Ayuda de la interfaz web de PAN-OS

Version 9.1

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

© 2019-2020 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

June 29, 2020

Table of Contents

Conceptos básicos de la interfaz web....13
- Descripción general del cortafuegos....15
- Características y ventajas....16
- Último acceso e intentos de inicio de sesión fallidos....17
- Mensaje del día....18
- Gestor de tareas....19
- Idioma....21
- Alarmas....22
- Compilación de cambios....23
- Guardar configuraciones candidatas....27
- Invertir cambios....31
- Bloquear configuraciones....35
- Búsqueda global....37
- Detalles de amenaza....38
- Resumen de inteligencia de AutoFocus....40
- Exportación de la tabla de configuración....43

Dashboard (Panel)....45
- Widgets de panel....47

ACC....49
- Información básica sobre el ACC....51
- Pestañas de ACC....53
- Widgets de ACC....54
- Acciones de ACC....56
  - Uso de las pestañas y widgets....56
  - Uso de los filtros: Filtros locales y filtros globales....57

Monitor (Supervisar)....61
- Supervisar > Logs....63
  - Tipos de log....63
  - Acciones de log....68
- Supervisar > Logs externos....71
- Supervisar > Motor de correlación automatizada....72
  - Monitor > Automated Correlation Engine > Correlation Objects....72
  - Monitor > Automated Correlation Engine > Correlated Events....73
- Monitor > Packet Capture....75
  - Descripción general de captura de paquetes....75
  - Componentes de una captura de paquetes personalizada....76
  - Habilitación de captura de paquetes de amenazas....79
- Supervisar > Appscope....81
  - Descripción general de Appscope....81
  - Informe de resumen de Appscope....82
  - Informe del supervisor de cambios de Appscope....82
  - Informe del supervisor de amenazas de Appscope....83
  - Informe de mapa de amenazas de Appscope....85
  - Informe del supervisor de red de Appscope....86

Informe del mapa de tráfico de Appscope 87
Monitor > Session Browser 89
Supervisar > Lista de direcciones IP a bloquear 90
Entradas de lista de direcciones IP a bloquear 90
Ver o eliminar entradas de lista de direcciones IP a bloquear 91
Monitor > Botnet 92
Configuración de informe de Botnet 92
Ajustes de configuración de Botnet 93
Supervisar > Informes en PDF 95
Monitor > PDF Reports > Manage PDF Summary 95
Monitor > PDF Reports > User Activity Report 96
Monitor > PDF Reports > SaaS Application Usage 98
Monitor > PDF Reports > Report Groups 100
Monitor > PDF Reports > Email Scheduler 101
Monitor > Manage Custom Reports 102
Monitor > Reports 104

Políticas 105
Tipos de políticas 107
Traslado o duplicación de una regla de política 108
Auditar archivo de comentarios 109
Comentarios de auditoría 109
Logs de configuración (entre confirmaciones) 109
Cambios de la regla 110
Consulta de recuento de resultado de uso de regla 111
Uso de regla de dispositivo para la consulta de recuento de resultados de regla 111
Políticas > Seguridad 113
Descripción general de las políticas de seguridad 113
Componentes de una regla de política de seguridad 114
Creación y gestión de políticas 123
Cancelación o reversión de una regla de política de seguridad 127
Aplicaciones y uso 129
Optimizador de política de seguridad 132
Políticas > NAT 134
Pestaña General de políticas NAT 134
Pestaña Paquete original de NAT 135
Pestaña Paquete traducido de NAT 136
Pestaña Enlace HA Activo/Activo de NAT 139
Políticas > QoS 141
Políticas > Reenvío basado en políticas 145
Pestaña general de reenvío basado en políticas 145
Pestaña de origen de reenvío basado en políticas 146
Pestaña de Destino/Aplicación/Servicio de reenvío basado en políticas 147
Pestaña de reenvío de reenvío basado en políticas 148
Políticas > Descifrado 150
Pestaña general de descifrado 150
Pestaña Origen de descifrado 151
Pestaña de destino de descifrado 152
Pestaña Categoría de URL/Servicio de descifrado 153
Pestaña Opciones de descifrado 153
Políticas> Inspección de túneles 155
Componentes básicos de una política de inspección de túnel 155
Policies > Application Override 161
Pestaña general de anulación de aplicación 161

Pestaña de origen de anulación de aplicación....162
Pestaña de destino de anulación de aplicación....163
Pestaña de aplicación/protocolo de anulación de aplicación....163
Políticas > Autenticación....165
Componentes básicos de una regla de política de autenticación....165
Crear y gestionar la política de autenticación....170
Políticas > Protección DoS....172
Pestaña general de protección DoS....172
Pestaña de origen de protección DoS....173
Pestaña de destino de protección DoS....174
Pestaña de protección/opción de protección DoS....174
Políticas > SD-WAN....178
Pestaña General de SD-WAN....178
Pestaña Origen de SD-WAN....179
Pestaña Destino de SD-WAN....180
Pestaña Aplicación/Servicio de SD-WAN....180
Pestaña Selección de ruta de SD-WAN....182
Pestaña Destino de SD-WAN....182

Objetos....185
Mover, clonar, cancelar o revertir objetos....187
«Mover o duplicar un objeto»....187
Cancelación o reversión de un objeto....187
Objetos > Direcciones....189
Objetos > Grupos de direcciones....191
Objetos > Regiones....193
Objectos > Grupos de usuarios dinámicos....194
Objetos > Aplicaciones....196
Descripción general de aplicaciones....196
Acciones admitidas en aplicaciones....200
Definición de aplicaciones....203
Objetos > Grupos de aplicaciones....208
Objetos > Filtros de aplicaciones....209
Objetos > Servicios....210
Objetos > Grupos de servicios....212
Objetos > Etiquetas....213
Crear etiquetas....213
Ver base de reglas como grupos....215
Gestión de etiquetas....218
Objects > External Dynamic Lists....221
Objetos > Objetos personalizados....226
Objetos > Objetos personalizados > Patrones de datos....226
Objetos > Objetos personalizados > Spyware/vulnerabilidad....230
Objetos > Objetos personalizados > Categoría de URL....234
Objetos > Perfiles de seguridad....236
Acciones en perfiles de seguridad....236
Objects > Security Profiles > Antivirus....240
Objetos > Perfiles de seguridad > Perfil de antispyware....242
Objetos > Perfiles de seguridad > Protección de vulnerabilidades....247
Objetos > Perfiles de seguridad > Filtrado de URL....252
Configuración general del filtrado de URL....252
Categorías de filtrado de URL....253
Configuración de filtrado URL....256
Detección de credencial de usuario....257

