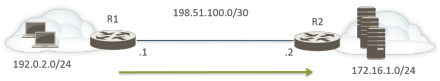
La implementación de Virtual Wire de un cortafuegos Palo Alto Networks cuenta con la ventaja de ofrecer seguridad de forma transparente a los dispositivos de destino. Se puede configurar NAT para interfaces configuradas en un Virtual Wire. Están permitidos todos los tipos de NAT: NAT de origen (IP dinámica, IP y puerto dinámicos, estática) y NAT de destino.

Dado que las interfaces en un Virtual Wire no tienen una dirección IP asignada, no es posible traducir una dirección IP a una dirección IP de interfaz. Debe configurar un grupo de direcciones IP.

Si ejecuta NAT en interfaces de cable virtual, es recomendable que traduzca las direcciones de origen a una subred diferente de la subred con la que se comunican los dispositivos vecinos. El cortafuegos no utilizará ARP proxy para direcciones NAT. Debe configurarse un enrutamiento correcto en los enrutadores anteriores y posteriores para que los paquetes se traduzcan en el modo Virtual Wire. Los dispositivos vecinos solamente podrán resolver solicitudes ARP para direcciones IP que residan en la interfaz del dispositivo en el otro extremo del cable virtual. Consulte ARP proxy para grupos de direcciones NAT para acceder a más explicaciones sobre el ARP proxy.

En el siguiente ejemplo de NAT de origen, las políticas de seguridad (no se muestran) están configuradas desde la zona de cable virtual denominada vw-trust hasta la zona denominada vw-untrust.

En el topología siguiente, hay dos enrutadores configurados para ofrecer conectividad entre las subredes 192.0.2.0/24 y 172.16.1.0/24. El enlace entre los enrutadores está configurado en la subred 198.51.100.0/30. El enrutamiento estático está configurado en ambos enrutadores para establecer conexión entre las redes. Antes de implementar el cortafuegos en el entorno, la topología y la tabla de enrutamiento para cada enrutador son similares a esta:



Ruta en R1:

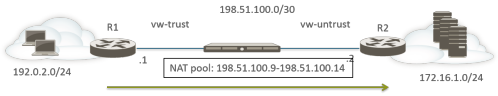
IP Destino	siguiente salto
172.16.1.0/24	198.51.100.2

Ruta en R2:

© 2020 Palo Alto Networks, Inc.

IP Destino	siguiente salto
192.0.2.0/24	198.51.100.1

Ahora el cortafuegos está implementado en modo Virtual Wire entre los dos dispositivos de Capa 3. Se configura en el cortafuegos un grupo de direcciones IP de NAT con el intervalo 198.51.100.9 a 198.51.100.14. Todas las comunicaciones de clientes en la subred 192.0.2.0/24 que acceden a servidores en la red 172.16.1.0/24 llegarán a R2 con una dirección de origen traducida en el intervalo 198.51.100.9 a 198.51.100.14. La respuesta de los servidores se dirigirá a esas direcciones.



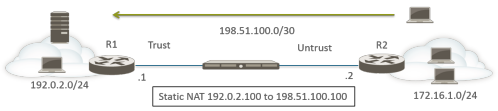
Para que la NAT de origen funcione, debe configurar el enrutamiento adecuado en R2, de modo que los paquetes dirigidos a otras direcciones no sean descartados. La siguiente tabla de enrutamiento muestra la tabla de enrutamiento modificada en R2; la ruta garantiza que el tráfico a los destinos 198.51.100.9 a 198.51.100.14 (es decir, hosts en la subred 198.51.100.8/29) se enviará de vuelta a R1 a través del cortafuegos.

Ruta en R2:

IP Destino	siguiente salto
198.51.100.8/29	198.51.100.1

Ejemplo de NAT estática de Virtual Wire

En este ejemplo, las políticas de seguridad están configuradas desde la zona Virtual Wire denominada Trust hasta la zona de Virtual Wire denominada Untrust. El host 192.0.2.100 se traduce estáticamente a la dirección 198.51.100.100. Con la opción **Bi-directional (Bidireccional)** habilitada, el cortafuegos genera una política NAT desde la zona Untrust hasta la zona Trust. Los clientes en la zona Untrust acceden al servidor usando la dirección IP 198.51.100.100, que el cortafuegos traduce a 198.0.2.100. Cualquier conexión iniciada por el servidor en 192.0.2.100 se traduce a la dirección IP de origen 198.51.100.100.



Ruta en R2:

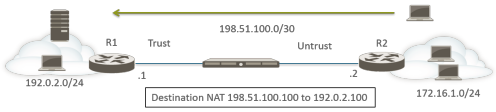
IP Destino	siguiente salto
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

© 2020 Palo Alto Networks, Inc.

Ejemplo de NAT de destino de Virtual Wire

Los clientes de la zona Untrust acceden al servidor usando la dirección IP 198.51.100.100, que el cortafuegos traduce a 192.0.2.100. Tanto la NAT como las políticas de seguridad deben estar configuradas desde la zona Untrust hacia la zona Trust.



Ruta en R2:

IP Destino	siguiente salto
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

© 2020 Palo Alto Networks, Inc.

NPTv6

La traducción de prefijos de red IPv6 a IPv6 (NPTv6) realiza una traducción estática y sin estado de un prefijo IPv6 a otro prefijo IPv6 (los números de puerto no cambian). NPTv6 ofrece cuatro ventajas principales:

- Puede impedir problemas de enrutamiento asimétrico que hacen que las direcciones que no dependen del proveedor se anuncien a varios centros de datos.
- NPTv6 permite anunciar rutas más específicas, de modo que el tráfico de retorno llegue al mismo cortafuegos que lo transmitió.
- Las direcciones privadas y públicas son independientes; puede cambiar una sin que las otras se vean afectadas.
- Tiene la habilidad de traducir Direcciones locales exclusivas a direcciones enrutables globalmente.

Este tema se basa en conocimientos básicos de NAT. Debe estar familiarizado con los conceptos de NAT antes de configurar NPTv6.

- Resumen de NPTv6
- Funcionamiento de NPTv6
- Proxy NDP
- Ejemplo de NPTv6 y Proxy NDP
- Creación de una política NPTv6

Resumen de NPTv6

Esta sección describe la traducción de prefijos de red IPv6 a IPv6 (NPTv6) y el modo de configurarla. NPTv6 se define en RFC 6296. Palo Alto Networks no implementa la funcionalidad completa definida en la RFC, pero la funcionalidad que ha implementado cumple la RFC.

NPTv6 realiza una traducción sin estado de un prefijo IPv6 a otro prefijo IPv6. No tiene estado, lo que implica que no guarda un registro de los puertos o sesiones de las direcciones traducidas. NPTv6 se diferencia de NAT66, que sí tiene estado. Palo Alto Networks admite la traducción de prefijos NPTv6 RFC 6296; no admite NAT66.

Con la limitación de direcciones en el espacio IPv4, la NAT se veía obligada a traducir direcciones IPv4 privadas no enrutables a una o más direcciones IPv4 enrutables a nivel global.

Las organizaciones que usan el direccionamiento IPv6 no necesitan traducir las direcciones IPv6 a direcciones IPv6 gracias a la abundancia de direcciones IPv6. Sin embargo, hay Razones para usar NPTv6 con el fin de traducir prefijos de IPv6 en el cortafuegos.

NPTv6 traduce la parte del prefijo de una dirección IPv6 pero no la parte del host ni los números de puerto de la aplicación. La parte del host simplemente se copia, por lo que permanece igual en ambos lados del cortafuegos. La parte de host también permanece visible del encabezado del paquete.

- NPTv6 no aporta seguridad
- Compatibilidad del modelo con NPTv6
- Direcciones locales exclusivas
- Razones para usar NPTv6

NPTv6 no aporta seguridad

Es importante comprender que NPTv6 no aporta seguridad. En general, la traducción de direcciones de red sin estado no aporta seguridad; solo aporta una función de traducción de direcciones. NPTv6 no oculta ni traduce números de puerto. Debe configurar las políticas de seguridad del cortafuegos correctamente en cada dirección para garantizar que el tráfico se controla del modo deseado.

© 2020 Palo Alto Networks, Inc.

Compatibilidad del modelo con NPTv6

NPTv6 es compatible con los siguientes modelos (NPTv6 con búsqueda de hardware, paquetes a través de la CPU): Cortafuegos PA-7000 Series, PA-5200 Series, PA-800 y PA-220. Los modelos VM-Series son compatibles, pero no pueden hacer que el hardware realice una búsqueda de sesión.

Direcciones locales exclusivas

RFC 4193, Direcciones IPv6 de unidifusión locales únicas, define direcciones locales únicas (ULA, Unique Local Address), que son direcciones IPv6 de unidifusión. Se pueden considerar equivalentes IPv6 de las direcciones IPv4 privadas identificadas en RFC 1918, Asignación de direcciones para Internet privadas, que no se pueden enrutar globalmente.

Una ULA es única a nivel internacional, pero no es de esperar que se pueda enrutar globalmente. Su uso está previsto para comunicaciones locales y para ser enrutable en un área limitada, como un sitio o entre un número pequeño de sitios. Palo Alto Networks no recomienda asignar ULA, pero un cortafuegos configurado con NPTv6 traducirá los prefijos que se le envíen, incluidas las ULA.

Razones para usar NPTv6

Aunque no hay escasez de direcciones IPv6 enrutables globalmente, hay varias razones para traducir las direcciones IPv6. NPTv6:

- **Evita el enrutamiento asimétrico**: se puede producir enrutamiento asimétrico si varios centros de datos anuncian en Internet global un espacio de dirección que no depende del proveedor (/48, por ejemplo). Al usar NPTv6, puede anunciar rutas más específicas desde cortafuegos regionales, y el tráfico de retorno llegará al mismo cortafuegos en el que se tradujo la dirección IP de origen.
- **Proporciona independencia de direcciones**: No es necesario que cambie los prefijos IPv6 usados dentro de su red local tras un cambio de los prefijos globales (realizado, por ejemplo, por el proveedor de servicios de Internet o como resultado de una fusión de organizaciones). Por el contrario, puede cambiar las direcciones interiores discrecionalmente sin interrumpir las direcciones usadas para acceder a los servicios en la red privada desde Internet. En cada caso, debe actualizar una regla NAT en lugar de reasignar las direcciones de red.
- **Traduce ULA para enrutamiento**: tiene Direcciones locales exclusivas asignadas dentro de su red privada, y puede hacer que el cortafuegos las traduzca a direcciones enrutables globalmente. Por lo tanto, puede disfrutar tanto de direccionamiento privado como de direcciones traducidas enrutables.
- **Reduce la exposición a prefijos IPv6**: Los prefijos IPv6 están menos expuestos que si no traduce los prefijos de red; sin embargo, NPTv6 no es una medida de seguridad. La parte del identificador de interfaz de cada dirección IPv6 no se traduce; permanece igual en cada lado del cortafuegos, y visible para cualquiera que pueda ver el encabezado del paquete. Asimismo, los prefijos no son seguros; pueden ser determinados por otros.

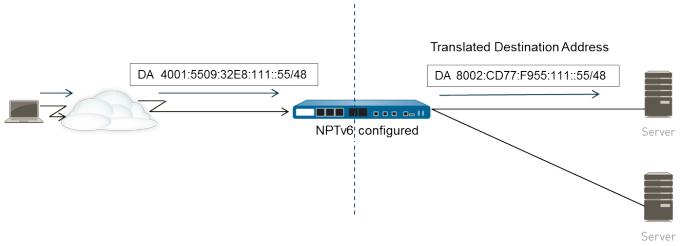
Funcionamiento de NPTv6

Cuando configura una política NPTv6, el cortafuegos de Palo Alto Networks realiza una traducción de IPv6 uno a uno estática en ambas direcciones. La traducción está basada en el algoritmo descrito en RFC 6296.

En un caso de uso, el cortafuegos que realiza NPTv6 se encuentra entre una red interna y una externa (como Internet) que usa prefijos enrutables globalmente. Cuando los datagramas van en dirección de salida, el prefijo de origen interno se sustituye por un prefijo externo, lo que se conoce como traducción de origen.

En otro caso de uso, cuando los datagramas van en dirección de entrada, se sustituye el prefijo se sustituye por el prefijo interno, lo que se conoce como traducción de destino. La siguiente figura ilustra la traducción de destino y una característica de NPTv6: solo se traduce la parte del prefijo de una dirección IPv6. La parte del host de la traducción no se traduce y permanece en el mismo lado del cortafuegos. En la siguiente figura, el identificador del host es 111::55 a ambos lados del cortafuegos.

© 2020 Palo Alto Networks, Inc.



Es importante comprender que NPTv6 no aporta seguridad. Al planificar sus políticas NAT NPTv6, recuerde también configurar las políticas de seguridad en cada dirección.

Una regla de políticas NAT o NPTv6 no puede tener las dos direcciones (origen y destino) configuradas en Cualquiera.

En un entorno en el que quiera traducción de prefijos IPv6, se combinan tres funciones del cortafuegos: Políticas NAT NPTv6, políticas de seguridad y Proxy NDP.

El cortafuegos no traduce lo siguiente:

- Las direcciones que el cortafuegos tiene en su caché de Detección de vecinos (ND, Neighbor Discovery).
- La subred 0xFFFF (de acuerdo con RFC 6296, Apéndice B).
- Direcciones de multidifusión IP.
- Direcciones IPv6 con una longitud de prefijo de /31 o inferior.
- Direcciones locales de vínculo Si el cortafuegos está funcionando en el modo Virtual Wire, no hay direcciones IP que traducir, y el cortafuegos no traduce direcciones locales de vínculo.
- Direcciones de sesiones para TCP que autentican peers usando la opción de autenticación TCP (RFC 5925).

Al usar NPTv6, el rendimiento del tráfico de método rápido se ve afectado porque NPTv6 se realiza en el método lento.

NPTv6 funcionará con IPSec IPv6 solo si el cortafuegos se origina y termina en el túnel. El tráfico de tránsito IPSec fallaría porque la dirección IPv6 de origen o destino se modificaría. Una técnica NAT transversal que encapsulara el paquete permitiría a IPSec IPv6 trabajar con NPTv6.

- Asignación neutral de suma de comprobación
- Traducción bidireccional
- NPTv6 aplicada a un servicio específico

Asignación neutral de suma de comprobación

Las traducciones de asignaciones NPTv6 que realiza el cortafuegos son neutrales de suma de comprobación, lo que significa que "... dan como resultado encabezados IP que generarán la misma suma de comprobación de pseudoencabezado IPv6 cuando se calcule la suma de comprobación usando el algoritmo de suma de comprobación de Internet estándar [RFC 1071]." Consulte RFC 6296, Sección 2.6, para obtener más información acerca de la asignación neutral de suma de comprobación.

Si usa NPTv6 para realizar la NAT de destino, puede ofrecer la dirección de IPv6 interna y de la longitud de prefijo/prefijo externa de la interfaz del cortafuegos en la sintaxis del comando **`test nptv6`** de la CLI. La CLI responde con una dirección de IPv6 pública neutral de suma de comprobación que se usa en su configuración NPTv6 para alcanzar ese destino.

Traducción bidireccional

Con Creación de una política NPTv6, la opción **Bi-directional (Bidireccional)** en la pestaña **Translated Packet (Paquete traducido)** le ofrece una forma cómoda de hacer que el cortafuegos cree una NAT correspondiente o una traducción de NPTv6 en la dirección contraria a la traducción que ha configurado. Por defecto, la traducción **Bi- directional** está deshabilitada.

© 2020 Palo Alto Networks, Inc.

Si habilita la traducción bidireccional, es extremadamente importante asegurarse de tener establecidas políticas de seguridad para controlar el tráfico en ambas direcciones. Sin dichas políticas, la función Bi-directional permitirá la traducción automática de paquetes en ambas direcciones, algo que quizás no desee.

NPTv6 aplicada a un servicio específico

La implementación de Palo Alto Networks de NPTv6 ofrece la capacidad de filtrar paquetes para limitar qué paquetes están sujetos a traducción. Recuerde que NPTv6 no realiza traducción de puertos. No existe el concepto de traducción de IP y puertos dinámicos (DIPP) porque NPTv6 solo traduce prefijos IPv6. Sin embargo, puede especificar que solo se realice traducción NPTv6 de los paquetes de un cierto puerto de servicios. Para ello, realice la Creación de una política NPTv6 que especifique un **Service (Servicio)** en el paquete original.

Proxy NDP

El protocolo de detección de vecinos (NDP) para IPv6 realiza funciones similares a las que ofrece el protocolo de resolución de direcciones (ARP) para IPv4. RFC 4861 define la detección de vecinos para IP versión 6 (IPv6). Hosts, enrutadores y cortafuegos usan NDP para determinar las direcciones de capa de enlace de los vecinos en enlaces conectados, llevar un seguimiento de los vecinos con los que se puede contactar y actualizar las direcciones de capa de enlace de los vecinos que han cambiado. Los peers anuncian sus propias direcciones MAC y su dirección IPv6, y solicitan además direcciones de los peers.

NDP también es compatible con el concepto de *proxy*, cuando un nodo tiene un dispositivo vecino que es capaz de reenviar paquetes en nombre del nodo. El dispositivo (cortafuegos) actúa como Proxy NDP.

Los cortafuegos de Palo Alto Networks son compatibles con NDP y Proxy NDP en sus interfaces. Al configurar el cortafuegos para que actúe como un Proxy NDP para direcciones, este puede enviar anuncios de detección de vecinos (ND) y responder a solicitudes de ND de peers que están solicitando direcciones MAC de prefijos IPv6 asignados a dispositivos tras el cortafuegos. También puede configurar direcciones para las que el cortafuegos no responderá a solicitudes de proxy (direcciones negadas).

De hecho, NDP está habilitado de manera predeterminada, y necesita configurar Proxy NDP al configurar NPTv6 por estos motivos:

- NPTv6 no tiene estado, por lo que necesita un modo de indicar al cortafuegos que responda a paquetes de ND enviados a direcciones de Proxy NDP especificadas, y que no responda a direcciones Proxy NDP negadas.

  Se recomienda que niegue las direcciones de sus vecinos en la configuración de Proxy NDP, ya que Proxy NDP indica que el cortafuegos contactará con esas direcciones tras el cortafuegos, pero los vecinos no están tras el cortafuegos.
- NDP hace que el cortafuegos guarde las direcciones MAC y las direcciones IPv6 de los vecinos en su caché de ND. (Consulte la figura en Ejemplo de NPTv6 y Proxy NDP). El cortafuegos no realiza traducción NPTv6 de direcciones que encuentra en la caché de ND porque provocaría un conflicto. Si la parte del host de una dirección en la memoria caché coincide con la parte del host de la dirección de un vecino, y el prefijo en la caché se traduce al mismo prefijo que el del vecino (porque la interfaz de salida del cortafuegos pertenece a la misma subred del vecino), tendrá una dirección traducida exactamente igual que la dirección IPv6 legítima del vecino, lo que provoca un conflicto. (Si se intenta realizar una traducción NPTv6 en una dirección en la memoria caché de ND, un mensaje de syslog informativo registra el evento: `NPTv6 Translation Failed`).

Cuando una interfaz con proxy NDP habilitado recibe una solicitud de ND en la que le pide una dirección MAC para una dirección IPv6, se produce la secuencia siguiente:

- ☐ El cortafuegos busca en la memoria caché de ND para asegurarse de que no está ahí la dirección IPv6 de la solicitud. Si la dirección está ahí, el cortafuegos ignora la solicitud ND.

© 2020 Palo Alto Networks, Inc.

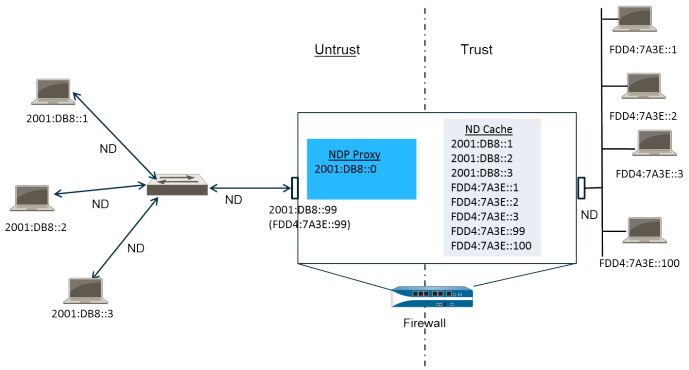
- Si la dirección IPv6 es 0, significa que el paquete es un paquete de detección de dirección duplicada, y el cortafuegos ignora la solicitud de ND.
- El cortafuegos realiza una búsqueda de la coincidencia de prefijo más larga de las direcciones de Proxy NDP y encuentra la mejor coincidencia de la dirección en la solicitud. Si el campo Negar de la coincidencia está marcado (en la lista Proxy NDP), el cortafuegos descarta la solicitud de ND.
- Solo si la coincidencia de prefijo más larga busca coincidencias, y si la dirección coincidente no está negada, el Proxy NDP responderá a la solicitud de ND. El cortafuegos responde con un paquete ND, proporcionando su propia dirección MAC como dirección MAC del siguiente salto hacia el destino consultado.

Para una correcta compatibilidad con NDP, el cortafuegos no realiza Proxy NDP para lo siguiente:

- Detección de direcciones duplicadas (DAD)
- Direcciones en la caché de ND (dado que tales direcciones no pertenecen al cortafuegos; pertenecen a los vecinos detectados).

Ejemplo de NPTv6 y Proxy NDP

La siguiente figura ilustra cómo funcionan juntos NPTv6 y Proxy NDP.



- Caché de ND en el ejemplo de NPTv6
- Proxy ND en el ejemplo de NPTv6
- La traducción NPTv6 en el ejemplo de NPTv6
- Los vecinos en caché ND no se traducen

Caché de ND en el ejemplo de NPTv6

En el ejemplo anterior, varios peers conectan con el cortafuegos a través de un conmutador, y la ND se produce entre los peers y el conmutador, entre el conmutador y el cortafuegos y el cortafuegos y los dispositivos en el lado de confianza.

Cuando el cortafuegos detecta peers, guarda sus direcciones en su caché de ND. Los peers de confianza FDDA:7A3E::1, FDDA:7A3E::2 y FDDA:7A3E::3 se conectan al cortafuegos por el lado de confianza. FDDA:7A3E::99 es la dirección no traducida del propio cortafuegos; su dirección pública es 2001:DB8::99. Las direcciones de los peers en el lado no fiable se han detectado y aparecen en la caché de ND: 2001:DB8::1, 2001:DB8::2 y 2001:DB8::3.

Proxy ND en el ejemplo de NPTv6

En nuestro escenario, queremos que el cortafuegos actué como un Proxy NDP para los prefijos tras el cortafuegos. Cuando el cortafuegos es un Proxy NDP para un conjunto especificado de direcciones/intervalos/prefijos y ve una dirección de este intervalo en un anuncio o solicitud de ND, el cortafuegos responde siempre que no responda antes un dispositivo con esta dirección específica, la dirección no esté negada en la configuración de Proxy NDP y la dirección no esté en la caché ND. El cortafuegos realiza la

© 2020 Palo Alto Networks, Inc.

traducción del prefijo (descrita más abajo) y envía el paquete al lado fiable, donde esa dirección puede estar asignada o no a un dispositivo.

En este ejemplo, la tabla de Proxy ND contiene la dirección de red 2001:DB8::0. Cuando la interfaz ve una ND para 2001:DB8::100, ningún otro dispositivo en el conmutador L2 reclama el paquete, de modo que el intervalo de proxy hace que el cortafuegos no reclame, y tras la traducción a FDD4:7A3E::100, el cortafuegos lo envía a la zona fiable.

La traducción NPTv6 en el ejemplo de NPTv6

En este ejemplo, el **Original Packet** está configurado con una **Source Address** de FDD4:7A3E::0 y un **Destination** de **Any**. El **Translated Packet** está configurado con la **Translated Address** de 2001:DB8::0.

Por lo tanto, los paquetes salientes con un origen FDD4:7A3E::0 se traducen a 2001:DB8::0. Los paquetes entrantes con un prefijo de destino en la red 2001:DB8::0 se traducen a FDD4:7A3E::0.

Los vecinos en caché ND no se traducen

En nuestro ejemplo, hay hosts tras el cortafuegos con identificadores de host :1, :2 y :3. Si los prefijos de aquellos hosts están traducidos a un prefijo que existe más allá del cortafuegos, y si esos dispositivos no tienen identificadores de host :1, :2 y :3 (ya que la parte del identificador de host de la dirección permanece inalterada), la dirección traducida resultante pertenecería al dispositivo existente, y se produciría un conflicto de dirección. Para evitar un conflicto con identificadores de host coincidentes, NPTv6 no traduce direcciones que encuentra en la caché de ND.

Creación de una política NPTv6

Realice esta tarea cuando quiera configurar una política NPTv6 de NAT para traducir un prefijo IPv6 a otro prefijo IPv6. Los requisitos previos de esta tarea son:

- Habilite IPv6. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)**. Haga clic en **Edit** y seleccione **IPv6 Firewalling**.
- Configure una interfaz Ethernet de capa 3 con una dirección IPv6 válida y con IPv6 habilitado. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**, seleccione una interfaz y en la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
- Cree políticas de seguridad de red, ya que NPTv6 no proporciona seguridad.
- Decida si quiere traducción de origen, de destino o ambas.
- Identifique las zonas a las que quiere aplicar la política NPTv6.
- Identifique sus prefijos IPv6 originales y traducidos.

STEP 1 | Cree una política NPTv6.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un nombre descriptivo en **Name (Nombre)** para la regla de política de NPTv6.
3. (Opcional) Introduzca una **Description (Descripción)** y **Tag (Etiqueta)**.
4. Para **NAT Type (Tipo de NAT)**, seleccione **NPTv6**.

STEP 2 | Especifique los criterios de coincidencia para los paquetes entrantes; los paquetes que coinciden en todos los criterios están sujetos a la traducción de NPTv6.

Las zonas son necesarias para ambos tipos de traducción.

1. En la pestaña **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, deje **Any (Cualquiera)** o haga clic en **Add (Añadir)** para introducir la zona de origen a la que se aplica la política.
2. Introduzca la **Destination Zone (Zona de destino)** a la que se aplica la política.

© 2020 Palo Alto Networks, Inc.

3. (Opcional) Seleccione una **Destination Interface**.
4. (Opcional) Seleccione un **Service (Servicio)** para restringir los tipos de paquetes que se traducen.
5. Si está realizando una traducción de origen, introduzca una **Source Address (Dirección de origen)** o seleccione **Any (Cualquiera)**. Esta dirección puede ser un objeto de dirección. Se aplican las siguientes restricciones a la **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)**:
   - Los prefijos de **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)** para **Original Packet (Paquete original)** y **Translated Packet (Paquete traducido)** deben tener el formato xxxx:xxxx::/yy, aunque los ceros de inicio en el prefijo se pueden omitir.
   - La dirección IPv6 no puede tener definida una parte de identificador de interfaz (host).
   - El intervalo admitido de longitudes de prefijo es de /32 a /64.
   - No es posible definir tanto la **Source Address** como la **Destination Address** en **Any**.
6. Si está realizando la traducción de origen, tiene la opción de introducir una **Destination Address**. Si está realizando una traducción de destino, la **Destination Address (Dirección de destino)** es obligatoria. La dirección de destino (se permite un objeto de dirección) debe ser una máscara de red, no solo una dirección IPv6 y no un intervalo. La extensión del prefijo debe ser un valor desde /32 hasta /64, inclusive. Por ejemplo, 2001:db8::/32.

STEP 3 | Especifique el paquete traducido.

1. En la pestaña **Translated Packet**, si desea realizar la traducción de origen, en la sección Source Address Translation, para el **Translation Type**, seleccione **Static IP**. Si no desea realizar traducción de origen, seleccione **None**.
2. Si ha elegido **Static IP**, se muestra el campo **Translated Address**. Introduzca el objeto de dirección o el prefijo IPv6 traducido. Consulte las restricciones enumeradas en el paso anterior.

   Se recomienda configurar su Translated Address para que sea el prefijo de la dirección de interfaz no fiable de su cortafuegos. Por ejemplo, si su interfaz no fiable tiene la dirección 2001:1a:1b:1::99/64, configure su Translated Address (Dirección traducida) como 2001:1a:1b:1::0/64.
3. (Opcional) Seleccione **Bi-directional (Bidireccional)** si desea que el cortafuegos cree una traducción NPTv6 correspondiente en la dirección opuesta de la traducción que configure.

   Si habilita la traducción Bi-directional, es muy importante asegurarse de tener establecidas políticas de seguridad para controlar el tráfico en ambas direcciones. Sin dichas reglas de política, la traducción Bi-directional permitirá la traducción automática de paquetes en ambas direcciones, algo que quizás no desee.
4. Si desea realizar una traducción de destino, seleccione **Destination Address Translation (Traducción de dirección de destino)**. En el campo **Translated Address (Dirección traducida)**, seleccione un objeto de dirección o introduzca la dirección de destino interna.
5. Haga clic en **OK (Aceptar)**.

STEP 4 | Configuración del NDP Proxy.

Al configurar el cortafuegos para que actúe como un Proxy NDP para direcciones, este puede enviar anuncios de detección de vecinos (ND) y responder a solicitudes de ND de peers que están solicitando direcciones MAC de prefijos IPv6 asignados a dispositivos tras el cortafuegos.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz.
2. En la pestaña **Advanced (Avanzado)** > **NDP Proxy**, seleccione **Enable NDP Proxy (Habilitar proxy NDP)** y haga clic en **Add (Añadir)**.
3. Introduzca las **IP Address(es)** para las que está habilitado Proxy NDP. Puede ser una dirección, un intervalo de direcciones o un prefijo y longitud de prefijo. El orden de las direcciones IP es indiferente. Lo idóneo es que estas direcciones sean las mismas que las direcciones traducidas que ha configurado en una política NPTv6.

© 2020 Palo Alto Networks, Inc.



Si la dirección es una subred, el Proxy NDP responderá a todas las direcciones en la subred, de modo que deberá enumerar los vecinos en la subred con Negate (Negar) seleccionado, como se describe en el siguiente paso.

4. (Opcional) Introduzca una o más direcciones para las que no desea habilitar Proxy NDP, y seleccione **Negate (Negar)**. Por ejemplo, desde un intervalo de dirección IP o intervalo de prefijos configurado en el paso anterior, puede negar un subconjunto pequeño de direcciones. Se recomienda negar las direcciones de los vecinos del cortafuegos.

STEP 5 | Confirme la configuración.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

NAT64

NAT64 proporciona una manera de pasar a IPv6 cuando sigue necesitando comunicarse con redes IPv4. Cuando debe comunicarse desde una red solo IPv6 a una red IPv4, utiliza NAT64 para traducir direcciones de origen y de destino desde IPv6 a IPv4 y viceversa. NAT64 permite que los clientes de IPv6 accedan a servidores IPv4; y que los clientes de IPv4 accedan a servidores IPv6. Debe comprender NAT antes de configurar NAT64.

- Descripción general de NAT64
- Dirección IPv6 integrada en la dirección IPv4
- Servidor DNS64
- Detección de MTU de ruta
- Comunicación de Pv6 iniciada
- Configuración de NAT64 para la comunicación iniciada por IPv6
- Configuración de NAT64 para la comunicación iniciada por IPv4
- Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto

Descripción general de NAT64

Puede configurar dos tipos de traducción NAT64 en un cortafuegos Palo Alto Networks; cada uno realiza una traducción bidireccional entre dos familias de direcciones IP:

- El cortafuegos admite NAT64 con estado para la Comunicación de Pv6 iniciada, que asigna varias direcciones IPv6 a una dirección IPv4, además de conservar las direcciones IPv4. (No admite NAT64 sin estado, que asigna una dirección IPv6 a una dirección IPv4, y, por lo tanto, no conserva las direcciones IPv4). Configuración de NAT64 para la comunicación iniciada por IPv6.
- El cortafuegos admite la comunicación de IPv4 iniciada con un enlace estático que asigna una dirección IPv4 y un número de puerto a una dirección IPv6. Configuración de NAT64 para la comunicación iniciada por IPv4. También admite la reescritura de puertos, lo que permite conservar incluso más direcciones IPv4 traduciendo una dirección IPv4 y un número de puerto a una dirección IPv6 con varios números de puerto. Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto.

Una dirección IPv4 puede utilizarse para NAT44 y NAT64; no reserva un grupo de direcciones IPv4 solo para NAT64.

NAT64 opera en las interfaces, subinterfaces e interfaces de túnel de capa 3. Para utilizar NAT64 en el cortafuegos de Palo Alto Networks para la comunicación iniciada por IPv6, debe contar con un Servidor DNS64 externo o una solución para separar la función de consultas de DNS de la función NAT. El servidor DNS64 traduce entre su host IPv6 y un servidor DNS IPv4 codificando la dirección IPv4 que recibe de un servidor DNS público en una dirección IPv6 para el host IPv6.

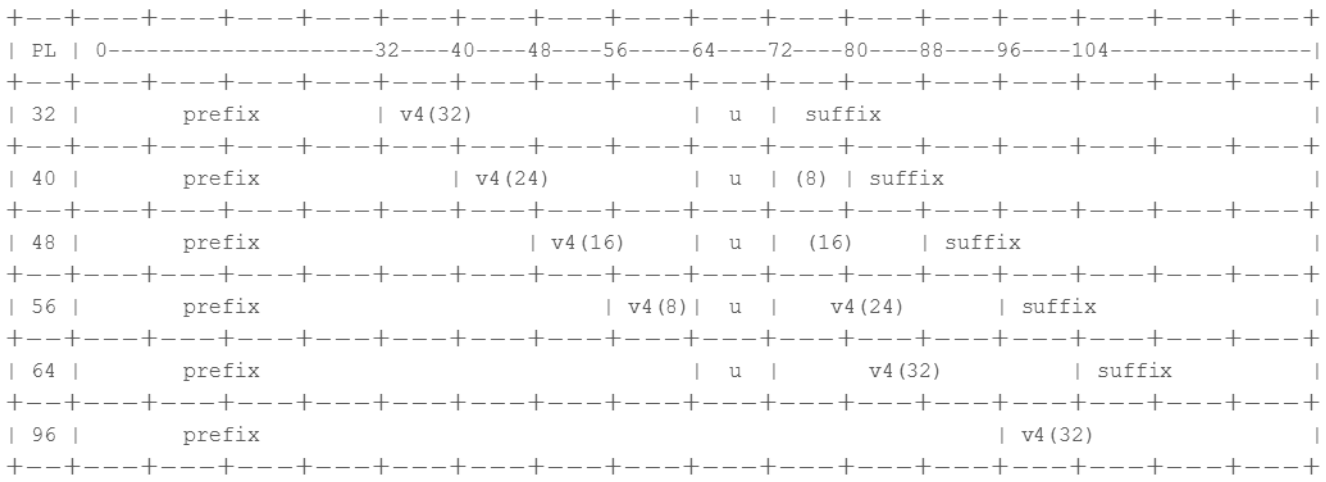
Palo Alto Networks admite las siguientes funciones de NAT64:

- Redirección (Giro en U de NAT); además, NAT64 previene los ataques de bucle de redirección descartando todos los paquetes IPv6 entrantes que cuenten con un prefijo de origen 64::/n.
- Traducción de paquetes TCP/UDP/ICMP según RFC 6146 y el cortafuegos se esfuerza por traducir otros protocolos que no utilizan una puerta de enlace de nivel de aplicación (application-level gateway, ALG). Por ejemplo, el cortafuegos puede traducir un paquete GRE. Esta traducción tiene la misma limitación que NAT44: si no cuenta con una ALG para un protocolo que pueda utilizar un canal de control y datos separado, es posible que el cortafuegos no comprenda el flujo del tráfico de retorno.
- La traducción entre IPv4 y IPv6 del atributo de longitud de ICMP del campo de datagrama original, según RFC 4884.

© 2020 Palo Alto Networks, Inc.

Dirección IPv6 integrada en la dirección IPv4

NAT64 utiliza una dirección IPv6 integrada en la dirección IPv4 como se describe en RFC 6052, Direccionamiento de IPv6 para traductores de IPv4/IPv6. Una dirección IPv6 integrada en la dirección IPv4 es una dirección IPv6 con una dirección IPv4 decodificada en 32 bits. La longitud del prefijo (PL en la figura) de IPv6 determina donde se decodifica la dirección IPv4 en la dirección IPv6, de la siguiente manera:



El cortafuegos admite la traducción de subredes /32, /40, /48, /56, /64 y /96 utilizando estos prefijos. Un cortafuegos único admite múltiples prefijos; cada regla NAT64 utiliza un prefijo. El prefijo puede ser un prefijo conocido (64:FF9B::/96) o un prefijo específico de la red (NSP) que es único en la organización que controla el traductor de direcciones (el dispositivo DNS64). Por lo general, un NSP es una red dentro del prefijo IPv6 de la organización. Normalmente, el dispositivo DNS64 configura el campo u y el sufijo en cero; el cortafuegos ignora estos campos.

Servidor DNS64

Si desea utilizar DNS y realizar una traducción de NAT64 utilizando una Comunicación de Pv6 iniciada, debe utilizar un servidor DNS64 externo u otra solución DNS64 que se configure con el prefijo conocido o su NSP. Cuando un host IPv6 intenta acceder a un host ipV4 o un dominio en internet, el servidor DNS64 le solicita a un servidor DNS autorizado la dirección IPv4 asignada a ese nombre de host. El servidor DNS le envía un registro de dirección (registro A) al servidor DNS64 con la dirección IPv4 del nombre de host.

El servidor DNS64 convierte la dirección IPv4 en formato hexadecimal y la cifra en los octetos adecuados del prefijo IPv6 que su configuración le permite utilizar (el prefijo conocido o su NSP) en función de la longitud del prefijo, lo que produce una Dirección IPv6 integrada en la dirección IPv4. El servidor DNS64 envía un registro AAAA al host IPv6 que asigna la dirección IPv6 integrada en la dirección IPv4 al nombre de host IPv4.

Detección de MTU de ruta

IPv6 no fragmenta los paquetes, de modo que el cortafuegos utiliza dos métodos para reducir la necesidad de fragmentación de paquetes:

- Cuando el cortafuegos traduce paquetes IPv4 con un bit de no fragmentar (don't fragment, DF) en cero, esto indica que el remitente espera que el cortafuegos fragmente los paquetes que son demasiado grandes, pero que el cortafuegos no fragmenta paquetes para la red IPv6 (tras la traducción) debido a que IPv6 no fragmenta paquetes. En cambio, puede configurar el tamaño mínimo en el que el cortafuegos fragmentará los paquetes IPv4 antes de traducirlos. El valor **NAT64 IPv6 Minimum Network**

© 2020 Palo Alto Networks, Inc.

MTU (MTU de red mínima de IPv6 de NAT64e) forma parte de la configuración, que cumple con RFC 6145, el algoritmo de traducción de IP/ICMP. Puede establecer la **NAT64 IPv6 Minimum Network MTU (MTU de red mínima de IPv6 de NAT64)** en su valor máximo (**Device [Dispositivo]** > **Setup [Configuración]** > **Session [Sesión]**), lo que provoca que el cortafuegos fragmente paquetes IPv4 en el tamaño mínimo de IPv6 antes de traducirlos a IPv6. (La **NAT64 IPv6 Minimum Network MTU [MTU de red mínima de IPv6 de NAT64]** no cambia la MTU de la interfaz).

- El otro método que utiliza el cortafuegos para reducir la fragmentación es la detección de MTU de ruta (Path MTU Discovery, PMTUD). En una comunicación de IPv4 iniciada, si un paquete IPv4 que se traducirá tiene un conjunto de bits de DF y la MTU de la interfaz de salida es más pequeña que el paquete, el cortafuegos utiliza la PMTUD para descartar el paquete y devolver un mensaje de ICMP "Destination Unreachable - fragmentation needed" (Destino inalcanzable: se requiere la fragmentación) al origen. El origen reduce la MTU de ruta para ese destino y reenvía el paquete hasta que las reducciones sucesivas en la MTU de ruta permiten la entrega del paquete.

Comunicación de Pv6 iniciada

La comunicación de IPv6 iniciada con el cortafuegos es similar a una NAT de origen en una topología IPv4. Realice la Configuración de NAT64 para la comunicación de IPv4 iniciada cuando su host IPv6 deba comunicarse con un servidor IPv4.

En la regla de la política NAT64, configure el origen original como dirección host IPv6 o como todos. Configure la dirección IPv6 de destino como prefijo conocido o el NSP que utiliza el servidor DNS64. (No configure la dirección IPv6 de destino completa en la regla).

Si debe utilizar un DNS, deberá utilizar un servidor DNS64 para convertir un resultado “A” DNS de IPv4 en un resultado “AAAA” fusionado con el prefijo NAT64. Si no utiliza un DNS, debe crear la dirección utilizando la dirección de destino IPv4 y el prefijo NAT64 configurado en el cortafuegos respetando las reglas RFC 6052.

En los entornos que utilizan un DNS, el siguiente ejemplo de topología ilustra la comunicación con el servidor DNS64. El servidor DNS64 debe configurarse de modo que se utilice el prefijo conocido 64:FF9B::/96 o el prefijo específico de la red, que debe cumplir con RFC 6052 (/32, /40,/48,/56,/64 o /96).

En el lado traducido del cortafuegos, el tipo de traducción debe ser IP dinámica y puerto para implementar NAT64 con estado. Configure la dirección de origen traducida para que sea la dirección IPv4 de la interfaz de salida en el cortafuegos. No configure el campo de traducción de destino; el cortafuegos traduce la dirección buscando la longitud del prefijo en la dirección original de destino de la regla y, luego, en función del prefijo, extrayendo la dirección IPv4 codificada de la dirección IPv6 de destino original en el paquete entrante.

Antes de que el cortafuegos observe la regla NAT64, el cortafuegos debe realizar una búsqueda de ruta para encontrar la zona de seguridad de destino de un paquete entrante. Debe garantizar que el prefijo NAT64 pueda alcanzarse mediante la asignación de zona de destino debido a que el cortafuegos no debe poder enrutar el prefijo NAT64. Probablemente, el cortafuegos asignaría el prefijo NAT64 a la ruta predeterminada o descartaría el prefijo NAT64 debido a que no existe una ruta para él. El cortafuegos no encontrará una zona de destino debido a que el prefijo NAT64 no se encuentra en la tabla de enrutamiento, asociado a la interfaz y la zona de salida.

Además, debe configurar una interfaz de túnel (sin punto de terminación). Aplique el prefijo NAT64 al túnel y aplique la zona adecuada para garantizar que el tráfico IPv6 con el prefijo NAT64 se asigna a la zona de destino correcta. El túnel también posee la ventaja de descartar el tráfico IPv6 con el prefijo NAT64 si el tráfico no coincide con la regla NAT64. El protocolo de enrutamiento configurado en el cortafuegos busca el prefijo IPv6 en su tabla de enrutamiento para buscar la zona de destino y busca en la regla NAT64.

La siguiente figura ilustra la función del servidor DNS64 en el proceso de resolución de nombres. En este ejemplo, el servidor DNS64 se configura de modo que se utilice el prefijo conocido 64:FF9B::/96.

1. Un usuario en el host IPv6 ingresa a la URL www.abc.com, lo que genera una búsqueda en el servidor de nombres (nslookup) para el servidor DNS64.

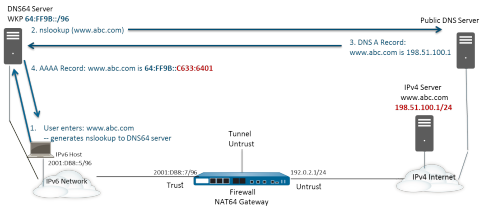
© 2020 Palo Alto Networks, Inc.

2. El servidor DNS64 envía una nslookup de www.abc.com en el servidor DNS público y solicita su dirección IPv4.

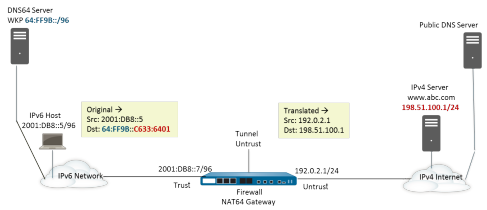
3. El servidor DNS devuelve un registro A que proporciona la dirección IPv4 al servidor DNS64.

4. El servidor DNS64 envía un registro AAAA al usuario IPv6, lo que convierte la dirección IPv4 decimal delimitada con puntos 198.51.100.1 en la dirección hexadecimal C633:6401 y la integra en su propio prefijo IPv6, 64:FF9B::/96. [198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] El resultado es la dirección IPv6 integrada en la dirección IPv4 64:FF9B::C633:6401.

Tenga en cuenta que en un prefijo /96, la dirección IPv4 se compone de los últimos cuatro octetos codificados en la dirección IPv6. Si el servidor DNS64 utiliza un prefijo /32, /40, /48, /56 o /64, la dirección IPv4 se codifica como se muestra en RFC 6052.



Tras la resolución de nombres transparente, el host IPv6 envía un paquete al cortafuegos con su dirección IPv6 de origen y su dirección IPv6 de destino 64:FF9B::C633:6401, como lo determina el servidor DNS64. El cortafuegos realiza la traducción de NAT64 en función de su regla NAT64.



Configuración de NAT64 para la comunicación iniciada por IPv6

Esta tarea de configuración y sus direcciones corresponden a las figuras de Comunicación iniciada por IPv6.

STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree un objeto de dirección para la dirección de destino IPv6 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, servidor nat64-IPv4.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese el prefijo IPv6 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96). Este es el prefijo conocido o su prefijo específico de red que está configurado en el servidor DNS64.

   Para este ejemplo, ingrese 64:FF9B::/96.

   El origen y el destino deben tener la misma máscara de red (extensión del prefijo).

© 2020 Palo Alto Networks, Inc.

(Usted no introduce una dirección de destino completa porque, según la extensión del prefijo, el cortafuegos extrae la dirección IPv4 de la dirección IPv6 de destino original en el paquete entrante. En este ejemplo, el prefijo del paquete entrante está codificado con C633:6401 en hexadecimal, que es la dirección de destino IPv4 198.51.100.1).

4. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Cree un objeto de dirección para la dirección de origen IPv6 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección del host IPv6; en este ejemplo, 2001:DB8::5/96.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Cree un objeto de dirección para la dirección de origen IPv4 (traducida).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv4 de la interfaz de salida del cortafuegos; en este ejemplo, 192.0.2.1.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv6_init.
3. (Opcional) Introduzca una **descripción**.
4. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 6 | Especifique la información de origen y destino original.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona fiable.
2. Seleccione la **Destination Zone (Zona de destino)**; en este ejemplo, la zona no fiable.
3. (Opcional) Seleccione una **Destination Interface (Interfaz de destino)** o la opción predeterminada (**any [cualquiera]**).
4. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección que creó para el host IPv6.
5. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** para añadir el objeto de dirección que creó para el destino IPv6; en este ejemplo, servidor nat64-IPv4.
6. (Opcional) Para **Service (Servicio)**, seleccione **any (cualquiera)**.

STEP 7 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, para **Translation Type (Tipo de traducción)**, seleccione **Dynamic IP and Port (IP dinámica y puerto)**.
2. Para **Address Type (Tipo de dirección)**, seleccione una de las siguientes opciones:
   - Seleccione **Translated Address (Dirección traducida)** y luego **Add (Añadir)** para añadir el objeto que creó para la dirección de origen IPv4.
   - Seleccione **Interface Address (Dirección de interfaz)**, en cuyo caso la dirección de origen traducida es la dirección IP y la máscara de red de la interfaz de salida del cortafuegos. Para esta opción, debe seleccionar **Interface (Interfaz)** y opcionalmente una **IP Address (Dirección IP)** si la interfaz tiene más de una dirección IP.

© 2020 Palo Alto Networks, Inc.

3. Deje **Destination Address Translation (Traducción de dirección de destino)** sin seleccionar. (El cortafuegos extrae la dirección IPv4 del prefijo IPv6 en el paquete entrante, según la extensión del prefijo especificada en el destino original de la regla NAT64).
4. Haga clic en **OK (Aceptar)** para guardar la regla de política de NAT64.

STEP 8 | Configure una interfaz de túnel para emular una interfaz de bucle invertido con una máscara de red que no sea 128.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir un túnel.
2. En **Interfaz Name (Nombre de interfaz)**, especifique un sufijo numérico, como .2.
3. En la pestaña **Config**, seleccione el **Virtual Router (Enrutador virtual)** donde configuró NAT64.
4. Para **Security Zone (Zona de seguridad)**, seleccione la zona de destino asociada con el destino de servidor IPv4 (zona fiable).
5. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
6. Haga clic en **Add (Añadir)** y para **Address (Dirección)**, seleccione **New Address (Nueva dirección)**.
7. Introduzca en **Name (Nombre)** un nombre para el perfil.
8. (Opcional) Introduzca una **Description (Descripción)** para la dirección de túnel.
9. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese su prefijo IPv6 y la extensión del prefijo; en este ejemplo, 64:FF9B::/96.
10. Haga clic en **OK (Aceptar)**.
11. Seleccione **Enable address on interface (Habilitar la dirección en la interfaz)** y haga clic en **OK (Aceptar)**.
12. Haga clic en **OK (Aceptar)**.
13. Haga clic en **OK (Aceptar)** para guardar el túnel.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Trust (Fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **Untrust (No fiable)**.
5. Para **Application (Aplicación)**, seleccione **Any (Cualquiera)**.
6. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
7. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

STEP 11 | Solucione los problemas o visualice una sesión NAT64.

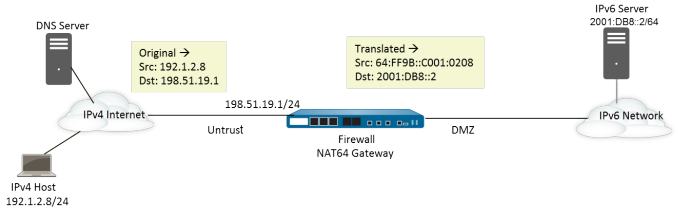
```
> show session id <session-id>
```

Configuración de NAT64 para la comunicación iniciada por IPv4

La comunicación de IPv4 iniciada con un servidor IPv6 es similar a una NAT de destino en una topología IPv4. La dirección IPv4 de destino se asigna a la dirección IPv6 de destino mediante una traducción de IP estática uno a uno (no una traducción de varios a uno).

© 2020 Palo Alto Networks, Inc.

El cortafuegos codifica la dirección IPv4 de origen en el prefijo conocido 64:FF9B::/96 como se define en RFC 6052. La dirección de destino traducida no es la dirección IPv6 real. Por lo general, el caso de uso de la comunicación de IPv4 iniciada se presenta cuando una organización proporciona acceso de la zona pública Untrust a un servidor IPv6 en la zona DMZ de la organización. Esta topología no utiliza un servidor DNS64.



STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cuando un paquete IPv4 posee su bit DF configurado en cero (y debido a que IPv6 no fragmenta los paquetes), asegúrese de que el paquete IPv6 traducido no supera la ruta MTU para la red IPv6 de destino.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. En **NAT64 IPv6 Minimum Network MTU (MTU de red mínima de IPv6 de NAT64)**, introduzca la cantidad mínima de bytes en la que el cortafuegos fragmentará los paquetes IPv4 para la traducción a IPv6 (rango: 1280 a 9216, valor predeterminado: 1280).

   Si no desea que el cortafuegos fragmente un paquete IPv4 antes de la traducción, configure el MTU en 9216. Si el paquete IPv6 traducido supera este valor, el cortafuegos descarta el paquete y emite un paquete ICMP que indica que el destino es inalcanzable y que se necesita fragmentación.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un objeto de dirección para la dirección de destino IPv4 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_ip4server.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red)** e ingrese la dirección IPv4 de la interfaz del cortafuegos en la zona no fiable. La dirección no debe usar una máscara de red o solo una máscara de red de /32. Este ejemplo utiliza 198.51.19.1/32.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Cree un objeto de dirección para la dirección de origen IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name (Nombre)**; por ejemplo, nat64_ip6source.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 NAT64 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96).

   Para este ejemplo, ingrese 64:FF9B::/96.

   (El cortafuegos codifica el prefijo con la dirección de origen IPv4 192.1.2.8, que es C001:0209 en hexadecimal).
4. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Cree un objeto de dirección para la dirección de destino IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_server_2.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 del servidor IPv6 (destino). La dirección no debe usar una máscara de red o solo una máscara de red de /128. Este ejemplo utiliza 2001:DB8::2/128.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv4_init.
3. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 7 | Especifique la información de origen y destino original.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona no fiable.
2. Seleccione la **Destination Zone (Zona de destino)**, probablemente una zona fiable o DMZ.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección para el host IPv4.
4. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** el objeto de dirección para el destino IPv4; en este ejemplo, nat64_ip4server.
5. En **Service (Servicio)**, seleccione **any (cualquiera)**.

STEP 8 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)**.
2. Para **Translated Address (Dirección traducida)**, seleccione el objeto de dirección traducida que creó, nat64_ip6source.
3. En **Destination Address Translation (Traducción de dirección de destino)**, para **Translated Address (Dirección traducida)**, especifique una unica dirección IPv6 (el objeto de dirección; en este ejemplo, nat64_server_2 o la dirección IPv6 del servidor).
4. Haga clic en **OK (Aceptar)**.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona no fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Untrust (No fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **DMZ**.
5. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

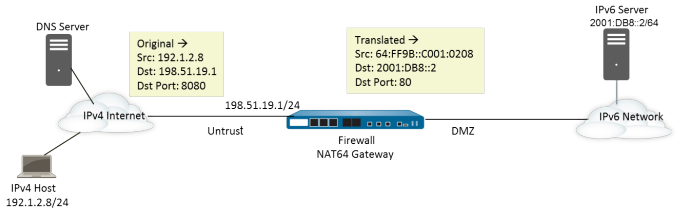
STEP 11 | Solucione los problemas o visualice una sesión NAT64.

© 2020 Palo Alto Networks, Inc.

```
> show session id <session-id>
```

Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto

Esta tarea parte de la tarea de configuración de NAT64 para la comunicación iniciada por IPv4, pero la organización que controla la red IPv6 prefiere traducir el número de puerto de destino público a un número de puerto de destino interno y, por lo tanto, mantenerlo en privado para los usuarios del lado no fiable IPv4 del cortafuegos. En este ejemplo, el puerto 8080 se traduce en el puerto 80. Para hacer eso, en la regla de política NAT64, cree un nuevo servicio que especifique que el puerto de destino es 8080. Para el paquete traducido, el puerto traducido es 80.



STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cuando un paquete IPv4 posee su bit DF configurado en cero (y debido a que IPv6 no fragmenta los paquetes), asegúrese de que el paquete IPv6 traducido no supera la ruta MTU para la red IPv6 de destino.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Para **NAT64 IPv6 Minimum Network MTU (MTU de red mínima IPv6 NAT64)**, ingrese el número más bajo de bytes en los cuales el cortafuegos fragmentará los paquetes IPv4 para la traducción en IPv6 (el intervalo es 1280 a 9216; el valor predeterminado es 1280).

   Si no desea que el cortafuegos fragmente un paquete IPv4 antes de la traducción, configure el MTU en 9216. Si el paquete IPv6 traducido supera este valor, el cortafuegos descarta el paquete y emite un paquete ICMP que indica que el destino es inalcanzable y que se necesita fragmentación.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un objeto de dirección para la dirección de destino IPv4 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_ip4server.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red)** e ingrese la dirección IPv4 y máscara de red de la interfaz del cortafuegos en la zona no fiable. Este ejemplo utiliza 198.51.19.1/24.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Cree un objeto de dirección para la dirección de origen IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.

© 2020 Palo Alto Networks, Inc.

2. Introduzca un nombre para el objeto en **Name (Nombre)**; por ejemplo, nat64_ip6source.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 NAT64 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96).

   Para este ejemplo, ingrese 64:FF9B::/96.

   (El cortafuegos codifica el prefijo con la dirección de origen IPv4 192.1.2.8, que es C001:0209 en hexadecimal).
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree un objeto de dirección para la dirección de destino IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_server_2.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 del servidor IPv6 (destino). Este ejemplo utiliza 2001:DB8::2/64.

   El origen y el destino deben tener la misma máscara de red (extensión del prefijo).
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv4_init.
3. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 7 | Especifique la información de origen y destino original, y cree un servicio para limitar la traducción a un solo número de puerto de ingreso.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona no fiable.
2. Seleccione la **Destination Zone (Zona de destino)**, probablemente una zona fiable o DMZ.
3. Para **Service (Servicio)**, seleccione New **Service (Nuevo servicio)**.
4. Introduzca un nombre para el servicio en **Name**, tal como Port_8080.
5. Seleccione **TCP** como el **Protocol (Protocolo)**.
6. Para **Destination Port (Puerto de destino)**, ingrese 8080.
7. Haga clic en **OK (Aceptar)** para guardar el servicio.
8. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección para el host IPv4.
9. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** el objeto de dirección para el destino IPv4; en este ejemplo, nat64_ip4server.

STEP 8 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)**.
2. Para **Translated Address (Dirección traducida)**, seleccione el objeto de dirección traducida que creó, nat64_ip6source.
3. En **Destination Address Translation (Traducción de dirección de destino)**, para **Translated Address (Dirección traducida)**, especifique una unica dirección IPv6 (el objeto de dirección; en este ejemplo, nat64_server_2 o la dirección IPv6 del servidor).
4. Especifique el número de **Translated Port (Puerto traducido)** de destino privado al cual el cortafuegos traducirá el número de puerto de destino público; en este ejemplo, 80.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona no fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Untrust (No fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **DMZ**.
5. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

STEP 11 | Solucione los problemas o visualice una sesión NAT64.

```
> show session id <session-id>
```


© 2020 Palo Alto Networks, Inc.

ECMP

El procesamiento de trayectoria múltiple a igual coste (ECMP) es una función de red que permite al cortafuegos usar hasta cuatro rutas de igual coste hacia el mismo destino. Sin esta función, si hay múltiples rutas del mismo coste al mismo destino, el enrutador virtual selecciona una de estas rutas de la tabla de enrutamiento y la añade a su tabla de envío; no usará ninguna de las demás rutas a no ser que se interrumpa la ruta seleccionada.

La habilitación de la funcionalidad ECMP en un enrutador virtual permite que el cortafuegos tenga hasta cuatro rutas del mismo coste a un destino en esta tabla de reenvío, permitiendo que el cortafuegos:

- Equilibre la carga de los flujos (sesiones) al mismo destino en múltiples enlaces del mismo coste.
- Use de forma eficiente el ancho de banda disponible en enlaces hacia el mismo destino, en lugar de dejar algunos enlaces sin usar.
- Cambie dinámicamente el tráfico a otro miembro de ECMP hacia el mismo destino si falla un enlace, en lugar de tener que esperar a que el protocolo de enrutamiento o la tabla RIB seleccione una ruta alternativa. Esto puede ayudar a reducir el tiempo de inactividad cuando falla el enlace.

Para obtener información sobre la selección de la ruta ECMP cuando se produce un fallo en un peer de HA, consulte ECMP en modo HA activa/activa.

Las siguientes secciones describen ECMP y cómo configurarlo.

- Algoritmos de equilibrio de carga de ECMP
- Compatibilidad con modelo de ECMP, interfaz y enrutamiento de IP
- Configuración de ECMP en un enrutador virtual
- Habilitación de ECMP para varios sistemas BGP autónomos
- Verificación de ECMP

Algoritmos de equilibrio de carga de ECMP

Supongamos que la base de información de enrutamiento (RIB, Routing Information Base) del cortafuegos tiene múltiples trayectorias a igual coste a un único destino. El número máximo de rutas a igual coste es 2 de manera predeterminada. ECMP elige las dos mejores rutas de igual coste de la RIB para copiarlas a la base de información de reenvío (FIB, Forwarding Information Base). ECMP determina a continuación y basándose en el método de equilibrio de carga, cuál de las dos rutas en la FIB usará el cortafuegos para la designación durante esta sesión.

El equilibrio de carga de ECMP se realiza en este nivel de sesión, no en el nivel de paquete; el inicio de una nueva sesión se produce cuando el cortafuegos (ECMP) elige una ruta a igual coste. Las rutas a igual coste a un único destino se consideran miembros de la ruta de ECMP o miembros del grupo ECMP. ECMP determina cuál de las múltiples rutas a un destino en la FIB se utiliza para un flujo de ECMP, en función del algoritmo de equilibrio de carga que haya definido. Un enrutador virtual solo puede usar un algoritmo de equilibrio de carga.



Habilitar, deshabilitar o cambiar ECMP en un enrutador virtual existente provoca que el sistema reinicie el enrutador virtual, lo cual podría ocasionar que se cierren las sesiones existentes.

Cada uno de los cuatro algoritmos posibles hace hincapié en una prioridad diferente, tal y como se indica a continuación:

- **Los algoritmos basados en hash dan prioridad a la permanencia de la sesión**: los algoritmos **IP Modulo** e **IP Hash** usan hashes basados en la información del encabezado de paquete, como las direcciones de origen y destino. Dado que el encabezado de cada flujo en una sesión determinada contiene la misma información de origen y destino, estas opciones conceden prioridad a la *pegajosidad* de la sesión. Si

© 2020 Palo Alto Networks, Inc.

elige el algoritmo **IP Hash**, el hash puede basarse en las direcciones de origen y destino, o el hash puede basarse en la dirección de origen únicamente (en PAN-OS 8.0.3 y versiones posteriores). Al usar un hash IP basado únicamente en la dirección de origen, todas las sesiones que pertenecen a la misma dirección IP tomarán siempre la misma ruta de las diversas rutas disponibles. Por lo tanto, la ruta se considera adhesiva y es más fácil detectar problemas en ella si fuera necesario. Puede definir opcionalmente un valor de **Hash Seed (Inicialización de hash)** para aleatorizar aún más el equilibrio de carga si tiene un gran número de sesiones hacia el mismo destino y no se están distribuyendo de manera uniforme entre los enlaces ECMP.

- **Los algoritmos equilibrados dan prioridad al equilibrio de carga**: el algoritmo **Balanced Round Robin (Operación por turnos equilibrada)** distribuye las sesiones entrantes equitativamente entre los enlaces, dando prioridad al equilibrio de carga sobre la permanencia de la sesión. (La operación por turnos indica una secuencia en la que se elige el elemento que hace más tiempo que no se escoge). Asimismo, si se añaden nuevas rutas o se eliminan de un grupo ECMP (por ejemplo, si una ruta del grupo deja de estar disponible), el enrutador virtual reequilibrará las sesiones en todos los enlaces del grupo. Además, si los flujos en una sesión tienen que conmutar rutas debido a una caída del servicio, cuando la ruta original asociada a la sesión vuelva a estar disponible, los flujos de la sesión se revertirán a la ruta original cuando el enrutador virtual reequilibre de nuevo la carga.
- **Weighted algorithm prioritizes link capacity and/or speed**: como una extensión del estándar del protocolo ECMP, la implementación de Palo Alto Networks ofrece una opción de equilibrio de carga para **Weighted Round Robin** que tiene en cuenta las diferentes capacidades y velocidades de los enlaces en las interfaces de salida del cortafuegos. Con esta opción, puede asignar **ECMP Weights** (el intervalo es 1-255; el valor por defecto es 100) a las interfaces basadas en el rendimiento de enlaces usando factores tales como la capacidad, velocidad y latencia de los enlaces para garantizar que las cargas se equilibran con el fin de aprovechar completamente los enlaces disponibles.

  Por ejemplo, imaginemos que el cortafuegos tiene enlaces redundantes a un ISP: Ethernet 1/1 (100 Mbps) y Ethernet 1/8 (200 Mbps). Aunque son rutas a igual coste, el enlace a través de Ethernet 1/8 ofrece un mayor ancho de banda y por lo tanto puede gestionar una mayor carga que el enlace Ethernet 1/1. Por lo tanto, para garantizar que la funcionalidad de equilibrio de carga tiene en cuenta la capacidad y velocidad de los enlaces, debe asignar a Ethernet 1/8 un peso de 200 y a Ethernet 1/1 un peso de 100. La relación de ponderación 2:1 hace que el enrutador virtual envíe el doble de sesiones a Ethernet 1/8 que a Ethernet 1/1. Sin embargo, dado que el protocolo ECMP se basa esencialmente en sesiones, al usar el algoritmo **Weighted Round Robin (Operación por turnos ponderada)**, el cortafuegos podrá equilibrar la carga a todos los enlaces de ECMP basándose solo en la mejor opción.

  Tenga en cuenta que los pesos de ECMP se asignan a las interfaces para determinar el equilibrio de carga (para influir qué ruta *a igual coste* se elige), no para la selección de ruta (una elección de ruta entre rutas que podrían tener diferentes costes).

  Asigne enlaces de menor velocidad o capacidad con un peso menor. Asigne enlaces de mayor velocidad o capacidad con un peso mayor. De este modo, el cortafuegos puede distribuir sesiones basándose en estas relaciones, en lugar de saturar un enlace de baja capacidad que es una de las rutas a igual coste.

Compatibilidad con modelo de ECMP, interfaz y enrutamiento de IP

El modelo de rutas múltiples a igual coste (equal cost multiple path, ECMP) se admite en todos los modelos de cortafuegos de Palo Alto Networks y ofrece compatibilidad con el reenvío mediante hardware en los cortafuegos PA-7000 Series, PA-5200 y PA-3200. Los cortafuegos VM-Series admiten ECMP solo mediante software. El rendimiento se ve afectado para las sesiones que no se pueden descargar mediante hardware.

ECMP es compatible con Capa 3, subinterfaz de Capa 3, VLAN, túnel e interfaces de Ethernet de agregación.

© 2020 Palo Alto Networks, Inc.

ECMP se puede configurar para rutas estáticas y cualquiera de los protocolos de enrutamiento dinámico compatibles con el cortafuegos.

ECMP afecta a la capacidad de la tabla de enrutamiento porque la capacidad se basa en el número de rutas, de modo que una ruta ECMP con cuatro rutas consumirá cuatro entradas de la capacidad de la tabla de enrutamiento. La implementación de ECMP puede reducir ligeramente la capacidad de la tabla de enrutamiento porque se utiliza más memoria para usar etiquetas basadas en sesiones para asignar los flujos de tráfico a interfaces particulares.

El enrutamiento de enrutador a enrutador virtual mediante rutas estáticas no es compatible con ECMP.

Configuración de ECMP en un enrutador virtual

Utilice el siguiente procedimiento para habilitar ECMP en un enrutador virtual. Los requisitos previos son:

- Especifique las interfaces que pertenecen a un enrutador virtual (**Network [Red]** > **Virtual Routers [Enrutadores virtuales]** > **Router Settings [Configuración de enrutador]** > **General [General]**).
- Especifique el protocolo de enrutamiento de IP.

La habilitación, deshabilitación o cambio de ECMP para un enrutador virtual existente hace que el sistema reinicie el enrutador virtual, que puede causar la terminación de las sesiones.

STEP 1 | Habilitación de ECMP para un enrutador virtual.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual en el que se habilitará ECMP.
2. Seleccione **Router Settings (Configuración de enrutador)** > **ECMP** y seleccione **Enable (Habilitar)**.

STEP 2 | (Opcional) Habilite el retorno simétrico de paquetes del servidor al cliente.

Seleccione **Symmetric Return (Retorno simétrico)** para que los paquetes de retorno salgan de la misma interfaz a la que llegaron los paquetes de entrada asociados. Es decir, que el cortafuegos usará la interfaz de entrada a la que enviar los paquetes de retorno, en lugar de usar la interfaz ECMP. El ajuste de **Symmetric Return** anula el equilibrio de carga. Este comportamiento solo se produce con flujos de tráfico del servidor al cliente.

STEP 3 | Habilite **Strict Source Path (Ruta de origen estricta)** para asegurarse de que el tráfico IKE e IPSec que se origina en el cortafuegos salga de la interfaz física a la que pertenece la dirección IP de origen del túnel IPSec.

Cuando habilite ECMP, el tráfico IKE e IPSec que se origina en el cortafuegos de forma predeterminada, sale de una interfaz que determina un método de equilibrio de carga ECMP. También puede habilitar Strict Source Path (Ruta de origen estricta) para asegurarse de que el tráfico IKE e IPSec que se origina en el cortafuegos siempre salga de la interfaz física a la que pertenece la dirección IP de origen del túnel IPSec. Debe habilitar esta función cuando el cortafuegos tenga más de un ISP que proporcione rutas de igual coste al mismo destino. Los ISP suelen realizar una verificación de reenvío de ruta (RPF, Path Forwarding) inversa (o una verificación diferente para evitar la suplantación de direcciones IP) para confirmar que el tráfico está saliendo por la misma interfaz por la que llegó. Debido a que ECMP elegiría una interfaz de salida basada en el método ECMP configurado (en lugar de elegir la interfaz de origen como interfaz de salida), no sería el comportamiento esperado por el ISP y este podría bloquear el tráfico de retorno legítimo. En ese caso, habilite la ruta de origen estricta para que el cortafuegos use la interfaz de salida que es la interfaz a la que pertenece la dirección IP de origen del túnel IPSec, en la que se realiza la verificación RPF correctamente y donde el ISP permite el tráfico de retorno.

STEP 4 | Especifique el número máximo de rutas a igual coste (a una red de destino) que se pueden copiar desde la base de información de rutas (RIB) a la base de información de reenvío (FIB).

Para el valor máximo de rutas permitidas, en **Max Path (Ruta máxima)**, introduzca **2**, **3** o **4**. Default: 2.

© 2020 Palo Alto Networks, Inc.

STEP 5 | Seleccione el algoritmo de equilibrio de carga para el enrutador virtual. Para obtener más información sobre los métodos de equilibrio de carga y sus diferencias, consulte Algoritmos de equilibrio de carga ECMP .

En **Load Balance (Equilibrio de carga)**, seleccione una de las siguientes opciones en la lista **Method (Método)**:

- **IP Modulo** (predeterminado): usa un hash de las direcciones IP de origen y destino en el encabezado del paquete para determinar qué ruta ECMP se usará.
- **IP Hash**: existen dos métodos de hash IP que determinan qué ruta ECMP se usará (seleccione las opciones de hash en el paso 5):
  - Use un hash de la dirección de origen (disponible en PAN-OS 8.0.3 y versiones posteriores).
  - Utilice un hash de las direcciones IP de origen y destino (el método de hash IP predeterminado).
- **Balanced Round Robin (Operación por turnos equilibrada)**: usa operación por turnos entre rutas ECMP y reequilibra las rutas cuando cambia el número de rutas.
- **Weighted Round Robin**: usa operación por turnos y un peso relativo para seleccionar entre las rutas ECMP. Especifique los grados de ponderación en el paso 6 siguiente.

STEP 6 | (IP Hash únicamente) Configure las opciones de hash de IP.

Si ha seleccionado **IP Hash** como el **Method**:

1. Seleccione **Use Source Address Only (Usar dirección de origen únicamente)** (disponible en PAN-OS 8.0.3 y versiones posteriores) si desea asegurarse de que todas las sesiones que pertenecen a la misma dirección IP tomen siempre la misma ruta de las múltiples rutas disponibles. Esta opción de hash de IP proporcionan permanencia de la ruta y facilita la resolución de problemas. Si no selecciona esta opción o utiliza una versión anterior a PAN-OS 8.0.3, el hash de IP se basa en las direcciones IP de origen y destino (el método de hash de IP predeterminado).

   Si selecciona Use Source Address Only (Usar dirección de origen únicamente), no debe enviar la configuración de Panorama a los cortafuegos que ejecutan PAN-OS 8.0.2, 8.0.1 o 8.0.0.
2. Seleccione **Use Source/Destination Ports** si desea usar los números de puerto de origen y destino en el cálculo de **IP Hash**.

   La habilitación de esta opción junto con Use Source Address Only (Usar la dirección de origen únicamente) asignará aleatoriamente la selección de ruta incluso para las sesiones que pertenecen a la misma dirección IP de origen.
3. Introduzca un valor **Hash Seed (Inicialización de hash)** (un valor entero con un máximo de nueve dígitos). Especifique un valor **Hash Seed** para aleatorizar aún más el equilibrio de carga. Especificar un valor de inicialización de hash resulta útil si tiene un gran número de sesiones con la misma información de tupla.

STEP 7 | (Solo para Weighted Round Robin [Operación por turnos ponderada]) Defina un peso para cada interfaz en el grupo ECMP.

Si ha seleccionado **Weighted Round Robin** como **Method**, defina un peso para cada una de las interfaces que constituyen los puntos de salida para enrutar el tráfico a los mismos destinos (es decir, interfaces que forman parte de un grupo ECMP, como las interfaces que ofrecen enlaces redundantes a su ISP o interfaces a las aplicaciones empresariales fundamentales de su red corporativa).

A mayor peso, con mayor frecuencia se seleccionará la ruta a igual coste para una nueva sesión.

Aporte a los enlaces de mayor velocidad un peso más alto que a los enlaces más lentos, con el fin de que haya más tráfico ECMP que atraviese el enlace más rápido.

© 2020 Palo Alto Networks, Inc.

1. Para crear un grupo de ECMP, haga clic en **Add (Añadir)** y seleccione una interfaz en **Interface (Interfaz)**.
2. Seleccione **Add** para añadir las otras interfaces en el grupo ECMP.
3. Haga clic en **Weight (Peso)** y especifique el peso relativo de cada interfaz (el intervalo es 1-255; el valor por defecto es 100).

STEP 8 | Guarde la configuración.

1. Haga clic en **OK (Aceptar)**.
2. En el mensaje de cambio de configuración ECMP, haga clic en **Yes** para reiniciar el enrutador virtual. Al reiniciar el enrutador virtual, puede que se terminen las sesiones existentes.

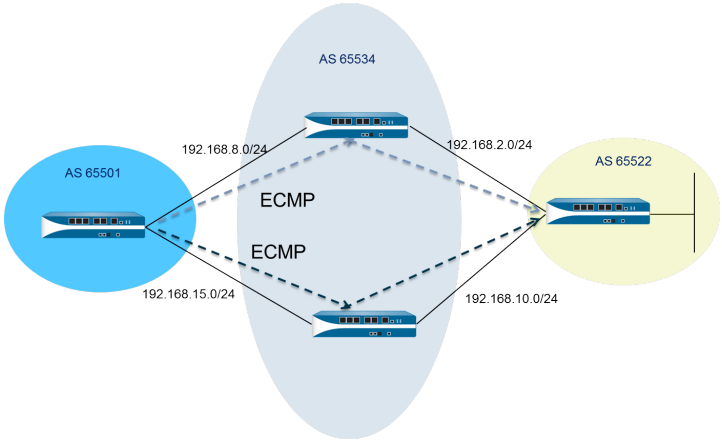
Este mensaje se muestra solo si está modificando un enrutador virtual con ECMP.

STEP 9 | Confirme los cambios.

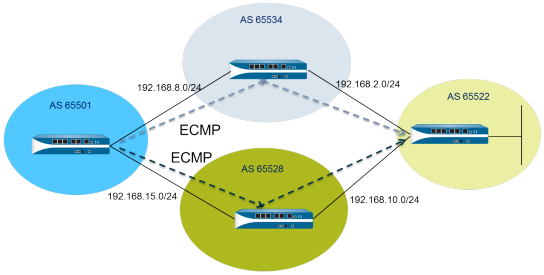
Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Habilitación de ECMP para varios sistemas BGP autónomos

Realice la siguiente tarea si ha configurado BGP y quiere habilitar ECMP en varios sistemas autónomos. Para esta tarea se da por hecho que ya ha configurado BGP. En la figura siguiente, dos rutas ECMP a un destino atraviesan dos cortafuegos que pertenecen a un único ISP en un único sistema BGP autónomo.



En la figura siguiente, dos rutas ECMP a un destino atraviesan dos cortafuegos que pertenecen a dos ISP diferentes en sistemas BGP autónomos distintos.



STEP 1 | Configurar ECMP.

© 2020 Palo Alto Networks, Inc.

Consulte Configuración de ECMP en un enrutador virtual.

STEP 2 | Para el enrutamiento de BGP, habilite ECMP en múltiples sistemas autónomos.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual en el que se habilitará ECMP para múltiples sistemas BGP autónomos.
2. Seleccione **BGP** > **Advanced (Avanzado)** y seleccione **ECMP Multiple AS Support (Soporte de AS de múltiple ECMP)**.

STEP 3 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Verificación de ECMP

Un enrutador virtual configurado para ECMP indica en la base de información de reenvío (FIB) qué rutas son ECMP. Una marca ECMP (E) para una ruta indica que está participando en ECMP para la interfaz de salida al siguiente salto para esa ruta. Para verificar el ECMP, utilice el siguiente procedimiento para observar la FIB y confirmar que algunas rutas son rutas múltiples a igual coste.

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.

STEP 2 | En la fila del enrutador virtual en el que ha habilitado ECMP, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 3 | Seleccione **Routing (Enrutamiento)** > **Forwarding Table (Tabla de reenvío)** para ver la FIB.



En la tabla, observe que varias rutas al mismo destino (excepto una interfaz diferente) tienen la marca E. Un asterisco (*) indica la ruta preferida para el grupo ECMP.

© 2020 Palo Alto Networks, Inc.

LLDP

Los cortafuegos de Palo Alto Networks son compatibles con el protocolo de detección de nivel de enlace (LLDP, Link Layer Discovery Protocol), que funciona como la capa de enlace para detectar dispositivos vecinos y sus capacidades. LLDP permite al cortafuegos y a otros dispositivos de la red intercambiar (enviar y recibir) unidades de datos LLDP (LLDPDU) con los vecinos. El dispositivo receptor almacena la información en un MIB, a la que puede acceder el protocolo simple de administración de redes (SNMP). LLDP facilita la solución de problemas, especialmente en el caso de implementaciones de virtual wire donde el cortafuegos suele pasar desapercibido en una topología de red.

- Descripción general de LLDP
- TLV compatibles con LLDP
- Mensajes de Syslog LLDP y capturas de SNMP
- Configuración de LLDP
- Visualización de estados y configuración de LLDP
- Borrado de estadísticas de LLDP

Descripción general de LLDP

LLDP opera en la Capa 2 del modelo OSI, usando direcciones MAC. Una LLDPDU es una secuencia de elementos de tipo-longitud-valor (TLV) encapsulados en una trama Ethernet. El estándar IEEE 802.1AB define tres direcciones MAC para LLDPDU: 01-80-C2-00-00-0E, 01-80-C2-00-00-03 y 01-80-C2-00-00-00.

El cortafuegos Palo Alto Networks solo admite una dirección MAC para transmitir y recibir unidades de datos LLDP: 01-80-C2-00-00-0E. Al transmitir, el cortafuegos usa 01-80-C2-00-00-0E como la dirección MAC de destino. Al recibir, el cortafuegos procesa los datagramas con 01-80-C2-00-00-0E como dirección MAC de destino. Si el cortafuegos recibe cualquiera de las otras dos direcciones MAC para LLDPDU en sus interfaces, realiza la misma acción de reenvío que realizó antes de esta función, del siguiente modo:

- Si el tipo de interfaz es vwire, el cortafuegos reenvía el datagrama al otro puerto.
- Si el tipo de interfaz es L2, el cortafuegos proyecta el datagrama al resto de VLAN.
- Si el tipo de interfaz es L3, el cortafuegos descarta los datagramas.

No se admiten Panorama ni dispositivos de WildFire.

Los tipos de interfaz que admiten LLDP son TAP, alta disponibilidad (HA), reflejo de descifrado, subinterfaces virtual wire/vlan/L3 e interfaces de tarjeta de procesamiento de logs (LPC) de PA-7000 Series.

Una trama Ethernet LLDP tiene el siguiente formato:

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Con la trama Ethernet LLDP, la estructura TLV tiene el siguiente formato:

© 2020 Palo Alto Networks, Inc.

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

TLV compatibles con LLDP

Las LLDPDU incluyen TLV obligatorios y opcionales. La siguiente tabla enumera los TLV obligatorios compatibles con el cortafuegos:

TLV obligatorios	Tipo de TLV	Description (Descripción)
TLV de ID de bastidor	1	Identifica el bastidor del cortafuegos. Cada cortafuegos debe tener exactamente un único ID de bastidor. El subtipo de ID de bastidor es 4 (dirección MAC) y los modelos de Palo Alto Networks utilizarán la dirección MAC de Eth0 para garantizar la exclusividad.
TLV de ID de puerto	2	Identifica el puerto desde el que se envía la LLDPDU. Cada cortafuegos usa un ID de puerto para cada mensaje de LLDPDU transmitido. El subtipo de ID de puerto es 5 (nombre de interfaz) e identifica de manera exclusiva el puerto de transmisión. El cortafuegos usa ifname de la interfaz como el ID de puerto.
TLV de tiempo de vida (TTL)	3	Especifica cuánto tiempo (en segundos) se retiene la información de LLDPDU recibida del peer como válida en el cortafuegos local (el intervalo es 0-65.535). El valor es un múltiplo del multiplicador de tiempo de retención de LLDP. Cuando el valor de TTL es 0, la información asociada al dispositivo deja de ser válida y el cortafuegos elimina esa entrada de la MIB.
Fin de TLV de LLDPDU	0	Indica el fin de la TLV en la trama Ethernet de LLDP.

La siguiente tabla enumera los TLV opcionales compatibles con el cortafuegos de Palo Alto Networks:

TLV opcionales	Tipo de TLV	Finalidad y notas relacionadas con la implementación del cortafuegos
TLV de descripción del puerto	4	Describe el puerto del cortafuegos en formato alfanumérico. Se utiliza el objeto ifAlias.
TLV de nombre del sistema	5	Nombre configurado del cortafuegos en formato alfanumérico. Se utiliza el objeto sysName.

© 2020 Palo Alto Networks, Inc.

TLV opcionales	Tipo de TLV	Finalidad y notas relacionadas con la implementación del cortafuegos
TLV de descripción del sistema	6	Describe el cortafuegos en formato alfanumérico. Se utiliza el objeto sysDescr.
Capacidades del sistema	7	Describe el modo de implementación de la interfaz del siguiente modo: • Se anuncia una interfaz L3 con capacidad de enrutador (bit 6) y el "otro" bit (bit 1). • Se anuncia una interfaz L2 con capacidad de puente para MAC (bit 3) y el "otro" bit (bit 1). • Se anuncia una interfaz virtual wire con capacidad de repetidor (bit 2) y el "otro" bit (bit 1).
Dirección de gestión	8	Una o más direcciones IP usadas para la gestión del cortafuegos, del siguiente modo: • Dirección IP de la interfaz de gestión (MGT) • Dirección IPv4 o IPv6 de la interfaz • Dirección de bucle invertido • Dirección definida por el usuario en el campo de dirección de gestión Si no se indica una dirección IP de gestión, la predeterminada es la dirección MAC de la interfaz de transmisión. Se incluye el número de interfaz de la dirección de gestión especificada. También se incluye el OID de la interfaz de hardware con la dirección de gestión especificada (si se aplica). Si se ha especificado más de una dirección de gestión, se enviará en el orden especificado, empezando por el principio de la lista. Se admite un máximo de cuatro direcciones de gestión. Es un parámetro opcional que puede dejarse deshabilitado.

Mensajes de Syslog LLDP y capturas de SNMP

El cortafuegos almacena información de LLDP en las MIB, que puede supervisar un Gestor SNMP. Si desea que el cortafuegos envíe notificaciones de capturas de SNMP y mensajes de syslog acerca de eventos de LLDP, debe habilitar **SNMP Syslog Notification** en un perfil LLDP.

Conforme a RFC 5424, el protocolo de Syslog, y RFC 1157, Un protocolo simple de gestión de redes, LLDP envía mensajes de capturas de SNMP y syslog cuando hay un cambio en la MIB. Estos mensajes están limitados por frecuencia según el **Notification Interval**, un ajuste global de LLDP que se establece por defecto en 5 segundos y que se puede configurar.

Dado que los mensajes de captura de SNMP y syslog LLDP están limitados por frecuencia, es posible que parte de la información de LLDP proporcionada a esos procesos no coincida con las estadísticas de LLDP actuales cuando realice la Visualización de la información de estado del LLDP. Se trata del comportamiento normal y esperado.

Puede recibir un máximo de 5 MIB por interfaz (Ethernet o AE). Cada origen diferente tiene una MIB. Si se supera el límite, se lanza el mensaje de error `tooManyNeighbors`.

© 2020 Palo Alto Networks, Inc.

Configuración de LLDP

Para configurar el LLDP y crear un perfil de LLDP, debe ser superusuario o administrador del dispositivo (deviceadmin). Una interfaz de un cortafuegos admite un máximo de cinco peers LLDP.

STEP 1 | Habilite LLDP en el cortafuegos.

Seleccione **Network (Red)** > **LLDP** y edite la sección General de LLDP; seleccione **Enable (Habilitar)**.

STEP 2 | (Opcional) Cambie la configuración global de LLDP.

1. Para **Transmit Interval (sec) (Intervalo de transmisión [s])**, especifique el intervalo (en segundos) con el que se transmiten las LLDPDU. Default: 30 segundos. Intervalo: 1-3600 segundos.
2. Para **Transmit Delay (sec) (Retardo de transmisión [s])**, especifique el tiempo de retraso (en segundos) entre las transmisiones de LLDP enviadas después de hacer un cambio en un elemento de TLV. Este intervalo impide la inundación del segmento con LLDPDU si muchos cambios de red aumentan el número de cambios LLDP o si la interfaz provoca flaps. El **Retraso de transmisión** debe ser inferior al **Intervalo de transmisión**. Default: 2 segundos. Intervalo: 1-600 segundos.
3. Para **Hold Time Multiple (Múltiplo del tiempo de espera)**, especifique un valor que se multiplicará por el **Transmit Interval (Intervalo de transmisión)** para determinar el Tiempo de espera total de TTL. Default: 4. Intervalo: 1-100. El tiempo de espera TTL máximo es 65 535 segundos, independientemente del valor de multiplicador.
4. En **Notification Interval (Intervalo de notificaciones)**, especifique el intervalo (en segundos) con el que se transmiten los Mensajes de Syslog LLDP y capturas de SNMP cuando se producen cambios en la MIB. Default: 5 segundos. Intervalo: 1-3600 segundos.
5. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un perfil de LLDP.

Para obtener descripciones de los TLV opcionales, consulte TLV compatibles con LLDP.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **LLDP Profile (Perfil de LLDP)** y **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil de LLDP.
2. En **Mode**, seleccione **transmit-receive** (opción por defecto), **transmit-only** o **receive-only**.
3. Seleccione **SNMP Syslog Notification (Notificación Syslog SNMP)** para habilitar notificaciones de SNMP y mensajes de syslog. Si se habilita, se usa el **Notification Interval (Intervalo de notificación)**. El cortafuegos enviará ambos, una trampa SNMP y un evento de syslog, como está configurado en **Device (Dispositivo)** > **Log Settings (Configuración de log)** > **System (Sistema)** > **SNMP Trap Profile (Perfil de trampa SNMP)** y **Syslog Profile (Perfil de Syslog)**.
4. En Optional TLVs (TLV opcionales), seleccione los TLV que desea transmitir:
   - **Descripción de puerto**
   - **Nombre del sistema**
   - **Descripción del sistema**
   - **Capacidades del sistema**
5. (Opcional) Seleccione **Management Address** para añadir una o más direcciones de gestión y seleccione **Add** para añadir un nombre en **Name**.
6. Seleccione la **Interface** desde la cual obtener la dirección de gestión. Se requiere al menos una dirección de gestión si se ha activado el TLV **Management Address (Dirección de gestión)**. Si no se configura la dirección IP de gestión, el sistema usa la dirección MAC de la interfaz de transmisión como la dirección de gestión de TLV.
7. Seleccione **IPv4** o **IPv6** y, en el campo adyacente, seleccione una dirección IP en la lista de direcciones configuradas en la interfaz seleccionada o bien introduzca una.
8. Haga clic en **OK (Aceptar)**.
9. Se permiten hasta cuatro direcciones de gestión. Si ha especificado más de una **Management Address**, se enviarán en el orden especificado, empezando por la parte superior de la lista. Para

© 2020 Palo Alto Networks, Inc.

cambiar el orden de las direcciones, seleccione una dirección y use los botones **Move Up** o **Move Down**.

10. Haga clic en **OK (Aceptar)**.

STEP 4 | Asigne un perfil de LLDP a una interfaz.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz a la que asignará un perfil de LLDP.
2. Seleccione **LLDP** > **Advanced (Avanzado)**.
3. Seleccione **Enable LLDP** para asignar un perfil de LLDP a la interfaz.
4. En **Profile (Perfil)**, seleccione el perfil que ha creado. Si selecciona **None (Ninguno)**, se habilita LLDP con funcionalidades básicas: envía los tres TLV obligatorios y habilita el modo **transmit-receive (transmisión-recepción)**.

   Si desea crear un nuevo perfil, haga clic en **LLDP Profile (Perfil de LLDP)** y siga las instrucciones de los pasos a continuación.
5. Haga clic en **OK (Aceptar)**.

STEP 5 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Visualización de estados y configuración de LLDP

Realice el siguiente procedimiento para ver los estados y la configuración de LLDP.

STEP 1 | Vea la configuración global de LLDP.

Seleccione **Network (Red)** > **LLDP**.

En la pantalla General de LLDP, la casilla de verificación **Enable (Habilitar)** indica si LLDP está o no habilitado.

- Si LLDP está habilitado, se muestran los ajustes globales configurados (Intervalo de transmisión, Retraso de transmisión, Múltiple tiempo de espera e Intervalo de notificaciones).
- Si LLDP no está habilitado, se muestran los valores predeterminados de los ajustes globales.

Para acceder a las descripciones de estos valores, consulte el segundo paso de la Configuración de LLDP.

STEP 2 | Vea la información de estado de LLDP.

1. Seleccione la pestaña **State (Estado)**.
2. (Opcional) Introduzca un filtro para restringir la información que se muestra.

   Información de la interfaz:

   - **Interface (Interfaz)**: nombre de las interfaces que tienen asignados perfiles LLDP.
   - **LLDP**: estado de LLDP (habilitado o deshabilitado).
   - **Mode (Modo)**: modo LLDP de la interfaz: Tx/Rx, Tx solo o Rx solo.
   - **Profile (Perfil)**: nombre del perfil asignado a la interfaz.

   Información de transmisión:

   - **Total Transmitted (Total transmitido)**: recuento de las LLDPDU transmitidas fuera de la interfaz.
   - **Dropped Transmit (Transmisión descartada)**: número de LLDPDU que no se han transmitido fuera de la interfaz por un error. Por ejemplo, un error de longitud cuando el sistema construye un LLDPDU para la transmisión.