Inserción del encabezado HTTP 259
Objetos > Perfiles de seguridad > Bloqueo de archivo 262
Objetos > Perfiles de seguridad > Análisis de WildFire 264
Objetos > Perfiles de seguridad > Filtrado de datos 266
Objetos > Perfiles de seguridad > Protección DoS 268
Objetos > Perfiles de seguridad > Protección GTP 272
Objetos > Perfiles de seguridad > Protección SCTP 278
Objetos > Grupos de perfiles de seguridad 284
Objetos > Reenvío de logs 285
Objetos > Autenticación 289
Objetos > Perfil de descifrado 291
Configuración general de perfiles de descifrado 291
Configuración para controlar el tráfico SSL descifrado 292
Configuración para controlar el tráfico que no está descifrado 298
Configuración para controlar el tráfico SSH descifrado 298
Objetos > Perfil de descifrado > Perfil de reenvío 300
Objetos > Gestión de enlaces de SD-WAN 303
Objetos > Gestión de enlaces de SD-WAN > Perfil de calidad de la ruta 303
Objetos > Gestión de enlaces de SD-WAN > Distribución de tráfico 304
Objetos > Programaciones 306

network 307
Red > Interfaces 309
Resumen de las interfaces de cortafuegos 310
Componentes comunes de las interfaces de cortafuegos 310
Componentes comunes de interfaces de cortafuegos de la serie PA-7000 312
Interfaz de Tap 312
Interfaz HA 313
Interfaz de cable virtual 314
Subinterfaz de cable virtual 315
Interfaz de la capa 2 de la serie PA-7000 316
Subinterfaz de la capa 2 de la serie PA-7000 318
Interfaz de la capa 3 de la serie PA-7000 319
Subinterfaz de la capa 3 330
Interfaz de tarjeta de log 340
Subinterfaz de tarjeta de log 342
Interfaz de reflejo de descifrado 343
Grupo de interfaz de Ethernet agregados (AE) 343
Interfaz de Ethernet agregados (AE) 347
Network > Interfaces > VLAN 354
Network > Interfaces > Loopback 364
Network > Interfaces > Tunnel 367
Network (Red) > Interfaces (Interfaces) > SD-WAN 369
Network > Zones 370
Descripción general de zona de seguridad 370
Componentes de las zonas de seguridad 370
Network > VLANs 374
Network > Virtual Wires 375
Network > Virtual Routers 376
Ajustes generales de un enrutador virtual 376
Rutas estáticas 377
Redistribución de ruta 380
RIP 381
OSPF 384

OSPFv3....389
BGP....396
IP de multidifusión....411
ECMP....415
Más estadísticas de tiempo de ejecución para un enrutador virtual....417
Network > IPSec Tunnels....429
Gestión de túnel VPN IPSec....429
Pestaña General del túnel IPSec....429
Pestaña Identificadores proxy de túnel IPSec....432
Estado del túnel IPSec en el cortafuegos....433
Reiniciar o actualizar el túnel IPSec....433
Network (Red) > GRE Tunnels (Túneles GRE)....434
Túneles GRE....434
Network > DHCP....436
Descripción general de DHCP....436
Direccionamiento DHCP....436
Servidor DHCP....437
Retransmisión DHCP....440
Cliente DHCP....441
Network > DNS Proxy....442
Resumen del proxy DNS....442
Configuración del proxy DNS....443
Acciones adicionales de proxy DNS....445
Red > QoS....447
Configuración de la interfaz de QoS....447
Estadísticas de la interfaz de QoS....449
Network > LLDP....451
Descripción general de LLDP....451
Componentes del LLDP....451
Red > Perfiles de red....454
Red > Perfiles de red > Criptográfico IPSec de GlobalProtect....454
Network > Network Profiles > IKE Gateways....454
Red > Perfiles de red > Criptográfico IPSec....461
Red > Perfiles de red > Criptográfico IKE....463
Red > Perfiles de red > Supervisar....464
Network > Network Profiles > Interface Mgmt....464
Network > Network Profiles > Zone Protection....466
Red > Perfiles de red > QoS....485
Network > Network Profiles > LLDP Profile....487
Network > Network Profiles > BFD Profile....488
Network (Red) > Network Profiles (Perfiles de red) > SD-WAN Interface Profile (Perfil de interfaz de SD-WAN)....490

Dispositivo....493
Dispositivo > Configuración....495
Device (Dispositivo) > Setup (Configuración) > Management (Gestión)....496
Device > Setup > Operations....523
Habilitación de supervisión de SNMP....530
Device > Setup > HSM....533
Ajustes del proveedor del módulo de seguridad de hardware....533
Autenticación HSM....534
Operaciones de seguridad de hardware....534
Configuración y estado del proveedor del módulo de seguridad de hardware....535
Estado de módulo de seguridad de hardware....536

Device > Setup > Services....537
Configurar servicios para sistemas globales y virtuales....537
Configuración de servicios globales....538
Soporte IPv4 e IPv6 para la configuración de la ruta de servicio....540
Ruta de servicio de destino....544
Dispositivo > Configuración > Interfaces....545
Dispositivo > Configuración > Telemetría....549
Device > Setup > Content-ID....552
Device > Setup > WildFire....558
Device > Setup > Session....562
Configuración de sesión....562
Tiempos de espera de sesión....566
Ajustes de TCP....568
Ajustes de descifrado: Comprobación de revocación de certificado....570
Ajustes de descifrado: Reenvío de los ajustes de certificados del servidor proxy....571
Configuración de sesión de VPN....572
Device > High Availability....574
Consideraciones importantes para la configuración de alta disponibilidad (HA)....574
Configurar los ajustes de HA....575
Device (Dispositivo) > Log Forwarding Card (Tarjeta de reenvío de logs)....586
Device > Config Audit....588
Dispositivo > Perfiles de la contraseña....589
Requisitos de nombre de usuario y contraseña....589
Device > Administrators....591
Device > Admin Roles....594
Device > Access Domain....597
Device > Authentication Profile....598
Perfil de autenticación....598
Exportación de metadatos SAML desde un perfil de autenticación....606
Device > Authentication Sequence....608
Device > VM Information Sources....610
Ajustes para habilitar los orígenes de información de la VM para los servidores ESXi de VMware o vCenter....612
Ajustes para habilitar los orígenes de información de la VM para AWS VPC....613
Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine....614
Device (Dispositivo) > Troubleshooting (Solución de problemas)....617
Coincidencia de política de seguridad....617
Coincidencia de política de QoS....619
Coincidencia de política de autenticación....620
Coincidencia de política de descifrado/SSL....621
Coincidencia de política de NAT....622
Coincidencia de política de reenvío basado en políticas....624
Coincidencia de política de DoS....625
Enrutamiento....626
Probar Wildfire....628
Cámara de amenazas....628
Ping....629
Realizar seguimiento de ruta....631
Conectividad de recopilador de logs....632
Lista dinámica externa....633
Actualizar servidor....634
Comprobar el estado del servicio de logging en nube....635
Comprobar el estado del servicio GP en nube....635
Device > Virtual Systems....636

Device > Shared Gateways....639
Dispositivo > Gestión de certificados....640
Device > Certificate Management > Certificates....641
Gestión de certificación de cortafuegos y Panorama....641
Gestión de entidades de certificación de confianza predeterminadas....647
Device > Certificate Management > Certificate Profile....648
Device > Certificate Management > OCSP Responder....651
Device > Certificate Management > SSL/TLS Service Profile....653
Device > Certificate Management > SCEP....655
Device > Certificate Management > SSL Decryption Exclusion....659
Dispositivo > Páginas de respuesta....662
Device > Log Settings....665
Selección de destinos de reenvío de logs....665
Definición de la configuración de alarma....668
Borrar logs....670
Dispositivo > Perfiles de servidor > Netflow....671
Dispositivo > Perfiles de servidor > Trap SNMP....672
Device > Server Profiles > Syslog....674
Device > Server Profiles > Email....676
Dispositivo > Perfiles de servidor > HTTP....678
Device > Server Profiles > NetFlow (Dispositivo > Perfiles de servidor > Netflow)....681
Device > Server Profiles > RADIUS....683
Device > Server Profiles > TACACS+....685
Device > Server Profiles > LDAP....687
Device > Server Profiles > Kerberos....690
Dispositivo > Perfiles de servidor > Proveedor de identidad SAML....691
Device > Server Profiles > DNS....695
Dispositivo> Perfiles de servidor> Autenticación de múltiples factores....696
Device > Local User Database > Users....699
Dispositivo > Base de datos de usuario local > Grupos de usuarios....700
Dispositivo > Programación de la exportación de logs....701
Device > Software....703
Device > Dynamic Updates....705
Device > Support....709
Device > Master Key and Diagnostics....710
Implementar clave maestra....711