   Información recibida:

   - **Total Received (Total recibido)**: número de tramas LLDP recibidas en la interfaz.
   - **Dropped TLV (TLV descartada)**: número de las tramas LLDP descartadas en la recepción.

© 2020 Palo Alto Networks, Inc.

- **Errors (Errores)**: número de TLV que se recibieron en la interfaz y contenían errores. Entre los tipos de errores de TLV se incluyen: falta de uno o más TLV obligatorios, mal funcionamiento, información fuera de alcance o error de longitud.
- **Unrecognized (No reconocido)**: número de TLV recibidos en la interfaz que no reconoce el agente local de LLDP. Por ejemplo, el tipo TLV está en el intervalo de TLV reservado.
- **Aged Out (Caducado)**: número de elementos eliminados desde Receive MIB por una caducidad TTL adecuada.

STEP 3 | Ver resumen de información de LLDP para cada vecino visto en una interfaz.

1. Seleccione la pestaña **Peers**.
2. (Opcional) Si lo desea, puede incluir un filtro para restringir la información que se muestra.

   Local Interface: interfaz en el cortafuegos que detectó el dispositivo vecino.

   Remote Chassis ID: ID de bastidor del peer. Se usará la dirección MAC.

   Port ID: ID del puerto del peer.

   Name: nombre del peer.

   More info: ofrece la siguiente información del peer remoto, que se basa en TLV obligatorios y opcionales.

   - Tipo de bastidor: Dirección MAC.
   - Dirección MAC: La dirección MAC del peer.
   - Nombre del sistema: Nombre del peer.
   - Descripción del sistema: Descripción del peer.
   - Descripción de puerto: Descripción del puerto del peer.
   - Tipo de puerto: Nombre de interfaz.
   - ID de puerto: El cortafuegos usa el ifname de la interfaz.
   - Capacidades del sistema: Funcionalidades del sistema. O=Otro, P=Repetidor, B=Puente, W=LAN-Inalámbrico, R=Enrutador, T=Teléfono
   - Capacidades habilitadas: Funcionalidades habilitadas en el peer.
   - Dirección de gestión: Dirección de gestión del peer.

Borrado de estadísticas de LLDP

Puede borrar las estadísticas de LLDP para interfaces específicas.

Borre las estadísticas de LLDP para interfaces específicas.

1. Seleccione **Network (Red)** > **LLDP** > **Status (Estado)** y en la columna izquierda, seleccione una o más interfaces en las que desea borrar las estadísticas de LLDP.
2. Haga clic en **Clear LLDP Statistics (Borrar estadísticas de LLDP)** en la parte inferior de la pantalla.

© 2020 Palo Alto Networks, Inc.

BFD

El cortafuegos admite la detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) (RFC 5880), un protocolo que reconoce un fallo en la ruta bidireccional entre dos peers de enrutamiento. La detección del fallo de BFD es extremadamente rápida, lo que brinda una conmutación por error más rápida que la alcanzada por la supervisión de enlaces o las comprobaciones de enrutamiento dinámico frecuentes, como los paquetes de bienvenida o heartbeats. Los centro de datos y redes de misión crítica que requieren alta disponibilidad y una conmutación por error sumamente rápida necesitan la detección de conmutación por error sumamente rápida que ofrece BFD.

- Descripción general de BFD
- Configuración de BFD
- Referencia: detalles de BFD

Descripción general de BFD

Al habilitar BFD, se establece una sesión desde un extremo (el cortafuegos) hacia su peer BFD en el extremo de un enlace que utiliza un protocolo de enlace de tres pasos. Los paquetes de control realizan el protocolo de enlace y negocian los parámetros configurados en el perfil BFD, incluidos los intervalos mínimos en los que los peers pueden enviar y recibir paquetes de control. Los paquetes de control BFD para IPv4 e IPv6 se transmiten por el puerto UDP 3784. Los paquetes de control BFD para compatibilidad con salto entre redes se transmiten por el puerto UDP 4784. Los paquetes de control BFD transmitidos por cualquiera de los puertos se encapsulan en los paquetes UDP.

Una vez que se establece la sesión BFD, la implementación de Palo Alto Networks de BFD opera en modo asíncrono, lo que significa que ambos extremos se envían paquetes de control (que funcionan como paquetes de saludo) en el intervalo negociado. Si un peer no recibe un paquete de control dentro del período de detección (calculado como el intervalo de transmisión negociado multiplicado por un multiplicador de tiempo de detección), el peer considera la sesión como inactiva. (El cortafuegos no admite el modo de demanda, en el que los paquetes de control se envían únicamente si es necesario en lugar de periódicamente).

Cuando usted habilita BFD para una ruta estática y una sesión BFD entre el cortafuegos y el peer BFD falla, el cortafuegos elimina de las tablas RIB y FIB la ruta que falló, y permite que una ruta alternativa con una prioridad menor tome el control. Cuando usted habilita BFD para un protocolo de enrutamiento, BFD notifica al protocolo de enrutamiento que debe cambiar a una ruta alternativa al peer. Por lo tanto, el cortafuegos y peer BFD vuelven a converger en una nueva ruta.

Un perfil BFD le permite realizar la Configuración de BFD y aplicar estos ajustes a uno o más protocolos de enrutamiento o rutas estáticas en el cortafuegos. Si habilita BFD sin configurar un perfil, el cortafuegos usa su perfil BFD por defecto (con todos los ajustes por defecto). No puede cambiar el perfil BFD por defecto.

Cuando una interfaz ejecuta varios protocolos que usan diferentes perfiles BFD, BFD usa el perfil que tiene el **Desired Minimum Tx Interval** más bajo. Consulte BFD para protocolos de enrutamiento dinámico.

Los peers HA activos/pasivos sincronizan configuraciones y sesiones BFD; los peers HA activos/activos no.

BFD está estandarizado en RFC 5880. PAN-OS no admite todos los componentes de RFC 5880; consulte Componentes RFC no compatibles de BFD.

PAN-OS también admite RFC 5881, http://www.rfc-editor.org/rfc/rfc5881.txt. En este caso, BFD realiza un seguimiento de un solo salto entre dos sistemas que usan IPv4 o IPv6, de manera que los dos sistemas se conectan directamente entre sí. BFD también realiza el seguimiento de varios saltos de peers conectados por BGP. PAN-OS sigue la encapsulación de BFD según se describe en RFC 5883, https://www.rfc-editor.org/rfc/rfc5883.txt. Sin embargo, PAN-OS no admite la autenticación.

- Modelo, interfaz y soporte al cliente de BFD

© 2020 Palo Alto Networks, Inc.

- Componentes RFC no compatibles de BFD
- BFD para rutas estáticas
- BFD para protocolos de enrutamiento dinámico

Modelo, interfaz y soporte al cliente de BFD

Los siguientes modelos de cortafuegos no admiten BFD: cortafuegos PA-800 Series, PA-220 y VM-50. Los modelos que admiten una cantidad máxima de sesiones de BFD, como se enumera en la herramienta Selección de producto.

BFD se ejecuta en Ethernet física, Ethernet de agregación (Aggregated Ethernet, AE), VLAN e interfaces de túnel (VPN de sitio a sitio y LSVPN) y en subinterfaces de capa 3.

Los clientes BFD compatibles son los siguientes:

- Rutas estáticas (IPv4 e IPv6), que constan de un solo salto.
- OSPFv2 y OSPFv3 (los tipos de interfaz incluyen difusión, punto a punto y punto a multipunto).
- BGP IPv4 e IPv6 (IBGP, EBGP) consta de un solo salto o varios saltos.
- RIP (único salto).

Componentes RFC no compatibles de BFD

- Modo de demanda
- Autenticación
- El envío o la recepción de paquetes Echo; sin embargo, el cortafuegos pasará los paquetes Echo que lleguen en una interfaz de modo tap o por Virtual Wire. (Los paquetes Echo de BFD tienen la misma dirección IP para el origen y el destino).
- Secuencias de sondeo
- Control de congestión

BFD para rutas estáticas

Para usar BFD en una ruta estática, tanto el cortafuegos como el peer en el otro extremo de la ruta estática deben admitir las sesiones BFD. Una ruta estática puede tener un perfil BFD únicamente si el tipo **Next Hop (Próximo salto)** es **IP Address (Dirección IP)**.

Si una interfaz está configurada con más de una ruta estática a un peer (la sesión BFS tiene la misma dirección IP de origen y la misma dirección IP de destino), una sola sesión BFD maneja automáticamente las múltiples rutas estáticas. Este comportamiento reduce las sesiones BFD. Si las rutas estáticas tienen diferentes perfiles BDF, el perfil con el **Desired Minimum Tx Interval (Intervalo Tx mínimo deseado)** se activa.

En una implementación en la que desea configurar BFD para una ruta estática en una interfaz cliente DHCP o PPPE, debe realizar dos confirmaciones. La habilitación de BFD para una ruta estática requiere que el tipo **Next Hop (Próximo salto)** sea **IP Address (Dirección IP)**. Pero al momento de una confirmación de interfaz DHCP o PPPoE, la dirección IP de la interfaz y la dirección IP de siguiente salto (puerta de enlace por defecto) son desconocidas.

Primero debe habilitar un cliente DHCP o PPPoE para la interfaz, realizar una confirmación y esperar que el servidor DHCP o PPPoE envíen al cortafuegos la dirección IP del cliente y la dirección IP de la puerta de enlace por defecto. Luego puede configurar la ruta estática (usando la dirección de la puerta de enlace por defecto del cliente DHCP o PPPE como el siguiente salto), habilitar BFD y realizar una segunda confirmación.

© 2020 Palo Alto Networks, Inc.

BFD para protocolos de enrutamiento dinámico

Además de BFD para rutas estáticas, el cortafuegos admite BFD para los protocolos de enrutamiento BGP, OSPF y RIP.



La implementación de Palo Alto Networks de BFD de varios saltos sigue la parte de encapsulación de RFC 5883, Detección de reenvío bidireccional (BFD) para rutas de varios saltos, pero no admite la autenticación. Una solución alternativa es configurar BFD en un túnel VPN para BGP. El túnel VPN puede brindar autenticación sin la duplicación de la autenticación de BFD.

Cuando habilita BFD para las interfaces de difusión OSPFv2 o OSPFv3, OSPF establece una sesión BFD únicamente con su enrutador designado (Designated Router, DR) y el enrutador designado de respaldo (Backup Designated Router, BDR). En las interfaces de punto a punto, OSPF establece una sesión BFD con el vecino directo. En las interfaces de punto a punto, OSPF establece una sesión BFD con cada peer.

El cortafuegos no admite BFD en un OSPF o enlace virtual OSPFv3.

Cada protocolo de enrutamiento puede tener sesiones BFD independientes en una interfaz. O bien, dos o más protocolos de enrutamiento (BGP, OSPf y RIP) pueden compartir una sesión de BFD común para una interfaz.

Cuando habilita BFD para múltiples protocolos en la misma interfaz, y la dirección IP de origen y la dirección IP de destino para los protocolos también son las mismas, los protocolos comparten una sola sesión BFD, con lo cual se reducen ambas cargas de trabajo del plano de datos (CPU) y carga de trabajo en la interfaz. Si configura diferentes perfiles BFD para estos protocolos, solo se usa un perfil BFD: el que tiene el **Desired Minimum Tx Interval** más bajo. Si los perfiles tienen el mismo **Desired Minimum Tx Interval (Intervalo Tx mínimo deseado)**, se activa el perfil utilizado por la primera sesión creada. En el caso de que una ruta estática y OSPF compartan la misma sesión, debido a que una sesión estática se crea inmediatamente después de una confirmación, si bien el OSPF espera hasta que haya una adyacencia activa, el perfil de la ruta estática tiene prevalencia.

El beneficio de usar una sola sesión de BFD en estos casos es que este comportamiento utiliza recursos de manera más eficiente. El cortafuegos puede utilizar los recursos guardados para admitir más sesiones de BFD en diferentes interfaces o admitir BFD para diferentes ares de dirección IP de origen y de destino.

IPv4 e IPv6 en la misma interfaz siempre crea diferentes sesiones BFD, incluso aunque usen el mismo perfil BFD.



*Si implementa ambos BFD para el control de ruta HA y BGP, Palo Alto Networks le recomienda no implementar el BGP Graceful Restart (Reinicio correcto BGP). Cuando fallan la interfaz del peer de BFD y la supervisión de rutas, BFD **puede** eliminar las rutas afectadas de la tabla de enrutamiento y sincronizar este cambio en el cortafuegos de HA pasivo antes de que se produzca el reinicio correcto. Si decide implementar BFD para BGP, el reinicio correcto para BGP y el control de ruta HA, debe configurar BFD con un intervalo Tx mínimo deseado superior y un multiplicador de tiempo de detección superior a los valores predeterminados.*

Configuración de BFD

Tras leer la Descripción general de BFD, que incluye información sobre los modelos de cortafuegos y las interfaces compatibles, realice los siguientes pasos antes de configurar BFD:

- Configure uno o más enrutadores virtuales.
- Configure una o más rutas estáticas si está aplicando BFD a rutas estáticas.
- Configure un protocolo de enrutamiento (BGP, OSPF, OSPFv3 o RIP) si está aplicando BFD a un protocolo de enrutamiento.

© 2020 Palo Alto Networks, Inc.

La eficacia de su implementación de BFD depende de diversos factores, tales como las cargas de tráfico, las condiciones de la red, qué tan agresiva es su configuración de BFD y qué tan ocupado está el plano de datos.

STEP 1 | Cree un perfil de BFD.

Si cambia un ajuste en un perfil de BFD que una sesión de BFD existente está utilizando y confirma el cambio, antes de que el cortafuegos elimine esa sesión BFD y vuelva a crearla con el nuevo ajuste, el cortafuegos envía un paquete BFD con el estado local configurado con el administrador inactivo. El dispositivo del peer puede o no alternar el protocolo de enrutamiento o ruta estática, según la implementación del peer de RFC 5882, Sección 3.2.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **BFD Profile (Perfil BFD)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil BFD. El nombre distingue entre mayúsculas y minúsculas y debe ser único en el cortafuegos. Utilice solamente letras, números, espacios, guiones y guiones bajos.
2. Seleccione el **Mode (Modo)** en el que BFD operará:
   - **Active**: BFD inicia el envío de los paquetes de control (por defecto). Al menos uno de los peers de BFD debe estar activo; ambos pueden estar activos.
   - **Passive**: BFD espera que el peer envíe los paquetes de control y responde según corresponda.

STEP 2 | Configure los intervalos de BFD.

1. Introduzca el **Desired Minimum Tx Interval (ms)**. Este es el intervalo mínimo, en milisegundos, con el cual usted desea que el protocolo BFD (denominad BFD) envíe paquetes de control BFD; con lo cual usted está negociando el intervalo de transmisión con el peer. El mínimo en cortafuegos PA-7000 y PA-5200 Series es 50; el mínimo en cortafuegos VM-Series es 200. El máximo es 2.000; el valor por defecto es 1.000.

   Se recomienda configurar Desired Minimum Tx Interval (Intervalo Tx mínimo deseado) en 100 o más en los cortafuegos PA-7000 Series; un valor inferior a 100 puede causar fluctuaciones en la BFD.

   Si tiene múltiples protocolos de enrutamiento que usan diferentes perfiles BFD en la misma interfaz, configure los perfiles BFD con el mismo valor de Desired Minimum Tx Interval.
2. Introduzca el **Required Minimum Rx Interval (ms)**. Este es el intervalo mínimo, en milisegundos, en el cual BFD puede recibir paquetes de control BFD. El mínimo en cortafuegos PA-7000 y PA-5200 Series es 50; el mínimo en cortafuegos VM-Series es 200. El máximo es 2.000; el valor por defecto es 1.000.

   Se recomienda configurar Required Minimum Rx Interval (Intervalo Rx mínimo necesario) en 100 o más en los cortafuegos PA-7000 Series; un valor inferior a 100 puede causar fluctuaciones en la BFD.

STEP 3 | Configure el multiplicador de tiempo de detección BFD.

Introduzca el **Detection Time Multiplier**. El sistema local calcula el tiempo de detección como el **Detection Time Multiplier (Multiplicador de tiempo de detección)** recibido del sistema remoto, multiplicado por el intervalo de transmisión acordado del sistema remoto (el valor más alto de **Required Minimum Rx Interval [Intervalo Rx mínimo necesario]** y el último **Desired Minimum Tx Interval [Intervalo Tx mínimo deseado]** recibido). Si BFD no recibe un paquete de control BFD desde su peer antes de que se agote el tiempo de detección, se produjo un fallo. El intervalo va de 2 a 50 y el valor predeterminado es 3.

© 2020 Palo Alto Networks, Inc.

Por ejemplo, un intervalo de transmisión de 300 ms x 3 (multiplicador del tiempo de detección) = 900 ms de tiempo de detección.



Al configurar un perfil BFD, tenga en cuenta que el cortafuegos es un dispositivo basado en la sesión generalmente en el extremo de una red o centro de datos, y puede tener enlaces más lentos que un enrutador dedicado. Por lo tanto, el cortafuegos probablemente necesita un intervalo más prolongado y un multiplicador más alto de lo que permiten los ajustes más rápidos. Un tiempo de detección demasiado breve puede causar falsas detecciones de fallos cuando el problema es en realidad la congestión del tráfico.

STEP 4 | Configure el tiempo de retención de BFD.

Introduzca el **Hold Time (ms)**. Esta es la demora, en milisegundos, una vez que un enlace se activa antes de que BFD transmita los paquetes de control de BFD. **Hold Time (Tiempo de espera)** se aplica al modo activo de BFD únicamente. Si el BFD recibe paquetes de control BFD durante el **tiempo de espera**, los ignora. El intervalo es de 0-120000. El valor por defecto de 0, que significa que no se utiliza el **tiempo de espera** de transmisión; el BFD envía y recibe paquetes de control BFD de inmediato después de que establece el enlace.

STEP 5 | (Opcional: para una implementación de IPv4 de BGP únicamente) configure ajustes relacionados con el salto para el perfil BFD.

1. Seleccione **Multihop (Múltiples pasos)** para habilitar BFD en varios saltos de BGP.
2. Introduzca el **Minimum Rx TTL**. Este es el valor mínimo de período de vida (cantidad de saltos) que BFD aceptará (recibirá) en un paquete de control de BFD cuando BGP admite varios saltos de BFD. (El intervalo es 1-254; no hay valor por defecto).

   El cortafuegos descarta el paquete si recibe un TTL menor que el **Minimum Rx TTL (TTL Rx mínimo)** configurado. Por ejemplo, si el peer está a 5 saltos de distancia y el peer transmite un paquete BFD con un TTL de 100 al cortafuegos, y si el valor **Minimum Rx TTL (TTL Rx mínimo)** para el cortafuegos está configurado en 96 o más, el cortafuegos descarta el paquete.

STEP 6 | Guarde el perfil BFD.

Haga clic en **OK (Aceptar)**.

STEP 7 | (Opcional) Habilite BFD para una ruta estática.

el cortafuegos y el peer en el otro extremo de la ruta estática deben admitir las sesiones BFD.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual donde esté configurada la ruta estática.
2. Seleccione la pestaña **Static Routes**.
3. Seleccione la pestaña **IPv4** o **IPv6**.
4. Seleccione la ruta estática donde desea aplicar el BFD.
5. Seleccione una **Interface** (incluso aunque esté usando una dirección DHCP). El ajuste de **Interface** no puede ser **None**.
6. Para **Next Hop**, seleccione **IP Address** e introduzca la dirección IP si aún no la especificó.
7. En **BFD Profile**, seleccione una de las opciones siguientes:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.



La selección de None (Disable BFD) (Ninguno [deshabilitar BFD]) deshabilita BFD para la ruta estática.

© 2020 Palo Alto Networks, Inc.

8. Haga clic en **OK (Aceptar)**.

Una columna BFD en la pestaña **IPv4** o **IPv6** indica el perfil BFD configurado para la ruta estática.

STEP 8 | (Opcional) Habilite BFD para todas las interfaces BGP o para un solo peer BGP.

Si habilita o deshabilita BFD de forma global, todas las interfaces que ejecutan BGP se desactivan y se vuelven a activar con la función BFD. Esto puede interrumpir todo el tráfico BGP. Cuando habilita BFD en la interfaz, el cortafuegos detendrá la conexión BGP al peer para programar BFD en la interfaz. El dispositivo del peer notará la caída de la conexión de BGP, lo cual podrá resultar en una nueva convergencia. Habilite BFD en las interfaces BGP durante un horario de menor demanda, cuando la nueva convergencia no afecte el tráfico de producción.

Si implementa ambos BFD para el control de ruta HA y BGP, Palo Alto Networks le recomienda no implementar el BGP Graceful Restart (Reinicio correcto BGP). Cuando la interfaz del peer de BFD falla y el control de ruta falla, BFD puede eliminar las rutas afectadas de la tabla de rutas y sincronizar este cambio con el cortafuegos HA pasivo antes de que el reinicio correcto surta efecto. Si decide implementar BFD para BGP, el reinicio correcto para BGP y el control de ruta HA, debe configurar BFD con un intervalo Tx mínimo deseado superior y un multiplicador de tiempo de detección superior a los valores predeterminados.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, y seleccione el enrutador virtual donde está configurado BGP.
2. Seleccione la pestaña **BGP**.
3. (Opcional) Para aplicar la BFD a todas las interfaces de BGP del enrutador virtual, seleccione una de las siguientes opciones en la lista **BFD** y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   La selección de None (Disable BFD) (Ninguno [Deshabilitar BFD]) deshabilita BFD para todas las interfaces BGP en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz BGP.
4. (Opcional) Para habilitar BFD para una sola interfaz de peer BGP (con lo cual se cancela el ajuste de **BFD** para BGP, siempre y cuando no esté deshabilitado), realice las siguientes tareas:
   1. Seleccione la pestaña **Peer Group (Grupo de peers)**.
   2. Seleccione un grupo de peers.
   3. Seleccione un peer.
   4. En la lista **BFD**, seleccione una de las siguientes opciones:

      default (predeterminado): usa únicamente los ajustes por defecto.

      Inherit-vr-global-setting (valor por defecto): el peer BGP hereda el perfil BFD que usted seleccionó globalmente para BGP para el enrutador virtual.

      Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

      La selección de Disable BFD (Deshabilitar BFD) deshabilita BFD para el peer BGP.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

Una columna BFD en BGP - Grupo de peers/Lista de peers indica el perfil BFD configurado para la interfaz.

STEP 9 | (Opcional) Habilite BFD para OSPF u OSPFv3 globalmente para una interfaz OSPF.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual donde OSPF u OSPFv3 están configurados.
2. Seleccione la pestaña **OSPF** u **OSPFv3**.
3. (Opcional) En la lista **BFD**, seleccione una de las siguientes opciones para habilitar la BFD en todas las interfaces de OSPF o de OSPF v. 3 y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   La selección de None (Disable BFD) (Ninguno [Deshabilitar BFD]) deshabilita BFD para todas las interfaces OSPF en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz OSPF.
4. (Opcional) Para habilitar BFD para una sola interfaz de peer OSPF (con lo cual se cancela el ajuste de **BFD** para OSPF, siempre y cuando no esté deshabilitado), realice las siguientes tareas:
   1. Seleccione la pestaña **Areas** y seleccione un área.
   2. En la pestaña **Interface (Interfaz)**, seleccione una interfaz.
   3. En la lista **BFD**, seleccione una de las siguientes opciones para configurar la BFD en el peer de OSPF especificado:

      default (predeterminado): usa únicamente los ajustes por defecto.

      Inherit-vr-global-setting (valor por defecto): el peer OSPF hereda el ajuste de **BFD** para OSPF u OSPFv3 para el enrutador virtual.

      Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

      La selección de Disable BFD deshabilita BFD para la interfaz OSPF u OSPFv3.
   4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **OK (Aceptar)**.

Una columna BFD en la pestaña de OSPF **Interface** indica el perfil BFD configurado para la interfaz.

STEP 10 | (Opcional) Habilite BFD para RIP globalmente o para una sola interfaz RIP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, y seleccione el enrutador virtual donde está configurado RIP.
2. Seleccione la pestaña RIP.
3. (Opcional) En la lista **BFD**, seleccione una de las siguientes opciones para habilitar la BFD en todas las interfaces de RIP del enrutador virtual y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   La selección de None (Disable BFD) (Ninguno [Deshabilitar BFD]) deshabilita BFD para todas las interfaces RIP en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz RIP.
4. (Opcional) Para habilitar BFD para una sola interfaz RIP (con lo cual se cancela el ajuste de **BFD** para RIP, siempre y cuando no esté deshabilitado), realice las siguientes tareas:

© 2020 Palo Alto Networks, Inc.

1. Seleccione la pestaña **Interfaces** y seleccione una interfaz.
2. En la lista **BFD**, seleccione una de las siguientes opciones:

   default: usa únicamente los ajustes por defecto.

   Inherit-vr-global-setting (heredar ajuste global para el enrutador virtual) (valor por defecto): la interfaz RIP hereda el perfil BFD que usted seleccionó globalmente para RIP para el enrutador virtual.

   Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

   La selección de None (Disable BFD) deshabilita BFD para la interfaz RIP.
3. Haga clic en **OK (Aceptar)**.

5. Haga clic en **OK (Aceptar)**.

La columna BFD en la pestaña **Interface** indica el perfil BFD configurado para la interfaz.

STEP 11 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

STEP 12 | Visualización de resumen y detalles de BFD

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, busque el enrutador virtual de su interés y haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. Seleccione la pestaña **BFD Summary Information (Información de resumen BFD)** para ver la información resumida, tal como el estado de BFD y las estadísticas del tiempo de ejecución.
3. (Opcional) Seleccione **details (detalles)** en la fila de la interfaz en la que está interesado para ver Referencia: detalles de BFD.

STEP 13 | Supervise los perfiles de BFD a los que hace referencia una configuración de enrutamiento; supervise las estadísticas de BFD, el estado y la condición.

Use los siguientes comandos operativos de CLI:

- show routing bfd active-profile [<name>]
- **show routing bfd details [interface**<*name*>**][local-ip**<*ip*>**][multihop][peer-ip** <*ip*>**][session-id][virtual-router**<*name*>**]**
- show routing bfd drop-counters session-id <session-id>
- **show counter global | match bfd**

STEP 14 | (Opcional) Borre los contadores de transmisión, recepción y descarte de BFD.

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | (Opcional) Borre las sesiones de BFD para la depuración.

```
clear routing bfd session-state session-id all | <1-1024>
```

Referencia: Detalles de BFD

Para ver la siguiente información BFD de un enrutador virtual, puede consultar el paso Visualización de resumen y detalles de BFD.

© 2020 Palo Alto Networks, Inc.

Nombre	Valor (ejemplo)	Description (Descripción)
Session ID (ID de sesión)	1	Número de ID de la sesión BFD.
Interface (Interfaz)	ethernet1/12	Interfaz que seleccionó donde BFD se está ejecutando.
Protocolo	STATIC(IPV4) OSPF	Ruta estática (familia de dirección IP de ruta estática) y/o protocolo de enrutamiento dinámico que está ejecutando BFD en la interfaz.
Dirección IP local	10.55.55.2	Dirección IP de la interfaz.
Dirección IP vecina	10.55.55.1	Dirección IP del vecino de BFD.
Perfil BFD	valor por defecto *(Esta sesión BFD tiene varios perfiles BFD. El "intervalo de Tx deseado mínimo [ms]" más bajo se utiliza para seleccionar el perfil efectivo).	Nombre del perfil BFD aplicado a la interfaz. Debido a que la interfaz de muestra tiene una ruta estática y OSPF que ejecuta BFD con diferentes perfiles, el cortafuegos utiliza el perfil con el **intervalo de Tx deseado mínimo** más bajo. En este ejemplo, el perfil utilizado es el perfil por defecto.
Estado (local/remoto)	activo/activo	Estados de BFD de los peers de BFD locales y remotos. Los estados posibles son administrador inactivo, inactivo, inicializado y activo.
Tiempo de activación	2 h 36 m 21 s 419 ms	Período de tiempo que BFD estuvo activo (horas, minutos, segundos y milisegundos).
Discriminador (local/ remoto)	1391591427/1	Discriminadores para peers BFD locales y remotos.
Modo	Activo	Modo en el que BFD está configurado en la interfaz: Activo o pasivo.
Modo de demanda	Disabled (Deshabilitado)	PAN-OS no admite el modo de demanda BFD, por lo cual siempre está en estado deshabilitado.
Multihop	Disabled (Deshabilitado)	Pasos múltiples de BFD: Habilitado o deshabilitado.
Multihop TTL		TTL de múltiples pasos; el intervalo es 1-254. El campo está vacío si Multihop está deshabilitado.
Local Diag Code	0 (sin diagnóstico)	Los códigos de diagnóstico indican el motivo del último cambio de estado del sistema local: 0: sin diagnóstico 1: vencimiento del tiempo de detección de control

© 2020 Palo Alto Networks, Inc.

Nombre	Valor (ejemplo)	Description (Descripción)
		2: error de la función Echo 3: sesión de señalización de vecino inactiva 4: restablecimiento del plano de reenvío 5: ruta inactiva 6: ruta concatenada inactiva 7: función administrativa inactiva 8: ruta concatenada inversa inactiva
Last Received Remote Diag Code	0 (sin diagnóstico)	Último código de diagnóstico recibido del peer BFD.
Tiempo de espera de transmisión	0 ms	Tiempo de espera (en milisegundos) luego de que un enlace se activa antes de que BFD transmita los paquetes de control de BFD. Un tiempo de espera de 0 ms significa que se transmitirá inmediatamente. El intervalo es de 0-120.000 ms.
Received Min Rx Interval	1000 ms	Intervalo de Rx mínimo recibido del peer; el intervalo en el cual el peer BFD puede recibir paquetes de control. El valor máximo es de 2000 ms.
Negotiated Transmit Interval	1000 ms	El intervalo de transmisión (en milisegundos) que los peers de BFD han acordado para enviarse paquetes de control BFD mutuamente. El valor máximo es de 2000 ms.
Received Multiplier	3	Valor de multiplicador de tiempo de detección recibido del peer BFD. El tiempo de transmisión multiplicado por el multiplicador es igual al tiempo de detección. Si BFD no recibe un paquete de control BFD desde su peer antes de que se agote el tiempo de detección, se produjo un fallo. El intervalo es de 2-50.
Detect Time (exceeded)	3000ms (0)	Tiempo de detección calculado (intervalo de transmisión negociado multiplicado por el multiplicador) y la cantidad de milisegundos que se excedió el tiempo de detección.
Tx Control Packets (last)	9383 (420 ms atrás)	Cantidad de paquetes de control BFD transmitidos (y tiempo desde que BFD transmitió el paquete de control más reciente).
Rx Control Packets (last)	9384 (407 ms atrás)	Cantidad de paquetes de control BFD recibidos (y tiempo desde que BFD recibió el paquete de control más reciente).
Agent Data Plane	Ranura 1 - DP 0	En los cortafuegos de la serie PA-7000, el CPU del plano de datos que se asignó para manejar los paquetes para esta sesión BFD.

© 2020 Palo Alto Networks, Inc.

Nombre	Valor (ejemplo)	Description (Descripción)
Errores	0	Cantidad de errores de BFD.
Último paquete que causó el cambio de estado		
versión	1	Versión de BFD.
Poll Bit	0	Bit de sondeo de BFD; 0 indica que no está configurado.
Desired Min Tx Interval	1000 ms	Intervalo de transmisión mínimo deseado del último paquete que causó un cambio de estado.
Required Min Rx Interval	1000 ms	Intervalo de recepción mínimo necesario del último paquete que causó un cambio de estado.
Detect Multiplier	3	Multiplicador de detección del último paquete que causó un cambio de estado.
My Discriminator	1	Discriminador remoto. Un discriminador es un valor único distinto de cero que los peers utilizan para distinguir varias sesiones BFD entre sí.
Your Discriminator	1391591427	Discriminador local. Un discriminador es un valor único distinto de cero que los peers utilizan para distinguir varias sesiones BFD entre sí.
Diagnostic Code	0 (sin diagnóstico)	Código de diagnóstico del último paquete que causó un cambio de estado.
Length	24	Extensión del paquete de control de BFD en bytes.
Demand Bit	0	PAN-OS no admite el modo de demanda BFD, por lo cual el bit de demanda siempre está configurado en 0 (deshabilitado).
Final Bit	0	PAN-OS no admite la secuencia de sondeo, por lo cual el bit final siempre está configurado en 0 (deshabilitado).
Multipoint Bit	0	Este bit está reservado para futuras extensiones de punto a multipunto para BFD. Debe ser cero en la transmisión y la recepción.
Control Plane Independent Bit	1	• Si está configurado en 1, la implementación BFD del sistema de transmisión no comparte el destino con su plano de control (es decir, BFD se implementa en el plano de reenvío y puede continuar funcionando a pesar de las alteraciones del plano de control). En PAN-OS, este bit siempre está configurado en 1. • Si está configurado en 0, la implementación de BFD del sistema de transmisión comparte el destino con su plano de control.

© 2020 Palo Alto Networks, Inc.

Nombre	Valor (ejemplo)	Description (Descripción)
Authentication Present Bit	0	PAN-OS no admite la autenticación BFD, por lo cual el bit de presencia de autenticación siempre está configurado en 0.
Required Min Echo Rx Interval	0 ms	PAN-OS no admite la función Echo de BFD, por lo cual este valor siempre será 0 ms.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión y tiempos de espera de sesión

Esta sección describe la configuración global que afecta a las sesiones TCP, UDP e ICMPv6, además de IPv6, NAT64, sobresuscripción NAT, tamaño de trama gigante, MTU, vencimiento acelerado y autenticación del portal autenticación. También hay un ajuste (Rematch Sessions [Reanalizar sesiones establecidas]) que le permite aplicar las políticas de seguridad recién configuradas a las sesiones que ya están en curso.

El primero de los siguientes temas ofrece breves resúmenes de la capa de transporte del modelo OSI, TCP, UDP e ICMP. Para obtener más información acerca de los protocolos, consulte sus RFC respectivos. El resto de temas describen la configuración y los tiempos de espera de sesión.

- Sesiones de capa de transporte
- TCP
- UDP
- ICMP
- Control de tipos y códigos específicos de ICMP o ICMPv6
- Configuración de los tiempos de espera de sesión
- Política de distribución de sesiones
- Configuración de los ajustes de sesión
- Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP

Sesiones de capa de transporte

Una sesión de red es un intercambio de mensajes que se produce entre dos o más dispositivos de comunicación, durante cierto periodo de tiempo. Cada sesión se establece, y luego se anula cuando termina. En las tres capas del modelo OSI tienen lugar distintos tipos de sesiones: la capa de transporte, la capa de sesión y la capa de aplicación.

La capa de transporte funciona en la capa 4 del modelo OSI y proporciona una entrega punto a punto, fiable o no fiable, y un control del flujo de los datos. Los protocolos de Internet que implementan sesiones en la capa de transporte incluyen el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP).

TCP

El protocolo de control de transmisión (TCP) (RFC 793) es uno de los protocolos principales del conjunto de protocolos de Internet (IP), y está tan extendido que a menudo se le hace referencia junto a IP como *TCP/IP*. Se considera que el TCP es un protocolo de transporte fiable, ya que ofrece comprobación de errores mientras transmite y recibe segmentos, reconoce los segmentos recibidos y reorganiza los segmentos recibidos en un orden incorrecto. TCP también solicita y ofrece la retransmisión de segmentos que faltaban. TCP se basa en el estado y conexión, lo que significa que la conexión entre el remitente y el receptor se establece durante la duración de la sesión. TCP ofrece un control del flujo de paquetes para que pueda gestionar la gestión de las redes.

TCP realiza un protocolo de enlace durante la configuración de la sesión para iniciar y reconocer una sesión. Cuando se han transferido los datos, la sesión se cierra de manera ordenada: cada lado transmite un paquete FIN y lo reconoce con un paquete ACK. El protocolo de enlace que inicia la sesión TCP suele ser un protocolo de enlace en tres pasos (un intercambio de tres mensajes) entre el iniciador y el agente de escucha, o puede ser una variación, como un protocolo de enlace en cuatro o cinco pasos o abierto simultáneo. En Descarte de paquetes de protocolo de enlace dividido de TCP se explica el proceso de Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP.

© 2020 Palo Alto Networks, Inc.

Entre las aplicaciones que usan TCP como protocolo de transporte se incluyen el protocolo de transferencia de hipertexto (HTTP), protocolo HTTP seguro (HTTPS), protocolo de transferencia de archivos (FTP), protocolo simple de transferencia de correo (SMTP), Telnet, protocolo de oficina de correos versión 3 (POP3), protocolo de acceso a mensajes de Internet (IMAP) y shell seguro (SSH).

Los siguientes temas tienen información detallada sobre la implementación PAN-OS de TCP.

- Temporizadores de TCP semicerrado y de Tiempo de espera TCP
- Temporizador RST sin verificar
- Descarte de paquetes de protocolo de enlace dividido de TCP
- Tamaño de segmento máximo (MSS)

Puede utilizar los Perfiles de protección de zonas en el cortafuegos para configurar la protección de ataque basado en paquetes y descartar paquetes IP, TCP y IPv6 con características indeseables o descartar opciones indeseables de los paquetes antes de permitirlos en la zona. También puede configurar la protección contra inundaciones especificando la tasa de conexiones por segundo de UDP (que no coinciden con una sesión existente) que activan una alarma, provocan que el cortafuegos descarte paquetes SYN o utilice cookies de SYN de manera aleatoria, y causan que el cortafuegos descarte paquetes SYN que superan la tasa máxima.

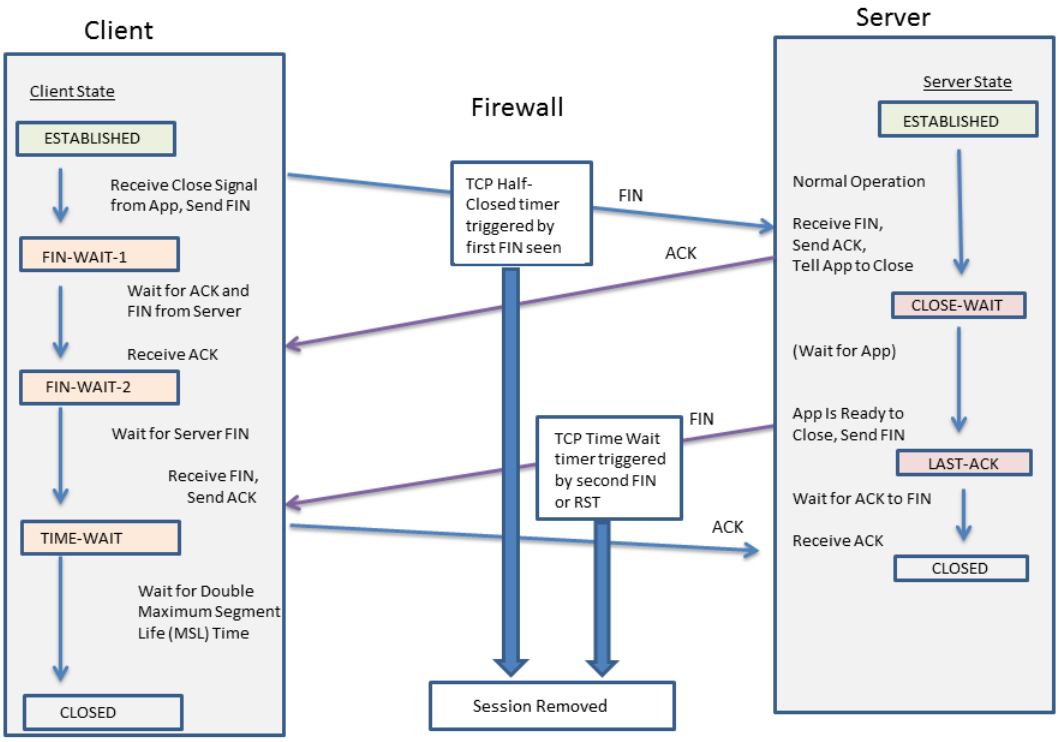
Temporizadores de TCP semicerrado y de Tiempo de espera TCP

El procedimiento de terminación de la conexión TCP usa un temporizador semicerrado TCP, que se activa con el primer FIN que detecta el cortafuegos para una sesión. El temporizador se denomina TCP semicerrado porque solo una parte de la conexión ha enviado un FIN. Un segundo temporizador, el de tiempo de espera TCP, se activa después de recibir el segundo FIN o RST.

Si en el cortafuegos solo se activara un temporizador con el primer FIN, un ajuste demasiado corto cerraría prematuramente las sesiones semicerradas. Por otro lado, un ajuste demasiado alto haría crecer demasiado la tabla de la sesión, y probablemente agotaría todas las sesiones. Dos temporizadores le permiten tener un temporizador TCP semicerrado relativamente largo y un temporizador de tiempo de espera TCP corto, lo que hace vencer rápidamente las sesiones totalmente cerradas y controla el tamaño de la tabla de sesión.

La siguiente ilustración muestra el momento en que dos temporizadores del cortafuegos se activan durante el procedimiento de terminación de la conexión TCP.

© 2020 Palo Alto Networks, Inc.



El temporizador de tiempo de espera de TCP debe definirse con un valor inferior al temporizador semicerrado TCP por los siguientes motivos:

- Mientras más tiempo se permita tras ver el primer FIN, más tiempo tiene la otra parte de la conexión para cerrar por completo la sesión.
- El tiempo de espera más corto se debe a que no hay necesidad de que la sesión permanezca abierta durante mucho tiempo tras ver el segundo FIN o RST. Un tiempo de espera más breve libera los recursos antes, pero deja tiempo para que el cortafuegos vea la confirmación final y la posible retransmisión de otros datagramas.

Si configura un temporizador de tiempo de espera TCP con un valor más alto que el del TCP semicerrado, se aceptará la confirmación, pero en la práctica el temporizador de tiempo de espera TCP no superará el valor de TCP semicerrado.

Los temporizadores pueden definirse globalmente o por aplicación. Los ajustes globales se utilizan para todas las aplicaciones de forma predeterminada. Si configura las temporizadores de espera TCP en el nivel de aplicación, estos ajustes sustituirán a los ajustes globales.

Temporizador RST sin verificar

Si el cortafuegos recibe un paquete a RST que no puede comprobarse (porque tiene un número de secuencia inesperado con la ventana TCP o tiene una ruta asimétrica), el temporizador de RST sin verificar controla el vencimiento de la sesión. Cambia de forma predeterminada a 30 segundos, el intervalo es de 1-600 segundos. El temporizador RST sin verificar ofrece una medida de seguridad adicional, que se explica en el segundo párrafo que aparece a continuación.

Un paquete RST tendrá uno de las tres resultados posibles:

- El paquete RST queda fuera de la ventana TCP y se omite.

© 2020 Palo Alto Networks, Inc.

- El paquete RST queda dentro de la ventana TCP pero no tiene el número de secuencia esperado, por lo que queda sin verificar y está sujeto al ajuste de temporizador RST sin verificar. Este comportamiento evita los ataques de denegación de servicio (DoS), en los que se intenta interrumpir las sesiones existentes enviando paquetes RST aleatorios al cortafuegos.
- El paquete RST queda dentro de la ventana TCP y tiene el número de secuencia exacto esperado, por lo que queda sujeto al ajuste de temporizador de tiempo de espera RST.

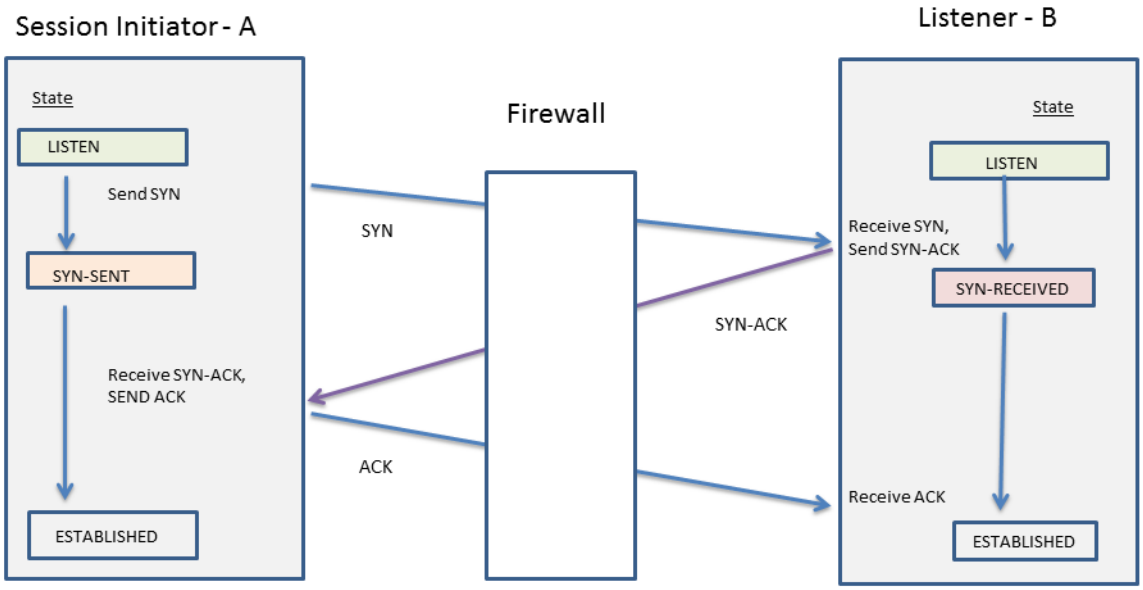
Descarte de paquetes de protocolo de enlace dividido de TCP

La opción **Split Handshake (Protocolo de enlace dividido)** en un perfil de protección de zona evitará que se establezca una sesión TCP si el procedimiento de establecimiento de sesión no utiliza el protocolo de enlace de tres pasos reconocido, sino una variación, como un protocolo de enlace dividido en cuatro o cinco pasos, o un procedimiento abierto simultáneo.

El cortafuegos del última generación de Palo Alto Networks gestiona correctamente sesiones y todos los procesos de capa 7 para el protocolo de enlace dividido y un establecimiento de sesión abierta simultánea sin habilitar la opción **Split Handshake**. Sin embargo, la opción **Split Handshake (Protocolo de enlace dividido)** (que origina un descarte del protocolo de enlace dividido de TCP) pasa a estar disponible. Cuando se configura la opción de **Split Handshake (Protocolo de enlace dividido)** para un perfil de protección de zona y el perfil se aplica a una zona, las sesiones TCP para las interfaces de esa zona deben establecerse utilizando un protocolo de enlace estándar de tres direcciones; no se permiten las variaciones.

La opción **Split Handshake (Protocolo de enlace dividido)** está deshabilitada de manera predeterminada.

A continuación se ilustra el protocolo de enlace en tres pasos estándar usado para establecer una sesión TCP con un cortafuegos PAN-OS entre el iniciador (normalmente un cliente) y el agente de escucha (normalmente un servidor).



La opción **Split Handshake** está configurada para un perfil de Protección de zona que está asignado a una zona. Una interfaz que forme parte de la zona descarta cualquier paquete de sincronización (SYN) enviado desde el servidor, evitando así las siguientes variaciones de protocolos de enlace. La letra A en la figura representa al iniciador de la sesión y la B, al agente de escucha. Cada segmento numerado del protocolo de enlace tiene una flecha que indica la dirección del segmento desde el remitente hasta el destinatario, y cada segmento indica el ajuste de control de bits.

© 2020 Palo Alto Networks, Inc.

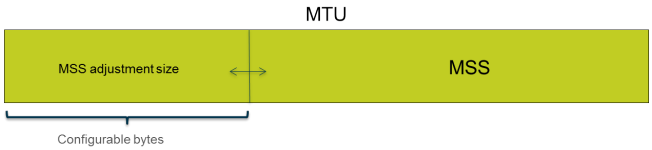
4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

Puede garantizar la Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP.

Tamaño de segmento máximo (MSS)

La unidad de transmisión máxima (maximum transmission unit, MTU) es un valor que indica la cantidad más grande de bytes que pueden transmitirse en un solo paquete TCP. La MTU incluye la extensión de los encabezados, por lo que la MTU menos la cantidad de bytes de los encabezados es igual al tamaño máximo del segmento (maximum segment size, MSS), que es la cantidad máxima de bytes de datos que pueden transmitirse en un solo paquete.

Un tamaño de ajuste de MSS configurable (se muestra a continuación) permite a su cortafuegos pasar el tráfico que tiene encabezados más extensos de lo que permite el ajuste por defecto. La encapsulación añade longitud a los encabezados, por lo que puede aumentar el tamaño de ajuste MSS para habilitar bytes, por ejemplo, para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.



Si el bit de no fragmentar (don't fragment, DF) se configura para un paquete, resulta especialmente útil tener un tamaño de ajuste de MSS mayor y un MSS menor, a fin de que los encabezados más extensos no generen una extensión de paquete que exceda la MTU permitida. Si se configuró el bit DF y se superó la MTU, los paquetes más grandes de descartarán.

Puede configurar el cortafuegos globalmente para fragmentar los paquetes IPv4 que excedan la MTU de la interfaz de salida, incluso cuando el bit de DF esté configurado en el paquete. Habilite esto para las interfaces físicas de capa 3 y las interfaces de túnel IPSec con el comando de la CLI ***debug dataplane set ip4-df-ignore yes****. Restaure el cortafuegos al comportamiento predeterminado mediante el comando de la CLI* ***debug dataplane set ipv4-df-ignore no****.*

El cortafuegos admite un tamaño de ajuste de MSS configurable para direcciones IPv4 e IPv6 en los siguientes tipos de interfaz de capa 3: Ethernet, subinterfaces, Ethernet de agregación (AE), VLAN y bucle invertido. El tamaño de ajuste de MSS de IPv6 se aplica únicamente si IPv6 está habilitada en la interfaz.

Si IPv4 e IPv6 están habilitadas en una interfaz y el tamaño de ajuste de MSS difiere entre los dos formatos de dirección IP, se usa el valor de MSS correspondiente al tipo de IP para el tráfico TCP.

© 2020 Palo Alto Networks, Inc.

Para las direcciones IPv4 e IPv6, el cortafuegos permite extensiones de encabezado TCP mayores de lo previsto. En el caso en que un paquete TCP tiene un encabezado más extenso de lo previsto, el cortafuegos elige para el tamaño de ajuste de MSS el mayor de los siguientes dos valores:

- El tamaño de ajuste de MSS configurado.
- La suma de la extensión del encabezado TCP (20) + la extensión de los encabezados IP en TCP SYN.

Este comportamiento significa que el cortafuegos cancela el tamaño de ajuste de MSS configurado si es necesario. Por ejemplo, si configura un tamaño de ajuste de MSS de 42, se prevé que el MSS sea igual a 1458 (el tamaño de MTU por defecto menos el tamaño de ajuste [1500 - 42]). Sin embargo, el paquete TCP tiene 4 bytes adicionales de opciones IP en el encabezado, por lo que el tamaño de ajuste (20+20+4) es igual a 44 que es mayor que el tamaño de ajuste de MSS configurado de 42. El MSS resultante es 1500-44=1456 bytes, menor de lo esperado.

Para configurar el tamaño de ajuste de MSS, consulte Configuración de los ajustes de sesión.

UDP

El protocolo de datagramas de usuario (UDP) (RFC 768) es otro de los principales protocolos del conjunto IP, y ofrece una alternativa al TCP. El UDP es independiente del estado y la conexión en el sentido de que no hay un protocolo para establecer sesión ni ninguna conexión entre el remitente y el receptor; los paquetes pueden tomar distintas rutas para llegar a un único destino. UDP no se considera un protocolo fiable porque no ofrece reconocimientos, comprobación de errores, retransmisión ni reorganización de datagramas. Al no tener la carga de trabajo necesaria para ofrecer estas funciones, UDP tiene una latencia reducida y es más rápido que TCP. UDP es conocido como el protocolo de menor esfuerzo, sin ningún mecanismo o forma de garantizar que los datos llegarán a su destino.

Un datagrama UDP se encapsula en un paquete IP. Aunque UDP usa una suma de comprobación para saber la integridad de los datos, no realizará ninguna comprobación de errores a nivel de la interfaz de red. Se asume que la comprobación de errores no es necesaria o que la realiza la aplicación en lugar del propio UDP. UDP no tiene ningún mecanismo para gestionar el control de flujo de paquetes.

UDP a menudo se usa con aplicaciones que requieren velocidades más altas y una entrega en tiempo real sensible al tiempo, como voz sobre IP (VoIP), transmisión de audio y vídeo y los juegos en línea. UDP se basa en las transacciones, por lo que también se usa para aplicaciones que responden a pequeñas consultas de muchos clientes, como el sistema de nombres de dominio (DNS) y el protocolo trivial de transferencia de archivos (TFTP).

Utilice Perfiles de protección de zonas para configurar la protección contra inundaciones y especificar la tasa de conexiones por segundo de UDP (que no coinciden con una sesión existente) que activan una alarma, provocan que el cortafuegos descarte paquetes UDP de manera aleatoria y causan que el cortafuegos descarte paquetes UDP que superan la tasa máxima. (A pesar de que el UDP es un protocolo sin conexión, el cortafuegos rastrea los datagramas UDP en los paquetes IP en función de las sesiones; por lo tanto, si el paquete UDP no coincide con una sesión existente, se considera una nueva sesión y se cuenta como una conexión en los umbrales).

ICMP

El protocolo de mensajes de control de Internet (ICMP) (RFC 792) es otro de los protocolos principales del conjunto de protocolos de Internet (IP), y opera en la capa de red del modelo OSI. El ICMP se usa para diagnóstico y control; para enviar mensajes de error sobre operaciones de IP o mensajes sobre servicios solicitados o el alcance de un host o enrutador. Hay utilidades de red como traceroute y ping que se implementan mediante varios mensajes ICMP.

ICMP es un protocolo sin conexión que no abre ni mantiene sesiones reales. Sin embargo, los mensajes ICMP entre dos dispositivos pueden considerarse una sesión.

© 2020 Palo Alto Networks, Inc.

Los cortafuegos de Palo Alto Networks admiten ICMPv4 e ICMPv6. Puede controlar los paquetes ICMPv4 e ICMPv6 de varias maneras:

- Cree Reglas de la política de seguridad basadas en paquetes ICMP e ICMPv6 y seleccione la aplicación **icmp** o **ipv6-icmp** en la regla.
- Controle la Límite de tasa ICMPv6 cuando realice la Configuración de los ajustes de sesión.
- Utilice Perfiles de protección de zonas para configurar la protección contra inundaciones, especifique la tasa de conexiones por segundo de ICMP o ICMPv6 (que no coincidan con una sesión existente) que activan una alarma, active el cortafuegos para que descarte paquetes ICMP o ICMPv6 de manera aleatoria y provoque que el cortafuegos descarte paquetes ICMP o ICMPv6 que superen la tasa máxima.
- Utilice Perfiles de protección de zonas para configurar la protección de ataques basada en paquetes:
  - En el caso del ICMP, puede descartar determinados tipos de paquetes o suprimir el envío de determinados paquetes.
  - En el caso de los paquetes ICMPv6 (tipos 1, 2, 3, 4 y 137), puede especificar que el cortafuegos utilice la clave de la sesión de ICMP para encontrar una coincidencia con la regla de la política de seguridad, lo que determina si se permite o no el paquete ICMPv6. (El cortafuegos utiliza la regla de la política de seguridad y anula el comportamiento predeterminado de utilizar el paquete integrado para determinar una coincidencia con la sesión). Cuando el cortafuegos descarta paquetes ICMPv6 que coinciden con una regla de la política de seguridad, el cortafuegos registra los detalles en los logs de tráfico.

Reglas de la política de seguridad basadas en paquetes ICMP e ICMPv6

El cortafuegos reenvía paquetes ICMP o ICMPv6 solo si una regla de la política de seguridad permite la sesión (como en el caso de otros tipos de paquetes). El cortafuegos determina una coincidencia con la sesión de dos maneras, en función de si el paquete es un paquete de error o un paquete de redirección ICMP o ICMPv6 en lugar de un paquete de información ICMP o ICMPv6:

- **ICMP tipos 3, 5, 11 y 12, e ICMPv6 tipos 1, 2, 3, 4 y 137**: de manera predeterminada, el cortafuegos busca los bytes de información del paquete IP integrado del datagrama que causó el error (el paquete de invocación). Si el paquete integrado coincide con una sesión existente, el cortafuegos reenvía o descarta el paquete ICMP o ICMPv6 según la acción definida en la regla de la política de seguridad que coincide con esa sesión. (Puede utilizar los Perfiles de protección de zonas con la protección contra ataques basados en paquetes para anular este comportamiento predeterminado para los tipos ICMPv6).
- **Tipos de paquetes ICMP o ICMPv6 restantes:** el cortafuegos trata el paquete ICMP o ICMPv6 como si perteneciera a una nueva sesión. Si una regla de la política de seguridad coincide con el paquete (y el cortafuegos lo reconoce como una sesión **icmp** o **ipv6-icmp**), el cortafuegos reenvía o descarta el paquete en función de la acción de la regla de la política de seguridad. Los contadores de la política de seguridad y los logs de tráfico reflejan las acciones.

  Si ninguna regla de la política de seguridad coincide con el paquete, el cortafuegos aplica sus reglas predeterminadas de la política de seguridad, lo que permite tráfico intrazona y bloquea tráfico intrazona (la creación de logs está deshabilitada de manera predeterminada para estas reglas).

  A pesar de que puede anular las reglas predeterminadas para habilitar la creación de logs o cambiar la acción predeterminada, no recomendamos que modifique el comportamiento predeterminado para un caso específico dado que impactará en todo el tráfico que esas reglas predeterminadas afectan. En cambio, cree reglas de la política de seguridad para controlar y registrar paquetes ICMP o ICMPv6 explícitamente.

  Existen dos maneras de crear reglas explícitas de la política de seguridad para manejar paquetes ICMP o ICMPv6 que no son paquetes de error o redirigidos:

  - **Cree una regla de la política de seguridad para permitir (o denegar) todos los paquetes ICMP o ICMPv6:** en esta regla de la política de seguridad, especifique el **icmp** o **ipv6-icmp** de la aplicación;

© 2020 Palo Alto Networks, Inc.

el cortafuegos permite (o deniega) todos los paquetes IP que coincidan con el número de protocolo ICMP (1) o el número de protocolos ICMPv6 (58), respectivamente, mediante el cortafuegos.

- **Cree una aplicación personalizada y una regla de la política de seguridad para permitir (o denegar) paquetes desde o hacia esa aplicación:** este enfoque más detallado le permite Control de tipos y códigos específicos de ICMP o ICMPv6.

Límite de tasa ICMPv6

La limitación de tasa ICMPv6 es un mecanismo de limitación que evita las inundaciones y los intentos de DDoS. La implementación utiliza una tasa de paquetes de error y un depósito de tokens, que colaboran para permitir la limitación y garantizar que los paquetes de ICMP no inundan los segmentos de red protegidos por el cortafuegos.

Primero, la **tasa de paquetes de errores ICMPv6 globales (por segundo)** controla la tasa a la cual se permite pasar los paquetes de errores ICMP por el cortafuegos; el valor predeterminado es de 100 paquetes por segundo, el rango es de 10 a 65535 paquetes por segundo. Si el cortafuegos alcanza la tasa de paquetes de error de ICMPv6, el depósito de tokens se utiliza para activar la limitación, del siguiente modo.

El concepto de depósito de tokens lógico controla la velocidad a la que se pueden transmitir los mensajes ICMP. La cantidad de tokens en el depósito puede configurarse, y cada token representa un mensaje ICMPv6 que puede enviarse. El recuento de tokens se reduce cada vez que se envía un mensaje ICMPv6; cuando el depósito llega a cero tokens, ya no es posible enviar más mensajes ICMPv6 hasta que se añada otro token al depósito. El tamaño predeterminado del depósito de tokens es de 100 tokens (paquetes), y el intervalo es de 10 a 65535 tokens.

Para cambiar el tamaño predeterminado de tokens o la tasa de paquetes de errores, consulte la sección Configuración de los ajustes de sesión.

Control de tipos y códigos específicos de ICMP o ICMPv6

Utilice esta tarea para crear una aplicación ICMP o ICMPv6 personalizada y crear una regla en la política de seguridad que permita o deniegue la aplicación.

STEP 1 | Cree una aplicación personalizada para tipos y códigos de mensajes ICMP o ICMPv6.

1. Seleccione **Object (Objeto)** > **Applications (Aplicaciones)** y **Add (Añadir)** para añadir una aplicación personalizada.
2. En la pestaña **Configuration (Configuración)**, introduzca un nombre en **Name (Nombre)** para la aplicación personalizada y una descripción en **Description (Descripción)**. Por ejemplo, introduzca el nombre ping6.
3. En **Category (Categoría)**, seleccione **networking (redes)**.
4. En **Subcategory (Subcategoría)**, seleccione **ip-protocol (Protocolo IP)**.
5. En **Technology (Tecnología)**, seleccione **network-protocol (Protocolo de red)**.
6. Haga clic en **OK (Aceptar)**.
7. En la pestaña **Advanced (Avanzado)**, seleccione **ICMP Type (Tipo ICMP)** o **ICMPv6 Type (Tipo ICMPv6)**.
8. En **Type (Tipo)**, introduzca un número (rango: 0 a 255) que designe el tipo de mensaje ICMP o ICMPv6 que desea permitir o denegar. Por ejemplo, 128 corresponde al mensaje Echo Request (Solicitud de Echo) (ping).
9. Si el campo Type (Tipo) incluye los códigos, introduzca el número de **Code (Código)** (rango: 0 a 255) que aplique al valor de **Type (Tipo)** que desea permitir o denegar. Algunos valores de **Type (Tipo)** tienen solo un código 0.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree una regla en la política de seguridad que permita o deniegue la aplicación personalizada que creó.

© 2020 Palo Alto Networks, Inc.

Creación de una regla de política de seguridad. En la pestaña **Application (Aplicación)**, especifique el nombre de la aplicación personalizada que acaba de crear.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

Configuración de los tiempos de espera de sesión

El tiempo de espera de una sesión define la duración para la que PAN-OS mantiene una sesión en el cortafuegos después de la inactividad en esa sesión. De forma predeterminada, cuando la sesión agota su tiempo de espera para el protocolo, PAN-OS cierra la sesión. Puede definir un número de tiempos de espera para sesiones TCP, UDP e ICMP por separado. El tiempo de espera predeterminado se aplica a cualquier otro tipo de sesión. Estos tiempos de espera son globales, lo que significa que se aplican a todas la sesiones de ese tipo en el cortafuegos.

También puede configurar un ajuste global de tiempo de espera de caché de ARP, que controla el tiempo durante el cual el cortafuegos conserva las entradas de ARP (asignaciones de direcciones IP a direcciones de hardware) en su caché.

Además de los ajustes globales, puede definir los tiempos de espera para cada aplicación en la pestaña **Objects (Objetos)** > **Applications (Aplicaciones)**. El cortafuegos aplica los tiempos de espera de la aplicación a una aplicación que esté en estado establecido. Cuando se configuran, los tiempos de espera para una aplicación anulan los tiempos de espera globales de la sesión TCP o UDP.

Si cambia los temporizadores de TCP o UDP en el nivel de la aplicación, estos temporizadores para las aplicaciones predefinidas y las aplicaciones personalizadas compartidas se implementarán en todos los sistemas virtuales. Si desea que el temporizador de una aplicación sea diferente del temporizador de un sistema virtual, debe crear una aplicación personalizada, asignarle temporizadores únicos y asignar la aplicación personalizada a un sistema virtual único.

Realice la siguiente tarea si desea cambiar los valores predeterminados de los ajustes de tiempos de espera de sesión globales para TCP, UDP, ICMP, autenticación del portal de autenticación u otros tipos de sesiones. Todos los valores se indican en segundos.

Los valores predeterminados son valores óptimos. Sin embargo, puede modificarlos según las necesidades de su red. Si configura un valor demasiado bajo, puede hacer que se detecten retrasos mínimos en la red, lo que podría producir errores a la hora de establecer conexiones con el cortafuegos. Si configura un valor demasiado alto, entonces podría retrasarse la detección de errores.

STEP 1 | Acceda a los tiempos de espera de la sesión.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique los tiempos de espera de la sesión.

STEP 2 | (Opcional) Cambie los tiempos de espera mixtos.

- **Predeterminado**: tiempo máximo que una sesión que no es TCP/UDP ni ICMP puede estar abierta sin una respuesta (el intervalo es de 1 a 15 999 999; el valor predeterminado es 30).
- **Descartar valor predeterminado**: tiempo máximo que una sesión no TCP/UDP permanece abierta cuando PAN-OS rechaza una sesión debido a las políticas de seguridad configuradas en el cortafuegos (el intervalo es de 1 a 15 999 999; el valor predeterminado es 60).

© 2020 Palo Alto Networks, Inc.

- **Análisis**: tiempo máximo de espera en el que una sesión seguirá abierta después de considerarse inactiva; se considera que una aplicación está inactiva cuando supera el umbral de generación de aplicaciones que tiene definido (el intervalo es de 5 a 30; el valor predeterminado es 10).
- **Portal de autenticación**: Tiempo de espera de la sesión de autenticación para el formato web del portal de autenticación. Para acceder al contenido solicitado, el usuario debe introducir las credenciales de autenticación en este formato y autenticarse correctamente (el intervalo es de 1 a 15 999 999; el valor predeterminado es 30).
- Para definir otros tiempos de espera del portal de autenticación, como el temporizador de inactividad y el tiempo que debe transcurrir para volver a autenticar al usuario, seleccione **Device (Dispositivo)** > **User Identification (Identificador de usuario)** > **Authentication Portal Settings (Configuración del portal de autenticación)**. Consulte Configuración del portal de autenticación.

STEP 3 | (Opcional) Cambio de los tiempos de espera TCP.

- **Descartar TCP**: La longitud máxima de tiempo que una sesión TCP permanece abierta cuando se deniega una sesión debido a las políticas de seguridad configuradas en el cortafuegos. Default: 90. Intervalo: 1 a 15.999.999.
- **TCP**: Tiempo máximo que una sesión TCP permanece abierta sin una respuesta después de que una sesión TCP active el estado Establecido (después de que se complete el protocolo o la transmisión de datos haya comenzado). Default: 3600. Intervalo: 1 a 15.999.999.
- **Protocolo de enlace TCP**: Tiempo máximo entre la recepción de SYN-ACK y la siguiente ACK para establecer completamente la sesión. Default: 10. Intervalo: 1 a 60.
- **Inicialización de TCP**: Tiempo máximo permitido entre la recepción de SYN y SYN-ACK antes de iniciar el temporizador del protocolo de enlace TCP. Default: 5 Intervalo: 1 a 60.
- **TCP Half Closed (TCP semicerrado)**: Tiempo máximo entre la recepción del primer FIN y la recepción del segundo FIN o RST. Default: 120. Intervalo: 1 a 604 800.
- **Tiempo de espera TCP**: Tiempo máximo después de recibir el segundo FIN o RST. Default: 15. Intervalo: 1 a 600.
- **RST sin verificar**: Tiempo máximo después de recibir un RST que no se puede verificar (el RST está dentro de la ventana TCP pero tiene un número de secuencia inesperado o el RST procede de una ruta asimétrica). Default: 30. Intervalo: 1 a 600.
- Consulte también el tiempo de espera de **Scan (Exploración)** en la sección (Opcional) Cambio de diversos tiempos de espera.

STEP 4 | (Opcional) Cambio de los tiempos de espera UDP.

- **Descartar UDP**: La longitud máxima de tiempo que una sesión UDP permanece abierta cuando se deniega una sesión debido a las políticas de seguridad configuradas en el cortafuegos. Default: 60. Intervalo: 1 a 15.999.999.
- **UDP**: Tiempo máximo que una sesión UDP permanece abierta sin una respuesta de UDP. Default: 30. Intervalo: 1 a 15.999.999.
- Consulte también el tiempo de espera de **Scan (Exploración)** en la sección (Opcional) Cambio de diversos tiempos de espera.

STEP 5 | (Opcional) Cambio de los tiempos de espera ICMP.

- **ICMP**: Tiempo máximo que una sesión ICMP puede permanecer abierta sin una respuesta de ICMP. Default: 6. Intervalo: 1 a 15.999.999.
- Consulte también el tiempo de espera de **Discard Default (Descartar valor predeterminado)** y **Scan (Explorar)** en la sección (Opcional) Cambio de tiempos de espera mixtos.

STEP 6 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 7 | (Opcional) Cambie el tiempo de espera de caché de ARP.

© 2020 Palo Alto Networks, Inc.

1. Acceda a la CLI y especifique durante cuántos segundos el cortafuegos mantiene las entradas de ARP en el caché. Use el comando operativo **`set system setting arp-cache-timeout`** <*value*>, en el que el rango es de 60 a 65 535; el valor predeterminado es de 1800.

   Si disminuye el tiempo de espera y las entradas existentes en el caché poseen un TTL mayor que el nuevo valor de tiempo de espera, el cortafuegos elimina estas entradas y actualiza el caché de ARP. Si aumenta el tiempo de espera y las entradas existentes poseen un TTL mayor que el nuevo valor de tiempo de espera, estas vencen según el TTL y el cortafuegos almacena en caché las entradas nuevas con un valor de tiempo de espera mayor.
2. Vea la configuración de tiempo de espera de la caché de ARP con el comando operativo de la CLI **`show system setting arp-cache-timeout`**.

Configuración de los ajustes de sesión

En este tema se describen varios ajustes de las sesiones distintos de los valores de tiempo de espera. Realice esas tareas si necesita cambiar los ajustes por defecto.

STEP 1 | Cambie los ajustes de sesión.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.

STEP 2 | Especifique si aplicará las reglas de política de seguridad recientemente configuradas a las sesiones que están en curso.

Seleccione **Rematch all sessions on config policy change (Volver a cotejar todas las sesiones tras el cambio a la política configurada)** para aplicar las reglas de política de seguridad recientemente configurada a las sesiones que están en curso. Esta capacidad está habilitada de manera predeterminada. Si desmarca esta casilla de verificación, los cambios de la regla de política que realice se aplicarán únicamente a las sesiones iniciadas después de que confirmó el cambio de la política.

Por ejemplo, si se ha iniciado una sesión de Telnet mientras estaba configurada una política que permitía Telnet y usted posteriormente compiló un cambio de política para denegar Telnet, el cortafuegos aplica la política modificada a la sesión actual y la bloquea.

STEP 3 | Configure los ajustes de IPv6.

- **ICMPv6 Token Bucket Size (Tamaño de depósito de testigo de ICMPv6)**: predeterminado 100 tokens. Consulte la sección Límite de tasa de ICMPv6.
- **Tasa de paquetes (por segundo) de errores de ICMPv6** : Valor predeterminado: 100. Consulte la sección Límite de tasa de ICMPv6.
- **Enable IPv6 Firewalling (Habilitar cortafuegos IPv6)**: permite funciones de cortafuegos para IPv6. Todas las configuraciones basadas en IPv6 se ignorarán si IPv6 no se habilita. Incluso si IPv6 está activado para una interfaz, el ajuste **Cortafuegos IPv6** también debe estar activado para que IPv6 funcione.

STEP 4 | Habilite las tramas gigantes y establezca la MTU.

1. Seleccione **Enable Jumbo Frame (Habilitar tramas gigantes)** para habilitar la compatibilidad con tramas gigantes en interfaces de Ethernet. Las tramas gigantes tienen una unidad de transmisión máxima (MTU) de 9.216 bytes y están disponibles en determinados modelos.
2. Configure la **Global MTU**, dependiendo de si habilitó o no tramas gigantes:
   - Si no habilitó las tramas gigantes, la **MTU global** vuelve al valor por defecto de 1.500 bytes; el intervalo es de 576 a 1.500 bytes.
   - Si habilitó tramas gigantes, la **Global MTU** vuelve al valor por defecto de 9.192 bytes; el intervalo es de 9192 a 9.216 bytes.

© 2020 Palo Alto Networks, Inc.

Las tramas gigantes pueden ocupar hasta cinco veces más memoria en comparación con los paquetes normales, y pueden reducir la cantidad de búferes de paquetes disponibles en un 20 %. Esto reduce el tamaño de las colas dedicadas a tareas de procesamiento de paquetes fuera de servicio, identificación de aplicaciones y otras tareas de procesamiento de paquetes. A partir de PAN-OS 8.1, si habilita la configuración de MTU global de trama gigante y reinicia el cortafuegos, los búferes de paquetes se redistribuyen para procesar las tramas gigantes de manera más eficiente.

Si habilita las tramas gigantes y tiene interfaces donde la MTU no está específicamente configurada, estas interfaces heredarán automáticamente el tamaño de la traga gigante. Por lo tanto, antes de que active las tramas gigantes, si no desea que alguna interfaz las adopte, debe establecer la MTU para esa interfaz en 1500 bytes u otro valor.

STEP 5 | Establezca los ajustes detallados de la sesión NAT.

- **Tamaño mínimo de MTU para NAT64 en IPv6**: Introduzca la MTU global para el tráfico IPv6 traducido. El valor predeterminado de 1.280 bytes se basa en la MTU mínima estándar para el tráfico IPv6.
- **NAT Oversubscription Rate (Ratio de sobresuscripción NAT)**: si NAT se configura como traducción de IP dinámica y puerto (DIPP), es posible configurar una ratio de sobresuscripción para multiplicar el número de veces que se puede usar simultáneamente el mismo par de puertos y direcciones IP traducidas. El ratio es de 1, 2, 4 u 8. El ajuste predeterminado se basa en el modelo del cortafuegos.
- Una ratio de 1 significa que no existe ninguna sobresuscripción; cada par de dirección IP y puerto traducido se puede utilizar solo una vez en cada ocasión.
- Si el ajuste es **Platform Default (Valor predeterminado de plataforma)**, la configuración del usuario de la tasa está inhabilitada y se aplica la tasa de sobresuscripción predeterminada para el modelo.

La reducción de la ratio de sobresuscripción disminuye el número de traducciones de dispositivo de origen, pero proporciona más capacidades de regla de NAT.

STEP 6 | Establezca los ajustes detallados del vencimiento acelerado.

Seleccione **Accelerated Aging (Vencimiento acelerado)** para habilitar el vencimiento más rápido de las sesiones inactivas. También puede cambiar el umbral (%) y el factor de escala:

- **Accelerated Aging Threshold (Umbral de vencimiento acelerado)**: porcentaje de la tabla de sesión que se llena cuando comienza el vencimiento acelerado. El valor predeterminado es del 80%. Cuando la tabla de sesión alcanza este umbral (% lleno), PAN-OS aplica el factor de escala de vencimiento acelerado a los cálculos de vencimiento de todas las sesiones.
- **Accelerated Aging Scaling Factor (Factor de escala de vencimiento acelerado)**: factor de escala usado en los cálculos de vencimiento acelerado. El factor de escala predeterminado es 2, lo que significa que el vencimiento acelerado se produce a una velocidad dos veces más alta que el tiempo de espera de inactividad configurado. El tiempo de espera de inactividad configurado dividido entre 2 tiene como resultado un tiempo de espera más rápido (la mitad). Para calcular el vencimiento acelerado de la sesión, PAN-OS divide el tiempo de inactividad configurado (para ese tipo de sesión) entre el factor de escala para determinar un tiempo de espera más corto.

Por ejemplo, si se utiliza el factor de escala de 10, una sesión que por lo general vencería después de 3600 segundos lo hará 10 veces más rápido (en 1/10 del tiempo), es decir, 360 segundos.

STEP 7 | Habilite la protección de búfer de paquetes.

1. Seleccione **Packet Buffer Protection (Protección de búfer de paquetes)** para habilitar el cortafuegos para que tome medidas contra las sesiones que pueden inundar el búfer de paquetes y hacer que el tráfico no legítimo sea descartado; se habilita de forma predeterminada.

© 2020 Palo Alto Networks, Inc.

2. Si usted habilita la protección de búfer de paquetes, puede ajustar los umbrales y temporizadores que indican de qué manera el cortafuegos responde al uso indebido del búfer de paquetes.
   - **Alert (%) (Alerta)**: Cuando la utilización del búfer de paquetes supera este umbral, el cortafuegos crea un evento de logs. El umbral se configura en el 50 % de manera predeterminada y el intervalo es del 0 % al 99 %. Si el valor se configura en 0 %, el cortafuegos no crea un evento de log.
   - **Activate (%) (Activar)**: Cuando la utilización de un búfer de paquetes supera este umbral, el cortafuegos aplica el descarte aleatorio temprano (random early drop, RED) a las sesiones negativas. El umbral se configura en el 80 % de manera predeterminada y el intervalo es del 0 % al 99 %. Si el valor se configura en 0 %, el cortafuegos no aplica el RED.

   Los eventos de alerta se registran en el log del sistema. Los eventos para el tráfico descartado, las sesiones descartadas y la dirección IP bloqueada se registran en el log de amenazas.

   - **Block Hold Time (sec) (Tiempo de espera de bloqueo [s])**: el tiempo que se permite continuar a la sesión mitigada con RED antes de que se descarte. Por defecto, el tiempo de espera del bloqueo es de 60 segundos. El intervalo es de 0 a 65.535. Si el valor se configura en 0, el cortafuegos no descarta las sesiones en función de la protección de búfer de paquetes.
   - **Block Duration (sec) (Duración del bloqueo [s])**: Este ajuste define por cuánto tiempo se descarta una sesión o se bloquea una dirección IP. El valor predeterminado es 3600 segundos con un intervalo de 0 segundos a 15 999 999 segundos. Si este valor se configura en 0, el cortafuegos no descarta las sesiones ni bloquea las direcciones IP en función de la protección de búfer de paquetes.

STEP 8 | Habilite el almacenamiento en búfer de los paquetes de configuración de ruta de multidifusión.

1. Seleccione **Multicast Route Setup Buffering**para habilitar al cortafuegos para preservar el primer paquete en una sesión de multidifusión cuando la ruta multidifusión o la entrada de la base de información de reenvío (forwarding information base, FIB) todavía no existe para el grupo de multidifusión correspondiente. De manera predeterminada, el cortafuegos no almacena en búfer el primer paquete multicast en una sesión nueva, en cambio, usa el primer paquete para configurar la ruta multicast. Este es un funcionamiento esperado para el tráfico multicast. Solo debe habilitar la configuración de buffering de ruta multicast si los servidores de contenido están directamente conectados con el cortafuegos y su aplicación personalizada no puede resistir que el primer paquete de la sesión se omita. Esta opción está deshabilitada de manera predeterminada.
2. Si habilita el almacenamiento en búfer, también puede ajustar el **Buffer Size (Tamaño de búfer)**, que especifica el tamaño del búfer según el flujo. El cortafuegos puede almacenar en búfer un máximo de 5000 paquetes.

   También puede ajustar la duración, en segundos, durante la cual una ruta de multidifusión permanece en la tabla de enrutamiento en el cortafuegos después de que la sesión finaliza al configurar los ajustes de multidifusión en el enrutador virtual que maneja su enrutador virtual (configure Multicast Route Age Out Time [sec] [Tiempo de vencimiento de ruta de multidifusión [s]] en la pestaña Multicast [Multidifusión] > Advanced [Avanzado] en la configuración de enrutador virtual).

STEP 9 | Guarde los ajustes de sesión.

Haga clic en **OK (Aceptar)**.

STEP 10 | Configure los ajustes detallados de Maximum Segment Size (MSS) (Tamaño máximo del segmento) para una interfaz de capa 3.

1. Seleccione **Network (Red)** > **Interfaces**, seleccione **Ethernet**, **VLAN** o **Loopback (Bucle invertido)**, y seleccione la interfaz de capa 3.
2. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**.

© 2020 Palo Alto Networks, Inc.

3. Seleccione **Adjust TCP MSS (Ajustar tamaño máximo del segmento de TCP)** e introduzca un valor para una de las dos opciones siguientes, o ambas:
   - **IPv4 MSS Adjustment Size (Tamaño de ajuste de MSS de IPv4)**: el intervalo va de 40 a 300 bytes y el valor predeterminado es 40 bytes.
   - **IPv6 MSS Adjustment Size (Tamaño de ajuste de MSS de IPv6)**: el intervalo va de 60 a 300 bytes y el valor predeterminado es 60 bytes.
4. Haga clic en **OK (Aceptar)**.

STEP 11 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

STEP 12 | Reinicie el cortafuegos después de cambiar la configuración de tramas gigantes.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Reboot Device (Reiniciar dispositivo)**.

Política de distribución de sesiones

Las políticas de distribución de sesiones definen cómo los cortafuegos serie PA-5200 y PA-7000 distribuyen el procesamiento de seguridad (App-ID, Content-ID, filtrado de URL, cifrado SSL e IPSec) entre los procesadores de plano de datos (DP) en el cortafuegos. Cada política se diseña específicamente para un tipo determinado de entorno de red y configuración de cortafuegos para garantizar que el cortafuegos distribuya sesiones con máxima eficacia. Por ejemplo, la política de distribución de sesiones de hash es la mejor opción en los entornos que utilizan NAT de origen a gran escala.

La cantidad de DP en un cortafuegos varía según el modelo del cortafuegos:

Modelo de cortafuegos	Procesadores de planos de datos
PA-7000 Series	Depende de la cantidad de tarjetas de procesamiento de red (Network Processing Card, NPC). Cada NPC tiene varios procesadores de plano de datos (DP) y puede instalar varios NPC en el cortafuegos.
Cortafuegos PA-5220	1  *El cortafuegos PA-5220 solo tiene un DP, de modo que las políticas de distribución de sesiones no causan efecto. Conserve la política establecida en el modo predeterminado (round-robin).*
Cortafuegos PA-5250	2
Cortafuegos PA-5260 y PA-5280	3

Los siguientes temas proporcionan información sobre las políticas de distribución de sesiones disponibles, cómo cambiar una política activa y cómo ver las estadísticas de distribución de sesiones.

- Descripciones de las políticas de distribución de sesiones
- Cambio de la política de distribución de sesiones y visualización de las estadísticas

© 2020 Palo Alto Networks, Inc.

Descripciones de las políticas de distribución de sesiones

La siguiente tabla proporciona información sobre las Políticas de distribución de sesiones para ayudarle a decidir cuál es la política que se adapta mejor a su entorno y su configuración de cortafuegos.

Política de distribución de sesiones	Description (Descripción)
Fixed	Le permite especificar el procesador de plano de datos (DP) que utilizará el cortafuegos para el procesamiento de seguridad. Utilice esta política para la depuración.
Hash	El cortafuegos distribuye las sesiones basándose en un hash de la dirección de origen o destino. La distribución basada en hash mejora la eficiencia de la gestión de recursos de direcciones NAT y reduce la latencia de la configuración de sesiones NAT evitando posibles conflictos de puertos o direcciones IP. Utilice esta política en entornos que utilizan NAT de origen a gran escala con traducción de IP dinámicas, traducción de puertos e IP dinámicas o ambas. Cuando utilice la traducción de IP dinámicas, seleccione la opción de dirección de **`origen`**. Cuando utilice la traducción de puertos e IP dinámicas, seleccione la opción de dirección de **`destino`**.
Ingres-slot (predeterminado en cortafuegos serie PA-7000)	(Solo cortafuegos serie PA-7000) Las sesiones nuevas se asignan a un DP en la misma NPC a la que llegó el primer paquete de la sesión. La selección de DP se basa en el algoritmo session-load, pero, en este caso, las sesiones se limitan a los DP en la NPC de ingreso. Según el tráfico y la topología de red, esta política generalmente reduce las posibilidades que necesitará el tráfico para atravesar la matriz de conmutación. Utilice esta política para reducir la latencia si la NPC de ingreso y la NPC de salida se encuentran en la misma NPC. Si el cortafuegos cuenta con una combinación de NPC (por ejemplo, PA-7000 20G y PA-7000 20GXM), esta política puede aislar la capacidad aumentada a la NPC correspondiente y ayudar a aislar el impacto de los fallos de la NPC.
Random	De manera aleatoria, el cortafuegos selecciona un DP para el procesamiento de sesiones.
Round-robin (predeterminado en cortafuegos serie PA-5200)	El cortafuegos selecciona el procesador del plano de datos en función de un algoritmo round-robin entre planos de datos activos de modo que la entrada, la salida y las funciones de procesamiento de seguridad se compartan entre todos los planos de datos. Utilice esta política en entornos de baja a media exigencia donde alcanzará un algoritmo de equilibrio de carga simple y predecible.

© 2020 Palo Alto Networks, Inc.

Política de distribución de sesiones	Description (Descripción)
	En entornos de alta exigencia, recomendamos que utilice el algoritmo session-load.
Session-load	Esta política es similar a la política round-robin, pero utiliza un algoritmo basado en el peso para determinar cómo distribuir sesiones para lograr un equilibrio entre los DP. Debido a la variedad en la duración de una sesión, es probable que el DP no experimente siempre una carga uniforme. Por ejemplo, si el cortafuegos tiene tres DP y DP0 se encuentra al 25 % de la capacidad; DP1, al 25 % de la capacidad; y DP2, al 50 % de capacidad, se preferirá que la asignación de la nueva sesión se incline por la DP con menor capacidad. Esto permite mejorar el equilibrio de carga con el tiempo. Utilice esta política en entornos donde las sesiones se distribuyen a través de varias ranuras NPC, tales como un grupo de interfaces agregadas de varias ranuras o en entornos con reenvío asimétrico. También puede utilizar esta política o la política ingress-slot si el cortafuegos tiene una combinación de NPC con diferentes capacidades para las sesiones (como una combinación de NPC PA-7000 20G y PA-7000 20GXM).
Hash simétrico	(Cortafuegos serie PA-5200 y PA-7000 que ejecutan PAN-OS 8.0 o posterior) El cortafuegos selecciona el DP con un hash de direcciones IP de origen y de destino ordenadas. Esta política ofrece los mismos resultados para el tráfico server-to-client (s2c) y client-to-server (c2s) (suponiendo que el cortafuegos no utiliza NAT). Utilice esta política en implementaciones de IPSec o GTP de alta exigencia. Con estos protocolos, cada dirección se trata como un flujo unidireccional donde las tuplas de flujo no se pueden dividir. Esta política mejora el rendimiento y reduce la latencia garantizando que ambas direcciones se asignen al mismo DP, lo que elimina la necesidad de una comunicación entre DP.

Cambio de la política de distribución de sesiones y visualización de las estadísticas

La siguiente tabla describe cómo ver y cambiar las Políticas de distribución de sesiones activas y describe cómo ver las estadísticas de las sesiones de cada procesador del plano de datos (DP) en el cortafuegos.

Tarea	Comando
Mostrar la política activa de distribución de sesiones.	Utilice el comando **`show session distribution policy`** para ver la política activa de distribución de sesiones. El siguiente resultado muestra un cortafuegos PA-7080 con cuatro NPC instaladas en las ranuras 2, 10, 11 y 12 con la política de distribución ingress-slot habilitada:

© 2020 Palo Alto Networks, Inc.

Tarea	Comando

	`> show session distribution policy`
	
	`Ownership Distribution Policy: ingress-slot`
	
	`Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12]`

Cambiar la política activa de distribución de sesiones.	Utilice el comando **set session distribution-policy *<policy>*** para cambiar la política activa de distribución de sesiones. Por ejemplo, para seleccionar la política session-load, introduzca el siguiente comando: `> set session distribution-policy session-load`

Ver estadísticas de distribución de sesiones.	Utilice el comando **show session distribution statistics** para ver los procesadores del plano de datos (DP) en el cortafuegos y la cantidad de sesiones en cada DP activo.
	El siguiente resultado es de un cortafuegos PA-7080:
	`> show session distribution statistics`
	`DP Active Dispatched Dispatched/sec`
	`----------------------------------------`
	`s1dp0 78698 7829818 1473`
	`s1dp1 78775 7831384 1535`
	`s3dp0 7796 736639 1488`
	`s3dp1 7707 737026 1442`
	La `columna Active DP (DP activos)` enumera cada plano de datos en las NPC instaladas. Los primeros dos caracteres indican el número de ranura y los últimos tres caracteres indican el número de plano de datos. Por ejemplo, s1dp0 indica que el plano de datos es 0 en la NPC instalada en la ranura 1 y s1dp1 indica que el plano de datos es 1 en la NPC instalada en la ranura 1.
	La columna `Dispatched (Enviados)` muestra el número total de sesiones que ha procesado el plano de datos desde la última vez que se reinició el cortafuegos.
	La columna `Dispatched/sec (Enviados/s)` indica la tasa de envío. Si se suman los números en la columna `Dispatched (Enviados)`, el total equivale al número de sesiones activas en el cortafuegos. También podrá ver el número total de sesiones activas al ver el resultado del comando de la CLI **show session info**.

© 2020 Palo Alto Networks, Inc.

Tarea	Comando
	El resultado del cortafuegos serie PA-5200 será similar, excepto porque el número de los DP depende del modelo y que solo hay una ranura de NPC (s1).

Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP

Puede configurar un descarte del protocolo de enlace dividido de TCP en un perfil de protección de zona para evitar que se establezcan sesiones de TCP a menos que se utilice el protocolo de enlace en tres pasos estándar. Esta tarea supone que usted asigne una zona de seguridad para la interfaz en la que desea evitar que los protocolos de enlace divididos de TCP establezcan una sesión.

STEP 1 | Configure un perfil de Zona de protección para impedir que las sesiones de TCP establezcan una sesión si no es mediante un protocolo de enlace en tres pasos.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y haga clic en **Add (Añadir)** para añadir un nuevo perfil (o seleccione un perfil existente).
2. Si está creando un nuevo perfil, introduzca un nombre en **Name** para el perfil y una descripción opcional en **Description**.
3. Seleccione **Packet Based Attack Protection (Protección contra ataques basados en paquetes)** > **TCP Drop (Descarte de TCP)** y seleccione **Split Handshake (Protocolo de enlace dividido)**.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Aplique el perfil a una o más zonas de seguridad.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione la zona a la que desea asignar el perfil de protección de zona.
2. En la lista **Zone Protection Profile (Perfil de protección de zona)** de la ventana Zone (Zona), seleccione el perfil configurado en el paso anterior.

   O bien, puede iniciar la creación de un nuevo perfil al hacer clic en **Zone Protection Profile**, en cuyo caso debe continuar según corresponda.
3. Haga clic en **OK (Aceptar)**.
4. (Opcional) Repita los pasos del 1 al 3 para aplicar el perfil a zonas adicionales.

STEP 3 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Inspección del contenido del túnel

El cortafuegos puede inspeccionar el contenido del tráfico de los protocolos de túneles de texto sin cifrar sin tener que finalizar los túneles:

- Encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) (RFC 2784)
- Tráfico IPSec no cifrado (NULL Encryption Algorithm for IPSec [Algoritmo de cifrado nulo para IPSec] [RFC 2410] y modo de transporte AH IPSec)
- Protocolo de túnel del servicio general de paquetes vía radio para datos de usuario (general packet radio service [GPRS] tunneling protocol for user data, GTP-U)
- Red de área local ampliable virtual (virtual extensible local area network, VXLAN) (RFC 7348)



La inspección de contenido de túnel es para los túneles de texto normal, no para túneles de VPN o LSVPN, que transportan tráfico cifrado.

Puede utilizar la inspección del contenido del túnel para aplicar las políticas de seguridad, las políticas de protección contra DoS y las políticas de QoS en el tráfico en estos tipos de túneles y en el tráfico anidado dentro de otro túnel de texto normal (por ejemplo, un túnel IPSec con cifrado nulo dentro de un túnel GRE). Puede consultar los logs de inspección del túnel y la actividad del túnel en el ACC para verificar que el tráfico de túnel cumple con sus políticas corporativas de seguridad y uso.

Todos los modelos de cortafuegos admiten la inspección del contenido de los túneles con los protocolos GRE, IPSec sin cifrar y VXLAN. Solo admiten la inspección del contenido de los túneles con GTP-U los cortafuegos que admiten la seguridad de GTP. Consulte las versiones de PAN-OS por modelos que admiten la seguridad de GTP y SCTP en la matriz de compatibilidad.

De forma predeterminada, los cortafuegos compatibles realizan la aceleración de túneles para mejorar el rendimiento y la producción del tráfico que pasa por túneles GRE, VXLAN y GTP-U. La aceleración del túnel proporciona descarga de hardware para reducir el tiempo que se tarda en realizar búsquedas de flujo y permite que el tráfico del túnel se distribuya de manera más eficiente en función del tráfico interno. Sin embargo, puede Deshabilitación de aceleración de túneles para solucionar el problema.

- Descripción general de la inspección del contenido del túnel
- Configuración de la inspección del contenido del túnel
- Visualización de actividad de túneles inspeccionados
- Visualización de información del túnel en logs
- Creación de un informe personalizado basado en el tráfico de túnel etiquetado
- Deshabilitación de aceleración de túneles

Descripción general de la inspección del contenido del túnel

Su cortafuegos puede inspeccionar el contenido del túnel en cualquier parte de la red donde no tenga la oportunidad de finalizar el túnel en primer lugar. Siempre que el cortafuegos esté en la ruta de un túnel de GRE, IPSec sin cifrar, GTP-U o VXLAN, puede inspeccionar el contenido del túnel.

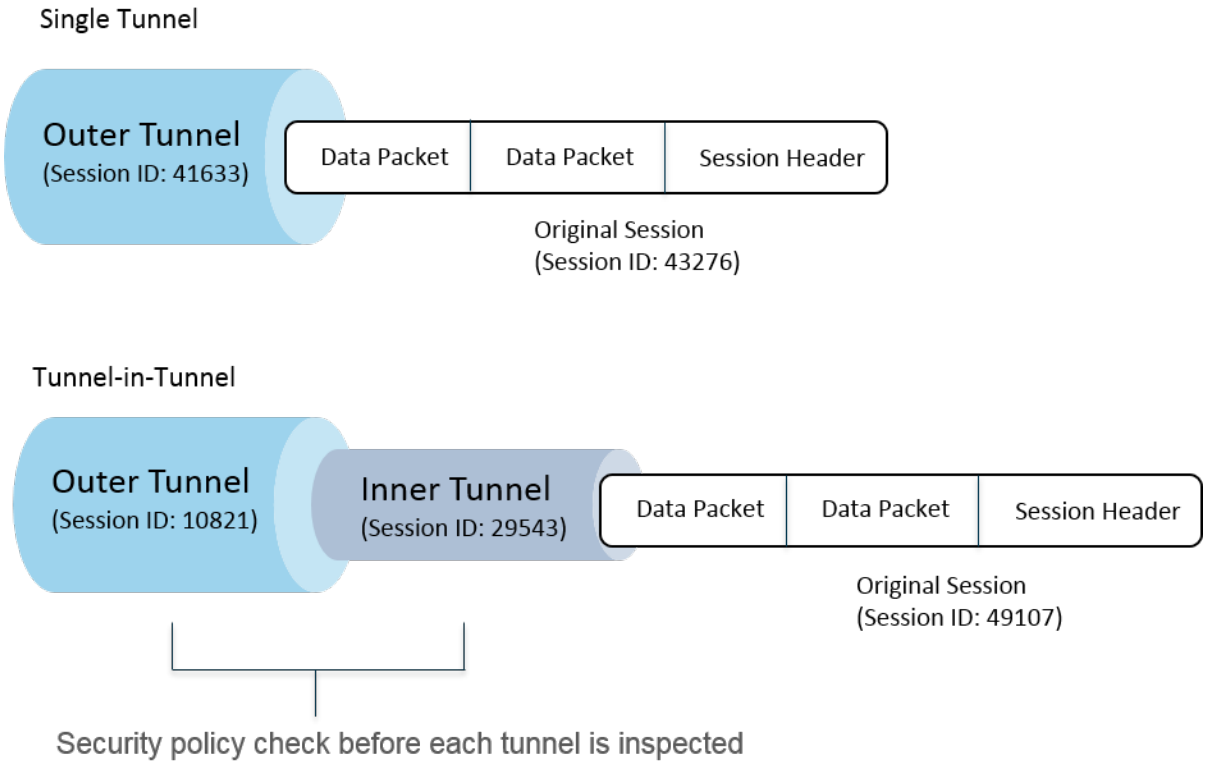
- Los clientes empresariales que deseen usar la inspección del contenido de los túneles pueden tener parte o la totalidad del tráfico en el cortafuegos tunelizado por medio de GRE, VXLAN o IPSec sin cifrar. Por motivos de seguridad, QoS y presentación de informes, debe inspeccionar el tráfico dentro del túnel.
- Los clientes de proveedores de servicio usan GTP-U para tunelizar el tráfico de datos desde dispositivos móviles. Debe inspeccionar el contenido interno sin finalizar el protocolo de túnel y debe registrar los datos de usuario desde sus usuarios.

El cortafuegos admite la inspección del contenido de los túneles en interfaces de Ethernet, subinterfaces, interfaces de Ethernet agregada (aggregate Ethernet, AE), interfaces de VLAN e interfaces de túneles de VPN y LSVPN. (El túnel de texto no cifrado que el cortafuegos inspecciona puede estar dentro de un

© 2020 Palo Alto Networks, Inc.

túnel VPN o LSVPN que finalice en el cortafuegos; por lo tanto, una interfaz de túnel VPN o LSVPN. En otras palabras, cuando el cortafuegos es un endpoint VPN o LSVPN, el cortafuegos puede inspeccionar el tráfico de cualquier protocolo de túnel no cifrado que la inspección del contenido de túnel admita).

La inspección del contenido de túnel se admite en las implementaciones de capa 3, capa 2, cable virtual y tap. La inspección del contenido de túnel funciona en puertas de enlace compartidas y en comunicaciones de sistema virtual a sistema virtual.



La figura anterior ilustra los dos niveles de inspección de túnel que el cortafuegos pueda realizar. Cuando un cortafuegos configurado con las reglas de política de inspección de túnel recibe un paquete:

- El cortafuegos primero realiza una comprobación de política de seguridad para determinar si el protocolo de túnel (aplicación) en el paquete está permitido o denegado. (Los paquetes IPv4 e IPv6 son protocolos compatibles dentro del túnel).
- Si la política de seguridad permite el paquete, el cortafuegos compara el paquete con una regla de política de inspección de túnel basada en la zona de origen, la dirección de origen, el usuario de origen, la zona de destino y la dirección de destino. La regla de política de inspección de túnel determina los protocolos de túnel que el cortafuegos inspecciona, el nivel máximo de encapsulación permitida (un solo túnel o un túnel dentro de un túnel), si permitir paquetes que contengan un protocolo de túnel que no aprueba la inspección de encabezado estricto según RFC 2780, y si permitir paquetes que contengan protocolos desconocidos.
- Si el paquete supera los criterios de coincidencia de la regla de la política de inspección de túnel, el cortafuegos inspecciona el contenido interno, que está sujeto a su política de seguridad (obligatoria) y las políticas opcionales que pueda especificar. (Los tipos de política admitidos para la sesión original se enumeran en la tabla siguiente).
- Si, por el contrario, el cortafuegos encuentra otro túnel, el cortafuegos recursivamente analiza el paquete para el segundo encabezado y ahora está al nivel dos de encapsulación, de manera que la segunda regla de política de inspección de túnel, que coincide con una zona de túnel, debe permitir un nivel un máximo de inspección de túnel de dos niveles para que el cortafuegos continúe procesando el paquete.

© 2020 Palo Alto Networks, Inc.

- Si su regla permite dos niveles de inspección, el cortafuegos realiza una comprobación de política de seguridad en este túnel interno y luego la comprobación de política de inspección de túnel. El protocolo de túnel que usted utiliza en un túnel interno puede ser diferente al protocolo de túnel que utiliza en el túnel externo.
- Si su regla no permite dos niveles de inspección, el cortafuegos basa su acción según si usted lo configuró para que descarte paquetes que tienen más niveles de encapsulación que el nivel de inspección de túnel máximo que usted configuró.

De manera predeterminada, el contenido encapsulado en un túnel pertenece a la misma zona de seguridad que el túnel, y está sujeto a las reglas de política de seguridad que protegen esa zona. Sin embargo, puede configurar una *zona de túnel*, que le da flexibilidad para configurar las reglas de política de seguridad para el contenido interno que difiere de las reglas de política de seguridad para el túnel. Si utiliza una política de inspección de túnel diferente para la zona de túnel, siempre debe tener un nivel de inspección de túnel máximo de dos niveles, debido a que, por definición, el cortafuegos busca el segundo nivel de encapsulación.

El cortafuegos no admite una regla de política de inspección de túnel que compare el tráfico de un túnel que finalice en el cortafuegos, el cortafuegos descarta los paquetes que coinciden con la sesión de túnel interno. Por ejemplo, cuando un túnel IPSec finaliza en el cortafuegos, no cree una regla de política de inspección de túnel que coincida con el túnel que usted finaliza. El cortafuegos ya inspecciona el tráfico del túnel interno, por lo que no hace falta ninguna regla de la política de inspección de túneles.

Si bien la inspección de contenido de túnel funciona en puertas de enlace compartidas en comunicaciones de sistema virtual a sistema virtual, no puede asignar zonas de túnel a puertas de enlace compartidas o comunicaciones de sistema virtual a sistema virtual; estas están sujetas a las mismas reglas de política de seguridad que las zonas a las cuales pertenecen.

Tanto las sesiones del túnel interno como las del túnel externo cuentan para la capacidad máxima de sesiones del modelo de cortafuegos.

La siguiente tabla indica con una marca de verificación qué tipos de política puede aplicar a una sesión de túnel externa, una sesión de túnel interna y la sesión original interna:

Tipo de política	Sesión de túnel externa	Sesión de túnel interna	Sesión original interna
Cancelación de aplicación	✓ Solo en VXLAN	–	✓
Protección DoS	✓	✓	✓
NAT	✓	–	–
Reenvío basado en políticas (PBF) y retorno simétrico	✓	–	–
QoS	–	–	✓
Seguridad (obligatorio)	✓	✓	✓

© 2020 Palo Alto Networks, Inc.

Tipo de política	Sesión de túnel externa	Sesión de túnel interna	Sesión original interna
User-ID	✓	✓	✓
Protección de zona	✓	✓	✓

VXLAN es diferente de otros protocolos. El cortafuegos puede usar cualquiera de los dos conjuntos diferentes de claves de sesiones para crear sesiones de VXLAN en el túnel externo.

- VXLAN UDP Session (Sesión de UDP de VXLAN): la clave es una tupla de seis elementos (zona, IP de origen, IP de destino, protocolo, puerto de origen y puerto de destino) que crea una sesión de UDP de VXLAN.
- VNI Session (Sesión de VNI): la clave es una tupla de cinco elementos que incorpora el ID del túnel (identificador de red VXLAN [VXLAN network identifier, VNI]) y utiliza la zona, la IP de origen, la IP de destino, el protocolo y el ID del túnel para crear una sesión de VNI.

Puede Visualizar la actividad de túnel inspeccionado en el ACC o Visualizar la información de túnel en logs. Para facilitar una visualización rápida, configure una etiqueta de supervisión para poder supervisar la actividad del túnel y filtrar los resultados de log según esa etiqueta.

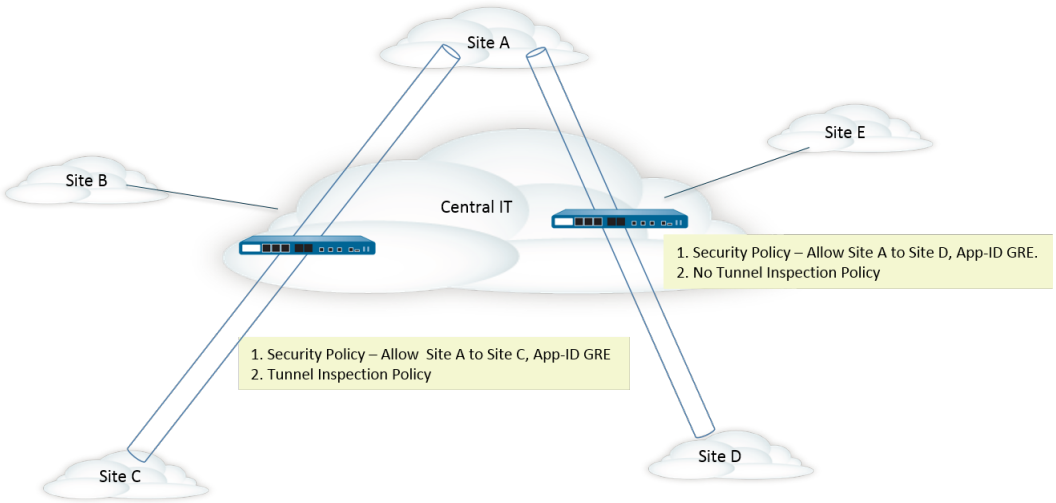
La actividad de túnel ACC proporciona datos en diferentes vistas. Para el uso de ID de túnel, etiqueta de supervisión de túnel y uso de aplicación de túnel, los datos de **bytes**, **sessions (sesiones)**, **threats (amenazas)**, **content (contenido)** y **URL** provienen de la base de datos de resumen de tráfico. Para el usuario del túnel, la IP de origen tunelizada y la actividad de IP de destino tunelizada, los datos de **bytes** y **sessions (sesiones)** provienen de la base de datos de resumen de tráfico, los datos de **threats (amenazas)** provienen del resumen de amenazas, los datos de **URL** provienen del resumen de URL y los datos de **contents (contenido)** provienen de la base de datos Data (Datos), que es un subconjunto de los logs de amenazas.

Si usted habilita NetFlow en la interfaz, NetFlow capturará las estadísticas del túnel externo únicamente, para evitar el recuento doble (recuento de bytes en los flujos interno y externo).

Para obtener información sobre la regla de política de inspección de túnel y las prestaciones de zona de túnel para su modelo de cortafuegos, consulte la Herramienta de selección de producto.

La siguiente figura ilustra una corporación que incluye varias divisiones y utiliza diferentes políticas de seguridad y una política de inspección de túnel. Un equipo de TI central se encarga de la conectividad entre las regiones. Un túnel conecta la ubicación A con la ubicación C; otro túnel conecta la ubicación A con la ubicación D. TI Central coloca un cortafuegos en la ruta de cada túnel; el cortafuegos en el túnel entre las ubicaciones A y C realiza la inspección de túnel; el cortafuegos en el túnel entre las ubicaciones A y D no posee una política de inspección de túnel debido a que el tráfico es muy delicado.

© 2020 Palo Alto Networks, Inc.



Configuración de la inspección del contenido del túnel

Realice esta tarea para configurar la inspección del contenido del túnel para un protocolo de túnel que usted permita en un túnel.

STEP 1 | Cree una regla de política de seguridad para permitir los paquetes que utilizan una aplicación específica (como la aplicación GRE) en el túnel desde la zona de origen a la zona de destino.

Creación de una regla de política de seguridad

El cortafuegos puede crear logs de inspección de túnel al inicio, al final de la sesión o en ambos momentos. Cuando especifique Actions (Acciones) para la regla de política de seguridad, seleccione Log at Session Start (Registrarse al inicio de la sesión) para las sesiones de túnel de larga duración, como las sesiones GRE.

STEP 2 | Cree una regla de política de inspección de túnel.

1. Seleccione **Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y luego **Add (Añadir)** para añadir una regla de políticas.
2. En la pestaña **General**, introduzca en **Name (Nombre)** un nombre para la regla de la política de inspección de túneles; debe empezar por un carácter alfanumérico y puede incluir caracteres alfanuméricos, guiones bajos, guiones, puntos y espacios.
3. (Opcional) Introduzca una **descripción**.
4. (Opcional) Especifique una **Tag (Etiqueta)** que identifique los paquetes que están sujetos a la regla de política de inspección de túnel, para fines de informes y registro.

STEP 3 | Especifique los criterios que determinan el origen de los paquetes a los cuales se aplica la regla de política de inspección de túneles.

1. Seleccione la pestaña **Source (Origen)**.
2. Seleccione **Add (Añadir)** para añadir una **Source Zone (Zona de origen)** en la lista de zonas (el valor predeterminado es **Any [Cualquiera]**).
3. (Opcional) Seleccione **Add (Añadir)** para añadir una **Source Address (Dirección de origen)**. Puede introducir una dirección IPv4 o IPv6, un grupo de direcciones o un objeto de dirección de región geográfica (**Any [Cualquiera]**).
4. (Opcional) Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las que especifica.

© 2020 Palo Alto Networks, Inc.

5. (Opcional) Haga clic en **Add (Añadir)** para añadir un **Source User (Usuario de origen)** (el valor predeterminado es **any [cualquiera]**). **Known-user (Usuario conocido)** es un usuario que se ha autenticado; un usuario **Unknown (Desconocido)**, no se ha autenticado.

STEP 4 | Especifique los criterios que determinan el destino de los paquetes a los cuales se aplica la regla de política de inspección de túneles.

1. Seleccione la pestaña **Destination (Destino)**.
2. Seleccione **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)** de la lista de zonas (el valor predeterminado es **Any [Cualquiera]**).
3. (Opcional) Seleccione **Add (Añadir)** para añadir una **Destination Address (Dirección de destino)**. Puede introducir una dirección IPv4 o IPv6, un grupo de direcciones o un objeto de dirección de región geográfica (el valor predeterminado es **Any [Cualquiera]**).

   También puede configurar una nueva dirección o grupo de direcciones.
4. (Opcional) Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las que especifica.

STEP 5 | Especifique los protocolos de túnel que el cortafuegos inspeccionará para esta regla.

1. Seleccione la pestaña **Inspection (Inspección)**.
2. **Add (Añadir)** uno o más **Protocols (Protocolos)** de túnel que desea que el cortafuegos inspeccione:
   - **GRE**: el cortafuegos inspecciona los paquetes que utilizan encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) en el túnel.
   - **GTP-U**: el cortafuegos inspecciona los paquetes que utilizan el protocolo de túnel General Packet Radio Service (GPRS) para datos de usuario (GTP-U) en el túnel.
   - **Non-encrypted IPSec (IPSec sin cifrar)**: el cortafuegos inspecciona los paquetes que utilizan IPSec sin cifrar (IPSec con cifrado nulo o IPSec con encabezado de autenticación [authentication header, AH] en modo de transporte) en el túnel.
   - **VXLAN**: el cortafuegos inspecciona los paquetes que utilizan el protocolo de tunelización de red de área local ampliable virtual (virtual extensible local area network, VXLAN) en el túnel.

STEP 6 | Especifique cuántos niveles de encapsulación inspeccionará el cortafuegos y las condiciones en las que el cortafuegos descartará un paquete.

1. Seleccione **Inspect Options (Opciones de inspección)**.
2. Seleccione los **Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)** que el cortafuegos inspeccionará:
   - **One Level (Un nivel)** (predeterminado): el cortafuegos inspecciona el contenido que está en túnel externo únicamente.

     Con VXLAN, el cortafuegos inspecciona la carga útil de VXLAN para buscar el contenido o las aplicaciones encapsulados dentro del túnel. Debe seleccionar **One Level (Un nivel)** porque la inspección de VXLAN solo se realiza en el túnel externo.
   - **Two Levels (Tunnel In Tunnel) (Dos niveles [túnel en túnel)**: el cortafuegs inspecciona el contenido que está en el túnel externo y el contenido que está en el túnel interno.
3. Para especificar si el cortafuegos descarta los paquetes en determinadas circunstancias, seleccione una de estas opciones, todas o ninguna de ellas:
   - **Drop packet if over maximum tunnel inspection level (Descartar paquete si se supera el nivel máximo de inspección de túnel)**: el cortafuegos descartará el paquete que contenga más niveles de encapsulación de los que están configurados para **Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)**.
   - **Drop packet if tunnel protocol fails strict header check (Descartar paquete si el protocolo del túnel falla en la comprobación estricta de encabezado)**: el cortafuegos descarta un paquete que contiene un protocolo de túnel que utiliza un encabezado que no cumple con el RFC para el

© 2020 Palo Alto Networks, Inc.

protocolo. Los encabezados no compatibles pueden indicar paquetes sospechosos. Esta opción hace que el cortafuegos verifique los encabezados GRE contra RFC 2890.

Si su cortafuegos tuneliza GRE con un dispositivo que implementa una versión de GRE anterior a RFC 2890, no debe habilitar la opción de Drop packet if tunnel protocol fails strict header check (Descartar paquete si el protocolo de túnel falla en la comprobación estricta de encabezado).

- **Drop packet if unknown protocol inside tunnel (Descartar paquete si hay un protocolo desconocido dentro del túnel)**: el cortafuegos descartará el paquete que contenga un protocolo dentro del túnel que el cortafuegos no pueda identificar.

  Por ejemplo, si esta opción está seleccionada, el cortafuegos descartará los paquetes IPSec cifrados que coincidan con la regla de política de inspección de túnel debido a que el cortafuegos no podrá leerlos. Por lo tanto, puede permitir los paquetes IPSec y el cortafuegos permitirá solo los paquetes AH IPsec e IPSec con cifrado Null.
- **Return scanned VXLAN tunnel to source (Devolver el túnel de VXLAN analizado al origen)**: cuando el tráfico se redirige al cortafuegos, VXLAN encapsula el paquete. La redirección del tráfico es una práctica habitual en los entornos de nube pública. Marque **Return scanned VXLAN tunnel to source (Devolver el túnel de VXLAN analizado al origen)** para restituir el paquete encapsulado al terminal del túnel de VXLAN (VXLAN tunnel endpoint, VTEP) de origen. Esta opción solo se admite en la capa 3, la subinterfaz de capa 3, la interfaz agregada de capa 3 y VLAN.

4. Haga clic en **OK (Aceptar)**.

STEP 7 | Gestione las reglas de política de inspección de túnel.

Utilice lo siguiente para gestionar las reglas de política de inspección de túnel:

- (Campo de filtro): muestra solo las reglas de política de túnel nombradas en el campo de filtro.
- **Delete (Eliminar)**: elimina las reglas de política de túnel seleccionadas.
- **Clone (Clonar)**: una alternativa al botón **Add (Añadir)**, que duplica la regla seleccionada con un nuevo nombre, que luego puede modificar.
- **Enable (Habilitar)**: habilita las reglas de política de túnel seleccionadas.
- **Disable (Deshabilitar)**: deshabilita las reglas de política de túnel seleccionadas.
- **Move (Mover)**: desplaza las reglas de política de túnel seleccionadas hacia arriba o hacia abajo en la lista; los paquetes son evaluados según las reglas en orden descendente.
- **Highlight Unused Rules (Destacar reglas no utilizadas)**: resalta las reglas de política de túnel que no coinciden con ningún paquete desde la última vez que el cortafuegos se ha reiniciado.

STEP 8 | (Opcional) Cree una zona de origen de túnel y una zona de destino de túnel para el contenido de túnel y configure una regla de política de seguridad para cada zona.

La práctica recomendada es crear zonas de túnel para su tráfico de túnel. Por lo tanto, el cortafuegos crea sesiones separadas para los paquetes tunelizados y no tunelizados que tienen la misma tupla de cinco (dirección IP y puerto de origen, dirección IP y puerto de destino, y protocolo).

La asignación de zonas de túnel al tráfico de túnel en un cortafuegos de la serie PA-5200 hace que el cortafuegos realice la inspección de túnel en el software; la inspección de túnel no se descarga en el hardware.

1. Si desea que el contenido del túnel esté sujeto a diferentes reglas de la política de seguridad de las reglas de política de seguridad para la zona del túnel externo (configurado anteriormente), seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir un **Name (Nombre)** para Tunnel Source Zone (Zona de origen del túnel).

© 2020 Palo Alto Networks, Inc.

2. Para **Location (Ubicación)**, seleccione el sistema virtual.
3. En **Tipo**, seleccione **Tunnel (Túnel)**.
4. Haga clic en **OK (Aceptar)**.
5. Repita estos pasos secundarios para crear la zona de destino de túnel.
6. Configure una regla de política de seguridad para la zona de origen del túnel.

   Debido a que quizás no conozca al originador del tráfico de túnel o la dirección del flujo del tráfico y no desea prohibir accidentalmente el tráfico para una aplicación a través del túnel, especifique ambas zonas de túnel como la Source Zone (Zona de origen) y ambas zonas de túnel como la Destination Zone (Zona de destino) en su regla de política de seguridad, o seleccione Any (Cuaquiera) para las zonas de origen y destino; y luego especifique las Applications (Aplicaciones).
7. Configure una regla de política de seguridad para la zona de destino del túnel. El consejo en el paso anterior para configurar una regla de política de seguridad para la zona de origen del túnel se aplica también a la zona de destino del túnel.

STEP 9 | (Opcional) Especifique la zona de origen de túnel y la zona de destino de túnel para el contenido interno.

1. Especifique la zona de origen del túnel y la zona de destino del túnel (que acaba de añadir) como las zonas para el contenido interno. Seleccione **Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y en la pestaña **General**, seleccione el **Name (Nombre)** de la regla de política de inspección que ha creado.
2. Seleccione **Inspection (Inspección)**.
3. Seleccione **Security Options (Opciones de seguridad)**.
4. Seleccione **Enable Security Options (Habilitar opciones de seguridad)** (deshabilitado de manera predeterminada) para hacer que el origen del contenido interno pertenezca a la **Tunnel Source Zone (Zona de origen del túnel)** que especifique y que el destino de contenido interno pertenezca a la **Tunnel Destination Zone (Zona de destino del túnel)** que especifique.

   Si no elige **Enable Security Options (Habilitar opciones de seguridad)**, el origen del contenido interno pertenecerá a la misma zona de origen que el origen del túnel externo y el destino de contenido interno pertenecerá a la misma zona de destino que el destino del túnel externo, y por lo tanto estarán sujetos a las mismas reglas de política de seguridad que se aplican a esas zonas externas.
5. En **Tunnel Source Zone (Zona de origen del túnel)**, seleccione la zona de túnel correspondiente que creó en el paso anterior, de modo que las políticas asociadas con esa zona se apliquen a la zona de origen del túnel. De lo contrario, de manera predeterminada, el contenido interno utilizará la misma zona de origen que se utiliza en el túnel externo y las políticas de la zona de origen del túnel externo también aplican a la zona de origen de contenido interno.
6. En **Tunnel Destination Zone (Zona de destino del túnel)**, seleccione la zona de túnel correspondiente que creó en el paso anterior, de modo que las políticas asociadas con esa zona se apliquen a la zona de destino del túnel. De lo contrario, de manera predeterminada, el contenido interno utilizará la misma zona de destino que se utiliza en el túnel externo y las políticas de la zona de destino del túnel externo también aplican a la zona de destino de contenido interno.

   Si configura los valores de Tunnel Source Zone (Zona de origen de túnel) y Tunnel Destination Zone (Zona de destino de túnel) en la regla de la política de inspección de túneles, debe configurar zonas concretas en los campos Source Zone (Zona de origen) (paso 3) y Destination Zone (Zona de destino) (paso 4) de los criterios de coincidencia de dicha regla; no puede especificar Any (Cualquiera) en Source Zone (Zona de origen) ni en Destination Zone (Zona de destino). De este modo, se asegura de que el sentido de la reasignación de zonas se corresponde correctamente con las zonas principales.

© 2020 Palo Alto Networks, Inc.

En los cortafuegos PA-5200 Series y PA-7080, si utiliza la capa subyacente de multidifusión e inspecciona VXLAN, la sesión interna se duplica en varios planos de datos y se pueden producir condiciones de carrera. Para evitar que se descarten algunos paquetes, son imprescindibles los siguientes requisitos:

- *Configure una regla distinta de inspección del contenido de los túneles que busque coincidencias en los paquetes de VXLAN externos que se dirigen a cada uno de los VTEP.*
- *En esa regla independiente, asigne una zona de túnel distinta. De esa forma, la sesión interna es diferente para cada terminal y no se producen condiciones de carrera, ni se descartan paquetes.*

7. Haga clic en **OK (Aceptar)**.

STEP 10 | Establezca opciones de supervisión para el tráfico que coincida con una regla de la política de inspección de túnel.

1. Seleccione **Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y seleccione el nombre de la regla de política de inspección de túnel que ha creado.
2. Seleccione **Inspection (Inspección)** > **Monitor Options (Opciones de supervisión)**.
3. Introduzca un **Monitor Name (Nombre de supervisor)** para agrupar el tráfico similar para fines de registro y elaboración de informes.
4. Introduzca una **Monitor Tag (number) (Etiqueta de supervisión [número])** para agrupar tráfico similar para fines de registro y elaboración de informes (el intervalo es de 1 a 16 777 215). El número de etiqueta se define globalmente.

   Este campo no se aplica al protocolo VXLAN. Los logs de VXLAN usan automáticamente el identificador de red VXLAN (VXLAN network identifier, VNI) del encabezado de VXLAN.

   Si marca el tráfico de túnel, posteriormente puede filtrar la etiqueta de supervisión en el log de inspección de túnel y usar el ACC para ver la actividad del túnel basada en la etiqueta de supervisión.
5. **Anule la configuración de logs de las reglas de seguridad** para permitir las opciones de generación y reenvío de logs para las sesiones que cumplen con la regla de la política de inspección de túnel seleccionada. Si no selecciona esta configuración, la generación y el reenvío de logs de túnel se definen con la configuración de logs de la regla de la política de seguridad que se aplica al tráfico del túnel. Puede anular los ajustes de reenvío de logs en las reglas de la política de seguridad que controlan los logs de tráfico configurando los ajustes de logs de inspección de túnel de modo que los logs de túnel y los logs de tráfico se almacenen por separado. Los logs de inspección de túneles almacenan las sesiones del túnel externo (GRE, IPSec sin cifrar, VXLAN o GTP-U) y los logs de tráfico, los flujos del tráfico interno.
6. Seleccione **Log at Session Start (Log al inicio de la sesión)** para crear logs de tráfico al inicio de la sesión.

   La práctica recomendada para los logs de túnel es crear logs al inicio de la sesión y al final de la sesión debido a que los túneles pueden ser duraderos. Por ejemplo, los túneles de GRE pueden activarse cuando el enrutador se reinicia y no finalizar hasta que el enrutador se reinicie. Si no crea logs al inicio de la sesión, nunca verá si existe un túnel de GRE activo en el ACC.
7. Seleccione **Log at Session End (Log al final de la sesión)** para crear logs de tráfico al final de la sesión.
8. Seleccione un perfil de **Log Forwarding (Reenvío de logs)** que determine dónde reenvía el cortafuegos los logs de túnel de las sesiones que cumplen con la regla de inspección de túnel. De manera alternativa, puede crear un nuevo perfil de reenvío de logs si realiza la Configuración de reenvío de logs.

© 2020 Palo Alto Networks, Inc.

9. Haga clic en **OK (Aceptar)**.

STEP 11 | (Opcional, solo en VXLAN) **Configure un VNI**. Todas las interfaces de red VXLAN se inspeccionan de manera predeterminada. Si configura VNI, la política solo inspecciona los configurados.

VXLAN es el único protocolo que utiliza la pestaña Tunnel ID (ID de túnel) para especificar el VNI.

1. Seleccione la pestaña **Tunnel ID (ID de túnel)** y haga clic en **Add (Añadir)**.
2. Asigne un nombre en **Name (Nombre)**. El nombre es un factor para mayor comodidad, no para la creación de logs, la supervisión o la creación de informes.
3. En el campo **VXLAN ID (VNI) (ID de VXLAN [VNI])**, introduzca un VNI único, una lista de VNI separados por comas, un intervalo de VNI separados por guiones o una combinación de estas opciones. Por ejemplo, puede especificar lo siguiente:

   ```
   1677002,1677003,1677011-1677038,1024
   ```

STEP 12 | (Opcional) Si habilitó **Rematch Sessions (Volver a cotejar sesiones)** (**Device [Dispositivo]** > **Setup [Configuración]** > **Session [Sesión]**), asegúrese de que el cortafuegos no descarte las sesiones existentes cuando cree o revise una política de inspección de túnel deshabilitando **Reject Non-SYN TCP (Rechazar TCP no sincronizados)** para las zonas que controlen sus políticas de seguridad de túnel.

El cortafuegos muestra la siguiente advertencia cuando usted:

- Cree una regla de política de inspección de túnel.
- Edite una regla de política de inspección de túnel añadiendo un **Protocol (Protocolo)** o aumentando los **Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)** de **One Level (Un nivel)** a **Two Levels (Dos niveles)**.
- Seleccione **Enable Security Options (Habilitar las opciones de seguridad)** en la pestaña **Security Options (Opciones de seguridad)** al añadir nuevas zonas o cambiar una zona por otra.

Advertencia: La habilitación de políticas de inspección de túnel en las sesiones de túnel existentes harán que las sesiones TCP existentes dentro del túnel sean tratadas como flujos non-syn-tcp. Para garantizar que las sesiones existentes no se descarten cuando la política de inspección de túnel esté habilitada, configure el ajuste Reject Non-SYN TCP (Rechazar TCP Non-SYN) para las zonas en no, usando un perfil de protección de zona y aplíquelo a las zonas que controlan las políticas de seguridad del túnel. Una vez que las sesiones existentes han sido reconocidas por el cortafuegos, puede volver a habilitar el ajuste Reject Non-SYN TCP (Rechazar TCP Non-SYN) al configurarlo en yes (sí) o global.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un **Name (Nombre)** para el perfil.
3. Seleccione **Packet Based Attack Protection (Protección contra ataques basados en paquetes)** > **TCP Drop (Descarte de TCP)**.
4. Para **Reject Non-SYN TCP (Rechazar TCP Non-SYN)**, seleccione **no**.
5. Haga clic en **OK (Aceptar)**.
6. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione la zona que controla las reglas de la política de seguridad de túnel.
7. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil de protección de zona que acaba de crear.

© 2020 Palo Alto Networks, Inc.

8. Haga clic en **OK (Aceptar)**.
9. Repita los pasos 12.f, 12.g y 12.h anteriores para aplicar el perfil de protección de zonas a las demás zonas que controlan las reglas de la política de seguridad de los túneles.
10. Una vez que las sesiones existentes han sido reconocidas por el cortafuegos, puede volver a habilitar el ajuste **Reject Non-SYN TCP (Rechazar TCP Non-SYN)** al configurarlo en **yes (sí)** o **global**.

STEP 13 | (Opcional) Limite la fragmentación del tráfico en un túnel.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y **Add (Añadir)** para añadir un perfil por **Name (Nombre)**.
2. Introduzca una **Description (Descripción)**.
3. Seleccione una **Packet Based Attack Protection (Protección contra ataques basados en paquetes)** > **IP Drop (Descarte de IP)** > **Fragmented traffic (Tráfico de fragmentación)**.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione la zona de túnel en la que desea limitar la fragmentación.
6. Para **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil que acaba de crear para aplicar el perfil de protección de zona a la zona de túnel.
7. Haga clic en **OK (Aceptar)**.

STEP 14 | **Commit (Confirmar)** los cambios.

Visualización de actividad de túneles inspeccionados

Realice la siguiente tarea para ver la actividad de los túneles inspeccionados.

STEP 1 | Seleccione **ACC** y seleccione un **Virtual System (Sistema virtual)** o **All (Todos)** los sistemas virtuales.

STEP 2 | Seleccione Tunnel Activity (Actividad del túnel).

STEP 3 | Seleccione un Time period (Período) para ver, como Last 24 Hrs (Últimas 24 horas) o Last 30 Days (Últimos 30 días).

STEP 4 | En Global Filters (Filtros globales), haga clic en los botones + o - para utilizar los filtros de ACC en la actividad del túnel.

STEP 5 | Vea la actividad del túnel inspeccionado; puede mostrar u ordenar los datos en cada ventana por **bytes**, **sessions (sesiones)**, **threats (amenazas)**, **content (contenido)** o **URLs**. Cada ventana muestra un aspecto diferente de los datos del túnel en un gráfico o una tabla:

- **Tunnel ID Usage (Uso de ID de túnel):** cada protocolo de túnel enumera los ID de túnel de los túneles que utilizan este protocolo. Las tablas brindan la cantidad total de bytes, las sesiones, las amenazas, el contenido y las URL del protocolo. Coloque el cursor sobre el ID de túnel para obtener un desglose de cada ID de túnel.
- **Tunnel Monitor Tag (Etiqueta de supervisión de túnel):** cada protocolo de túnel enumera las etiquetas de supervisión de túnel de los túneles que utilizan esta etiqueta. Las tablas brindan la cantidad total de bytes, las sesiones, las amenazas, el contenido y las URL de la etiqueta y el protocolo. Coloque el cursor sobre la etiqueta de supervisión de túnel para obtener un desglose de cada etiqueta.
- **Tunneled Application Usage (Uso de aplicaciones de transmisión mediante túneles):** las categorías de aplicaciones muestran mediante gráficos los tipos de aplicaciones agrupados por medios, interés general, colaboración y redes, y códigos de color según su riesgo. Las tablas de las aplicaciones también incluyen un recuento de los usuarios por aplicación.

© 2020 Palo Alto Networks, Inc.

- **Tunneled User Activity (Actividad de usuarios de transmisión mediante túneles):** muestra un gráfico de los bytes enviados y recibidos, por ejemplo, en un eje x de fecha y hora. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto. La tabla de usuario de origen y de usuario de destino brinda datos por usuario.
- **Tunneled Source IP Activity (Actividad IP de origen de transmisión mediante túneles):**muestra gráficos y tablas de bytes, sesiones, y amenazas, por ejemplo, de un atacante en una dirección IP. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto.
- **Tunneled Destination IP Activity (Actividad IP de destino de transmisión mediante túneles):** muestra gráficos y tablas basadas en las direcciones IP de destino. Vea las amenazas de cada víctima en una dirección IP, por ejemplo. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto.

Visualización de información del túnel en logs

Puede ver logs de inspección del túnel o ver información de inspección del túnel en otros tipos de logs.

Protocolos GRE, IPSec sin cifrar y GTP-U

- Cuando se produce una coincidencia con la regla de tráfico de inspección del contenido de los túneles (tunnel content inspection, TCI), los protocolos de encapsulación de enrutamiento genérico (generic routing encapsulation, GRE), de seguridad del protocolo de internet (internet protocol security, IPSec) y de túnel del servicio general de paquetes vía radio para datos de usuario (general packet radio service [GPRS] tunneling protocol for user data, GTP-U) se registran en el log de inspección de túneles con el tipo log Tunnel (Túnel) y el protocolo coincidente, así como el nombre y la etiqueta (número) de supervisión configurados.
- Si no hay ninguna coincidencia con la regla de TCI, todos los protocolos se registran en los logs de tráfico.

Protocolo VXLAN

- Cuando se produce una coincidencia con la regla de TCI, el protocolo VXLAN se registra en el log de inspección de túneles con el tipo log Tunnel (VXLAN) (Túnel [VXLAN]), el nombre de supervisión configurado y el ID del túnel (identificador de red VXLAN [VXLAN network identifier, VNI]).

  En el log de tráfico de la sesión interna, la marca Tunnel Inspected (Túnel inspeccionado) indica una sesión de VNI. La sesión principal es la sesión que estaba activa cuando se creó la sesión interna, por lo que es posible que el ID no coincida con el ID de la sesión actual.
- Si no hay ninguna coincidencia con la regla de TCI, las sesiones de VNI se registran en los logs de tráfico con el protocolo de datagramas de usuario (user datagram protocol, UDP), el puerto de origen 0 y el puerto de destino 4789 (predeterminado).

- Ver logs de inspección del túnel.
  1. Seleccione **Monitor (Supervisión)** > **Logs** > **Tunnel Inspection (Inspección de túneles)** y consulte los datos del log para identificar en **Applications (Aplicaciones)** las aplicaciones de túneles que se utilizan en el tráfico y los posibles problemas, como recuentos elevados de paquetes que no superan la comprobación estricta de encabezados.
  2. Haga clic en el icono de vista detallada () para obtener información detallada sobre el log.

- Visualice otros logs para obtener información sobre la inspección del túnel.
  1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
  2. Seleccione **Traffic (Tráfico)**, **Threat (Amenaza)**, **URL Filtering (Filtrado de URL)**, **WildFire Submissions (Envíos de WildFire)**, **Data Filtering (Filtrado de datos)** o **Unified (Unificado)**.
  3. Haga clic en el icono de vista detallada () en una entrada del log.

© 2020 Palo Alto Networks, Inc.

4. En la ventana Flags (Marcas), consulte si se ha seleccionado la marca **Tunnel Inspected (Túnel inspeccionado)**. Una marca Tunnel Inspected (Túnel inspeccionado) indica que el cortafuegos utilizó una regla de la política Tunnel Inspection (Inspección del túnel) para inspeccionar el contenido interno o túnel interno. La información de Parent Session (Sesión principal) corresponde a un túnel exterior (en relación a un túnel interior) o un túnel interno (en relación al contenido interno).

   En los logs **Traffic (Tráfico)**, **Threat (Amenaza)**, **URL Filtering (Filtrado de URL)**, **WildFire Submissions (Envíos de WildFire)**, **Data Filtering (Filtrado de datos)**, solo la información principal directa aparece en la vista detallada del log de sesión interna, no la información del log del túnel. Si configuró dos niveles de inspección de túnel, puede seleccionar la sesión principal de la información principal directa para ver el segundo log principal. (Debe supervisar el log **Tunnel Inspection [Inspección de túnel]** como se muestra en el paso anterior para ver la información de log de túnel).
5. Mientras consulta el log de una sesión interna en la que se inspeccionan los túneles, haga clic en el enlace **View Parent Session (Ver sesión principal)** de la sección General para ver la información sobre la sesión externa.

Creación de un informe personalizado basado en el tráfico de túnel etiquetado

Puede crear un informe para recoger información en función de la etiqueta que aplicó al tráfico de túnel.

STEP 1 | Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** y haga clic en **Add (Añadir)**.

STEP 2 | En Database (Base de datos), seleccione el log de Tráfico, Amenaza, URL, Filtrado de datos o envíos de WildFire.

STEP 3 | En Available Columns (Columnas disponibles), seleccione Flags (Marcas) y Monitor Tag (Etiqueta de supervisión), además de otros datos que desee incluir en el informe.

También puede generar informes personalizados.

Deshabilitación de aceleración de túneles

De forma predeterminada, los cortafuegos compatibles realizan la aceleración de túneles para mejorar el rendimiento y la producción del tráfico que pasa por túneles GRE, VXLAN y GTP-U. La aceleración del túnel proporciona descarga de hardware para reducir el tiempo que se tarda en realizar búsquedas de flujo y permite que el tráfico del túnel se distribuya de manera más eficiente en función del tráfico interno.

La aceleración del túnel GRE y VXLAN es compatible con los cortafuegos PA-3200 Series y los cortafuegos PA-7000 Series con PA-7000-100G-NPC-A y PA-7050-SMC-B o PA-7080-SMC-B. Puede deshabilitar la aceleración del túnel para solucionar problemas. Cuando deshabilite la aceleración del túnel, lo hará para los túneles GRE, VXLAN y GTP-U simultáneamente.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes generales.

STEP 2 | Anule la selección de **Tunnel Acceleration (Aceleración de túnel)** para desactivarla.

STEP 3 | Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione **Confirmar**.

STEP 5 | Reinicie el cortafuegos.

© 2020 Palo Alto Networks, Inc.

STEP 6 | (Opcional) Verifique el estado de la aceleración del túnel.

1. Acceda la CLI.
2. > **show tunnel-acceleration**

   La salida del sistema puede tener estos estados `Enabled (Habilitado)` o `Disabled (Deshabilitado)`. Estado adicional y motivo de GTP-U únicamente:

   - `Disabled (Deshabilitado)`: la aceleración del túnel GTP-U no es compatible con el modelo de cortafuegos o la seguridad GTP está deshabilitada.
   - `Error (TCI with GTP-U configured unexpectedly) (Error [TCI con GTP-U configurado inesperadamente])`: el TCI con el protocolo GTP-U está configurado cuando Tunnel Acceleration (Aceleración de túnel) está habilitada.
   - `Enabled (Habilitada)`: Tunnel Accelaration (Aceleración de túnel) está habilitada; GTP-U Tunnel Acceleration (Aceleración de túnel GTP-U) no se está ejecutando todavía. La seguridad de GTP está habilitada, pero aún no se reinicia.
   - `Installed (Instalado)`: se está ejecutando la aceleración del túnel GTP-U.

© 2020 Palo Alto Networks, Inc.

Política

Las políticas le permiten aplicar reglas y realizar acciones. Los diferentes tipos de reglas de políticas que puede crear en el cortafuegos son: las políticas de seguridad, NAT, calidad de servicio (QoS), reenvío basado en políticas (PBF), descifrado, cancelación de aplicaciones, autenticación, denegación de servicio (DoS) y protección de zonas. Todas estas diferentes políticas funcionan conjuntamente para permitir, denegar, priorizar, reenviar, cifrar, descifrar, realizar excepciones, autenticar el acceso y restablecer conexiones según sea necesario para ayudar a proteger su red. Los siguientes temas describen cómo trabajar con políticas:

- Tipos de políticas
- Política de seguridad
- Objetos de políticas
- Perfiles de seguridad
- Seguimiento de las reglas de las bases de reglas
- Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas
- Duplicación o traslado de una regla de políticas u objeto a un sistema virtual diferente
- Uso de objetos de dirección para representar direcciones IP
- Uso de etiquetas para agrupar objetos y distinguirlos visualmente
- Uso de una lista dinámica externa en políticas
- Registro de direcciones IP y etiquetas dinámicamente
- Uso de grupos de usuarios dinámicos en políticas
- Uso de etiquetado automático para automatizar acciones de seguridad
- Supervisión de cambios en el entorno virtual
- Comandos de la CLI para etiquetas y direcciones IP
- Identificación de usuarios conectados a través de un servidor proxy
- Reenvío basado en políticas
- Comprobación de las reglas de las políticas

© 2020 Palo Alto Networks, Inc.

Tipos de políticas

El cortafuegos de nueva generación de Palo Alto Networks admite diversos tipos de políticas que se complementan mutuamente para habilitar aplicaciones en su red.

En todos los tipos de políticas, cuando realiza el procedimiento Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas, puede usar el archivo de observaciones de auditoría para comprobar cómo han cambiado sus reglas a lo largo del tiempo. Este archivo incluye tanto el historial de observaciones de auditoría como los logs de configuración, lo que permite comparar las versiones de configuración y comprobar quiénes han creado o modificado elementos y por qué.

Tipo de política	Description (Descripción)
Security	Determina si una sesión se bloqueará o se permitirá basándose en atributos del tráfico, como la zona de seguridad de origen y destino, la dirección IP de origen y destino, la aplicación, el usuario y el servicio. Para obtener información detallada, consulte Política de seguridad.
NAT	Indica al cortafuegos qué paquetes necesitan traducción y cómo realizarla. El cortafuegos admite tanto la traducción de puerto y/o dirección de origen como la traducción de puerto y/o dirección de destino. Para obtener información detallada, consulte NAT.
QoS	Identifica el tráfico que requiere un tratamiento de QoS (ya sea un tratamiento preferente o una limitación del ancho de banda) mediante un parámetro definido o varios parámetros y le asigna una clase. Para obtener información detallada, consulte Calidad de servicio.
Reenvío basado en políticas	Identifica el tráfico que debería usar una interfaz de salida diferente a la que debería usar según la tabla de enrutamiento. Para obtener información detallada, consulte Reenvío basado en políticas.
descifrado	Identifica el tráfico que quiere inspeccionar para ganar visibilidad, control y seguridad granular. Para obtener información detallada, consulte Decifrado.
Cancelación de aplicación	Identifica sesiones que no quiere que procese el motor de App-ID, lo cual es una inspección de capa 7. El tráfico que coincida con una política de cancelación de aplicación obliga a que el cortafuegos gestione la sesión como un cortafuegos de inspección de estado normal en la capa 4. Para obtener información detallada, consulte Gestión de aplicaciones personalizadas o desconocidas.
Autenticación	Identifica el tráfico que requiere que los usuarios se autentiquen. Para obtener información detallada, consulte Política de autenticación.
Protección DoS	Identifica ataques de políticas de denegación de servicio (DoS) y toma medidas de protección que responden a las coincidencias de reglas. Para obtener información detallada, consulte Perfiles de protección DoS.

© 2020 Palo Alto Networks, Inc.

Política de seguridad

La política de seguridad protege los recursos de la red frente a amenazas e interrupciones y facilita su asignación óptima para aumentar la productividad y mejorar la eficiencia de los procesos empresariales. En un cortafuegos de Palo Alto Networks, las reglas de la política de seguridad determinan si una sesión se bloqueará o se permitirá, en función de atributos del tráfico, tales como la zona de seguridad de origen y destino, la dirección IP de origen y destino, la aplicación, el usuario y el servicio.

Para garantizar que los usuarios finales se autentican cuando intentan acceder a los recursos de red, el cortafuegos evalúa la política de autenticación antes que la de seguridad.

Se buscan coincidencias entre todo el tráfico que atraviesa el cortafuegos y una sesión, y entre cada sesión y una regla de la política de seguridad. Cuando se encuentra una coincidencia, el cortafuegos aplica la regla de la política de seguridad coincidente al tráfico bidireccional de esa sesión (cliente a servidor y servidor a cliente). Para el tráfico que no coincide con ninguna regla definida, se aplican las reglas predeterminadas. Las reglas predeterminadas (que aparecen al final de la base de reglas de seguridad) están predefinidas para permitir todo el tráfico dentro de una zona (intrazona) y denegar todo el tráfico entre zonas (interzona). Aunque estas reglas forman parte de la configuración predefinida y son de solo lectura de forma predeterminada, puede sustituirlas y cambiar algunos ajustes, como las etiquetas, la acción (permitir o bloquear), la configuración de los logs y los perfiles de seguridad.

Las reglas de la política de seguridad se evalúan de izquierda a derecha y de arriba a abajo. Un paquete coincide con la primera regla que cumpla los criterios definidos; después de activar una coincidencia, las reglas posteriores no se evalúan. Por lo tanto, las reglas más específicas deben preceder a las más genéricas para aplicar los mejores criterios de coincidencia. El tráfico que coincide con una regla genera una entrada de log al final de la sesión en el log de tráfico, si permite la creación de logs para esa regla. Las opciones de creación de logs pueden configurarse para cada regla. Por ejemplo, se pueden configurar para crear logs al inicio de una sesión en lugar o además de crear logs al final de una sesión.

Cuando el administrador termina la configuración, puede consultar el uso de las reglas de la política para averiguar cuándo y cuántas veces coincide el tráfico con ellas, así como para determinar su eficacia. A medida que se desarrolla la base de reglas, los cambios y la información de auditoría se van perdiendo, a menos que los archive en el momento en que se crean o modifican las reglas. Realice el procedimiento Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas para garantizar que todos los administradores introduzcan las observaciones de auditoría. De ese modo, puede ver el archivo de observaciones de auditoría para consultar el historial de observaciones de auditoría y de logs de configuración, además de comparar las versiones de configuración de las reglas seleccionadas. En conjunto, ahora dispone de más visibilidad sobre la base de reglas y ejerce un mayor control sobre ella.

- Componentes de una regla de política de seguridad
- Acciones de la política de seguridad
- Creación de una regla de política de seguridad

Componentes de una regla de política de seguridad

La construcción de la regla de política de seguridad permite una combinación de los cambios obligatorios y opcionales como se detalla en la tabla siguiente:

Obligatori Opcional	Campo	Description (Descripción)
Obligatorio	**Nombre**	Esta etiqueta de 63 caracteres como máximo identifica la regla.

© 2020 Palo Alto Networks, Inc.

Obligatori Opcional	Campo	Description (Descripción)
	UUID	El identificador único universal (universally unique identifier, UUID) es una cadena exclusiva de 32 caracteres que identifica las reglas de forma permanente y permite realizar su seguimiento aunque sufran modificaciones, por ejemplo, si se cambia el nombre.
	Tipo de regla	Especifica si la regla se aplica al tráfico en una zona, entre zonas o ambas. • **universal** (predeterminado): aplica la regla a todo el tráfico coincidente de interzona e intrazona en las zonas de origen y destino especificadas. Por ejemplo, si crea una regla universal con las zonas de origen A y B y las zonas de destino A y B, esta se aplicará a todo el tráfico dentro de la zona A, a todo el tráfico de la zona B, a todo el tráfico que vaya de la zona A a la B y a todo el tráfico de la zona B a la A. • **intrazone (intrazona)**: aplica la regla a todo el tráfico coincidente dentro de las zonas de origen especificadas (no puede especificar una zona de destino para las reglas de intrazona). Por ejemplo, si establece la zona de origen en A y B, la regla se aplicará a todo el tráfico dentro de la zona A y a todo el tráfico dentro de la zona B, pero no al tráfico entre las zonas A y B. • **intrazone (interzona)**: aplica la regla a todo el tráfico coincidente entre la zona de origen especificada y las zonas de destino. Por ejemplo, si establece la zona de origen en A, B y C y la zona de destino en A y B, la regla se aplicará al tráfico que va de la zona A a la B, de la zona B a la A, de la zona C a la A y de la zona C a la B, pero no al tráfico dentro de las zonas A, B o C.
	Zona de origen	Zona en la que se origina el tráfico.
	Zona de destino	Zona en la que termina el tráfico. Si utiliza NAT, asegúrese de hacer referencia siempre a la zona posterior a NAT.
	Application (Aplicación)	Indica la aplicación que desea controlar. El cortafuegos utiliza App-ID, la tecnología de clasificación de tráfico, para identificar el tráfico de su red. App-ID permite controlar las aplicaciones y ofrece visibilidad al crear políticas de seguridad que bloquean las aplicaciones desconocidas, al tiempo que se habilitan, inspeccionan y moldean las que están permitidas.
	Acción	Especifica la acción *Allow (Permitir)* o *Deny (Denegar)* que se debe aplicar al tráfico según los criterios que defina en la regla. Si configura el cortafuegos para denegar el tráfico, restablece la conexión o descarta los paquetes en segundo plano. Si desea mejorar la experiencia del usuario, puede configurar opciones pormenorizadas para denegar el tráfico en lugar de descartar paquetes en segundo plano, lo que puede provocar que algunas aplicaciones fallen o no respondan. Para obtener más detalles, consulte Acciones de política de seguridad.
Opcional	**Tag (Etiqueta)**	Palabra clave o frase que le permite filtrar las reglas de seguridad. Esto es de utilidad cuando ha definido muchas reglas y desea revisar las que están etiquetadas con una palabra clave específica, como por ejemplo, *aplicaciones aprobadas por TI* o *aplicaciones de alto riesgo*.

© 2020 Palo Alto Networks, Inc.

Obligatori Opcional	Campo	Description (Descripción)
	Description (Descripción)	Campo de texto, de hasta 1024 caracteres, utilizado para describir la regla.
	Dirección de origen	Defina direcciones IP de host, subredes, objetos de dirección (de estos tipos: máscara de red de IP, intervalo de IP, FQDN o máscara comodín de IP), grupos de direcciones o valores aplicados por países. Si utiliza NAT, asegúrese de hacer siempre referencia a las direcciones IP originales del paquete (es decir, la dirección IP anterior a NAT).
	Dirección de destino	Indica la ubicación o el destino del paquete. Defina direcciones IP, subredes, objetos de dirección (de estos tipos: máscara de red de IP, intervalo de IP, FQDN o máscara comodín de IP), grupos de direcciones o valores aplicados por países. Si utiliza NAT, asegúrese de hacer siempre referencia a las direcciones IP originales del paquete (es decir, la dirección IP anterior a NAT).
	Usuario	Usuario o grupo de usuarios a los que se aplica la política. Debe tener habilitado User-ID en la zona. Para habilitar User-ID, consulte Descripción general de la ID de usuario.
	URL Category (Categoría de URL)	El uso de la categoría de URL como criterios de coincidencia le permite personalizar perfiles de seguridad (antivirus, antispyware, vulnerabilidades, bloqueo de archivos, filtrado de datos y DoS) según la categoría de URL. Por ejemplo, puede impedir la descarga/carga de archivos .exe para las categorías de URL que representen un riesgo más alto mientras que sí lo permite para otras categorías. Esta funcionalidad también le permite adjuntar programaciones a categorías de URL específicas (permitir sitios web de redes sociales durante el almuerzo y después de las horas de trabajo), marcar determinadas categorías de URL con QoS (financiera, médica y empresarial) y seleccionar diferentes perfiles de reenvío de logs según la categoría de URL. Aunque puede configurar categorías de URL manualmente en el cortafuegos, adquiera una licencia de URL Filtering para aprovechar las actualizaciones dinámicas de categorización de URL disponibles con los cortafuegos de Palo Alto Networks. *Para bloquear o permitir el tráfico basado en la categoría de URL, deberá aplicar un perfil de filtrado de URL a las reglas de políticas de seguridad. Defina la categoría de URL como Cualquiera y adjunte un perfil de filtrado de URL a la política de seguridad. Consulte* Configuración de una política de seguridad básica *para obtener información sobre el uso de los perfiles predeterminados de su política de seguridad.*
	service	Le permite seleccionar un puerto de capa 4 (TCP o UDP) para la aplicación. Puede seleccionar *any (cualquiera)*, especificar un puerto o usar un *application-default (valor predeterminado de aplicación)* para permitir el uso del puerto basado en estándares de la aplicación. Por ejemplo, en el caso de las aplicaciones con números de puerto conocidos,

© 2020 Palo Alto Networks, Inc.

Obligatori Opcional	Campo	Description (Descripción)
		como DNS, la opción *application-default (valor predeterminado para la aplicación)* solo coincide con el tráfico de DNS del puerto TCP 53. También puede añadir una aplicación personalizada y definir los puertos que puede utilizar la aplicación. *Para reglas de permiso entrante (por ejemplo, de no fiable a fiable), el uso de Valor predeterminado de aplicación impide que las aplicaciones se ejecuten en puertos y protocolos inusuales. El valor por defecto de aplicación es la opción por defecto; si bien el cortafuegos sigue comprobando todas las aplicaciones en todos los puertos, con esta configuración, las aplicaciones solamente están permitidas en sus puertos/protocolos estándar.*
	Perfiles de seguridad	Proporciona una protección adicional frente a amenazas, vulnerabilidades y fugas de datos. Los perfiles de seguridad solo se evalúan con las reglas que tienen la acción *allow (permitir)*.
	HIP Profile (Perfil HIP) (para GlobalProtect)	Le permite identificar a clientes con el perfil de información de host (Host Information Profile, HIP) y, a continuación, aplicar privilegios de acceso.
	Opciones	Le permite definir logging para la sesión, registrar ajustes de reenvío, cambiar marcas de calidad de servicio (Quality of Service, QoS) de paquetes que coincidan con la regla y planificar cuándo (día y hora) debería ser efectiva la regla de seguridad.

Acciones de la política de seguridad

Para el tráfico que coincida con los atributos definidos en una política de seguridad, seleccione una de las acciones siguientes:

Acción	Description (Descripción)
Allow (Permitir) (acción predeterminada)	Permite el tráfico.
Deny (Denegar)	Bloquea el tráfico y aplica la acción por defecto *Denegar* definida para la aplicación que se está denegando. Para ver la acción de denegación definida de manera predeterminada para una aplicación, vea la información detallada de la aplicación en **Objects (Objetos)Applications (Aplicaciones)** o consulte los detalles de las aplicaciones en Applipedia.
Descartar	Descarta en segundo plano el tráfico; para una aplicación, sobrescribe la acción de cancelación predeterminada. No se envía un restablecimiento de TCP al host o la aplicación. Para las interfaces de Capa 3, para enviar opcionalmente una respuesta ICMP inalcanzable al cliente, defina la acción: Seleccione **Drop (Descartar)**

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)
	y habilite la casilla de verificación **Send ICMP Unreachable (Enviar ICMP inalcanzable)**. Cuando está habilitado, el cortafuegos envía el código ICMP que indica que la *comunicación con el destino está administrativamente prohibida*; ICMPv4: Tipo 3, Código 13; ICMPv6: Tipo 1, Código 1.
Reset client (Restablecer cliente)	Envía un restablecimiento de TCP al dispositivo de la parte del cliente.
Reset server (Restablecer servidor)	Envía un restablecimiento de TCP al dispositivo de la parte del servidor.
Reset both (Restablecer ambos)	Envía un restablecimiento de TCP tanto al dispositivo de la parte del cliente como al de la parte del servidor.

Un restablecimiento solo se envía después de que se forme una sesión. Si la sesión se bloquea antes de completar el protocolo de enlace en tres direcciones, el cortafuegos no enviará un restablecimiento.

Para una sesión TCP con una acción de restablecimiento, el cortafuegos no envía una respuesta de ICMP inalcanzable.

Para una sesión UDP con una acción de restablecimiento o descarte, si la casilla de verificación **ICMP Unreachable** está seleccionada, el cortafuegos envía un mensaje de ICMP al cliente.

Creación de una regla de política de seguridad

STEP 1 | (Opcional) Elimine la regla de política de seguridad predeterminada.

Por defecto, el cortafuegos incluye una regla de seguridad denominada *regla1* que permite todo el tráfico desde la zona Fiable a la zona No fiable. Puede eliminar la regla o modificarla para reflejar su convención de denominación de zonas.

STEP 2 | Añada una regla

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)** para añadir una nueva regla.
2. En la pestaña **General**, introduzca un **Name** para la regla.
3. Seleccione un **Rule Type (Tipo de regla)**.

STEP 3 | Defina los criterios de coincidencia para los campos de origen en el paquete.

1. En la pestaña **Source (Origen)**, seleccione la **Source Zone (Zona de origen)**.
2. Especifique una **Source IP Address (Dirección IP de origen)** o deje el valor configurado en **any (cualquiera)**.

   Si decide negar una región como dirección de origen, asegúrese de que todas las regiones que contienen direcciones IP privadas se añadan a la dirección de origen para evitar la pérdida de conectividad entre esas direcciones IP privadas.
3. Especifique un **User (Usuario)** de origen o deje el valor configurado en **any (cualquiera)**.

STEP 4 | Defina los criterios de coincidencia para los campos de destino en el paquete.

1. En la pestaña **Destination (Destino)**, seleccione la **Destination Zone (Zona de destino)**.

© 2020 Palo Alto Networks, Inc.

2. Especifique una **Destination IP Address (Dirección IP de destino)** o deje el valor configurado en **any (cualquiera)**.



Si decide negar una región como dirección de destino, asegúrese de que todas las regiones que contienen direcciones IP privadas se añadan a la dirección de destino para evitar la pérdida de conectividad entre esas direcciones IP privadas.



Se recomienda utilizar objetos de dirección en Destination Address (Dirección de destino) para franquear el acceso únicamente a servidores o grupos de servidores concretos, en particular para servicios como DNS y SMTP, que suelen presentar vulnerabilidades de seguridad. Si restringe el acceso de los usuarios a direcciones del servidor de destino concretas, previene no solo que se filtren datos, sino también que el tráfico de comando y control establezca la comunicación mediante técnicas como la tunelización de DNS.

STEP 5 | Especifique la aplicación que la regla permitirá o bloqueará.



Se recomienda usar siempre reglas de política de seguridad basadas en la aplicación en lugar de reglas basadas en el puerto y establezca siempre Service (Servicio) en application-default (Valor predeterminado de aplicación), a menos que esté utilizando una lista más restrictiva de puertos que los puertos estándar para una aplicación.

1. En la pestaña **Applications (Aplicaciones)**, seleccione **Add (Añadir)** para añadir la **Application (Aplicación)** que desea habilitar de modo seguro. Puede seleccionar varias aplicaciones o utilizar grupos de aplicaciones o filtros de aplicación.
2. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, mantenga Service (Servicio) configurado en **application-default (aplicación-predeterminado)** para garantizar que todas las aplicaciones que la regla permite se permitan únicamente en los puertos estándar.

STEP 6 | (Opcional) Especifique una categoría de URL como criterio de coincidencia para la regla.

En la pestaña **Service/URL Category (Categoría de URL/servicio)**, seleccione la **URL Category (Categoría de URL)**.

Si selecciona una categoría de URL, solo el tráfico web coincidirá con la regla y solo si el tráfico se destina a la categoría especificada.

STEP 7 | Defina qué acción desea que el cortafuegos realice para el tráfico que coincide con la regla.

En la pestaña **Actions**, seleccione una **acción**. Consulte Acciones de política de seguridad para obtener una descripción de cada acción.

STEP 8 | Configure los ajustes de log.

- Por defecto, la regla está configurada en **Log at Session End**. Puede deshabilitar esta configuración si no desea que se generen logs cuando el tráfico coincide con esta regla o seleccione **Log at Session Start (Log al iniciar sesión)** para una generación de logs más detallada.
- Seleccione un perfil de **Log Forwarding**.



Se recomienda que no seleccione la casilla de verificación para Disable Server Response Inspection (Deshabilitar inspección de respuesta de servidor) (DSRI). Si selecciona esta opción, evitará que el cortafuegos inspeccione paquetes desde el servidor al cliente. Para obtener una mejor postura de seguridad, el cortafuegos debe inspeccionar los flujos de cliente a servidor y de servidor a cliente para detectar y prevenir amenazas.

© 2020 Palo Alto Networks, Inc.

STEP 9 | Adjunte perfiles de seguridad para habilitar el cortafuegos para que explore todo el tráfico permitido en busca de amenazas.

Asegúrese de crear perfiles de seguridad recomendados que protejan su red contra amenazas conocidas y desconocidas.

En la pestaña **Actions (Acciones)**, seleccione **Profiles (Perfiles)** en el menú desplegable **Profile Type (Tipo de perfil)** y luego seleccione los perfiles de seguridad individuales para adjuntar la regla.

O bien, seleccione **Group** en el menú desplegable **Profile Type** y seleccione un **Group Profile** de seguridad para adjuntar.

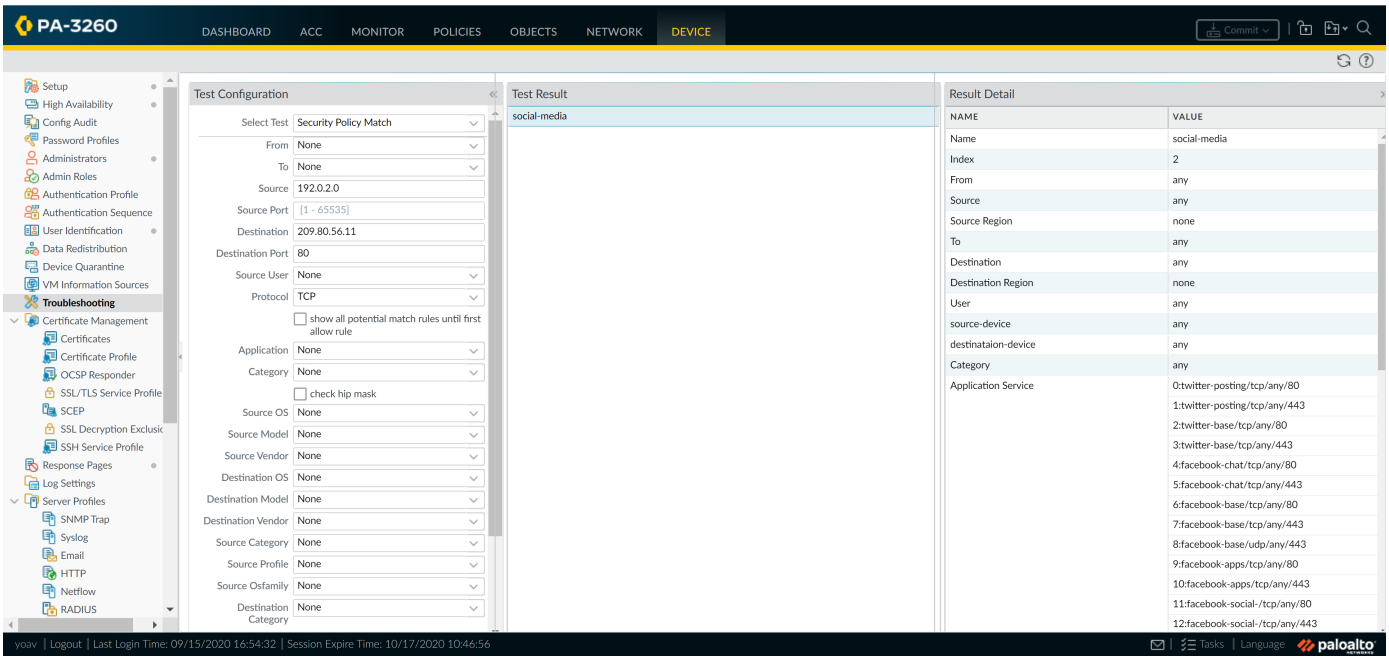
STEP 10 | Haga clic en **Commit (Confirmar)** para guardar la regla de la política en la configuración que se está ejecutando en el cortafuegos.

STEP 11 | Para verificar que ha configurado las políticas de seguridad básicas de manera eficaz, compruebe si se están evaluando sus reglas y determine cuál de ellas se aplica a cada flujo de tráfico.

El resultado muestra la regla que coincide mejor con la dirección IP de origen y destino especificada en el comando de la CLI.

Por ejemplo, para verificar la regla de política que se aplicará a un servidor en el centro de datos con la dirección IP 208.90.56.11 cuando accede al servidor de actualización de Microsoft:

1. Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y, luego, seleccione **Security Policy Match (Coincidencia con política de seguridad)** en el menú desplegable Select Test (Seleccionar prueba).
2. Introduzca las direcciones IP correspondientes en Source (Origen) y en Destination (Destino).
3. Introduzca el protocolo.
4. Haga clic en **Execute (Ejecutar)** para comprobar la coincidencia con la política de seguridad.



© 2020 Palo Alto Networks, Inc.

STEP 12 | Tras esperar lo suficiente para permitir que el tráfico pase a través del cortafuegos, vea la utilización de la regla de la política para supervisar el estado de la utilización de la regla de la política y determinar la efectividad de la regla de la política.

© 2020 Palo Alto Networks, Inc.

Objetos de políticas

Un *objeto de política* es un objeto único o una unidad colectiva que agrupa identidades discretas, como direcciones IP, URL, aplicaciones o usuarios. Con objetos de políticas que sean unidades colectivas, podrá hacer referencia al objeto en la política de seguridad en lugar de seleccionar manualmente varios objetos de uno en uno. Por lo general, al crear un objeto de política, se agrupan objetos que requieran permisos similares en la política. Por ejemplo, si su organización utiliza un conjunto de direcciones IP de servidor para autenticar usuarios, podrá agrupar el conjunto de direcciones IP de servidor como objeto de política de *grupo de direcciones* y hacer referencia al grupo de direcciones en la política de seguridad. Al agrupar objetos, podrá reducir significativamente la carga administrativa al crear políticas.



Si debe exportar partes específicas de la configuración para una revisión o auditoría interna, puede realizar la Exportación de los datos de la tabla de configuración *como un archivo PDF o CSV.*

Puede crear los siguientes objetos de políticas en el cortafuegos:

Objeto de política	Description (Descripción)
Dirección/Grupo de direcciones, Región	Le permite agrupar direcciones de origen o destino específicas que requieren el mismo cumplimiento de política. El objeto de dirección puede incluir una dirección IPv4 o IPv6 (una IP, un intervalo o una subred), una dirección comodín de IP (una dirección IPv4 o una máscara comodín) o un FQDN. También puede definir una región por las coordenadas de latitud y longitud o seleccionar un país y definir la dirección IP o el intervalo de IP. A continuación puede agrupar un conjunto de objetos de dirección para crear un objeto de grupo de direcciones. También puede utilizar grupos de direcciones dinámicas para actualizar dinámicamente direcciones IP en entornos donde las direcciones IP de host cambian frecuentemente. *Las listas dinámicas externas (external dynamic list, EDL) predefinidas del cortafuegos cuentan para el número máximo de objetos de dirección que admite ese modelo de cortafuegos.*
Usuario/grupo de usuarios	Le permite crear una lista de usuarios desde la base de datos local, una base de datos externa o criterios de coincidencia, y agruparlos.
Grupo de aplicaciones y Filtro de aplicación	Un Filtro de aplicación le permite filtrar aplicaciones dinámicamente. Le permite filtrar y guardar un grupo de aplicaciones mediante los atributos definidos en la base de datos de la aplicación en el cortafuegos. Por ejemplo, puede realizar la Creación de un filtro de aplicaciones según uno o más atributos (categoría, subcategoría, tecnología, riesgo y características). Con un filtro de aplicaciones, cuando se produce una actualización de contenido, las nuevas aplicaciones que coincidan con sus criterios de filtro se añadirán automáticamente a su filtro de aplicación guardado. Un grupo de aplicaciones le permite crear un grupo estático de aplicaciones específicas que desee agrupar para un grupo de usuarios, para un servicio en

© 2020 Palo Alto Networks, Inc.

Objeto de política	Description (Descripción)
	concreto o para lograr un objetivo de políticas concreto. Consulte Creación de un grupo de aplicaciones.
Servicio/Grupos de servicios	Le permite especificar los puertos de origen y destino y el protocolo que puede utilizar un servicio. El cortafuegos incluye dos servicios predefinidos (servicio-http y servicio-https) que utilizan los puertos 80 y 8080 de TCP para HTTP y el puerto 443 de TCP para HTTPS. Sin embargo, puede crear cualquier servicio personalizado en cualquier puerto TCP/UDP de su elección para restringir el uso de la aplicación a puertos específicos de su red (dicho de otro modo, puede definir el puerto predeterminado para la aplicación).  *Para ver los puertos estándar utilizados por una aplicación, en Objects (Objetos) > Applications (Aplicaciones), busque la aplicación y haga clic en el enlace. Aparecerá una descripción concisa.*

© 2020 Palo Alto Networks, Inc.

Perfiles de seguridad

Si bien con las reglas de política de seguridad puede permitir o bloquear el tráfico en su red, los perfiles de seguridad le ayudan a definir una regla de *permitir pero inspeccionar*, que explora las aplicaciones permitidas en busca de amenazas, tales como virus, software malintencionado, spyware y ataques DDOS. Cuando el tráfico coincida con la regla de permiso definida en la política de seguridad, los perfiles de seguridad vinculados a la regla se aplicarán para reglas de inspección de contenido adicionales, como comprobaciones antivirus y filtrado de datos.

Los perfiles de seguridad no se utilizan en los criterios de coincidencia de un flujo de tráfico. El perfil de seguridad se aplica para explorar el tráfico después de que la política de seguridad permita la aplicación o categoría.

El cortafuegos proporciona perfiles de seguridad por defecto que puede utilizar inmediatamente para empezar a proteger su red frente a amenazas. Consulte Configuración de una política de seguridad básica para obtener información sobre el uso de los perfiles predeterminados de su política de seguridad. Cuando conozca mejor las necesidades de seguridad de su red, consulte Creación de perfiles de seguridad recomendados para la puerta de enlace de internet para descubrir cómo crear perfiles personalizados.

Para obtener recomendaciones sobre los ajustes recomendados para perfiles de seguridad, consulte Creación de perfiles de seguridad recomendados para la puerta de enlace de internet*.*

Puede añadir perfiles de seguridad que se aplican habitualmente juntos para crear un grupo de perfiles de seguridad; este conjunto de perfiles se puede tratar como una unidad y añadirlo a las políticas de seguridad en un solo paso (o incluirlo en políticas de seguridad de manera predeterminada, si opta por configurar un grupo de perfiles de seguridad predeterminado).

Tipo de perfil	Description (Descripción)
Perfiles de antivirus	Los perfiles de antivirus protegen contra virus, gusanos, troyanos y descargas de spyware. Al usar un motor de prevención contra software malintencionado basado en secuencias, que analiza el tráfico nada más recibir el primer paquete, la solución antivirus de Palo Alto Networks puede ofrecer protección para clientes sin que esto tenga un impacto significativo en el rendimiento del cortafuegos. Este perfil analizará una gran variedad de software malintencionado en archivos ejecutables, PDF, HTML y virus JavaScript, incluida la compatibilidad con el análisis dentro de archivos comprimidos y esquemas de codificación de datos. Si ha habilitado el Decryption (Descifrado) en el cortafuegos, el perfil también habilita el análisis de contenido descifrado. El perfil predeterminado inspecciona todos los decodificadores de protocolos enumerados para virus y genera alertas para protocolos SMTP, IMAP y POP3 al tiempo que bloquea protocolos FTP, HTTP y SMB. Puede configurar la acción para una firma de decodificador o antivirus, y especificar cómo responde el cortafuegos ante un evento de amenaza: • **Default (Predeterminado)**: para cada firma de amenazas y firma de antivirus que define Palo Alto Networks, se especifica internamente una acción predeterminada. Por lo general, la acción predeterminada es una alerta o un restablecimiento de ambos. La acción predeterminada se muestra entre paréntesis, por ejemplo predeterminado (alertar) en la firma de amenazas o antivirus.

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	• **Permitir**: Permite el tráfico de la aplicación.  *La acción Allow (Permitir) no genera logs relacionados con firmas o perfiles.* • **Alert (Alerta)**: genera una alerta para el flujo de tráfico de cada aplicación. La alerta se guarda en el log de amenazas. • **Drop (Descartar)**: cancela el tráfico de la aplicación. • **Reset Client**: para TCP, restablece la conexión de la parte del cliente. Para UDP, cancela la conexión. • **Reset Server**: para TCP, restablece la conexión de la parte del servidor. Para UDP, cancela la conexión. • **Reset Both (Restablecer ambos)**: para TCP, restablece la conexión tanto en el extremo del cliente como en el del servidor. Para UDP, cancela la conexión. Los perfiles personalizados se pueden utilizar para minimizar la exploración antivirus para el tráfico entre zonas de seguridad fiables y para maximizar la inspección o el tráfico recibido de zonas no fiables, como internet, así como el tráfico enviado a destinos altamente sensibles, como granjas de servidores. El sistema WildFire de Palo Alto Networks también ofrece firmas para amenazas persistentes más evasivas y que todavía no han sido descubiertas por otras soluciones de antivirus. A medida que WildFire detecta amenazas, se van creando las firmas rápidamente y después se integran en las firmas de antivirus estándar que los suscriptores de prevención de amenazas pueden descargar todos los días (o cada menos de una hora en el caso de suscriptores de WildFire).
perfil de antispyware	Los perfiles de antispyware impiden que el spyware intente realizar llamadas a casa o balizamiento a servidores externos de comando y control (C2) en hosts comprometidos, lo que le permite detectar el tráfico malintencionado que sale de la red desde clientes infectados. Puede aplicar diversos niveles de protección entre zonas. Por ejemplo, tal vez desee tener perfiles antispyware personalizados que reduzcan al mínimo la inspección entre zonas fiables y amplíen al máximo la inspección del tráfico procedente de una zona no fiable, como zonas de Internet. Cuando un servidor de gestión Panorama es el encargado de administrar el cortafuegos, el ThreatID se asigna a la amenaza personalizada correspondiente en el cortafuegos para permitir que este genere un log de amenazas con el ThreatID personalizado configurado. Puede definir sus propios perfiles antispyware, o bien elegir uno de los siguientes perfiles predefinidos al aplicar antispyware a una regla de política de seguridad: • **Predeterminado**: Usa la acción predeterminada para cada firma, tal como especifica Palo Alto Networks al crear la firma. • **Estricto**: Anula la acción predeterminada de amenazas de gravedad crítica, alta y media para la acción de bloqueo, independientemente de la acción definida en el archivo de firma. Este perfil sigue usando la acción predeterminada para firmas de gravedad baja o informativa. Cuando el cortafuegos detecte un evento de amenazas, puede configurar las siguientes acciones en un perfil antispyware:

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	• **Default (Predeterminado)**: para cada firma de amenazas y firma de antispyware que define Palo Alto Networks, se especifica internamente una acción por defecto. Por lo general, la acción predeterminada es una alerta o un restablecimiento de ambos. La acción predeterminada se muestra entre paréntesis, por ejemplo predeterminado (alertar) en la firma de amenazas o antivirus. • **Allow**: permite el tráfico de la aplicación.  *La acción Allow (Permitir) no genera logs relacionados con firmas o perfiles.* • **Alert (Alerta)**: genera una alerta para el flujo de tráfico de cada aplicación. La alerta se guarda en el log de amenazas. • **Drop (Descartar)**: cancela el tráfico de la aplicación. • **Reset Client**: para TCP, restablece la conexión de la parte del cliente. Para UDP, cancela la conexión. • **Reset Server**: para TCP, restablece la conexión de la parte del servidor. Para UDP, cancela la conexión. • **Reset Both (Restablecer ambos)**: para TCP, restablece la conexión tanto en el extremo del cliente como en el del servidor. Para UDP, cancela la conexión.  *En algunos casos, cuando la acción del perfil se configura en reset-both (Restablecer ambos), el log de amenazas asociado podría mostrar la acción como reset-server (Restablecer servidor). Esto ocurre cuando el cortafuegos detecta una amenaza al comienzo de una sesión y presenta al cliente una página de bloqueo 503. Debido a que la página de bloqueo impide la conexión, el lado del cliente no necesita restablecerse y solo se restablece la conexión del lado del servidor.* • **Block IP (Bloquear IP)**: esta acción bloquea el tráfico de un par de origen u origen-destino. Es configurable durante un periodo de tiempo especificado. Asimismo, puede habilitar la acción de sinkholing de DNS en perfiles de antispyware para que el cortafuegos genere una respuesta errónea a una consulta DNS para un dominio malintencionado conocido, lo que hace que el nombre de dominio malintencionado se resuelva en una dirección IP que usted defina. Esta característica ayuda a identificar los hosts infectados en la red protegida usando tráfico DNS. Los hosts infectados pueden identificarse fácilmente en los logs de tráfico y amenaza porque cualquier host que intente conectarse a la dirección IP sinkhole está infectado casi con toda seguridad con software malintencionado. Los perfiles de protección contra vulnerabilidades y antispyware se configuran de forma similar.
Perfiles de protección de vulnerabilidades	Los perfiles de protección de vulnerabilidades detienen los intentos de explotación de fallos del sistema y de acceso no autorizado a los sistemas. Mientras que los perfiles antispyware ayudan a identificar hosts infectados como tráfico que abandona la red, los perfiles de protección de vulnerabilidades protegen contra las amenazas que acceden a la red. Por ejemplo, los perfiles de protección de vulnerabilidades ayudan a proteger

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	contra desbordamiento de búfer, ejecución de código ilegal y otros intentos de explotar las vulnerabilidades del sistema. El perfil predeterminado de protección contra vulnerabilidades protege a clientes y servidores de todas las amenazas conocidas de gravedad crítica, alta y media. También puede crear excepciones, que le permiten cambiar la respuesta a una firma concreta. Cuando un servidor de gestión Panorama es el encargado de administrar el cortafuegos, el ThreatID se asigna a la amenaza personalizada correspondiente en el cortafuegos para permitir que este genere un log de amenazas con el ThreatID personalizado configurado. Cuando el cortafuegos detecte un evento de amenazas, puede configurar las siguientes acciones en un perfil antispyware: • **Default (Predeterminado)**: para cada firma de amenazas y firma de antispyware que define Palo Alto Networks, se especifica internamente una acción por defecto. Por lo general, la acción predeterminada es una alerta o un restablecimiento de ambos. La acción predeterminada se muestra entre paréntesis, por ejemplo predeterminado (alertar) en la firma de amenazas o antivirus. • **Allow**: permite el tráfico de la aplicación.  *La acción Allow (Permitir) no genera logs relacionados con firmas o perfiles.* • **Alert (Alerta)**: genera una alerta para el flujo de tráfico de cada aplicación. La alerta se guarda en el log de amenazas. • **Drop (Descartar)**: cancela el tráfico de la aplicación. • **Reset Client**: para TCP, restablece la conexión de la parte del cliente. Para UDP, cancela la conexión. • **Reset Server**: para TCP, restablece la conexión de la parte del servidor. Para UDP, cancela la conexión. • **Reset Both (Restablecer ambos)**: para TCP, restablece la conexión tanto en el extremo del cliente como en el del servidor. Para UDP, cancela la conexión.  *En algunos casos, cuando la acción del perfil se configura en reset-both (Restablecer ambos), el log de amenazas asociado podría mostrar la acción como reset-server (Restablecer servidor). Esto ocurre cuando el cortafuegos detecta una amenaza al comienzo de una sesión y presenta al cliente una página de bloqueo 503. Debido a que la página de bloqueo impide la conexión, el lado del cliente no necesita restablecerse y solo se restablece la conexión del lado del servidor.* • **Block IP (Bloquear IP)**: esta acción bloquea el tráfico de un par de origen u origen-destino. Es configurable durante un periodo de tiempo especificado.
Perfiles de filtrado de URL	Los perfiles de filtrado de URL le permiten supervisar y controlar el modo en que los usuarios acceden a la web a través de HTTP y HTTPS. El cortafuegos incluye un perfil predeterminado que está configurado para bloquear sitios web tales como sitios conocidos de software malintencionado, de phishing y con contenido para adultos. Puede utilizar el perfil predeterminado en una política de seguridad, duplicarlo para utilizarlo como punto de partida

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	para nuevos perfiles de filtrado de URL o añadir un nuevo perfil de URL que tenga todas las categorías establecidas como permitidas para lograr visibilidad del tráfico de su red. A continuación, podrá personalizar los perfiles de URL recién añadidos y añadir listas de sitios web específicos que siempre deberían bloquearse o permitirse, lo que proporciona un control más detallado de las categorías de URL.
Perfiles de filtrado de datos	Los perfiles de filtrado de datos evitan que la información confidencial, como los números de tarjeta de crédito o seguridad social, salga de la red protegida. El perfil de filtrado de datos también le permite filtrar por palabras clave, como el nombre de un proyecto confidencial o la palabra confidencial. Es importante centrar su perfil en el tipo de archivos deseado para reducir los falsos positivos. Por ejemplo, puede que solo quiera buscar documentos de Word o Excel. O tal vez solo quiera analizar el tráfico de navegación web o FTP. Puede crear objetos de patrón de datos personalizados y adjuntarlos a un perfil de filtrado de datos para definir el tipo de información que desea filtrar. Cree objetos de patrón de datos basados en lo siguiente: • **Predefined Patterns (Patrones predefinidos)**: filtre números de tarjeta de crédito y seguridad social (con o sin guiones) usando patrones predefinidos. • **Regular Expressions (Expresiones regulares)**: filtre por cadena de caracteres. • **File Properties (Propiedades de archivo)**: filtre por propiedades de archivo y valores basados en el tipo de archivo.  *Si utiliza soluciones de prevención de pérdida de datos (data loss prevention, DLP) de endpoint de terceros para completar las propiedades de archivo a fin de indicar contenido delicado, esta opción permite que el cortafuegos aplique su política DLP.* Para comenzar, realice la Configuración del filtrado de datos.
Perfiles de bloqueo de archivo	El cortafuegos usa los perfiles de bloqueo de archivos para bloquear tipos de archivos especificados y en la dirección de flujo de sesión especificada (entrante/saliente/ambas). Puede establecer el perfil para emitir alertas o realizar bloqueos en cargas y descargas y puede especificar qué aplicaciones quedarán sujetas al perfil de bloqueo de archivos. También puede configurar páginas de bloqueo personalizadas que aparecerán cuando un usuario intente descargar el tipo de archivo especificado. Esto permite al usuario dedicar unos instantes a considerar si desea o no descargar el archivo. Puede definir sus propios perfiles de bloqueo de archivo, o bien elegir uno de los siguientes perfiles predefinidos al aplicar bloqueo de archivos a una regla de política de seguridad: Los perfiles predefinidos, que están disponibles con la versión de actualización de contenido 653 y posteriores, le permiten habilitar rápidamente los ajustes recomendados de bloqueo de archivos: • **basic file blocking (bloqueo de archivo básico)**: adjunte este perfil para las reglas de política de seguridad que permiten el tráfico hacia y desde las aplicaciones menos sensibles para bloquear archivos que habitualmente

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	se incluyen en campañas de ataques de malware o que no tienen un caso de uso real para la carga/descarga. Este perfil bloquea la carga y descarga de archivos PE (.scr, .cpl, .dll, .ocx, .pif, .exe), archivos Java (.class, .jar), archivos de ayuda (.chm, .hlp) y otros archivos posiblemente malintencionados, incluidos .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. Además, solicita a los usuarios una confirmación al intentar descargar archivos rar o zip cifrados. Esta regla alerta sobre todos los otros tipos de archivo, a fin de brindarle visibilidad completa de todos los tipos de archivo que entran a la red y que salen de ella. • **strict file blocking (bloqueo de archivo estricto)**: use este perfil más estricto en las reglas de política de seguridad que permiten el acceso a sus aplicaciones más delicadas. Este perfil bloquea los mismos tipos de archivo que el otro perfil, y además bloquea archiso flash, .tar, codificación multinivel, .cab, .msi, y archivos rar y zip cifrados. Configure un perfil de bloqueo de archivos con las siguientes acciones: • **Alertar**: Cuando se detecta el tipo de archivo especificado, se genera un log en el log de filtrado de datos. • **Bloquear**: Cuando se detecta el tipo de archivo especificado, se bloquea el archivo y se presenta al usuario una página de bloqueo personalizable. También se genera un log en el log de filtrado de datos. • **Continuar**: Cuando se detecta el tipo de archivo especificado, se presenta al usuario una página de respuesta personalizable. El usuario puede hacer clic en la página para descargar el archivo. También se genera un log en el log de filtrado de datos. Dado que este tipo de acción de reenvío requiere la interacción del usuario, solo se aplica al tráfico web. Para comenzar, realice la Configuración del filtrado de datos.
Perfiles de análisis de WildFire	Use un perfil de análisis de WildFire para permitir que el cortafuegos reenvíe los archivos o enlaces de correo electrónico desconocidos para el análisis de WildFire. Especifique los archivos que se enviarán para el análisis basado en aplicaciones, el tipo de archivo y la dirección de la transmisión (carga o descarga). Los archivos o enlaces de correo electrónico comparados con la regla de perfil se reenvían a la nube pública de WildFire o la nube privada de WildFire (alojadas con un dispositivo WF-500), en función de la ubicación del análisis definido para la regla. Si una regla de perfil está configurada para reenviar archivos a la nube pública de WildFIre, el cortafuegos también debe reenviar los archivos que coincidan con las firmas de antivirus existentes, además de los archivos desconocidos. También puede usar perfiles de análisis de WildFire para configurar una implementación de nube híbrida de WildFire. Si está usando un dispositivo WildFire para analizar archivos sensibles localmente (como PDF), puede especificar tipos de archivos menos sensibles (como archivos PE) o tipos de archivo no compatibles con el análisis de dispositivos WildFire (como APK) para que se analicen mediante la nube pública de WildFire. El uso del dispositivo WildFire y la nube WildFire para el análisis le permite disfrutar de un rápido veredicto de los archivos que ya hayan sido procesados por la nube y de los archivos que no admiten el análisis del dispositivo; además, libera la capacidad del dispositivo para procesar el contenido sensible.