Identificación de usuarios....713
Device > User Identification > User Mapping....715
Configuración del agente User-ID de Palo Alto Networks....715
Supervisión de servidores....725
Incluir o excluir subredes para la asignación de usuarios....728
Dispositivo > Identificación de usuarios > Seguridad de conexión....730
Device > User Identification > User-ID Agents....731
Configuración de acceso a agentes User-ID....731
Gestión de acceso a agentes User-ID....733
Dispositivo > Identificación de usuarios > Agentes de servidor de terminal....735
Device (Dispositivo) > User Identification (Identificación del usuario) > Pestaña Group Mapping Settings (Ajustes de asignación de grupos)....737
Device > User Identification > Captive Portal Settings....742

GlobalProtect....747
Red > GlobalProtect > Portales....749

Pestaña general de Portales de GlobalProtect....750
Pestaña GlobalProtect Portals Authentication (Autenticación de portales de GlobalProtect)....751
Pestaña Portal Data Collection (Recopilación de datos de portal) de los portales de GlobalProtect....754
Pestaña GlobalProtect Portals Agent (Agente de portales de GlobalProtect)....754
Pestaña VPN sin cliente de portales GlobalProtect....780
Pestaña Satélite del portal de GlobalProtect....784
Red > GlobalProtect > Puertas de enlace....788
Pestaña general de Puertas de enlace de GlobalProtect....788
Pestaña Autenticación de Puerta de enlace de GlobalProtect....789
Pestaña Agente de Puertas de enlace de GlobalProtect....791
Pestaña Satélite de la puerta de enlace de GlobalProtect....803
Red > GlobalProtect > MDM....807
Network > GlobalProtect > Device Block List....808
Red> GlobalProtect> Aplicaciones sin cliente....809
Red> GlobalProtect> Grupos de aplicaciones sin cliente....810
Objetos > GlobalProtect > Objetos HIP....811
Pestaña general de Objetos HIP....811
Pestaña Dispositivo móvil de Objetos HIP....813
Pestaña Administración de parches de Objetos HIP....815
Pestaña de cortafuegos de Objetos HIP....816
Pestaña Antimalware de Objetos HIP....816
Pestaña de copia de seguridad de disco de Objetos HIP....817
Pestaña de cifrado de disco de Objetos HIP....817
Pestaña de prevención de pérdida de datos de objetos HIP....818
Pestaña Certificado de objetos HIP....819
Pestaña de comprobaciones personalizadas de objetos HIP....819
Objetos > GlobalProtect > Perfiles HIP....821
Dispositivo > Cliente de GlobalProtect....823
Gestión del software de la aplicación de GlobalProtect....823
Configuración de aplicación de GlobalProtect....824
Uso de la aplicación de GlobalProtect....825

Interfaz web de Panorama....827
Uso de la interfaz web de Panorama....829
Conmutador de contexto....834
Operaciones de compilación de Panorama....835
Definición de políticas en Panorama....844
Particiones de almacenamiento de log para un dispositivo virtual de Panorama en modo Legado....846
Panorama > Configuración > Interfaces....848
Panorama > Alta disponibilidad....851
Panorama > Clústeres Wildfire gestionados....854
Tareas de clústeres Wildfire gestionados....854
Tareas de dispositivos Wildfire gestionados....855
Información de Wildfire gestionada....856
Clúster WildFire gestionado y administración de dispositivos....860
Panorama > Administradores....872
Panorama > Funciones de administrador....875
Panorama > Access Domains....877
Panorama > Managed Devices > Summary (Panorama > Dispositivos gestionados > Resumen)....879
Administración de cortafuegos gestionado....879

Información del cortafuegos gestionado....880
Software de cortafuegos y actualizaciones de contenido....884
Copias de seguridad de cortafuegos....885
Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)....886
Estado detallado de dispositivos en Panorama....888
Panorama > Plantillas....893
Plantillas....893
Pilas de plantillas....894
Panorama > Templates (Plantillas) > Template Variables (Variables de plantilla)....895
Panorama > Grupos de dispositivos....898
Panorama > Recopiladores gestionados....900
Información del recopilador de logs....900
Configuración del recopilador de logs....901
Actualizaciones de software para recopiladores de logs dedicados....910
Panorama > Grupos de recopiladores....912
Configuración del grupo de recopiladores....912
Información del grupo de recopiladores....918
Panorama> Complementos....920
Panorama > VMware NSX....921
Configuración de una notificación a grupo....921
Creación de definiciones de servicio....922
Configuración de acceso al NSX Manager....923
Creación de reglas de dirección....925
Panorama > Perfil de ingestión de logs....927
Panorama > Configuración de log....928
Panorama > Exportación de configuración programada....930
Panorama > Software....932
Gestión de actualizaciones del software de Panorama....932
Visualización de la información de actualización del software de Panorama....933
Panorama > Implementación de dispositivo....934
Gestión de software y actualizaciones de contenido....934
Visualización de la información sobre la actualización de contenido y software....937
Programación de actualizaciones de contenido dinámico....938
Restablecimiento de las versiones de contenido de Panorama....939
Gestión de licencias de cortafuegos....940

Conceptos básicos de la interfaz web

Los siguientes temas proporcionan una descripción general del cortafuegos y describen las tareas administrativas básicas.

- Descripción general del cortafuegos
- Características y ventajas
- Último acceso e intentos de inicio de sesión fallidos
- Mensaje del día
- Gestor de tareas
- Idioma
- Alarmas
- Compilación de cambios
- Guardar configuraciones candidatas
- Invertir cambios
- Bloquear configuraciones
- Búsqueda global
- Detalles de amenaza
- Resumen de inteligencia de AutoFocus

© 2020 Palo Alto Networks, Inc.

Descripción general del cortafuegos

Los cortafuegos de nueva generación de Palo Alto Networks® inspeccionan todo el tráfico (incluidas las aplicaciones, las amenazas y el contenido) y lo vinculan con el usuario, independientemente de su ubicación o del tipo de dispositivo. El usuario, la aplicación y el contenido (es decir, los elementos que mueven su negocio) se convierten así en componentes integrales de la política de seguridad empresarial. Esto le permite alinear la seguridad con sus políticas empresariales y también escribir reglas que sean fáciles de entender y de mantener.