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
Perfiles de protección DoS	Los perfiles de protección DoS ofrecen un control detallado de las políticas de protección contra ataques por denegación de servicio (DoS). Las políticas DoS permiten controlar el número de sesiones entre interfaces, zonas, direcciones y países, basadas en sesiones agregadas o direcciones IP de origen o destino. Hay dos mecanismos de protección DoS compatibles con los cortafuegos de Palo Alto Networks. • **Protección contra inundaciones**: Detecta y evita los ataques en los que la red está inundada con paquetes y esto provoca que haya muchas sesiones a medio abrir o servicios que no pueden responder a cada solicitud. En este caso la dirección de origen del ataque suele estar falsificada. Consulte Protección DoS contra inundaciones de nuevas sesiones. • **Protección de recursos**: Detecta y previene los ataques de agotamiento por sesiones. En este tipo de ataque, se usa un gran número de hosts (bots) para establecer el mayor número posible de sesiones completas para consumir todos los recursos del sistema. Puede habilitar ambos tipos de mecanismos de protección en un único perfil de protección DoS. El perfil DoS se usa para especificar el tipo de acción que se llevará a cabo y los detalles de los criterios de coincidencia para la política DoS. El perfil DoS define ajustes para inundaciones de ICMP, SYN y UDP, puede habilitar la protección de recursos y define el número máximo de conexiones simultáneas. Una vez configurado el perfil de protección DoS, agréguelo a una política DoS. Al configurar protección DoS, es importante analizar su entorno para establecer los umbrales correctos y, debido a algunas de las complejidades para definir las políticas de protección DoS, esta guía no ofrece ejemplos detallados.
Perfiles de protección de zonas	Los perfiles de protección de zona ofrecen protección adicional entre zonas de red específicas para protegerlas de los ataques. El perfil debe aplicarse a toda la zona, así que es importante probar cuidadosamente los perfiles para evitar que surjan problemas cuando el tráfico normal cruce la zona. Si define límites de umbral de paquetes por segundo (pps) de perfiles de protección de zonas, el umbral se basa en los paquetes por segundo que no coinciden con ninguna sesión establecida previamente.
Grupo de perfiles de seguridad	Un grupo de perfiles de seguridad es un conjunto de perfiles de seguridad que se puede tratar como una unidad y añadirse después fácilmente a las políticas de seguridad. Los perfiles que se suelen asignar juntos se pueden combinar en grupos de perfiles para simplificar la creación de políticas de seguridad. También puede configurar un grupo de perfiles de seguridad predeterminado: las nuevas políticas de seguridad usarán los ajustes definidos en el grupo de perfiles de seguridad predeterminado para comprobar y controlar el tráfico coincidente con la política de seguridad. Asigne un nombre al grupo de perfiles de seguridad predeterminado para permitir que los perfiles de ese grupo se añadan a las nuevas políticas de seguridad de manera predeterminada. Esto le permite incluir consistente y automáticamente los ajustes de perfiles preferidos de su organización en nuevas políticas, sin necesidad de añadir manualmente perfiles de seguridad cada vez que crea nuevas reglas.

© 2020 Palo Alto Networks, Inc.

Tipo de perfil	Description (Descripción)
	Consulte Creación de un grupo de perfiles de seguridad y Configuración o cancelación de un grupo de perfiles de seguridad predeterminado. *Para obtener recomendaciones sobre los ajustes recomendados para perfiles de seguridad, consulte* Creación de perfiles de seguridad recomendados para la puerta de enlace de internet.

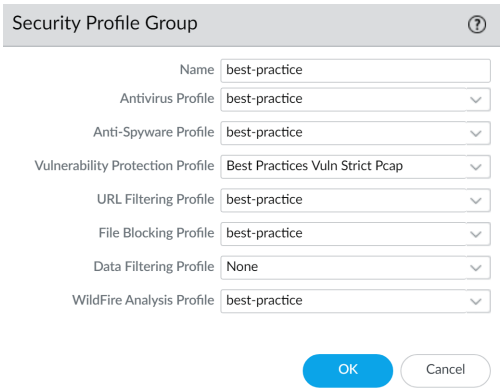
Creación de un grupo de perfiles de seguridad

Siga estos pasos para crear un grupo de perfiles de seguridad y añadirlo a una política de seguridad.

STEP 1 | Cree un grupo de perfiles de seguridad.

Si nombra el grupo como `default`, el cortafuegos automáticamente lo adjuntará a las reglas nuevas que cree. Esto permite ahorrar tiempo si tiene un conjunto preferido de perfiles de seguridad que desea asegurarse de adjuntar a cada nueva regla.

1. Seleccione **Objects (Objetos)** > **Security Profile Groups (Grupos de perfiles de seguridad)** y haga clic en **Add (Añadir)** para añadir un grupo nuevo.
2. Asígnele un **nombre** descriptivo al grupo de perfiles, p. ej., Amenazas.
3. Si el cortafuegos está en modo de Sistema virtual múltiple, habilite el perfil para que sea **Shared** y puedan compartirlo todos los sistemas virtuales.
4. Añada perfiles existentes al grupo.



5. Haga clic en **Aceptar** para guardar el grupo de perfiles.

STEP 2 | Añada un grupo de perfiles de seguridad a una política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de política de seguridad.
2. Seleccione la pestaña **Actions (Acciones)**.
3. En la sección Profile Setting (Configuración de perfil), seleccione **Group (Grupo)** para el **Profile Type (Tipo de perfil)**.
4. En el menú desplegable **Group Profile (Perfil de grupo)**, seleccione el grupo que ha creado (por ejemplo, seleccione el grupo recomendado):

© 2020 Palo Alto Networks, Inc.



5. Haga clic en **OK (Aceptar)** para guardar la política y en **Commit (Confirmar)** para confirmar sus cambios.

STEP 3 | Guarde los cambios.

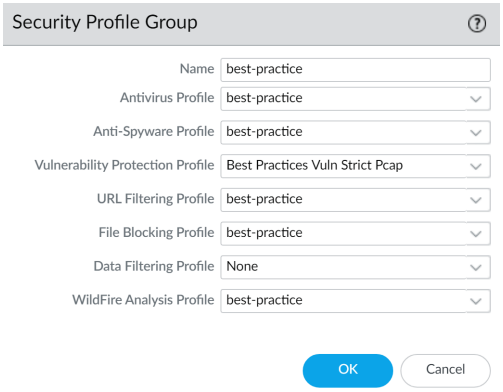
Haga clic en **Commit (Confirmar)**.

Configuración o cancelación de un grupo de perfiles de seguridad predeterminado

Use las siguientes opciones para configurar un grupo de perfiles de seguridad predeterminado y usarlo en las nuevas políticas de seguridad, o bien para cancelar un grupo predeterminado existente. Cuando un administrador crea una nueva política de seguridad, el grupo de perfiles predeterminado se selecciona automáticamente como los ajustes de perfil de la política, y el tráfico que coincida con la política se comprobará siguiendo los ajustes definidos en el grupo de perfiles (el administrador puede optar por seleccionar manualmente los distintos ajustes de perfil si lo desea). Use las siguientes opciones para configurar un grupo de perfiles de seguridad predeterminado o cancelar sus ajustes predeterminados.

Si no hay ningún perfil de seguridad predeterminado, la configuración del perfil para la nueva política de seguridad se establece en Ninguno de forma predeterminada.

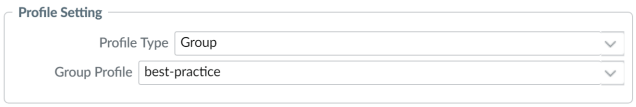
- Cree un grupo de perfiles de seguridad.
  1. Seleccione **Objects (Objetos)** > **Security Profile Groups (Grupos de perfiles de seguridad)** y haga clic en Add (Añadir) para añadir un grupo nuevo.
  2. Asígnele un **nombre** descriptivo al grupo de perfiles, p. ej., Amenazas.
  3. Si el cortafuegos está en modo de Sistema virtual múltiple, habilite el perfil para que sea **Shared** y puedan compartirlo todos los sistemas virtuales.
  4. Añada perfiles existentes al grupo. Para obtener información detallada sobre la creación de perfiles, consulte Perfiles de seguridad.



  5. Haga clic en **Aceptar** para guardar el grupo de perfiles.
  6. Añada el grupo de perfiles de seguridad a una política de seguridad.
  7. Seleccione **Add (Añada)** para añadir o modifique una regla de política de seguridad y seleccione la pestaña **Actions (Acciones)**.
  8. Seleccione **Group (Grupo)** para el **Profile Type (Tipo de perfil)**.

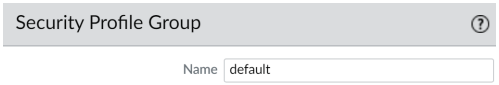
© 2020 Palo Alto Networks, Inc.

9. En el menú desplegable **Group Profile (Perfil de grupo)**, seleccione el grupo que ha creado (por ejemplo, seleccione el grupo Threats [Amenazas]):



10. Haga clic en **OK (Aceptar)** para guardar la política y en **Commit (Confirmar)** para confirmar sus cambios.

- Configurar un grupo de perfil de seguridad predeterminado
  1. Seleccione **Objects (Objetos)** > **Security Profile Groups (Grupos de perfiles de seguridad)** y añada un nuevo grupo de perfil de seguridad o modifique un grupo de perfiles de seguridad existente.
  2. Asigne al grupo de perfiles de seguridad el **Nombre** `predeterminado`:



  3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
  4. Confirme que el grupo de perfiles de seguridad predeterminado está incluido en las nuevas políticas de seguridad de manera predeterminada:
     1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)** para añadir una nueva política de seguridad.
     2. Seleccione la pestaña **Acciones** y mire los campos **Ajuste de perfil**:



        De manera predeterminada, la nueva política de seguridad muestra correctamente el **Profile Type (Tipo de perfil)** definido en Group (Grupo) y el **Group Profile (Perfil de grupo)** predeterminado está seleccionado.

- Cancele un grupo de perfiles de seguridad predeterminado.

  Si ya tiene un grupo de perfiles de seguridad predeterminado y no quiere que el conjunto de perfiles se añada a una nueva política de seguridad, puede continuar para modificar los campos de Ajuste de perfil según sus preferencias. Comience por seleccionar un tipo de perfil diferente para su política (**Policies [Políticas]** > **Security [Seguridad]** > **Security Policy Rule [Regla de la política de seguridad]** > **Actions [Acciones]**).

© 2020 Palo Alto Networks, Inc.

Seguimiento de las reglas de las bases de reglas

Para realizar el seguimiento de alguna regla de una base de reglas, consulte el *número de regla*, que varía según el orden que ocupe. El número de regla indica el orden en que la aplica el cortafuegos.

El *identificador único universal (universally unique identifier, UUID)* de las reglas no cambia nunca, aunque las modifique, por ejemplo, si cambia el nombre. El UUID permite realizar el seguimiento de las reglas por las bases de reglas aunque las elimine.

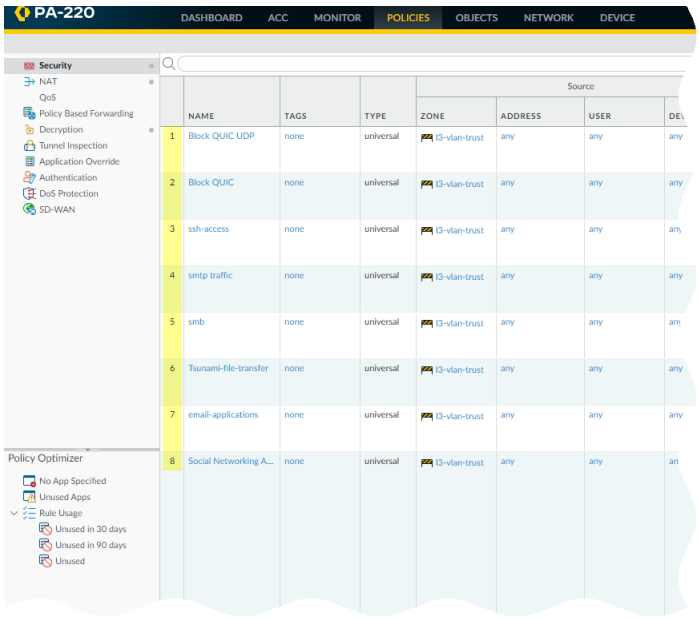
Números de regla

El cortafuegos numera las reglas de cada base de forma automática. Cuando mueve o reordena las reglas, los números cambian según el nuevo orden. Si filtra la lista para buscar reglas que se correspondan con determinados criterios, el cortafuegos muestra las coincidencias junto con su número en el contexto del conjunto completo de la base de reglas y su posición en el orden de evaluación.

Panorama numera las reglas previas, posteriores y predeterminadas de manera independiente. Cuando Panorama envía las reglas a un cortafuegos, la numeración de la regla refleja la jerarquía y el orden de evaluación de las reglas compartidas, las reglas previas de grupos de dispositivos, las reglas de cortafuegos, las reglas posteriores de grupo de dispositivos y las reglas por defecto. Es posible acceder a la **Preview Rules (Vista previa de reglas)** en Panorama, que ofrece una lista ordenada del número total de reglas de un cortafuegos.

- Consulte la lista numerada de reglas en el cortafuegos.

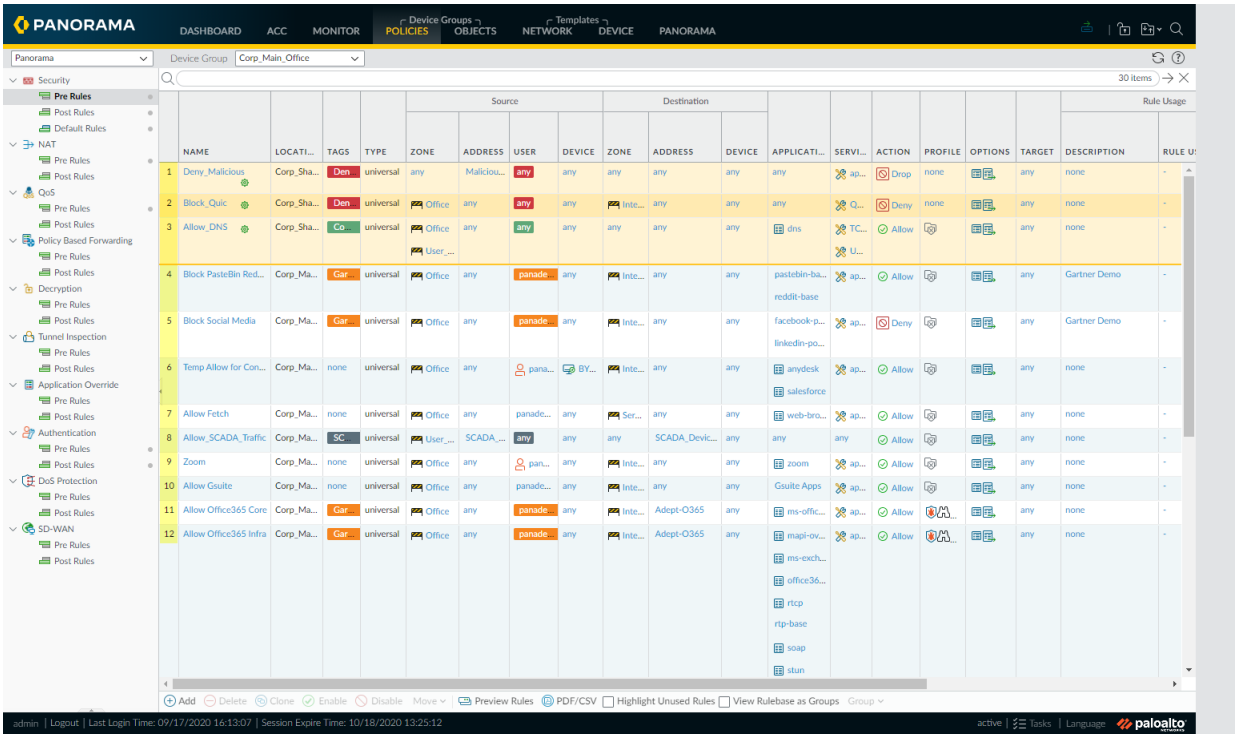
  Seleccione **Políticas** y cualquier base de reglas dentro de la misma. Por ejemplo, **Policies (Políticas)** > **Security (Seguridad)**. La columna más a la izquierda de la tabla muestra el número de regla.



- Consulte la lista numerada de reglas en Panorama.

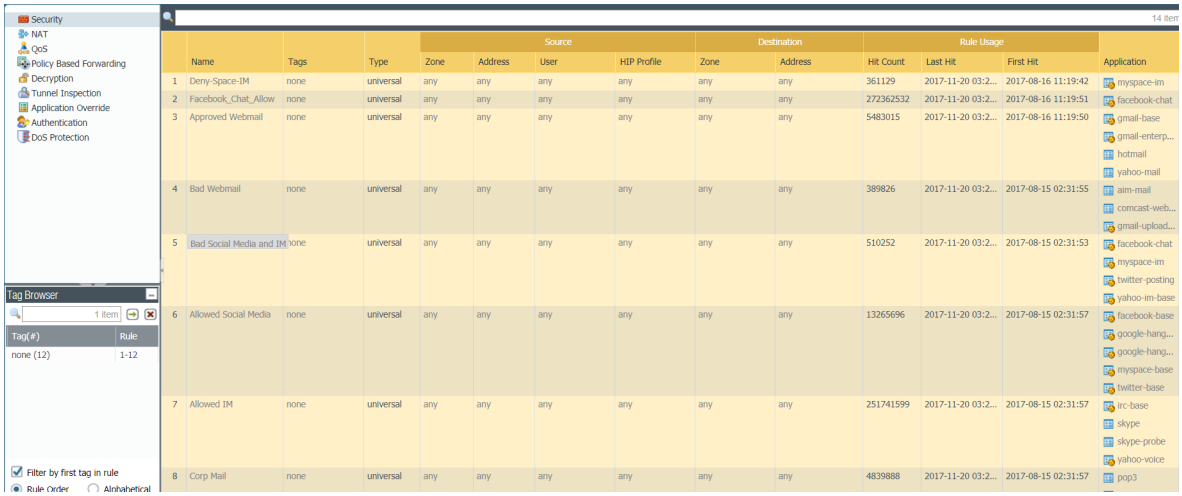
  Seleccione **Políticas** y cualquier base de reglas dentro de la misma. Por ejemplo, **Policies (Políticas)** > **Security (Seguridad)** > **Pre-rules (Reglas previas)**.

© 2020 Palo Alto Networks, Inc.



- Tras enviar las reglas desde Panorama, consulte la lista completa de reglas con números en el dispositivo gestionado.

  En la interfaz web del cortafuegos, seleccione **Policies (Políticas)** y elija cualquier base de reglas en ella. Por ejemplo, seleccione **Policies (Políticas)** > **Security (Seguridad)** y visualice el conjunto completo de las reglas numeradas que evaluará el cortafuegos.



UUID de las reglas

El UUID de las reglas es una cadena de 32 caracteres basada en datos como la dirección de red y la marca de tiempo de creación que el cortafuegos o Panorama les asignan. El UUID sigue el formato 8-4-4-4-12, donde 8, 4 y 12 representan el número de caracteres únicos separados por guiones. Los UUID identifican las reglas de las bases de reglas de todas las políticas. También sirven para identificar las reglas aplicables a

© 2020 Palo Alto Networks, Inc.

estos tipos de logs: Traffic (Tráfico), Threat (Amenazas), URL Filtering (Filtrado de URL), WildFire Submission (Envíos de WildFire), Data Filtering (Filtrado de datos), GTP, SCTP, Tunnel Inspection (Inspección de túneles), Configuration (Configuración) y Unified (Unificados).

Si realiza búsquedas por UUID, puede localizar reglas concretas entre miles con nombres idénticos o parecidos. Además, los UUID simplifican la automatización de las reglas y su integración en sistemas externos que no admiten nombres, por ejemplo, de tickets o de orquestación.

En algunos casos, tiene que generar UUID nuevos para bases de reglas existentes. Por ejemplo, si exporta una configuración a otro cortafuegos, debe *volver a generar los UUID* de las reglas cuando la importe para que no haya UUID duplicados. Cuando vuelve a generar los UUID, ya no puede hacer el seguimiento de esas reglas usando los UUID anteriores; además, se restablecen a cero los datos sobre resultados y sobre el uso de las aplicaciones.

El cortafuegos o Panorama asignan los UUID cuando realiza estas acciones:

- Crea reglas.
- Clona reglas existentes.
- Sustituye las reglas de seguridad predeterminadas.
- Carga configuraciones con nombre y vuelve a generar los UUID.
- Carga configuraciones con nombre que contienen reglas nuevas que no están en las configuraciones en ejecución.
- Actualiza el cortafuegos o Panorama a la versión PAN-OS 9.0.

Si carga una configuración que contiene reglas con UUID, el cortafuegos considera que son las mismas si coinciden en nombre, base de reglas y sistema virtual; Panorama considera que son las mismas si coinciden el nombre de las reglas, la base de reglas y el grupo de dispositivos.

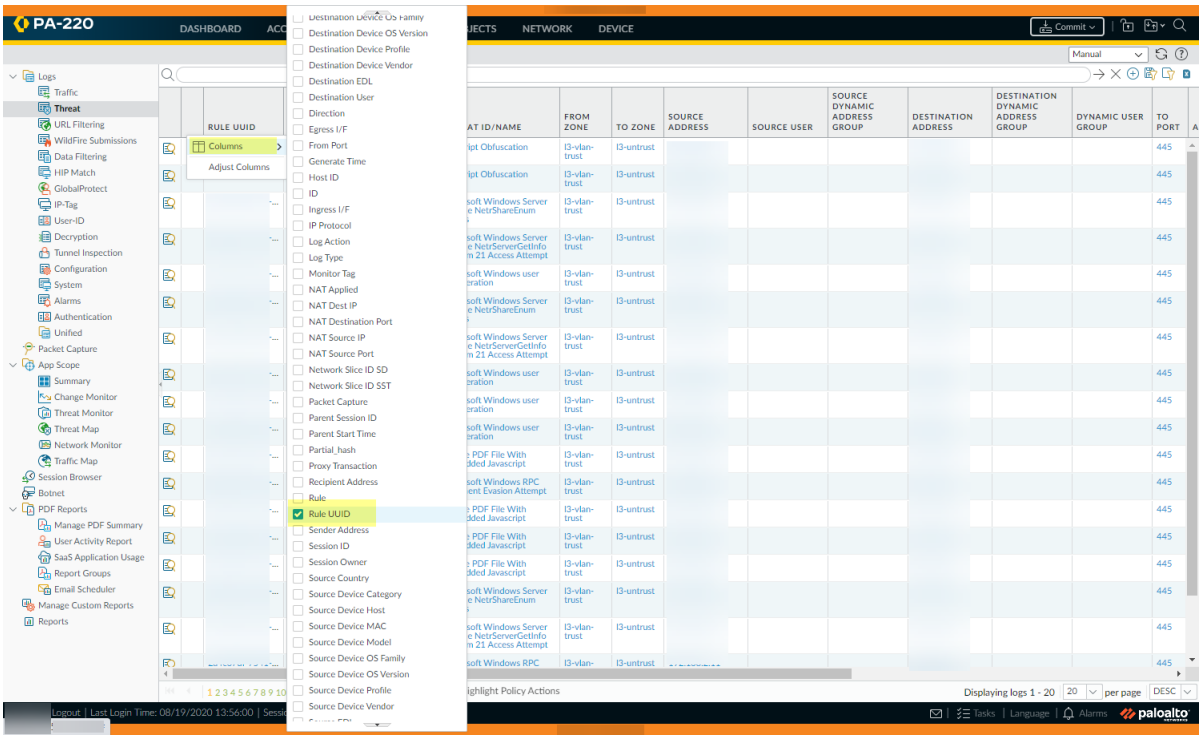
Tenga en cuenta los siguientes puntos en relación con los UUID:

- Si gestiona la política del cortafuegos en Panorama, los UUID se generan en Panorama y, por lo tanto, debe enviarlos desde Panorama. Si no envía la configuración desde Panorama antes de actualizar los cortafuegos a PAN-OS 9.0, no se puede realizar la actualización porque carece de los UUID.
- Además, después de actualizar a PAN-OS 9.0 un par de alta disponibilidad (high availability, HA), cada peer asigna los UUID a cada regla de la política de manera independiente. Por ello, los peers no aparecen sincronizados. Debe sincronizar la configuración con **Dashboard (Panel)** > **Widgets** > **System (Sistema)** > **High Availability (Alta disponibilidad)** > **Sync to peer (Sincronizar con peer)**.
- Si elimina una configuración de HA existente después de actualizar a PAN-OS 9.0, debe volver a generar los UUID en uno de los peers con **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** > **Load named configuration snapshot (Cargar instantánea de configuración con nombre)** > **Regenerate UUIDs for the selected named configuration (Volver a generar UUID de la configuración con nombre seleccionada)** y confirmar los cambios para que no se dupliquen.
- Todas las reglas que envía Panorama comparten el mismo UUID y todas las reglas locales del cortafuegos tienen UUID diferentes. Si crea una regla local en el cortafuegos después de enviar las de Panorama, posee un UUID propio.
- Si desea sustituir una instancia de Panorama con una autorización para la devolución de bienes (return merchandise authorization, RMA), no olvide marcar **Retain Rule UUIDs (Conservar UUID de reglas)** cuando cargue la instantánea de la configuración con nombre de Panorama. Si no lo hace, Panorama elimina todos los UUID anteriores de la instantánea de configuración y asigna UUID nuevos a las reglas en Panorama. Eso implica que no se conserva la información asociada a los antiguos UUID, por ejemplo, el recuento de resultados de las reglas de las políticas.
- Muestre la columna Rule UUID (UUID de regla) en los logs y la columna UUID en las reglas de las políticas.

© 2020 Palo Alto Networks, Inc.

Para ver los UUID, debe mostrar la columna, que está oculta de manera predeterminada.

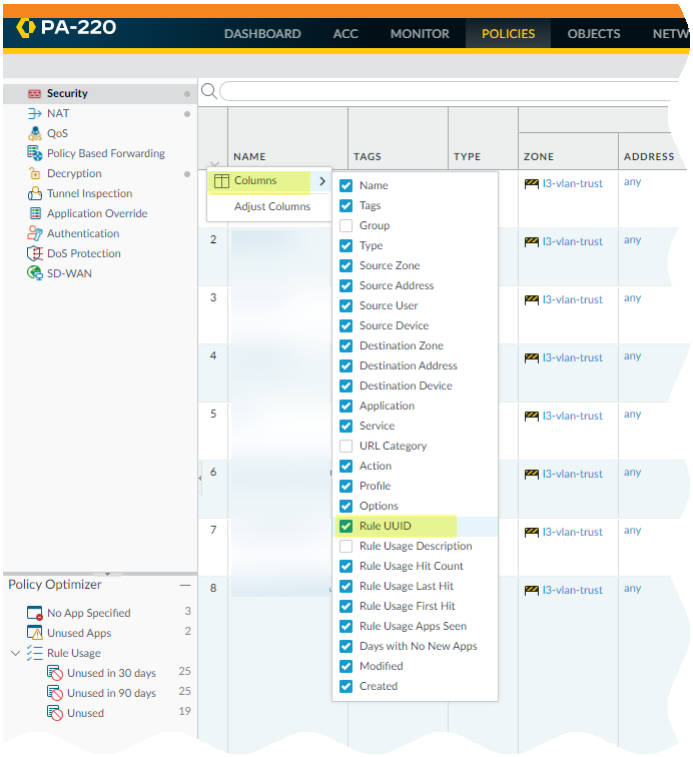
- Para mostrar los UUID en los logs:
  1. Seleccione **Monitor (Supervisión)** y expanda el encabezado de las columnas ( ).
  2. Seleccione **Columns (Columnas)**.
  3. Marque **Rule UUID (UUID de regla)**.



- Para mostrar los UUID en la base de reglas de políticas:
  1. Seleccione **Policies (Políticas)** y expanda el encabezado de las columnas ( ).
  2. Seleccione **Columns (Columnas)**.
  3. Marque **Rule UUID (UUID de regla)**.

     Están disponibles los UUID de las bases de reglas de todas las políticas.

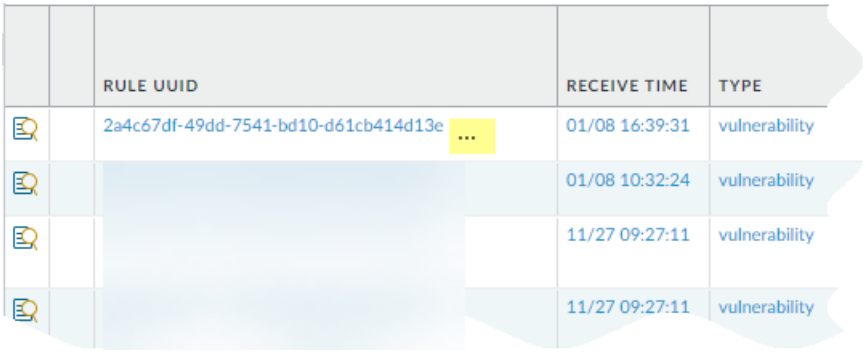
© 2020 Palo Alto Networks, Inc.



- Copie el UUID de un log o una regla de una política.

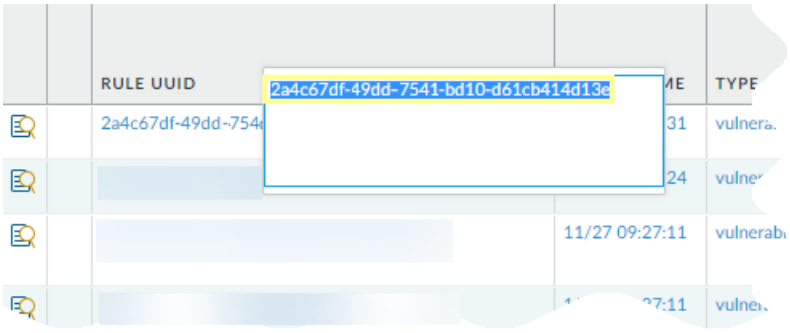
  Puede copiar el UUID para pegarlo en las búsquedas, el centro de control de aplicaciones (application command center, ACC), los informes personalizados, los filtros o cualquier otra ubicación a fin de localizar la regla correspondiente.

  1. Haga clic en los puntos suspensivos que aparecen al mover el cursor por encima de la entrada de la columna Rule UUID (UUID de regla).

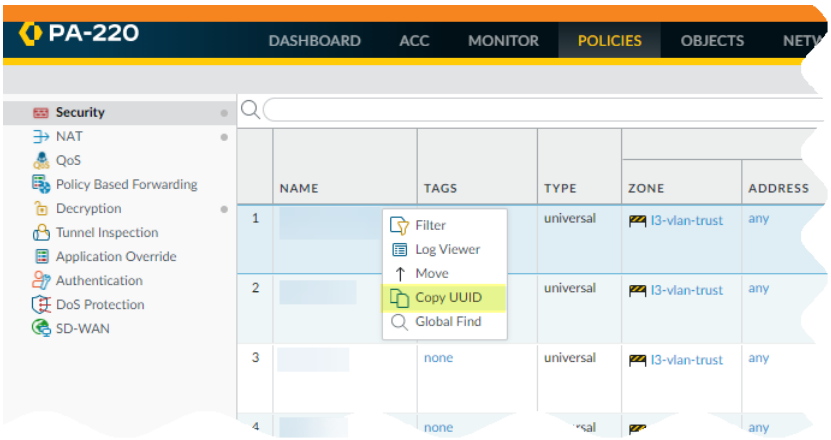


  2. Copie el UUID de la ventana emergente.

© 2020 Palo Alto Networks, Inc.



También puede ir a la pestaña **Policies (Políticas)**, hacer clic en la flecha que está a la derecha del nombre de la regla y hacer clic en **Copy UUID (Copiar UUID)**.



- Consulte los logs de configuración para ver los UUID de las reglas eliminadas.

  Para ver el UUID de una regla eliminada, seleccione **Monitor (Supervisar)** > **Logs [Logs]** > **Configuration (Configuración)**.

© 2020 Palo Alto Networks, Inc.

Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas

Cuando cree o modifique reglas de las políticas, puede exigir que se introduzcan una descripción, etiquetas u observaciones de auditoría para garantizar que la base se organiza y se agrupa correctamente, así como para conservar el importante historial de las reglas con fines de auditoría. Si estos datos son obligatorios, resulta más fácil consultar la base de reglas de las políticas, ya que las reglas están bien agrupadas, y se registran en el historial de cambios todas las ocasiones en que se crean o modifican reglas. Para uniformar las observaciones de auditoría, configure requisitos concretos sobre su contenido.

La introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría no está habilitada de forma predeterminada. Puede especificar que sea obligatorio cualquiera de estos datos o cualquier combinación de ellos para añadir o modificar reglas. En el archivo de observaciones de auditoría, puede leer los comentarios introducidos sobre la regla seleccionada, consultar el historial de logs de configuración y comparar las versiones de configuración de las reglas.

STEP 1 | Inicio de la interfaz web.

STEP 2 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite Policy Rulebase Settings (Configuración de base de reglas de políticas).

STEP 3 | Configure los ajustes que desea aplicar. En este ejemplo, es obligatorio introducir etiquetas y observaciones de auditoría en todas las políticas.



Las observaciones de auditoría permiten conocer el motivo por el que el administrador crea o modifica las reglas de las políticas. Si se exige su introducción, resulta más sencillo mantener un historial preciso de las reglas con fines de auditoría.

STEP 4 | En Audit Comment Regular Expression (Expresión regular de observaciones de auditoría), especifique el formato de estas notas.

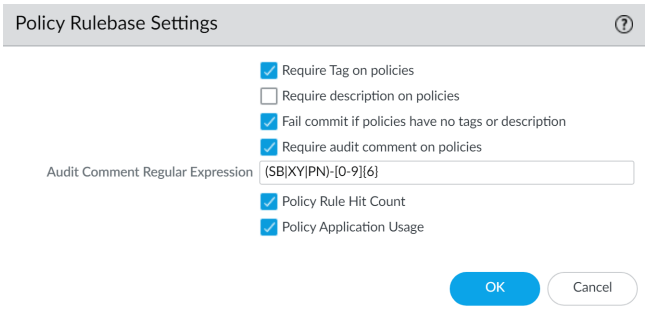
Puede exigir que, al crear o modificar reglas, los administradores escriban observaciones con un formato ajustado a sus requisitos empresariales y de auditoría. Para ello, especifique expresiones formadas por letras y números; por ejemplo, introduzca una expresión regular que coincida con el formato de sus números tickets:

- **`[0-9]{<número de cifras>}`**: exige que las observaciones de auditoría incluyan un número mínimo de cifras del 0 al 9. Por ejemplo, **`[0-9]{6}`** exige seis cifras como mínimo en una expresión con números del 0 al 9.
- **`<Expresión con letras>`**: exige que las observaciones de auditoría incluyan alguna expresión alfabética. Por ejemplo, **`Reason for Change- (Motivo del cambio:)`** exige que el administrador empiece las observaciones con estas palabras.
- **`<Expresión con letras>-[0-9]{<número de cifras>}`**: exige que las observaciones de auditoría incluyan un carácter predeterminado, seguido de un número mínimo de cifras del 0 al 9. Por ejemplo, **`SB-[0-9]{6}`** exige que las observaciones empiecen con **`SB-`**, seguido de una expresión con seis cifras como mínimo del 0 al 9. Por ejemplo, **`SB-012345`**.
- **`(<Expresión con letras>)|(<expresión con letras>)|(<expresión con letras>)|-[0-9]{<número de cifras>}`**: exige que las observaciones de auditoría incluyan un prefijo (consistente en algunas de las expresiones alfabéticas predeterminadas) con un número

© 2020 Palo Alto Networks, Inc.

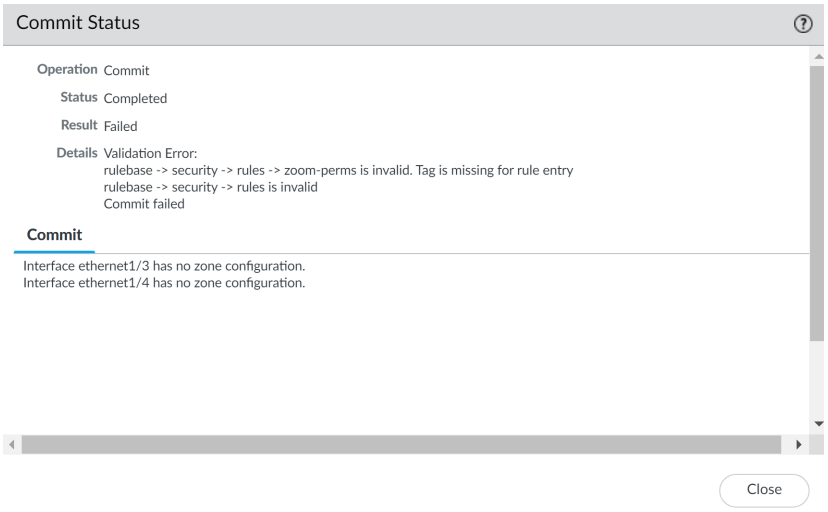
mínimo de cifras del 0 al 9. Por ejemplo, **`(SB|XY|PN)-[0-9]{6}`** exige que las observaciones empiecen con **`SB-`**, **`XY-`** o **`PN-`**, seguido de una expresión con seis cifras como mínimo del 0 al 9; ejemplo: **`SB-012345`**, **`XY-654321`** o **`PN-012543`**.

STEP 5 | Haga clic en **OK (Aceptar)** para aplicar la nueva configuración de la base de reglas de las políticas.



STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar los cambios.

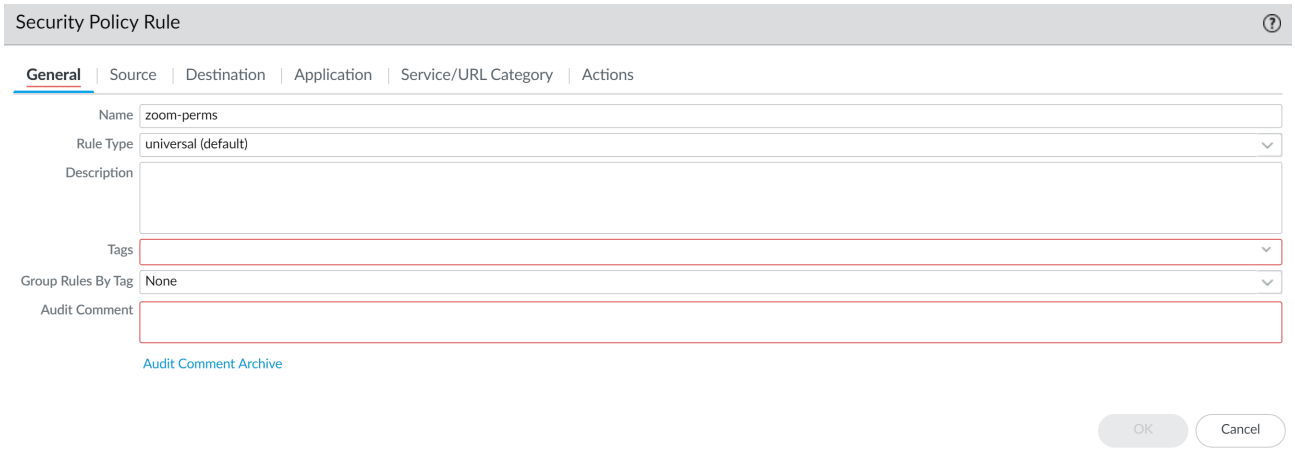
Después de confirmar los cambios en la configuración de la base de reglas de las políticas, modifique la regla existente según los ajustes que ha aplicado.



STEP 7 | Verifique que el cortafuegos aplica la nueva configuración de la base de reglas de las políticas.

1. Seleccione **Policies (Políticas)** y haga clic en **Add (Añadir)** para añadir una regla nueva.
2. Confirme que debe añadir una etiqueta e introducir observaciones de auditoría y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.



© 2020 Palo Alto Networks, Inc.

Duplicación o traslado de una regla de políticas u objeto a un sistema virtual diferente

En un cortafuegos que tiene más de un sistema virtual (vsys), puede trasladar los objetos y reglas de políticas a una ubicación compartida o vsys diferente o duplicarlos. La duplicación y traslado le ahorra los esfuerzos de eliminar, recrear o cambiar el nombre de reglas y objetos. Si el objeto o la regla de política que duplica o traslada desde un vsys tiene referencias a objetos de ese vsys, duplique o mueva también los objetos a los que se hace referencia. Si las referencias son hacia objetos compartidos, no tiene que incluirlos cuando los duplique o mueva. Puede implementar el Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama para acceder a las referencias.

Cuando clona varias reglas de la política, el orden en el que selecciona las reglas determinará el orden en el que se copian al grupo de dispositivos. Por ejemplo, si tiene las reglas de 1 a 4 y su orden de selección es 2-1-4-3, el grupo de dispositivos donde se clonarán estas reglas mostrará las reglas en el mismo orden en el que las seleccionó. Sin embargo, puede reorganizar las reglas como lo desee cuando se copien correctamente.

STEP 1 | Seleccione el tipo de política (por ejemplo, **Policy [Política]** > **Security [Seguridad]**) o el tipo de objeto (por ejemplo, **Objects [Objetos]** > **Addresses [Direcciones]**).

STEP 2 | Seleccione el **Virtual System (Sistema virtual)** y seleccione uno o más objetos o reglas de política.

STEP 3 | Seleccione uno de los siguientes pasos:

- Seleccione **Move (Mover)** > **Move to other vsys (Mover a otro vsys)** (para reglas de políticas).
- Haga clic en **Move (Mover)** (para objetos).
- Haga clic en **Clone** (para objetos o reglas de política).

STEP 4 | En el menú desplegable **Destination**, seleccione el nuevo sistema virtual o **Shared**.

STEP 5 | (Solo reglas de política) Seleccione el **Rule order (Orden de reglas)**:

- **Move top**: la regla precederá al resto de las reglas.
- **Move bottom**: la regla seguirá a todas las demás reglas.
- **Before rule**: en el menú desplegable adyacente, seleccione la regla que viene después de las reglas seleccionadas.
- **After rule**: en el menú desplegable adyacente, seleccione la regla que viene antes de las reglas seleccionadas.

STEP 6 | La casilla de verificación **Error out on first detected error in validation (Detener tras el primer error detectado en la validación)** está seleccionada por defecto. El cortafuegos deja de realizar las comprobaciones para la acción de traslado y duplicación cuando encuentra el primer error, y solo muestra este error. Por ejemplo, si se produce un error cuando el vsys de **Destination** no tiene un objeto al que haga referencia la regla de política que está moviendo, el cortafuegos mostrará el error y detendrá cualquier otra validación. Cuando mueva o duplique múltiples elementos a la vez, seleccione esta casilla de verificación para ver los errores uno a uno y solucionarlos. Si cancela la selección de la casilla de verificación, el cortafuegos recoge y muestra una lista de errores. Si hay errores en la validación, el objeto no se traslada o duplica hasta que solucione todos los errores.

© 2020 Palo Alto Networks, Inc.

STEP 7 | Haga clic en **OK** para iniciar la validación de errores. Si el cortafuegos muestra errores, soluciónelos y vuelva intentar la operación de traslado o duplicación. Si el cortafuegos no muestra errores, el objeto se traslada o duplica con éxito. Cuando finalice la operación, haga clic en **Commit**.

© 2020 Palo Alto Networks, Inc.

Uso de objetos de dirección para representar direcciones IP

Cree objetos de dirección en los cortafuegos para agrupar direcciones IP o para especificar un FQDN. Luego, haga referencia a ellos en las reglas de las políticas, los filtros u otras funciones de los cortafuegos para no tener que especificar uno por uno sus componentes.

Es más, como puede hacer referencia al mismo objeto en múltiples reglas, filtros o funciones diversas, se ahorra especificar las mismas direcciones en cada uso. Por ejemplo, puede crear un objeto de dirección que especifique un intervalo de direcciones IPv4 para hacer referencia a él en las reglas de la política de seguridad, las reglas de la política de traducción de direcciones de red (network address translation, NAT) y los filtros de los logs de los informes personalizados.

- Objetos de dirección
- Creación de objetos de dirección

Objetos de dirección

Los objetos de dirección son conjuntos de direcciones IP que se pueden gestionar a la vez y usar en múltiples reglas de políticas, filtros y otras funciones de los cortafuegos. Hay cuatro tipos de objetos de dirección: **IP Netmask (Máscara de red de IP)**, **IP Range (Intervalo de IP)**, **IP Wildcard Mask (Máscara comodín de IP)** y **FQDN**.

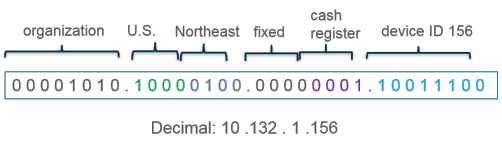
Los objetos de dirección de los tipos **IP Netmask (Máscara de red de IP)**, **IP Range (Intervalo de IP)** y **FQDN** pueden especificar direcciones IPv4 o IPv6, Un objeto de dirección de tipo **IP Wildcard Mask** solo puede especificar direcciones IPv4.

Si el tipo es **IP Netmask (Máscara de red IP)**, debe introducir la dirección IP o la red con barra diagonal para indicar la red IPv4 o la longitud del prefijo de IPv6, por ejemplo, 192.168.18.0/24 o 2001:db8:123:1::/64.

Si el tipo es **IP Range (Intervalo de IP)**, debe introducir el intervalo de direcciones IPv4 o IPv6 separadas con guiones.

El tipo **FQDN** (por ejemplo, paloaltonetworks.com) es el más fácil de usar porque DNS proporciona la resolución de los FQDN en las direcciones IP, es decir, no tiene que saber las direcciones IP ni actualizarlas manualmente cada vez que los FQDN se resuelven en otras distintas.

El tipo **IP Wildcard Mask (Máscara comodín de IP)** resulta útil si define direcciones IPv4 privadas en los dispositivos internos y la estructura de asignación de direcciones otorga significado a determinados bits de estas. Por ejemplo, la dirección IP de la caja registradora (cash register) 156 de la zona noreste de EE. UU. (Northeast, U.S.) puede ser 10.132.1.156 en función de estas asignaciones de bits:



Los objetos de dirección del tipo **IP Wildcard Mask (Máscara comodín de IP)** especifican qué direcciones de origen o destino están sujetas a reglas de la política de seguridad. Por ejemplo, 10.132.1.1/0.0.2.255. El bit cero (0) de la máscara indica que el bit que se compara debe coincidir con el bit de la dirección IP cubierta por el cero. El bit uno (1) de la máscara es el bit comodín que indica que el bit que se compara no tiene por qué coincidir con el bit de la dirección IP. Los siguientes fragmentos de una dirección IP y una máscara comodín ilustran cómo arrojan cuatro coincidencias:

© 2020 Palo Alto Networks, Inc.



Después de realizar el procedimiento Creación de objetos de dirección:

- Puede hacer referencia a objetos de dirección de los tipos **IP Netmask (Máscara de red de IP)**, **IP Range (Intervalo de IP)** o **FQDN** en las reglas de las políticas de seguridad, autenticación, traducción de direcciones de red (network address translation, NAT), NAT64, descifrado, protección contra denegación de servicio (denial of service, DoS), reenvío basado en políticas (policy-based forwarding, PBF), calidad de servicio (quality of service, QoS), sustitución de aplicaciones e inspección de túneles; también sirven para los grupos de direcciones de NAT, los túneles de red privada virtual (virtual private network, VPN), la supervisión de rutas, las listas dinámicas externas, la protección contra reconocimiento, el filtro global del centro de control de aplicaciones (application command center, ACC), el filtro de logs o el filtro de logs de informes personalizados.
- Puede hacer referencia a objetos de dirección del tipo **IP Wildcard Mask** solo en las reglas de la política de seguridad.

Creación de objetos de dirección

Cree Objetos de dirección para representar direcciones IP y, luego, hacer referencia a ellos en las reglas de políticas, los filtros u otras funciones de los cortafuegos. Si desea modificar un conjunto de direcciones, puede hacerlo en el objeto que las representa, en lugar de aplicar los cambios en cada filtro o regla de políticas, lo que reduce la carga de trabajo.

STEP 1 | Cree un objeto de dirección.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)** para añadir un objeto de dirección en **Name (Nombre)**. El nombre debe ser único, puede tener hasta 63 caracteres y solo puede incluir letras, números, espacios, guiones y guiones bajos. Además, se distingue entre mayúsculas y minúsculas.
2. En **Type (Tipo)**, seleccione el tipo de objeto de dirección:
   - **IP Netmask (Máscara de red de IP)**: especifique una sola dirección IPv4 o IPv6, una red IPv4 con barra diagonal o una dirección IPv6 con prefijo, Por ejemplo, 192.168.80.0/24 o 2001:db8:123:1::/64. Si lo desea, haga clic en **Resolve (Resolver)** para ver el nombre de dominio completo (fully qualified domain name, FDQN) asociado, según la configuración de DNS del cortafuegos o de Panorama. Para cambiar el tipo del objeto de dirección de **IP Netmask (Máscara de red de IP)** a **FQDN**, seleccione el FQDN y haga clic en **Use this FQDN (Usar este FQDN)**. El valor de **Type (Tipo)** cambia a **FQDN** y el FQDN seleccionado aparece en el campo de texto.
   - **IP Range (Intervalo de IP)**: especifique un intervalo de direcciones IPv4 o IPv6 separadas con guiones, por ejemplo, 192.168.40.1-192.168.40.255 o 2001:db8:123:1::1-2001:db8:123:1::22.
   - **IP Wildcard Mask (Máscara comodín de IP)**: especifique una dirección IP comodín, es decir, una dirección IPv4 seguida por una barra diagonal y una máscara, que debe empezar por cero (0). Por ejemplo, 10.5.1.1/0.127.248.2. El cero (`0`) de la máscara indica el bit que se compara y debe coincidir con el bit de la dirección IP cubierta por el cero. El uno (`1`) de la máscara es el bit comodín que indica que el bit que se compara no tiene por qué coincidir con el bit de la dirección IP cubierta por el uno.
   - **FQDN**: especifique el nombre de dominio. FQDN se resuelve inicialmente en el momento de la compilación. Después, el cortafuegos actualiza el FQDN basándose en su tiempo de vida (time-to-live, TTL) en DNS, siempre que dicho valor sea igual o superior al **`tiempo mínimo de actualización de los FQDN`** que configure (o al valor predeterminado de 30 segundos).

© 2020 Palo Alto Networks, Inc.

Resuelven el FQDN el servidor DNS del sistema o el objeto de proxy DNS oportuno, si ha configurado un proxy. Haga clic en **Resolve (Resolver)** para ver la dirección IP asociada, según la configuración de DNS del cortafuegos o de Panorama. Para cambiar el tipo del objeto de dirección de FQDN a IP Netmask (Máscara de red de IP), seleccione una máscara y haga clic en **Use this address (Usar esta dirección)**. El valor de **Type (Tipo)** cambia a **IP Netmask (Máscara de red de IP)** y la dirección IP seleccionada aparece en el campo de texto.

3. (Opcional) Introduzca una o más Uso de etiquetas para agrupar objetos y distinguirlos visualmente que aplicar al objeto de dirección.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | **Commit (Confirmar)** los cambios.

STEP 3 | Consulte los logs filtrados por objetos de dirección, grupos de direcciones o direcciones comodín.

1. Por ejemplo, seleccione **Monitor (Supervisión)** > **Logs** > **Traffic (Tráfico)** para ver los logs de tráfico.
2. Haga clic en + para añadir un filtro de logs.
3. Seleccione el atributo **Address (Dirección)** y el operador **in (de)** e introduzca el nombre del objeto de dirección cuyos logs desea consultar. También puede introducir el nombre de un grupo de direcciones o una dirección comodín, como 10.155.3.4/0.0.240.255.
4. Haga clic en **Apply (Aplicar)**.

STEP 4 | Consulte un informe personalizado basado en un objeto de dirección.

1. Seleccione **Monitor (Supervisión)** > **Manage Custom Reports (Gestionar informes personalizados)** y seleccione un informe que utilice una base de datos, por ejemplo, la de logs de tráfico.
2. Seleccione **Filter Builder (Generador de filtro)**.
3. Seleccione un atributo, como **Address (Dirección)**, **Destination Address (Dirección de destino)** o **Source Address (Dirección de origen)**, seleccione un operador e introduzca el nombre del objeto de dirección cuyo informe desea consultar.

STEP 5 | Use un filtro del centro de control de aplicaciones (application command center, ACC) para ver la actividad en la red de una dirección IP de origen o de destino que emplea un objeto de dirección.

1. Seleccione **ACC** > **Network Activity (Actividad de red)**.
2. Consulte **Source IP Activity—For Global Filters (Actividad de IP de origen: filtros globales)** y haga clic en + para añadir un filtro y seleccione una de las siguientes opciones: {0>Address (Dirección)<0}, **Source (Origen)** > **Source Address (Dirección de origen)** o **Destination (Destino)** > **Destination Address (Dirección de destino)**; luego, seleccione un objeto de dirección.
3. Consulte **Destination IP Activity—For Global Filters (Actividad de IP de destino: filtros globales)** y haga clic en + para añadir un filtro y seleccionar una de las siguientes opciones: {0>Address (Dirección)<0}, **Source (Origen)** > **Source Address (Dirección de origen)** o **Destination (Destino)** > **Destination Address (Dirección de destino)**; luego, seleccione un objeto de dirección.

© 2020 Palo Alto Networks, Inc.

Uso de etiquetas para agrupar objetos y distinguirlos visualmente

Puede etiquetar objetos para agrupar elementos relacionados y añadir un color a la etiqueta para distinguirlos y facilitar el análisis. Puede crear etiquetas para los siguientes objetos: objetos de dirección, grupos de direcciones, grupos de usuarios, zonas, grupos de servicios y reglas de políticas.

El cortafuegos y Panorama admiten etiquetas estáticas y etiquetas dinámicas. Las etiquetas dinámicas se registran desde diversas fuentes y no se muestran con las etiquetas estáticas, ya que las etiquetas dinámicas no forman parte de la configuración del cortafuegos o Panorama. Consulte Registro de direcciones IP y etiquetas dinámicamente para obtener información sobre cómo registrar etiquetas de forma dinámica. Las etiquetas descritas en esta sección se añaden estáticamente y forman parte de la configuración.

Usted puede aplicar una o más etiquetas a objetos y reglas de política, hasta un máximo de 64 etiquetas por objeto. Panorama admite un máximo de 10.000 etiquetas que se pueden distribuir a través de Panorama (grupos de dispositivos y compartidos) y los cortafuegos gestionados (incluidos los cortafuegos con sistemas virtuales múltiples).

- Creación y aplicación de etiquetas
- Modificación de etiquetas
- Consulta de las reglas por grupos de etiquetas

Creación y aplicación de etiquetas

Use etiquetas para identificar la finalidad de las reglas o los objetos de configuración y para organizar mejor la base de reglas. Para asegurarse de que las reglas de políticas están bien etiquetadas, consulte Introducción obligatoria de la descripción, las etiquetas y las observaciones de auditoría en las reglas de las políticas. Consulte también Consulta de las reglas por grupos de etiquetas para ver las reglas por grupos: primero, cree una etiqueta y, luego, configúrela como etiqueta de grupo.

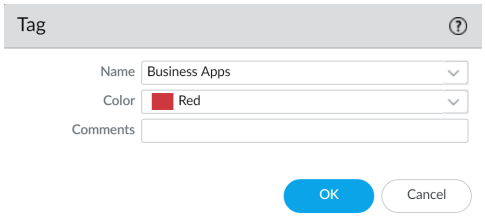
STEP 1 | Crear etiquetas



Para etiquetar una zona, debe crear una etiqueta con el mismo nombre que la zona. Cuando la zona está incluida en las reglas de política, el color de la etiqueta se muestra automáticamente como el color de fondo en contraste con el nombre de la zona.

1. Seleccione **Objects (Objetos)** > **Tags (Etiquetas)**.
2. En Panorama o un cortafuegos de sistema virtual múltiple, seleccione el **grupo de dispositivos** o el **sistema virtual** para el que la etiqueta estará disponible.
3. **Añada** una etiqueta e introduzca un **nombre** para identificar la etiqueta, o seleccione un **nombre** de zona para crear una etiqueta para una zona. La longitud máxima es de 127 caracteres.
4. (Opcional) Seleccione **Shared (Compartido)** para crear el objeto en una ubicación compartida para el acceso como un objeto compartido en Panorama para el uso en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple.
5. (Opcional) Asigne un **color** de los 17 colores predefinidos. Por defecto, **Color** está configurado en **None**.

© 2020 Palo Alto Networks, Inc.



6. Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para guardar los cambios.

STEP 2 | Aplique etiquetas a una política.

1. Seleccione **Políticas** y cualquier base de reglas dentro de la misma.
2. **Añada** una regla de políticas y use los objetos etiquetados que creó en el paso 1.
3. Verifique que las etiquetas estén en uso.

				Source				Destination	
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	General Business Apps	Business Apps	universal	any	any	known-user	any	any	any

STEP 3 | Aplique etiquetas a un objeto de dirección, grupo de direcciones, servicio o grupo de servicios.

1. Cree el objeto.

   Por ejemplo, para crear un grupo de servicios, seleccione **Objects (Objetos)** > **Service Groups (Grupos de servicio)** > **Add (Añadir)**.
2. Seleccione una etiqueta (**Tags (Etiquetas)**) o introduzca un nombre en el campo para crear una nueva etiqueta

   Para editar una etiqueta o añadirle color, consulte seleccione Modificación de etiquetas.

Modificación de etiquetas

- Seleccione **Objects (Objetos)** > **Tags (Etiquetas)** para realizar cualquiera de las siguientes operaciones con etiquetas:
  - Haga clic en el **nombre** para editar las propiedades de una etiqueta.
  - Seleccione una etiqueta de la tabla y **elimine** la etiqueta del cortafuegos.
  - **Clone** una etiqueta para duplicarla con las mismas propiedades. Se añade un sufijo numérico al nombre de etiqueta (por ejemplo, FTP-1).

  Para obtener información detallada sobre cómo se crean las etiquetas, consulte Creación y aplicación de etiquetas. Para obtener información sobre cómo trabajar con las etiquetas, consulte Consulta de las reglas por grupos de etiquetas.

Consulta de las reglas por grupos de etiquetas

Consulte la base de reglas de las políticas por grupos de etiquetas para que las reglas se agrupen visualmente según la estructura de etiquetado que haya creado. En esta vista, puede realizar distintos procedimientos de manera más sencilla, como añadir reglas al grupo de etiquetas seleccionado, eliminarlas de él y cambiarlas de orden. Aunque visualice la base de reglas por grupos de etiquetas, el orden de evaluación no varía. Además, la misma etiqueta puede aparecer varias veces para conservar visualmente la jerarquía de las reglas.

Debe crear una etiqueta para poder asignarla como etiqueta de grupo en una regla. A las reglas de las políticas que ya están etiquetadas al actualizar a PAN-OS 9.0 se les asigna como etiqueta de grupo la

© 2020 Palo Alto Networks, Inc.

primera etiqueta de forma automática. Antes de actualizar a PAN-OS 9.0, revise las reglas etiquetadas de la base para comprobar que están bien agrupadas. Si no es así, debe editar manualmente cada una de ellas y configurar la etiqueta de grupo correcta después de actualizar a PAN-OS 9.0.

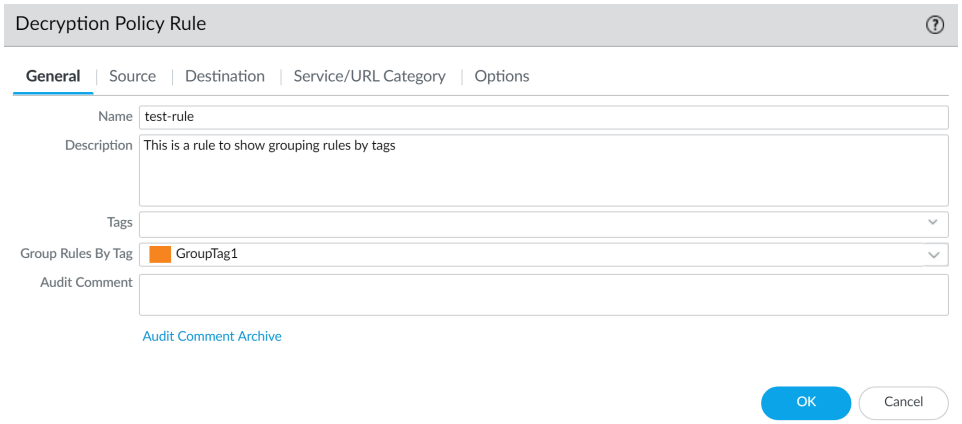


STEP 1 | Inicio de la interfaz web.

STEP 2 | Creación y aplicación de etiquetas que desee usar para agrupar las reglas.

STEP 3 | Asigne una regla de una política a un grupo de etiquetas.

1. Cree una regla de una política. Consulte Política para obtener más información sobre la creación de las reglas de las políticas.
2. En el menú desplegable del campo **Group Rules By Tag (Agrupar reglas por etiqueta)**, seleccione la etiqueta y haga clic en **OK (Aceptar)**.



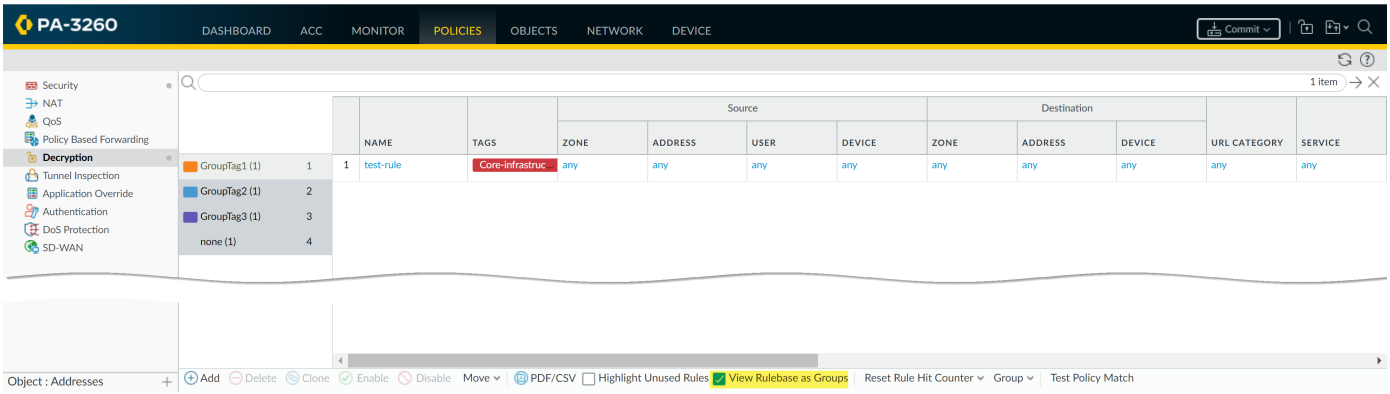
3. **Commit (Confirmar)** los cambios.

STEP 4 | Consulte la base de reglas de las políticas por grupos.

1. (Solo en Panorama) En **Device Group (Grupo de dispositivos)**, seleccione la base de reglas del grupo de dispositivos que desea consultar o bien todas las reglas compartidas.
2. Haga clic en **Policies (Políticas)** y seleccione la base donde ha creado las reglas en el paso 2.
3. Seleccione la opción **View Rulebase as Groups (Ver base de reglas por grupos)** (en la parte inferior).

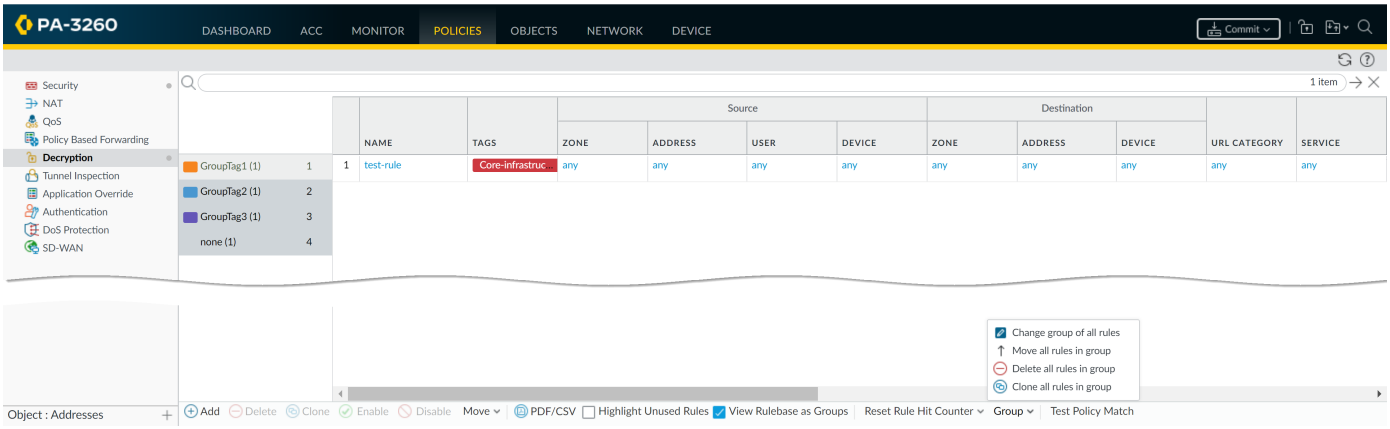
En las reglas que no tienen asignado ningún grupo de etiquetas, se muestra None (Ninguno).

© 2020 Palo Alto Networks, Inc.



STEP 5 | Realice con los grupos las operaciones oportunas.

1. Haga clic en **Group (Grupo)** para ejecutar operaciones con las reglas del grupo de etiquetas seleccionado.
   - (Solo en Panorama) **Move rules in group to different rulebase or device group (Mover reglas del grupo a otra base de reglas u otro grupo de dispositivos)**: mueva todas las reglas de políticas del grupo de etiquetas seleccionado a las bases de reglas previas o posteriores o bien trasladándolas a un grupo de dispositivos diferente.
   - **Change group of all rules (Cambiar grupo de todas las reglas)**: mueva todas las reglas del grupo de etiquetas seleccionado a otro grupo de etiquetas.
   - **Move all rules in group (Mover todas las reglas del grupo)**: mueva todas las reglas del grupo de etiquetas seleccionado para cambiar su orden de prioridad.
   - **Delete all rules in group (Eliminar todas las reglas del grupo)**: elimine todas las reglas del grupo de etiquetas seleccionado.
   - **Clone all rules in group (Clonar todas las reglas del grupo)**: clone todas las reglas del grupo de etiquetas seleccionado.



2. **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

Uso de una lista dinámica externa en políticas

Una lista dinámica externa (anteriormente denominada lista de bloqueo dinámico) es un archivo de texto que usted u otra fuente aloja en un servidor web externo de manera que el cortafuegos pueda importar objetos (direcciones IP, URL, dominios) para aplicar la política en las entradas de la lista. A medida que actualiza la lista, el cortafuegos importa dinámicamente la lista con el intervalo configurado y aplica la política sin necesidad de realizar un cambio o confirmación de la configuración en el cortafuegos.

- Lista dinámica externa
- Directrices de formato para listas dinámicas externas
- Listas dinámicas externas integradas
- Configuración del cortafuegos para acceder a una lista dinámica externa
- Recuperación de una lista dinámica externa del servidor web
- Visualización de entradas de lista dinámica externa
- Exclusión de entradas de una lista dinámica externa
- Aplicación de la política en una lista dinámica externa
- Búsqueda de listas dinámicas externas con autenticación fallida
- Deshabilitación de autenticación para una lista dinámica externa

Lista dinámica externa

Una lista dinámica externa es un archivo de texto que está alojado en un servidor web externo de manera que el cortafuegos pueda importar objetos (direcciones IP, URL, dominios, International Mobile Equipment Identities (IMEI, identidad internacional de equipo móvil), International Mobile Subscriber Identities (IMSI, identidad internacional de suscriptor móvil)) incluidos en la lista y aplicar la política. Para aplicar la política de seguridad en las entradas incluidas en la lista dinámica externa, debe hacer referencia a la lista en una regla o perfil de política compatible. Si hace referencia a varias listas, puede priorizar el orden de evaluación para garantizar que se confirmen las EDL más importantes antes de que se alcancen los límites de capacidad. A medida que modifica la lista, el cortafuegos importa dinámicamente la lista con el intervalo configurado y aplica la política sin necesidad de realizar un cambio o confirmación de la configuración en el cortafuegos. Si no se puede establecer la conexión con el servidor web, el cortafuegos usará la última lista recuperada correctamente para la aplicación de la política hasta que se recupere la conexión con el servidor web. En los casos en que la autenticación de la EDL falle, la política de seguridad dejará de hacer que la EDL se cumpla. Para recuperar la lista dinámica externa, el cortafuegos utiliza la interfaz configurada con la ruta de servicio **Palo Alto Networks Services (Servicios de Palo Alto Networks)**.

El cortafuegos admite estos tipos de listas dinámicas externas:

- **Predefined IP Address (Dirección IP predefinida)**: este tipo hace referencia a las listas de IP integradas y dinámicas que tienen un contenido fijo o predefinido. Estas listas dinámicas externas incorporadas, que están concebidas para proveedores de alojamiento blindado y direcciones IP malintencionadas y de alto riesgo, se añaden automáticamente al cortafuegos si dispone de una licencia activa de Threat Prevention. Estas listas también pueden hacer referencia a las EDL que emplean las listas integradas como origen. Como no puede modificar el contenido de las listas predefinidas, úselas como origen de otras EDL si desea añadir o excluir entradas de lista.
- **Predefined URL List (Lista de URL predefinidas)**: este tipo de lista dinámica externa contiene URL completadas previamente que las aplicaciones utilizan para servicios en segundo plano, como actualizaciones o comprobaciones de lista de revocación de certificados (CRL, Certificate Revocation List), que el cortafuegos puede excluir de forma segura de la política de autenticación. Palo Alto Networks revisa y mantiene este tipo de lista dinámica externa, que también se conoce como "lista de exclusión del portal de autenticación", a través de actualizaciones de contenido.
- **IP Address (Dirección IP):** el cortafuegos en general aplica la política para una dirección de origen o destino que esté definida como objeto estático en el cortafuegos (consulte Aplicación de política en una

© 2020 Palo Alto Networks, Inc.

lista dinámica externa). Si necesita agilidad en la aplicación de la política para una lista de direcciones IP de origen y destino que emergen ad hoc, puede usar una lista dinámica externa de direcciones IP como objeto de dirección de origen o destino en reglas de política, y configurar el cortafuegos para que deniegue o permita el acceso a las direcciones IP (dirección IPv4 e IPv6, intervalo IP y subredes IP) incluidas en la lista. También puede usar una EDL de dirección IP en el origen o destino de una regla de políticas de SD-WAN. El cortafuegos considera la lista dinámica externa de tipo de dirección IP como un objeto de dirección; todas las direcciones IP incluidas en una lista se manejan como un objeto de dirección.

- **Domain (Dominio)**: este tipo de lista dinámica externa le permite importar nombres de dominio personalizados en el cortafuegos para aplicar la política usando un perfil antispyware o regla de políticas de SD-WAN. Una EDL en un perfil antispyware resulta muy útil si se suscribe a inteligencia de amenazas de terceros y desea proteger su red contra nuevas fuentes de amenazas o malware, tan pronto como toma conocimiento de un dominio malintencionado. Para cada dominio que incluye en la lista dinámica externa, el cortafuegos crea una firma de spyware basado en DNS de manera que usted puede habilitar el sinkholing de DNS. La firma de spyware basada en DNS es de tipo spyware con gravedad intermedia y cada firma se denomina **`Custom Malicious DNS Query <domain name>`**. También puede especificar que el cortafuegos incluya los subdominios del dominio indicado. Por ejemplo, si la lista de dominios incluye paloaltonetworks.com, también se incluyen como parte de la lista todos los componentes inferiores de este dominio, como *.paloaltonetworks.com. Si habilita este ajuste, hace falta una entrada adicional para cada uno de los dominios de cada lista, lo cual se traduce en que se duplica el número de entradas. Para obtener información sobre cómo configurar las listas de dominios, consulte Configuración del sinkholing de DNS para una lista de dominios personalizados.
- **URL**: este tipo de lista dinámica externa le proporciona la agilidad para proteger su red contra nuevos orígenes de amenazas o malware. El cortafuegos maneja una lista dinámica externa con URL como una categoría de URL personalizada y usted puede usar la lista de dos maneras:
  - Como criterio de coincidencia en reglas de la política de seguridad, reglas de política de descifrado y reglas de política QoS para permitir, denegar, descifrar, no descifrar o asignar ancho de banda para las URL en la categoría personalizada.
  - En un perfil de filtrado de URL en el que puede definir acciones más pormenorizadas, tales como continuar, alertar o cancelar, antes de adjuntar el perfil a una regla de política de seguridad (consulte Uso de una lista dinámica externa en un perfil de filtrado URL).
- **Equipment Identity (Identidad de equipo)**: puede hacer referencia a una lista dinámica externa de dispositivos IoT definidos por identidades internacionales de equipo móvil (IMEI, International Mobile Equipment Identities) en una regla de políticas de seguridad que controla el tráfico de los equipos conectados a una red 5G o 4G. Consulte Introducción a la infraestructura de red móvil para obtener información sobre cómo configurar la seguridad de ID de equipo en modelos de cortafuegos compatibles.
- **Subscriber Identity (Identidad de suscriptor)**: puede hacer referencia a una lista dinámica externa de identidades internacionales de suscriptor móvil (IMSI, International Mobile Subscriber Identities) en una regla de políticas de seguridad que controla el tráfico de los suscriptores conectados a una red 5G o 4G. Consulte Introducción a la infraestructura de red móvil para obtener información sobre cómo configurar la seguridad de ID de suscriptor en modelos de cortafuegos compatibles.

Según el modelo del cortafuegos, puede añadir hasta 30 EDL personalizadas con orígenes únicos para aplicar las políticas. La lista dinámica externa no se aplica a Panorama. Al usar Panorama para gestionar un cortafuegos que está habilitado para múltiples sistemas virtuales, si supera el límite del cortafuegos, Panorama muestra un error de confirmación. Un origen es una URL que incluye la dirección IP o nombre de host, la ruta y el nombre del archivo para la lista dinámica externa. El cortafuegos busca la coincidencia con la URL (cadena completa) para determinar si un origen es único.

Si bien el cortafuegos no impone un límite en el número de listas para un tipo específico, se aplican los siguientes límites:

- IP Address (Dirección IP): los cortafuegos PA-5200 Series y PA-7000 Series admiten un máximo de 150 000 direcciones IP en total; todos los demás modelos admiten un máximo de 50 000 direcciones IP

© 2020 Palo Alto Networks, Inc.

en total. No se aplican límites para el número de direcciones IP por lista. Cuando se alcanza el límite máximo de direcciones IP admitidas en el cortafuegos, el cortafuegos genera un mensaje de syslog. Las direcciones IP en las listas de direcciones IP predefinidas no cuentan para este límite.

- URL y Domain (Dominio): el número máximo de URL y dominios admitido varía según el modelo. No se aplica ningún límite en cuanto al número de entradas de URL o de dominios por lista. Consulte la siguiente tabla para conocer la información específica de su modelo:

Modelo	Límite de entradas en las listas de URL	Límite de entradas en las listas de dominios
PA-5200 Series o PA-7000 Series (actualizados con las tarjetas de procesamiento de red [network processing card, NPC] PA-7000 20GXM, PA-7000 20GQXM o PA-7000 100G)  *Los dispositivos PA-7000 con distintas NPC solo admiten la capacidad estándar.*	250 000	4 000 000
VM-500, VM-700	100 000	2 000 000
PA-850, PA-820 o PA-3200 Series	100 000	1 000 000
PA-7000 Series (y dispositivos actualizados con las NPC PA-7000 20GQ o PA-7000 20G) o VM-300	100 000	500 000
PA-220, VM-50, VM-50 (Lite), VM-100, VM-1000-HV	50 000	50 000

Las entradas de lista solo cuentan para los límites del cortafuegos si pertenecen a una lista dinámica externa mencionada en la política.



- *Al analizar la lista, el cortafuegos omite las entradas que no coinciden con el tipo de lista e ignora las entradas que superan la cantidad máxima admitida para el modelo. Para garantizar que las entradas no superen el límite, verifique la cantidad de entradas que se utilizan actualmente en la política. Seleccione Objects (Objetos) > External Dynamic Lists (Listas dinámicas externas) y haga clic en List Capacities (Capacidades de la lista).*
- *Una lista dinámica externa debe contener entradas. Si desea dejar de utilizar la lista, elimine la referencia de la regla de la regla de políticas o el perfil en lugar de dejar la*

© 2020 Palo Alto Networks, Inc.

lista vacía. Si la lista no contiene entradas, el cortafuegos no logra actualizarla y sigue utilizando la última información recuperada.

- *Palo Alto Networks recomienda usar EDL compartidas cuando se emplean varios sistemas virtuales. Si recurre a EDL individuales con entradas duplicadas para cada sistema virtual, se consume más memoria y, por ende, se utilizan en exceso los recursos del cortafuegos.*
- *En el número de entradas de las EDL de los cortafuegos que ejecutan varios sistemas virtuales influyen otros factores (como los grupos de direcciones dinámicas [dynamic address groups, DAG], el número de sistemas virtuales o las bases de reglas), que se deben tener en cuenta para generar un listado más preciso sobre el uso de la capacidad. Eso puede provocar discrepancias en el uso de la capacidad tras actualizar las versiones PAN-OS 8.x.*
- *Según las funciones habilitadas en el cortafuegos y debido a las actualizaciones en la asignación de memoria, es posible que se supere el límite de uso de la memoria antes que el de capacidad de las EDL. Palo Alto Networks recomienda revisar las capacidades de las EDL y, si es preciso, eliminar algunas o consolidar otras en listas compartidas a fin de reducir el uso de la memoria al mínimo.*

Directrices de formato para listas dinámicas externas

Una lista dinámica externa de un tipo (dirección IP, URL o dominio) debe incluir entradas de ese tipo únicamente. Las entradas en una lista de direcciones IP predefinida cumplen con las directrices de formato para listas de direcciones IP.

- Lista de direcciones IP
- Lista de dominios
- Lista de URL

Lista de direcciones IP

La lista dinámica externa puede incluir direcciones IP individuales, direcciones de subred (dirección/máscara) o un intervalo de direcciones IP. Además, la lista de bloque puede incluir comentarios y caracteres especiales tales como **`*`** , **`:`** , **`;`** , **`#`**, or **`/`**. La sintaxis para cada línea de la lista es **`[dirección IP, IP/máscara o intervalo inicial IP-intervalo final IP] [espacio] [comentario]`**

Introduzca cada dirección/intervalo/subred IP en una nueva línea; la lista no admite URL ni dominios. Una subred o un intervalo de direcciones IP, como 92.168.20.0/24 o 192.168.20.40-192.168.20.50, cuentan como una entrada de dirección IP y no como varias direcciones. Si añade comentarios, deben incluirse en la misma línea que la dirección/intervalo/subred IP. El espacio al final de la dirección IP es el delimitador que separa un comentario de la dirección IP.

Ejemplo de lista de direcciones IP:

```
192.168.20.10/32
 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet
 2001:db8:123:1::/64 test internal IPv6 range
 192.168.20.40-192.168.20.50
```

Para una dirección IP bloqueada, puede mostrar una página de notificación solo si el protocolo es HTTP.

© 2020 Palo Alto Networks, Inc.

Lista de dominios

Utilice marcadores de posición en las listas de dominios para configurar una sola entrada que coincida con múltiples subdominios de sitios web, páginas, dominios de nivel superior enteros o páginas web concretas.

Siga estas directrices cuando cree las entradas de las listas de dominios:

- Introduzca cada nombre de dominio en una nueva línea; la lista no admite URL ni direcciones IP.
- No añada el prefijo del protocolo al nombre de dominio, http:// or https://.
- Use un asterisco (*) para indicar un valor de comodín.
- Use un símbolo de intercalación (^) para indicar un valor de coincidencia exacta.
- Los siguientes caracteres se consideran separadores de token: . / ? & = ; +

  Cada cadena separada con uno o dos de estos caracteres es un token. Utilice caracteres comodines como marcadores de posición de token, que indican que un token específico puede contener cualquier valor.
- Los caracteres de comodín deben ser el único carácter en un token; sin embargo, una entrada puede contener varios comodines.
- Las entradas de dominio pueden tener hasta 255 caracteres de longitud.

Cuándo utilizar comodines de asterisco (*):

Utilice un comodín de asterisco (*) para indicar uno o varios subdominios variables. Por ejemplo, para especificar la aplicación en el sitio web de Palo Alto Network independientemente de la extensión de dominio utilizada, que puede incluir uno o dos subdominios según la ubicación, puede añadir la entrada: **`*.paloaltonetworks.com`**. Esta entrada coincide tanto con docs.paloaltonetworks.com como con support.paloaltonetworks.com.

Este comodín también sirve para indicar dominios de nivel superior enteros. Por ejemplo, para especificar la aplicación de un dominio de nivel superior llamado .work, debe añadir la entrada: **`*.work`**. Así se buscan coincidencias con todos los sitios web que terminan por .work.

El comodín del asterisco (*) solo puede ir antepuesto en las entradas de dominios.

Ejemplos con asteriscos (*)

Entrada de la EDL de dominios	Sitios que coinciden
`*.company.com`	eng.tools.company.com support.tools.company.com tools.company.com docs.company.com
`*.clic`	Todos los sitios web que terminan por un dominio de nivel superior de .clic

Cuándo utilizar el símbolo de intercalación (^):

Use el símbolo de intercalación (^) para indicar una coincidencia exacta con un subdominio. Por ejemplo, **`^paloaltonetworks.com`** solo busca coincidencias con paloaltonetworks.com. Esta entrada no se corresponde con ningún otro sitio.

Ejemplos con signos de intercalación (^)

© 2020 Palo Alto Networks, Inc.

Entrada de la EDL de dominios	Sitios que coinciden
`^empresa.es`	empresa.es
`^es.empresa.es`	es.empresa.es

Lista de URL

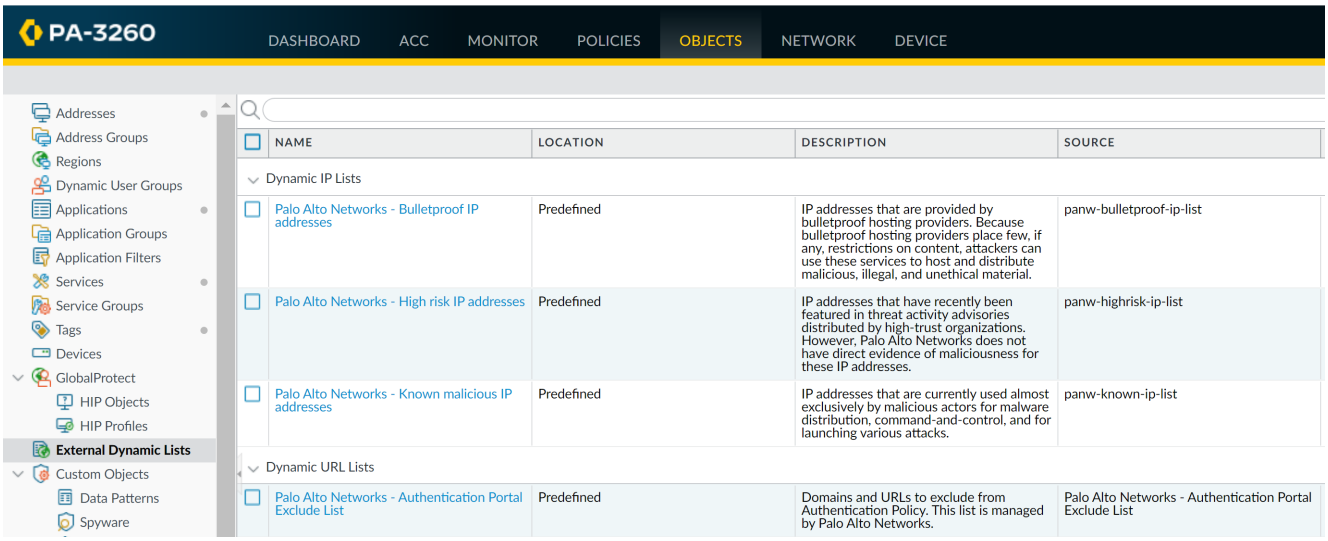
Consulte Excepciones de la categoría de URL.

Listas dinámicas externas integradas

Con la licencia activa de Threat Prevention, Palo Alto Networks proporciona listas dinámicas externas (external dynamic list, EDL) integradas de direcciones IP que sirven como protección contra los hosts malintencionados.

- **Palo Alto Networks Bulletproof IP Addresses (Direcciones IP blindadas de Palo Alto Networks)**: incluye direcciones IP suministradas por proveedores de alojamiento blindado. Como esos proveedores apenas imponen restricciones al contenido o no imponen ninguna, los atacantes suelen recurrir a estos servicios para alojar y distribuir material malintencionado, ilegal e indebido.
- **Direcciones IP de alto riesgo de Palo Alto Networks**: contiene direcciones IP malintencionadas de asesores de amenazas emitidos por organizaciones externas de confianza. Palo Alto Networks compila la lista de asesores de amenazas, pero no cuenta con evidencia directa de que las direcciones IP sean malintencionadas.
- **Direcciones IP malintencionadas conocidas de Palo Alto Networks**: contiene direcciones IP que se comprueban como malintencionadas en función de un análisis de WildFire, una investigación de Unit 42 (Unidad 42) y los datos que se recopilan mediante la telemetría (Uso compartido de la inteligencia de amenazas con Palo Alto Networks). Los atacantes utilizan estas direcciones IP de manera casi exclusiva para distribuir malware, iniciar actividades de comando y control, e iniciar ataques.

Como el cortafuegos recibe actualizaciones para estas fuentes en las actualizaciones de contenido, aplica automáticamente la política basándose en la última inteligencia contra amenazas de Palo Alto Networks. No puede modificar el contenido de las listas integradas. Úselas tal cual (consulte Aplicación de la política en una lista dinámica externa) o bien cree EDL personalizadas que las empleen como origen (consulte Configuración del cortafuegos para acceder a una lista dinámica externa) y excluya las entradas que no procedan.



© 2020 Palo Alto Networks, Inc.

Configuración del cortafuegos para acceder a una lista dinámica externa

Debe establecer la conexión entre el cortafuegos y el origen que aloja la lista dinámica externa para poder aplicar la política a una lista dinámica externa.

STEP 1 | (Opcional) Personalice la ruta de servicio que el cortafuegos utiliza para recuperar listas dinámicas externas.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Service Route Configuration (Configuración de ruta de servicio)** > **Customize (Personalizar)** y modifique la ruta de servicio de **listas dinámicas externas**.

El cortafuegos no emplea la ruta de servicio External Dynamic Lists (EDL, Listas dinámicas externas) para recuperar las Listas dinámicas externas integradas; su contenido se modifica o actualiza por medio de las actualizaciones de contenido, que exigen una licencia activa de Threat Prevention.

STEP 2 | Busque una lista dinámica externa para usar con el cortafuegos.

- Cree una lista dinámica externa y alójela en un servidor web. Ingrese las direcciones IP, dominios o URL en un archivo de texto en blanco. Cada entrada de la lista debe estar en una línea separada. Por ejemplo:

  ```
  financialtimes.co.in

  www.wallaby.au/joey

  www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx
  ```

  Consulte las Directrices de formato para una lista dinámica externa, a fin de asegurarse de que el cortafuegos no omita entradas de la lista. Para evitar errores de confirmación y entradas no válidas, no incluya el prefijo http:// o https:// en ninguna de las entradas.
- Utilice una lista dinámica externa alojada por otro origen y verifique que siga las Directrices de formato para una lista dinámica externa.

STEP 3 | Seleccione **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**.

STEP 4 | Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** descriptivo para la lista.

STEP 5 | (Opcional) Seleccione **Shared (Compartida)** para compartir la lista con todos los sistemas virtuales en un dispositivo que esté habilitado para varios sistemas virtuales. De manera predeterminada, el objeto se crea en el sistema virtual que esté seleccionado actualmente en el menú desplegable **Sistemas virtuales**.

Palo Alto Networks recomienda usar EDL compartidas cuando se emplean varios sistemas virtuales. Si recurre a EDL individuales con entradas duplicadas para cada sistema virtual, se consume más memoria y, por ende, se utilizan en exceso los recursos del cortafuegos.