Como parte de nuestra plataforma Security Operating Platform, los cortafuegos de nueva generación le brindan a su organización la capacidad de hacer lo siguiente:

- Habilitar de forma segura aplicaciones (incluidas las de software como servicio, o SaaS), usuarios y contenido clasificando todo el tráfico (independientemente del puerto).
- Reducir el riesgo de un ataque mediante un modelo de aplicación de políticas positivo que permita todas las aplicaciones deseadas y bloquee todo lo demás.
- Aplicar políticas de seguridad que bloqueen los exploits de vulnerabilidad, virus, ransomware, spyware, botnets y otro malware desconocido, como las amenazas avanzadas persistentes, por ejemplo.
- Proteger sus centros de datos (incluidos los centros de datos virtualizados), al segmentar los datos y las aplicaciones, por un lado, y al aplicar el principio Zero Trust (confianza cero), por el otro.
- Instaurar un sistema de seguridad uniforme en todos sus entornos, tanto los locales como en la nube.
- Adoptar un modelo informático móvil seguro que acerque la plataforma Security Operating Platform a usuarios y dispositivos, independientemente de su ubicación.
- Disfrutar de visibilidad centralizada y optimizar la seguridad en la red mediante el aprovechamiento de los datos para evitar que los ciberataques consigan sus objetivos.
- Identificar y evitar los intentos de robo de credenciales al detener el envío de credenciales corporativas válidas a sitios web ilegítimos, y al neutralizar la posibilidad de que el atacante utilice las credenciales robadas para realizar movimientos laterales o comprometer la seguridad de la red mediante políticas de autenticación en la capa de red.

© 2020 Palo Alto Networks, Inc.

Características y ventajas

Los cortafuegos de nueva generación de Palo Alto Networks ofrecen un control detallado del tráfico que tiene permiso para acceder a su red. Las principales características y ventajas incluyen las siguientes:

- **Cumplimiento de políticas basadas en aplicaciones (App-ID™)**: el control de acceso según el tipo de aplicación es mucho más eficaz cuando la identificación de las aplicaciones no se basa únicamente en el protocolo y el número de puerto. El servicio App-ID puede bloquear aplicaciones de alto riesgo, así como comportamientos de alto riesgo, como el intercambio de archivos, y el tráfico cifrado con el protocolo Secure Sockets Layer (SSL) puede descifrarse e inspeccionarse.
- **Identificación de usuarios (User-ID™)**: la identificación de usuarios (User-ID) permite que los administradores configuren y apliquen políticas de cortafuegos basadas en usuarios y grupos de usuarios, en lugar de zonas y direcciones de red, o además de estas. El cortafuegos puede comunicarse con numerosos servidores de directorio, como Microsoft Active Directory, eDirectory, SunOne, OpenLDAP y la mayoría de los otros servidores de directorio basados en LDAP, para proporcionar información de usuarios y grupos al cortafuegos. A continuación podrá utilizar esta información para una habilitación segura de aplicaciones que puede definirse por usuario o por grupo. Por ejemplo, el administrador podría permitir que una organización utilizara una aplicación basada en Internet e impedir que cualquier otra organización de la empresa utilizarla la misma aplicación. También puede configurar un control detallado de determinados componentes de una aplicación basándose en usuarios y grupos (consulte Identificación del usuario).
- **Prevención de amenazas**: los servicios de prevención de amenazas que protegen la red frente a virus, gusanos, spyware y otro tráfico malintencionado pueden variar según la aplicación y el origen del tráfico (consulte Objects > Security Profiles).
- **Filtrado de URL**: las conexiones salientes pueden filtrarse para impedir el acceso a sitios web inadecuados (consulte Objects > Security Profiles > URL Filtering).
- **Visibilidad del tráfico**: los extensos informes, logs y mecanismos de notificación ofrecen una visibilidad detallada del tráfico de aplicaciones y los eventos de seguridad en la red. El centro de comando de aplicación (ACC) de la interfaz web identifica las aplicaciones con mayor tráfico y el mayor riesgo de seguridad (consulte Monitor).
- **Versatilidad de red y velocidad**: el cortafuegos de Palo Alto Networks puede añadirse o sustituir a su cortafuegos existente, y puede instalarse de manera transparente en cualquier red o configurarse para permitir un entorno conmutado o enrutado. Las velocidades a varios gigabits y la arquitectura de un único paso le ofrecen estos servicios sin apenas afectar a la latencia de red.
- **GlobalProtect**: el software GlobalProtect™ protege los sistemas cliente, como ordenadores portátiles, que se utilizan a nivel de campo, permitiendo iniciar sesión de manera fácil y segura desde cualquier parte del mundo.
- **Funcionamiento a prueba de fallos**: la alta disponibilidad (HA) ofrece tolerancia a fallos automática en el caso de cualquier interrupción en el hardware o el software (consulte Device > Virtual Systems).
- **Elaboración de análisis e informes sobre software malintencionado**: el servicio de análisis basado en la nube WildFire™ proporciona análisis e informes detallados sobre el software malintencionado que pasa por el cortafuegos. La integración con el servicio de inteligencia de amenazas AutoFocus™ le permite evaluar el riesgo asociado con el tráfico de red a niveles de organización, industria y globales.
- **Cortafuegos de la VM-Series**: un cortafuegos de VM-Series proporciona una instancia virtual de PAN-OS® situada para su uso en un entorno de centro de datos virtualizado y es perfecto para sus entornos de computación en la nube privados, públicos e híbridos.
- **Gestión y Panorama**: puede gestionar cada cortafuegos mediante una interfaz web intuitiva o una interfaz de línea de comandos (CLI). Del mismo modo, puede gestionar todos los cortafuegos de manera centralizada mediante el sistema de gestión centralizado de Panorama™, que cuenta con una interfaz web muy parecida a la interfaz web de los cortafuegos de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Último acceso e intentos de inicio de sesión fallidos

Para detectar el uso indebido y evitar la explotación de una cuenta privilegiada, como una cuenta administrativa en un cortafuegos o Panorama de Palo Alto Networks, la interfaz web y la interfaz de línea de comandos (command line interface, CLI) muestran la última vez que inició sesión y cualquier intento de inicio de sesión con errores de su nombre de usuario. Esta información le permite fácilmente identificar si alguien utiliza sus credenciales administrativas para iniciar un ataque.

Tras iniciar sesión en la interfaz web, verá la información de la última vez que inició sesión en la parte inferior izquierda de la ventana. Si el inicio de sesión falló una o varias veces desde el último inicio de sesión correcto, aparecerá un icono de advertencia a la derecha de la última información de inicio de sesión. Pase el cursor del ratón por el símbolo de advertencia para conocer el número de intentos fallidos o haga clic en él para abrir la ventana **Failed Login Attempts Summary (Resumen de intentos de registros en logs fallidos)**, la cual detalla el nombre de cuenta del administrador, la dirección IP de origen y el motivo del fallo de cada inicio de sesión.

Si usted ve múltiples intentos de inicio de sesión fallidos que no los reconoce como propios, debe comunicarse con su administrador de red para localizar el sistema que lleva a cabo el ataque de fuerza bruta y luego investigar a computadora de host y usuario para identificar y erradicar cualquier actividad malintencionada. Si usted observa que la fecha y hora del último inicio de sesión indica un peligro para la cuenta, debe cambiar su contraseña de inmediato y llevar a cabo una auditoría de configuración para determinar si se confirmaron cambios de configuración sospechosos. Revierta la configuración a una configuración conocida si observa que los logs se borraron o si tiene dificultadas para determinar si se realizaron cambios inadecuados con su cuenta.

© 2020 Palo Alto Networks, Inc.