STEP 6 | (Panorama únicamente) Seleccione **Disable override** para garantizar que un administrador de cortafuegos no pueda invalidar los ajustes en un cortafuegos que hereda esta configuración a través de una confirmación de grupo de dispositivos de Panorama.

STEP 7 | Seleccione el **Type (Tipo)** para la lista (por ejemplo, **URL List [Lista de URL]**).

© 2020 Palo Alto Networks, Inc.

Asegúrese de que la lista solo incluya entradas para el tipo de lista. Consulte Verificar si las entradas en la lista dinámica externa se ignoraron u omitieron.

Si utiliza listas de dominios, tiene la opción de habilitar **Automatically expand to include subdomains (Incluir subdominios automáticamente)** para que también se incluyan los subdominios del dominio especificado. Por ejemplo, si la lista de dominios incluye paloaltonetworks.com, también se incluyen como parte de la lista todos los componentes inferiores de este dominio, como *.paloaltonetworks.com. Tenga en cuenta que, si habilita este ajuste, hace falta una entrada adicional para cada uno de los dominios de cada lista, lo cual se traduce en que se duplica el número de entradas usado.

STEP 8 | Introduzca el **Source (Origen)** de la lista que acaba de crear en el servidor web. El origen deben incluir la ruta completa para acceder a la lista. Por ejemplo, https://1.2.3.4/EDL_IP_2015.

- Si está creando una lista dinámica externa de IP predefinida, seleccione una fuente de dirección IP malintencionada de Palo Alto Networks para usar como origen.
- Si crea una lista dinámica externa de URL predefinida, seleccione **panw-auth-portal-exclude-list** como origen.

STEP 9 | Si el origen de la lista está asegurado con SSL (es decir, listas con URL HTTPS), habilite la autenticación de servidor. Seleccione un **Certificate Profile (Perfil de certificado)** o cree un **New Certificate Profile (Perfil de certificado nuevo)** para autenticar el servidor que aloja la lista. El perfil de certificado que seleccione debe tener certificados de autoridad CA raíz y certificados CA intermedios que coincidan con los certificados instalados en el servidor que usted está autenticando.

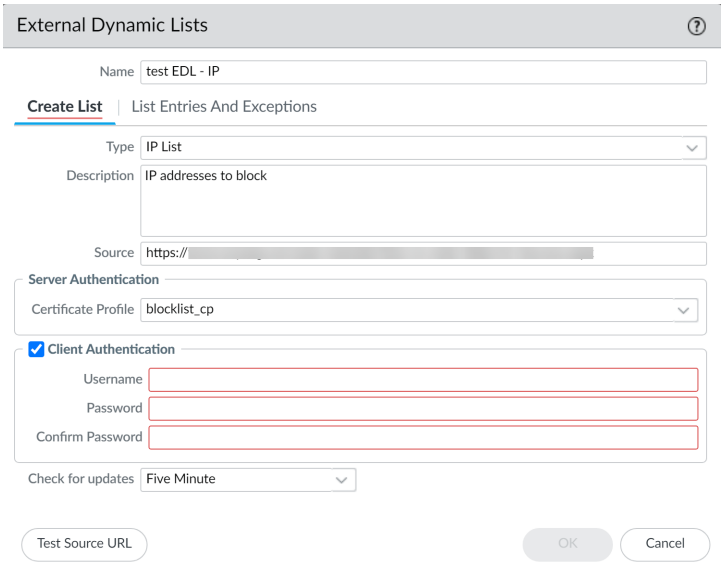


Maximice la cantidad de listas dinámicas externas que puede usar para aplicar la política. Utilice el mismo perfil de certificado para autenticar las listas dinámicas externas de la misma URL de origen. Si asigna diferentes perfiles de certificado a listas dinámicas externas de la misma URL de origen, el cortafuegos cuenta cada lista como lista dinámica externa única.

STEP 10 | Habilite la autenticación del cliente si el origen de la lista posee una URL HTTPS y requiere una autenticación HTTP para el acceso a la lista.

1. Seleccione **Client Authentication (Autenticación de cliente)**.
2. Ingrese un nombre de usuario válido en **Username (Nombre de usuario)** para acceder a la lista.
3. Especifique el valor de **Contraseña** y seleccione **Confirmar contraseña**.

© 2020 Palo Alto Networks, Inc.



STEP 11 | (No disponible en Panorama o para EDL de URL predefinida) Haga clic en **Test Source URL (Comprobar URL de origen)** para comprobar que el cortafuegos pueda conectarse al servidor web.

La función Test Source URL (URL de origen de prueba) no está disponible cuando se utiliza la autenticación para el acceso de EDL.

STEP 12 | (Opcional) Especifique la frecuencia con la que el cortafuegos debe **buscar actualizaciones** en la lista. Por defecto, el cortafuegos recupera la lista una vez por hora y confirma los cambios.

El intervalo es relativo a la última confirmación. Entonces, para el intervalo de cinco minutos , la confirmación se produce en 5 minutos si la última confirmación fue una hora atrás. Para recuperar la lista inmediatamente, consulte Recuperar una lista dinámica externa del servidor web.

STEP 13 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 14 | (Opcional) Las EDL se muestran por orden de evaluación de arriba abajo. Use los controles de dirección situados en la parte inferior de la página para cambiar el orden de la lista. Esto permite ordenar las listas para garantizar que se confirmen las EDL más importantes antes de que se alcancen los límites de capacidad.

Solo puede cambiar el orden de las EDL si no está seleccionada la opción Group By Type (Agrupar por tipo).

STEP 15 | Aplique la política en una lista dinámica externa.

Si la autenticación del servidor o cliente falla, el cortafuegos deja de aplicar la política en función de la última lista dinámica externa recuperada correctamente. Busque las listas dinámicas externas que fallaron en la autenticación *y vea los motivos del fallo de la autenticación.*

© 2020 Palo Alto Networks, Inc.

Recuperación de una lista dinámica externa del servidor web

Cuando realiza la Configuración del cortafuegos para acceder a la lista dinámica externa, configura el cortafuegos para recuperar la lista del servidor web cada hora (valor predeterminado), cada cinco minutos, cada día, cada semana o cada mes. Si ha añadido o eliminado direcciones IP de la lista y necesita realizar una actualización inmediata, utilice el siguiente proceso para recuperar la lista actualizada.

STEP 1 | Para recuperar la lista a demanda, seleccione **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**.

STEP 2 | Seleccione la lista que desea actualizar y haga clic en **Import Now (Importar ahora)**. La tarea de importar la lista se añadirá a la cola.

STEP 3 | Para ver el estado de la tarea en el gestor de tareas, consulte Gestión y supervisión de tareas administrativas.

STEP 4 | (Opcional) Una vez que el cortafuegos recupere la lista, lleve a cabo la Visualización de entradas de lista dinámica externa.

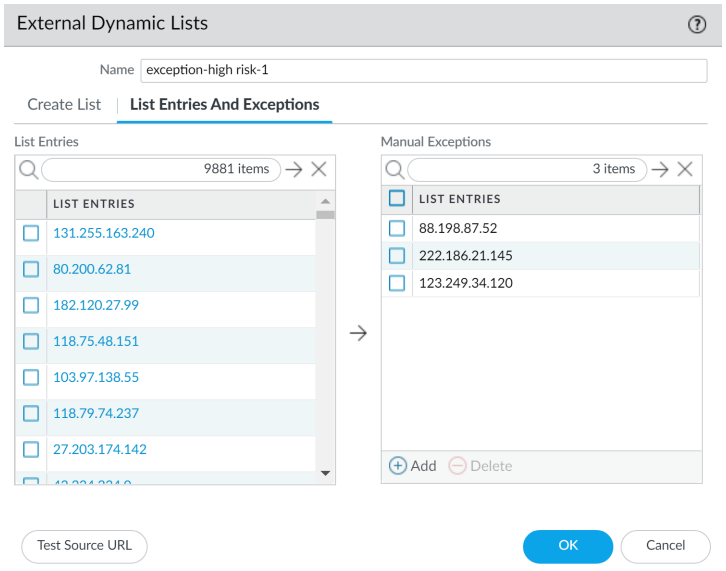
Visualización de entradas de lista dinámica externa

Antes de realizar la Aplicación de la política en una lista dinámica externa, puede ver el contenido de una lista dinámica externa directamente en el cortafuegos para comprobar que contiene las direcciones IP, los dominios o las URL. Las entradas que se muestran se basan en la versión de la lista dinámica externa que el cortafuegos recuperó más recientemente.

STEP 1 | Seleccione **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**.

STEP 2 | Haga clic en la lista dinámica externa que desea ver.

STEP 3 | Haga clic en **List Entries and Exceptions (Entradas y excepciones de la lista)** y vea los objetos que el cortafuegos recuperó de la lista.



Es posible que la lista esté vacía si se producen las siguientes condiciones:

© 2020 Palo Alto Networks, Inc.

- El cortafuegos aún no recuperó la lista dinámica externa. Para obligar al cortafuegos a recuperar una lista dinámica externa de inmediato, lleve a cabo la Recuperación de una lista dinámica externa del servidor web.
- El cortafuegos es incapaz de acceder al servidor que aloja la lista dinámica externa. Haga clic en **Test Source URL (Probar URL de origen)** para comprobar que el cortafuegos puede conectarse al servidor.

STEP 4 | Introduzca una dirección IP, un dominio o una URL (según el tipo de lista) en el campo de filtro y haga clic en Apply Filter (Aplicar filtro) (→) para comprobar que se encuentre en la lista. Realice la Exclusión de entradas de una lista dinámica externa en función de las direcciones IP, los dominios y las URL que desea bloquear o permitir.

STEP 5 | (Opcional) Vea el resumen de inteligencia de AutoFocus para obtener información sobre una entrada de la lista. Coloque el cursor sobre una entrada para abrir el menú desplegable y haga clic en **Autofocus**.

Exclusión de entradas de una lista dinámica externa

Cuando visualiza las entradas de una lista dinámica externa, puede excluir hasta 100 entradas de la lista. La capacidad de excluir entradas de una lista dinámica externa le ofrece la opción de aplicar la política a algunas de las entradas (no a todas) en una lista. Esto es útil si no puede editar el contenido de una lista dinámica externa (como la fuente de direcciones IP de alto riesgo de Palo Alto Networks) debido a que proviene de un origen externo.

STEP 1 | Visualización de entradas de lista dinámica externa.

STEP 2 | Seleccione hasta 100 entradas para excluir de la lista y haga clic en Submit (Enviar) (→) o **Add (Añadir)** para añadir manualmente una excepción de la lista.

- No puede guardar los cambios de la lista dinámica externa si tiene entradas duplicadas en la lista de excepciones manuales. Para identificar las entradas duplicadas, busque entradas con un subrayado rojo.
- Una excepción manual debe coincidir con una entrada en la lista con exactitud. Por ejemplo, si el rango de una dirección IP es una entrada de la lista e introduce manualmente una dirección IP única dentro de este rango como excepción de la lista, el cortafuegos aplicará la política en todas las direcciones IP en este rango. De modo que para excluir esa dirección IP única, primero debe asegurarse de que sea una entrada independiente de la lista dinámica externa y agregar la misma dirección IP a la lista de excepciones.

STEP 3 | Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** para guardar los cambios.

STEP 4 | (Opcional) Aplicación de la política en una lista dinámica externa.

Aplicación de la política en una lista dinámica externa

Bloquee o permita el tráfico en función de las direcciones IP o URL en una lista dinámica externa, o utilice una lista de dominios dinámicos con un sinkhole de DNS para prevenir el acceso a dominios maliciosos.

Consejos sobre la aplicación de la política en el cortafuegos con listas dinámicas externas:

- *Cuando se visualizan listas dinámicas externas en el cortafuegos (Objects [Objetos] > External Dynamic Lists [Listas dinámicas externas]), haga clic en List Capacities (Capacidades de la lista) para comparar cuántas direcciones IP, dominios y URL se*

© 2020 Palo Alto Networks, Inc.

utilizan actualmente en la política con la cantidad total de entradas que admite el cortafuegos en cada tipo de lista.

- *Lleve a cabo el* Uso de Global Find para buscar el cortafuegos o servidor de gestión de Panorama *para un dominio, dirección IP o URL que pertenece a una o más listas dinámicas externas y se utiliza en la política. Esto es útil para determinar la lista dinámica externa (se menciona en una regla de la política de seguridad) que causa que el cortafuegos bloquee o permita un dominio, dirección IP o URL determinado.*
- *Use los controles de dirección situados en la parte inferior de la página para cambiar el orden de evaluación de las EDL. Esto permite ordenar las listas para garantizar que se confirmen las entradas más importantes de las EDL antes de que se alcancen los límites de capacidad.*



Solo puede cambiar el orden de las EDL si no está seleccionada la opción Group By Type (Agrupar por tipo).

- Configuración del sinkholing de DNS para una lista de dominios personalizados.
- Uso de una lista dinámica externa en un perfil de filtro de URL.
- **Utilice una lista dinámica externa de tipo URL como criterio de coincidencia en una regla de política de seguridad.**
  1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
  2. Haga clic en **Add** e introduzca un nombre descriptivo en **Name** para la lista.
  3. En la pestaña **Source**, seleccione la **Source Zone**.
  4. En la pestaña **Destination**, seleccione la **Destination Zone**.
  5. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, haga clic en **Add (Añadir)** para seleccionar la lista dinámica externa de la lista de categorías URL.
  6. En la pestaña **Actions (Acciones)**, defina **Action Setting (Configuración de acción)** en **Allow (Permitir)** o **Deny (Denegar)**.
  7. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.
  8. Verifique si las entradas en la lista dinámica externa se ignoraron u omitieron.

     Use el siguiente comando CLI en un cortafuegos para revisar los detalles de una lista.

     ```
     request
     system external-list show type <domain | ip | url> name_of_list
     ```

     Por ejemplo:

     ```
     request system
     external-list show type url EBL_ISAC_Alert_List
     ```
  9. Compruebe que la acción de política esté forzada.
     1. Realice la Visualización de las entradas de la lista dinámica externa para la lista de URL e intente acceder a la URL desde la lista.
     2. Verifique que la acción que definió se haya aplicado.
     3. Para supervisar la actividad del cortafuegos:
        - Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de la red y la actividad bloqueada para la URL a la cual accedió.

© 2020 Palo Alto Networks, Inc.

- Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)** para acceder a la vista detallada del log.

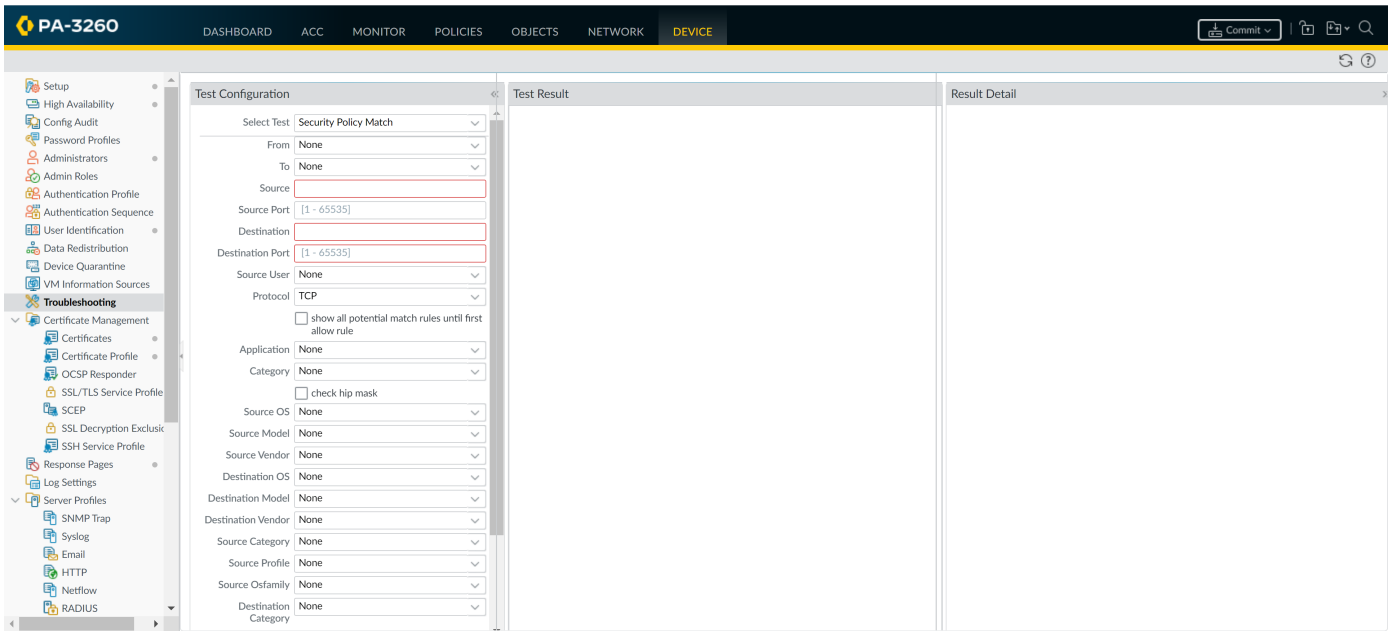
- **Utilice una lista dinámica externa IP o una lista dinámica externa IP predefinida como un objeto de dirección de origen o destino en una regla de la política de seguridad.**

  Esta capacidad resulta útil si implementa nuevos servidores y desea permitir el acceso a dichos servidores sin requerir una confirmación de cortafuegos.

  1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
  2. Haga clic en **Add (Añadir)** y asigne un nombre descriptivo a la regla en **Name (Nombre)**.
  3. En las pestañas **Source (Origen)** y **Destination (Destino)**, defina las EDL que se deben usar como direcciones de origen y destino, respectivamente.
  4. En la pestaña Service/URL Category (Servicio/Categoría de URL), compruebe que **Service (Servicio)** está definido en **application-default (valor predeterminado para la aplicación)**.
  5. En la pestaña Actions (Acciones), configure Action Setting (Configuración de acción) para **Allow (Permitir)** o **Deny (Denegar)**.

     Cree listas dinámicas externas separadas si desea especificar acciones de permiso y denegación para direcciones IP concretas.
  6. Deje el resto de opciones con los valores predeterminados.
  7. Haga clic en **OK (Aceptar)** para guardar los cambios.
  8. Haga clic en **Commit (Confirmar)** para confirmar los cambios.
  9. Compruebe que la acción de política esté forzada.

     1. Realice la Visualización de las entradas de la lista dinámica externa para la lista dinámica externa e intente acceder a una dirección IP desde la lista.
     2. Verifique que la acción que definió se haya aplicado.
     3. Seleccione **Monitor (Supervisar)** > **Logs** > **Traffic (Tráfico)** y visualice la entrada del log de la sesión.
     4. Para verificar la regla de la política que coincide con un flujo, seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y ejecute la prueba Security Policy Match (Coincidencia con política de seguridad):



© 2020 Palo Alto Networks, Inc.

- **Utilice una lista dinámica externa URL predefinida para excluir los dominios benignos que utilizan las aplicaciones para el tráfico en segundo plano de la política de autenticación.**

  Cuando seleccione el tipo de EDL **panw-auth-portal-exclude-list**, podrá excluir fácilmente de la aplicación de la política de autenticación los dominios que muchas aplicaciones utilizan para el tráfico en segundo plano, como actualizaciones y otros servicios de confianza. Esto garantiza que el cortafuegos no bloquee el tráfico necesario para estos servicios y que el mantenimiento de la aplicación no se interrumpa.

  1. Seleccione **Policies (Políticas)** > **Authentication (Autenticación)**.
  2. En la pestaña **Service/URL Category (Categoría de URL/servicio)**, seleccione la EDL de URL predefinida como **URL Category (Categoría de URL)**.
  3. En la pestaña **Actions (Acciones)**, seleccione **`default-no-captive-portal`** como **Authentication Enforcement (Aplicación de la autenticación)**.
  4. Haga clic en **OK (Aceptar)**.
  5. **Mueva** la regla a la parte superior para que sea la primera regla de la política.
  6. **Commit (Confirmar)** los cambios.

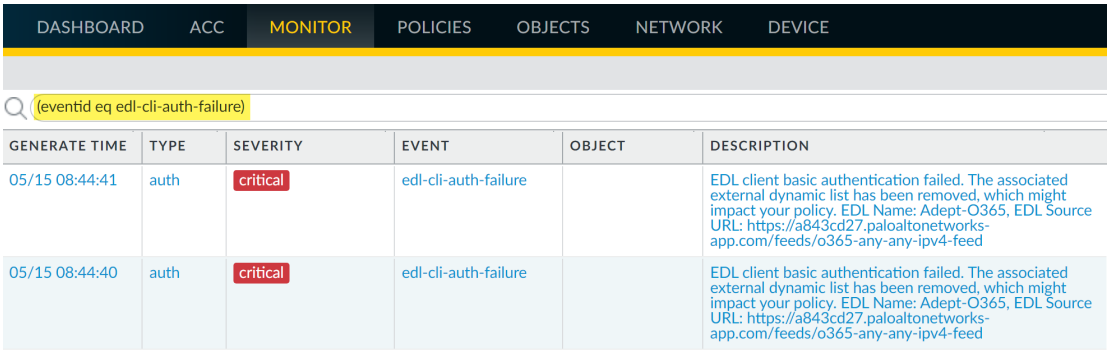
Búsqueda de listas dinámicas externas con autenticación fallida

Cuando una lista dinámica externa que requiere SSL falla la autenticación de cliente o servidor, el cortafuegos genera un log de sistema de gravedad crítica. El log es crítico debido a que el cortafuegos interrumpe la aplicación de la política basada en la lista dinámica externa una vez falla la autenticación. Utilice el siguiente proceso para visualizar los mensajes del log del sistema crítico que le informan del fallo de autenticación relacionado con las listas dinámicas externas.

STEP 1 | Seleccione **Monitor (Supervisar)** > **Logs** > **System (Sistema)**.

STEP 2 | Construya los siguientes filtros para visualizar todos los mensajes relacionados con fallos de autenticación y aplique los filtros. Para obtener más información, revise el flujo de trabajo completo para realizar el Filtrado de logs.

- Fallo de autenticación de servidor: **`(eventid eq tls-edl-auth-failure)`**
- Fallo de autenticación de cliente: **`(eventid eq edl-cli-auth-failure)`**



STEP 3 | Revise los mensajes del log del sistema. La descripción del mensaje incluye el nombre de la lista dinámica externa, la URL de origen de la lista y el motivo del fallo de autenticación.

El servidor que aloja la lista dinámica externa falla la autenticación si el certificado ha vencido. Si ha configurado el perfil del certificado para comprobar el estado de revocación de certificados mediante la lista de revocación de certificados (CRL) o el protocolo de estado de certificado en línea (OCSP), es posible que es servidor también falle la autenticación si se cumple alguna de las siguientes condiciones:

- El certificado se ha revocado.

© 2020 Palo Alto Networks, Inc.

- El estado de revocación del certificado es desconocido.
- Se acaba el tiempo de espera de la conexión mientras el cortafuegos intenta conectarse al servicio de CRL/OCSP.

Para obtener más información sobre la configuración del perfil de certificados, consulte los pasos para realizar la Configuración de un perfil de certificado.

Compruebe que añadió la CA de raíz y la CA intermedia del servidor para el perfil de certificados que configuró con la lista dinámica externa. De lo contrario, el cortafuegos no autenticará la lista adecuadamente.

La autenticación de cliente falla si introdujo la combinación de nombre de usuario y contraseña incorrecta para la lista dinámica externa.

STEP 4 | (Opcional) Realice la Deshabilitación de autenticación para una lista dinámica externa que falló la autenticación como una medida provisional hasta que el propietario de la lista renueve el certificado del servidor que aloja la lista.

Deshabilitación de autenticación para una lista dinámica externa

Palo Alto Networks recomienda que habilite la autenticación en los servidores que alojan las listas dinámicas externas configuradas en su cortafuegos. Sin embargo, si realiza la Búsqueda de listas dinámicas externas con autenticación fallida y prefiere deshabilitar la autenticación de servidor en estas listas, puede realizarlo mediante la CLI. El procedimiento a continuación solo se aplica a las listas dinámicas externas protegidas con SSL (es decir, las listas con URL de HTTPS); el cortafuegos no aplica la autenticación de servidor en las listas con una URL de HTTP.

Si deshabilita la autenticación de servidor en una lista dinámica externa, también se deshabilitará la autenticación de cliente. Si la autenticación de cliente está deshabilitada, el cortafuegos no podrá conectarse a una lista dinámica externa que requiera un nombre de usuario y una contraseña para el acceso.

STEP 1 | Ejecute la CLI y cámbiela a modo de configuración de la siguiente manera:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

El cambio del símbolo > al símbolo # indica que se encuentra en modo de configuración.

STEP 2 | Introduzca el comando de la CLI adecuado para el tipo de lista:

- Dirección IP

```
set external-list <external dynamic list name> type ip certificate-profile
 None
```

- Dominio

```
set external-list <external dynamic list name> type domain certificate-
profile None
```


© 2020 Palo Alto Networks, Inc.

- URL

```
set external-list <external dynamic list name> type url certificate-
profile None
```

STEP 3 | Compruebe que la autenticación se encuentre deshabilitada para la lista dinámica externa.

Actualice la lista (consulte Recuperación de una lista dinámica externa del servidor web). Si el cortafuegos recupera la lista correctamente, la autenticación de servidor está deshabilitada.

© 2020 Palo Alto Networks, Inc.

Registro de direcciones IP y etiquetas dinámicamente

Para reducir los desafíos de diversidad de tamaños, falta de flexibilidad y rendimiento, la arquitectura de las redes de hoy en día permite asignar, cambiar y eliminar máquinas virtuales (Virtual Machines, VM) y aplicaciones bajo demanda. Sin embargo, esta agilidad plantea un desafío a los administradores de seguridad, ya que tienen una visibilidad limitada de las direcciones IP de las VM y numerosas aplicaciones con asignación dinámica que pueden habilitarse en estos recursos virtuales.

Los cortafuegos (modelos basados en hardware y VM-Series) admiten la capacidad de registrar direcciones IP, grupos de IP (intervalos IP y subredes) y etiquetas de forma dinámica. Las direcciones IP y las etiquetas se pueden registrar en el cortafuegos directamente o mediante Panorama. Además, puede eliminar etiquetas automáticamente de las direcciones IP de origen y destino que se incluyen en un log del cortafuegos.



PAN-OS solo admite intervalos y subredes IP IPv4 en grupos de direcciones dinámicas.

Puede habilitar el proceso de registro dinámico con cualquiera de las siguientes opciones:

- **User-ID agent for Windows (Agente de User-ID para Windows)**: en un entorno donde ha implementado el agente User-ID, puede habilitar el agente User-ID para supervisar 100 servidores VMware ESXi o vCenter, o una combinación de ambos. Al asignar o modificar máquinas virtuales en estos servidores VMware, el agente puede recuperar los cambios de direcciones IP y compartirlos con el cortafuegos.
- **VM Information Sources (Orígenes de información de VM)**: le permite supervisar los servidores VMware ESXi y vCenter, así como AWS-VPC y Google Compute Engine de forma nativa en el cortafuegos para recuperar los cambios de direcciones IP cuando asigna o modifica máquinas virtuales en estas fuentes. Las opción de orígenes de información de VM sondean en busca de un conjunto predefinido de atributos y no requiere secuencias de comandos externas para registrar las direcciones IP a través de la API XML. Consulte Supervisión de cambios en el entorno virtual.
- **Panorama Plugin (Complemento de Panorama)**: permite habilitar un dispositivo virtual o M-Series de Panorama™ para que se conecten al entorno de nube pública de AWS o Azure y recuperen información sobre las máquinas virtuales implementadas con su suscripción o en la VPC. Después, Panorama registra la información de la VM en los cortafuegos gestionados de Palo Alto Networks que tiene configurados para las notificaciones y, por lo tanto, puede usar los atributos para definir grupos de direcciones dinámicas y adjuntarlos a las reglas de política de seguridad a fin de permitir o denegar el tráfico desde y hacia estas VM.
- **VMware Service Manager (Administrador de servicios VMware)** (solo para la solución NSX integrada): la solución NSX integrada está diseñada para la asignación y distribución automáticas de la Security Operating Platform® de próxima generación de Palo Alto Networks y para el ofrecimiento de políticas de seguridad dinámicas basadas en contexto mediante Panorama. NSX Manager actualiza Panorama con la información más reciente de las etiquetas, grupos de IP y direcciones IP asociadas a las máquinas virtuales implementadas en esta solución integrada. Para obtener información sobre esta solución, consulte Configuración de un cortafuegos VM-Series NSX Edition.
- **API XML**: El cortafuegos y Panorama admiten una API XML que use solicitudes HTTP estándar para enviar y recibir datos. Puede usar esta API para registrar direcciones IP y etiquetas en el cortafuegos o Panorama. Puede realizar llamadas directamente desde utilidades de líneas de comando como cURL o usando cualquier marco de secuencias de comandos o aplicaciones compatible con servicios basados en REST. Consulte la Guía de uso de PAN-OS XML API para obtener más información.
- **Auto-Tag (Etiquetado automático)**: etiquete la dirección IP de origen o de destino automáticamente cuando se genere un log en el cortafuegos, y registre la dirección IP y la asignación de etiquetas a un agente de User-ID en el cortafuegos o en Panorama, o a un agente de User-ID remoto que utilice un

© 2020 Palo Alto Networks, Inc.

perfil de servidor HTTP. Por ejemplo, siempre que el cortafuegos genere un log de amenaza, puede configurar el cortafuegos de modo que etiquete la dirección IP de origen en el log de amenaza con un nombre de etiqueta. Para obtener más información, consulte Uso de etiquetado automático para automatizar acciones de seguridad.

Además, puede configurar el cortafuegos de modo que anule el registro de las etiquetas de forma dinámica cuando transcurra el tiempo de espera configurado. Por ejemplo, puede configurar el tiempo de espera para que tenga la misma duración que el tiempo de espera de la concesión de DHCP para la dirección IP. Esto permite que la asignación de la dirección IP a la etiqueta caduque al mismo tiempo que la concesión de DHCP, por lo que no se aplicará la política accidentalmente cuando se reasigne la dirección IP.

Consulte Reenvío de logs a un destino HTTP(S).

Para obtener información sobre cómo crear y utilizar grupos de direcciones dinámicas, consulte Uso de grupos de direcciones dinámicas en políticas.

Para conocer los comandos de la CLI para registrar etiquetas dinámicamente, consulte Comandos de la CLI para etiquetas y direcciones IP.

© 2020 Palo Alto Networks, Inc.

Uso de grupos de usuarios dinámicos en políticas

Los grupos de usuarios dinámicos lo ayudan a crear una política que proporcione una corrección automática para el comportamiento anómalo del usuario y la actividad maliciosa a la vez que mantiene la visibilidad del usuario. Después de crear el grupo y confirmar los cambios, el cortafuegos registra los usuarios y las etiquetas asociadas y, después, actualiza automáticamente la pertenencia al grupo de usuarios dinámicos. Puesto que las actualizaciones de la pertenencia al grupo de usuarios dinámicos son automáticas, el uso de grupos de usuarios dinámicos en lugar de objetos de grupo estáticos le permite responder a cambios en el comportamiento del usuario o amenazas potenciales sin cambios manuales de políticas.

Para determinar qué usuarios incluir como miembros, un grupo de usuarios dinámico utiliza etiquetas como criterios de filtrado. En cuanto un usuario coincide con los criterios de filtrado, el usuario se convierte en miembro del grupo de usuarios dinámico. El filtro basado en etiquetas usa los operadores lógicos *y* y *o*. Cada etiqueta es un elemento de metadatos o un par de atributo-valor que registra en la fuente de forma estática o dinámica. Las etiquetas estáticas forman parte de la configuración del cortafuegos, mientras que las etiquetas dinámicas son parte de la configuración del tiempo de ejecución. Como resultado, no necesita enviar actualizaciones a las etiquetas dinámicas si ya están asociadas a una política que ha confirmado en el cortafuegos.

Para registrar etiquetas dinámicamente, puede usar las siguientes opciones:

- XML API
- El agente de User-ID
- Panorama
- La interfaz web en el cortafuegos

El cortafuegos redistribuye las etiquetas para el grupo de usuarios dinámicos a los agentes de redistribución de escucha, que incluyen otros cortafuegos, Panorama o un recopilador de logs dedicado, así como aplicaciones Cortex.



Para admitir la redistribución de etiquetas de grupos de usuarios dinámicos, todos los cortafuegos deben usar PAN-OS 9.1 para recibir las etiquetas de las fuentes de registro.

El cortafuegos redistribuye las etiquetas para el grupo de usuarios dinámicos al siguiente salto y puede configurar el reenvío de logs para enviar los logs a un servidor específico. El reenvío de logs también le permite usar el etiquetado automático para añadir o eliminar automáticamente miembros de grupos de usuarios dinámicos en función de los eventos en los logs.

STEP 1 | Seleccione **Objects (Objetos)** > **Dynamic User Groups (Grupos de usuarios dinámicos)** y **añada** un nuevo grupo de usuario dinámico.

STEP 2 | Defina la pertenencia del grupo de usuarios dinámicos.

1. Introduzca un **nombre** para el grupo.
2. (Opcional) Introduzca una **descripción** para el grupo.
3. **Añada criterios de coincidencia** con etiquetas dinámicas para definir los miembros en el grupo de usuarios dinámicos.
4. (Opcional) Utilice los operadores **And** o **Or** con las etiquetas que quiera usar para filtrar o aplicar criterios de coincidencia.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

6. (Opcional) Seleccione las **etiquetas** que desee asignar al propio grupo.

   Esta etiqueta se muestra en la columna Tags (Etiquetas) en la lista de grupo de usuarios dinámicos y define el objeto de grupo dinámico, no los miembros del grupo.
7. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

   Si actualiza el filtro de objetos del grupo de usuarios, debe confirmar los cambios para actualizar la configuración.

STEP 3 | Según la información de log que desee utilizar como criterios de coincidencia, configure el etiquetado automático mediante la creación de un perfil de reenvío de logs o la configuración de los ajustes del log.

- Para los logs de autenticación, datos, amenazas, tráfico, inspección de túnel, URL y WildFire, cree un perfil de reenvío de logs.
- Para los logs de User-ID, coincidencias HIP, GlobalProtect e IP-Tag, establezca la configuración de log.

STEP 4 | (Opcional) Para devolver a los miembros del grupo de usuarios dinámicos a sus grupos originales después de un periodo específico, especifique un valor de **tiempo de espera** en minutos (el valor predeterminado es 0, el intervalo es de 0 a 43 200).

STEP 5 | Utilice el grupo de usuarios dinámico en una política para regular el tráfico de los miembros del grupo.

Deberá crear al menos dos reglas: una para permitir que el tráfico inicial complete el grupo de usuarios dinámico y otra para negar el tráfico para la actividad que desee evitar. Para etiquetar usuarios, la regla para permitir el tráfico debe tener un número de regla más alto en su base de reglas que la regla que niega el tráfico.

1. Seleccione el grupo de usuarios dinámicos del paso 1 como **usuario de origen**.
2. Cree la regla en la que la **acción** deniegue el tráfico a los miembros del grupo de usuarios dinámicos.
3. Cree la regla que permita que el tráfico complete los miembros del grupo de usuarios dinámicos.
4. Si configuró un perfil de **reenvío de logs** en el paso 3, selecciónelo para añadirlo a la política.
5. **Commit (Confirmar)** los cambios.

STEP 6 | (Opcional) Refine la pertenencia del grupo y defina la fuente de registro para las actualizaciones de asignación de etiqueta al usuario.

Si la asignación inicial de la etiqueta al usuario recupera usuarios que no deberían ser miembros o si no incluye a los usuarios que deberían serlo, modifique los miembros del grupo para incluir a los usuarios para los que desea aplicar la política y especifique el origen para las asignaciones.

1. En la columna **Users (Usuarios)**, seleccione **more (más)**.
2. **Registre usuarios** para añadirlos al grupo y seleccione el **origen de registro** para las etiquetas y asignaciones de etiqueta al usuario.
   - **Local** (predeterminado): registre las etiquetas y asignaciones para los miembros del grupo de usuarios dinámicos localmente en el cortafuegos.
   - **Agente de User-ID de Panorama**: registre las etiquetas y asignaciones para los miembros del grupo de usuarios dinámicos en un agente de User-ID conectado a Panorama. Si el grupo de usuarios dinámicos se origina en Panorama, la fila se muestra en amarillo y el nombre del grupo, la descripción, los criterios de coincidencia y las etiquetas son de solo lectura. Sin embargo, puede registrar o cancelar el registro de usuarios del grupo.

© 2020 Palo Alto Networks, Inc.

- **Agente de User-ID de dispositivo remoto**: registre las etiquetas y asignaciones para los miembros del grupo de usuarios dinámicos en un agente de User-ID remoto. Para seleccionar esta opción, primero debe configurar un perfil de servidor HTTP.

3. Seleccione las **etiquetas** que desee registrar en el origen con las etiquetas que utilizó para configurar el grupo.
4. (Opcional) Para devolver a los miembros del grupo de usuarios dinámicos a sus grupos originales después de un periodo específico, especifique un valor de **tiempo de espera** en minutos (el valor predeterminado es 0, el intervalo es de 0 a 43 200).
5. **Añada** o **elimine** usuarios según sea necesario.
6. (Opcional) **Anule el registro de usuarios** para eliminar sus etiquetas y asignaciones de etiqueta al usuario.

STEP 7 | Compruebe que el cortafuegos complete correctamente los usuarios en el grupo de usuarios dinámicos.

1. Confirme que la columna **Dynamic User Group (Grupo de usuarios dinámicos)** en los logs de tráfico, amenaza, filtrado de URL, envíos de WildFire, filtrado de datos e inspección de túnel se muestran los grupos de usuarios dinámicos correctamente.
2. Utilice el comando **`show user group list dynamic`** para Ver una lista de todos los grupos de usuarios dinámicos, así como el número total de esos grupos.
3. Utilice el comando **`show object registered-user all`** para mostrar una lista de usuarios que son miembros registrados de grupos de usuarios dinámicos.
4. Utilice el comando **`show user group name`** ***`group-name`*** para ver información sobre el grupo de usuarios dinámicos, como el tipo de origen.

© 2020 Palo Alto Networks, Inc.

Uso de etiquetado automático para automatizar acciones de seguridad

El etiquetado automático permite que el cortafuegos o Panorama etiquete un objeto de política cuando reciba un log que coincida con criterios específicos y establezca una asignación de etiqueta a la dirección IP o al usuario. Por ejemplo, siempre que el cortafuegos genere un log de amenazas, puede configurar el cortafuegos de modo que etiquete la dirección IP de origen o el usuario de origen en el log de amenaza con un nombre de etiqueta. Después, puede usar esas etiquetas para completar automáticamente los objetos de política, como grupos de usuarios dinámicos o grupos de direcciones dinámicas, que puede utilizar posteriormente para automatizar acciones de seguridad en políticas de seguridad, autenticación o descifrado. Por ejemplo, cuando cree un filtro para los logs de URL para `yes (sí)` en la columna **Credential Detected (Credencial detectada)**, puede aplicar una etiqueta al usuario que aplique una política de autenticación que requiera que un usuario se autentique mediante la autenticación multifactor (Multi-Factor Authentication, MFA).

Para redistribuir las asignaciones en su red, registre las asignaciones de la etiqueta a la dirección IP y al usuario en un agente de User-ID integrado en PAN-OS en el cortafuegos o Panorama o en un agente de User-ID remoto mediante un perfil de servidor HTTP . El cortafuegos puede eliminar (anular el registro) automáticamente una etiqueta asociada a una dirección IP o usuario cuando configure un tiempo de espera como parte de una acción integrada para un perfil de reenvío de logs o como parte de la configuración de reenvío de logs. Por ejemplo, si el cortafuegos detecta que un usuario tiene credenciales potencialmente comprometidas, puede configurar el cortafuegos para que requiera la autenticación MFA para ese usuario durante un periodo determinado y, después, configurar un tiempo de espera para eliminar el usuario del grupo de requisitos de MFA.

STEP 1 | Según el tipo de log que desee utilizar para el etiquetado, cree un perfil de reenvío de logs o establezca la configuración de logs para definir cómo desea que el cortafuegos o Panorama gestione los logs.

- Para los logs de autenticación, datos, amenazas, tráfico, inspección de túnel, URL y WildFire, cree un perfil de reenvío de logs.
- Para los logs de User-ID, coincidencias HIP, GlobalProtect e IP-Tag, establezca la configuración de log.

STEP 2 | Defina los criterios de la lista de coincidencias que determinan cuándo el cortafuegos o Panorama añaden la etiqueta al objeto de política.

Por ejemplo, puede usar un filtro para configurar un umbral o definir un valor (como **`user eq "unknown"`** para identificar a los usuarios que el cortafuegos aún no ha asignado); cuando el cortafuegos alcance ese umbral o detecte ese valor, añadirá la etiqueta.

- Para crear un perfil de reenvío de logs, **añádalo** y seleccione el **tipo de log** que desee supervisar para los criterios de la lista de coincidencias (**Objects (Objetos)** > **Log Forwarding (Reenvío de logs)**).
- Para establecer la configuración de log, **añada** la configuración de log para el tipo de log que desee supervisar para los criterios de la lista de coincidencias (**Device (Dispositivo)** > **Log Settings (Configuración de log)**).

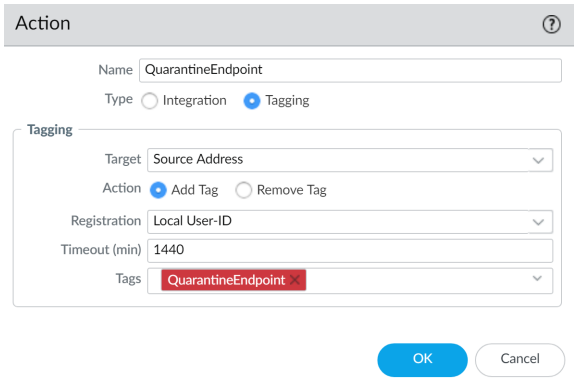
STEP 3 | Copie y pegue un valor de **filtro** o use el **generador de filtros** para definir los criterios de coincidencia para la etiqueta.

STEP 4 | Añada una acción integrada para etiquetar el objeto de política.

© 2020 Palo Alto Networks, Inc.

1. **Añada** las **acciones incorporadas** que desee que el cortafuegos o Panorama tome cuando los logs contengan una entrada que cumpla con los criterios de la lista de coincidencias.
2. **Establezca un nombre** para la acción.
3. Seleccione el tipo de **destino** que desee etiquetar (**Destination Address (Dirección de destino)**, **Source Address (Dirección de origen)**, **User (Usuario)** o **X-Forwarded-For Address (Dirección X-Forwarded-For)**).
4. Confirme que **Add Tag (Añadir etiqueta)** es la **acción**.
5. Seleccione el origen de **registro** para la etiqueta para determinar cómo el cortafuegos o Panorama redistribuye la asignación de la etiqueta a la dirección IP.
   - **Local User-ID (User-ID local)**: redistribuya la asignación de la etiqueta a la dirección IP en el agente de User-ID en el cortafuegos o Panorama.
   - **Panorama User-ID (User-ID de Panorama)**: redistribuya la asignación de la etiqueta a la dirección IP en Panorama.
   - **Remote User-ID (User-ID remoto)**: redistribuya la asignación de la etiqueta a la dirección IP en otro agente de User-ID con un perfil de servidor HTTP. Si selecciona esta opción, debe configurar un perfil de servidor HTTP (consulte el paso 5).
6. Especifique o seleccione las **etiquetas** que desee añadir al objeto de política.

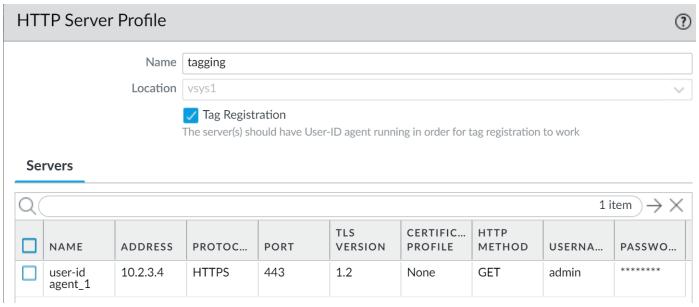
   Es posible que tenga que hacer clic fuera del campo o pulsar Intro para habilitar el botón **OK (Aceptar)**.
7. Haga clic en **OK (Aceptar)**.



STEP 5 | (Solo User-ID remoto) Configure un perfil de servidor HTTP para reenviar logs a un agente de User-ID remoto.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **HTTP**.
2. **Añada** un perfil y especifique un **nombre** para el perfil de servidor.
3. (Solo sistemas virtuales) Seleccione la **ubicación**. El perfil puede ser **Shared (Compartido)**entre todos los sistemas virtuales o aplicado a un sistema virtual específico.
4. Seleccione **Tag Registration (Registro de etiqueta)** para habilitar el cortafuegos para que registre la dirección IP y la asignación de etiquetas con el agente de User-ID en un cortafuegos remoto. Con el registro de etiqueta habilitado, usted no puede especificar el formato de carga útil.
5. **Añada** los detalles de conexión del servidor para acceder al agente de User-ID remoto y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.



6. Seleccione el perfil de reenvío de logs que creó y, a continuación, seleccione este perfil de servidor como el perfil del servidor HTTP para el **registro** de la etiqueta de **User-ID remoto**.

STEP 6 | Defina los objetos de política a los que desee aplicar las etiquetas.

1. Cree o seleccione uno de los siguientes objetos de política: grupos de direcciones dinámicas, Uso de grupos de usuarios dinámicos en políticas, direcciones, grupos de direcciones, zonas, reglas de políticas, servicios o grupos de servicios.
2. Especifique las etiquetas que desee aplicar al objeto como criterios de **coincidencia**.

   Confirme que la etiqueta es idéntica a la etiqueta del paso 4.

STEP 7 | Añada los objetos de política etiquetados a su política.

Este flujo de trabajo utiliza una política de seguridad como ejemplo, pero también puede usar objetos de política etiquetados en la política de autenticación.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** y escriba un **Name (Nombre)** y, opcionalmente, una **Description (Descripción)** para la política.
3. Añada la **zona de origen** en la que se origina el tráfico.
4. Añada la **zona de destino** en la que finaliza el tráfico.
5. Seleccione el objeto de **origen** que creó en el paso 5.1.
6. Seleccione si la regla **permitirá** o **denegará** el tráfico.

STEP 8 | Si configuró un perfil de reenvío de logs, asígnelo a su política de seguridad.

Puede asignar un perfil de reenvío de logs para cada política, pero puede asignar varios métodos y acciones por perfil. Por ejemplo, consulte Uso de grupos de direcciones dinámicas en políticas.

STEP 9 | **Commit (Confirmar)** los cambios.

STEP 10 | (Opcional) Configure un tiempo de espera para eliminar la etiqueta del objeto de política una vez transcurrido el tiempo especificado.

Especifique la cantidad de tiempo (en minutos) que transcurre antes de que el cortafuegos elimine la etiqueta del objeto de política. El intervalo es de 0 a 43 200. Si establece el tiempo de espera en cero, la asignación de la etiqueta a la dirección IP no se agota y debe eliminarse con una acción explícita. Si establece el tiempo de espera en un máximo de 43 200 minutos, el cortafuegos elimina la etiqueta después de 30 días.

Si elige la acción Remove Tag (Eliminar etiqueta), no puede configurar el tiempo de espera.

1. Seleccione un perfil de reenvío de logs.
2. **Añada** o edite una de las **acciones integradas**.
3. Especifique el **tiempo de espera** (en minutos). Cuando transcurra el tiempo especificado, el cortafuegos o Panorama eliminará la etiqueta.

© 2020 Palo Alto Networks, Inc.



Establezca el mismo tiempo de espera para la etiqueta IP y el arrendamiento de DHCP para esa dirección IP. Esto permite que la asignación de la dirección IP a la etiqueta caduque al mismo tiempo que la concesión de DHCP, por lo que no se aplicará la política accidentalmente cuando se reasigne la dirección IP.

4. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

© 2020 Palo Alto Networks, Inc.

Supervisión de cambios en el entorno virtual

Para proteger las aplicaciones y evitar amenazas en un entorno en el que aparecen constantemente nuevos usuarios y servidores, su política de seguridad ha de ser ágil. Para que sea ágil, el cortafuegos debe ser capaz de aprender las direcciones IP nuevas o modificadas y aplicar las políticas de manera consistente sin necesidad de realizar cambios de configuración en el cortafuegos.

Esta capacidad se proporciona mediante la coordinación entre las funciones de **VM Information Sources (Orígenes de información de VM)** y **Dynamic Address Groups (Grupos de direcciones dinámicas)** en el cortafuegos. El cortafuegos y Panorama ofrecen un modo automatizado de recopilar información en el inventario de máquinas virtuales (o invitadas) en cada origen supervisado y crear objetos de políticas que permanecen sincronizadas con los cambios dinámicos de la red.

- Habilitación de supervisión de VM para el registro de cambios en la red virtual
- Atributos supervisados en máquinas virtuales en plataformas en la nube
- Uso de grupos de direcciones dinámicas en políticas

Habilitación de supervisión de VM para el registro de cambios en la red virtual

Las fuentes de información de VM ofrecen un modo automatizado de recopilar información en el inventario de la máquina virtual (Virtual Machine, VM) en cada fuente supervisada (host); el cortafuegos puede supervisar los servidores VMware ESXi y vCenter, AWS-VPC, Microsoft Azure VNet y Google Cloud. Al implementar o mover equipos virtuales (invitados), el cortafuegos recopila una serie de atributos predefinidos (o elementos de metadatos) como etiquetas; estas etiquetas se pueden usar para definir grupos de direcciones dinámicas (consulte Uso de grupos de direcciones dinámicas en políticas) y buscar coincidencias en la política.

Puede configurar directamente el cortafuegos o usar las plantillas Panorama para supervisar hasta 10 fuentes de información de VM. **VM Information Sources (Fuentes de información de VM)** ofrece una configuración sencilla y le permite supervisar un conjunto de 16 elementos o atributos de metadatos. Consulte los Atributos supervisados en máquinas virtuales en plataformas en la nube de la lista. De manera predeterminada, el tráfico entre el cortafuegos y los orígenes supervisados usa el puerto de gestión (MGT) en el cortafuegos.



- *Si supervisa hosts ESXi que forman parte de la solución VM-Series NSX Edition, use grupos de direcciones dinámicas en lugar de orígenes de información de máquinas virtuales para obtener información sobre los cambios en el entorno virtual. Para la solución VM-Series edición NSX, NSX Manager le brinda a Panorama la información sobre el grupo de seguridad de NSX al cual pertenece una dirección IP. La información de NSX Manager brinda el contexto completo para definir los criterios de coincidencia en un grupo de direcciones dinámicas porque usa el ID de perfil de servicio como un atributo distintivo y le permite aplicar políticas de forma adecuada cuando tiene direcciones IP superpuestas en los diferentes grupos de seguridad. Se pueden registrar hasta un máximo de 32 etiquetas (del servidor vCenter y NSX Manager) en una dirección IP.*
- *Para supervisar las máquinas virtuales en su implementación de Microsoft Azure, en lugar de las fuentes de supervisión de VM, debe implementar la secuencia de comandos de supervisión de VM que se ejecuta en una máquina virtual dentro de la nube pública de Azure. La secuencia de comandos recopila información sobre la asignación de direcciones IP a etiquetas para sus activos de Azure, y lo publica en los cortafuegos y los sistemas virtuales correspondientes que especifica en la secuencia de comandos.*

© 2020 Palo Alto Networks, Inc.

- *Para la versión de Panorama 8.1.3 y posteriores, también puede usar el complemento de Panorama para AWS o Azure para recuperar la información de la VM y registrarla en los cortafuegos administrados. Consulte los* Atributos supervisados en máquinas virtuales en plataformas en la nube *para obtener más detalles.*

STEP 1 | Habilite la supervisión de VM.

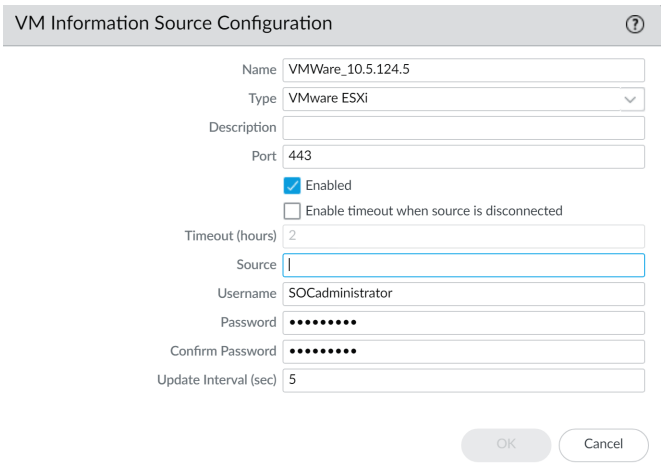
Puede configurar hasta 10 fuentes de información de VM en cada cortafuegos o para cada sistema virtual en cortafuegos con capacidad para varios sistemas virtuales.

Si sus cortafuegos están configurados con alta disponibilidad:

- En una configuración activa/pasiva, solo el cortafuegos activo supervisa las fuentes de VM.
- En una configuración activa/activa, solo el cortafuegos con el valor de prioridad principal supervisa las fuentes de VM.

1. Seleccione **Device (Dispositivo)** > **VM Information Sources (Fuentes de información de equipo virtual)**. Este ejemplo le muestra cómo añadir servidores VMware ESX(i) o vCenter.
2. Haga clic en **Add (Añadir)** y especifique la siguiente información:
   - Un **Name (Nombre)** para identificar la fuente que desea supervisar.
   - Seleccione el **Type (Tipo)** para indicar si la fuente es un **AWS VPC**, una instancia de **Google Compute Engine**, un servidor **VMware ESX(i)** o un servidor **VMware vCenter**.

     El tipo que selecciona determina los campos que se muestran.
   - Especifique el **puerto** en el que el origen está efectuando la escucha.
   - Para cambiar el valor predeterminado, seleccione la casilla de verificación **Habilitar el tiempo de espera cuando la fuente esté desconectada** y especifique el valor. Cuando se alcanza el límite especificado o si no se puede acceder al host o este no responde, el cortafuegos cerrará la conexión a la fuente.
   - Añada las credenciales (**Nombre de usuario** y **Contraseña**) para autenticar el servidor especificado más arriba.
   - Defina el **origen**: nombre de host o dirección IP.
   - (Opcional) Modifique el **Update interval (Intervalo de actualización)** a un valor entre 5-600 segundos. De manera predeterminada, el cortafuegos sondea cada 5 segundos. Las llamadas de la API se ponen en cola y recuperan cada 60 segundos, de modo que las actualizaciones pueden tardar hasta 60 segundos, más el intervalo de sondeo configurado.



   - Haga clic en **OK (Aceptar)** y seleccione **Commit (Confirmar)** los cambios.

© 2020 Palo Alto Networks, Inc.

- Compruebe que el **Status (Estado)** de conexión aparezca como conectado.

STEP 2 | Comprobar el estado de conexión

Compruebe que el **Status (Estado)** de conexión aparezca como conectado.



Si el estado de conexión está pendiente o desconectado, compruebe que el origen está operativo y que el cortafuegos puede acceder al origen. Si usa un puerto diferente a MGT para la comunicación con la fuente supervisada, debe cambiar la ruta de servicios (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]**, hacer clic en el enlace **Service Route Configuration [Configuración de ruta de servicios]** y modificar la **Source Interface [Interfaz de fuente]** para el servicio **VM Monitor [Supervisor de VM]**).

Atributos supervisados en máquinas virtuales en plataformas en la nube

A medida que aprovisiona o elimina las máquinas virtuales de la nube pública o privada, puede usar un complemento de Panorama, una secuencia de comandos de supervisión de VM o el origen de información de la VM en el cortafuegos de próxima generación para supervisar cambios en las máquinas virtuales (virtual machines, VM) implementadas en los entornos virtuales.

Orígenes de información de la VM: en un hardware o un cortafuegos VM-Series, puede supervisar instancias de máquinas virtuales y recuperar cambios a medida que aprovisiona o modifica los invitados configurados en los orígenes supervisados: AWS, ESXi o vCenter Server, o AWS. En cada cortafuegos (o sistema virtual si su cortafuegos admite varios sistemas virtuales), puede configurar hasta 10 orígenes. Para obtener información sobre cómo funcionan de forma sincronizada los orígenes de información de la VM y los grupos de direcciones dinámicas, y poder supervisar los cambios en el entorno virtual, consulte la Guía de implementación de VM-Series. Si sus cortafuegos están configurados con alta disponibilidad:

- En una configuración activa/pasiva, solo el cortafuegos activo supervisa los orígenes de la información de la VM.
- En una configuración activa/activa, solo el cortafuegos principal supervisa los orígenes de la información de la VM.

Complemento de Panorama: en un dispositivo virtual o dispositivo de hardware Panorama que ejecute la versión 8.1.3, puede instalar el complemento para Microsoft Azure y AWS. El complemento le permite conectar Panorama con sus suscripciones a la nube pública de Azure o los VPC de AWS y recuperar la asignación de direcciones IP a etiquetas para sus máquinas virtuales. Panorama registra la información de la VM en los cortafuegos gestionados de Palo Alto Networks® que configuró para las notificaciones.

Utilice las siguientes secciones para revisar las opciones admitidas en cada proveedor de nube y los atributos de la máquina virtual que puede supervisar para crear grupos de direcciones dinámicas:

- VMware ESXi
- Amazon Web Services (AWS)
- Microsoft Azure
- Google

© 2020 Palo Alto Networks, Inc.

VMware ESXi

Las VM de servidores ESXi o vCenter supervisados deben tener las herramientas de VMware instaladas y en ejecución. Las herramientas de VMware dan la posibilidad de deducir las direcciones IP y otros valores asignados a cada VM.

Cuando supervisa los hosts ESXi que son parte de la solución serie VM edición NSX, utilice los grupos de direcciones dinámicas (en lugar de usar los orígenes de información de VM) para obtener información sobre los cambios en el entorno virtual. Para la solución VM-Series edición NSX, NSX Manager le brinda a Panorama la información sobre el grupo de seguridad de NSX al cual pertenece una dirección IP. La información de NSX Manager brinda el contexto completo para definir los criterios de coincidencia en un grupo de direcciones dinámicas porque usa el ID de perfil de servicio como un atributo distintivo y le permite aplicar políticas de forma adecuada cuando tiene direcciones IP superpuestas en los diferentes grupos de seguridad.

Se pueden registrar hasta 32 etiquetas (del servidor vCenter y NSX Manager) en una dirección IP.

Para recopilar valores asignados a las VM supervisadas, use los Orígenes de información de la VM del cortafuegos para supervisar el siguiente conjunto de atributos de ESXi predefinidos:

Atributos supervisados en un origen de VMware
UUID
Nombre
Sistema operativo invitado
Estado de máquina virtual: el estado de alimentación es apagado, encendido, en espera y desconocido.
Anotación
versión
Red: nombre del conmutador virtual, nombre del grupo de puerto e ID de VLAN
Nombre del contenedor: nombre de vCenter, nombre del objeto del centro de datos, nombre del grupo de recursos, nombre del clúster, host, dirección IP del host.

Amazon Web Services (AWS)

A medida que proporciona o modifica máquinas virtuales en su VPC de AWS, tiene dos maneras de supervisar estas instancias y recuperar las etiquetas para usarlas como criterio de coincidencia en grupos de direcciones dinámicas.

- **Fuente de información de la VM:** en un cortafuegos de última generación, puede supervisar hasta 32 etiquetas: 14 pares de clave-valor predefinidos y 18 pares de clave-valor definidos por el usuario (etiquetas). Los siguientes atributos (o nombres de etiquetas) están disponibles como criterios de coincidencias para grupos de direcciones dinámicas.
- **Plugin de AWS en Panorama**: el plugin de Panorama para AWS le permite conectar Panorama a su VPC de AWS y recuperar la asignación de dirección IP a etiqueta para sus máquinas virtuales de AWS. Panorama registra la información de la VM en los cortafuegos gestionados de Palo Alto Networks®

© 2020 Palo Alto Networks, Inc.

que configuró para las notificaciones. Con el complemento, Panorama puede recuperar un total de 32 etiquetas para cada máquina virtual, 11 etiquetas predefinidas y hasta 21 etiquetas definidas por el usuario.

Atributos supervisados en el AWS-VPC	Fuente de información de la VM en el cortafuegos	Complemento de AWS en Panorama
Arquitectura	yes (sí)	No
Sistema operativo invitado	yes (sí)	No
ID de AMI	yes (sí)	yes (sí)
Perfil de instancia IAM	No	yes (sí)
ID de instancia	yes (sí)	No
Estado de instancia	yes (sí)	No
Tipo de instancia	yes (sí)	No
Nombre de clave	yes (sí)	yes (sí)
ID de propietario	No	yes (sí)
Selección de ubicación: inquilino	yes (sí)	yes (sí)
Selección de ubicación: nombre de grupo	yes (sí)	yes (sí)
Selección de ubicación: zona de disponibilidad	yes (sí)	yes (sí)
Nombre DNS privado	yes (sí)	No
Nombre DNS público	yes (sí)	yes (sí)
ID de subred	yes (sí)	yes (sí)
ID de grupo de seguridad	No	yes (sí)
Nombre del grupo de seguridad	No	yes (sí)
ID de VPC	yes (sí)	yes (sí)
Etiqueta (clave, valor)	Yes;	Yes;

© 2020 Palo Alto Networks, Inc.

Atributos supervisados en el AWS-VPC	Fuente de información de la VM en el cortafuegos	Complemento de AWS en Panorama
	Se admiten hasta 18 etiquetas definidas por el usuario como máximo. Las etiquetas definidas por el usuario se ordenan alfabéticamente y las primeras 18 etiquetas están disponibles para usarlas en los cortafuegos.	Se admiten hasta 21 etiquetas definidas por el usuario como máximo. Las etiquetas definidas por el usuario se ordenan alfabéticamente y las primeras 21 etiquetas se pueden usar en Panorama y los cortafuegos.

Microsoft Azure

Para la monitorización de la VM en Azure existen dos maneras de recuperar la asignación de la etiqueta a la dirección IP para VM de Azure y que estén disponibles como criterios de coincidencia en los grupos de direcciones dinámicas. El plugin de Panorama para Microsoft Azure le permite conectar Panorama a sus suscripciones a la nube pública de Azure y recuperar la asignación de dirección IP a etiqueta para sus máquinas virtuales de Azure. Panorama puede recuperar un total de 26 etiquetas para cada máquina virtual, 11 etiquetas predefinidas y hasta 15 etiquetas definidas por el usuario, y registra la información de la VM en los cortafuegos gestionados de Palo Alto Networks® que ha configurado para la notificación.

Con el plugin de Panorama para Azure, puede supervisar el siguiente conjunto de atributos de máquina virtual en su implementación de Microsoft Azure.

Atributos supervisados en Microsoft Azure	Complemento de Azure en Panorama
Nombre de la VM	yes (sí)
Tamaño de la VM	No
Nombre de grupo de seguridad de red	yes (sí)
Tipo de sistema operativo	yes (sí)
Editor del sistema operativo	yes (sí)
Oferta de sistema operativo	yes (sí)
SKU del sistema operativo	yes (sí)
Subred	yes (sí)
VNet	yes (sí)
Región de Azure	yes (sí)
Nombre del grupo de recursos	yes (sí)
ID de suscripción	yes (sí)
Etiquetas definidas por el usuario	yes (sí) Se admiten hasta 15 etiquetas definidas por el usuario como máximo. Las

© 2020 Palo Alto Networks, Inc.

Atributos supervisados en Microsoft Azure	Complemento de Azure en Panorama
	etiquetas definidas por el usuario se clasifican alfabéticamente. Las primeras 15 etiquetas están disponibles para su uso en Panorama y los cortafuegos.

Google

Con Orígenes de información de la VM en el cortafuegos de próxima generación, puede supervisar los siguientes conjuntos predefinidos de atributos de Google Compute Engine (GCE).



La alta disponibilidad no es compatible con los cortafuegos.

Atributos supervisados en Google Compute Engine (GCE)
Hostname of the VM (Nombre de host de VM)
Machine type (Tipo de máquina)
Project ID (ID de proyecto)
Source (Origen) (tipo de SO)
estado
Subnetwork (Subred)
VPC Network (Red de VPC)

Uso de grupos de direcciones dinámicas en políticas

En las políticas se usan grupos de direcciones dinámicas. Estos permiten crear políticas que se adaptan a los cambios automáticamente, añadiendo, moviendo o eliminando servidores. También permite aplicar diferentes reglas al mismo servidor en función de las *etiquetas* que definen su función en la red, el sistema operativo o los diferentes tipos de tráfico que procesa.

Un grupo de direcciones dinámicas usa etiquetas como criterios de filtrado para determinar a sus miembros. El filtro usa los operadores lógicos *y* y *o*. Todas las direcciones o grupos de direcciones IP que coincidan con los criterios de filtrado se hacen miembros del grupo de direcciones dinámicas. Las etiquetas se pueden definir estáticamente en el cortafuegos o registrarse (dinámicamente) en el cortafuegos. La diferencia entre etiquetas estáticas y las dinámicas es que las etiquetas estáticas forman parte de la configuración del cortafuegos y las dinámicas forman parte de la configuración del tiempo de ejecución. Esto significa que no se requiere una confirmación para actualizar etiquetas dinámicas; no obstante, las etiquetas deben ser usadas por grupos de direcciones dinámicas a las que se haga referencia en la política, y la política debe estar confirmada en el cortafuegos.

Para registrar etiquetas dinámicamente, puede usar la API XML o el agente de supervisión VM en el cortafuegos o usar el agente User-ID. Cada etiqueta es un elemento de metadatos o par de atributo y valor registrado en el cortafuegos o Panorama. Por ejemplo, IP1 {tag1, tag2,.....tag32}, donde la dirección IP y

© 2020 Palo Alto Networks, Inc.

las etiquetas asociadas se mantienen como una lista; cada dirección IP registrada puede tener hasta 32 etiquetas como el sistema operativo, el centro de datos o el conmutador virtual al que pertenece. Tras recibir la llamada a la API, el cortafuegos registra tanto la dirección IP como las etiquetas asociadas y actualiza automáticamente la información de pertenencia a los grupos de direcciones dinámicas.

El número máximo de direcciones IP que se puede registrar para cada modelo es diferente. Use la siguiente tabla para conocer la información específica de su modelo:

Modelo	Número máximo de direcciones IP registradas dinámicamente
Dispositivos virtuales M-Series o Panorama	500 000
PA-5200 Series o VM-7000 SMC-B Series	500 000
VM-500, VM-700	300 000
PA-3200 Series o VM-300	200 000
PA-7000 Series	100 000
PA-850, VM-100	2.500
PA-820, PA-220 o VM-50	1000

Un conjunto de IP, como un intervalo de IP o una subred, se considera una única dirección IP registrada cuando se cuenta para el número máximo de direcciones IP registradas admitidas por cada modelo de cortafuegos.

El siguiente ejemplo muestra cómo los grupos de direcciones dinámicas pueden simplificar la aplicación forzada de seguridad de la red. El flujo de trabajo de ejemplo muestra cómo:

- Habilitar el agente de supervisión VM en el cortafuegos para supervisar el host VMware ESX(i) o el servidor vCenter y registrar las direcciones IP de la VM y las etiquetas asociadas.
- Crear grupos de direcciones dinámicas y definir etiquetas para el filtro. En este ejemplo se han creado dos grupos de direcciones. Uno que solo filtra por etiquetas dinámicas y otro que filtra por etiquetas tanto estáticas como dinámicas para añadir los miembros del grupo.
- Comprobar que los miembros del grupo de direcciones dinámicas se han añadido al cortafuegos.
- Usar grupos de direcciones dinámicas en la política. Este ejemplo usa dos políticas de seguridad diferentes:
  - Una política de seguridad para todos los servidores Linux que se implementan como servidores FTP; esta regla busca coincidencias con las etiquetas registradas dinámicamente.
  - Una política de seguridad para todos los servidores Linux que se implementan como servidores; esta regla busca coincidencias con el grupo de direcciones dinámicas que usa etiquetas estáticas y dinámicas.
- Comprobar que los miembros de los grupos de direcciones dinámicas están actualizados como nuevos servidores FTP o que se implementan servidores web. De este modo se garantiza que se fuercen las reglas de seguridad también en estas nuevas máquinas virtuales.

STEP 1 | Habilite la supervisión de orígenes VM.

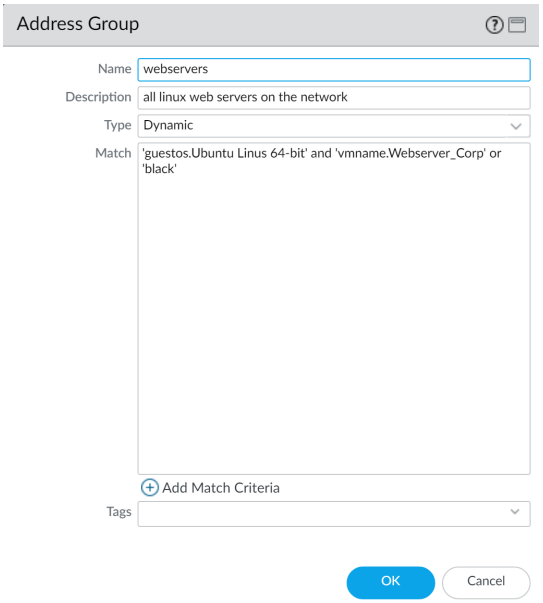
© 2020 Palo Alto Networks, Inc.

Consulte Habilitación de la supervisión de VM para el registro de cambios en la red virtual.

STEP 2 | Cree grupos de direcciones dinámicas en el cortafuegos.

Vea el tutorial para obtener información detallada de la función.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Object (Objeto)** > **Address Groups (Grupos de direcciones)**.
3. Haga clic en **Add (Añadir)** e introduzca un **Name (Nombre)** y una **Description (Descripción)** para el grupo de direcciones.
4. Defina el **Type (Tipo)** como **Dynamic (Dinámico)**.
5. Defina los criterios de coincidencia. Puede seleccionar etiquetas dinámicas y estáticas como los criterios de coincidencia para añadir miembros del grupo. Haga clic en **Add Match Criteria (Añadir criterios de coincidencia)** y seleccione el operador **And (Y)** u **Or (O)** ; seleccione además los atributos por los que le gustaría filtrar o buscar coincidencias y haga clic en **OK (ACEPTAR)**.

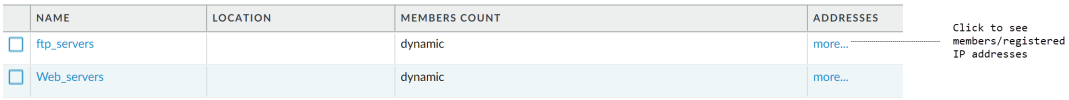


6. Haga clic en **Commit (Confirmar)**.

STEP 3 | Los criterios de coincidencia para cada grupo de direcciones dinámicas en este ejemplo son los siguientes:

ftp_server: coincidencias en el sistema operativo invitado “Linux 64-bit” y anotado como “ftp” ('guestos.Ubuntu Linux 64-bit' y 'annotation.ftp').

web-servers: coincidencias en dos criterios: la etiqueta negra o si el sistema operativo invitado es Linux 64 bits y el nombre del servidor es Web_server_Corp. ('guestos.Ubuntu Linux 64-bit' and 'vmname.WebServer_Corp' or 'black')



STEP 4 | Usar grupos de direcciones dinámicas en la política.

© 2020 Palo Alto Networks, Inc.

Consulte el tutorial.

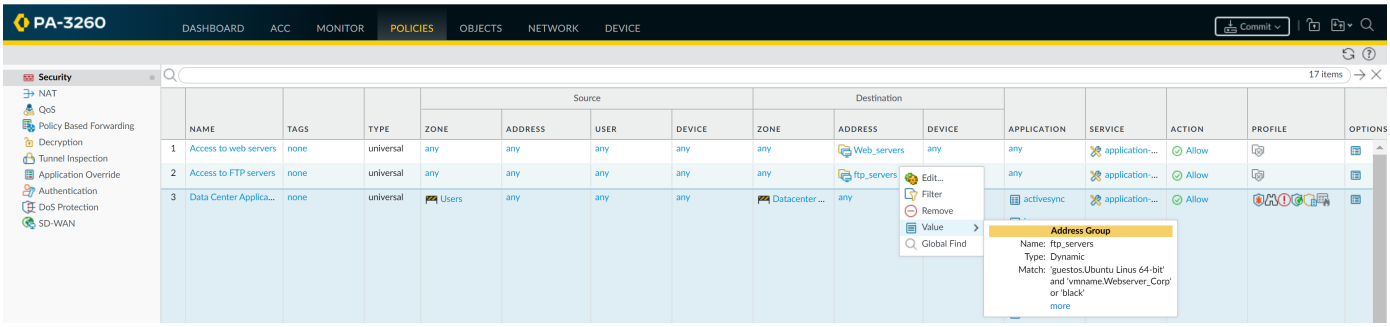
1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. Haga clic en **Add (Añadir)** y escriba un **Name (Nombre)** y una **Description (Descripción)** para la política.
3. Añada la **Source Zone (Zona de origen)** para especificar la zona desde la que se origina el tráfico.
4. Añada la **Destination Zone (Zona de destino)** donde finaliza el tráfico.
5. Para la **Destination Address (Dirección de destino)**, seleccione el grupo de direcciones dinámicas que ha creado anteriormente.
6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, de manera opcional, incluya los perfiles de políticas de seguridad en la regla.
7. Repita los pasos del 1 al 6 para crear otra regla de política.
8. Haga clic en **Commit (Confirmar)**.

STEP 5 | Este ejemplo muestra cómo crear dos políticas: una para todo el acceso a los servidores FTP y otro para el acceso a los servidores web.

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTI
1	Access to web servers	none	universal	any	any	any	any	any	Web_servers	any	any	application-...	Allow		
2	Access to FTP servers	none	universal	any	any	any	any	any	ftp_servers	any	any	application-...	Allow		

STEP 6 | Comprobar que los miembros del grupo de direcciones dinámicas se han añadido al cortafuegos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla.
2. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Value (Valor)**. También puede comprobar si los criterios de coincidencia son precisos.



3. Haga clic en el vínculo **more (más)** y compruebe que se muestra la lista de direcciones IP registradas.

   La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

Si desea eliminar todas las direcciones IP registradas, use el comando de la CLI ***`debug object registered-ip clear all`*** *y luego reinicie el cortafuegos después de borrar las etiquetas.*

© 2020 Palo Alto Networks, Inc.

Comandos de la CLI para etiquetas y direcciones IP

La interfaz de línea de comandos del cortafuegos y Panorama le ofrecen una vista detallada de los diferentes orígenes desde los que se registran las etiquetas y direcciones IP dinámicamente. También le permite auditar las etiquetas registradas y no registradas. Los siguientes ejemplos ilustran las funcionalidades de la CLI.

Ejemplo	Comando de la CLI
Ver todas las direcciones IP registradas que coincidan con la etiqueta `state.poweredOn` o que no estén etiquetadas como `vSwitch0`.	**show log iptag tag_name equal state.poweredOn** **show log iptag tag_name not-equal switch.vSwitch0**
Ver todas las direcciones IP registradas dinámicamente con origen en Orígenes de información de VM con el nombre `vmware1` y etiquetadas como `poweredOn`.	**show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all** registered IP Tags ---------- ---------- fe80::20c:29ff:fe69:2f76 "state.poweredOn" 10.1.22.100 "state.poweredOn" 2001:1890:12f2:11:20c:29ff:fe69:2f76"state.poweredOn" fe80::20c:29ff:fe69:2f80 "state.poweredOn" 192.168.1.102 "state.poweredOn" 10.1.22.105 "state.poweredOn" 2001:1890:12f2:11:2cf8:77a9:5435:c0d"state.poweredOn" fe80::2cf8:77a9:5435:c0d "state.poweredOn"
Borrar todas las direcciones IP y etiquetas obtenidas desde un origen de supervisión de VM sin desconectar el origen	**debug vm-monitor clear source-name *<name>***
Mostrar direcciones IP registradas desde todos los orígenes	**show object registered-ip all**
Mostrar el recuento de direcciones IP registradas desde todos los orígenes	**show object registered-ip all option count**
Borrar direcciones IP registradas desde todos los orígenes	**debug object registered-ip clear all**
Añadir o eliminar etiquetas para una dirección IP dada que se ha registrado usando la API XML	**debug object registered-ip test [<register/unregister>] <ip/netmask><tag>**

© 2020 Palo Alto Networks, Inc.

Ejemplo	Comando de la CLI
Ver todas las etiquetas registradas desde un origen de información específico	**show vm-monitor source source-name vmware1 tag all** vlanId.4095 vswitch.vSwitch1 host-ip.10.1.5.22 portgroup.TOBEUSED hostname.panserver22 portgroup.VM Network 2 datacenter.ha-datacenter vlanId.0 state.poweredOn vswitch.vSwitch0 vmname.Ubuntu22-100 vmname.win2k8-22-105 resource-pool.Resources vswitch.vSwitch2 guestos.Ubuntu Linux 32-bit guestos.Microsoft Windows Server 2008 32-bit annotation. version.vmx-08 portgroup.VM Network vm-info-source.vmware1 uuid.564d362c-11cd-b27f-271f-c361604dfad7 uuid.564dd337-677a-eb8d-47db-293bd6692f76 Total: 22
Ver todas las etiquetas registradas desde un origen de datos específico, por ejemplo, desde el agente de supervisión de VM en el cortafuegos, la API XML, el agente de User-ID de Windows o la CLI.	• Para ver etiquetas registradas desde la CLI: **show log iptag datasource_type equal unknown** • Para ver etiquetas registradas desde la API XML: **show log iptag datasource_type equal xml-api** • Para ver etiquetas registradas desde orígenes de información de VM: **show log iptag datasource_type equal vm-monitor** • Para ver etiquetas registradas desde el agente User-ID de Windows: **show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent**

© 2020 Palo Alto Networks, Inc.

Ejemplo	Comando de la CLI
Ver todas las etiquetas registradas para una dirección IP específica (en todos orígenes).	`debug object registered-ip show tag-source ip ip_address tag all`

© 2020 Palo Alto Networks, Inc.

Cumplimiento de la política en endpoints y usuarios detrás de un dispositivo de subida

Si tiene un dispositivo de subida, como un servidor proxy explícito o un equilibrador de carga, implementados entre los usuarios en su red y el cortafuegos, el cortafuegos puede ver la dirección IP del dispositivo de subida como la dirección IP de origen en el tráfico HTTP/HTTPS que el proxy reenvía en lugar de la dirección IP del cliente que ha solicitado el contenido. En muchos casos, el dispositivo de subida añade un encabezado X-Forwarded-For (XFF) a las solicitudes de HTTP que incluyen la dirección IPv4 o IPv6 real del cliente que solicitó el contenido desde o hacia el que se origina la solicitud.

En esos casos, puede configurar el cortafuegos para extraer la dirección IP del campo XFF y asignarla a un usuario con User-ID o aplicar una política de seguridad basada en la dirección IP.

- **Use X-Forwarded-For Header in User-ID (Usar el encabezado X-Forwarded-For en User-ID)**: esto le permite aplicar una política basada en el usuario para permitir el acceso seguro a aplicaciones basadas en la web para sus usuarios detrás de un servidor proxy. Además, si el ID de usuario puede asignar la dirección IP XFF a un nombre de usuario, el cortafuegos muestra ese nombre de usuario como el usuario de origen de los logs de tráfico, amenazas, envíos de WildFire y filtrado de URL para garantizar la visibilidad de la actividad web de los usuarios detrás del proxy.
- **Use X-Forwarded-For Header in Security Policy (Usar el encabezado X-Forwarded-For en la política de seguridad)**: esto le permite hacer cumplir la política de seguridad según la dirección IP de origen mediante la dirección IP en el campo XFF del encabezado HTTP. Además, cuando se aplica una política al tráfico que incluye una dirección IP en el campo XFF, puede configurar los logs de tráfico, amenazas, filtrado de datos y envío de incendios forestales para ayudar en la resolución de problemas y la corrección.

Para garantizar que los atacantes no puedan leer ni aprovechar los valores XFF en paquetes de solicitud web que salen del cortafuegos para recuperar el contenido desde un servidor externo, también puede configurar el cortafuegos para quitar los valores XFF desde paquetes salientes. El uso de la dirección IP XFF para el User-ID o en la política y la eliminación del valor XFF no son mutuamente excluyentes: si configura ambos, el cortafuegos pone a cero los valores XFF solo después de usarlos en la aplicación de políticas y el log.



No puede configurar el cortafuegos para usar la dirección IP en el campo XFF en User-ID y política de seguridad al mismo tiempo.

- Uso de los valores XFF para usuarios de orígenes de logging y políticas
- Uso de valores de la dirección IP de XFF en la política de seguridad y logs
- Uso de la dirección IP en el encabezado de XFF para eventos de solución de problemas

Uso de valores XFF para políticas basadas en usuarios de origen

Puede configurar el cortafuegos para que asigne la dirección IP en el encabezado XFF a un nombre de usuario utilizando el ID de usuario, de modo que obtenga visibilidad y control de la política basada en el usuario en el tráfico web de los usuarios detrás de un servidor proxy que no se pueden identificar de otro modo. Para asignar direcciones IP de los encabezados XFF a nombres de usuario, primero debe realizar la Habilitación de ID de usuario.

Con esta opción habilitada, el cortafuegos utiliza la dirección IP en el encabezado XFF únicamente para la asignación de usuarios. La dirección IP de origen que guarda el cortafuegos es la del servidor proxy, no la del usuario de origen. Cuando observa un evento de log atribuido a un usuario que el cortafuegos asignó utilizando una dirección IP que se extrajo de un encabezado XFF, es posible que sea difícil realizar

© 2020 Palo Alto Networks, Inc.

el seguimiento del dispositivo específico asociado al evento. Para simplificar la depuración y la solución de problemas de los eventos atribuidos a usuarios detrás del servidor proxy, también debe configurar el cortafuegos para que rellene la columna X-Forwarded-For en el log de filtrado de URL con la dirección IP en el encabezado XFF, de modo que pueda realizar un seguimiento del usuario y el dispositivo específicos asociados a un evento de log correlacionado con la entrada del log de filtrado de URL.

El encabezado XFF que su servidor proxy añade debe contener la dirección IP de origen del usuario final que originó la solicitud. Si el encabezado contiene varias direcciones IP, el cortafuegos utiliza únicamente la primera dirección IP. Si el encabezado contiene información diferente a la dirección IP, el cortafuegos no podrá realizar la asignación de usuarios.

Permitir que el cortafuegos utilice los encabezados X-Forwarded-For para realizar la asignación de usuarios no habilita al cortafuegos para utilizar la dirección IP del cliente en el encabezado XFF como la dirección de origen en los logs; los logs aún muestran la dirección IP del servidor proxy como la dirección de origen. Sin embargo, para simplificar el proceso de depuración y solución de problemas, puede configurar el cortafuegos para la Adición de valores XFF a logs de filtrado de URL *a fin de mostrar la dirección IP de cliente del encabezado XFF en los logs de filtrado de URL.*

STEP 1 | Habilite el cortafuegos para que use los valores de XFF en las políticas y en los campos de usuario de origen de los logs.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)** y edite la configuración de X-Forwarded-For Headers.
2. Seleccione **Use X-Forwarded-For Header in User-ID (Utilizar el encabezado X-Forwarded-For en User-ID)**.

STEP 2 | Quite los valores XFF de las solicitudes web salientes.

1. Seleccione **Strip X-Forwarded-For Header (Quitar el encabezado X-Forwarded-For)**.
2. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

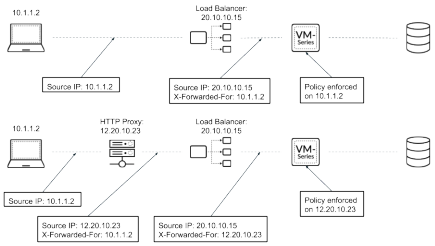
STEP 3 | Compruebe que el cortafuegos rellena los campos de logs del usuario de origen.

1. Seleccione un tipo de log que tenga un campo de usuario de origen (por ejemplo, **Monitor [Supervisar]** > **Logs [Logs]** > **Traffic [Tráfico]**).
2. Compruebe que la columna Usuario de origen muestra los nombres de usuario de los usuarios que acceden a las aplicaciones web.

Uso de valores de la dirección IP de XFF en la política de seguridad y logs

Puede configurar el cortafuegos para usar la dirección IP en el campo X-Forwarded-For (XFF) del encabezado HTTP para hacer cumplir la política de seguridad. Si el paquete pasa a través de un solo servidor proxy antes de llegar al cortafuegos, el campo XFF contiene la dirección IP del endpoint de origen y el cortafuegos puede usar esa dirección IP para hacer cumplir la política de seguridad. Sin embargo, si el paquete pasa a través de varios dispositivos de subida, el cortafuegos usa la dirección IP añadida más recientemente para hacer cumplir la política o usar otras funciones que dependen de la información IP.

© 2020 Palo Alto Networks, Inc.



- Uso de valores XFF en la política
- Visualización de valores XFF en logs
- Visualización de valores XFF en informes

Uso de valores XFF en la política

Complete el siguiente procedimiento para utilizar la dirección IP del cliente en el encabezado XFF al aplicar la política de seguridad.

En Microsoft Azure, de forma predeterminada, una puerta de enlace de aplicaciones inserta la dirección IP y el puerto de origen originales en el encabezado XFF. Para usar encabezados XFF en la política de su cortafuegos, debe configurar la puerta de enlace de la aplicación para omitir el puerto del encabezado XFF. Para obtener más información, consulte la Documentación de Azure*.*

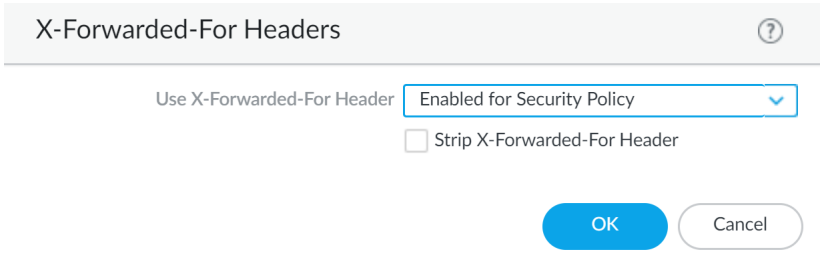
STEP 1 | Inicie sesión en el cortafuegos.

STEP 2 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **X-Forwarded-For Headers (Encabezados X-Forwarded-For)**.

STEP 3 | Haga clic en el icono de edición.

STEP 4 | Seleccione **Enabled for Security Policy (Habilitado para la política de seguridad)** en el menú desplegable **Use X-Forwarded-For Header (Usar encabezado Forwarded-For Header)**.

No puede habilitar Use X-Forwarded-For Header (Usar encabezado Forwarded-For Header) para la política de seguridad y el User-ID al mismo tiempo.



STEP 5 | (Opcional) Seleccione **Strip X-Forwarded-For Header (Quitar el encabezado X-Forwarded-For)**. Al seleccionar esta opción, se elimina el encabezado XFF antes de que el cortafuegos reenvíe la solicitud. Esta opción no deshabilita el uso de encabezados XFF; el cortafuegos utiliza el encabezado XFF para la aplicación de políticas y creación de logs.

STEP 6 | Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 7 | **Commit (Confirmar)** los cambios.

Visualización de valores XFF en logs

Además del uso del encabezado XFF en la política de seguridad, puede ver la dirección IP XFF en varios logs, informes y el Centro de control de aplicaciones (ACC, Application Command Center) para ayudar en la supervisión y la resolución de problemas. Puede añadir la columna X-Forwarded-For en los logs de tráfico, amenazas, filtrado de datos y envíos de Wildfire.

Para ver la dirección IP XFF en sus logs, complete los siguientes pasos.

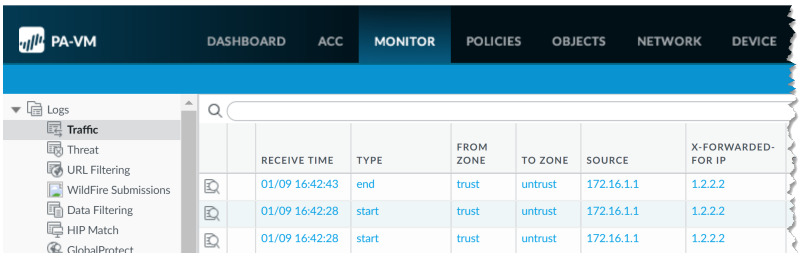
STEP 1 | Inicie sesión en el cortafuegos.

STEP 2 | Seleccione **Monitoring (Supervisión)** > **Logs**.

STEP 3 | Seleccione **Traffic (Tráfico)**, **Threat (Amenaza)**, **Data Filtering (Filtrado de datos)** o **WildFire Submissions (Envíos de WildFire)**.

STEP 4 | Haga clic en la flecha a la derecha de cualquier encabezado de columna y seleccione **Columns (Columnas)**.

STEP 5 | Seleccione **X-Forwarded-For IP (IP X-Forwarded-For)** para mostrar la IP XFF en su log.



Visualización de valores XFF en informes

Los informes predefinidos que genera el cortafuegos no contienen valores XFF. Para ver las direcciones IP XFF en los informes, el cortafuegos incluye plantillas de informes integradas que incorporan información XFF.

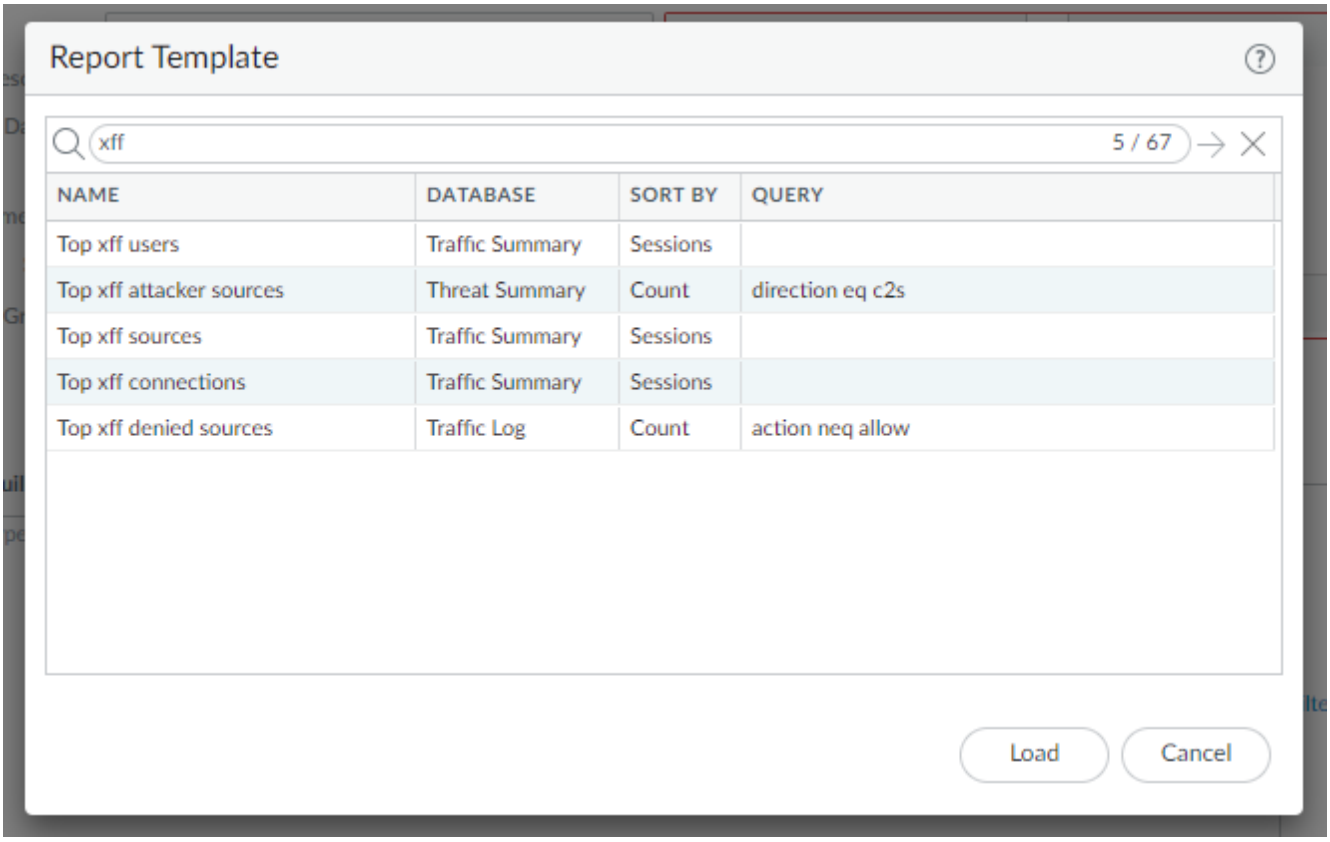
STEP 1 | Inicie sesión en el cortafuegos.

STEP 2 | Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** > **Add (Añadir)**.

STEP 3 | Haga clic en **Load Template (Cargar plantilla)**.

STEP 4 | Especifique XFF en la barra de búsqueda y haga clic en el botón de búsqueda para ubicar las plantillas de informes XFF integradas.

© 2020 Palo Alto Networks, Inc.



STEP 5 | Haga clic en **Load (Cargar)**.

STEP 6 | Utilice las opciones Configure your custom report (Configurar informe personalizado) **Time Frame (Período)**, **Sort By (Ordenar por)** y **Group By (Agrupar)** para ver la información XFF de la forma que más se adapte a sus necesidades.

STEP 7 | (Opcional) Haga clic en **Run Now (Ejecutar ahora)** para generar su informe a petición en lugar de en una **hora programada**, o además de ella.

Uso de la dirección IP en el encabezado de XFF para eventos de solución de problemas

De manera predeterminada, el cortafuegos no crea logs de la dirección de origen de un cliente detrás de un servidor proxy, incluso si utiliza esta dirección desde un encabezado de X-Forwarded-For (XFF) para la asignación de usuarios. Por lo tanto, a pesar de que puede identificar el usuario específico asociado al evento de log, no podrá identificar con facilidad el dispositivo de origen que originó el evento de log. Para simplificar la depuración y la solución de problemas de los eventos de usuarios detrás del servidor proxy, debe habilitar la opción X-Forwarded-For dentro de la creación de encabezados HTTP en el perfil de filtrado de URL que adjunta a las reglas de la política de seguridad que permite el acceso a aplicaciones basadas en la web. Con esta opción habilitada, el cortafuegos crea logs de la dirección IP desde el encabezado de XFF como la dirección de origen para todo el tráfico que coincide con la regla.

Habilitar el cortafuegos para utilizar un encabezado XFF como la dirección de origen en los logs de filtrado de URL no habilita la asignación de usuarios en la dirección de origen. Para

© 2020 Palo Alto Networks, Inc.

rellenar los campos de usuario de origen, consulte Uso de los valores XFF en las políticas y en el registro de usuarios de origen.

STEP 1 | Habilite la opción X-Forwarded-For en HTTP Header Logging (Registro de encabezado HTTP) en el perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y seleccione el perfil de filtrado de URL que desee configurar o añada uno nuevo.

   No puede habilitar el logging XFF en el perfil de filtrado de URL.

2. Seleccione la pestaña **Settings (Configuración)** y seleccione **X-Forwarded-For**.
3. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 2 | Adjunte el perfil de filtrado de URL a las reglas de la política de seguridad que permiten el acceso a las aplicaciones web.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la regla.
2. Seleccione la pestaña **Actions (Acciones)**, establezca el **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione el perfil de **URL Filtering (Filtrado de URL)** que acaba de configurar para el registro de encabezado HTTP.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 3 | Compruebe que el cortafuegos está haciendo el logging de los valores XFF.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**.
2. Vea los valores XFF de uno de las siguientes maneras:

   - Para mostrar el valor XFF en un único log de filtrado de URL, haga clic en el icono de lupa para que el log muestre los detalles. La sección Encabezados HTTP muestra el valor de X-Forwarded-For.
   - Para mostrar los valores XFF de todos los logs de filtrado de URL: abra la lista desplegable en cualquier encabezado de columna, seleccione **Columns (Columnas)** y seleccione **X-Forwarded-For**. La sección Encabezados HTTP mostrará una columna X-Forwarded-For.

STEP 4 | Utilice el campo XFF en el log de filtrado de URL para solucionar problemas de un evento de log en otro tipo de log.

A pesar de que únicamente los logs de filtrado de URL muestran la dirección IP del usuario de origen en la columna X-Forwarded-For de los logs, si observa un evento asociado a tráfico HTTP/HTTPS, pero no puede identificar la dirección IP de origen debido a que es la de un servidor proxy, puede utilizar el valor de X-Forwarded-For en un log de filtrado de URL correlacionado para identificar la dirección de origen asociada al evento del log. Para hacerlo:

1. Busque un evento que desea investigar en un log de tráfico, amenazas o envíos de WildFire que muestre la dirección IP del servidor proxy como la dirección de origen.
2. Haga clic en el icono de lupa para acceder a los detalles del log y buscar el log de filtrado de URL asociado en la parte inferior de la ventana del visor de logs detallados.
3. Seleccione la fila del encabezado y seleccione **X-Forwarded-For** en el menú desplegable **Columns (Columnas)** para mostrar este valor. La dirección IP en la columna X-Forwarded-For representa la dirección IP del usuario de origen detrás del servidor proxy. Utilice esta dirección IP para realizar el seguimiento del dispositivo que activó el evento que investiga.

© 2020 Palo Alto Networks, Inc.

Reenvío basado en políticas

Normalmente, el cortafuegos usa la dirección IP de destino en un paquete para determinar la interfaz de salida. El cortafuegos usa la tabla de enrutamiento asociada al enrutador virtual al que la interfaz está conectada para realizar la búsqueda de rutas. El reenvío basado en políticas (PBF) le permite anular la tabla de enrutamiento y especificar la interfaz saliente o *de salida* basándose en parámetros específicos como la dirección IP de origen o destino o el tipo de tráfico.

- PBF
- Creación de una regla de reenvío basada en políticas
- Caso de uso: PBF para acceso saliente con ISP duales

PBF

Las reglas PBF permiten al tráfico tomar una ruta alternativa desde el siguiente salto especificado en la tabla de enrutamiento, y se suelen usar para especificar una interfaz de salida por razones de seguridad o rendimiento. Imaginemos que su empresa tiene dos enlaces entre la oficina corporativa y la sucursal: un enlace de internet de bajo coste y una línea alquilada de mayor coste. La línea alquilada es un enlace de gran ancho de banda y baja latencia. Para una mayor seguridad, puede utilizar la PBF para enviar aplicaciones que no son de tráfico cifrado, como el tráfico FTP, a través de la línea de alquiler privada y el resto del tráfico a través del enlace de internet. O bien, si se da prioridad al rendimiento, puede elegir enrutar las aplicaciones críticas para la empresa a través de la línea alquilada y enviar el resto del tráfico, como la navegación web, a través del enlace de bajo coste.

- Ruta de salida y retorno simétrico
- Supervisión de rutas para PBF
- Servicio frente a aplicaciones en PBF

Ruta de salida y retorno simétrico

Mediante PBF, puede dirigir el tráfico a una interfaz específica en el cortafuegos, descartar el tráfico o dirigirlo a otro sistema virtual (en sistemas habilitados para múltiples sistemas virtuales).

En las redes con rutas asimétricas, como un entorno de proveedor de servicios de Internet (ISP) dual, los problemas de productividad se producen cuando el tráfico llega a una interfaz en el cortafuegos y sale desde otra interfaz. Si la ruta es asimétrica, en la que los paquetes de salida (paquetes SYN) y de retorno (SYN/ACK) son diferentes, el cortafuegos no puede seguir el estado del tráfico de toda la sesión, y esto ocasiona un fallo de conexión. Para garantizar que el tráfico usa una ruta simétrica, lo que significa que el tráfico llega y sale desde la misma interfaz en la que se creó la sesión, puede habilitar la opción *Symmetric Return (Retorno simétrico)*.

Con el retorno simétrico, el enrutador virtual anula una búsqueda de rutas para el tráfico de retorno y en su lugar dirige el flujo de vuelta a la dirección MAC desde la que recibió el paquete SYN (o primer paquete). Sin embargo, si la dirección IP de destino está en la misma subred que la dirección IP de las interfaces de entrada/salida, se realiza una búsqueda de rutas y no se fuerza el retorno simétrico. Este comportamiento evita que el tráfico se descarte de forma silenciosa.



Para determinar el siguiente salto para retornos simétricos, el cortafuegos usa una tabla de protocolo de resolución de direcciones (ARP). El número máximo de entradas que admite esta tabla ARP está limitado por el modelo de cortafuegos, y el usuario no puede configurar el valor. Para conocer el límite de su modelo, use el comando de la CLI: ***`show pbf return-mac all`***.

© 2020 Palo Alto Networks, Inc.

Supervisión de rutas para PBF

La supervisión de rutas le permite verificar la conectividad a una dirección IP, de modo que el cortafuegos pueda dirigir el tráfico a través de una ruta alternativa en caso necesario. El cortafuegos usa pings ICMP como *latidos* para comprobar que se puede alcanzar la dirección IP especificada.

Un perfil de supervisión permite especificar el número de latidos (umbral) para determinar si se puede alcanzar la dirección IP. Si no se puede alcanzar la dirección IP supervisada, puede deshabilitar la regla PBF o especificar una acción de *conmutación por error* o *esperar recuperación*. Deshabilitar la regla PBF permite al enrutador virtual tomar el control de las decisiones de enrutamiento. Cuando se realiza la acción de conmutación por error o esperar recuperación, el perfil de supervisión sigue supervisando si la dirección IP de destino puede alcanzarse y, cuando vuelve a estar disponible, el cortafuegos vuelve a usar la ruta original.

La siguiente tabla enumera las diferencias de comportamiento ante un fallo de supervisión de ruta en una nueva sesión frente a una sesión establecida.

Comportamiento de una sesión en un fallo de supervisión	Si la regla permanece habilitada cuando no se alcanza la dirección IP	Si la regla está deshabilitada cuando no se alcanza la dirección IP
Para una sesión establecida	**wait-recover (esperar recuperación)**: continúa usando la interfaz de salida especificada en la regla PBF	**wait-recover (esperar recuperación)**: continúa usando la interfaz de salida especificada en la regla PBF
	conmutación por error: Usa la ruta determinada por la tabla de enrutamiento (no PBF)	**conmutación por error**: Usa la ruta determinada por la tabla de enrutamiento (no PBF)
Para una sesión nueva	**wait-recover (esperar recuperación)**: usa la ruta determinada por la tabla de enrutamiento (no PBF)	**esperar recuperación**: Comprueba las reglas PBF restantes. Si no hay coincidencia, usa la tabla de enrutamiento
	conmutación por error: Usa la ruta determinada por la tabla de enrutamiento (no PBF)	**conmutación por error**: Comprueba las reglas PBF restantes. Si no hay coincidencia, usa la tabla de enrutamiento

Servicio frente a aplicaciones en PBF

Las reglas PBF se aplican tanto al primer paquete (SYN) o a la respuesta al primer paquete (SYN/ACK). Esto significa que se puede aplicar una regla PBF antes de que el cortafuegos tenga suficiente información para determinar la aplicación. Por lo tanto, no se recomienda usar las reglas específicas de aplicación con PBF. Cuando sea posible, use un objeto de servicio, que es el puerto de capa 4 (TCP o UDP) usado por el protocolo o la aplicación.

Sin embargo, si especifica una aplicación en una regla PBF, el cortafuegos realiza un *almacenamiento en caché de App-ID*. Cuando una aplicación atraviesa un cortafuegos por primera vez, el cortafuegos no tiene suficiente información para identificarla y, por tanto, no puede forzar la regla PBF. Conforme van llegando más paquetes, el cortafuegos determina la aplicación y crea una entrada en la caché de App-ID y retiene este App-ID durante la sesión. Cuando se crea una nueva sesión con la misma IP de destino, el puerto de destino, el ID de protocolo y el cortafuegos pueden identificar la aplicación como la misma de la sesión inicial (basada en la caché de App-ID) y aplicar la regla PBF. Por lo tanto, una sesión que no es una coincidencia exacta y no es la misma aplicación puede reenviarse basándose en la regla PBF.

© 2020 Palo Alto Networks, Inc.

Más aún, las aplicaciones tienen dependencias y la identidad de la aplicación puede cambiar a medida que el cortafuegos va recibiendo más paquetes. Puesto que PBF toma una decisión de ruta al inicio de la sesión, el cortafuegos no puede forzar un cambio en la identidad de la aplicación. YouTube, por ejemplo, comienza como navegación web pero cambia a Flash, RTSP o YouTube en función de los diferentes enlaces y vídeos incluidos en la página. No obstante, con PBF, dado que el cortafuegos identifica la aplicación como navegación web al inicio de la sesión, el cambio de la aplicación no se reconoce a partir de ese momento.

No puede utilizar aplicaciones personalizadas, filtros de aplicaciones o grupos de aplicaciones en las reglas PBF.

Creación de una regla de reenvío basada en políticas

Use una regla PBF para dirigir el tráfico a una interfaz de salida específica en el cortafuegos y anule la ruta predeterminada para el tráfico.

STEP 1 | Cree una regla de reenvío basado en políticas (Policy-Based Forwarding, PBF).

Al crear una regla de PBF, debe especificar un nombre, una interfaz o zona de origen y una interfaz de salida. El resto de componentes son opcionales o tienen un valor predeterminado.

Puede especificar las direcciones de origen y destino con una dirección IP, un objeto de dirección o un FQDN.

1. Seleccione **Policies (Políticas)** > **Policy Based Forwarding (Reenvío basado en políticas)** y **añada** una regla de políticas PBF.
2. Asigne un nombre descriptivo a la regla (**General**).
3. Seleccione **Source (Origen)** y configure lo siguiente:
   1. Seleccione el **tipo** (**Zone (Zona)** o **Interface (Interfaz)**) en el que aplicar la política de reenvío y especifique la interfaz o zona relevantes. Si desea aplicar el retorno simétrico, debe seleccionar una interfaz de origen.

      Solo admiten PBF las interfaces de capa 3, pero las interfaces de bucle invertido no.
   2. (Opcional) En **Source Addres (Dirección de origen)**, especifique la dirección a la que se debe aplicar la regla de PBF. Por ejemplo, una dirección IP específica o dirección IP de subred desde la que quiere reenviar el tráfico a la zona o interfaz especificada en esta regla.

      Haga clic en Negate (Negar) para excluir direcciones de origen de la regla de PBF. Por ejemplo, si la regla PBF dirige todo el tráfico desde la zona especificada a Internet, Negate (Negar) le permite excluir las direcciones IP internas de la regla PBF.

      El orden de evaluación es de arriba abajo. Los paquetes se cotejan con la primera regla que cumple los criterios definidos; cuando se encuentra una coincidencia, no se evalúan más reglas.
   3. (Opcional) Haga clic en **Add (Añadir)** y seleccione el **Source User (Usuario de origen)** o los grupos de usuarios a los que se aplican las políticas.
4. Seleccione **Destination/Application/Service (Destino/Aplicación/Servicio)** y configure lo siguiente:
   1. **Destination Address (Dirección de destino)**: de forma predeterminada, la regla se aplica a **cualquier** dirección IP. Haga clic en **Negate (Negar)** para excluir direcciones IP de destino de la regla de PBF.
   2. **Añada** cualquier **aplicación** y **servicio** que quiera controlar mediante PBF.

© 2020 Palo Alto Networks, Inc.

No es conveniente usar reglas específicas de aplicaciones con PBF porque es posible que las reglas de PBF se apliquen antes de que el cortafuegos tenga información suficiente para determinar la aplicación concreta. Cuando sea posible, use un objeto de servicio, que es el puerto de capa 4 (TCP o UDP) usado por el protocolo o la aplicación. Si desea información más detallada, consulte Servicio frente a aplicaciones en PBF*.*

STEP 2 | Especifique cómo se deben reenviar los paquetes que coinciden con la regla.

Si está configurando PBF en un entorno multi-VSYS, debe crear reglas PBF separadas para cada sistema virtual (y crear las reglas de política de seguridad apropiadas para habilitar el tráfico).

1. Seleccione **Forwarding (Reenvío)**.
2. Establezca la **acción** que tomar con los paquetes coincidentes:
   - **Forward (Reenviar)**: dirige el paquete a la interfaz especificada en **Egress Interface (Interfaz de salida)**.
   - **Forward to VSYS (Reenviar a vsys)** (en cortafuegos habilitados para varios sistemas virtuales): seleccione el sistema virtual al que se debe reenviar el paquete.
   - **Discard (Descartar)**: descarta el paquete.
   - **No PBF (Sin PBF)**: excluye los paquetes que coinciden con los criterios de origen, destino, aplicación o servicio definidos en la regla. Los paquetes coincidentes usan la tabla de enrutamiento en lugar de PBF; el cortafuegos usa la tabla de enrutamiento para excluir el tráfico coincidente del puerto redirigido.
3. Para activar la acción especificada una sola vez o con una frecuencia diaria o semanal, cree y añada una programación en **Schedule (Programar)**.
4. En **Next Hop (Próximo salto)**, seleccione una de las siguientes opciones:
   - **IP Address (Dirección IP)**: introduzca la dirección IP a la que el cortafuegos reenvía los paquetes coincidentes o bien seleccione un objeto de dirección del tipo IP Netmask (Máscara de red IP). Un objeto de dirección IPv4 debe tener una máscara de red /32 y un objeto de dirección IPv6 debe tener una máscara de red /128.
   - **FQDN**: introduzca el FQDN al que el cortafuegos reenvía los paquetes coincidentes o bien seleccione o cree un objeto de dirección del tipo FQDN. El FQDN se puede resolver en una dirección IPv4, una dirección IPv6 o ambas. Si el FQDN se resuelve en ambas, la regla de PBF tiene dos saltos después: uno para la dirección IPv4 y otro para la dirección IPv6. Puede usar la misma regla de PBF para el tráfico IPv4 y IPv6. El tráfico IPv4 se reenvía al siguiente salto para IPv4 y el tráfico IPv6, al siguiente salto para IPv6.

     Este FQDN se debe resolver en una dirección IP que pertenezca a la misma subred que la interfaz configurada para PBF; de lo contrario, el cortafuegos rechaza la resolución y el FQDN se queda sin resolver.

     El cortafuegos solo emplea una dirección IP (de cada tipo de familia, esto es, IPv4 o IPv6) de la resolución de DNS del FQDN. Si se devuelven varias direcciones, el cortafuegos utiliza la dirección IP preferida que coincida con el tipo de familia de IP (IPv4 o IPv6) configurado para el siguiente salto. La dirección IP preferida es la primera dirección que devuelve el servidor DNS en su respuesta inicial. El cortafuegos la mantiene como preferida mientras siga apareciendo en las respuestas posteriores, aunque el orden sea distinto.
   - **None (Ninguno)**: significa que se usa la dirección IP de destino del paquete como siguiente salto. El reenvío falla si la dirección IP de destino no está en la misma subred que la interfaz de salida.

© 2020 Palo Alto Networks, Inc.

5. (Opcional) Habilite la supervisión para verificar la conectividad a una dirección IP de destino o, si no se especifica ninguna, a la dirección IP de **Next Hop (Siguiente salto)**. Seleccione **Monitor (Supervisión)** y, en **Profile (Perfil)**, vincule el perfil de supervisión predeterminado o personalizado que especifica la acción adecuada cuando no se puede acceder a la dirección supervisada.
   - Puede **deshabilitar esta regla si no se puede acceder al siguiente salto o la IP de supervisión**.
   - En **IP Address (Dirección IP)**, introduzca la dirección de destino que se debe supervisar.

   En **Egress Interface (Interfaz de salida)** puede haber tanto direcciones IPv4 como direcciones IPv6, y el FQDN de **siguiente salto** se puede resolver en cualquiera de las dos. En este caso:

   1. Si la interfaz de salida tiene direcciones tanto IPv4 como IPv6, pero el FQDN del siguiente salto solo se resuelve en uno solo de esos tipos, el cortafuegos supervisa las direcciones IP resueltas. Si el FQDN se resuelve en ambas direcciones (IPv4 e IPv6), pero la interfaz de salida solo tiene un tipo, el cortafuegos supervisa la dirección de siguiente salto resuelta que coincide con la familia de direcciones de dicha interfaz.
   2. Si tanto la interfaz de salida como el FQDN de siguiente salto tienen direcciones IPv4 y IPv6, el cortafuegos supervisa la dirección IPv4 de siguiente salto.
   3. Si la interfaz de salida tiene una dirección de una familia y el FQDN de siguiente salto se resuelve en una dirección de la otra familia, el cortafuegos no supervisa nada.
6. (Obligatorio en entornos de enrutamiento asimétrico; opcional en los demás casos) **Aplique el retorno simétrico** y haga clic en **Add (Añadir)** para añadir direcciones IP en la **lista de direcciones de siguiente salto**. Puede añadir hasta 8 direcciones IP de próximo salto; las interfaces PPoE y de túnel no están disponibles como direcciones IP de próximo salto.

   Al habilitar el retorno simétrico se garantiza que el tráfico de retorno (por ejemplo, desde la zona fiable en la LAN hacia Internet) se reenvíe a través de la misma interfaz por la que el tráfico entra desde Internet.

STEP 3 | **Commit (Confirmar)** los cambios. La regla PBF está en vigor.

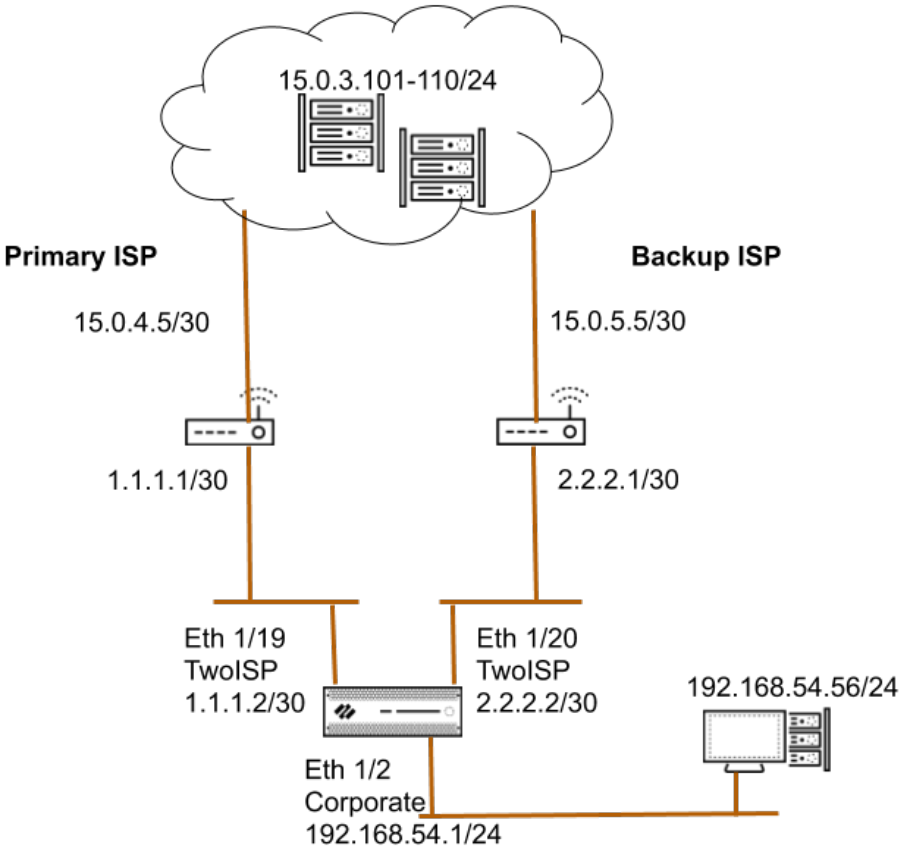
	Source			Destination			Forwarding			Monitoring	
NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	DISABLE IF UNREACHABLE
pdf2	ethernet1/3	any	any	HQ-subnet	service-http	forward	ethernet1/1.100	192.168.100.2	false	none	false

Caso de uso: PBF para acceso saliente con ISP duales

En este caso de uso, la sucursal tiene una configuración de ISP dual e implementa PBF para el acceso redundante a internet. El ISP de reserva es la ruta predeterminada para el tráfico desde el cliente a los servidores web. Para habilitar el acceso redundante a internet sin usar un protocolo de Internet como BGP, usamos PBF con NAT de origen basada en interfaz de destino y rutas estáticas, y configuramos el cortafuegos de la siguiente manera:

- Habilite una regla PBF que enrute el tráfico a través del ISP principal y añada un perfil de supervisión a la regla. El perfil de supervisión activa el cortafuegos para que use la ruta predeterminada a través de un ISP de reserva cuando el principal no está disponible.
- Defina las reglas NAT de origen tanto para el ISP principal como el de reserva que indican al cortafuegos que use la dirección IP de origen asociada con la interfaz de salida para el ISP correspondiente. De este modo se garantiza que el tráfico saliente tiene la dirección IP de salida correcta.
- Añada una ruta estática al ISP de reserva, de modo que cuando el ISP principal no esté disponible, entre en vigor la ruta predeterminada y el tráfico se dirija a través del ISP de reserva.

© 2020 Palo Alto Networks, Inc.



STEP 1 | Configurar las interfaces de entrada y salida en el cortafuegos

Las interfaces de salida pueden estar en la misma zona.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz que desea configurar.

   La configuración de la interfaz del cortafuegos usada en este ejemplo es la siguiente:

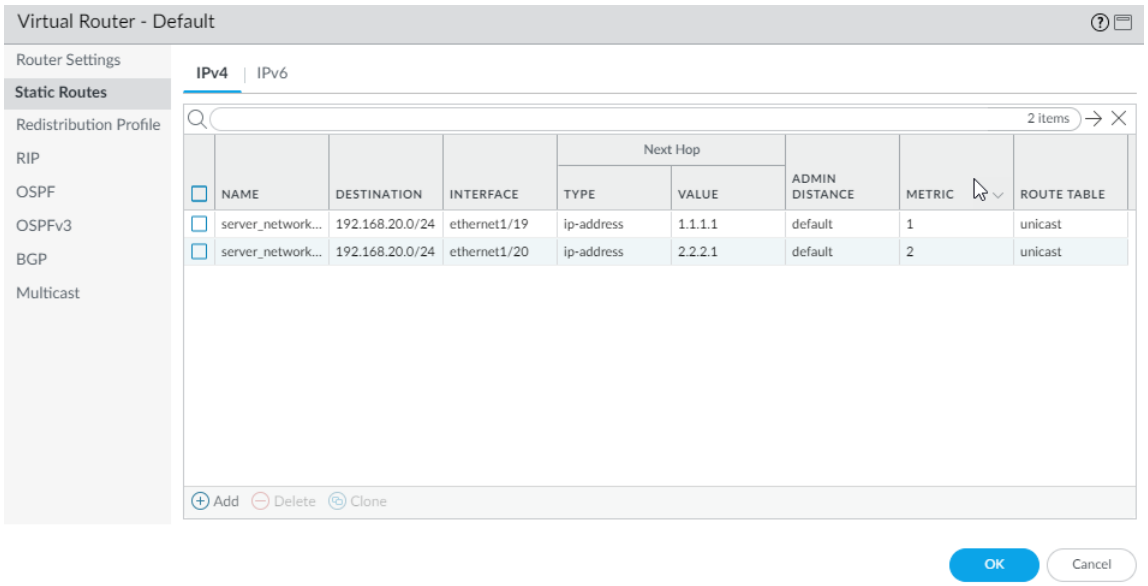
   - Ethernet 1/19 conectada al ISP principal:
     - Zona: TwoISP
     - IP address: 1.1.1.2/30
     - Enrutador virtual: predeterminado
   - Ethernet 1/20 conectada al ISP de reserva:
     - Zona: TwoISP
     - IP address: 2.2.2.2/30
     - Enrutador virtual: predeterminado
   - Ethernet 1/2 es la interfaz de entrada que los clientes de la red usan para conectarse a internet:
     - Zona: Corporate (Corporativa)
     - IP address: 192.168. 54.1/24
     - Enrutador virtual: predeterminado

© 2020 Palo Alto Networks, Inc.

2. Para guardar la configuración de la interfaz, haga clic en **OK (Aceptar)**.

STEP 2 | En el enrutador virtual, añadir una ruta estática al ISP de reserva

1. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y elija el enlace **default (predeterminado)** para que se abra el cuadro de diálogo Virtual Router (Enrutador virtual).
2. Seleccione **Static Routes (Rutas estáticas)** y haga clic en **Add (Añadir)**. Introduzca un **Name (Nombre)** para la ruta y especifique la dirección IP de **Destination (Destino)** para la que está definiendo la ruta estática. En este ejemplo, usamos 0.0.0.0/0 para todo el tráfico.
3. Seleccione el botón de opción **IP Address (Dirección IP)** y defina la dirección IP de **Next Hop (Siguiente salto)** para su enrutador que se conecta con la puerta de enlace de Internet alternativa (no puede usar un nombre de dominio para el siguiente salto). En este ejemplo, 2.2.2.1.
4. Especifique una métrica de coste para la ruta.



5. Haga clic en **OK (Aceptar)** dos veces para guardar la configuración de enrutador virtual.

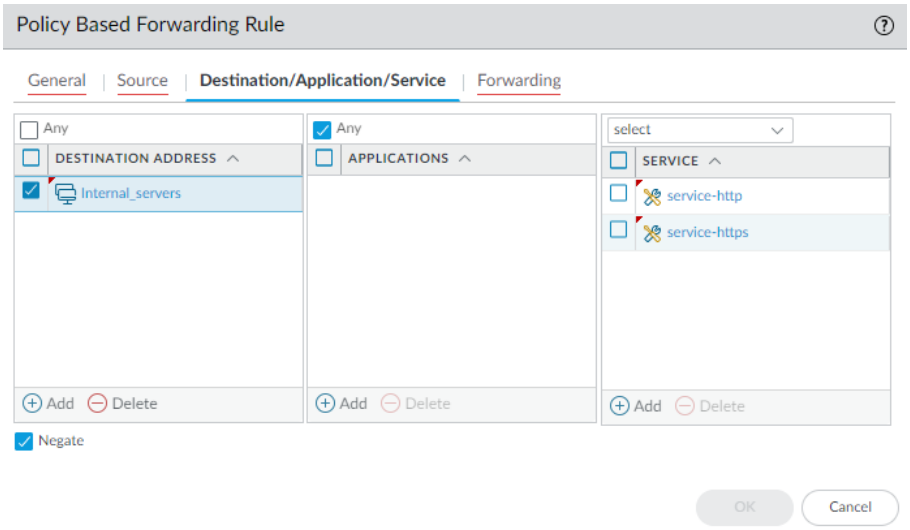
STEP 3 | Crear una regla PBF que redirija el tráfico a la interfaz que está conectada al ISP principal

Asegúrese de excluir el tráfico destinado a direcciones IP/servidores internos desde PBF. Defina una regla de negación para que el tráfico destinado a direcciones IP internas no se enrute a través de la interfaz de salida definida en la regla PBF.

1. Seleccione **Policies (Políticas)** > **Policy Based Forwarding (Reenvío basado en políticas)** y haga clic en **Add (Añadir)**.
2. Use un **Name (Nombre)** descriptivo para la regla en la pestaña **General**.
3. En la pestaña **Source (Origen)**, establezca la **zona de origen**; en este ejemplo, la zona es Corportate (Corporativa).
4. En la pestaña **Destination/Application/Service (Destino/aplicación/servicio)**, defina lo siguiente:
    1. En la sección Dirección de destino, **Add (Añadir)** las direcciones IP o el intervalo de direcciones para los servidores en la red interna o cree un objeto de dirección para sus servidores internos. Seleccione **Negate (Negar)** para excluir de usar esta regla a las direcciones IP u objetos de direcciones enumerados anteriormente.
    2. En la sección Servicio, **Add (Añadir)** los servicios **service-http** y **service-https** para permitir que el tráfico HTTP y HTTPS use estos puertos predeterminados. Para el resto de tráfico permitido por una política de seguridad, se usa la ruta predeterminada.

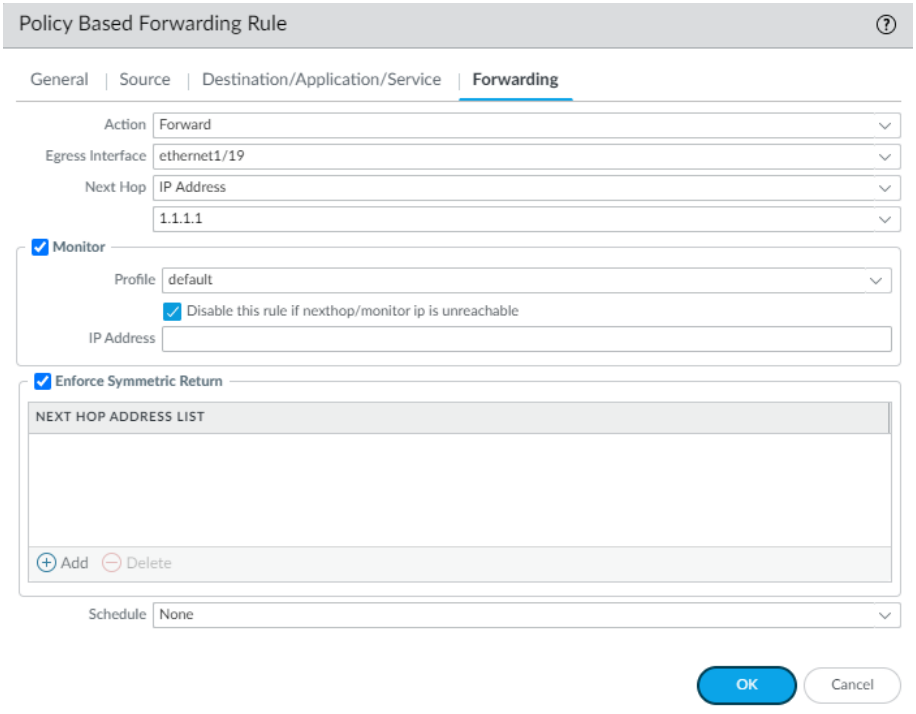
© 2020 Palo Alto Networks, Inc.

Para reenviar todo el tráfico usando PBF, defina el Servicio en Any (Cualquiera).



STEP 4 | Especifique adónde reenviar el tráfico.

1. En la pestaña **Forwarding (Reenvío)**, especifique la interfaz a la que quiere reenviar el tráfico y habilite la supervisión de rutas.
2. Para reenviar el tráfico, defina la **Action (Acción)** en **Forward (Reenviar)** y seleccione la **Egress Interface (Interfaz de salida)** y especifique el **Next Hop (Siguiente salto)**. En este ejemplo, la interfaz de salida es ethernet1/19, y la dirección IP de siguiente salto es 1.1.1.1 (no puede usar un FQDN para el siguiente salto).



3. Habilite la opción **Monitor (Supervisar)** y añada el perfil de supervisión predeterminado para activar una conmutación por error al ISP de reserva. En este ejemplo no especificamos una dirección

© 2020 Palo Alto Networks, Inc.

IP de destino para la supervisión. El cortafuegos supervisará la dirección IP de siguiente salto; si no se puede alcanzar esta dirección IP, el cortafuegos dirigirá el tráfico a la ruta predeterminada especificada en el enrutador virtual.

4. (Obligatorio si tiene rutas asimétricas) Seleccione **Enforce Symmetric Return (Aplicar vuelta simétrica)** para garantizar que el tráfico de retorno desde la zona corporativa a internet se reenvíe por la misma interfaz a través de la que el tráfico accedió desde internet.
5. NAT garantiza que el tráfico desde internet regrese a la dirección IP/interfaz correcta en el cortafuegos.
6. Haga clic en **OK (Aceptar)** para guardar los cambios.

		Source			Destination				Forwarding			Monitoring		
	NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	APPLICATION	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	TARGET	DISABLE IF UNR
1	pbf_rule_source_zone	Corporate	192.168.10.2	any	any	any	service-http service-https	forward	ethernet1/19	1.1.1.1	true	default	none	true

STEP 5 | Crear reglas NAT basadas en la interfaz de salida e ISP. Estas reglas garantizar que se use la dirección IP de origen correcta para conexiones salientes.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En este ejemplo, la regla NAT que creamos para cada ISP es la siguiente:

   NAT para ISP principal

   En la pestaña **Original Packet (Paquete original)**,

   Zona de origen: Corporate (Corporativa)

   Destination Zone (Zona de destino) : TwoISP

   En la pestaña **Translated Packet (Paquete traducido)**, en Traducción de dirección de origen

   Translation Type (Tipo de traducción): Dynamic IP and Port

   Tipo de dirección: Interface Address

   Interface (Interfaz): ethernet1/19

   IP Address (Dirección IP): 1.1.1.2/30

   NAT para ISP de reserva

   En la pestaña **Original Packet (Paquete original)**,

   Zona de origen: Corporate (Corporativa)

   Destination Zone (Zona de destino) : TwoISP

   En la pestaña **Translated Packet (Paquete traducido)**, en Traducción de dirección de origen

   Translation Type (Tipo de traducción): Dynamic IP and Port

   Tipo de dirección: Interface Address

   Interface (Interfaz): ethernet1/20

   IP Address (Dirección IP): 2.2.2.2/30

© 2020 Palo Alto Networks, Inc.

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATI
1	NAT for Primary ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/19 1.1.1.2/30	none
2	NAT for Backup ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/20 2.2.2.2/30	none

STEP 6 | Cree una política de seguridad para permitir el acceso saliente a internet.

Para habilitar aplicaciones de forma segura, cree una regla que permita acceder a internet y añada los perfiles de seguridad disponibles en el cortafuegos.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. Use un **Name (Nombre)** descriptivo para la regla en la pestaña **General**.
3. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en Corporate (Corporativa).
4. En la pestaña **Destination (Destino)**, establezca la **Destination Zone (Zona de destino)** como TwoISP.
5. En la pestaña **Service/ URL Category (Categoría de URL/servicio)**, deje la opción por defecto de **application-default (valor predeterminado de aplicación)**.
6. En la ficha **Actions (Acciones)** , realice estas tareas:
    1. Establezca **Action Setting (Configuración de acción)** como **Allow (Permitir)**.
    2. Adjunte los perfiles por defecto para la protección antivirus, antispyware y contra vulnerabilidades, y para el filtrado de URL, en **Profile Setting (Ajuste de perfil)**.
7. En **Options (Opciones)**, compruebe que el registro está activado al final de una sesión. Solo se registra el tráfico que coincida con una regla de seguridad.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Copr2ISP	none	universal	Corporate	any	any	any	TwoISP	any	any	any	any	Allow

STEP 7 | Guarde las políticas en la configuración que se esté ejecutando en el cortafuegos.

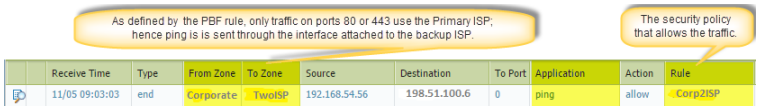
Haga clic en **Commit (Confirmar)**.

STEP 8 | Compruebe que la regla PBF está activa y que se usa el ISP principal para el acceso de internet.

1. Inicie un explorador web y acceda al servidor web En el cortafuegos, compruebe el log de tráfico para la actividad de navegación web.
2. Desde un cliente de la red, use la utilidad ping para comprobar la conectividad a un servidor web en internet y compruebe el tráfico en el cortafuegos.

```
C:\Users\pm-user1>ping 198.51.100.6
Pinging 198.51.100.6 with 32 bytes of data:
Reply from 198.51.100.6: bytes=32 time=34ms TTL=117
Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
Reply from 198.51.100.6: bytes=32 time=25ms TTL=117
Reply from 198.51.100.6: bytes=32 time=3ms TTL=117
Ping statistics for 198.51.100.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum = 3ms, Maximum = 34ms, Average = 18ms
```


© 2020 Palo Alto Networks, Inc.



3. Para confirmar que la regla PBF está activa, use el siguiente comando CLI:

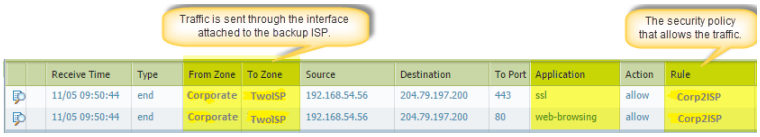
```
admin@PA-NGFW> show pbf rule all
Rule        ID     Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ==============
Use ISP-Pr 1 Active     Forward ethernet1/1 1.1.1.1
```

STEP 9 | Compruebe que se produce la conmutación por error al ISP de reserva y que la NAT de origen se aplica correctamente.

1. Desactive la conexión al ISP principal.
2. Confirme que la regla PBF esté inactiva mediante el siguiente comando CLI:

```
admin@PA-NGFW> show pbf rule all
Rule        ID     Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ============== ===
Use ISP-Pr 1 Disabled Forward ethernet1/19     1.1.1.1
```

3. Acceda al servidor web y compruebe que el log de tráfico se reenvía a través del ISP de reserva.



4. Consulte los detalles de la sesión para confirmar que la regla NAT funciona correctamente.

```
admin@PA-NGFW> show session all
--------------------------------------------------------
ID Application    State   Type Flag Src[Sport]/Zone/Proto (translated
 IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------
87212 ssl ACTIVE  FLOW  NS   192.168.54.56[53236]/Corporate/6
 (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP (204.79.197.200[443])
```

5. Obtenga el número de identificación de sesión de la salida y consulte los detalles de la sesión.

La regla PBF no se usa y, por lo tanto, no se incluye en la salida.

```
admin@PA-NGFW> show session id 87212
Session           87212
c2s flow:
                source:      192.168.54.56 [Corporate]
                dst:         204.79.197.200
                proto:       6
                sport:       53236           dport:       443
                state:       ACTIVE          type:        FLOW
                src user:    unknown
                dst user:    unknown
s2c flow:
                source:      204.79.197.200 [TwoISP]
                dst:         2.2.2.2
                proto:       6
```


© 2020 Palo Alto Networks, Inc.

```
                sport:       443             dport:      12896
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
start time                    : Wed Nov5 11:16:10 2014
        timeout                          : 1800 sec
        time to live                     : 1757 sec
        total byte count(c2s)            : 1918
        total byte count(s2c)            : 4333
        layer7 packet count(c2s)         : 10
        layer7 packet count(s2c)         : 7
        vsys                             : vsys1
        application                      : ssl
        rule                             : Corp2ISP
        session to be logged at end      : True
        session in session ager          : True
        session synced from HA peer      : False
        address/port translation         : source
       nat-rule           : NAT-Backup ISP(vsys1)
        layer7 processing                : enabled
        URL filtering enabled            : True
        URL category                     : search-engines
        session via syn-cookies          : False
        session terminated on host       : False
        session traverses tunnel         : False
        authentication portal session          : False
        ingress interface        : ethernet1/2
    egress interface        : ethernet1/20
        session QoS rule                 : N/A (class 4)
```


© 2020 Palo Alto Networks, Inc.

Comprobación de las reglas de las políticas

Compruebe las reglas de la configuración activa para verificar que las políticas permiten o deniegan tanto el tráfico como el acceso a las aplicaciones y los sitios web de acuerdo con los requisitos y las necesidades de la empresa. Para probar y verificar que se permite o se deniega el tráfico correcto, ejecute pruebas de coincidencia con las políticas de los cortafuegos directamente en la interfaz web.

STEP 1 | Inicio de la interfaz web.

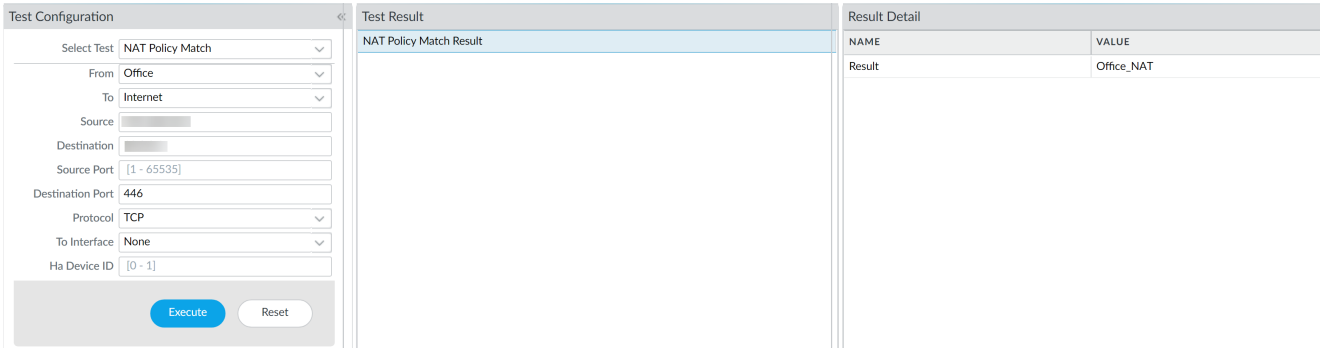
STEP 2 | Seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** para ejecutar una prueba de conectividad o de coincidencia con la política.

STEP 3 | Introduzca los datos precisos para ejecutar la prueba de coincidencia con políticas, En este ejemplo, se ejecuta una prueba de coincidencia con la política de traducción de direcciones de red (network address translation, NAT).

1. **Select Test (Seleccionar prueba)**: seleccione **NAT Policy Match (Coincidencia con política de NAT)**.
2. **From (De)**: seleccione la zona en la que se origina el tráfico.
3. **To (A)**: seleccione la zona de destino del tráfico.
4. **Source (Origen)**: introduzca la dirección IP en la que se origina el tráfico.
5. **Destination (Destino)**: introduzca la dirección IP del dispositivo de destino del tráfico.
6. **Destination Port (Puerto de destino)**: introduzca el puerto que se usa para el tráfico. Este puerto varía en función del protocolo IP que especifique a continuación.
7. **Protocol (Protocolo)**: introduzca el protocolo IP que se usa para el tráfico.
8. Si es preciso, introduzca cualquier otro dato pertinente para comprobar la regla de la política de NAT.

STEP 4 | Haga clic en **Execute (Ejecutar)** para comprobar la coincidencia con la política de NAT.

STEP 5 | Consulte la sección **NAT Policy Match Result (Resultado de coincidencia con la política de NAT)** para ver las reglas que coinciden con los criterios de la prueba.



Virtual Systems

Este tema describe los sistemas virtuales, sus ventajas, los casos de uso típicos y cómo configurarlos. También proporciona enlaces a los otros temas donde se documentan los sistemas virtuales cuando actúan con otras funciones.

> Descripción general de los sistemas virtuales
> Comunicación entre sistemas virtuales
> Puerta de enlace compartida
> Configuración de sistemas virtuales
> Configuración de la comunicación entre sistemas virtuales dentro del cortafuegos
> Configuración de un gateway compartido
> Personalización de rutas de servicio para un sistema virtual
> Funcionalidad de sistema virtual con otras funciones

© 2020 Palo Alto Networks, Inc.

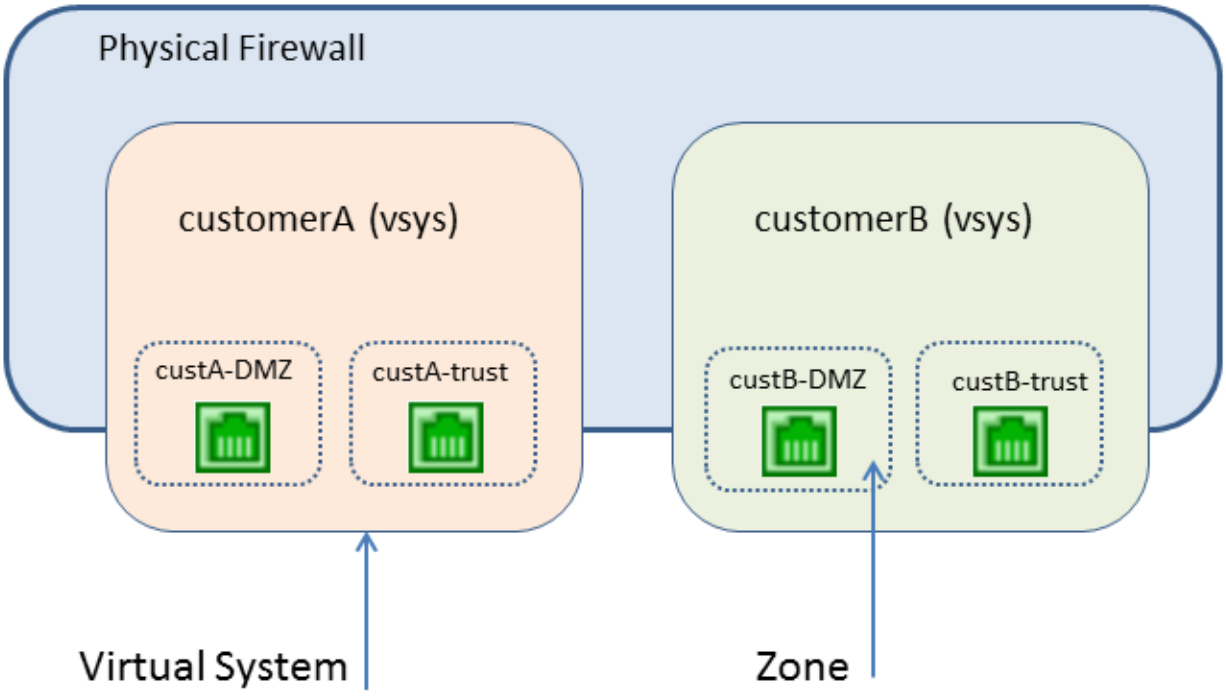
Descripción general de los sistemas virtuales

Los sistemas virtuales son instancias de cortafuegos separados y lógicos en un único cortafuegos físico de Palo Alto Networks. En lugar de usar múltiples cortafuegos, las empresas y proveedores de servicios gestionados pueden usar un único par de cortafuegos (para una alta disponibilidad) y habilitar en ellos sistemas virtuales. Cada sistema virtual (vsys) es un cortafuegos independiente y gestionado de forma separada cuyo tráfico está separado del de otros sistemas virtuales.

- Componentes y segmentación de los sistemas virtuales
- Ventajas de los sistemas virtuales
- Casos de uso de sistemas virtuales
- Compatibilidad con plataformas y licencias de sistemas virtuales
- Funciones de administrador para sistemas virtuales
- Objetos compartidos para sistemas virtuales

Componentes y segmentación de los sistemas virtuales

Un sistema virtual es un objeto que crea un límite administrativo, tal y como se muestra en la siguiente ilustración.



Un sistema virtual se compone de un conjunto de interfaces y subinterfaces físicas y lógicas (que incluyen VLAN y virtual wires), enrutadores virtuales y zonas de seguridad. Puede seleccionar el modo de implementación (cualquier combinación de Virtual Wire, capa 2 o capa 3) de cada sistema virtual. Puede usar los sistemas virtuales para segmentar cualquiera de los siguientes elementos:

- Acceso administrativo
- Gestión de todas las políticas: seguridad, traducción de direcciones de red (network address translation, NAT), calidad de servicio (quality of service, QoS), reenvío basado en políticas, descifrado, sustitución de aplicaciones, inspección de túneles, autenticación y protección contra DoS

© 2020 Palo Alto Networks, Inc.

- Todos los objetos (como objetos de dirección, grupos y filtros de aplicaciones, listas externas dinámicas, perfiles de seguridad, perfiles de descifrado, objetos personalizados, etc.)
- User-ID
- Gestión de certificados
- Perfiles del servidor
- Funciones de logging, informes y visibilidad

Los sistemas virtuales afectan a las funciones de seguridad del cortafuegos, pero por sí solos no afectan a las funciones de red como el enrutamiento estático y dinámico. Puede segmentar el enrutamiento de cada sistema virtual creando uno o más enrutadores virtuales para cada sistema virtual, como en los siguientes casos de uso:

- Si tiene sistemas virtuales para los departamentos de una organización y el tráfico de red de todos los departamentos está en una red común, puede crear un único enrutador virtual para múltiples sistemas virtuales.
- Si desea segmentar el enrutamiento y el tráfico de cada sistema virtual debe aislarse de los demás sistemas, puede crear uno o más enrutadores virtuales para cada sistema virtual.
- Si desea segmentar las asignaciones de usuarios para que no se compartan todas entre los sistemas virtuales, configure los orígenes de User-ID en un sistema virtual distinto del núcleo de User-ID. Consulte Asignaciones de User-ID compartidas entre sistemas virtuales.

Ventajas de los sistemas virtuales

Los sistemas virtuales ofrecen las mismas funciones básicas que un cortafuegos físico, junto con las siguientes ventajas:

- **Administración segmentada**: las diferentes organizaciones (o clientes o unidades de negocio) pueden controlar (y supervisar) una instancia de cortafuegos separada, de modo que tienen control sobre su propio tráfico sin interferir en el tráfico o las políticas de otra instancia de cortafuegos en el mismo dispositivo físico.
- **Flexibilidad**: Una vez configurado el cortafuegos físico, la adición o eliminación de clientes o unidades comerciales puede realizarse con eficiencia. Un ISP, un proveedor de servicios de seguridad gestionados o una empresa pueden ofrecer distintos servicios de seguridad a cada cliente.
- **Reducción del capital y los gastos operativos**: Los sistemas virtuales eliminan la necesidad de tener múltiples cortafuegos físicos en una misma ubicación, ya que los sistemas virtuales coexisten en el mismo cortafuegos. Al no tener que adquirir múltiples cortafuegos, una organización puede ahorrar en gastos de hardware, consumo eléctrico y espacio en los racks, y puede reducir los gastos de gestión y mantenimiento.
- **Posibilidad de compartir las asignaciones de direcciones IP a nombres de usuario**: si designa un sistema virtual como núcleo de User-ID, puede compartir estas asignaciones entre los sistemas virtuales para aprovechar toda la capacidad de User-ID del cortafuegos y reducir la complejidad operativa.

Casos de uso de sistemas virtuales

Hay muchas formas de usar los sistemas virtuales en una red. Un caso de uso común es que un ISP o un proveedor de servicios de seguridad gestionados (MSSP) ofrezca servicios a múltiples clientes con un único cortafuegos. Los clientes pueden elegir entre una amplia gama de servicios que pueden habilitarse o deshabilitarse fácilmente. La administración basada en funciones del cortafuegos permite que el ISP o el MSSP controle el acceso de cada cliente a la funcionalidad (como el logging y creación de informes) a la vez que oculta o muestra funcionalidades de solo lectura para las demás funciones.

Otro caso de uso común es en una gran empresa que requiera distintas instancias de cortafuegos por cuestiones técnicas o de confidencialidad entre múltiples departamentos. Como en el caso anterior, diferentes grupos pueden tener distintos niveles de acceso, siendo el personal de TI quien gestiona el

© 2020 Palo Alto Networks, Inc.

propio cortafuegos. Los servicios pueden supervisarse o facturarse a los departamentos y crear una contabilidad financiera distinta en una organización.

Compatibilidad con plataformas y licencias de sistemas virtuales

Se admiten sistemas virtuales en los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series. Cada serie de cortafuegos admite un número base de sistemas virtuales, que variará según la plataforma. Se requiere una licencia de sistemas virtuales para admitir varios sistemas virtuales en el cortafuegos PA-3200 Series y para crear más de la cantidad base de sistemas virtuales que admite una plataforma.

Para obtener información sobre la licencia, consulte Suscripciones. Para ver el número base y máximo de sistemas virtuales admitidos, consulte la herramienta Comparar cortafuegos.

No se admiten varios sistemas virtuales en los cortafuegos PA-220, PA-800 Series ni VM-Series.

El valor predeterminado es vsys1. No puede eliminar vsys1 porque es relevante para la jerarquía interna en el cortafuegos; vsys1 aparece incluso en modelos de cortafuegos que no admiten varios sistemas virtuales.

Si limita las asignaciones de recursos a sesiones, reglas y túneles de red privada virtual (virtual private network, VPN) que se permiten en los sistemas virtuales, mantiene bajo control los recursos de los cortafuegos. En cada opción de recurso se muestra el intervalo de valores válidos, que varía según el modelo de cortafuegos. El ajuste predeterminado es 0, que significa que el límite del sistema virtual coincide con el límite del modelo de cortafuegos en cuestión. No obstante, el límite de un ajuste concreto no se reproduce en todos los sistemas virtuales. Por ejemplo, si un cortafuegos tiene cuatro sistemas virtuales, ninguno de ellos puede tener todas las reglas de descifrado que se permiten en el cortafuegos. En cuanto el número total de reglas de descifrado de todos los sistemas virtuales alcanza el límite del cortafuegos, ya no puede añadir más.

Funciones de administrador para sistemas virtuales

Los administradores que tienen la función **Superuser (Superusuario)** pueden crear sistemas virtuales y añadir las funciones **Device administrator (Administrador de dispositivos)**, **vsysadmin (administrador de sistemas virtuales)** y **vsysreader (lector de sistemas virtuales)**. La función **Device administrator (Administrador de dispositivos)** puede acceder a todos los sistemas virtuales, pero no puede añadir administradores. Cuando crea un perfil de funciones de administración y configura la función **Virtual System (Sistema virtual)**, esta se aplica a determinados sistemas virtuales del cortafuegos. En la pestaña **Command Line (Línea de comandos)**, hay dos tipos de funciones administrativas para sistemas virtuales:

- **vsysadmin (administrador de sistemas virtuales)**: tiene acceso a determinados sistemas virtuales del cortafuegos para crear y gestionar aspectos concretos de dichos sistemas. Estos administradores no tienen acceso a las interfaces de red, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de IPSec, los túneles de GRE, los perfiles de red, el proxy DNS, DHCP, QoS ni LLDP. Los usuarios que tienen este permiso solo pueden confirmar las configuraciones de los sistemas virtuales que tienen asignados.
- **vsysreader (lector de sistemas virtuales)**: tiene acceso de solo lectura a determinados sistemas virtuales del cortafuegos y a aspectos concretos de dichos sistemas. Estos administradores no tienen acceso a las interfaces de red, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de IPSec, los túneles de GRE, los perfiles de red, el proxy DNS, DHCP, QoS ni LLDP.

Un administrador de sistema virtual puede ver los logs únicamente de los sistemas virtuales que se le han asignado. Los usuarios con las funciones **Superuser (Superusuario)** o **Device administrator (Administrador de dispositivos)** pueden ver todos los logs, seleccionar sistemas virtuales para visualizarlos o configurar sistemas virtuales como núcleo de User-ID.

© 2020 Palo Alto Networks, Inc.

Objetos compartidos para sistemas virtuales

Si su cuenta de administrador abarca múltiples sistemas virtuales, puede optar por configurar objetos (como un objeto de dirección) y políticas para un sistema virtual específico o bien crear objetos compartidos que se aplicarán a todos los sistemas virtuales del cortafuegos. Si intenta crear un objeto compartido con el mismo nombre y tipo que un objeto existente de un sistema virtual, se usará el objeto del sistema virtual.

© 2020 Palo Alto Networks, Inc.

Comunicación entre sistemas virtuales

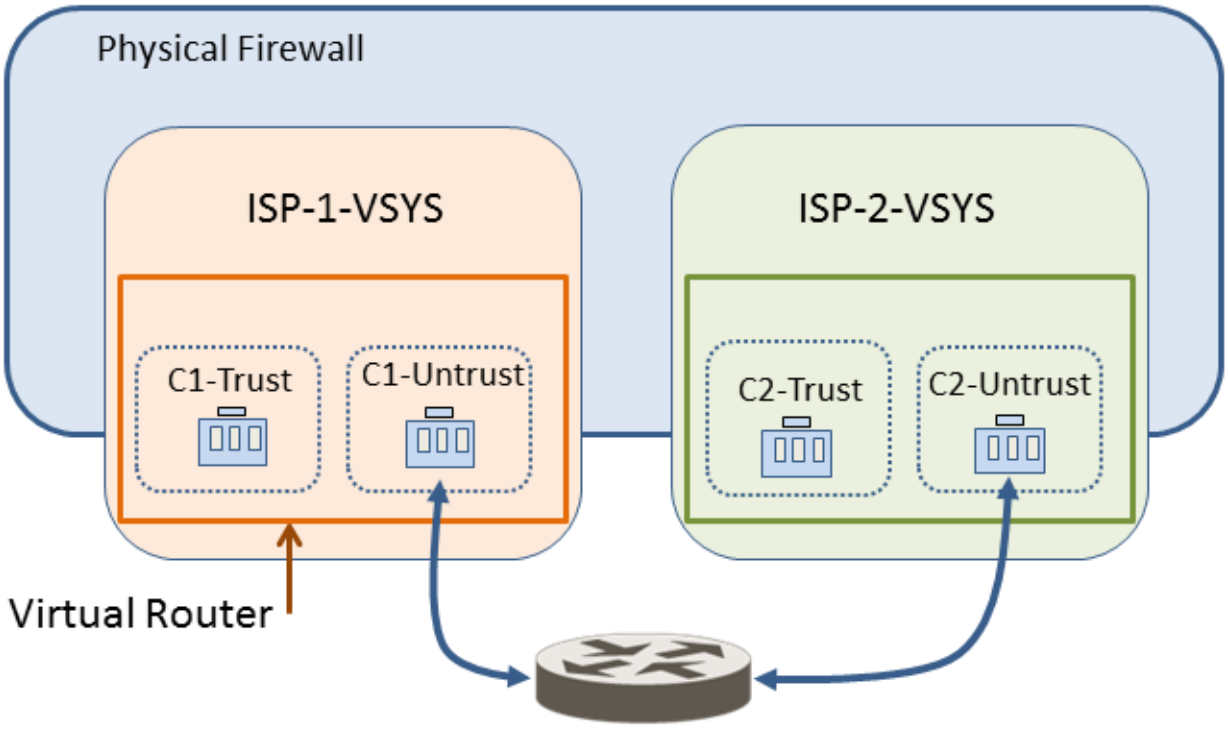
Hay dos situaciones típicas en las que es deseable que haya comunicación entre sistemas virtuales (tráfico inter-vsys). En un entorno multiempresa, la comunicación entre sistemas virtuales puede producirse haciendo que el tráfico salga del cortafuegos, salga a Internet y vuelva a entrar en el cortafuegos. En un entorno de organización única, la comunicación entre los sistemas virtuales puede permanecer dentro del cortafuegos. Esta sección describe ambas situaciones.

- Tráfico entre VSYS que debe abandonar el cortafuegos
- Tráfico entre VSYS que permanece en el cortafuegos
- La comunicación entre VSYS usa dos sesiones

Tráfico entre VSYS que debe abandonar el cortafuegos

Un ISP que tiene múltiples clientes en un cortafuegos (conocido como multiempresa) puede usar un sistema virtual para cada cliente, dando así a cada cliente control sobre la configuración de su sistema virtual. El ISP concede permisos de **vsysadmin** a los clientes. El tráfico y la gestión de cada cliente están aislados de los de los otros. Cada sistema virtual debe configurarse con su propia dirección IP y uno o más enrutadores virtuales para gestionar el tráfico y su propia conexión a Internet.

Si los sistemas virtuales tienen que comunicarse entre sí, ese tráfico sale del cortafuegos a otro dispositivo de enrutamiento de capa 3 y vuelve al cortafuegos, aunque los sistemas virtuales existen en el mismo cortafuegos físicos, tal y como se muestra en la siguiente ilustración.



Tráfico entre VSYS que permanece en el cortafuegos

A diferencia del caso multiempresa anterior, los sistemas virtuales de un cortafuegos pueden estar bajo el control de una única organización. La organización quiere tanto aislar el tráfico entre los sistemas virtuales como permitir las comunicaciones entre ellos. Este caso de uso común surge cuando la organización

© 2020 Palo Alto Networks, Inc.

desea proporcionar la separación entre departamentos pero también permitir que los departamentos se comuniquen entre sí o se conecten con la misma red. En esta situación, el tráfico inter-vsys sigue dentro del cortafuegos, tal y como se describe en los siguientes temas:

- Zona externa
- Zonas externas y políticas de seguridad para el tráfico dentro de un cortafuegos

Zona externa

La comunicación en el caso de uso anterior se consigue configurando políticas de seguridad que señalan hacia o desde una zona *externa*. Una zona externa es un objeto de seguridad que se asocia con un sistema virtual que puede alcanzar, la zona es externa al sistema virtual. Un sistema virtual solo puede tener una zona externa, independientemente del número de zonas de seguridad que contenga. Las zonas externas deben permitir el tráfico entre zonas en distintos sistemas virtuales, sin que llegue a salir del cortafuegos.

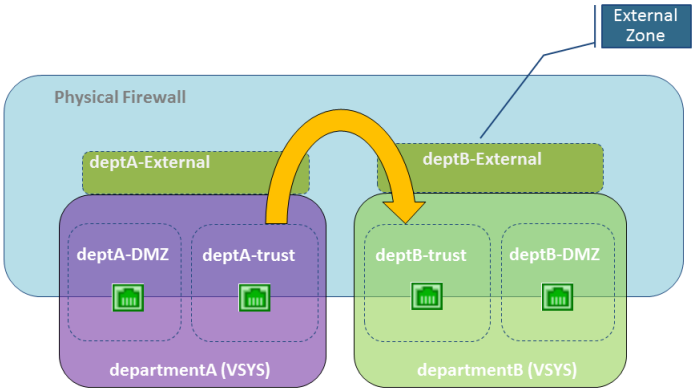
El administrador del sistema virtual configura las políticas de seguridad necesarias para permitir el tráfico entre dos sistemas virtuales. A diferencia de las zonas de seguridad, una zona externa no se asocia con una interfaz, se asocia con un sistema virtual. La política de seguridad permite o deniega el tráfico entre la zona de seguridad (interna) y la zona externa.

Como las zonas externas no tienen interfaces o direcciones IP asociadas, algunos perfiles de protección de zonas no se admiten en las zonas externas.

Recuerde que cada sistema virtual es una instancia diferente de un cortafuegos, lo que significa que cada paquete que se mueve entre sistemas virtuales se inspeccionará para una evaluación de App-ID y política de seguridad.

Zonas externas y políticas de seguridad para el tráfico dentro de un cortafuegos

En el siguiente ejemplo, una empresa tiene dos grupos administrativos: los sistemas virtuales del departamentoA y del departamentoB. La siguiente ilustración muestra la zona externa asociada con cada sistema virtual, y el tráfico que fluye desde una zona de confianza a la zona externa, sale de ahí hacia la zona externa de otro sistema virtual, y de ahí a su zona de confianza.



Para crear zonas externas, el administrador del cortafuegos debe configurar sistemas virtuales para que sean *visibles* entre sí. Las zonas externas no tienen políticas de seguridad entre ellas porque sus sistemas virtuales son visibles entre sí.

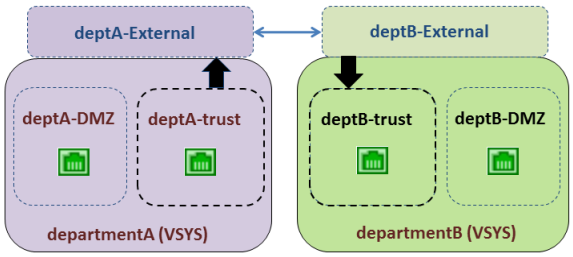
Para una comunicación entre sistemas virtuales, las interfaces de entrada y salida del cortafuegos se asignan a un único enrutador virtual o se conectan usando rutas estáticas entre enrutadores virtuales. El más sencillo de estos dos enfoques es asignar todos los sistemas virtuales que deben comunicarse entre sí a un único enrutador virtual.

© 2020 Palo Alto Networks, Inc.

Puede haber un motivo por el que los sistemas virtuales deben tener su propio enrutador virtual; por ejemplo, si los sistemas virtuales usan intervalos de direcciones IP superpuestos. El tráfico puede enrutarse entre los sistemas virtuales, pero cada enrutador virtual debe tener rutas estáticas que señalen al otro enrutador virtual como el siguiente salto.

En la situación anterior, debe haber una empresa con dos grupos administrativos: departamentoA y departamentoB. El grupo del departamentoA gestiona la red local y los recursos DMZ. El grupo del departamentoB gestiona el tráfico de salida o entrada del segmento de ventas de la red. Todo el tráfico se encuentra en la red local, por lo que solo se usa un enrutador virtual. Hay dos zonas externas configuradas para la comunicación entre los dos sistemas virtuales. El sistema virtual del departamentoA tiene tres zonas que se usan en políticas de seguridad: deptA-DMZ, deptA-confianza y deptA-Externa. El sistema virtual del departamentoB también tiene tres zonas: deptB-DMZ, deptB-confianza y deptB-Externa. Ambos grupos pueden controlar el tráfico que atraviesa sus sistemas virtuales.

Para permitir el tráfico entre el deptA-confianza al deptB-confianza, es obligatorio contar con dos políticas de seguridad. En la siguiente ilustración las dos flechas verticales indican dónde controlan el tráfico las políticas de seguridad (que se describe bajo la ilustración).



- Política de seguridad 1: En la ilustración anterior, el tráfico tiene como destino la zona deptB-confianza. El tráfico abandona la zona deptA-confianza y va a la zona deptA-Externa. Una política de seguridad debe permitir el tráfico de la zona de origen (deptA-confianza) a la zona de destino (deptA-Externa). Un sistema virtual permite que se use cualquier tipo de política para este tráfico, incluido el NAT.

  No hay necesidad de ninguna política entre las zonas externas porque el tráfico enviado a una zona externa aparece en las otras zonas externas y tiene acceso automático a las mismas si son visibles desde la zona externa original.
- Política de seguridad 2: En la ilustración anterior, el tráfico desde deptB-Externa sigue estando destinado a la zona deptB-confianza y es necesario configurar una política de seguridad para permitirlo. La política de seguridad debe permitir el tráfico de la zona de origen (deptB-Externa) a la zona de destino (deptB-confianza).

El sistema virtual del departamentoB podría configurarse para bloquear el tráfico desde el sistema virtual del departamentoA y viceversa. Al igual que con el tráfico de cualquier otra zona, la política debe permitir explícitamente que el tráfico de las zonas externas llegue a otras zonas de un sistema virtual.

Además de las zonas externas necesarias para el tráfico entre sistemas virtuales que no abandona el cortafuegos, también se necesitan zonas externas si configura una puerta de enlace compartida*, en cuyo caso el tráfico debe abandonar el cortafuegos.*

La comunicación entre VSYS usa dos sesiones

Resulta útil comprender que la comunicación entre dos sistemas virtuales usa dos sesiones, en lugar de la única sesión que se usa con un único sistema virtual. Comparemos las situaciones.

Situación 1: Vsys1 tiene dos zonas: confianza1 y nofiable1. Un host de la zona confianza1 inicia el tráfico cuando lo necesita para comunicarse con un dispositivo de la zona nofiable1. El host envía el tráfico al cortafuegos, y este crea una nueva sesión para la zona de origen confianza1 en la zona de destino nofiable1. Solo se necesita una sesión para este tráfico.

© 2020 Palo Alto Networks, Inc.

Situación 2: Un host de vsys1 necesita acceder a un servidor en vsys2. El host de la zona confianza1 inicia el tráfico al cortafuegos, y este crea una primera sesión: zona de origen confianza1 a zona de destino nofiable1. El tráfico se dirige a vsys2, ya sea interna o externamente. A continuación el cortafuegos crea una segunda sesión: zona de origen nofiable2 a zona de destino confianza2. En este tráfico entre vsys son necesarias dos sesiones.

© 2020 Palo Alto Networks, Inc.

Puerta de enlace compartida

Este tema incluye la siguiente información sobre los gateways compartidos:

- Zonas externas y puerta de enlace compartida
- Consideraciones de red para una puerta de enlace compartida

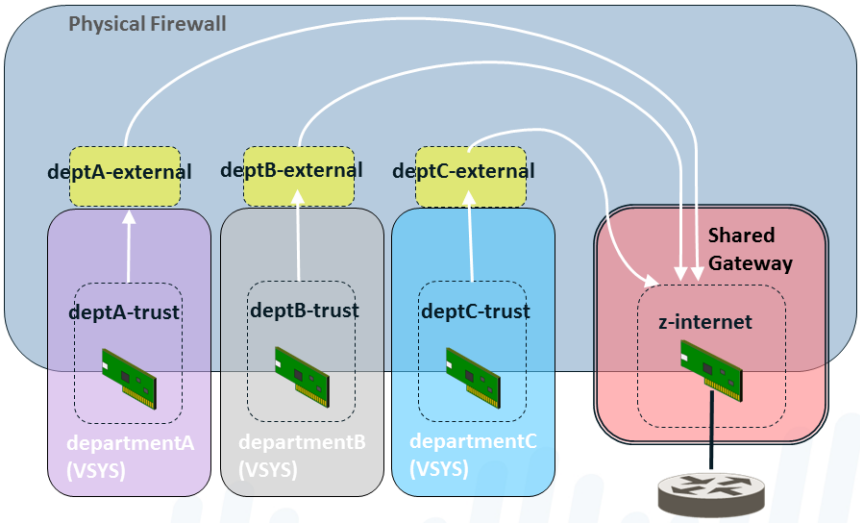
Zonas externas y puerta de enlace compartida

Un gateway compartido es una interfaz que comparten múltiples sistemas virtuales para poder comunicarse a través de Internet. Cada sistema virtual necesita una zona externa, que actúa como intermediaria, para configurar políticas de seguridad que permitan o denieguen el tráfico de la zona interna del sistema virtual a la puerta de enlace compartida.

El gateway compartido usa un único enrutador virtual para enrutar el tráfico para todos los sistemas virtuales. Un gateway compartido se usa en casos en los que una interfaz no necesita un límite administrativo completo o cuando múltiples sistemas virtuales deben compartir una única conexión a Internet. Este segundo caso surge si un ISP ofrece a una organización una única dirección IP (interfaz), pero hay múltiples sistemas virtuales que necesitan comunicación externa.

A diferencia del comportamiento entre sistemas virtuales, las evaluaciones de App-ID y política de seguridad no se realizan entre un sistema virtual y un gateway compartido. Por eso el uso de un gateway compartido para acceder a Internet implica una menor carga de trabajo que crear otro sistema virtual para lo mismo.

En la siguiente ilustración, tres clientes comparten un cortafuegos, pero solo hay una interfaz con acceso a Internet. La creación de otro sistema virtual añadiría la carga de una evaluación de política de seguridad y App-ID para el tráfico que se envía a la interfaz a través del sistema virtual añadido. Para evitar añadir otro sistema virtual, la solución es configurar un gateway compartido, tal y como se muestra en el siguiente diagrama.



El gateway compartido tiene una dirección IP enrutada globalmente que se usa para comunicarse con el mundo exterior. Las interfaces de los sistemas virtuales también tienen direcciones IP, pero puede tratarse de direcciones IP privadas y no enrutables.

Como recordará, el administrador debe especificar si un sistema virtual es visible para otros. A diferencia de los sistemas virtuales, un gateway compartido siempre es visible para todos los sistemas virtuales del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Un número de ID de puerta de enlace compartida aparece como **sg<ID** en la interfaz web. Se recomienda que asigne a su gateway compartido un nombre que incluya su número de ID.

Cuando añade objetos como zonas o interfaces a una puerta de enlace compartida, esta aparece como un sistema virtual disponible en el menú de sistemas virtuales.

Una puerta de enlace compartida es una versión limitada de un sistema virtual; admite NAT y el reenvío basado en políticas (PBF), pero no admite la seguridad, las políticas DoS, el QoS, el descifrado, la anulación de aplicaciones o las políticas de autenticación.

Consideraciones de red para una puerta de enlace compartida

Tenga en cuenta lo siguiente cuando configure un gateway compartido.

- Los sistemas virtuales de un caso de gateway compartido acceden a Internet a través de la interfaz física de la gateway usando una única dirección IP. Si las direcciones IP de los sistemas virtuales no pueden enrutarse globalmente, configure el NAT de origen para traducir esas direcciones a direcciones IP que sí puedan enrutarse globalmente.
- Un enrutador virtual enruta el tráfico de todos los sistemas virtuales a través del gateway compartido.
- La ruta predeterminada para los sistemas virtuales debe señalar la puerta de enlace compartida.
- Es necesario configurar políticas de seguridad para cada sistema virtual con el fin de permitir el tráfico entre la zona interna y la externa, que es visible para el gateway compartido.
- Un administrador de cortafuegos debe controlar el enrutador virtual, de modo que ningún miembro del sistema virtual pueda afectar al tráfico de los demás sistemas virtuales.
- En un cortafuegos de Palo Alto Networks, un paquete puede cambiar de un sistema virtual a otro o a un gateway compartido. Un paquete no puede atravesar más de dos sistemas virtuales o gateways compartidos. Por ejemplo, no puede ir del sistema virtual 1 al 2 y al 3, ni tampoco del sistema virtual 1 al 2 y a la puerta de enlace 1 porque ambos ejemplos implican más de dos sistemas virtuales, lo cual no está permitido.

Para ahorrar tiempo y esfuerzos de configuración, considere las siguientes ventajas de un gateway compartido:

- En vez de configurar el NAT para múltiples sistemas virtuales asociados con un gateway compartido, puede configurar NAT para el gateway compartido.
- En vez de configurar el enrutamiento basado en políticas (PBR) para múltiples sistemas virtuales asociados con un gateway compartido, puede configurar PBR para el gateway compartido.

© 2020 Palo Alto Networks, Inc.

Configuración de sistemas virtuales

Para crear un sistema virtual necesita lo siguiente:

- Una función administrativa de **superusuario**.
- Una interfaz configurada.
- Una licencia de sistemas virtuales si va a crear más sistemas virtuales que el número base admitido en la plataforma. Consulte Compatibilidad con plataformas y licencias de sistemas virtuales.

STEP 1 | Habilite sistemas virtuales.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite **General Settings (Configuración general)**.
2. Seleccione la casilla de verificación **Multi Virtual System Capability (Capacidad de cortafuegos virtuales)** y haga clic en **OK (Aceptar)**. Esta acción activa la confirmación si la aprueba.

   Solo después de habilitar los sistemas virtuales, la pestaña **Device (Dispositivo)** mostrará las opciones **Virtual Systems (Sistemas virtuales)** y **Shared Gateways (Puertas de enlace compartidas)**.

STEP 2 | Cree un sistema virtual.

1. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)**, haga clic en **Add (Añadir)** e introduzca un **ID** de sistema virtual, que se añade a “vsys” (el intervalo es 1 a 255).

   El valor predeterminado es vsys1. No puede eliminar vsys1 porque es relevante para la jerarquía interna en el cortafuegos; vsys1 aparece incluso en modelos de cortafuegos que no admiten varios sistemas virtuales.
2. Seleccione **Allow forwarding of decrypted content (Permitir reenvío de contenido descifrado)** si desea permitir que el cortafuegos reenvíe el contenido descifrado a un servicio exterior. Por ejemplo, debe habilitar esta opción para que el cortafuegos pueda enviar contenido descifrado a WildFire para su análisis.
3. Introduzca un **Nombre** descriptivo para el sistema virtual. Solo se permite un máximo de 31 caracteres alfanuméricos, espacios y guiones bajos.

STEP 3 | Asigne interfaces al sistema virtual.

Los enrutadores virtuales, cables virtuales o VLAN pueden estar configurados o configurarse después, momento en el cual usted especificará el sistema virtual que tiene asociado cada uno.

1. En la pestaña **General**, seleccione un objeto **DNS Proxy** si desea aplicar las reglas de proxy DNS a la interfaz.
2. En el campo **Interfaces**, haga clic en **Añadir** para introducir las interfaces o subinterfaces para asignarlas al sistema virtual. Una interfaz no puede pertenecer únicamente a un sistema virtual.
3. Realice cualquiera de las siguientes acciones, según el tipo de implementación que necesite en el sistema virtual:
   - En el campo **VLAN**, haga clic en **Add (Añadir)** para introducir las VLAN que se van a asignar al vsys.
   - En el campo **Virtual Wires (Cables virtuales)**, haga clic en **Add (Añadir)** para introducir los cables virtuales que se van a asignar al vsys.
   - En el campo **Virtual Routers (Enrutadores virtuales)**, haga clic en **Add (Añadir)** para introducir los enrutadores virtuales que se van a asignar al vsys.
4. En el campo **Visible Virtual System (Sistema virtual visible)**, seleccione todos los sistemas virtuales que deben ser visibles para el sistema virtual que está configurando. Esto es necesario para los sistemas virtuales que necesitan comunicarse entre sí.

© 2020 Palo Alto Networks, Inc.

En un escenario multiusuario que requiera límites administrativos estrictos, no se deben seleccionar sistemas virtuales.

5. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Limite las asignaciones de recursos por sesiones, reglas y túneles VPN permitidos para el sistema virtual. La flexibilidad de poder asignar límites por sistema virtual le permite controlar de forma eficaz los recursos de cortafuegos.

1. En la pestaña **Recurso**, defina si desea los límites de un sistema virtual. En cada campo se muestra el intervalo de valores válidos, que varía según el modelo de cortafuegos. El ajuste predeterminado es 0, que significa que el límite del sistema virtual coincide con el límite del modelo de cortafuegos en cuestión. No obstante, el límite de un ajuste concreto no se reproduce en todos los sistemas virtuales. Por ejemplo, si un cortafuegos tiene cuatro sistemas virtuales, ninguno de ellos puede tener todas las reglas de descifrado que se permiten en el cortafuegos. En cuanto el número total de reglas de descifrado de todos los sistemas virtuales alcanza el límite del cortafuegos, ya no puede añadir más.

   - **Límite de sesiones**

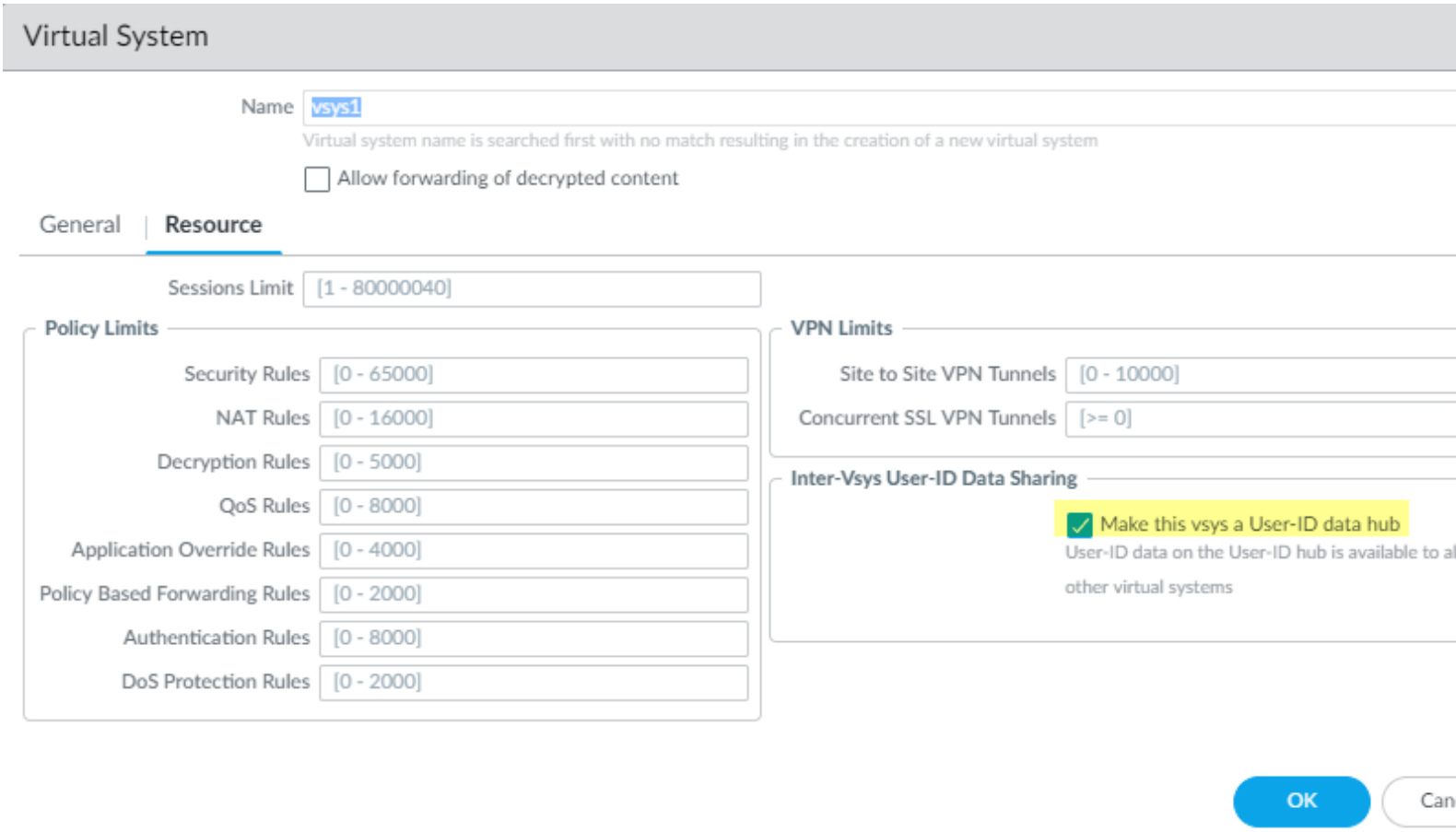
     Si utiliza el comando CLI show session meter, se mostrará la cantidad máxima de sesiones permitidas por plano de datos, la cantidad actual de sesiones que está utilizando el sistema virtual y la cantidad acelerada de sesiones por sistema virtual. En un cortafuegos de la serie PA-5200 o PA-7000, la cantidad actual de sesiones que se está utilizando puede ser mayor que el máximo configurado para el límite de sesiones, ya que existen varios planos de datos por cada sistemas virtual. El límite de sesiones que usted configura en un cortafuegos de la serie PA-5200 o PA-7000 es por plano de datos y derivará en un máximo más alto por cada sistema virtual.
   - **Reglas de seguridad**
   - **Reglas NAT**
   - **Reglas de descifrado**
   - **Reglas de QoS**
   - **Reglas de cancelación de aplicación**
   - **Reglas de reenvío basado en políticas**
   - **Reglas de autenticación**
   - **Reglas de protección contra ataques por denegación de servicio**
   - **Túneles VPN de sitio a sitio**
   - **Túneles de SSL-VPN simultáneos**
2. Haga clic en **OK (Aceptar)**.

STEP 5 | (Opcional) Configure un sistema virtual como núcleo de User-ID para compartir las asignaciones; consulte Asignaciones de User-ID compartidas entre sistemas virtuales.

La información sobre las asignaciones de direcciones IP y puertos a nombres de usuario de los agentes de servidores de terminal y los datos sobre las asignaciones de grupos no se comparten entre el núcleo y los sistemas virtuales conectados.

1. En los sistemas virtuales existentes, transfiera la configuración de los orígenes de User-ID que desea compartir (como servidores supervisados y agentes de User-ID) al sistema virtual que va a funcionar como núcleo.
2. En la pestaña **Resource (Recurso)**, marque **Make this vsys a User-ID data hub (Usar este sistema virtual como núcleo de datos de User-ID)**.