Mensaje del día

Si usted u otro administrador configuraron un mensaje del día, o Palo Alto Networks incorporó uno como parte de la versión de contenido o software, se mostrará automáticamente el cuadro de diálogo del mensaje del día cuando los usuarios inicien sesión en la interfaz web. Esto evita que desconozcan información importante, como un reinicio inminente del sistema que afecte a las tareas que intentan llevar a cabo.

El diálogo muestra un mensaje por página. Si el diálogo incluye la opción de seleccionar **Do not show again (No volver a mostrar)**, puede seleccionarla en cada mensaje cuyo cuadro de diálogo no desea ver tras varios inicios de sesión.

Siempre que se muestre el diálogo de Message of the Day (Mensaje del día):, el mensaje aparece en su próxima sesión aunque haya seleccionado Do not show again (No volver a mostrar) durante un inicio de sesión previo. Entonces, debe volver a seleccionar esta opción para evitar ver el mensaje modificado en las siguientes sesiones.

Para navegar por las páginas del diálogo, haga clic en las flechas derecha ( ) e izquierda ( ) junto a los laterales del diálogo o haga clic en un selector de página ( ) al final del diálogo. Luego de hacer clic en **Close (Cerrar)** para cerrar el diálogo, puede abrirlo manualmente haciendo clic en los mensajes ( ) al final de la interfaz web.

Para configurar el mensaje del día, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y edite la configuración de Banners y mensajes.

© 2020 Palo Alto Networks, Inc.

Gestor de tareas

Haga clic en **Tasks (Tareas)** en la parte inferior de la interfaz web para mostrar las operaciones que usted, otros administradores o PAN-OS iniciaron desde el último reinicio del cortafuegos (por ejemplo, confirmaciones manuales o actualizaciones de FQDN automáticas). Para cada tarea, el Gestor de tareas proporciona la información y las acciones descritas en la tabla siguiente.

Algunas columnas están ocultas de forma predeterminada. Para mostrar u ocultar una columna concreta, abra el menú desplegable de cualquier encabezado de columna, seleccione Columns (Columnas), y seleccione (muestre) o borre (oculte) las columnas como desee.

Campo/Botón	Description (Descripción)
	Para filtrar las tareas, introduzca una cadena de texto basada en un valor en una de las columnas y aplique el filtro ( ). Por ejemplo, introducir **`edl`** filtrará la lista para mostrar únicamente las tareas EDLFetch (extraer listas dinámicas externas). Para eliminar el filtrado, quite el filtro ( ).
Tipo	El tipo de operación, como la solicitud de logs, la actualización de licencias o la confirmación. Si la información relacionada con la tarea (por ejemplo, advertencias) es demasiado larga para caber en la columna Mensajes, puede hacer clic en el valor Tipo para ver todos los detalles.
estado	Indica si la operación está pendiente (como confirmaciones con estados En cola), en progreso (como solicitudes de logs con estado Activo), completo o con errores. Para las confirmaciones en progreso, Status indica el porcentaje de finalización.
Job ID (ID de trabajo)	Un número que identifica la tarea. Desde la CLI, puede utilizar el ID de trabajo para ver detalles adicionales sobre una tarea. Por ejemplo, puede ver la posición de una tarea de confirmación en la cola de confirmación introduciendo: `> show jobs id <job-id>` Esta opción está oculta de manera predeterminada.
Hora de finalización	La fecha y hora cuando concluyó la tarea. Esta opción está oculta de manera predeterminada.
Fecha de inicio	La fecha y hora cuando se inició la tarea. Para las operaciones de confirmación, Start Time indica cuándo se agregó una confirmación en la cola de confirmaciones.
Mensajes	Muestra los detalles de la operación. Si la entrada indica que existen demasiados mensajes, puede hacer clic en el tipo de tarea para ver los mensajes.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	Para las operaciones de confirmación, los mensajes incluyen el tiempo fuera de cola cuando PAN-OS comenzó a llevar a cabo la confirmación. Para ver la descripción que ingresó un administrador en una confirmación, haga clic en **Commit Description (Compilar descripción)**. Para obtener más información, consulte Confirmar cambios.
Acción	Hacer clic en **x** para cancelar una confirmación pendiente iniciada por un administrador o PAN-OS. Este botón sólo está disponible para administradores que tengan una de las siguientes funciones predefinidas: superusuario, administrador de dispositivos, administrador de sistema virtual o administrador de Panorama.
Mostrar	Seleccione la tarea que desea mostrar: • **All Tasks Todas las tareas** (defecto) • **All (Todas)** las tareas de cierto tipo (**Jobs (Trabajos)**, **Reports (Informes)**, o **Log Requests (Solicitudes de log)**) • Todas las tareas **Running (En ejecución)** (en curso) • Todas las tareas **Running (En ejecución)** de cierto tipo (**Jobs (Trabajos)**, **Reports (Informes)** o **Log Requests (Solicitudes de log)**) • (Panorama solamente) Utilice la segunda lista desplegable para mostrar las tareas de **Panorama** (predeterminado) o un cortafuegos gestionado específico.
Borrar la cola de confirmación	Cancele todas las confirmaciones pendientes iniciadas por los administradores o PAN-OS. Este botón sólo está disponible para administradores que tengan una de las siguientes funciones predefinidas: superusuario, administrador de dispositivos, administrador de sistema virtual o administrador de Panorama.

© 2020 Palo Alto Networks, Inc.

Idioma

De forma predeterminada, el idioma local de la computadora desde la cual se inicia sesión en el cortafuegos determina el idioma que se muestra en la interfaz web de gestión. Para modificar manualmente el idioma, haga clic en **Language (Idioma)** (esquina inferior derecha de la interfaz web), seleccione el idioma deseado en la lista desplegable y haga clic en **OK (Aceptar)**. La interfaz web se actualizará y mostrará la interfaz web en el idioma seleccionado.

Los idiomas compatibles incluyen los siguientes: francés, japonés, español, chino simplificado y chino tradicional.

© 2020 Palo Alto Networks, Inc.

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 (consulte Definición de la configuración de alarma). Cuando genera una alarma, el cortafuegos crea un log de alarma y abre el diálogo System Alarms (Alarmas del sistema) para mostrar la alarma. Luego de cerrar el diálogo, puede volver a abrirlo en cualquier momento haciendo clic en **Alarms (Alarmas)** ( ) al final de la interfaz web. Para evitar que el cortafuegos abra automáticamente el diálogo de una alarma en particular, seleccione Unacknowledged Alarms y haga clic en **Acknowledge (Reconocer)** para mover las alarmas a la lista Acknowledged Alarms.

© 2020 Palo Alto Networks, Inc.

Compilación de cambios

Haga clic en **Commit (Confirmar)** en la parte superior derecha de la interfaz web para especificar la operación que realizar respecto a los cambios pendientes en la configuración del cortafuegos: Confirmar (activar), validar o previsualizar. Puede filtrar los cambios pendientes por administrador o *ubicación* y luego previsualizar, validar y confirmar sólo esos cambios. La ubicación puede ser sistemas virtuales específicos, objetos y políticas compartidos, o configuración de red y dispositivos compartidos.

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.

Use el Task Manager para cancelar confirmaciones o ver detalles de la confirmaciones que están completas, pendientes, en progreso o que tienen errores.