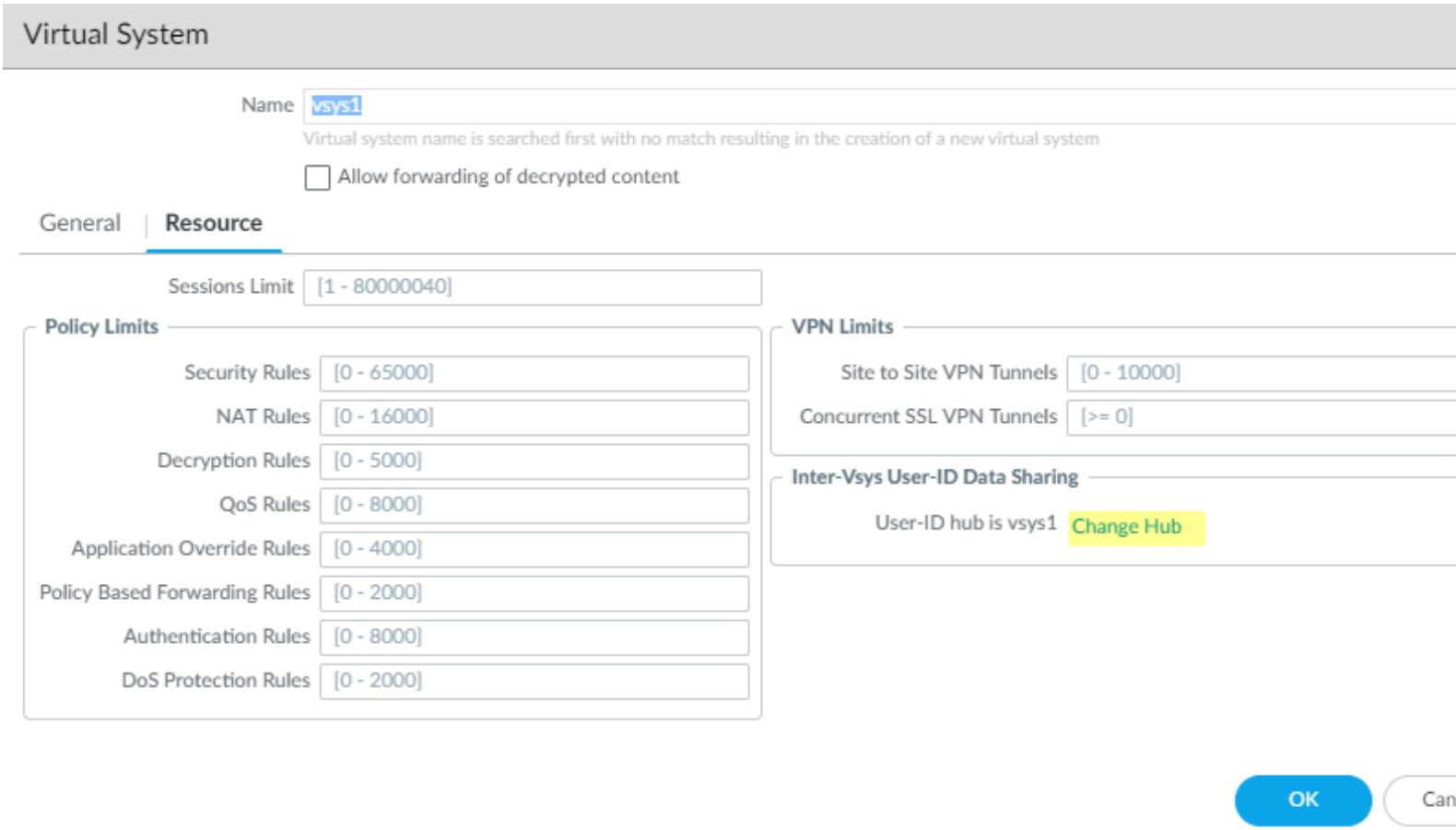
© 2020 Palo Alto Networks, Inc.



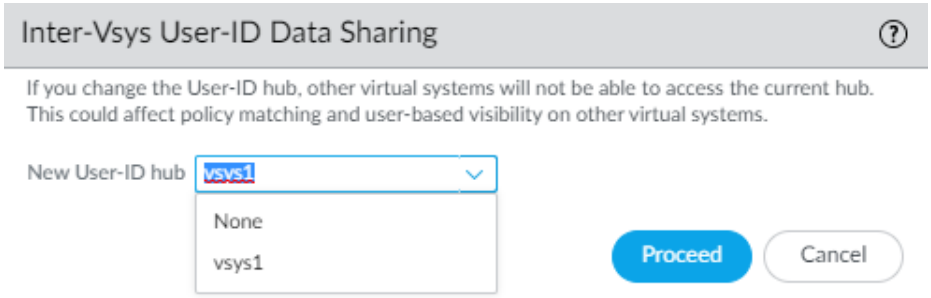
3. Haga clic en **Yes (Sí)** para confirmar la selección y, luego, haga clic en **OK (Aceptar)**.

   Si desea cambiar el núcleo de User-ID a otro sistema virtual o si quiere deshabilitarlo, seleccione el sistema virtual configurado como tal y, después, seleccione **Resource (Recurso)** > **Change Hub (Cambiar núcleo)**.

© 2020 Palo Alto Networks, Inc.



En la lista, seleccione otro núcleo en **New User-ID hub (Nuevo núcleo de User-ID)** o bien seleccione **none (ninguno)** para deshabilitarlo y dejar de compartir asignaciones entre los sistemas virtuales.



Haga clic en **Proceed (Continuar)** para confirmar los cambios.

STEP 6 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**. El sistema virtual es ahora un objeto accesible desde la pestaña **Objetos**.

STEP 7 | Cree al menos un enrutador virtual para el sistema virtual para que este sea capaz de realizar funciones de red, como el enrutamiento estático y dinámico.

Otra opción es que su sistema virtual use una VLAN o un Virtual Wire, dependiendo de su implementación.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y **Add (Añadir)** para añadir un enrutador virtual por **Name (Nombre)**.

© 2020 Palo Alto Networks, Inc.

2. En **Interfaces**, haga clic en **Add (Añadir)** y seleccione las interfaces que pertenecen al enrutador virtual.
3. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure una zona de seguridad para cada interfaz del sistema virtual.

Cree una zona de seguridad de capa 3 para al menos una interfaz. Consulte Configuración de interfaces y zonas.

STEP 9 | Configure las reglas de políticas de seguridad que permitan o denieguen el tráfico hacia y desde las zonas del sistema virtual.

Consulte Creación de una regla de política de seguridad.

STEP 10 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.



Una vez creado un sistema virtual, puede usar la CLI para confirmar una configuración para un sistema virtual específico únicamente:

```
commit partial vsys <vsys-id>
```

STEP 11 | (Opcional) Vea las políticas de seguridad configuradas para un sistema virtual.

Abra una sesión SSH para usar la CLI. Para ver las políticas de seguridad para un sistema virtual, en el modo operativo, use los siguientes comandos:

```
set system setting target-vsys <vsys-id>
```

```
show running security-policy
```


© 2020 Palo Alto Networks, Inc.

Configuración de la comunicación entre sistemas virtuales dentro del cortafuegos

Realice esta tarea si tiene un caso de uso, quizás en una única empresa, donde desee que los sistemas virtuales puedan comunicarse entre sí en el cortafuegos. Este escenario se describe en Tráfico entre VSYS que permanece dentro del cortafuegos. Para realizar esta tarea, se da por hecho que:

- Ha completado la tarea, la Configuración de sistemas virtuales.
- Durante la configuración de los sistemas virtuales, en el campo **Visible Virtual System (Sistema virtual visible)**, ha seleccionado las casillas de todos los sistemas virtuales que deben comunicarse entre sí para que sean visibles.

STEP 1 | Configure una zona externa para cada sistema virtual.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una nueva zona por **Name (Nombre)**.
2. En **Ubicación**, seleccione el sistema virtual para el que está creando una zona externa.
3. En **Tipo**, seleccione **Externa**.
4. En **Virtual Systems (Sistemas virtuales)**, haga clic en **Add (Añadir)** e introduzca el sistema virtual al que puede llegar la zona externa.
5. (Opcional) Seleccione un **Zone Protection Profile (Perfil de protección de zona)** (o configure uno más tarde) que proporcione protección contra desbordamiento, reconocimiento o ataques basados en paquetes.
6. (Opcional) En **Log Setting (Configuración de logs)**, seleccionar un perfil de reenvío de logs para reenviar los logs de protección de zona a un sistema externo.
7. (Opcional) Seleccione **Enable User Identification (Habilitar identificación de usuarios)** para habilitar el User-ID para la zona externa.
8. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure las reglas de la política de seguridad para permitir o denegar el tráfico desde las zonas internas a las externas del sistema virtual, y viceversa.

- Consulte Creación de una regla de política de seguridad.
- Consulte Tráfico entre VSYS que permanece en el cortafuegos.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Configuración de un gateway compartido

Realice esta tarea si necesita que múltiples sistemas virtuales compartan una interfaz (una puerta de enlace compartida) para internet. Para realizar esta tarea, se da por hecho que:

- Ha configurado una interfaz con una dirección IP enrutable globalmente, que será el gateway compartido.
- Ha completado el paso anterior, la Configuración de sistemas virtuales. Para la interfaz, ha seleccionado la interfaz externa con la dirección IP enrutable globalmente.
- Durante la configuración de los sistemas virtuales, en el campo **Visible Virtual System (Sistema virtual visible)**, ha seleccionado las casillas de todos los sistemas virtuales que deben comunicarse entre sí para que sean visibles.

STEP 1 | Configure una puerta de enlace compartida.

1. Seleccione **Device (Dispositivo)** > **Shared Gateway (Puerta de enlace compartida)**, y haga clic en **Add (Añadir)** e introduzca una **ID**.
2. Introduzca un **Name (Nombre)** útil, preferiblemente uno que incluya la **ID** de la puerta de enlace.
3. En el campo **DNS Proxy**, seleccione el objeto de proxy DNS si desea aplicar las reglas de proxy DNS a la interfaz.
4. **Añada** una **Interfaz** que conecte con el mundo exterior.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure la zona para el gateway compartido.

Cuando añade objetos como zonas o interfaces a una puerta de enlace compartida, esta aparece como un sistema virtual disponible en el menú de sistemas virtuales.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una nueva zona por **Name (Nombre)**.
2. En **Location (Ubicación)**, seleccione la puerta de enlace compartida para la que está creando una zona.
3. En **Type (Tipo)**, seleccione **Layer3 (Capa 2)**.
4. (Opcional) Seleccione un **Zone Protection Profile (Perfil de protección de zona)** (o configure uno más tarde) que proporcione protección contra desbordamiento, reconocimiento o ataques basados en paquetes.
5. (Opcional) En **Log Setting (Configuración de logs)**, seleccionar un perfil de reenvío de logs para reenviar los logs de protección de zona a un sistema externo.
6. (Opcional) Seleccione **Enable User Identification (Habilitar identificación de usuarios)** para habilitar el User-ID para la puerta de enlace compartida.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Personalización de rutas de servicio para un sistema virtual

Cuando se habilita un cortafuegos para múltiples sistemas virtuales, los sistemas virtuales heredan la configuración de servicio global y de ruta de servicio. Por ejemplo, el cortafuegos puede utilizar un servidor de correo electrónico compartido para originar alertas de correo electrónico en sus sistemas virtuales. En algunos casos, es posible que desee crear diferentes rutas de servicio para cada sistema virtual.

Un caso de uso para configurar rutas de servicio en el nivel de los sistemas virtuales es el de un ISP que necesita atender a múltiples empresas individuales en un único cortafuegos de Palo Alto Networks. Cada empresa requiere rutas de servicio personalizadas para el servicio de acceso como DNS, Kerberos, LDAP, NetFlow, RADIUS, TACACS+, autenticación multifactor, correo electrónico, captura de SNMP, Syslog, HTTP, agente de User-ID, supervisor de VM y Panorama (implementación de actualizaciones de contenido y software). Otro caso de uso es el de una organización de TI que quiere ofrecer autonomía completa a grupos que establecen servidores para servicios. Cada grupo puede contar con un sistema virtual y definir sus propias rutas de servicio.

Puede seleccionar un enrutador virtual para una ruta de servicio en un sistema virtual; no puede seleccionar la interfaz de salida. Después de seleccionar el enrutador virtual y de que el cortafuegos envíe el paquete desde el enrutador virtual, el cortafuegos selecciona la interfaz de salida basándose en la dirección IP de destino. Por lo tanto, si un sistema virtual tiene múltiples enrutadores virtuales, los paquetes dirigidos a todos los servidores para un servicio deben salir de un único enrutador virtual. Un paquete con una dirección de origen de interfaz puede salir de una interfaz diferente, pero el tráfico de retorno estaría en la interfaz que tiene la dirección IP de origen, creando así tráfico asimétrico.

- Personalización de rutas de servicio a servicios para un sistema virtual
- Configure un cortafuegos PA-7000 Series para logging por sistema virtual
- Configuración de acceso administrativo por sistema virtual o cortafuegos

Personalización de rutas de servicio a servicios para un sistema virtual

Cuando habilita la capacidad para múltiples sistemas virtuales, cualquier sistema virtual que no tenga rutas de servicio específicas configuradas hereda la configuración de las rutas de servicio y el servicio global para el cortafuegos. En cambio, puede configurar un sistema virtual para que utilice una ruta de servicio diferente, como se describe en el siguiente flujo de trabajo.

Un cortafuegos con múltiples sistemas virtuales debe tener interfaces y subinterfaces con direcciones IP no superpuestas. Una ruta de servicios por sistema virtual para las capturas SNMP o para Kerberos solo es compatible con IPv4.

La ruta de servicio de un servicio respeta estrictamente lo que configuró en el perfil del servidor para el servicio:

- Si define un perfil de servidor (**Device [Dispositivo]** > **Server Profiles [Perfiles de servicio]**) para la ubicación compartida, el cortafuegos utiliza la ruta de servicio global de ese servicio.
- Si define un perfil de servidor para un sistema virtual específico, el cortafuegos utiliza la ruta de servicio para el sistema virtual específico para ese servicio.
- Si define un perfil de servidor para un sistema virtual específico, pero la ruta de servicio para el sistema virtual específico no se configura, el cortafuegos utiliza la ruta de servicio global para ese servicio.

© 2020 Palo Alto Networks, Inc.

El cortafuegos admite reenvío de syslog en sistemas virtuales. Cuando hay más de un sistema virtual en un cortafuegos conectándose a un servidor de syslog mediante transporte SSL, el cortafuegos puede generar solo un certificado de comunicación segura. El cortafuegos no admite que cada sistema virtual tenga su propio certificado.

STEP 1 | Personalice rutas de servicio para un sistema virtual.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Virtual Systems (Sistemas virtuales)**, y seleccione el sistema virtual que desea configurar.
2. Haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.
3. Seleccione una opción:
   - **Inherit Global Service Route Configuration**: hace que el sistema virtual herede la configuración de la ruta de servicio global pertinente para un sistema virtual. Si selecciona esta opción, puede omitir el paso de personalización.
   - **Customize (Personalizar)**: le permite especificar una dirección de origen para cada servicio.
4. Si ha elegido **Customize (Personalizar)**, seleccione la pestaña **IPv4** o **IPv6**, dependiendo del tipo de direccionamiento que use el servidor que ofrece el servicio. Puede especificar direcciones tanto IPv4 como IPv6 para un servicio. Haga clic en un servicio. (Solo están disponibles los servicios relevantes para un sistema virtual).

   Para utilizar la misma dirección de origen en varios servicios, seleccione la casilla de verificación de los servicios, haga clic en Set Selected Routes (Establecer rutas seleccionadas) y continúe.

   - Para limitar la lista de direcciones de origen, seleccione una interfaz en **Source Interface (Interfaz de origen)** y, luego, una dirección de esa interfaz en Source Address (Dirección de origen) como ruta de servicio. Si selecciona **Any (Cualquiera)** en Source Interface (Interfaz de origen), están disponibles todas las direcciones IP de todas las interfaces del sistema virtual en la lista Source Address (Dirección de origen) en la que debe seleccionar una dirección. Puede seleccionar **Inherit Global Setting (Heredar configuración global)**.
   - En **Source Address (Dirección de origen)**, se indicará **Inherited (Heredada)** si ha seleccionado **Inherit Global Setting (Heredar configuración global)** para la **Source Interface (Interfaz de origen)** o indicará la dirección de origen que seleccionó. Si ha seleccionado **Any (Cualquiera)** en **Source Interface (Interfaz de origen)**, seleccione la dirección IP de origen que se debe usar en los paquetes enviados al servicio externo o introdúzcala con el formato de IPv4 o IPv6 correspondiente a la pestaña elegida.
   - Si modifica un objeto de dirección y el tipo de familia IP (IPv4/IPv6) cambia, es necesaria una **confirmación** para actualizar la familia de ruta de servicio que se usará.
5. Haga clic en **OK (Aceptar)**.
6. Repita los pasos anteriores para configurar direcciones de origen para otros servicios externos.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

Haga clic en **Commit** y en **OK**.

Si está configurando rutas de servicio por sistema virtual para servicios de creación de logs de un cortafuegos serie PA-7000, continúe con la tarea Configuración de un cortafuegos serie PA-7000 para la creación de logs por sistema virtual.

© 2020 Palo Alto Networks, Inc.

Configure un cortafuegos PA-7000 Series para logging por sistema virtual

El cortafuegos PA-7000 Series no emplea las rutas de servicio para los servicios de captura de SNMP, syslog y correo electrónico en los logs de estos tipos: Traffic (Tráfico), HIP Match (Coincidencia con HIP), Threat (Amenazas) y WildFire. En su lugar, permite utilizar tarjetas de almacenamiento de logs.

El cortafuegos puede tener uno de los tipos de tarjetas siguientes en función de su configuración:

- **Tarjeta de procesamiento de logs (log processing card, LPC)**: admite rutas específicas del sistema virtual desde las subinterfaces de LPC hasta un conmutador local al servicio correspondiente de un servidor. Para los logs de Sistema y Configuración, el cortafuegos PA-7000 Series usa rutas de servicio globales, no la LPC. Si el cortafuegos tiene instalada una LPC, debe configurar un puerto para la tarjeta de logs.
- **Tarjeta de reenvío de logs (log forwarding card, (LFC)**: admite el reenvío a gran velocidad de todos los logs de planos de datos a un recopilador de logs externo, por ejemplo, Panorama o servidores de syslog. Puede crear y configurar subinterfaces para los sistemas virtuales. Si el cortafuegos tiene instalada una LFC, no hace falta que configure un puerto para la tarjeta de logs.

En otros modelos de Palo Alto Networks, el plano de datos envía tráfico de rutas de servicio de creación de logs al plano de gestión, que envía el tráfico a los servidores de creación de logs. En los cortafuegos PA-7000 Series, la LPC o la LFC solo tienen una interfaz, y los planos de datos de varios sistemas virtuales envían el tráfico de los servidores de creación de logs (de los tipos antes mencionados) a la tarjeta de almacenamiento de logs del cortafuegos. La tarjeta de almacenamiento de logs está configurada con varias subinterfaces. Por medio de ellas, la plataforma envía el tráfico del servicio de creación de logs al conmutador del cliente, que puede estar conectado a distintos servidores de creación de logs.

Cada subinterfaz se puede configurar con un nombre de subinterfaz y un número de subinterfaz delimitado por puntos. La subinterfaz se asigna a un sistema virtual, que se configura para servicios de logging. Las otras rutas de servicio en un cortafuegos PA-7000 Series funcionan de modo similar a las rutas de servicio en otras plataformas de Palo Alto Networks. Para obtener información sobre la LPC o la LFC, consulte la guía de referencia del hardware de PA-7000 Series.

- Configuración de LPC de PA-7000 Series para el almacenamiento de logs por sistema virtual
- Configuración de LFC de PA-7000 Series para el almacenamiento de logs por sistema virtual

Configuración de LPC de PA-7000 Series para el almacenamiento de logs por sistema virtual

En los cortafuegos PA-7000 Series, si habilita la opción para usar varios sistemas virtuales e instala una tarjeta de procesamiento de logs (log processing card, LPC), puede configurar la creación de logs de diferentes sistemas virtuales como se describe en el siguiente flujo de trabajo.

STEP 1 | Cree una subinterfaz de Tarjeta de logs.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione la interfaz oportuna para la tarjeta de logs.
2. Introduzca el **Interface Name**.
3. En **Interface Type (Tipo de interfaz)**, seleccione **Log Card (Tarjeta de logs)**.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Añada una subinterfaz para cada usuario en la interfaz física de LPC.

1. Resalte la interfaz Ethernet que es un tipo de interfaz de tarjeta de logs y haga clic en **Add Subinterface**.

© 2020 Palo Alto Networks, Inc.

2. Para **Interface Name (Nombre de interfaz)**, introduzca la subinterfaz asignada al sistema virtual del usuario.
3. Para **Tag (Etiqueta)**, introduzca un valor de etiqueta VLAN.

   Se recomienda que la etiqueta coincida con el número de subinterfaz para facilitar su uso, aunque pueden tener números diferentes.
4. (Opcional) Introduzca un **Comment (Comentario)**.
5. En el campo **Assign Interface to Virtual System (Asignar interfaz a sistema virtual)** de la pestaña **Config (Configuración)**, seleccione el sistema virtual al que se debe asignar la subinterfaz de LPC. O bien, puede hacer clic en **Virtual Systems** para añadir un nuevo sistema virtual.
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Introduzca la dirección asignada a la subinterfaz y configure la gateway predeterminada.

1. Seleccione la pestaña **Log Card Forwarding** y realice uno de estos dos pasos, o ambos:
   - Para la sección IPv4, introduzca la **IP Address (Dirección IP)** y la **Netmask (Máscara de red)** asignada a la subinterfaz. Introduzca la **Default Gateway (Puerta de enlace predeterminada)** (el siguiente salto al que se enviarán los paquetes que no tengan dirección de siguiente salto conocida en la base de información de enrutamiento [RIB]).
   - Para la sección IPv6, introduzca la **IPv6 Address** asignada a la subinterfaz. Introduzca la **IPv6 Default Gateway (Puerta de enlace predeterminada IPv6)**.
2. Haga clic en **OK (Aceptar)**.

STEP 4 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

STEP 5 | Si aún no lo ha hecho, configure las rutas de servicio restantes para el sistema virtual.

Personalización de rutas de servicio para un sistema virtual.

Configuración de LFC de PA-7000 Series para el almacenamiento de logs por sistema virtual

En los cortafuegos PA-7000 Series, si habilita la opción para usar varios sistemas virtuales e instala una tarjeta de reenvío de logs (log forwarding card, LFC), puede configurar la creación de logs de diferentes sistemas virtuales como se describe en el siguiente flujo de trabajo.

STEP 1 | Cree una subinterfaz de LFC.

1. Seleccione **Device (Dispositivo)** > **Log Forwarding Card (Tarjeta de reenvío de logs)** y añada una subinterfaz.
2. Para **Interface Name (Nombre de interfaz)**, introduzca la subinterfaz asignada al sistema virtual del usuario.
3. (Opcional) Introduzca un **Comment (Comentario)**.
4. Para **Tag (Etiqueta)**, introduzca un valor de etiqueta VLAN.

   Se recomienda que la etiqueta coincida con el número de subinterfaz para facilitar su uso, aunque pueden tener números diferentes.
5. En el campo **Assign Interface to Virtual System (Asignar interfaz a sistema virtual)** de la pestaña **Config (Configuración)**, seleccione el sistema virtual al que se debe asignar la subinterfaz de LFC. O bien, puede hacer clic en **Virtual Systems** para añadir un nuevo sistema virtual.
6. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | (Opcional) Introduzca las direcciones asignadas a la subinterfaz y configure la puerta de enlace predeterminada.

1. Seleccione la pestaña **Network (Red)** y realice una de estas opciones o ambas:
   - Para la sección IPv4, introduzca la **IP Address (Dirección IP)** y la **Netmask (Máscara de red)** asignada a la subinterfaz. Introduzca la **Default Gateway (Puerta de enlace predeterminada)** (el siguiente salto al que se enviarán los paquetes que no tengan dirección de siguiente salto conocida en la base de información de enrutamiento [RIB]).
   - Para la sección IPv6, introduzca la **IPv6 Address** asignada a la subinterfaz. Introduzca la **IPv6 Default Gateway (Puerta de enlace predeterminada IPv6)**.
2. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Configuración de acceso administrativo por sistema virtual o cortafuegos

Si tiene una cuenta de administración de superusuario, puede crear y configurar permisos granulares para una función de administración de dispositivo o vsysadmin.

STEP 1 | Cree un perfil de función de administrador que conceda o deniegue el permiso de un administrador para configurar o tener acceso de solo lectura a diversas áreas de la interfaz web.

1. Seleccione **Device (Dispositivo)** > **Admin Roles (Funciones de administración)** y **Add (Añadir)** para añadir un **Admin Role Profile (Perfil de función de administración)**.
2. Introduzca un nombre en **Name** y una **Description (Descripción)** opcional del perfil.
3. Para **Role**, especifique el nivel de control al que afecta el perfil:
   - **Device (Dispositivo)**: el perfil permite gestionar la configuración global y cualquier sistema virtual.
   - **Virtual System (Sistema virtual)**: el perfil permite gestionar solo los sistemas virtuales asignados al administrador que tiene este perfil. (El administrador podrá acceder a **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Virtual Systems [Sistemas virtuales]**, pero no a la pestaña **Global**).
4. En la pestaña **Web UI** del perfil Admin Role Profile, desplácese hacia abajo hasta **Device** y deje la marca de verificación verde.
   - En **Device**, habilite **Setup**. En **Setup**, habilite las áreas a las que este perfil concederá acceso para el administrador, como se muestra a continuación. (El icono de solo lectura aparece en la rotación Habilitar/Deshabilitar si Solo lectura está habilitado para esa configuración).
     - **Management**: permite a un administrador con este perfil configurar ajustes en la pestaña **Management**.
     - **Operations**: permite a un administrador con este perfil configurar ajustes en la pestaña **Operations**.
     - **Services**: permite a un administrador con este perfil configurar ajustes en la pestaña **Services**. Un administrador debe haber habilitado los **Services (Servicios)** para acceder a la pestaña **Device (Dispositivo)** > **Setup Services (Servicios de configuración)** > **Virtual Systems (Sistemas virtuales)**. Si el campo **Role (Función)** se especificó como **Virtual System (Sistema virtual)** en el paso anterior, el campo **Services (Servicios)** es el único ajuste que se puede habilitar en **Device (Dispositivo)** > **Setup (Ajustes)**.
     - **Content-ID**: permite a un administrador con este perfil configurar ajustes en la pestaña **Content-ID**.
     - **WildFire**: permite a un administrador con este perfil configurar ajustes en la pestaña **WildFire**.

© 2020 Palo Alto Networks, Inc.

- **Session (Sesión)**: permite a un administrador con este perfil configurar ajustes en la pestaña **Session**.
- **HSM**: permite a un administrador con este perfil configurar ajustes en la pestaña **HSM**.

5. Haga clic en **OK (Aceptar)**.
6. (Opcional) Repite el paso completo para completar otro perfil de Función de administrador con diferentes permisos, según sea necesario.

STEP 2 | Aplique el perfil de función de administrador a un administrador.

1. Seleccione **Device (Dispositivo)** > **Administrators (Administradores)**, haga clic en **Add (Añadir)** e introduzca un nombre en **Name (Nombre)** para añadir un administrador.
2. (Opcional) Seleccione un **Authentication Profile (Perfil de autenticación)**.
3. (Opcional) Seleccione **Use only client certificate authentication (Utilizar solo la autenticación de certificado de cliente) (Web)** para autenticación bidireccional; para que el servidor autentique al cliente.
4. Introduzca una **Password** y seleccione **Confirm Password**.
5. (Opcional) Seleccione **Use Public Key Authentication (Utilizar autenticación de clave pública) (SSH)** si desea utilizar un método de autenticación mucho más fuerte basado en clave con una clave pública SSH en lugar de solo una contraseña.
6. Para **Administrator Type**, seleccione **Role Based**.
7. En **Profile**, seleccione el perfil que acaba de crear.
8. (Opcional) Seleccione un **Password Profile (Perfil de contraseña)**.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

Haga clic en **Commit (Confirmar)**.

© 2020 Palo Alto Networks, Inc.

Funcionalidad de sistema virtual con otras funciones

Muchas de las características y funcionalidades del cortafuegos pueden configurarse, verse, registrarse en logs o incluirse en informes por sistema virtual. Así, los sistemas virtuales se mencionan en otras ubicaciones relevantes de la documentación, y esa información no se repite aquí. Algunos de los capítulos específicos son los siguientes:

- Si está configurando la HA activa/pasiva, los dos cortafuegos deben tener la misma funcionalidad del sistema virtual (funcionalidad de sistema virtual múltiple o único). Consulte High Availability.
- Para configurar la calidad de servicio (quality of service, QoS) en los sistemas virtuales, consulte Configuración de QoS para un sistema virtual.
- Para obtener información sobre la configuración de cortafuegos con sistemas virtuales en una implementación de cable virtual que utilice subinterfaces (y etiquetas de VLAN), consulte Interfaces de cable virtual.
- Si configura User-ID y varios sistemas virtuales, puede compartir entre ellos las asignaciones de usuarios. Consulte Asignaciones de User-ID compartidas entre sistemas virtuales.

Protección de zona y protección contra DoS

La segmentación de la red en zonas funcionales y organizativas reduce la superficie de ataque de la red (la parte de la red y su tráfico expuestos a posibles atacantes). La protección de zona defiende a las zonas de red de los ataques de inundación, intentos de reconocimiento, ataques basados en paquetes y ataques que usan protocolos no IP. Ajuste un perfil de protección de zona para proteger cada zona (puede aplicar el mismo perfil a zonas similares). La protección de Denegación de servicio (Denial-of-service, DoS) defiende los sistemas críticos específicos de los ataques de inundación, en especial, los dispositivos que un usuario accede desde Internet, como servidores web y de bases de datos, y protege los recursos de las inundaciones de sesión. Ajuste los perfiles de protección DoS y las reglas de política para proteger cada conjunto de dispositivos importantes. Visite el portal de documentación recomendado para obtener una lista de comprobación de las recomendaciones de protección DoS y de protección de zona.



Compruebe y supervise el consumo de CPU del plano de datos en el cortafuegos para garantizar que cada cortafuegos tenga el tamaño adecuado para admitir la protección DoS y de zona junto con cualquier otra función que consuma ciclos de CPU, como el descifrado. Si usa Panorama para administrar los cortafuegos, use la supervisión de dispositivos (Panorama > Managed Devices [Dispositivos administrados] > Health [Estado]) para revisar y supervisar el consumo de CPU de todos los cortafuegos administrados a la vez.

- Segmentación de la red con zonas
- ¿Cómo las zonas protegen la red?
- Defensa de zona
- Configuración de la protección de la zona para aumentar la seguridad de la red
- Protección DoS contra inundaciones de nuevas sesiones

© 2020 Palo Alto Networks, Inc.

Segmentación de la red con zonas

Cuanto mayor es la red, más difícil es protegerla. Una red extensa y sin segmentar presenta una gran superficie de ataque que puede resultar difícil de administrar y proteger. Dado que el tráfico y las aplicaciones tienen acceso a toda la red, cuando un atacante accede a una red, este puede moverse lateralmente en una red para acceder a datos críticos. Además, una red extensa es más difícil de supervisar y controlar. La segmentación de la red limita la capacidad de un atacante de moverse por la red evitando el movimiento lateral entre las zonas.

Una zona de seguridad es un grupo de uno o más cortafuegos físicos o virtuales, y los segmentos de red conectados a las interfaces de la red. Puede controlar la protección de cada zona de manera individual, de modo que cada zona reciba la protección específica que necesita. Por ejemplo, es posible que una zona del departamento de finanzas no deba permitir todas las aplicaciones que permite una zona para TI.

Para proteger su red completamente, todo el tráfico debe fluir por el cortafuegos. Realice la Configuración de interfaces y zonas para crear zonas separadas para las diferentes áreas funcionales como la puerta de enlace de internet, el almacenamiento de datos confidenciales y las aplicaciones empresariales, y para los diferentes grupos de las organizaciones, como finanzas, TI, marketing e ingeniería. Siempre que exista una división lógica de la funcionalidad, el uso de la aplicación o los privilegios de acceso de los usuarios, podrá crear una zona separada para aislar y proteger el área, y aplicar las reglas adecuadas de la política de seguridad para evitar el acceso innecesario a los datos y las aplicaciones a los que solo deben acceder uno o algunos grupos. Cuanto más detalladas sean las zonas, mayores serán la visibilidad y el control que posee del tráfico de la red. La división de su red en zonas ayuda a crear una arquitectura de Zero Trust (confianza cero) que ejecuta una filosofía de seguridad basada en la ausencia de confianza en los usuarios, los dispositivos, las aplicaciones o los paquetes, donde se comprueba todo. El objetivo final es crear una red que permita el acceso solo a los usuarios, los dispositivos y las aplicaciones que posean necesidades empresariales legítimas, y denegar el resto del tráfico.

La restricción y el permiso de acceso adecuados a las zonas dependen del entorno de la red. Por ejemplo, es posible que los entornos como las plantas de producción de semiconductores o las plantas de montaje robótico, donde las estaciones de trabajo controlan equipo industrial delicado, o áreas con acceso muy restringido, requieran una segmentación física que no permita que los dispositivos externos accedan (sin acceso desde dispositivos móviles).

En los entornos donde los usuarios pueden acceder a la red con dispositivos móviles, la habilitación de User-ID y App-ID, además de la segmentación de red en zonas garantiza que los usuarios recibirán los privilegios de acceso adecuados independientemente de desde dónde accedan a la red, dado que los privilegios de acceso se encuentran vinculados a un usuario o a un grupo de usuarios, en lugar de a un dispositivo en una zona particular.

Es posible que los requisitos de protección de las diferentes áreas y grupos funcionales varíen. Por ejemplo, es posible que una zona que maneja una gran cantidad de tráfico requiera umbrales de protección contra inundaciones diferentes a los de una zona que, por lo general, gestiona menos tráfico. La capacidad de definir la protección adecuada para cada zona es otro motivo para segmentar la red. La protección adecuada depende de su arquitectura de red, lo que desea proteger y el tráfico que desea permitir y denegar.

© 2020 Palo Alto Networks, Inc.

¿Cómo las zonas protegen la red?

Las zonas no solo protegen su red segmentándola en áreas más pequeñas que se administran con mayor facilidad; las zonas también protegen la red debido a que puede controlar el acceso a las zonas y el movimiento de tráfico entre zonas.

Las zonas evitan que el tráfico no controlado fluya por las interfaces del cortafuegos hacia su red debido a que las interfaces del cortafuegos no pueden procesar tráfico hasta que las asigne a las zonas. El cortafuegos aplica la protección de zona a las interfaces de ingreso, donde el tráfico ingresa al cortafuegos en dirección del flujo desde el cliente de origen al servidor que responde (c2s) para filtrar el tráfico antes de que ingrese a una zona.

El tipo de interfaz y el tipo de zona del cortafuegos (de modo tap, cable virtual, L2, L3, túnel o externo) deben coincidir, lo que permite proteger la red contra el tráfico admitido que no pertenece a la zona. Por ejemplo, puede asignar una interfaz L2 a una zona L2 o una interfaz L3 a una zona L3, pero no puede asignar una interfaz L2 a una zona L3.

Además, una interfaz del cortafuegos puede pertenecer solo a una zona. El tráfico destinado a diferentes zonas no puede utilizar la misma interfaz, lo que permite evitar que el tráfico inadecuado ingrese a una zona y le permite configurar la protección adecuada para cada zona individual. Puede conectar más de una interfaz del cortafuegos a una zona para aumentar el ancho de banda, pero cada interfaz se puede conectar solo a una zona.

Una vez que el cortafuegos permita tráfico en una zona, el tráfico fluye libremente dentro de la zona y no se registra. Cuanto más detallada es una zona, mayor será el control que tendrá sobre el tráfico que accede a cada zona, y mayor será la dificultad para que el malware se mueva lateralmente dentro de la red entre las zonas. El tráfico no puede fluir entre las zonas a menos que una regla de la política de seguridad lo permita y las zonas sean del mismo tipo (de modo tap, cable virtual, L2, L3, túnel o externa). Por ejemplo, una regla de la política de seguridad puede permitir el tráfico entre dos zonas L3, pero no entre una zona L3 y una zona L2. El cortafuegos registra el tráfico que fluye entre las zonas cuando una regla de la política de seguridad permite el tráfico entre las zonas.

De manera predeterminada, las reglas de la política de seguridad evitan el movimiento lateral del tráfico entre las zonas, de modo que el malware no pueda acceder a una zona y moverse libremente dentro de la red hacia otros destinos.



Las zonas del túnel son para túneles no cifrados. Puede aplicar diferentes reglas de la política de seguridad al contenido del túnel y a la zona del túnel externo, como se describe en Descripción general de la inspección del contenido del túnel*.*

© 2020 Palo Alto Networks, Inc.

Defensa de zona

Los perfiles de protección de zona defienden las zonas de ataques basados en protocolos no IP, paquetes, reconocimiento y congestión. Los perfiles de protección DoS utilizados en las reglas de política de protección DoS defienden a los dispositivos críticos específicos de ataques basados en recursos y congestión. Un ataque de DoS sobrecarga la red o los sistemas críticos orientados con grandes cantidades de tráfico no deseado con el fin de interrumpir los servicios de la red.

Cree un plan para defender su red de los diferentes tipos de ataques DoS:

- **Ataques basados en aplicaciones:** aborde las debilidades de una aplicación determinada e intente agotar sus recursos para los usuarios legítimos no puedan usarla. Un ejemplo de ello es el ataque Slowloris.
- **Ataques basados en protocolos**: también denominados como ataques de agotamiento de estado, estos ataques apuntan a los puntos débiles del protocolo. Un ejemplo común es un ataque de congestión de SYN.
- **Ataques volumétricos:** ataques de gran volumen que intentan sobrecargar los recursos de red disponibles, especialmente el ancho de banda, y derribar el objetivo para evitar que los usuarios legítimos accedan a estos recursos. Un ejemplo de ello es un ataque de congestión de UDP.

No existen perfiles de protección de zona o perfiles de protección DoS y reglas de la política de protección DoS predeterminados. Configure y aplique la protección de zona en función de las características de tráfico de cada zona y configure la protección DoS sobre la base de los sistemas críticos que desea proteger en cada zona.

- Herramientas de defensa de zona
- ¿Cómo funcionan las herramientas de defensa de zona?
- Selección de ubicación del cortafuegos para la protección DoS
- Perfiles de protección de zonas
- Protección de búfer de paquetes
- Perfiles de protección y reglas de la política del DoS

Herramientas de defensa de zona

Una defensa efectiva contra los ataques DoS requiere un enfoque en capas. La primera capa de defensa debe ser un dispositivo dedicado de protección DDoS de gran volumen en el perímetro de red accesible desde Internet y un enrutador de perímetro, conmutador u otro dispositivo de descarte de paquetes basado en hardware con las listas de control de acceso (access control lists, ACL) apropiadas para defenderse de ataques volumétricos para los que el cortafuegos basado en sesiones no está diseñado. El cortafuegos añade capas más detalladas de defensa de ataque DoS y visibilidad en el tráfico de la aplicación que no proporcionan los dispositivos DDoS dedicados.

Los cortafuegos de Palo Alto Networks proporcionan herramientas complementarias a la protección DoS para sus zonas de red y dispositivos importantes:

- Los **Perfiles de protección de zona** defienden el borde de la zona de entrada contra ataques de inundación de IP, análisis de puertos de reconocimiento y barridos de host, ataques basados en paquetes de IP y ataques de protocolo no IP. La zona de entrada es donde el tráfico entra en el cortafuegos en la dirección del flujo desde el cliente hacia el servidor (client-to-server, c2s), donde el cliente es el originador del flujo y el servidor es el respondedor. Los perfiles de protección de zona proporcionan una segunda capa de defensa amplia contra los ataques DoS, en función del tráfico agregado que entra en la zona, mediante la imposición de un límite a las conexiones por segundo (connections-per-second, CPS) nuevas a la zona. Los perfiles de protección de zona no tienen en cuenta los dispositivos individuales (direcciones IP) porque los perfiles se aplican al tráfico agregado que entra a la zona.

© 2020 Palo Alto Networks, Inc.

Los perfiles de protección de zona protegen la red a medida que se forma la sesión, antes de que el cortafuegos realice búsquedas de regla de política de seguridad y política de protección DoS, y consume menos ciclos de CPU que una búsqueda de regla de política de seguridad o política de protección DoS. Si un perfil de protección de zona deniega el tráfico, el cortafuegos no emplea ciclos de CPU en las búsquedas de regla de política.

Aplique perfiles de protección de zona en cada zona, tanto en las internas como en las accesibles desde Internet.

- Los **perfiles de protección DoS y las reglas de política** protegen los recursos y endpoints individuales de los ataques de inundación, en especial, los objetivos de gran valor a los que los usuarios acceden desde Internet. Mientras que el perfil de protección de zona defiende la zona de los ataques de inundación, una regla de política de protección DoS con un perfil de protección DoS apropiado defiende los sistemas individuales importantes de una zona de los ataques de inundación orientados, lo que proporciona una tercera capa detallada de defensa contra los ataques DoS.

  Debido a que el objetivo de la protección DoS es defender los dispositivos importantes y debido a que consume recursos, esta protección defiende solo los dispositivos que especifique en una regla de política de protección DoS. No se protegen otros dispositivos.

  Los perfiles de protección DoS establecen umbrales de protección contra inundación (límites de CPS nuevas) para dispositivos individuales o grupos de dispositivos, umbrales de protección de recursos (límites de sesión para endpoints y recursos especificados) y si el perfil se aplica al tráfico agregado o clasificado. Las reglas de política de la protección DoS especifican criterios de coincidencia (origen, destino, puerto de servicio), la acción que debe llevarse a cabo cuando el tráfico coincide con la regla y los perfiles de protección DoS agregados y clasificados que están asociados con cada regla.

  Las reglas de política de la protección DoS *agregada* aplican los umbrales de CPS definidos en un perfil de protección DoS agregado al tráfico combinado de todos los dispositivos que cumplen con los criterios de coincidencia de la regla de política de protección DoS. Por ejemplo, si configura el perfil de protección DoS agregado para que limite la tasa de CPS a 20 000, este límite se aplica a la cantidad agregada de conexiones para todo el grupo. En este caso, un dispositivo podrá recibir la mayoría de las conexiones permitidas.

  Las reglas de política de la protección DoS *clasificada* aplican los umbrales de CPS definidos en un perfil de protección DoS clasificado a cada dispositivo individual que coincida con la regla de política. Por ejemplo, si configura el perfil de protección DoS clasificado para que limite la tasa de CPS a 4000, entonces ningún dispositivo del grupo podrá aceptar más de 4000 CPS. Una política de protección DoS puede tener un perfil agregado y un perfil clasificado.

  Los perfiles clasificados pueden clasificar las conexiones por IP de origen, IP de destino o ambas. Para las zonas accesibles desde Internet, clasifique únicamente por IP de destino porque el cortafuegos no puede aumentar la escala para cumplir la tabla de enrutamiento de Internet.

  Aplique la protección DoS solo a dispositivos importantes, en especial, a los que acceden los usuarios desde Internet y que sean el objetivo de ataques populares, como servidores web y de bases de datos.
- En las sesiones existentes, la **protección del búfer de paquetes** protege el cortafuegos (y, por lo tanto, la zona) de ataques DoS de sesión única que intentan sobrecargar el búfer de paquetes del cortafuegos, mediante el uso de umbrales y temporizadores para mitigar las sesiones abusivas. Configure la protección de búfer de paquetes de manera global y aplique esta configuración por zona.
- Las **reglas de política de seguridad** influyen tanto en el flujo de entrada como en el de salida de una sesión. Para establecer una sesión, el tráfico entrante debe coincidir con una regla de política de seguridad. Si no hay coincidencia, el cortafuegos descarta el paquete. Una política de seguridad permite

© 2020 Palo Alto Networks, Inc.

o rechaza el tráfico entre zonas (interzona) y dentro de las zonas (intrazona) usando criterios que incluyen zonas, direcciones IP, usuarios, aplicaciones, servicios y categorías URL.



Aplique el perfil de protección frente a vulnerabilidades recomendado a cada regla de política de seguridad para defenderla de los ataques DoS.

Las reglas de política de seguridad predeterminadas no permiten que el tráfico se desplace entre zonas, por lo que necesita configurar una regla de política de seguridad si desea permitir el tráfico interzona. Todo el tráfico intrazona está permitido de manera predeterminada. Puede configurar reglas de política de seguridad para cotejar y controlar el tráfico intrazona, interzona o universal (intrazona e interzona).



Los perfiles de protección de zona, los perfiles de protección DoS y las reglas de política, y las reglas de política de seguridad solo afectan al tráfico del plano de datos en el cortafuegos. El tráfico que se origina en la interfaz de gestión del cortafuegos no cruza el plano de datos, por lo que el cortafuegos no coteja el tráfico de gestión con estos perfiles o reglas de política.

- También puede buscar amenazas por hash, CVE, ID de firma, nombre de dominio, URL o dirección IP en la base de datos de amenazas de Palo Alto Networks (se requiere un inicio de sesión y cuenta de soporte válidos).

¿Cómo funcionan las herramientas de defensa de zona?

Cuando un paquete llega al cortafuegos, este intenta que el paquete coincida con una sesión existente, en función de una zona de ingreso, una zona de salida, una dirección IP de origen, una dirección IP de destino, un protocolo y una aplicación que se obtiene del encabezado del paquete. Si el cortafuegos encuentra una coincidencia, el paquete utiliza las reglas de la política de seguridad que ya controlan la sesión. Si el paquete no coincide con una sesión existente, el cortafuegos utiliza perfiles de protección zona, reglas de la política y perfiles de protección DoS, y reglas de la política de seguridad para determinar si establecer una sesión o descartar el paquete, y el nivel de acceso que recibe el paquete.

Después de que el tráfico pase por su dispositivo DDoS dedicado en el límite de red accesible desde Internet, la primera protección que aplica el cortafuegos es la defensa amplia del perfil de protección de zona, si está adjunto a la zona. El cortafuegos determina la zona de la interfaz donde llega el paquete (cada interfaz se asigna solo a una zona y todas las interfaces que transfieren tráfico deben pertenecer a una zona). Si el perfil de protección de zona rechaza el paquete, el cortafuegos lo descarta y ahorra los recursos al no tener que buscar la política de seguridad o de protección DoS. El cortafuegos aplica perfiles de protección de zona solo en las sesiones nuevas (los paquetes que no coinciden con una sesión existente). Una vez que el cortafuegos establece una sesión, este elude la búsqueda de los paquetes correctos en los perfiles de protección de zona en esa sesión.

Si el perfil de protección de zona no descarta el paquete, la segunda protección que aplica el cortafuegos es una regla de política de protección DoS. Si un perfil de protección de zona permite un paquete en función de la cantidad total de tráfico hacia la zona, es posible que una regla de la política de protección DoS rechace el paquete si se dirige a un destino particular o si proviene de un origen determinado que superó la configuración de protección contra inundaciones o de protección de recursos en el perfil de protección DoS de la regla. Si el paquete coincide con una regla de la política de protección DoS, el cortafuegos aplica la regla al paquete. Si la regla rechaza el acceso, el cortafuegos descarta el paquete y no realiza la búsqueda en la política de seguridad. Si la regla permite el acceso, el cortafuegos realiza la búsqueda en la política de seguridad. Al igual que el perfil de protección de zona, el cortafuegos aplica la política de protección DoS solo en las sesiones nuevas.

La tercera protección que aplica el cortafuegos es una búsqueda en la política de seguridad, que sucede solo si el perfil de protección de zona y las reglas de la política de protección DoS permiten el paquete. Si el cortafuegos no encuentra una coincidencia con el paquete en la regla de la política de seguridad, descarta el paquete. Si el cortafuegos encuentra una coincidencia en la regla de la política de seguridad, aplica la regla en el paquete. El cortafuegos aplica la regla de la política de seguridad en el tráfico en ambas

© 2020 Palo Alto Networks, Inc.

direcciones (c2s y s2c) por la duración de la sesión. Aplique el perfil de protección frente a vulnerabilidades recomendado en todas las reglas de política de seguridad para defenderlas de los ataques DoS.

La cuarta protección que aplica el cortafuegos es la protección del búfer de paquetes, que aplica a nivel global para proteger el dispositivo y que también puede aplicar de manera individual en las zonas para evitar los ataques DoS de sesión única que intentan sobrecargar el búfer del paquete del cortafuegos. Para la protección global, el cortafuegos usa Descarte aleatorio temprano (Random Early Drop, RED) para descartar paquetes (no sesiones) cuando el nivel de tráfico traspasa los umbrales de protección. Para la protección por zona, el cortafuegos bloquea la dirección IP de origen si infringe los umbrales del búfer de paquetes. A diferencia de la protección DoS y de zona, la protección del búfer de paquetes se aplica a las sesiones existentes.

Selección de ubicación del cortafuegos para la protección DoS

El cortafuegos es un dispositivo basado en sesiones que no está diseñado para aumentar la escala a millones de conexiones por segundo (connections-per-second, CPS) para proporcionar una defensa frente a grandes ataques DoS volumétricos. El cortafuegos trata cada flujo único (en función de la zona de entrada y salida, la IP de origen y destino, el protocolo y la aplicación) como una sesión, emplea ciclos de CPU en la inspección de paquetes en el puerto y el nivel de IP para proporcionar visibilidad en el tráfico de la aplicación, y deben contar cada sesión para los contadores de umbrales de inundación; por ello, la colocación del cortafuegos es imprescindible para evitar la inundación del cortafuegos.

Para lograr la mejor protección DoS, *coloque cortafuegos tan cerca de los recursos que protege como sea posible.* Esta acción reduce la cantidad de sesiones que el cortafuegos necesita administrar y, por tanto, la cantidad de recursos de cortafuegos necesarios para proporcionar la protección DoS.

En el perímetro accesible desde Internet, *no* coloque cortafuegos que use para la protección DoS o la protección de zona frente a los dispositivos DDoS dedicados y los conmutadores y enrutadores de perímetro. Convierta estos dispositivos de gran volumen en su primera línea de defensa DoS para mitigar los ataques volumétricos de inundación. Para la protección DoS y de zona en el perímetro, use cortafuegos de alta capacidad y colóquelos *detrás* de los dispositivos de gran volumen. Normalmente, cuanto más cerca esté el cortafuegos del perímetro, mayor deberá ser su capacidad para gestionar el volumen de tráfico.

La forma en que segmenta su red en las zonas puede ayudar a mitigar ataques DoS internos. Las zonas más pequeñas ofrecen mayor visibilidad en el tráfico y evitan mejor el movimiento lateral de malware porque hay más tráfico para atravesar las zonas, y para permitir el tráfico entre zonas es necesario que cree una regla de política de seguridad específica (todo el tráfico entre zonas está permitido de manera predeterminada). Considere revisar su enfoque de segmentación si su red está relativamente sin segmentar.

Medidas de CPS de referencia para establecer umbrales de inundación

Los umbrales de protección de inundación determinan cuántas conexiones por segundo (connections-per-second, CPS) nuevas se permiten en una zona (perfil de protección de zona), un grupo de dispositivos de una zona (política de protección DoS agregada) o dispositivos individuales de una zona (política de protección DoS clasificada), cuándo limitar conexiones nuevas para comenzar a mitigar un ataque de inundación potencial y cuándo descartar todas las conexiones nuevas. Los umbrales de protección de inundación del perfil de protección DoS y el perfil de protección de zona predeterminado no son apropiados para la mayoría de las redes porque cada red es única. Debe comprender las CPS máximas y normales agregadas de cada zona para configurar umbrales de perfiles de protección de zona efectivos, y también debe entender los sistemas críticos individuales que desea defender para configurar umbrales del perfil de protección DoS efectivos que no establezcan de manera inadvertida umbrales demasiados altos que permitan ataques de inundaciones o umbrales demasiados bajos que limiten el tráfico.

- Mediciones de CPS que se deben tomar
- Cómo medir CPS

© 2020 Palo Alto Networks, Inc.

Mediciones de CPS que se deben tomar

Mida el tráfico de CPS máximas y promedio durante al menos cinco días laborales o hasta que esté seguro de que las mediciones reflejen los patrones de tráfico típicos de la red; cuanto mayor sea el período de medición, más precisas resultarán las mediciones. Tenga en cuenta los eventos especiales, trimestrales y anuales que pueden aumentar la cantidad de CPS que debe respaldar. Es posible que deba ajustar los perfiles de protección de zona y programar reglas de política de protección DoS ajustadas para adaptarse a estos tipos de eventos si sus cortafuegos tienen la capacidad de gestionar tráfico adicional. Tome las siguientes mediciones de referencia:

- Para los perfiles de protección de zona, mida las CPS máximas y promedio que ingresan a cada zona.
- Para los perfiles de protección DoS agregados, mida las CPS máximas y promedio combinadas de cada grupo de dispositivos que desea proteger.
- Para los perfiles de protección DoS clasificados, mida las CPS máximas y promedio de los dispositivos individuales que desea proteger.

Además, comprenda la capacidad de sus cortafuegos cómo otras funciones que consumen recursos, como el descifrado, afectan la cantidad de conexiones que puede controlar cada cortafuegos. Por lo general, cuanto más cerca del perímetro esté el cortafuegos, mayor deberá ser su capacidad porque gestionará más tráfico. La hoja de datos de cada modelo de cortafuegos incluye el total de nuevas sesiones por segundo (sessions per second, CPS) que admite el cortafuegos y la herramienta de comparación de cortafuegos le permite comparar las CPS (y otras métricas) de diferentes modelos de cortafuegos.

Cómo medir CPS

Existen varias maneras de medir las CPS:

- Si usa Panorama para administrar sus cortafuegos, utilice la supervisión de dispositivos para medir las CPS que entran al cortafuegos (**Panorama** > **Managed Devices [Dispositivos administrados]** > **Health [Estado]** > **All Devices[Todos los dispositivos]**). La supervisión de dispositivos también puede mostrarle una línea de tendencia de 90 días del uso máximo y promedio de CPU para ayudarle a comprender la capacidad típica disponible de cada cortafuegos.
- Ejecute el comando operativo de la CLI **`show session info`**.

  *El comando operativo de la CLI **`show counter interface`** muestra dos veces el valor real de CPS. Si usa este comando, divida el valor de CPS entre dos para obtener el valor real de CPS.*
- Para configurar los umbrales apropiados del perfil de protección DoS, trabaje junto a los equipos de aplicación para conocer las CPS normales y máximas hacia sus servidores y las CPS máximas que estos servidores pueden admitir.

  Además, puede filtrar los logs de amenazas y los de tráfico del cortafuegos de las direcciones IP de destino de los dispositivos críticos que desee proteger para obtener información de actividad de sesión normal y máxima.
- Use herramientas de terceros como Wireshark o NetFlow para recopilar y analizar el tráfico de red.
- Use secuencias de comandos para automatizar la supervisión continua y la recopilación de información de CPS, y extraer información de los logs.
- Configure cada regla de política de seguridad en el cortafuegos en **Log at Session End (Registrar al final de la sesión)**. Si no cuenta con herramientas de gestión como NetFlow o Wireshark y no puede obtener o desarrollar secuencias de comandos automatizadas, **Log at Session End (Registrar al final de la sesión)** captura la cantidad de conexiones al final de la sesión. Aunque esto no proporciona información de CPS, le muestra el número de sesiones que finalizan en la duración seleccionada y puede hacer un cálculo aproximado de las sesiones por segundo a partir de esa información.

Para conservar recursos, el cortafuegos mide las CPS agregadas en intervalos de diez segundos. Por esa razón, es posible que las mediciones que ve en el cortafuegos no capten

© 2020 Palo Alto Networks, Inc.

ráfagas dentro del intervalo de diez segundos. Aunque las mediciones de CPS medias no se ven afectadas, las mediciones de CPS máximas pueden no ser precisas. Por ejemplo, si los logs del cortafuegos informan de una media de 5000 CPS en un intervalo de diez segundos, es posible que lleguen 4000 CPS en un aumento repentino de un segundo y otras 1000 CPS en los restantes nueve segundos.

Para recopilar datos históricos de CPS a lo largo del tiempo, en el caso de que use un servidor SNMP, puede usar sus propias herramientas de administración para sondear las MIB SNMP. Sin embargo, es importante comprender que las mediciones de CPS en las MIB muestran el doble del valor real de CPS (por ejemplo, si la verdadera medición de CPS es 10 000, las MIB muestran 20 000 como valor). Todavía puede ver las tendencias de las MIB y puede dividir los valores de CPS entre dos para obtener los valores reales. Los OID de la MIB de SNMP son los siguientes: PanZoneActiveTcpCps, PanZoneActiveUdpCps y PanZoneOtherIpCps. Sondee cada 10 segundos, ya que el cortafuegos solo toma medidas y actualiza el servidor SNMP con esa frecuencia.

Además, cree perfiles de reenvío de logs diferentes para los eventos de inundación, de modo que el administrador apropiado reciba correos electrónicos que contengan solo eventos de inundación (ataque DoS potencial). Configure el reenvío de logs para los eventos de umbral de protección DoS y protección de zona.

Después de implementar la protección DoS y de zona, use estos métodos para supervisar la implementación, de modo que a medida que su red evolucione y los patrones de tráfico cambien, usted pueda ajustar los umbrales de protección de inundación.

Perfiles de protección de zonas

Aplique un perfil de protección de zona a cada zona para defenderla en función del tráfico agregado entrante.

Además de configurar la protección de zona y la protección DoS, aplique el perfil de protección frente a vulnerabilidades recomendado a cada regla de política de seguridad para defenderla contra los ataques DoS.

- Protección contra inundaciones
- Protección de reconocimiento
- Protección de ataques basados en paquetes
- Protección de protocolo
- Protección de SGT Ethernet

Protección contra inundaciones

Un perfil de protección de zona con una protección de inundación configurada defiende una zona de entrada completa de los ataques de inundación SYN, ICMP, ICMPv6, UDP y otros tipos de inundación de IP. El cortafuegos mide la cantidad total de cada tipo de inundación que entra en la zona en conexiones nuevas por segundo (connections-per-second, CPS) y compara el total con los umbrales configurados en el perfil de protección de zona. (Proteja los dispositivos individuales importantes dentro de una zona con las reglas de política y perfiles de protección DoS).

Mida y supervise el consumo de CPU del plano de datos en el cortafuegos para garantizar que cada cortafuegos tenga el tamaño adecuado para admitir la protección DoS y de zona junto con cualquier otra función que consuma ciclos de CPU, como el descifrado. Si usa Panorama para administrar cortafuegos, la supervisión de dispositivos (Panorama > Managed Devices [Dispositivos gestionados] > Health [Estado] > All Devices [Todos los dispositivos]) le muestra el consumo de CPU y memoria de cada cortafuegos administrado.

© 2020 Palo Alto Networks, Inc.

También puede mostrarle una línea de tendencia de 90 días del uso máximo y promedio de CPU para ayudarlo a comprender la capacidad típica disponible de cada cortafuegos.

Para cada tipo de inundación, configure tres umbrales de las nuevas CPS que entran en la zona, y puede configurar una **Action (Acción)** de descarte para la inundación SYN. Si conoce las tasas de CPS de referencia de la zona, use estas pautas para configurar los umbrales iniciales y, luego, supervisarlos y ajustarlos según fuera necesario.

- **Tasa de alarma:** el umbral de CPS nuevas para activar una alarma. Configure **Alarm Rate (Tasa de alarma)** del 15 al 20% por encima de la tasa promedio de CPS para la zona, de modo que las fluctuaciones normales no activen alertas.
- **Activación:** el umbral de CPS nuevas para activar el mecanismo de protección de inundación y comenzar a descartar conexiones nuevas. Para ICMP, ICMPv6, UDP y otras inundaciones de IP, el mecanismo de protección es Descarte aleatorio temprano (Random Early Drop, RED, también conocido como Random Early Detection [Detección aleatoria temprana]). Solo para la inundación SYN, puede configurar la **Action (Acción)** de descarte para las cookies SYN o RED. Configure la tasa de **Activate (Activación)** sobre la tasa máxima de CPS de la zona para comenzar a mitigar las inundaciones potenciales.
- **Máximo:** la cantidad de conexiones por segundo necesarias para descartar los paquetes entrantes cuando el RED es el mecanismo de protección. Configure la tasa **Maximum (Máxima)** a aproximadamente el 80 o 90% de la capacidad del cortafuegos, para ello, tenga en cuenta otras funciones que consumen recursos del cortafuegos.

Si no conoce las tasas de CPS de referencia de la zona, comience por configurar la tasa de CPS **Maximum (Máxima)** a aproximadamente el 80 o 90% de la capacidad del cortafuegos y úsela para deducir las tasas razonables de activación y alarma de mitigación de inundación. Configure **Alarm Rate (Tasa de alarma)** y tasa de **Activate (Activación)** sobre la base de la tasa máxima. Por ejemplo, puede configurar la **Alarm Rate (Tasa de alarma)** a la mitad de la tasa **Maximum (Máxima)** y ajustarla según la cantidad de alarmas que reciba y los recursos del cortafuegos que se consuman. Tenga cuidado al configurar la **Activate Rate (Tasa de activación)** dado que comienza a descartar conexiones. Dado que la carga normal de tráfico sufre algunas fluctuaciones, se recomienda no descartar conexiones de manera muy agresiva. Sea cauto y ajuste la tasa cuando los recursos del cortafuegos se vean afectados.



La protección de inundación SYN es el único tipo para el que configura la Action (Acción) de descarte. Comience por configurar Action (acción) en SYN Cookies (Cookies SYN). Las cookies SYN tratan el tráfico legítimo de manera equitativa y solo descartan tráfico que no cumple con el protocolo de enlace SYN usando el Descarte aleatorio temprano para descartar el tráfico de manera aleatoria, de modo que RED puede afectar el tráfico legítimo. Sin embargo, las cookies SYN consumen un mayor número de recursos porque el cortafuegos actúa como un proxy para el servidor objetivo y administra el protocolo de enlace de tres vías para el servidor. El punto intermedio no es descartar tráfico legítimo (cookies SYN) frente a preservar recursos del cortafuegos (RED). Supervise el cortafuegos y, si las cookies SYN consumen muchos recursos, cambie a RED. Si no tiene un dispositivo de prevención de DDoS dedicado delante del cortafuegos, siempre use RED como el mecanismo de descarte.

Los valores del umbral predeterminado son altos, de modo que si se activa un perfil de protección de zona, no se descarte tráfico legítimo inesperadamente. Ajuste los umbrales a los valores apropiados del tráfico de su red. El mejor método para comprender cómo configurar umbrales de inundación razonables es tomar las mediciones de referencia de las CPS promedio y máximas de cada tipo de inundación para determinar las condiciones normales de tráfico de cada zona y conocer la capacidad del cortafuegos, incluido el impacto de otras funciones que consumen recursos como el descifrado. Supervise y ajuste los umbrales de inundación según sea necesario y a medida que evolucione su red.



Los cortafuegos con varios procesadores del plano de datos (dataplane processors, DP) distribuyen conexiones por los DP. En general, el cortafuegos divide la configuración del umbral de CPS equitativamente en sus DP. Por ejemplo, si un cortafuegos tiene cinco DP

© 2020 Palo Alto Networks, Inc.

y configura la Alarm Rate (tasa de alarma) en 20 000 CPS, cada DP tiene una Alarm Rate (Tasa de alarma) de 4000 CPS (20 000/5 = 4000), por lo tanto, si las sesiones nuevas en un DP superan el valor de 4000, activan el umbral de la Alarm Rate (Tasa de alarma) de ese DP.

Protección de reconocimiento

De manera similar a la definición del ejército del reconocimiento, la definición de seguridad de la red del reconocimiento se produce cuando los atacantes intentan obtener información sobre las vulnerabilidades de su red sondeando de manera secreta su red en busca de debilidades. Por lo general, las actividades de reconocimiento se producen antes de un ataque de red. *Habilite la protección de reconocimiento en todas las zonas* para defenderse contra los análisis de puerto y el barrido de host:

- **Los análisis de puertos** descubren los puertos abiertos de una red. Una herramienta de análisis de puertos envía solicitudes de cliente a distintos puertos en un host para ubicar un puerto activo que pueda aprovecharse en un ataque. Los perfiles de protección de zona lo defienden de los análisis de puertos con TCP y UDP.
- Las **limpiezas de hosts** examinan varios hosts para determinar si un puerto específico está abierto y vulnerable.

Puede utilizar herramientas de reconocimiento con fines legítimos como la prueba de penetración de la seguridad de la red o la fortaleza de un cortafuegos. Puede especificar hasta 20 direcciones IP u objetos de dirección de máscara de red que excluirá de la protección de reconocimiento, de modo que su departamento de TI interno pueda llevar a cabo pruebas de penetración para buscar y resolver las vulnerabilidades de la red.

Puede establecer la acción que se llevará a cabo cuando el tráfico de reconocimiento (excepto el tráfico de la prueba de penetración) supere el umbral que configuró cuando realizó la Configuración de la protección de reconocimiento. Conserve los valores predeterminados en **Interval (Intervalo)** y **Threshold (Umbral)** para registrar algunos paquetes para el análisis antes de bloquear el funcionamiento del reconocimiento.

Protección de ataques basados en paquetes

Los ataques basados en paquetes se presentan en diversas formas. Los perfiles de protección de zona comprueban los encabezados de paquetes IP, TCP, ICMP, IPv6 e ICMPv6 y protegen una zona de la siguiente manera:

- Descartando paquetes con características indeseables.
- Quitando las opciones indeseables de los paquetes antes de admitirlos en la zona.

Seleccione las características de descarte de cada tipo de paquetes cuando realiza la Configuración de la protección de ataques basada en paquetes. Las prácticas recomendadas para cada protocolo de IP son las siguientes:

- **IP Drop (Descarte de IP)**: descarte los paquetes en **Unknown (Desconocido)** y **Malformed (Con formato incorrecto)**. Descarte también **Strict Source Routing (Enrutamiento de fuente estricto)** y **Loose Source Routing (Enrutamiento de fuente no estricto)** porque si se permiten estas opciones, se admite que los adversarios omitan las reglas de política de seguridad que usen la dirección IP de destino como criterio de coincidencia. Únicamente en las zonas internas, marque **Spoofed IP Address (Dirección IP duplicada)** de modo que solo pueda acceder a la zona el tráfico con una dirección de origen que coincida con la tabla de enrutamiento del cortafuegos.
- **TCP Drop (Descarte de TCP)**: conserve los descartes predeterminados de **TCP SYN with Data (Sincronización TCP con datos)** y **TCP SYNACK with Data (Confirmación de sincronización TCP con datos)**, descarte los paquetes **Mismatched overlapping TCP segment (Segmento de TCP superpuesto no coincidente)** y **Split Handshake (Protocolo de enlace dividido)** y quite la **TCP Timestamp (Marca de tiempo TCP)** de los paquetes.

© 2020 Palo Alto Networks, Inc.

Habilitar Rematch Sessions (Volver a cotejar sesiones) (Device [Dispositivo] > Setup [Configuración] > Session [Sesión] > Session Settings [Configuración de sesión]) es la opción recomendada que aplica las reglas de política de seguridad recientemente configuradas o editadas y confirmadas a las sesiones existentes. Sin embargo, si configura la inspección de contenido del túnel en una zona y Rematch Sessions (Volver a cotejar sesiones) está habilitado, también debe deshabilitar Reject Non-SYN TCP (Rechazar TCP no sincronizados) (cambie la selección de Global a No), o de lo contrario, cuando habilite o edite una política de inspección de contenido del túnel el cortafuegos descartará todas las sesiones de túnel existente. Cree un perfil de protección de zona diferente para deshabilitar Reject Non-SYN TCP (Rechazar TCP no sincronizados) solo en las zonas que tienen políticas de inspección de contenido de túnel y solo cuando habilite Rematch Sessions (Volver a cotejar sesiones).

- **ICMP Drop (Descarte de ICMP)**: no hay una configuración estándar recomendada porque descartar paquetes de ICMP depende de cómo use ICMP (o si usa ICMP). Por ejemplo, si desea bloquear la actividad de ping, puede bloquear **ICMP Ping ID 0 (ID de 0 de ping de ICMP)**.
- **IPv6 Drop (Descarte de IPv6)**: si se deben cumplir las normas, asegúrese de que el cortafuegos descarte paquetes con encabezados de enrutamiento, extensiones, etc. que no cumplen con las normativas.
- **ICMPv6 Drop (Descarte de ICMPv6)**: si se deben cumplir las normas, asegúrese de que el cortafuegos descarte determinados paquetes si estos no coinciden con una regla de política de seguridad.

Protección de protocolo

En un perfil de protección de zona, la protección de protocolo lo defiende de ataques basados en protocolos no IP. Habilite la protección de protocolo para bloquear o permitir protocolos no IP entre las zonas de seguridad en una VLAN de capa 2 o en un cable virtual, o entre interfaces dentro de una sola zona en una VLAN de capa 2 (las zonas e interfaces de capa 3 descartan protocolos no IP de modo que no se aplique la protección de protocolo no IP). Configuración de la protección de protocolos para reducir riesgos de seguridad y facilitar el cumplimiento normativo a fin de evitar que protocolos menos seguros entren en una zona o una interfaz en una zona.

Si no configura un perfil de protección de zona que evite que los protocolos no IP de la misma zona vayan de una interfaz de capa 2 a otra, el cortafuegos permite el tráfico debido a que la intrazona predeterminada permite la regla de política de seguridad. Puede crear un perfil de protección de zona que bloquee protocolos como LLDP dentro de una zona para evitar el descubrimiento de redes disponibles mediante otras interfaces de zona.

Si necesita descubrir qué protocolos no IP se ejecutan en su red, use las herramientas de supervisión como NetFlow, Wireshark u otras herramientas de terceros que descubran protocolos no IP en su red. Los ejemplos de protocolos no IP que puede bloquear o permitir incluyen LLDP, NetBEUI, de árbol de conmutación, y los sistemas de Control y adquisición de datos (Supervisory Control And Data Acquisition, SCADA), como los Eventos de subestaciones orientados a objetos genéricos (Generic Object Oriented Substation Event, GOOSE), entre otros.

Cree una **Exclude List (Lista de exclusión)** o una **Include List (Lista de inclusión)** para configurar una protección de protocolo de una zona. La **Exclude List (Lista de exclusión)** es una lista negra: el cortafuegos bloquea todos los protocolos que coloca en la **Exclude List (Lista de exclusión)** y permite el resto. La **Include List (Lista de inclusión)** es una lista de permitidos: el cortafuegos permite solo los protocolos que especifica en la lista y bloquea el resto.

Use las listas de inclusión para la protección de protocolo en lugar de las listas de exclusión. Las listas de inclusión específicamente sancionan solo los protocolos que desea permitir y bloquea los que no necesita o no sabía que estaban en su red, lo que reduce la superficie de ataque y bloquea el tráfico desconocido.

© 2020 Palo Alto Networks, Inc.

Una lista admite hasta 64 entradas Ethertype; cada una se identifica por su código Ethertype hexadecimal IEEE. Otras fuentes de códigos Ethertype son standards.ieee.org/develop/regauth/ethertype/eth.txt y http://www.cavebear.com/archive/cavebear/Ethernet/type.html. Cuando configura una protección de zona para protocolos no IP en zonas que cuentan con interfaces de Ethernet agregado (Aggregated Ethernet, AE), no puede bloquear o permitir un protocolo no IP en solo un miembro de interfaz de AE debido a que los miembros de las interfaces de AE se consideran un grupo.

La protección de protocolos no permite bloquear IPv4 (Ethertype 0x0800), IPv6 (0x86DD), ARP (0x0806) o tramas con etiquetas VLAN (0x8100). El cortafuegos siempre permite de manera implícita estos cuatro Ethertypes en una Include List (Lista de inclusión), incluso si no los detalla explícitamente en la lista y no le permite añadirlos a una Exclude List (Lista de exclusión).

Protección de SGT Ethernet

En una red Cisco TrustSec, un motor de servicios de identidad (ISE, Identity Services Engine) de Cisco asigna una etiqueta de grupo de seguridad (SGT, Security Group Tag) de capa 2 de 16 bits a la sesión de un usuario o endpoint. Puede crear un perfil de protección de zona con protección de SGT Ethernet cuando su cortafuegos sea parte de una red Cisco TrustSec. El cortafuegos puede inspeccionar encabezados con 802.1Q (Ethertype 0x8909) para valores específicos de etiqueta de grupo de seguridad (SGT, Security Group Tag) de capa 2 y descartar el paquete si la SGT coincide con la lista que configura para el perfil de protección de zona adjunto a la interfaz. Determine a qué valores de SGT desea que denegar el acceso a una zona.

Protección de búfer de paquetes

La protección del búfer de paquetes le permite proteger su cortafuegos y su red de ataques DoS de sesión única que pueden sobrecargar el búfer de paquetes del cortafuegos y provocar que se descarte tráfico legítimo. Aunque no configure la protección del búfer de paquetes en un perfil de protección de zona o en una regla de política o perfil de protección DoS, la protección del búfer de paquetes defiende las zonas de entrada. Mientras que la protección DoS y de zona se aplica a nuevas sesiones (conexiones) y es detallada, la protección del búfer de paquetes se aplica a sesiones existentes y es global.

Configuración de la protección de búfer de paquetes a nivel global para proteger el cortafuegos completo y también habilite la protección del búfer de paquetes en cada zona para protegerlas:

- **Protección del búfer de paquetes global:** el cortafuegos supervisa las sesiones de todas las zonas (independientemente de si la protección del búfer de paquetes está habilitada en la zona) y cómo estas sesiones usan el búfer de paquetes. Debe configurar la protección del búfer de paquetes a nivel global (**Device [Dispositivo]Setup [Configuración]Session Settings [Configuración de sesión]**) para proteger al cortafuegos y habilitarlo en las zonas individuales. Cuando el consumo del búfer de paquetes llega al porcentaje configurado en **Activate (Activar)**, el cortafuegos usa (Random Early Drop, RED) para descartar paquetes de las sesiones infractoras (el cortafuegos no descarta sesiones completas a nivel global).
- **Protección del búfer de paquetes por zona:** habilite la protección del búfer de paquetes en cada zona (**Network [Red]** > **Zones [Zonas]**) para proporcionar un segundo nivel de protección. Cuando el consumo del búfer de paquetes cruza el umbral de **Activate (Activar)** y la protección global comienza a aplicar el RED al tráfico de la sesión, esto inicia el temporizador **Block Hold Time (Tiempo de espera de bloqueo)**. El **Block Hold Time (Tiempo de espera de bloqueo)** es la cantidad de tiempo en segundos que la sesión infractora puede continuar antes de que el cortafuegos bloquee la sesión completa. La sesión infractora permanece bloqueada hasta que pase el tiempo de **Block Duration (Duración del bloqueo)**.

  Debe habilitar la protección del búfer de paquetes globalmente para que esté activa en las zonas.

Hay dos tipos de protección del búfer de paquetes:

© 2020 Palo Alto Networks, Inc.

- Protección de búfer de paquetes basada en la utilización del búfer
- Protección de búfer de paquetes basada en la latencia

Protección de búfer de paquetes basada en la utilización del búfer

La protección de búfer de paquetes basada en la utilización del búfer está habilitada de forma predeterminada. Tome mediciones de referencia del uso del búfer de paquetes del cortafuegos durante un período de tiempo (al menos una semana laboral, pero un período de medición mayor ofrece una mejor referencia) para comprender el uso típico.

Para ver la utilización del búfer de paquetes durante un período específico (o para ver las cinco sesiones principales que usan al menos el 2 por ciento del búfer de paquetes), use el comando operativo de la CLI:

```
admin1138@thxvm1>show running resource-monitor [day | hour | ingress-backlogs
 | minute | second | week]
```

El comando de la CLI proporciona una instantánea de la utilización del búfer durante el período especificado, pero no es automático ni continuo. Para automatizar las mediciones continuas de la utilización del búfer de paquetes para que pueda supervisar los cambios en el comportamiento y los eventos anómalos, utilice un script. Su equipo de cuentas de Palo Alto Networks puede proporcionar un script de muestra que podrá modificar para desarrollar su propio script; sin embargo, el script no dispone de soporte oficial y no hay soporte técnico disponible para su uso o modificación.

Si las mediciones de referencia muestran de manera sistemática un uso del búfer de paquetes inusualmente alto, entonces es posible que la capacidad del cortafuegos sea reducida para las cargas típicas del tráfico. En este caso, considere cambiar el tamaño de la implementación del cortafuegos. De lo contrario, necesita ajustar los umbrales de protección del búfer de paquetes detenidamente para evitar que los búfer afectados se sobrecarguen (y que se descarte tráfico legítimo). Cuando el tamaño del cortafuegos es el correcto para la implementación, loo único que debe provocar un gran aumento en el uso del búfer es un ataque.

Sobrepasar el búfer de paquetes del cortafuegos afecta de manera negativa a las capacidades de reenvío de paquetes del cortafuegos. Cuando el búfer está completo, no pueden entrar paquetes al cortafuegos en ninguna interfaz, no solo la interfaz que sufrió el ataque.

Las prácticas recomendadas para la configuración de los umbrales son las siguientes:

- **Alert (Alertar)** y **Activate (Activar)**: comience por los valores de umbral predeterminados, supervise el uso del búfer y ajuste los umbrales según sea necesario. El valor predeterminado del umbral de **alerta** es del 50 %; cuando la utilización del búfer de paquetes supera el umbral durante más de 10 segundos, el cortafuegos crea una entrada de alerta en el log del sistema cada minuto. El valor predeterminado del umbral de **activación** es del 80 %; cuando se alcanza el umbral, el cortafuegos comienza a reducir las sesiones más abusivas. Si el cortafuegos tiene el tamaño correcto, el uso del búfer debería estar bien por debajo del 50%.
- **Block Hold Time (Tiempo de espera de bloqueo)**: cuando el uso del búfer de paquetes activa el umbral **Activate (Activar)**, el **Block Hold Time (Tiempo de espera de bloqueo)** configura la cantidad de tiempo que la sesión infractora puede continuar antes de que el cortafuegos la bloquee. Durante el **Block Hold Time (Tiempo de espera de bloqueo)**, el cortafuegos continúa aplicando RED a los paquetes de las sesiones infractoras. Comience con un valor de umbral predeterminado en **Block Hold Time (Tiempo de espera de bloqueo)** (60 segundos), supervise el uso del búfer de paquetes y ajuste el umbral según sea necesario. Si el porcentaje de uso del búfer de paquetes disminuye por debajo del umbral de **Activate (Activar)** antes de que caduque el **Block Hold Time (Tiempo de espera de bloqueo)**, el temporizador se reinicia y no comienza hasta que se vuelva a exceder el umbral de **Activate (Activar)**. Aumentar el

© 2020 Palo Alto Networks, Inc.

Block Hold Time (Tiempo de espera de bloqueo) impone una sanción mayor en las sesiones infractoras y reducirlo establece una sanción menor en ellas.

- **Block Duration (Duración del bloqueo)**: cuando caduca el **Block Hold Time (Tiempo de espera de bloqueo)**, el cortafuegos bloquea la sesión infractora durante el período de tiempo definido por la **Block Duration (Duración del bloqueo)**. Comience con el valor de umbral predeterminado en (3600 segundos), supervise el uso del búfer de paquetes y ajuste el umbral según sea necesario. Cuando habilite la protección del búfer de paquetes en una zona, la **Block Duration (Duración del bloqueo)** afecta todas las sesiones de la dirección IP, incluso si solo una sesión de la dirección IP hace un uso excesivo del búfer de paquetes. Si cree que bloquear una dirección IP durante una hora (3600 segundos) es una penalización demasiado grande, reduzca la **Block Duration (Duración del bloqueo)** a un valor aceptable.

Además de supervisar la utilización del búfer de sesiones individuales, la protección del búfer de paquetes puede bloquear una dirección IP si se cumplen determinados criterios. Cuando el cortafuegos supervisa el búfer de paquetes, si detecta una dirección IP de origen que crea sesiones rápidamente (lo que no se consideraría de manera individual un ataque), bloquea esa dirección IP durante el valor configurado en **Block Duration (Duración del bloqueo**.



La Traducción de direcciones de red (Network Address Translation, NAT) (un origen externo que tradujo su tráfico de Internet con una NAT de origen) puede dar la apariencia de un mayor uso del búfer de paquetes debido a la actividad de traducción de las direcciones IP. Si esto sucede, ajuste los umbrales de forma que penalice las sesiones individuales pero no las direcciones IP subyacentes (de modo que otras sesiones de la misma dirección IP no se vean afectadas). Para hacerlo, reduzca el Block Hold Time (Tiempo de espera de bloqueo) de modo que el cortafuegos bloquee las sesiones individuales que excedan el uso del búfer con mayor rapidez, y reduzca la Block Duration (Duración del bloqueo) de modo que las direcciones IP subyacentes no se penalicen de manera indebida.

Protección de búfer de paquetes basada en la latencia

Como alternativa a la protección del búfer de paquetes basada en la utilización, puede activar la protección del búfer de paquetes basada en la latencia de paquetes provocada por el búfer de paquetes del plano de datos, que indica una congestión en el cortafuegos. Esta protección del búfer de paquetes reduce el bloqueo de la cabecera de línea, ya que le alerta sobre la congestión y realiza un descarte aleatorio temprano (RED, Random Early Drop) en los paquetes. La protección de búfer de paquetes basada en la latencia puede activar la protección antes de que los protocolos o aplicaciones sensibles a la latencia se vean afectados.

Si su tráfico incluye protocolos o aplicaciones que son sensibles a la latencia, la protección del búfer de paquetes basada en la latencia será más útil que la protección del búfer de paquetes basada en la utilización del búfer.

La protección del búfer de paquetes basada en la latencia incluye el ajuste de un umbral de **alerta de latencia** (en milisegundos), por encima del cual el cortafuegos comenzará a generar un evento de log de alerta. El umbral de **activación de latencia** indica cuándo el cortafuegos activa RED en los paquetes entrantes y comienza a generar un log de activación. El umbral de **tolerancia máxima de latencia** indica cuándo el cortafuegos usa RED con casi el 100 % de probabilidad de descarte.

Los ajustes **Block Hold Time (Tiempo de espera de bloqueo)** y **Block Duration (Duración de bloqueo)** funcionan para la protección del búfer de paquetes basada en la latencia de la misma manera que lo hacen para la protección del búfer de paquetes basada en la utilización.

© 2020 Palo Alto Networks, Inc.

Perfiles de protección y reglas de la política del DoS

Los perfiles de protección DoS y las reglas de política de protección DoS se combinan para proteger recursos críticos individuales y en grupos de las inundaciones de sesión. En comparación con los perfiles de protección de zona, que protegen zonas completas de ataques de inundación, la protección DoS proporciona defensa pormenorizada para sistemas específicos, en especial, sistemas críticos a los que acceden los usuarios desde Internet y que con frecuencia son el objetivo de ataques, como servidores web y de bases de datos. Aplique ambos tipos de protección porque si solo aplica un perfil de protección de zona, un ataque DoS que apunte a un sistema determinado en la zona puede tener éxito si el total de conexiones por segundo (connections-per-second, CPS) no supera las tasas activas y máximas de la zona establecidas en **Activate (Activa)** y **Maximum (Máxima)**.

Utilice la protección DoS solo para sistemas críticos, ya que esta consume un mayor número de recursos. De manera similar a los perfiles de protección de zona, los perfiles de protección DoS especifican umbrales de inundación. Las reglas de política de protección DoS determinan los dispositivos, usuarios, zonas y servicios a los que se aplican los perfiles DoS.



Además de configurar la protección DoS y la protección de zona, aplique el perfil de protección frente a vulnerabilidades recomendado *a cada regla de política de seguridad para defenderla de los ataques DoS.*

- Protección DoS clasificada frente a agregada
- Perfiles de protección DoS
- Reglas de política de protección contra DoS

Protección DoS clasificada frente a agregada

Puede configurar Perfiles de protección DoS *aggregate (agregada)* y *classified (clasificada)* y aplicar un perfil o uno de cada tipo de perfil en Reglas de política de protección contra DoS cuando configure la protección DoS.

- **Aggregate (Agregada)**: Establece umbrales que se aplican al grupo completo de dispositivos especificados en una regla de política de protección DoS en lugar de a cada dispositivo individual, de modo que un dispositivo pueda recibir la mayor parte del tráfico permitido de conexión. Por ejemplo, si en **Max Rate (Tasa máxima)** se indican 20 000, el total de CPS del grupo es de 20 000, y un dispositivo individual puede recibir hasta 20 000 CPS si otros dispositivos no tienen conexiones. Las políticas de protección DoS agregada proporcionan otra capa de protección amplia (tras su dispositivo DDoS dedicado en los perfiles de protección de zona y perímetro de Internet) para un grupo determinado de dispositivos importantes cuando desea aplicar restricciones adicionales en subredes, usuarios o servicios específicos.
- **Classified (Clasificada)**: Establece umbrales de inundación que se aplican a cada dispositivo individual especificado en una regla de política de protección DoS. Por ejemplo, si se configura **Max Rate (Tasa máxima)** en 5000 CPS, cada dispositivo especificado en la regla puede aceptar hasta 5000 CPS antes de descartar conexiones nuevas. Si aplica una regla de política de protección DoS clasificada a más de un dispositivo, los dispositivos regidos por la regla deben ser similares en términos de capacidad y en la forma que desea controlar sus tasas de CPS, ya que los umbrales clasificados se aplican a cada dispositivo individual. Los perfiles clasificados protegen recursos importantes individuales.

  Cuando configura una regla de política de protección DoS con un perfil de protección DoS clasificada (**Option/Protection [Opción/protección]** > **Classified [Clasificada]** > **Address [Dirección]**), use el campo **Address (Dirección)** para especificar si las conexiones entrantes se contabilizan como parte de los umbrales del perfil sobre la base de los campos coincidentes de **source-ip-only**, **destination-ip-only** o **scr-dest-ip-both** (el cortafuegos contabiliza las coincidencias de direcciones IP de origen y destino como parte de los umbrales). Los contadores consumen recursos, por lo que el modo en que cuenta coincidencias de direcciones afecta al consumo de recursos del cortafuegos. Puede usar la protección DoS clasificada para lo siguiente:

© 2020 Palo Alto Networks, Inc.

- Proteja dispositivos importantes individuales, en especial, servidores a los que acceden los usuarios desde Internet y que con frecuencia son el objetivo de atacantes, como servidores web, servidores de bases de datos y servidores DNS. Establezca umbrales de protección de recursos e inundación en un perfil de protección DoS clasificado. Cree una regla de política de protección DoS que aplique el perfil a la dirección IP de cada servidor añadiendo las direcciones IP como el criterio de destino de la regla, y configure **Address (Dirección)** en **destination-ip-only**.

  No utilice la clasificación source-IP-only o src-dest-ip-both para zonas accesibles desde Internet en las reglas de política de protección DoS clasificada porque el cortafuegos no tiene la capacidad de almacenar contadores para cada dirección IP posible en Internet. Aumente el contador de umbral para las IP de origen solo en las reglas de zona interna o de la misma zona. En las zonas de perímetro, use destination-ip-only.
- Supervise la tasa de CPS de un host o un grupo de hosts sospechosos (la zona que contiene los hosts no puede ser accesible desde Internet). Configure un umbral de alarma adecuado en un perfil de protección DoS clasificada para recibir una notificación si un host inicia una cantidad de conexiones excepcionalmente considerable. Cree una regla de política de protección DoS que aplique el perfil al grupo de direcciones de origen o al origen individual, y configure **Address (Dirección)** en **source-ip-only**. Investigue los hosts que inicien suficientes conexiones nuevas para activar la alarma.

El modo en que configura **Address (Dirección)** (**source-ip-only**, **destination-ip-only** o **src-dest-ip-both**) para los perfiles clasificados depende de sus objetivos de protección DoS, lo que desea proteger y si los dispositivos protegidos están en zonas accesibles desde Internet.



El cortafuegos usa más recursos para realizar un seguimiento de src-dest-ip-both como Address (Dirección) que para source-IP-only o destination-ip-only porque los contadores consumen recursos tanto para las direcciones IP de origen como de destino en lugar de solo una de las dos.

Si aplica un perfil de protección DoS clasificado y uno agregado a la misma regla de política de protección DoS, el cortafuegos aplica el perfil agregado primero y, luego, el clasificado si es necesario. Por ejemplo, protegemos un grupo de cinco servidores web con ambos tipos de perfiles en una regla de política de protección DoS. La configuración del perfil agregado descarta las conexiones nuevas cuando el total combinado del grupo alcanza 25 000 CPS de **Max Rate (Tasa máxima)**. La configuración del perfil clasificado descarta las conexiones nuevas a cualquier servidor web individual del grupo cuando alcanza 6000 CPS de **Max Rate (Tasa máxima)**. Hay tres escenarios en los que el tráfico de conexiones nuevas cruza los umbrales de **Max Rate (Tasa máxima)**:

- La tasa de CPS nuevas supera el valor agregado de **Max Rate (Tasa máxima)** pero no supera el valor clasificado de **Max Rate (Tasa máxima)**. En este caso, el cortafuegos aplica el perfil agregado y bloquea las nuevas conexiones durante el tiempo configurado en Block Duration (Duración de bloqueo).
- La tasa de CPS nuevas no supera el valor agregado de **Max Rate (Tasa máxima)**, pero la CPS a uno de los servidores web supera el valor clasificado de **Max Rate (Tasa máxima)**. En este caso, el cortafuegos verifica el perfil agregado y descubre que la tasa del grupo es menor que 25 000 CPS, por lo que el cortafuegos no bloquea las conexiones nuevas en función de ello. Luego, el cortafuegos verifica el perfil clasificado y encuentra que la tasa de un servidor determinado es mayor que 6000 CPS. El cortafuegos aplica el perfil clasificado y bloquea las conexiones nuevas a ese servidor determinado durante el tiempo configurado en Block Duration (Duración de bloqueo). Debido a que los demás servidores del grupo están dentro del valor de **Max Rate (Tasa máxima)** del perfil clasificado, su tráfico no se ve afectado.
- La tasa de CPS nuevas supera el valor agregado de **Max Rate (Tasa máxima)** y también supera el valor clasificado de **Max Rate (Tasa máxima)** para uno de los servidores web. En este caso, el cortafuegos verifica el perfil agregado y descubre que la tasa del grupo es mayor que 25 000 CPS, por lo que el cortafuegos bloquea las conexiones nuevas para limitar el total de CPS del grupo. Luego, el cortafuegos verifica el perfil clasificado y encuentra que la tasa de un servidor determinado es mayor que 6000 CPS (de modo que el perfil agregado aplicó el límite combinado del grupo, pero no fue suficiente para

© 2020 Palo Alto Networks, Inc.

proteger a este servidor determinado). El cortafuegos aplica el perfil clasificado y bloquea las conexiones nuevas a ese servidor determinado durante el tiempo configurado en Block Duration (Duración de bloqueo). Debido a que los demás servidores del grupo están dentro del valor de **Max Rate (Tasa máxima)** del perfil clasificado, su tráfico no se ve afectado.



Si desea que un perfil de protección DoS clasificado y uno agregado se apliquen al mismo tráfico, debe aplicar ambos perfiles a la misma regla de política de protección DoS. Si aplica el perfil agregado a una regla y el perfil clasificado a otra regla diferente, incluso si especifican exactamente el mismo tráfico, el cortafuegos puede aplicar solo un perfil porque cuando el tráfico coincide con la primera regla de política de protección DoS, el cortafuegos ejecuta la Action (Acción) especificada en esa regla y no la compara con el tráfico en reglas subsiguientes, de modo que el tráfico nunca coincide con la segunda regla y el cortafuegos no puede aplicar su acción. (Las reglas de política de seguridad funcionan de esta misma forma).