El cuadro de diálogo Confirmar muestra las opciones descritas en la siguiente tabla.

Campo/Botón	Description (Descripción)
Commit All Changes	Compila todos los cambios para los que tiene privilegios administrativos (predeterminado). No puede filtrar manualmente el alcance de los cambios de configuración que el cortafuegos confirma al seleccionar esta opción. En su lugar, la función de administrador asignada a la cuenta utilizada para iniciar sesión determina el ámbito de compilación: • **Función de superusuario**: el cortafuegos confirma los cambios de todos los administradores. • **Rol personalizado**: los privilegios del perfil de rol de administrador asignado a su cuenta determinan el ámbito de confirmación (consulte Device > Admin Roles). Si el perfil incluye el privilegio de **Commit For Other Admins (Confirmar para otros administradores)**, el cortafuegos confirma los cambios configurados por cualquiera y todos los administradores. Si su perfil de rol de administrador no incluye el privilegio de **Commit For Other Admins (Confirmar para otros administradores)**, el cortafuegos confirma solamente sus cambios y no los de otros administradores. Si ha implementado dominios de acceso, el cortafuegos aplicará automáticamente esos dominios para filtrar el ámbito de confirmación (consulte Device > Access Domain). Independientemente de su función administrativa, el cortafuegos sólo confirma los cambios de configuración en los dominios de acceso asignados a su cuenta.
Commit Changes Made By	Filtra el alcance de los cambios de configuración que el cortafuegos confirma. La función administrativa asignada a la cuenta utilizada para iniciar sesión determina las opciones de filtrado: • **Función de superusuario**: puede limitar el ámbito de compilación a los cambios realizados por administradores específicos y a los cambios en ubicaciones específicas.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan las opciones de filtrado (consulte Device > Admin Roles). Si el perfil incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, puede limitar el ámbito de compilación a cambios configurados por administradores específicos y a cambios en ubicaciones específicas. Si su perfil de función de administración no incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, solo puede limitar el ámbito de compilación a los cambios realizados por usted mismo en ubicaciones específicas. Filtre el ámbito de compilación de la siguiente manera: • **Filtrar por administrador**: incluso si su función permite compilar los cambios de otros administradores, el ámbito de compilación incluye solo sus cambios de forma predeterminada. Para añadir otros administradores al ámbito de confirmación, haga clic en el enlace **<usernames>**, seleccione los administradores y haga clic en **OK (Aceptar)**. • **Filtrar por ubicación**: seleccione los cambios en ubicaciones específicas para incluir en la compilación Include in Commit. Si ha implementado dominios de acceso, el cortafuegos filtrará automáticamente el ámbito de confirmación basado en esos dominios (consulte Device > Access Domain). Independientemente de su función administrativa y de sus opciones de filtrado, el ámbito de compilación solo incluye los cambios de configuración en los dominios de acceso asignados a su cuenta. *Tras cargar una configuración (Device > Setup > Operations), debe Commit All Changes (Compilar todos los cambios).* Al realizar cambios en un sistema virtual, debe incluir los cambios de todos los administradores que añadieron, eliminaron o cambiaron las reglas para la misma base de reglas en ese sistema virtual.
Commit Scope	Enumera las ubicaciones donde hay cambios que compilar. Que la lista incluya todos los cambios o un subconjunto de ellos depende de varios factores, tal como se describe en las opciones Commit All Changes y Commit Changes Made By. Las ubicaciones pueden ser cualquiera de las siguientes opciones: • **shared-object (objeto compartido)**: ajustes definidos en la ubicación compartida. • **policy-and-objects (política y objetos)**: reglas de políticas o objetos que se definen en un cortafuegos que no tiene varios sistemas virtuales. • **device-and-network (dispositivo y red)**: las configuraciones de red y dispositivos que son globales (como los perfiles de gestión de interfaz) y no son específicas de un sistema virtual. Esto también se aplica a la configuración de red y dispositivos en un cortafuegos que no tiene varios sistemas virtuales.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **<virtual-system>**: el nombre del sistema virtual en el que se definen reglas u objetos de la política en un cortafuegos que tiene varios sistemas virtuales. Incluye configuraciones de red y dispositivos específicas de un sistema virtual (como las zonas).
Tipo de ubicación	Esta columna categoriza las ubicaciones de los cambios pendientes: • **Virtual Systems (Sistemas Virtuales)**: configuraciones que se definen en un sistema virtual específico. • **Other Changes (Otros Cambios)**: configuraciones que no son específicas de un sistema virtual (como objetos compartidos).
Include in Commit (compilación parcial únicamente)	Permite seleccionar los cambios que desea compilar. De manera predeterminada, se seleccionan todos los cambios en **Commit Scope (Ámbito de compilación)**. Esta columna solo se muestra tras elegir compilar los cambios realizados por administradores específicos (**Commit Changes Made By**). *Puede haber dependencias que afecten a los cambios que incluya en la compilación. Por ejemplo, si añade un objeto y otro administrador, a continuación, modifica ese objeto, no puede compilar el cambio del otro administrador sin compilar su propio cambio.*
Group by Location Type	Agrupa la lista de cambios de configuración en **Commit Scope (Ámbito de compilación)** por **Location Type (Tipo de ubicación)**.
Vista previa de cambios	Permite comparar las configuraciones seleccionadas en **Commit Scope (Ámbito de compilación)** con la configuración en ejecución. La ventana de vista previa utiliza codificación de colores para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo). Para ayudarle a comparar los cambios con las secciones de la interfaz web, puede configurar la ventana de vista previa para que muestre **Lines of Context (Líneas de contexto)** antes y después de cada cambio. Este contexto proviene de los archivos de las configuraciones candidata y en ejecución que está comparando. *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.*
Cambiar resumen	Enumera los ajustes individuales en los que está compilando cambios. La lista **Change Summary (Resumen de los cambios)** muestra la siguiente información para cada ajuste: • **Object Name (Nombre de objeto)**: el nombre que identifica la política, el objeto, el ajuste de red o la configuración del dispositivo. • **Type (Tipo)**: el tipo de ajuste (como Dirección, Regla de seguridad o Zona).

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Location Type (Tipo de ubicación)**: indica si el ajuste está definido en **Virtual Systems (Sistemas virtuales)**. • **Location (Ubicación)**: el nombre del sistema virtual donde se define el ajuste. La columna muestra **Shared (Compartido)** en los ajustes que no son específicos a un sistema virtual. • **Operations (Operaciones)**: indica todas las operaciones (crear, editar o eliminar) realizadas en la configuración desde la última compilación. • **Owner (Propietario)**: el administrador que realizó el último cambio en el ajuste. • **Will Be Committed (Se comprometerá)**: Indica si la confirmación incluye ahora el ajuste. • **Previous Owners (Propietarios anteriores)**: administradores que realizaron cambios en el ajuste antes del último cambio. Opcionalmente, puede agrupar por nombre de columna con **Group By (Agrupar por)** (como, por ejemplo, **Type [Tipo]**). Seleccione un objeto en la lista de cambios para ver la **diferencia de nivel de objeto**.
Validar compilación	Valida si la configuración del cortafuegos tiene sintaxis correcta y es semánticamente completa. Los resultados muestran los mismos errores y advertencias que una compilación, incluidas las advertencias de dependencia de aplicaciones y la observación de reglas. 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.
Description (Descripción)	Permite introducir una descripción (hasta 512 caracteres) para ayudar a otros administradores a comprender los cambios realizados. *El log del sistema corta las descripciones de compilación si superan los 512 caracteres.*
Commit (Confirmar)	Se inicia la confirmación o, si existen otras confirmaciones pendientes, la añade a la cola de confirmaciones.
Estado de compilación	Proporciona el progreso durante la compilación y, después, proporciona resultados después de dicha compilación. Los resultados de la compilación incluyen el estado correcto o erróneo, detalles de los cambios de compilación y advertencias de compilación. Entre las advertencias se incluyen las siguientes: • **Compilación**: permite ver advertencias de compilación generales. • **Dependencia de aplicaciones**: permite ver las dependencias de aplicaciones necesarias para las reglas existentes. • **Máscara de regla**: permite ver las reglas enmascaradas.

© 2020 Palo Alto Networks, Inc.

Guardar configuraciones candidatas

Seleccione **Config (Configuración)** > **Save Changes (Guardar cambios)** en la parte superior derecha del cortafuegos o de la interfaz web de Panorama para guardar un nuevo archivo de instantánea de la configuración candidata o para sobrescribir un archivo de configuración existente. Si el cortafuegos o Panorama se reinician antes de que compile los cambios, luego puede revertir la configuración candidata a la instantánea guardada para restablecer los cambios que realizó tras la última compilación. Para revertir a la instantánea, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)** y **Load named configuration snapshot (Cargar instantánea de configuración con nombre)**. Si no revierte a la instantánea tras el reinicio, la configuración candidata será la misma que la última configuración compilada (la configuración en ejecución).

Puede filtrar los cambios de configuración que desea guardar por administrador o *ubicación*. La ubicación puede ser sistemas virtuales específicos, objetos y políticas compartidos, o configuración de red y dispositivos compartidos.

Debe guardar los cambios periódicamente para que no los pierda si se reinicia el cortafuegos o Panorama.

Guardar los cambios en la configuración candidata no los activa; debe compilar los cambios (Commit Changes) para activarlos.

El cuadro de diálogo Save Changes muestra las opciones descritas en la siguiente tabla:

Campo/Botón	Description (Descripción)
Save All Changes	Guarda todos los cambios para los que tiene privilegios administrativos (predeterminado). No puede filtrar manualmente el ámbito de los cambios de configuración que guarda el cortafuegos cuando se selecciona esta opción. En su lugar, la función de administrador asignada a la cuenta utilizada para iniciar sesión determina el ámbito del guardado: • **Función de superusuario**: el cortafuegos guarda los cambios de todos los administradores. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan el ámbito de guardado (consulte Device > Admin Roles). Si el perfil incluye el privilegio **Save For Other Admins (Guardar por otros administradores)**, el cortafuegos guarda los cambios configurados por cualquiera de los administradores. Si su perfil de función de administración no incluye el privilegio **Save For Other Admins (Guardar por otros administradores)**, el cortafuegos guarda solo sus cambios y no los de los demás administradores. Si ha implementado dominios de acceso, el cortafuegos aplica automáticamente esos dominios para filtrar el ámbito de guardado (consulte Device > Access Domain). Independientemente de su función administrativa, el cortafuegos guarda solo los cambios de configuración en los dominios de acceso asignados a su cuenta.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
Save Changes Made By	Filtra el ámbito de los cambios de configuración que guarda el cortafuegos. La función administrativa asignada a la cuenta utilizada para iniciar sesión determina las opciones de filtrado: • **Función de superusuario**: puede limitar el ámbito de guardado a los cambios realizados por administradores específicos y a los cambios en ubicaciones específicas. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan las opciones de filtrado (consulte Device > Admin Roles). Si el perfil incluye el privilegio **Save For Other Admins (Guardar por otros administradores)**, puede limitar el ámbito de guardado a cambios configurados por administradores específicos y a cambios en ubicaciones específicas. Si su perfil de función de administración no incluye el privilegio **Save For Other Admins (Guardar por otros administradores)**, solo puede limitar el ámbito de guardado a los cambios realizados por usted mismo en ubicaciones específicas. Filtre el ámbito de guardado de la siguiente manera: • **Filtrar por administrador**: incluso si su función permite guardar los cambios de otros administradores, el ámbito de guardado incluye solo sus cambios de forma predeterminada. Para añadir otros administradores al ámbito de guardado, haga clic en el enlace **<usernames>**, seleccione los administradores y haga clic en **OK (Aceptar)**. • **Filtrar por ubicación**: seleccione los cambios en ubicaciones específicas para incluir en el guardado Include in Save. Si ha implementado dominios de acceso, el cortafuegos filtra automáticamente el ámbito de guardado en función de dichos dominios (consulte Device > Access Domain). Independientemente de su función administrativa y de sus opciones de filtrado, el ámbito de guardado solo incluye los cambios de configuración en los dominios de acceso asignados a su cuenta.
Save Scope	Enumera las ubicaciones donde hay cambios que guardar. Que la lista incluya todos los cambios o un subconjunto de ellos depende de varios factores, tal como se describe en las opciones Save All Changes y Save Changes Made By. Las ubicaciones pueden ser cualquiera de las siguientes opciones: • **shared-object (objeto compartido)**: ajustes definidos en la ubicación compartida. • **policy-and-objects (política-y-objetos)**: (solo cortafuegos) reglas de políticas u objetos que se definen en un cortafuegos sin varios sistemas virtuales. • **device-and-network (dispositivo-y-red)**: (solo cortafuegos) ajustes de red y dispositivo globales (como los perfiles de gestión de interfaz), no son específicos de un sistema virtual. • **<virtual-system>** (solo cortafuegos): el nombre del sistema virtual en el que se definen los objetos o reglas de la política en un cortafuegos con múltiples sistemas virtuales. Incluye

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	configuraciones de red y dispositivos específicas de un sistema virtual (como las zonas). • **<device-group>** (solo Panorama): el nombre del grupo de dispositivos en el que se definen los objetos o reglas de la política. • **<template>** (solo Panorama): el nombre de la plantilla o pila de plantillas en la que se definen los ajustes. • **<template>** (solo Panorama): el nombre del grupo de recopiladores en el que se definen los ajustes. • **<log-collector>** (solo Panorama): el nombre del recopilador de logs en el que se definen los ajustes.
Tipo de ubicación	Esta columna categoriza las ubicaciones donde se realizaron los cambios: • **Virtual Systems (Sistemas Virtuales)**: (solo cortafuegos) configuraciones definidas en un sistema virtual específico. • **Device Groups (Grupos de dispositivos)**: (solo Panorama) configuraciones definidas en un grupo de dispositivos específico. • **Templates (Plantillas)**: (solo Panorama) configuraciones definidas en una plantilla o pila de plantillas específica. • **Collector Groups (Grupos de recopiladores)**: (solo Panorama) ajustes específicos de una configuración de grupo de recopiladores.
Include in Save (guardado parcial únicamente)	Permite seleccionar los cambios que desea guardar. De manera predeterminada, se seleccionan todos los cambios en **Save Scope (Ámbito de guardado)**. Esta columna solo se muestra tras elegir guardar los cambios realizados por administradores específicos (**Save Changes Made By**). *Es posible que haya dependencias que afecten los cambios que incluye al guardar. Por ejemplo, si añade un objeto y otro administrador, a continuación, modifica ese objeto, no puede guardar el cambio del otro administrador sin guardar su propio cambio.*
Group by Location Type	Agrupa la lista de cambios de configuración en **Save Scope (Ámbito de guardado)** por **Location Type (Tipo de ubicación)**.
Vista previa de cambios	Permite comparar las configuraciones seleccionadas en **Save Scope (Ámbito de guardado)** con la configuración en ejecución. La ventana de vista previa utiliza codificación de colores para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo). Para ayudarle a comparar los cambios con las secciones de la interfaz web, puede configurar la ventana de vista previa para que muestre **Lines of Context (Líneas de contexto)** antes y después de cada cambio. Este contexto proviene de los archivos de las configuraciones candidata y en ejecución que está comparando. *Debido a que los resultados de previsualización se muestran en una ventana nueva, su navegador debe permitir ventanas emergentes. Si la ventana*