Perfiles de protección DoS

Los perfiles de protección DoS establecen umbrales que lo protegen de los ataques de inundación de IP de las sesiones nuevas y proporcionan protección a los recursos (límites de cantidad máxima de sesiones simultáneas para recursos y endpoints específicos). Los perfiles de protección DoS le permiten proteger dispositivos específicos (perfiles clasificados) y grupos de dispositivos (perfiles agregados) de ataques de inundación SYN, UDP, ICMP, ICMPv6 y otros ataques de inundación de IP. La configuración de los umbrales de protección de inundación en un perfil de protección DoS es similar a la configuración de Protección contra inundaciones en un perfil de protección de zona, pero estos últimos protegen todas las zonas de entrada, mientras que las reglas de políticas y los perfiles de protección DoS son detallados y orientados, y pueden incluso estar clasificados para un dispositivo único (dirección IP). El cortafuegos mide la cantidad total de conexiones por segundo (connections-per-second, CPS) a un grupo de dispositivos (perfil agregado) o mide las CPS a dispositivos individuales (perfil clasificado).



Mida y supervise el consumo de CPU del plano de datos en el cortafuegos para garantizar que cada cortafuegos tenga el tamaño adecuado para admitir la protección DoS y de zona junto con cualquier otra función que consuma ciclos de CPU, como el descifrado. Si usa Panorama para administrar cortafuegos, la supervisión de dispositivos (Panorama > Managed Devices [Dispositivos gestionados] > Health [Estado] > All Devices [Todos los dispositivos]) le muestra el consumo de CPU y memoria de cada cortafuegos administrado. También puede mostrarle una línea de tendencia de 90 días del uso máximo y promedio de CPU para ayudarlo a comprender la capacidad típica disponible de cada cortafuegos.

En cada tipo de inundación, configure tres umbrales para las nuevas CPS a un grupo de dispositivos (agregados) o a dispositivos individuales (clasificados) y una **Block Duration (Duración del bloqueo)**, y puede configurar una **Action (Acción)** de descarte para las inundaciones SYN:

- **Alarm Rate (Tasa de alarma)**: cuando las nuevas CPS superen este umbral, el cortafuegos genera una alarma de DoS. En los perfiles clasificados, configure la tasa del 15 al 20% sobre la tasa promedio de CPS del dispositivo, de modo que las fluctuaciones normales no provoquen alertas. Para los perfiles agregados, configure la tasa del 15 al 20% sobre la tasa promedio de CPS del grupo.
- **Activate Rate (Tasa de activación)**: cuando las nuevas CPS superen este umbral, el cortafuegos comienza a descartar conexiones nuevas para mitigar la inundación hasta que se reduzca la tasa de CPS por debajo del umbral. En los perfiles clasificados, la **Max Rate (Tasa máxima)** debe ser una tasa aceptable de CPS para los dispositivos que protege (la **Max Rate [Tasa máxima]** no provocará una inundación en los dispositivos más importantes). Puede configurar la **Activate Rate (Tasa de activación)** al mismo límite que la **Max Rate (Tasa máxima)** de modo que el cortafuegos no use RED o cookies SYN para comenzar a descartar tráfico antes de llegar a la **Max Rate (Tasa máxima)**. Configure la **Activate Rate (Tasa de activación)** para que sea menor que la **Max Rate (Tasa máxima)** solo si desea descartar tráfico antes de que llegue a la **Max Rate (Tasa máxima)**. En los perfiles agregados, configure el umbral justo por encima

© 2020 Palo Alto Networks, Inc.

de la tasa CPS máxima promedio del grupo para comenzar a mitigar las inundaciones con RED (o cookies SYN para las inundaciones SYN).

- **Max Rate (Tasa máxima)**: cuando las nuevas CPS superan este umbral, el cortafuegos bloquea (descarta) todas las conexiones nuevas desde la dirección IP infractora durante el período de tiempo especificado en **Block Duration (Duración del bloqueo)**. En los perfiles clasificados, el umbral de la **Max Rate (Tasa máxima)** debe estar basado en la capacidad de los dispositivos que protege, de modo que la tasa de CPS no produzca una inundación en ellos. En los perfiles agregados, configure del 80 al 90% de la capacidad del grupo.
- **Block Duration (Duración del bloqueo)**: cuando las nuevas CPS superan la **Max Rate (Tasa máxima)**, el cortafuegos bloquea las conexiones nuevas de la dirección IP infractora. La **Block Duration (Duración del bloqueo)** especifica la cantidad de tiempo que el cortafuegos continúa bloqueando las nuevas conexiones de la dirección IP. Mientras que el cortafuegos bloquea las conexiones nuevas, no cuenta las conexiones entrantes ni incrementa los contadores del umbral. En los perfiles agregados y clasificados, use el valor predeterminado (300 segundos) para bloquear la sesión del atacante sin penalizar sesiones legítimas del origen durante demasiado tiempo.

La protección de inundación SYN es el único tipo para el que configura la Action (Acción) de descarte. Comience por configurar Action (acción) en SYN Cookies (Cookies SYN). Las cookies SYN tratan el tráfico legítimo de manera equitativa y solo descartan tráfico que no cumple con el protocolo de enlace SYN usando el Descarte aleatorio temprano para descartar el tráfico de manera aleatoria, de modo que RED puede afectar el tráfico legítimo. Sin embargo, las cookies SYN consumen un mayor número de recursos porque el cortafuegos actúa como un proxy para el servidor objetivo y administra el protocolo de enlace de tres vías para el servidor. El punto intermedio no es descartar tráfico legítimo (cookies SYN) frente a preservar recursos del cortafuegos (RED). Supervise el cortafuegos y, si las cookies SYN consumen muchos recursos, cambie a RED. Si no tiene un dispositivo de prevención de DDoS dedicado delante del cortafuegos, siempre use RED como el mecanismo de descarte.

Los valores de umbral predeterminados son altos, de modo que los perfiles de protección DoS no descarten tráfico legítimo inesperadamente. Supervise el tráfico de la conexión y ajuste los umbrales a valores apropiados para su red. Comience por realizar mediciones de referencia de las CPS máximas y promedio de cada tipo de flujo para determinar las condiciones normales de tráfico de los dispositivos importantes que desea proteger. Dado que la carga normal de tráfico sufre algunas fluctuaciones, se recomienda no descartar conexiones de manera muy agresiva. Supervise y ajuste los umbrales de inundación según sea necesario y a medida que evolucione su red.

Otro método para configurar los umbrales de inundacón es usar las mediciones de referencia para configurar las CPS máximas que desea permitir y a partir de ello, deducir las tasas razonables de activación y alarma de mitigación de inundación.

Los cortafuegos con varios procesadores del plano de datos (dataplane processors, DP) distribuyen conexiones por los DP. En general, el cortafuegos divide la configuración del umbral de CPS equitativamente en sus DP. Por ejemplo, si un cortafuegos tiene cinco DP y configura la Alarm Rate (tasa de alarma) en 20 000 CPS, cada DP tiene una Alarm Rate (Tasa de alarma) de 4000 CPS (20 000/5 = 4000), por lo tanto, si las sesiones nuevas en un DP superan el valor de 4000, activan el umbral de la Alarm Rate (Tasa de alarma) de ese DP.

Además de la configuración de los umbrales de inundación de IP, también puede usar perfiles de protección DoS para detectar y evitar ataques de agotamiento de sesión en los que un gran número de hosts (bots) establecen tantas sesiones como sea posible para consumir los recursos de un objetivo. En la pestaña **Resources Protection (Protección de recursos)**, puede configurar la cantidad máxima de sesiones simultáneas que pueden recibir los dispositivos definidos en la regla de política de protección DoS a la

© 2020 Palo Alto Networks, Inc.

que aplica el perfil. Cuando la cantidad de sesiones simultáneas alcanza su límite máximo, se descartan las sesiones nuevas.

La cantidad máxima de sesiones simultáneas a configurar depende de su contexto de red. Comprenda la cantidad de sesiones simultáneas que pueden administrar los recursos que protege (definidos en la regla de política de protección DoS a la que adjunta el perfil). Configure el umbral a aproximadamente el 80% de la capacidad de los recursos, luego supervise y ajuste el umbral según sea necesario.

En los perfiles agregados, el umbral de **Resources Protection (Protección de recursos)** se aplica en todo el tráfico de los dispositivos definidos en la regla de política (origen y destino). En los perfiles clasificados, el umbral de **Resources Protection (Protección de recursos)** se aplica al tráfico en función de si la regla de política clasificada se aplica solo a la IP de origen, solo a la IP de destino o a ambas IP.

Reglas de política de protección contra DoS

Las reglas de política de protección DoS controlan los sistemas en los que el cortafuegos aplica la protección DoS (los umbrales de inundación configurados en los perfiles de protección DoS que adjunta a las reglas de política de protección DoS), qué acción tomar cuando el tráfico coincide con los criterios definidos en la regla y cómo registrar el tráfico DoS. Debido a que la protección DoS consume los recursos del cortafuegos, úsela solo para defender los recursos importantes contra inundaciones de sesión, en especial, los objetivos comunes a los que acceden los usuarios desde Internet, como los servidores web y de base de datos. Use los perfiles de protección de zona para proteger zonas completas contra inundaciones y otros ataques. Las reglas de la política de protección DoS proporcionan criterios de coincidencia más detallados, de modo que tenga la flexibilidad necesaria para definir de manera exacta lo que desea proteger:

- Zona, interfaz, dirección IP (incluidas regiones enteras) y usuario de origen.
- Zona, interfaz y dirección IP (incluidas regiones enteras) de destino.
- Servicios (por puerto o protocolo). La protección DoS solo se aplica a los servicios que especifica. Sin embargo, especificar servicios no implica que se permitan los servicios e implícitamente bloquear todos los demás servicios. Especificar servicios limita la protección DoS a esos servicios, pero no bloquea los demás.



Además de proteger puertos de servicio en uso en servidores importantes, también puede protegerlos contra ataques DoS en los puertos de servicio no utilizados de los servidores importantes. En los sistemas más importantes, puede hacerlo creando un perfil y una regla de política de protección DoS para proteger los puertos con servicios en ejecución, y un perfil y una regla de política de protección DoS para proteger puertos sin servicios en ejecución. Por ejemplo, puede proteger los puertos de servicio normales de un servidor web, como 80 y 443, con una política y un perfil, y proteger todos los demás puertos de servicios con la otra política/perfil. Tenga en cuenta la capacidad del cortafuegos de forma que el rendimiento no se vea afectado al proporcionar servicio a los contadores DoS.

Cuando el tráfico coincide con una regla de la política de protección DoS, el cortafuegos realiza una de las tres acciones:

- **Denegar:** el cortafuegos deniega el acceso y no aplica un perfil de protección DoS. El tráfico que coincide con la regla está bloqueado.
- **Permitir:** el cortafuegos permite el acceso y no aplica un perfil de protección DoS. Se permite el tráfico que coincide con la regla.
- **Proteger:** el cortafuegos protege los dispositivos definidos en la regla de política de protección DoS mediante la aplicación del umbral del perfil o los perfiles de protección DoS en el tráfico que coincida con la regla. Una regla puede tener un perfil de protección DoS agregado y un perfil de protección DoS clasificado, y en los perfiles clasificados, puede usar la IP de origen, IP de destino o ambas para aumentar los contadores del umbral de inundación, como se describe en Protección DoS clasificada frente a agregada. Los paquetes entrantes se consideran frente a ambos umbrales del perfil de protección DoS si coinciden con la regla.

© 2020 Palo Alto Networks, Inc.

El cortafuegos aplica los perfiles de protección DoS solo si la **Action (Acción)** es **Protect (Proteger)**. Si la **Action (Acción)** de la regla de la política de protección DoS es **Protect (Proteger)**, especifique el perfil de protección DoS agregado o clasificado correspondiente en la regla, de modo que el cortafuegos aplique los umbrales del perfil de protección DoS al tráfico que coincida con la regla. La mayoría de las reglas son **Protect (Proteger)**.

Las acciones **Allow (Permitir)** y **Deny (Rechazar)** le permiten realizar excepciones dentro de grupos más grandes pero no aplican la protección DoS en el tráfico. Por ejemplo, puede rechazar el tráfico de la mayor parte de un grupo, pero permitir un subconjunto de ese tráfico. Por otro lado, puede permitir el tráfico de la mayor parte de un grupo, pero rechazar un subconjunto de ese tráfico.

Haga clic en **Schedule (Programar)** para poder programar cuándo se activa una regla de política de protección DoS (hora de inicio y finalización, período de recurrencia). Un caso de uso para la programación es la aplicación de diferentes umbrales de inundación en diferentes momentos del día o de la semana. Por ejemplo, si su empresa experimenta mucho menos tráfico por la noche que durante el día, es posible que deba aplicar umbrales de inundación más altos durante el día que por la noche. Otro caso de uso es la programación de umbrales especiales para eventos especiales, siempre que el cortafuegos admita las tasas de CPS.

Para una gestión más sencilla y una realización de informes detallada, configure **Log Forwarding (Reenvío de logs)** para separar los logs de protección DoS de otros logs de amenazas. Reenvíe los eventos de infracción del umbral DoS directamente a los administradores por correo electrónico además de reenviar los logs a un servidor, como un servidor SNMP o syslog. Siempre que los cortafuegos sean del tamaño adecuado, las brechas en el umbral no deberían ser frecuentes y se proporcionarán indicadores sólidos de los intentos de ataque.

© 2020 Palo Alto Networks, Inc.

Configuración de la protección de la zona para aumentar la seguridad de la red

Los siguientes temas proporcionan ejemplos de configuración de la protección de la zona:

- Configuración de la protección de reconocimiento
- Configuración de la protección de ataques basada en paquetes
- Configuración de la protección de protocolos
- Configuración de la protección de búfer de paquetes
- Configuración de la protección de búfer de paquetes basada en la latencia
- Configuración de la protección de SGT Ethernet

Configuración de la protección de reconocimiento

Configure una de las siguientes medidas de Protección de reconocimiento para que el cortafuegos responda al intento de reconocimiento correspondiente:

- **Allow (Permiso)**: el cortafuegos permite el reconocimiento de la exploración de puertos o la limpieza de host para continuar.
- **Alert (Alerta)**: el cortafuegos genera una alerta para cada exploración de puertos o limpieza de host que coincida con el umbral configurado dentro del intervalo de tiempo especificado. La alerta es la medida predeterminada.
- **Block (Bloqueo)**: el cortafuegos descarta los siguientes paquetes enviados desde el origen al destino durante el resto del intervalo de tiempo especificado.
- **Block IP (IP de bloqueo)**: el cortafuegos descarta los siguientes paquetes para la **Duration (Duración)** especificada, en segundos (rango: 1 a 3600). **Track By (Rastrear por)** determina si el cortafuegos bloquea el tráfico de origen o el de origen y destino.

STEP 1 | Configure la protección de reconocimiento.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de redes)** > **Zone Protection (Protección de zonas)**
2. Seleccione un perfil de protección de zona o seleccione **Add (Añadir)** para añadir un perfil nuevo e introduzca un nombre en **Name (Nombre)**.
3. En la pestaña Reconnaissance Protection (Protección de reconocimiento), seleccione los tipos de exploración de los que debe protegerse.
4. Seleccione una **Action (Medida)** para cada exploración. Si selecciona Block IP (IP de bloqueo), también debe configurar **Track By (Rastrear por)** (tráfico de origen o el de origen y destino) y **Duration (Duración)**.
5. Configure el **Interval (Intervalo)** en segundos. Estas opciones definen el intervalo de tiempo para la detección de la exploración de puertos y la limpieza de host.
6. Configure el **Threshold (Umbral)**. El umbral define la cantidad de eventos de exploración de puertos o limpieza de host que suceden dentro del intervalo configurado previamente que activa una medida.

STEP 2 | (Opcional) Configure una exclusión de dirección de origen.

1. En la pestaña Reconnaissance Protection (Protección de reconocimiento), haga clic en **Add (Añadir)** para añadir una exclusión de dirección de origen.
    1. Introduzca un **nombre** descriptivo para la dirección que desee excluir.
    2. Configure **IPv4** o **IPv6** como Address Type (Tipo de dirección), y seleccione un objeto de dirección o introduzca una dirección IP.

© 2020 Palo Alto Networks, Inc.

3. Haga clic en **OK (Aceptar)**.
2. Haga clic en **OK (Aceptar)** para guardar el perfil de protección de zona.
3. **Commit (Confirmar)** los cambios.

Configuración de la protección de ataques basada en paquetes

Para mejorar la seguridad de una zona, Protección de ataques basados en paquetes le permite especificar si el cortafuegos debe descartar paquetes IP, IPv6, TCP, ICMP o ICMPv6 con ciertas características o quitar determinadas opciones de los paquetes.

Por ejemplo, puede descartar paquetes TCP SYN y SYN-ACK con datos en la carga durante un protocolo de enlace de tres pasos. Un perfil de protección de zona se configura de manera predeterminada para descartar paquetes SYN y SYN-ACK con datos (debe aplicar el perfil a la zona).

La opción TCP Fast Open (Apertura rápida de TCP) (RFC 7413) conserva la velocidad de una configuración de conexión incluyendo datos en la carga de los paquetes SYN y SYN-ACK. Un perfil de protección de zona trata a los protocolos de enlace que utilizan la opción de apertura rápida de TCP independientemente de otros paquetes SYN y SYN-ACK. De manera predeterminada, el perfil se configura para permitir los paquetes de protocolo de enlace si contienen cookies válidas de apertura rápida.

Si ya implementó perfiles de protección de zona cuando actualizó PAN-OS 8.0, las tres configuraciones predeterminadas se aplicarán a cada perfil y el cortafuegos actuará en consecuencia.

Comenzando por PAN-OS 8.1.2 y versiones posteriores, puede usar un comando de CLI (paso 4 en esta tarea) para permitir que el cortafuegos genere un log de amenazas cuando reciba y descarte los siguientes tipos de paquetes, de modo que pueda analizar más fácilmente estas ocurrencias y también satisfacer los requisitos de auditoría y cumplimiento:

- Ataque Teardrop
- Ataque DoS que usa el ping de la muerte

Además, el mismo comando de CLI también permite que el cortafuegos genere logs de amenazas para los siguientes tipos de paquetes si habilita la correspondiente protección de ataques basada en paquetes:

- Paquetes de IP fragmentados
- Duplicación de dirección IP
- Paquetes ICMP con un tamaño mayor de 1024 bytes
- Paquetes que contienen fragmentos ICMP
- Paquetes ICMP que se incrustan con un mensaje de error
- Primeros paquetes para una sesión TCP que no son paquetes SYN

STEP 1 | Cree un perfil de protección de zona y configure los ajustes de la protección de ataques basada en paquetes.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y **Add (Añadir)** para añadir un nuevo perfil.
2. En **Name (Nombre)**, introduzca un nombre para el perfil y, opcionalmente, una **Description (Descripción)**.
3. Seleccione **Packet Based Attack Protection (Protección de ataques basada en paquetes)**.
4. En cada pestaña (**IP Drop [Descarte de IP]**, **TCP Drop [Descarte de TCP]**, **ICMP Drop [Descarte de ICMP]**, **IPv6 Drop [Descarte de IPv6]** y **ICMPv6 Drop [Descarte de ICMPv6]**), seleccione los ajustes de protección de ataque basada en paquetes que desee aplicar para proteger una zona.
5. Haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Aplique el perfil de protección de zona a una zona de seguridad que se asigna a las interfaces que desea proteger.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione la zona a la que desea asignar el perfil de protección de zona.
2. **Add (Añada)** las **Interfaces (Interfaces)** de la zona.
3. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil que acaba de crear.
4. Haga clic en **OK (Aceptar)**.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | (PAN-OS 8.1.2 y versiones posteriores) Permita que el cortafuegos genere logs de amenazas para un ataque Teardrop y un ataque DoS con el ping de la muerte, y también genere logs de amenazas para los tipos de paquetes detallados anteriormente si habilita la correspondiente protección de ataques basados en paquetes (en el paso 1). Por ejemplo, si habilita la protección de ataques basados en paquetes para **Spoofed IP address (Dirección IP duplicada)**, usar la siguiente CLI provoca que el cortafuegos genere un log de amenazas cuando recibe y descarta un paquete con una dirección IP duplicada.

1. Acceda a la CLI.
2. Use el comando operativo de la CLI **`set systemsetting additional-threat-log on`**. El valor predeterminado es **`off`**.

Configuración de la protección de protocolos

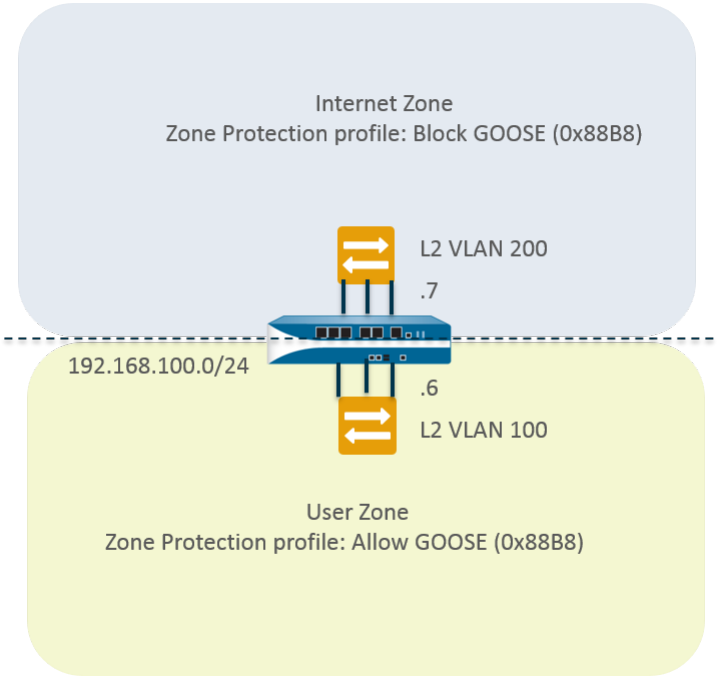
Proteja el cable virtual o las zonas de seguridad de capa 2 de los paquetes de protocolo no IP utilizando Protección de protocolo.

- Caso de uso: Protección de protocolo no IP entre zonas de seguridad en interfaces de capa 2
- Caso de uso: Protección de protocolo no IP dentro de una zona de seguridad en interfaces de capa 2

Caso de uso: Protección de protocolo no IP entre zonas de seguridad en interfaces de capa 2

En este caso de uso, el cortafuegos se encuentra en una VLAN de capa 2 dividida en dos subinterfaces. VLAN 100 es 192.168.100.1/24, subinterfaz .6. VLAN 200 es 192.168.100.1/24, subinterfaz .7. La protección de protocolo no IP se aplica a zonas de ingreso. En este caso de uso, si la zona de internet es la zona de ingreso, el cortafuegos bloquea el protocolo de eventos de subestaciones orientados a objetos genéricos (Generic Object Oriented Substation Event, GOOSE). Si la zona de usuario es la zona de ingreso, el cortafuegos permite el protocolo GOOSE. El cortafuegos permite implícitamente IPv4, IPv6, ARP y tramas con etiqueta de VLAN en ambas zonas.

© 2020 Palo Alto Networks, Inc.



STEP 1 | Configure dos subinterfaces VLAN.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en **Add (Añadir)** para añadir una interfaz.
2. El valor predeterminado de **Interface Name (Nombre de interfaz)** es vlan. Luego del punto, introduzca 7.
3. En la pestaña **Config (Configuración)**, configure **Assign Interface To (Asignar la interfaz a)** de la **VLAN** en 200.
4. Haga clic en **OK (Aceptar)**.
5. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en **Add (Añadir)** para añadir una interfaz.
6. El valor predeterminado de **Interface Name (Nombre de interfaz)** es vlan. Luego del punto, introduzca 6.
7. En la pestaña **Config (Configuración)**, configure **Assign Interface To (Asignar la interfaz a)** de la **VLAN** en 100.
8. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure la protección de protocolo en un perfil de protección de zona para bloquear los paquetes de protocolo GOOSE.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca en **Name (Nombre)** el nombre Block GOOSE.
3. Seleccione **Protocol Protection (Protección de protocolo)**.
4. Seleccione **Rule Type (Tipo de regla)** para la **Exclude List (Lista de exclusión)**.
5. Introduzca el nombre de protocolo GOOSE en **Protocol Name (Nombre de protocolo)** para identificar con facilidad el Ethertype en la lista. El cortafuegos no comprueba que el nombre que introduce coincida con el código Ethertype; solo utiliza el código Ethertype para el filtrado.
6. Introduzca el código **Ethertype** 0x88B8. Se debe introducir 0x antes del código Ethertype para indicar un valor hexadecimal. El rango es 0x0000 a 0xFFFF.
7. Seleccione **Enable (Habilitar)** para habilitar la protección del protocolo. Puede deshabilitar un protocolo de la lista, por ejemplo, para una prueba.

© 2020 Palo Alto Networks, Inc.

8. Haga clic en **OK (Aceptar)**.

STEP 3 | Aplique el perfil de protección de zona a la zona de internet.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una zona.
2. Introduzca en **Name (Nombre)** el nombre de la zona, Internet.
3. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
4. En **Type (Tipo)**, seleccione **Layer2 (Capa 2)**.
5. Haga clic en **Add (Añadir)** para añadir la interfaz que pertenezca a la zona, vlan.7 en **Interfaces**.
6. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil de bloqueo GOOSE.
7. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure la protección de protocolos para permitir los paquetes de protocolo GOOSE.

Cree otro perfil de protección de zona denominado Allow GOOSE (Permitir GOOSE) y seleccione el **Rule Type (Tipo de regla)** de la **Include List (Lista de inclusión)**.

Cuando configure la lista de inclusión, incluya todos los protocolos no IP necesarios; una lista incompleta puede provocar que se bloquee tráfico no IP legítimo.

STEP 5 | Aplique un perfil de protección de zona a la zona User (Usuario):

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una zona.
2. Introduzca el **Name (Nombre)** de la zona User (Usuario).
3. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
4. En **Type (Tipo)**, seleccione **Layer2 (Capa 2)**.
5. Haga clic en **Add (Añadir)** para añadir la interfaz que pertenezca a la zona, vlan.6 en **Interfaces**.
6. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil Allow GOOSE (Permitir GOOSE).
7. Haga clic en **OK (Aceptar)**.

STEP 6 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

STEP 7 | Vea la cantidad de paquetes no IP que el cortafuegos ha descartado en función de la protección de protocolos.

Acceso a la CLI.

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

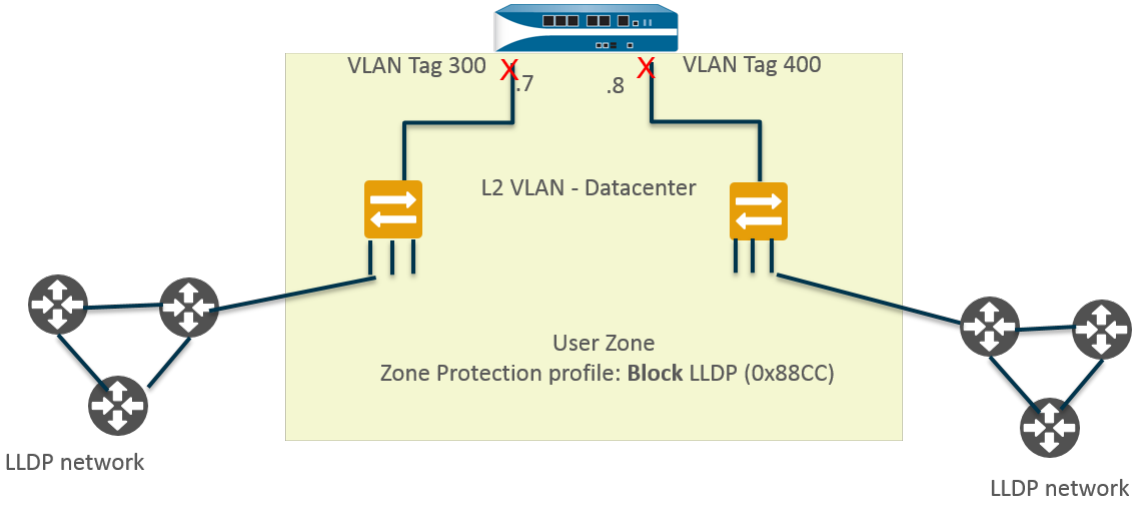
Caso de uso: Protección de protocolo no IP dentro de una zona de seguridad en interfaces de capa 2

Si no implementa un perfil de protección de zona con protección de protocolo no IP, el cortafuegos permite que los protocolos no IP en una zona se transporten de una interfaz de capa 2 a otra. En este caso de uso, bloquear los paquetes de LLDP garantiza que el LLDP de una red no detecte una red alcanzable desde otra interfaz en la zona.

En la siguiente figura, la VLAN de capa 2 denominada Datacenter (Centro de datos) se divide en dos subinterfaces: 192.168.1.1/24, subinterfaz .7 y 192.168.1.2/24, subinterfaz .8. La VLAN pertenece a la zona de usuario. Si se aplica un perfil de protección de zona que bloquee el LLDP a la zona de usuario:

© 2020 Palo Alto Networks, Inc.

- La subinterfaz .7 bloquea el LLDP de su conmutador al cortafuegos en la red X de la izquierda, lo que evita que el tráfico llegue a la subinterfaz .8.
- La subinterfaz .8 bloquea el LLDP de su conmutador al cortafuegos en la red X de la izquierda, lo que evita que el tráfico llegue a la subinterfaz .7.



STEP 1 | Cree una subinterfaz para una interfaz Ethernet.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz de capa 2, en este ejemplo, ethernet1/1.
2. Seleccione **Add Subinterfaces (Añadir subinterfaces)**.
3. El valor de **Interface Name (Nombre de interfaz)** vuelve al valor predeterminado de la interfaz (ethernet 1/1). Luego del punto, introduzca 7.
4. En **Tag (Etiqueta)**, introduzca 300.
5. En **Security Zone (Zona de seguridad)**, seleccione User (Usuario).
6. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree una segunda subinterfaz para la interfaz Ethernet.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione la interfaz de capa 2: ethernet1/1.
2. Seleccione **Add Subinterfaces (Añadir subinterfaces)**.
3. El valor de **Interface Name (Nombre de interfaz)** vuelve al valor predeterminado de la interfaz (ethernet 1/1). Luego del punto, introduzca 8.
4. En **Tag (Etiqueta)**, introduzca 400.
5. En **Security Zone (Zona de seguridad)**, seleccione User (Usuario).
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree una VLAN para la interfaz Layer2 y dos subinterfaces.

1. Seleccione **Network (Red)** > **VLANs (VLAN)** y haga clic en **Add (Añadir)** para añadir una VLAN.
2. Introduzca un nombre en **Name (Nombre)** de la VLAN; para este ejemplo, introduzca Datacenter (Centro de datos).
3. En **VLAN Interface (Interfaz de VLAN)**, seleccione **None (Ninguno)**.
4. En **Interfaces**, haga clic en **Add (Añadir)** y seleccione la interfaz de capa 2: ethernet1/1 y dos interfaces: ethernet1/1.7 y ethernet1/1.8.
5. Haga clic en **OK (Aceptar)**.

STEP 4 | Bloquee los paquetes de protocolo no IP en un perfil de protección de zona.

© 2020 Palo Alto Networks, Inc.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y **Add (Añadir)** para añadir un perfil.
2. Introduzca un nombre en **Name (Nombre)**, en este ejemplo, Block LLDP (LLDP de bloqueo).
3. Introduzca una descripción del perfil en **Description (Descripción)**: bloquee los paquetes LLDP provenientes de una red LLDP hacia otras interfaces de la zona (intrazona).
4. Seleccione **Protocol Protection (Protección de protocolo)**.
5. Seleccione **Rule Type (Tipo de regla)** para la **Exclude List (Lista de exclusión)**.
6. Introduzca el **Protocol Name (Nombre de protocolo)** LLDP.
7. Introduzca el código **Ethertype** 0x88cc. Se debe introducir 0x antes del código Ethertype para indicar un valor hexadecimal.
8. Seleccione **Enabled (Habilitado)**.
9. Haga clic en **OK (Aceptar)**.

STEP 5 | Aplique el perfil de protección de zona a la zona de seguridad a la que pertenece la VLAN de capa 2.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Haga clic en **Add (Añadir)** para añadir una zona.
3. Introduzca el **Name (Nombre)** de la zona User (Usuario).
4. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
5. En **Type (Tipo)**, seleccione **Layer2 (Capa 2)**.
6. Haga clic en **Add (Añadir)** para añadir una **Interface (Interfaz)** que pertenezca a la zona, ethernet1/1.7
7. Haga clic en **Add (Añadir)** para añadir una **Interface (Interfaz)** que pertenezca a la zona, ethernet1/1.8
8. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil Block LLDP (LLDP de bloqueo).
9. Haga clic en **OK (Aceptar)**.

STEP 6 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

STEP 7 | Vea la cantidad de paquetes no IP que el cortafuegos ha descartado en función de la protección de protocolos.

Acceso a la CLI.

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

Configuración de la protección de búfer de paquetes

Puede configurar la protección de búfer de paquetes en dos niveles: el nivel del dispositivo (global) y, si está habilitado globalmente, también puede habilitarlo en el nivel de zona. La protección global de búfer de paquetes (**Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)**) es para proteger los recursos del cortafuegos y garantizar que el tráfico malicioso no provoque que el cortafuegos deje de responder.

La protección de búfer de paquetes por zona de ingreso (**Network (Red)** > **Zones (Zonas)**) es una segunda capa de protección que comienza con el bloqueo de la dirección IP infractora si continúa superando los umbrales de protección de búfer de paquetes. El cortafuegos puede bloquear todo el tráfico de la dirección IP de origen infractora. Tenga en cuenta que si la dirección IP de origen es una dirección IP NAT traducida, puede que muchos usuarios estén utilizando la misma dirección IP. Si un usuario abusivo activa la protección de búfer de paquetes y la zona de ingreso tiene habilitada la protección de búfer de paquetes,

© 2020 Palo Alto Networks, Inc.

todo el tráfico de esa dirección IP de origen infractora (incluso de usuarios no abusivos) puede bloquearse cuando el cortafuegos coloque la dirección IP en la lista de bloqueo.

La forma más efectiva de bloquear los ataques DoS contra un servicio detrás del cortafuegos es configurar la protección de búfer de paquetes globalmente y por zona de ingreso.

Puede **habilitar la protección de búfer de paquetes para una zona**, pero no estará activa hasta que habilite la protección de búfer de paquetes globalmente y especifique la configuración.

STEP 1 | Habilite la protección de búfer de paquetes globalmente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Packet Buffer Protection (Protección de búfer de paquetes)**.
3. Defina el comportamiento de la protección de búfer de paquetes:
   - **Alert (%) [Alerta (%)]**: cuando la utilización del búfer de paquetes supera este umbral durante más de 10 segundos, el cortafuegos crea un evento de log cada minuto. El intervalo es del 0 al 99 %; el valor predeterminado es del 50 %. Si el valor es 0%, el cortafuegos no crea un evento de log.
   - **Activate (%) (Activar (%))**: cuando la utilización del búfer de paquetes alcance este umbral, el cortafuegos comenzará a reducir las sesiones más abusivas mediante la aplicación de descarte aleatorio temprano (Random Early Drop, RED). El intervalo es del 0 al 99 %; el valor predeterminado es del 50 %. Si el valor es 0%, el cortafuegos no aplica Random Early Drop (RED). Si el abusador está entrando en una zona que tiene habilitada la protección de búfer de paquetes, el cortafuegos también puede descartar la sesión abusiva o bloquear la dirección IP de origen infractora. Comience con el límite predeterminado y ajústelo si fuera necesario.

     El cortafuegos registra eventos de alerta en el log del sistema y eventos de tráfico descartado, sesiones descartadas y direcciones IP bloqueadas en el log de amenazas.
   - **Block Hold Time (sec) (Tiempo de espera del bloqueo (s))**: tiempo, en segundos, que se permite a la sesión con mitigación de RED continuar antes de que el cortafuegos la descarte. El intervalo es de 0 65,535; el valor predeterminado es 60. Si el valor es 0, el cortafuegos no descarta sesiones basadas en la protección de búfer de paquetes.
   - **Block Duration (sec) (Duración del bloqueo (s))**: número de segundos que una sesión permanece descartada o una dirección IP permanece bloqueada. El intervalo es de 1 a 15 999 999; el valor predeterminado es 3600.
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

STEP 2 | Habilite la protección del búfer de paquetes en una zona de ingreso.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Seleccione una zona de ingreso y haga clic en su nombre.
3. **Habilite la protección de búfer de paquetes** en la sección Zone Protection (Protección de zona).
4. Haga clic en **OK (Aceptar)**.
5. **Commit (Confirmar)** los cambios.

Configuración de la protección de búfer de paquetes basada en la latencia

Configure la protección del búfer de paquetes basada en la latencia y aplíquela a las zonas que tienen tráfico que consta de protocolos y aplicaciones que son sensibles a la latencia.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)**.

© 2020 Palo Alto Networks, Inc.

STEP 2 | Edite la sección Session Settings (Configuración de sesión) y habilite la **protección de búfer de paquetes**.

STEP 3 | Habilite **Buffering Latency Based (Almacenamiento en búfer basado en latencia)**.

STEP 4 | Especifique el umbral de **alerta de latencia (milisegundos)** por encima del que el cortafuegos comienza a generar un evento de log de alerta cada minuto; el intervalo es de 1 a 20 000; el valor predeterminado es 50.

STEP 5 | Especifique el umbral de **Latency Activate (miliseconds) (Activación de latencia [milisegundos])** por encima del que el cortafuegos activará el descarte temprano aleatorio (RED, Random Early Drop) en los paquetes entrantes y comenzará a generar un log de activación cada 10 segundos; el intervalo es de 1 a 20 000 ms; el valor predeterminado es 200 ms.

STEP 6 | Especifique el umbral de **Latency Max Tolerate (milliseconds) (Tolerancia máxima de latencia [milisegundos])** por encima del que el cortafuegos usará RED con una probabilidad de descarte cercana al 100 %; el intervalo es de 1 a 20 000 ms; el valor predeterminado es 500 ms.

Si la latencia actual es un valor entre el umbral de **Latency Activate (Activación de latencia)** y el umbral de **Latency Max Tolerate (Tolerancia máxima de latencia)**, el cortafuegos calcula la probabilidad de descarte de RED de la siguiente manera: (latencia actual - umbral de **Latency Activate (Activación de latencia)**) / (umbral de **Latency Max Tolerate (Tolerancia máxima de latencia)** - umbral de **Latency Activate (Activación de latencia)**). Por ejemplo, si la latencia actual es 300, **Latency Activate (Activación de latencia)** es 200 y **Latency Max Tolerate (Tolerancia máxima de latencia)** es 500. Por lo tanto, (300-200)/(500-200) = 1/3, lo que significa que el cortafuegos utiliza aproximadamente un 33 % de probabilidad de descarte de RED.

STEP 7 | Configure el **tiempo de espera de bloqueo** y la **duración de bloqueo** a partir de la protección de búfer de paquetes basada en la utilización.

STEP 8 | Haga clic en **OK (Aceptar)**.

STEP 9 | Habilite la segunda capa de protección para cada zona en la que desee protección de búfer de paquetes basada en latencia.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione una zona.
2. Habilite la **protección de búfer de paquetes**.

STEP 10 | Seleccione **Confirmar**.

Configuración de la protección de SGT Ethernet

Utilice la siguiente tarea para configurar un perfil Protección de SGT Ethernet.

STEP 1 | Cree un perfil de protección de zona para proporcionar protección de Ethernet SGT.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de redes)** > **Zone Protection (Protección de zonas)**
2. **Añada** un perfil de protección de zona por **nombre**.
3. Seleccione **Ethernet SGT Protection (Protección de SGT Ethernet)**.
4. **Añada** una **Lista de exclusión de SGT de capa 2** por nombre.
5. Especifique uno o más valores de **etiqueta** para la lista; el intervalo es de 0 a 65.535. Puede establecer entradas individuales que sean un intervalo contiguo de valores de etiqueta (por ejemplo, 100-500). Puede añadir hasta 100 entradas de etiquetas (individuales o de intervalo) en una lista de exclusión.

© 2020 Palo Alto Networks, Inc.

6. **Habilite** la lista de exclusión de SGT de capa 2. Puede deshabilitar la lista en cualquier momento.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Aplique el perfil de protección de zona a la zona de seguridad a la que pertenecen las interfaces de capa 2, cable virtual o de Tap.

1. Seleccione **Network (Red)** > **Zones (Zonas)**.
2. Haga clic en **Add (Añadir)** para añadir una zona.
3. Introduzca el **Name (Nombre)** de la zona.
4. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
5. Para **Type (Tipo)**, seleccione **Layer2 (Capa 2)**, **Virtual Wire (Cable virtual)** o **Tap**.
6. Haga clic en **Add (Añadir)** para añadir una **interfaz** que pertenezca a la zona.
7. En **Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil que ha creado.
8. Haga clic en **OK (Aceptar)**.

STEP 3 | Seleccione **Confirmar**.

STEP 4 | Vea el contador global de paquetes que el cortafuegos eliminó como resultado de todos los perfiles de protección de zona que emplean la protección Ethernet SGT.

1. Acceda la CLI.
2. > `show counter global name pan_flow_dos_l2_sec_tag_drop`

© 2020 Palo Alto Networks, Inc.

Protección DoS contra inundaciones de nuevas sesiones

La protección DoS contra la inundación de nuevas sesiones es útil contra los ataques de una sesión y múltiples sesiones de gran volumen. En un ataque de una única sesión, un atacante usa una única sesión para dirigirse contra un dispositivo situado tras el cortafuegos. Si una regla de seguridad admite el tráfico, la sesión se establece y el atacante inicia un ataque enviando paquetes a una tasa muy elevada con la misma dirección IP y número de puerto de origen, dirección IP y número de puerto de destino y protocolo para intentar sobrecargar al objetivo. En un ataque de múltiples sesiones, un atacante emplea múltiples sesiones (o conexiones por segundo [cps]) desde un único host para iniciar un ataque DoS.

Esta función solo protege contra los ataques DoS de nuevas sesiones, es decir, el tráfico que no se ha descargado en el hardware. Esta función no protege contra ataques descargados. Sin embargo, este tema describe cómo crear una regla de políticas de seguridad para restablecer el cliente; el atacante reinicia el ataque con numerosas conexiones por segundo y es bloqueado por las defensas que se indican en este tema.

Perfiles de protección y reglas de la política del DoS funcionan en conjunto para ofrecer protección contra inundaciones de diversos paquetes SYN, UDP, ICMP e ICMPv6 entrantes y otros tipos de paquetes IP. Puede determinar los umbrales que constituyen una inundación. Por lo general, el perfil de protección DoS establece los umbrales en los que el cortafuego genera una alarma DoS, realiza una acción como Random Early Drop (Descarte aleatorio temprano) y descarta conexiones entrantes adicionales. La regla de la política de protección DoS que se configura como protect (proteger) (en lugar de permitir o denegar paquetes) determina los criterios de coincidencia de los paquetes (como dirección de origen) que se tendrán en cuenta para el umbral. Esta flexibilidad le permite bloquear determinado tráfico o permitir determinado tráfico y tratar otro tráfico como tráfico DoS. Cuando la tasa entrante supera el umbral máximo, el cortafuegos bloquea el tráfico entrante de la dirección de origen.

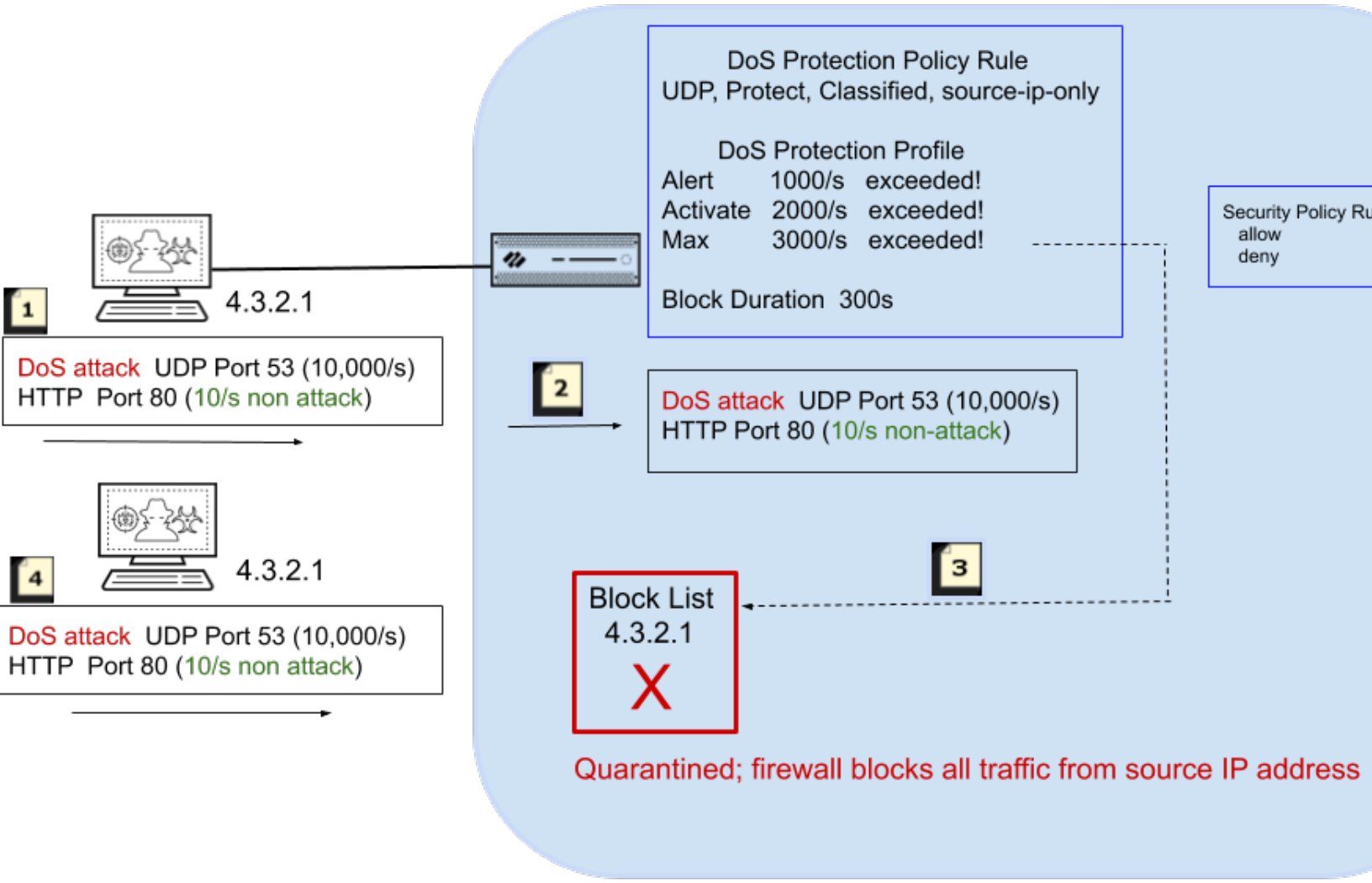
- Ataque DoS multisesión
- Ataque DoS de una sesión
- Configuración de protección DoS contra inundaciones de nuevas sesiones
- Finalización de un ataque DoS de una sesión
- Identificación de sesiones que utilizan un porcentaje excesivo del búfer de paquete
- Eliminación de una sesión sin confirmación

Ataque DoS multisesión

Realice la configuración de protección DoS contra inundaciones de nuevas sesiones configurando una regla de políticas de protección DoS, que determina los criterios que activan la acción **Protect (Proteger)** cuando coinciden con paquetes entrantes. El perfil de protección cuenta cada nueva conexión en los umbrales Tasa de alarma, Tasa de activación y Tasa máxima. Cuando las conexiones nuevas entrantes por segundo superan la Tasa máxima, el cortafuegos toma la medida especificada en el perfil de protección DoS.

La siguiente figura y tabla describen cómo funcionan juntas las reglas de políticas de seguridad, las reglas de política de protección DoS y el perfil en un ejemplo.

© 2020 Palo Alto Networks, Inc.



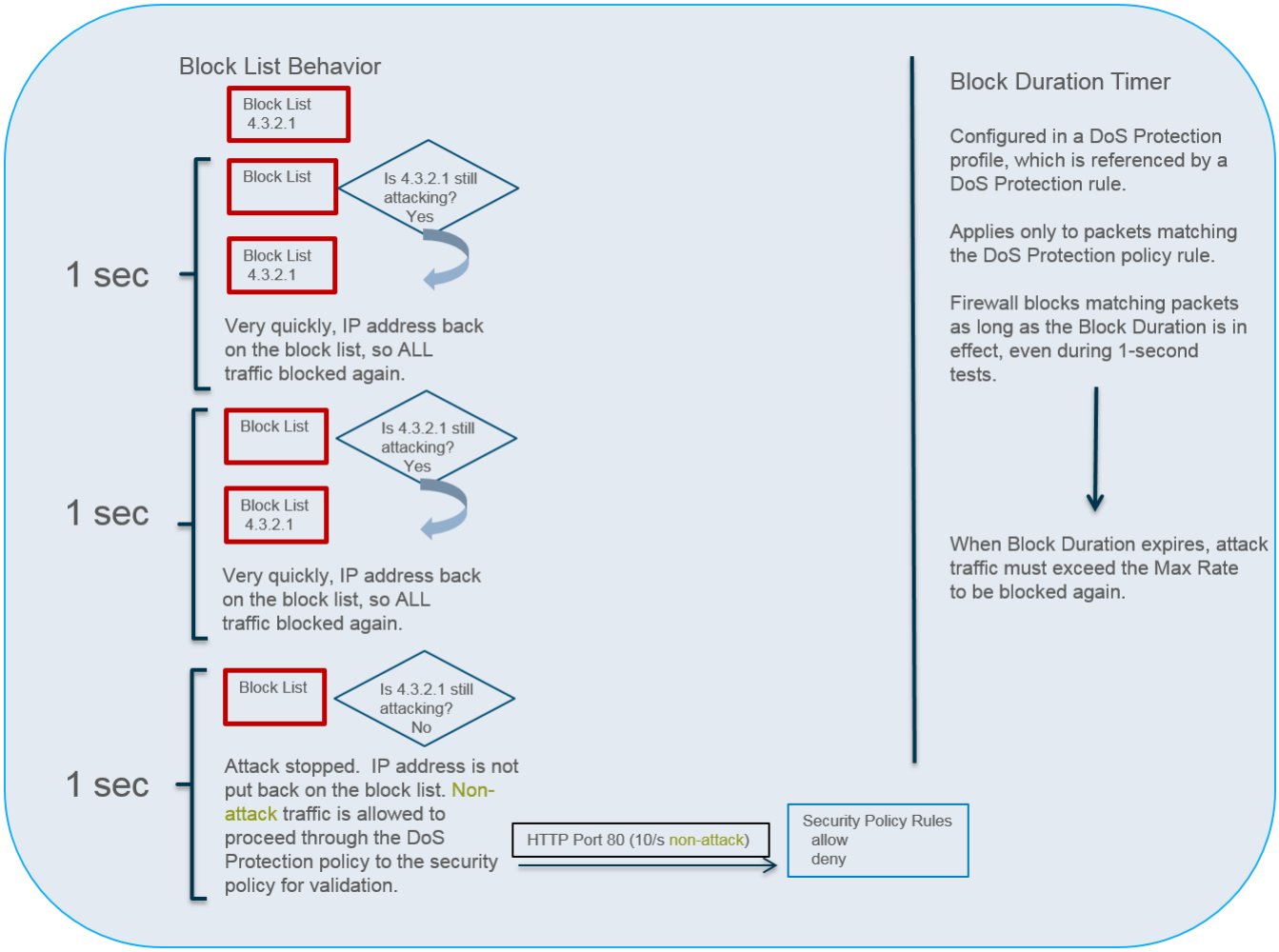
Secuencia de eventos cuando un cortafuegos pone una dirección IP en cuarentena	
1	En este ejemplo, un atacante inicia un ataque DoS a una tasa de 10 000 conexiones nuevas por segundo al puerto 53 de UDP. El atacante también envía 10 conexiones nuevas por segundo al puerto 80 de HTTP.
2	Las nuevas conexiones coinciden con los criterios de la regla de política de protección DoS, como una interfaz o zona de origen, dirección IP de origen, zona o interfaz de destino, dirección IP de destino o servicio, entre otros ajustes. En este ejemplo, la regla de política especifica UDP. La regla de política de protección DoS también especifica la acción **Protect (Proteger)** y **Classified (Clasificado)**, dos ajustes que dinámicamente poner en vigor los ajustes de perfil de protección DoS. El perfil de protección DoS especifica que se permite una tasa máxima de 3000 paquetes por segundo. Cuando los paquetes entrantes coinciden con la regla de política de protección DoS, las nuevas conexiones por

© 2020 Palo Alto Networks, Inc.

Secuencia de eventos cuando un cortafuegos pone una dirección IP en cuarentena	
	segundo se incluyen en los umbrales de **Alert (Alerta)**, **Activate (Activar)** y **Max Rate (Tasa máxima)**. *También puede usar una regla de políticas de seguridad para bloquear todo el tráfico desde la dirección IP de origen si considera que esa dirección es malintencionada siempre.*
3	Las 10 000 conexiones nuevas por segundo superan el umbral de Tasa máxima. Cuando se produce todo lo siguiente: • el umbral se supera, • se especifica una duración de bloque y • **Classified (Clasificado)** se define para incluir una dirección IP de origen, el cortafuegos incluye la dirección IP de origen infractora en la lista de bloqueados.
4	Una dirección IP en la lista de bloqueados está en cuarentena, lo que significa que todo el tráfico procedente de esa dirección IP queda bloqueado. El cortafuegos bloquea la dirección IP de origen antes de que los paquetes de ataque adicionales lleguen a la política de seguridad.

La siguiente figura describe más detalladamente lo que ocurre cuando una dirección IP que coincide con la regla de política de protección de DoS se incluye en la lista de bloqueados. También describe el temporizador de duración del bloqueo.

© 2020 Palo Alto Networks, Inc.



Cada segundo, el cortafuegos permite que la dirección IP salga de la lista de bloqueados para poder probar los patrones de tráfico y determinar si el ataque sigue activo. El cortafuegos realiza la siguiente acción:

- Durante este periodo de prueba de un segundo, el cortafuegos permite que los paquetes que no coinciden con los criterios de la política de protección DoS (tráfico HTTP en este ejemplo) atraviesen las reglas de políticas de protección DoS en la política de seguridad para la validación. Muy pocos paquetes, o ninguno, tienen tiempo para llegar, porque el primer paquete de ataque que recibe el cortafuegos después de dejar que la dirección IP salga de la lista de bloqueados coincidirá con los criterios de la política de protección DoS, lo que rápidamente hará que la dirección IP se devuelva rápidamente a la lista de bloqueados durante otro segundo. El cortafuegos repite esta prueba cada segundo hasta que el ataque se detiene.
- El cortafuegos evita que todo el tráfico de ataque pase las reglas de política de protección DoS (la dirección se mantiene en la lista de bloqueados) hasta que vence la duración de bloqueo.

En la figura anterior se ilustran las comprobaciones que se realizan cada segundo en los modelos de cortafuegos que tienen varias CPU de planos de datos y un procesador de red de hardware. Si los sistemas tienen un solo plano de datos o no tienen ningún procesador de red de hardware, ejecutan la mitigación en el software cada cinco segundos.

Cuando el ataque se detiene, el cortafuegos no devuelve la dirección IP a la lista de bloqueados. El cortafuegos permite que el tráfico que no sea de ataque atraviese las reglas de políticas de protección DoS a las reglas de política de seguridad para su evaluación. Debe configurar una regla de política de seguridad para permitir o denegar el tráfico porque, sin una, una regla de denegación implícita deniega todo el tráfico.

© 2020 Palo Alto Networks, Inc.

La lista de bloqueados se basa en una combinación de zona de origen y dirección de origen. Este comportamiento permite que las direcciones IP duplicadas existan siempre y cuando estén en distintas zonas que pertenecen a enrutadores virtuales separados.

El ajuste de duración de bloqueo en un perfil de protección DoS especifica durante cuánto tiempo el cortafuegos bloquea los paquetes (infractores) que coinciden exactamente con una regla de política de protección DoS. El tráfico del ataque sigue bloqueado hasta que vence la duración del bloqueo, después de lo cual el tráfico del ataque debe superar de nuevo el umbral de tasa máxima para que pueda volver a bloquearse.

Si el atacante usa múltiples sesiones o bots que inician múltiples sesiones de ataque, las sesiones cuentan hacia los umbrales del perfil de protección DoS sin una regla de denegación de política de seguridad vigente. Por lo tanto, un ataque de sesión única requiere una regla de denegación o descarte de política de seguridad para que cada paquete cuente en los umbrales; en cambio, un ataque de sesión múltiple no la necesita.

Por ello, la protección DoS contra la inundación de nuevas sesiones permite que el cortafuegos proteja eficientemente contra una dirección IP de origen mientras haya tráfico de ataque en curso, y permite que el tráfico que no sea de ataque pase en cuanto se detenga el ataque. El colocar la dirección IP infractora en la lista de bloqueados permite que la funcionalidad de protección DoS aproveche la lista de bloqueados, lo cual está diseñado para poner en cuarentena toda la actividad de esa dirección IP de origen, tal como paquetes con una aplicación diferente. Poner la dirección IP en cuarentena de toda actividad protege contra atacantes modernos que intentan un ataque de aplicación rotatorio, en el que el atacante simplemente cambia de aplicación para iniciar un nuevo ataque o usa una combinación de diferentes ataques en un ataque DoS híbrido. Puede Supervisar direcciones IP bloqueadas para visualizar la lista de bloqueo, eliminar entradas de dicha lista y obtener información adicional sobre una dirección IP de la lista de bloqueo.

A partir de PAN-OS 7.0.2, hay un cambio de comportamiento que hace que el cortafuegos sitúe la dirección IP de origen de ataque en la lista de bloqueo. Cuando el ataque se detiene, el tráfico de no ataque puede continuar con el cumplimiento de la política de seguridad. El tráfico de ataque que coincidía con el perfil de protección DoS y las reglas de política de protección DoS continúa bloqueado hasta que vence la duración de bloqueo.

Ataque DoS de una sesión

Un ataque DoS de una sesión no suele desactivar los perfiles de zona o protección DoS porque eran ataques que se formaban después de crear la sesión. La política de seguridad permite estos ataques porque se permite crear una sesión y, una vez que la sesión se ha creado, el ataque incrementa el volumen del paquete y anula el dispositivo de destino.

Configuración de protección DoS contra inundaciones de nuevas sesiones para proteger contra la inundación de nuevas sesiones (inundación de una sesión y múltiples sesiones). En caso de que haya un ataque de única sesión en curso, también puede realizar Finalización de un ataque DoS de una sesión.

Configuración de protección DoS contra inundaciones de nuevas sesiones

STEP 1 | Configure las reglas de política de seguridad para denegar el tráfico desde la dirección IP del atacante y permitir otro tráfico basado en sus necesidades de red. Puede especificar cualquier criterio de coincidencia en una regla de política de seguridad como la dirección IP de origen. (Obligatorio para la mitigación de ataques de una sesión o los ataques que no han activado el umbral de la política de protección DoS; opcional para la mitigación de ataques de sesión múltiple).

© 2020 Palo Alto Networks, Inc.

Este paso es uno de los pasos que suele realizarse para detener un ataque existente. Consulte Finalización de un ataque DoS de una sesión.

- Creación de una regla de política de seguridad

STEP 2 | Configure un perfil de protección DoS para la protección de inundación.

Como los ataques de inundación pueden ocurrir en múltiples protocolos, se recomienda activar la protección para todos los tipos de inundaciones en el perfil de protección DoS.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **DoS Protection (Protección DoS)** y **Add (Añadir)** para añadir un nombre de perfil en **Name (Nombre)**.
2. Seleccione **Classified (Clasificado)** como el **Type (Tipo)**.
3. Para **Flood Protection (Protección contra congestión)**, seleccione todos los tipos de protección contra congestión.
   - **Congestión SYN**
   - **Congestión UDP**
   - **Congestión ICMP**
   - **Congestión de ICMPv6**
   - **Otra congestión IP**
4. Cuando habilite **SYN Flood (Congestión SYN)**, seleccione la **Action (Acción)** que ocurre cuando las conexiones por segundo (cps) superan el umbral de la **Activate Rate (Tasa de activación)**:
   1. **Random Early Drop (Descarte aleatorio temprano)**: el cortafuegos utiliza un algoritmo para iniciar el descarte progresivo de ese tipo de paquete. Si el ataque continúa, cuanto más alta sea la tasa de cps entrantes (por encima de la **tasa de activación**), más paquetes descartará el cortafuegos. El cortafuegos descarta los paquetes hasta que la tasa de cps entrantes alcanza la **Max Rate (Tasa máxima)**, en cuyo punto el cortafuegos descarta todas las conexiones entrantes. **Random Early Drop (Descarte aleatorio temprano)** (RED) es la acción predeterminada para **SYN Flood (Congestión SYN)** y la única acción para **UDP Flood (Congestión UDP)**, **ICMP Flood (Congestión ICMP)**, **ICMPv6 Flood (Congestión ICMPv6)** y **Other IP Flood (Otra congestión IP)**. RED es más eficiente que las cookies SYN y puede manejar ataques mayores, pero no diferencia entre tráfico positivo y negativo.
   2. **SYN Cookies**: en lugar de enviar inmediatamente SYN al servidor, el cortafuegos genera una cookie (en nombre del servidor) para enviar en el SYN-ACK al cliente. El cliente responde con su ACK y la cookie, tras esta validación, el cortafuegos luego envía el SYN al servidor. La acción **SYN Cookies** requiere de más recursos del cortafuegos que **Random Early Drop (Descarte aleatorio temprano)**; permite diferenciar mejor, ya que afecta al tráfico negativo.
5. (Opcional) En cada una de las pestañas de "flood" (congestión), cambie los siguientes umbrales para ajustarlos a su entorno:
   - **Alarm Rate (connections/s) (Tasa de alarma [conexiones/s])**: especifique la tasa de umbral (cps) por encima de la cual se activa una alarma DoS. (El intervalo es 0-2.000.000; el valor predeterminado es 10.000.)
   - **Activate Rate (connections/s) (Tasa de activación [conexiones/s])**: especifique la tasa de umbral (cps) por encima de la cual se activa una respuesta DoS. Cuando se alcanza el umbral de **Activate Rate**, se produce un **Random Early Drop**. El intervalo es 0-2 000 000; el valor predeterminado es 10 000. (Para la congesión SYN, puede seleccionar la acción que ocurre).
   - **Max Rate (packets/s) (Tasa máxima [paquetes/s])**: especifique la tasa de umbral de conexiones entrantes por segundo que permite el cortafuegos. Cuando se supera el umbral, se descartan las nuevas conexiones que llegan. (El intervalo es 2-2 000 000; el valor predeterminado es 40 000).

© 2020 Palo Alto Networks, Inc.

Los valores de umbral predeterminados de este paso solo son puntos de inicio y pueden no ser adecuados para su red. Debe analizar el comportamiento de su red para definir adecuadamente valores de umbral iniciales.

6. En cada pestaña de congestión, especifique la **Block Duration** (en segundos), que es el período durante el cual el cortafuegos bloquea paquetes que coinciden con la regla de política de protección DoS que hace referencia a este perfil. Especifique un valor mayor que cero. (El intervalo es 1-21 600; el valor predeterminado es 300).

   Configure un valor de Block Duration (Duración de bloqueo) bajo si le preocupa que los paquetes que identificó incorrectamente como tráfico de ataque se bloqueen de manera innecesaria.

   Defina un valor de **Block Duration (Duración de bloqueo)** alto si está más preocupado por bloquear ataques volumétricos que por bloquear incorrectamente paquetes que no sean parte de un ataque.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure una regla de política de protección DoS que especifique los criterios para comparar el tráfico entrante.

Los recursos de cortafuegos son limitados, por lo cual no debería clasificar el uso de direcciones de origen en una zona accesible desde internet, debido a que puede haber una gran cantidad de direcciones IP únicas que coincidan con la regla de política de protección DoS. Eso requeriría numerosos contadores y el cortafuegos se quedaría sin recursos de rastreo. En su lugar, defina una regla de política de protección DoS que se clasifique usando la dirección de destino (del servidor que está protegiendo).

1. Seleccione **Policies (Políticas)** > **DoS Protection (Protección DoS)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** en la pestaña **General [General]**. El nombre distingue entre mayúsculas y minúsculas y puede tener un máximo de 31 caracteres, incluidas letras, números, espacios, guiones y guiones bajos.
2. En la pestaña **Source**, seleccione el **Type** para que sea una **Zone** o **Interface**, y después seleccione **Add** para añadir las zonas o interfaces. Elija la zona o interfaz según su implementación y lo que desea proteger. Por ejemplo, si tiene solo una interfaz que ingresa en el cortafuegos, elija una interfaz.
3. (Opcional) En **Source Address**, seleccione **Any** para que cualquier dirección IP entrante coincida con la regla o seleccione **Add** para añadir un objeto de dirección como una región geográfica.
4. (Opcional) Para **Source User (Usuario de origen)**, seleccione **any (cualquiera)** o especifique un usuario.
5. (Opcional) Seleccione **Negate** para que coincida con cualquier origen excepto los que especifique.
6. (Opcional) En la pestaña **Destination**, seleccione el **Type** para que sea una **Zone** o **Interface**, y después seleccione **Add** para añadir las zonas o interfaces. Por ejemplo, escriba la zona de seguridad que desee proteger.
7. (Opcional) En **Destination Address (Dirección de destino)**, seleccione **Any (Cualquiera)** o introduzca la dirección IP del dispositivo que desee proteger.
8. (Opcional) En la pestaña **Option/Protection (Opción/Protección)**, seleccione **Add (Añadir)** para añadir un **Service (Servicio)**. Seleccione un servicio o haga clic en **Service** e introduzca un nombre en **Name**. Seleccione **TCP** o **UDP**. Introduzca un **Destination Port**. Si no especifica un servicio concreto, la regla comparará la inundación de cualquier tipo de protocolo indistintamente del puerto específico de la aplicación.
9. En la pestaña **Option/Protection (Opción/Protección)**, para **Action (Acción)**, seleccione **Protect (Proteger)**.
10. Seleccione **Classified**.
11. En **Profile**, seleccione el nombre del perfil de **DoS Protection** que creó.

© 2020 Palo Alto Networks, Inc.

12. En **Address**, seleccione **source-ip-only** o **src-dest-ip-both**, lo que determina el tipo de dirección IP al que se aplica la regla. Seleccione el ajuste en función de cómo desea que el cortafuegos identifique el tráfico infractor:
    - Especifique **source-ip-only** si desea que el cortafuegos clasifique únicamente la dirección IP de origen. Debido a que los atacantes a menudo prueban toda la red en busca de hosts a los cuales atacar, **source-ip-only** es el ajuste típico para un examen más amplio.
    - Especifique **src-dest-ip-both** si desea proteger únicamente contra ataques DoS en el servidor que tiene una dirección de destino específica y asegurarse de que ninguna dirección IP de origen sobrepase un umbral específico de cps con ese servidor.
13. Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione Confirmar.

Haga clic en **Commit (Confirmar)**.

Finalización de un ataque DoS de una sesión

Para mitigar un ataque DoS de una sesión, debe realizar la Configuración de protección DoS contra inundaciones de nuevas sesiones por adelantado. En algún momento después de configurar la funcionalidad, es posible que se establezca una sesión antes de observar que hay en curso un ataque DoS (desde la dirección IP de esa sesión). Si detecta un ataque DoS de sesión única, realice la siguiente tarea para finalizar la sesión, de modo que los siguientes intentos de conexión desde esa dirección IP activen la protección DoS contra la inundación de nuevas sesiones.

STEP 1 | Identifique la dirección IP de origen que está causando el ataque.

Por ejemplo, use la función de captura de paquetes del cortafuegos con un filtro de destino para recopilar una muestra de todo el tráfico que va a la dirección IP de destino. De manera alternativa, utilice ACC para filtrar según la dirección de destino para ver la actividad en el host de destino que está siendo atacado.

STEP 2 | Cree una regla de política de protección DoS que bloqueará la dirección IP del atacante cuando se hayan superado los umbrales de ataque.

STEP 3 | Cree una regla de política de seguridad para denegar la dirección IP de origen y su tráfico de ataque.

STEP 4 | Finalice cualquier ataque existente desde la dirección IP de origen del ataque ejecutando el comando operativo **`clear session all filter source <ip-address>`**.

De manera alternativa, si conoce el ID de sesión, puede ejecutar el comando **`clear session id <value>`** para finalizar únicamente esa sesión.



*Si utiliza el comando **`clear session all filter source <ip-address>`**, todas las sesiones que coincidan con la dirección IP de origen se descartarán, lo que puede incluir tanto las sesiones correctas como las incorrectas.*

Cuando haya finalizado la sesión de ataque existente, cualquier intento posterior de formar una sesión de ataque será bloqueado por la política de seguridad. La política de protección DoS cuenta todos los intentos de conexión y los incluye en los umbrales. Cuando se alcanza el umbral máximo de la tasa, la dirección IP de origen se bloquea durante la duración del bloqueo, como se describe en Multiple-Session DoS Attack (Ataque de DoS de múltiples sesiones).

© 2020 Palo Alto Networks, Inc.

Identificación de sesiones que utilizan un porcentaje excesivo del búfer de paquete

Cuando un cortafuegos exhibe signos de vaciado de recursos, puede estar experimentando un ataque que envía una cantidad abrumadora de paquetes. En tales casos, el cortafuegos comienza a almacenar en búfer los paquetes entrantes. Puede identificar rápidamente las sesiones que están usando un porcentaje excesivo de almacenamiento en búfer de paquetes y mitigar el impacto al descartarlos.

Realice la siguiente tarea en cualquier modelo de cortafuegos basado en hardware (no un cortafuegos de la serie VM) para identificar, para cada ranura y plano de datos, el porcentaje utilizado de almacenamiento en búfer de paquetes, las cinco sesiones principales que usan más del dos por ciento del almacenamiento en búfer de paquetes y las direcciones IP de origen asociadas con dichas sesiones. El tener más información le permite tomar las medidas apropiadas.

STEP 1 | Visualice del uso de recursos del cortafuegos, las sesiones principales y los detalles de sesión Ejecute el siguiente comando operativo en la CLI (a continuación un ejemplo de resultado del comando):

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
6            92%   1        156                  7        1732
SESSION DETAILS SESS-ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-
IF    EGR-IF       APP
6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21 ethernet1/22
 undecided
```

El comando muestra un máximo de las cinco sesiones principales que usan el 2 % cada una o más del almacenamiento en búfer de paquetes.

El ejemplo de resultado anterior indica que la sesión 6 está utilizando el 92 % del almacenamiento en búfer de paquetes con paquetes TCP (protocolo 6) provenientes de la dirección IP 192.168.2.35.

- **SESS-ID**: indica el ID de sesión global que se utiliza en todos los demás comandos **`show session`**. El ID de sesión global es único dentro del cortafuegos.
- **GRP-ID**: indica una fase interna del procesamiento de paquetes.
- **COUNT**: indica cuántos paquetes hay en ese GRP-ID para esa sesión.
- **APP**: indica el App-ID extraído de la información de sesión que puede ayudarlo a determinar si el tráfico es legítimo. Por ejemplo, si los paquetes usan un puerto TCP o UDP común, pero el resultado de CLI indica una APP de `undecided`, los paquetes posiblemente sean tráfico de ataque. La APP es `undecided` cuando los decodificadores IP de la aplicación no pueden obtener suficiente información para determinar la aplicación. Una APP `unknown` indica que los decodificadores de IP de aplicación no pueden determinar la aplicación; una sesión de APP `unknown` que utiliza un alto porcentaje del almacenamiento en búfer de paquetes también es sospechosa.

Para restringir el resultado que se muestra:

En un modelo de la serie PA-7000, puede limitar el resultado a una ranura, un plano de datos o ambos. Por ejemplo:

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1 dp
 dp1
```


© 2020 Palo Alto Networks, Inc.

Solo en los modelos PA-5200 Series y PA-7000 Series, puede limitar el resultado a un plano de datos. Por ejemplo:

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp dp1
```

STEP 2 | Utilice el resultado de comando para determinar si el origen de la dirección IP de origen que usa un alto porcentaje del almacenamiento en búfer de paquetes está enviando tráfico legítimo o de ataque.

En el ejemplo de resultado anterior, probablemente se esté produciendo el ataque de una sola sesión. Una sola sesión (ID de sesión 6) está usando el 92 % del almacenamiento en búfer de paquetes para la ranura 1, DP1 y la aplicación en ese punto es `undecided`.

- Si determina que un solo usuario está enviando un ataque y el tráfico no es descargado, puede finalizar un ataque DoS de sesión única. Como mínimo, puede configurar protección DoS contra inundaciones de nuevas sesiones.
- En un modelo de hardware que tiene una matriz de puertas de campo programable (field-programmable gate array, FPGA), el cortafuegos descarga el tráfico en la FPGA cuando es posible para aumentar el rendimiento. Si el tráfico se descarga en el hardware, el borrar la sesión no ayuda, ya que luego es el software el que debe manejar el bombardeo de paquetes. En lugar de ello, debe eliminar una sesión sin confirmación.

Para ver si una sesión está descargada o no, use el comando operativo **`show session id <session-id>`** en la CLI como se muestra en el siguiente ejemplo. El valor `layer7processing (procesamiento de capa 7)` indica `completed (completado)` en las sesiones descargadas o `enabled (habilitado)` en las que no lo están.

© 2020 Palo Alto Networks, Inc.

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```

Eliminación de una sesión sin confirmación

Realice esta tarea para descartar de manera permanente una sesión, tal como una sesión que está sobrecargando el almacenamiento en búfer de paquetes. No se necesita confirmación; la sesión se elimina inmediatamente después de ejecutar el comando. Los comandos se aplican a las sesiones descargadas y no descargadas.

STEP 1 | En la CLI, ejecute el siguiente comando operativo en cualquier modelo de hardware:

```
admin@PA-7050> request session-discard [timeout <seconds>] [reason <reason-string>] id <session-id>
```

El tiempo de espera por defecto es de 3.600 segundos.

STEP 2 | Verifique que las sesiones se hayan eliminado.

© 2020 Palo Alto Networks, Inc.

```
admin@PA-7050> show session all filter state discard
```

Certificaciones

Los siguientes temas describen cómo configurar los cortafuegos y los dispositivos de Palo Alto Networks® para que admitan los criterios comunes y los estándares federales de procesamiento de la información 140-2 (FIPS 140-2), que son certificados de seguridad que garantizan un conjunto estándar de garantías y funciones de seguridad. Estos certificados suelen solicitarlos las agencias civiles del gobierno de EE. UU. y contratistas gubernamentales.

Si desea información detallada sobre las certificaciones de los productos y la validación externa, consulte la página de Certificaciones.

- Habilitación de FIPS y compatibilidad con criterios comunes
- Funciones de seguridad de FIPS-CC
- Limpieza de memoria de intercambio en un cortafuegos o dispositivos en modo FIPS-CC

© 2020 Palo Alto Networks, Inc.

Habilitación de FIPS y compatibilidad con criterios comunes

Utilice el siguiente procedimiento para habilitar el modo FIPS-CC en una versión de software que admita los criterios comunes y los estándares federales de procesamiento de la información 140-2 (FIPS 140-2). Cuando habilita el modo FIPS-CC, se incluye toda la funcionalidad FIPS y CC.

El modo FIPS-CC es compatible con todos los cortafuegos y todos los dispositivos de última generación de Palo Alto Networks, incluso los cortafuegos serie VM. Para habilitar el modo FIPS-CC, arranque el cortafuegos en la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT) y cambie el modo operativo de modo normal a modo FIPS-CC. El procedimiento necesario para cambiar el modo operativo es el mismo en todos los cortafuegos y dispositivos, pero el procedimiento necesario para acceder a la MRT varía.

Cuando habilita el modo FIPS-CC, el cortafuegos restablecerá la configuración predeterminada de fábrica; se eliminará toda la configuración.

- Acceda a la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT)
- Cambio del modo operativo a modo FIPS-CC

Acceda a la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT)

La MRT le permite realizar varias tareas en los cortafuegos y los dispositivos de Palo Alto Networks. Por ejemplo, puede revertir el cortafuegos o el dispositivo a la configuración predeterminada de fábrica, revertir el PAN-OS o una actualización de contenido a una versión previa, realizar el diagnóstico en el sistema de archivos, reunir información del sistema y extraer logs. Además, puede utilizar la MRT para llevar a cabo el Cambio de modo operativo a modo FIPS-CC o de modo FIPS-CC a modo normal.

Los siguientes procedimientos describen cómo acceder a la MRT en varios productos de Palo Alto Networks.

- Acceda a la MRT en los cortafuegos y los dispositivos del hardware (como los cortafuegos PA-220, los cortafuegos PA-7000 o los dispositivos de serie M).
  1. Establezca una sesión de consola serie hacia el cortafuegos o el dispositivo.
     1. Conecte un cable serie desde el puerto serie de su ordenador hasta el puerto de consola del cortafuegos o dispositivo.

        Si su ordenador no tiene un puerto serie de 9 clavijas, pero tiene un puerto USB, utilice el conversor de serie a USB para establecer la conexión. Si el cortafuegos tiene un puerto de consola micro USB, conéctelo al puerto con un cable estándar USB tipo A a micro USB.
     2. Abra el software de emulación de terminal en su ordenador y establézcalo como 9600-8-N-1, y conéctese al puerto COM correspondiente.

        En un sistema Windows, puede dirigirse al panel de control para ver la configuración del puerto COM de los dispositivos e impresoras y determinar el puerto COM que se asigna a la consola.
     3. Inicie sesión con una cuenta de administrador. (El nombre de usuario y la contraseña predeterminados son admin/admin).

© 2020 Palo Alto Networks, Inc.

2. Introduzca el siguiente comando de CLI y pulse **y** para confirmar:

```
debug system maintenance-mode
```

3. Después de que el cortafuegos o el dispositivo arranque con la pantalla de bienvenida de la MRT (en aproximadamente 2 a 3 minutos), pulse Intro en **Continue (Continuar)** para acceder al menú principal de la MRT.



*También puede acceder a la MRT reiniciando el cortafuegos o dispositivo, y escribiendo **maint** en el mensaje del modo de mantenimiento. Se requiere una conexión directa de consola serie.*

Después de que el cortafuegos o el dispositivo arranque con la MRT, puede acceder a la MRT de manera remota estableciendo una conexión SSH a la dirección IP del interfaz de administración (MGT). En el mensaje de inicio de sesión, introduzca **maint** como nombre de usuario y el número de serie del cortafuegos o el dispositivo como contraseña.

- Acceda a la MRT en los cortafuegos serie VM que se implementan en una nube privada (como en un hipervisor VMware ESXi o KVM).
  1. Establezca una sesión SSH para la dirección IP de administración del cortafuegos e inicie sesión con una cuenta de administrador.
  2. Introduzca el siguiente comando de CLI y pulse **y** para confirmar:

```
debug system maintenance-mode
```



El cortafuegos tardará aproximadamente 2 a 3 minutos en arrancar con la MRT. Durante este período, su sesión SSH se desconectará.

  3. Después de que el cortafuegos arranque en la pantalla de bienvenida de la MRT, inicie sesión en función del modo operativo:
     - **Modo normal:** Establezca una sesión SSH para la dirección IP de administración del cortafuegos e inicie sesión utilizando **maint** como nombre de usuario y el número de serie del cortafuegos o el dispositivo como contraseña.
     - **Modo FIPS-CC:** Acceda al dispositivo de administración de máquinas virtuales (como el cliente vSphere) y conéctese a la consola de máquinas virtuales.
  4. En la pantalla de bienvenida de la MRT, pulse Intro en **Continue (Continuar)** para acceder al menú principal de la MRT.

- Acceda a la MRT en los cortafuegos serie VM que se implementan en la nube privada (como AWS o Azure).
  1. Establezca una sesión SSH para la dirección IP de administración del cortafuegos e inicie sesión con una cuenta de administrador.
  2. Introduzca el siguiente comando de CLI y pulse **y** para confirmar:

```
debug system maintenance-mode
```



El cortafuegos tardará aproximadamente 2 a 3 minutos en arrancar con la MRT. Durante este período, su sesión SSH se desconectará.

  3. Después de que el cortafuegos arranque en la pantalla de bienvenida de la MRT, inicie sesión en función del tipo de máquina virtual:

© 2020 Palo Alto Networks, Inc.

- **AWS:** Inicie sesión como **`ec2-user`** y seleccione la clave pública de SSH asociada a la máquina virtual cuando la implementó.
- **Azure**: Introduzca las credenciales que creó cuando implementó el cortafuegos VM-Series.
- **GCP**: inicie sesión como **`gcp-user`** y seleccione la clave pública de SSH asociada a la máquina virtual al implementarla.

4. En la pantalla de bienvenida de la MRT, pulse Intro en **`Continue (Continuar)`** para acceder al menú principal de la MRT.

Cambio del modo operativo a modo FIPS-CC

El siguiente procedimiento describe cómo cambiar el modo operativo de un producto de Palo Alto Networks de modo normal a modo FIPS-CC.

STEP 1 | (Solo para cortafuegos de VM-Series o dispositivo virtual Panorama) Cree una clave SSH e inicie sesión en el cortafuegos o Panorama.

En algunas plataformas de nube pública, como Microsoft Azure, debe tener una clave SSH para evitar un error de autenticación después de cambiar al modo FIPS-CC. Verifique que ha implementado el cortafuegos para autenticarse mediante la clave SSH. Aunque en Azure puede implementar el cortafuegos de VM-Series o Panorama e iniciar sesión con un nombre de usuario y una contraseña, no podrá autenticarse con el nombre de usuario y la contraseña después de cambiar el modo operativo a FIPS-CC. Después del restablecimiento al modo FIPS-CC, debe usar la clave SSH para iniciar sesión y, continuación, podrá configurar un nombre de usuario y contraseña que podrá usar para iniciar sesión posteriormente en la interfaz web del cortafuegos.

STEP 2 | Conéctese al cortafuegos o al dispositivo y Acceda a la Maintenance Recovery Tool (Herramienta de recuperación de mantenimiento, MRT).

STEP 3 | Seleccione **`Set FIPS-CC Mode`** en el menú.

STEP 4 | Seleccione **`Enable FIPS-CC Mode (Habilitación del modo FIPS-CC)`**. Se inicia la operación de cambio de modo y un indicador de estado muestra el progreso. Una vez completado el cambio de modo, el estado es **`Success (Correcto)`**.

STEP 5 | Cuando se le solicite, seleccione **`Reboot`** para reiniciar.

*Si cambia el modo operativo en un cortafuegos serie VM implementado en una nube pública y pierde la conexión SSH a la MRT antes de poder **`reiniciar`**, debe esperar entre 10 y 15 minutos para que se complete el cambio de modo. Vuelva a iniciar sesión en la MRT y reinicie el cortafuegos para completar la operación. Después del restablecimiento al modo FIPS-CC, en algunos formatos virtuales (Panorama o VM-Series) solo puede iniciar sesión con la clave SSH, y si no ha configurado la autenticación con una clave SSH, ya no podrá iniciar sesión en el cortafuegos al reiniciar.*

Tras cambiar al modo FIPS-CC, observará el siguiente estado: `FIPS-CC mode enabled successfully (Modo FIPS-CC habilitado correctamente).`

Además, permanecen vigentes los siguientes cambios:

- FIPS-CC aparece siempre en la barra de estado de la parte inferior de la interfaz web.
- Las credenciales predeterminadas de inicio de sesión del administrador cambiarán a admin/paloalto.

Consulte Funciones de seguridad de FIPS-CC para obtener más información sobre las funciones de seguridad que se aplican en el modo FIPS-CC.

© 2020 Palo Alto Networks, Inc.

Funciones de seguridad de FIPS-CC

Cuando el modo FIPS-CC está habilitado, se aplican las siguientes funciones de seguridad en todos los cortafuegos y los dispositivos:

- Para iniciar sesión, el explorador debe ser compatible con TLS 1.1 (o superior); en un dispositivo WF-500, solo podrá gestionar el dispositivo mediante la CLI y debe conectarse utilizando una aplicación de cliente compatible con SSHv2.
- Todas las contraseñas deben contener al menos seis caracteres.
- Debe aplicar un valor de **Failed Attempts (Intentos erróneos)** y **Lockout Time (Tiempo de bloqueo) (min)** que sea mayor a 0 en entornos de autenticación. Si un administrador alcanza el umbral del valor de **Failed Attempts (Intentos erróneos)**, el administrador queda bloqueado durante el tiempo definido en el campo **Lockout Time (Tiempo de bloqueo) (min)**.
- Debe aplicar un valor **Idle Timeout (Tiempo de espera de inactividad)** superior a 0 en entornos de autenticación. Si una sesión iniciada está inactiva más tiempo del valor especificado, la cuenta del administrador cierra sesión automáticamente.
- Puede configurar la **Duración absoluta de la sesión** para establecer la duración máxima en minutos que un usuario puede iniciar sesión. La duración mínima que se puede configurar es de 60 minutos. Recibirá una advertencia de finalización de sesión 5 minutos antes del tiempo de espera. Esta función no se puede desactivar en el modo FIPS-CC y se establece de forma predeterminada en una sesión de 30 días.
- Puede configurar el **número máximo de sesiones** para establecer cuántos usuarios pueden iniciar sesión simultáneamente en la misma cuenta de administrador.
- El cortafuegos o dispositivo determina automáticamente el nivel adecuado de prueba automática y aplica el nivel de potencia apropiado en algoritmos de cifrado y conjuntos de cifrado.
- Los algoritmos FIPS-CC no aprobados no se descifran y, por lo tanto, se ignoran durante el descifrado.
- Cuando configure una VPN IPSec, el administrador debe seleccionar una opción de cifrado seguro que se le presenta durante la configuración de IPSec.
- (Solo en Panorama y WildFire) IPSec se puede habilitar en la interfaz de administración para proteger protocolos como NTP, RADIUS, TACACS y DNS.
- Los certificados autogenerados e importados deben contener claves públicas que son RSA de 2.048 bits (o más) o ECDSA de 256 bits (o más); debe utilizar un resumen de SHA256 o superior.

  No puede utilizar un módulo de seguridad de hardware (hardware security module, HSM) para guardar las claves ECDSA privadas utilizadas para el descifrado de Proxy SSL de reenvío o Inspección entrante de SSL.
- Las conexiones de gestión de Telnet, TFTP y HTTP no están disponibles.
- Debe habilitar el cifrado en el enlace de control de HA1. Debe configurar los parámetros del cambio de claves automático. Debe definir el parámetro data (datos) en un valor de 1000 MB como máximo, ya que no puede dejar el predeterminado. También debe configurar un intervalo, puesto que no se puede dejar deshabilitado.
- El puerto de la consola serie en el modo FIPS-CC funciona solo como un puerto de resultado de estado limitado; el acceso a la CLI no se encuentra disponible.
- El puerto de la consola serie en el hardware y en los cortafuegos de la nube privada serie VM que arrancan en la MRT proporciona acceso interactivo a la MRT.
- Los cortafuegos de la nube privada serie VM en el entorno del hipervisor que se arrancan en la MRT no admiten el acceso interactivo a la consola; solo puede acceder a la MRT utilizando SSH.

© 2020 Palo Alto Networks, Inc.

Limpieza de memoria de intercambio en un cortafuegos o aplicaciones que se ejecutan en modo FIPS-CC

Debe asegurarse de que elimina la información confidencial de la memoria de intercambio antes de retirar un cortafuegos o dispositivo (en modo FIPS-CC) o antes de enviarlo para su reparación. Use este procedimiento para eliminar toda la información del parámetro de seguridad criptográfico (cryptographic security parameter, CSP) de las particiones de la memoria de intercambio.

Si envía un cortafuegos gestionado con Panorama para la reparación, consulte los pasos para preparar la sustitución de cortafuegos con una autorización para la devolución de bienes.

STEP 1 | Abra una sesión de gestión SSH en el cortafuegos o el dispositivo.

STEP 2 | Ejecute el siguiente comando operativo:

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

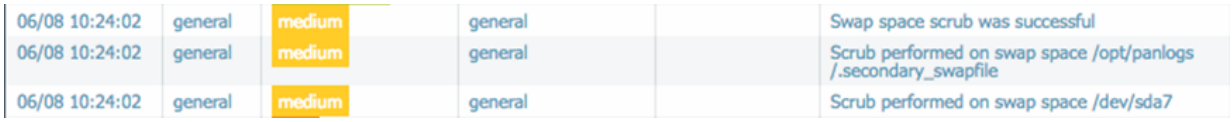
Por ejemplo, para apagar el cortafuegos o dispositivo y realizar una limpieza del Departamento de defensa (Department of Defense, DoD), ejecute el siguiente comando:

```
request shutdown system with-swap-scrub dod
```

STEP 3 | Presione **Y** en la ventana de advertencia para iniciar la limpieza.

STEP 4 | Verifique que se completó correctamente la limpieza. Visualice el log de **System (Sistema)** y filtre la palabra **swap**. El log de **System (Sistema)** indica el estado de la limpieza de cada partición de memoria de intercambio (una o dos particiones según el modelo) y también muestra una entrada de log que indica el estado general de la limpieza. Si la limpieza se completó correctamente en todas las particiones de la memoria de intercambio, el log de **System (Sistema)** muestra **Swap space scrub was successful**.

Si la limpieza falló en una o más particiones de la memoria de intercambio, el log de **System (Sistema)** muestra `Swap space scrub was unsuccessful`. La siguiente captura de pantalla muestra los resultados del log de un cortafuegos que tiene dos particiones.



06/08 10:24:02	general	medium	general		Swap space scrub was successful
06/08 10:24:02	general	medium	general		Scrub performed on swap space /opt/panlogs /.secondary_swapfile
06/08 10:24:02	general	medium	general		Scrub performed on swap space /dev/sda7

Para ver los logs de limpieza con la CLI, ejecute el comando ***show log system | match swap****.*

Si inicia la limpieza con el comando de apagado, el cortafuegos o dispositivo se apagarán después de que se complete la limpieza. Antes de poder encender el cortafuegos o dispositivo, primero debe desconectar y volver a conectar la fuente de alimentación.

© 2020 Palo Alto Networks, Inc.