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	de previsualización no se abre, consulte la documentación de su navegador para ver los pasos para desbloquear las ventanas emergentes.
Cambiar resumen	Enumera los ajustes individuales en los que está guardando cambios. La lista **Change Summary (Resumen de los cambios)** muestra la siguiente información para cada ajuste: • **Object Name (Nombre de objeto)**: el nombre que identifica la política, el objeto, el ajuste de red o la configuración del dispositivo. • **Type (Tipo)**: el tipo de ajuste (como Dirección, Regla de seguridad o Zona). • **Location Type (Tipo de ubicación)**: indica si el ajuste está definido en **Virtual Systems (Sistemas virtuales)**. • **Location (Ubicación)**: el nombre del sistema virtual donde se define el ajuste. La columna muestra **Shared (Compartido)** en los ajustes que no son específicos a un sistema virtual. • **Operations (Operaciones)**: indica todas las operaciones (crear, editar o eliminar) realizadas en la configuración desde la última compilación. • **Owner (Propietario)**: el administrador que realizó el último cambio en el ajuste. • **Will Be Saved (Se guardará)**: indica si el guardado incluirá el ajuste. • **Previous Owners (Propietarios anteriores)**: administradores que realizaron cambios en el ajuste antes del último cambio. Opcionalmente, puede agrupar por nombre de columna con **Group By (Agrupar por)** (como, por ejemplo, **Type [Tipo]**).
Guardar	Guarda los cambios seleccionados en un archivo de instantánea de configuración: • Si ha seleccionado **Save All Changes (Guardar todos los cambios)**, el cortafuegos sobrescribe el archivo de instantánea de configuración predeterminada (.snapshot.xml). • Si ha seleccionado **Save Changes Made By (Guardar los cambios realizados por)**, especifique el **Name (Nombre)** de un archivo de configuración nuevo o existente y haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

Invertir cambios

Seleccione **Config (Configuración)** > **Revert Changes (Revertir cambios)** en la parte superior derecha del cortafuegos o de la interfaz web de Panorama para deshacer los cambios realizados en la configuración candidata desde la última confirmación. Revertir cambios restaura la configuración a los valores de la configuración en ejecución. Puede filtrar los cambios de configuración que desea revertir por administrador o *ubicación*. La ubicación puede ser sistemas virtuales específicos, objetos y políticas compartidos, o configuración de red y dispositivos compartidos.

No se pueden revertir los cambios hasta que el cortafuegos o Panorama concluya el procesamiento de todas las compilaciones pendientes o en curso. Tras iniciar la reversión, el cortafuegos o Panorama bloquea automáticamente las configuraciones candidatas y en ejecución para que los demás administradores no puedan editar la configuración ni compilar cambios. Después de completar la reversión, el cortafuegos o Panorama quita el bloqueo automáticamente.

El cuadro de diálogo Revert Changes muestra las opciones descritas en la siguiente tabla:

Campo/Botón	Description (Descripción)
Revert All Changes	Revierte todos los cambios para los que tiene privilegios administrativos (predeterminado). No puede filtrar manualmente el ámbito de los cambios de configuración que revierte el cortafuegos cuando se selecciona esta opción. En su lugar, la función de administrador asignada a la cuenta utilizada para iniciar sesión determina el ámbito de reversión: • **Función de superusuario**: el cortafuegos revierte los cambios de todos los administradores. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan el ámbito de reversión (consulte Device > Admin Roles). Si el perfil incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, el cortafuegos revierte los cambios configurados por cualquiera de los administradores. Si su perfil de función de administración no incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, el cortafuegos revierte solo sus cambios y no los de los demás administradores. *En los perfiles de función de administración, los privilegios para compilación también se aplican a la reversión.* Si ha implementado dominios de acceso, el cortafuegos aplica automáticamente esos dominios para filtrar el ámbito de reversión (consulte Device > Access Domain). Independientemente de su función administrativa, el cortafuegos revierte solo los cambios de configuración en los dominios de acceso asignados a su cuenta.
Revert Changes Made By	Filtra el ámbito de los cambios de configuración que revierte el cortafuegos. La función administrativa asignada a la cuenta utilizada para iniciar sesión determina las opciones de filtrado:

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Función de superusuario**: puede limitar el ámbito de reversión a los cambios realizados por administradores específicos y a los cambios en ubicaciones específicas. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan las opciones de filtrado (consulte Device > Admin Roles). Si el perfil incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, puede limitar el ámbito de reversión a cambios configurados por administradores específicos y a cambios en ubicaciones específicas. Si su perfil de función de administración no incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, solo puede limitar el ámbito de reversión a los cambios realizados por usted mismo en ubicaciones específicas. Filtre el ámbito de reversión de la siguiente manera: • **Filtrar por administrador**: incluso si su función permite revertir los cambios de otros administradores, el ámbito de reversión incluye solo sus cambios de forma predeterminada. Para añadir otros administradores al ámbito de restablecimiento, haga clic en el enlace **<usernames>**, seleccione los administradores y haga clic en **OK (Aceptar)**. • **Filtrar por ubicación**: seleccione los cambios en ubicaciones específicas para incluir en la reversión Include in Revert. Si ha implementado dominios de acceso, el cortafuegos filtra automáticamente el ámbito de reversión en función de dichos dominios (consulte Device > Access Domain). Independientemente de su función administrativa y de sus opciones de filtrado, el ámbito de reversión solo incluye los cambios de configuración en los dominios de acceso asignados a su cuenta.
Revert Scope	Enumera las ubicaciones donde hay cambios que revertir. Que la lista incluya todos los cambios o un subconjunto de ellos depende de varios factores, tal como se describe en las opciones Revert All Changes y Revert Changes Made By. Las ubicaciones pueden ser cualquiera de las siguientes opciones: • **shared-object (objeto compartido)**: ajustes definidos en la ubicación compartida. • **policy-and-objects (política-y-objetos)**: (solo cortafuegos) reglas de políticas u objetos que se definen en un cortafuegos sin varios sistemas virtuales. • **device-and-network (dispositivo-y-red)**: (solo cortafuegos) ajustes de red y dispositivo globales (como los perfiles de gestión de interfaz), no son específicos de un sistema virtual. • **<virtual-system>** (solo cortafuegos): el nombre del sistema virtual en el que se definen los objetos o reglas de la política en un cortafuegos con múltiples sistemas virtuales. Incluye configuraciones de red y dispositivos específicas de un sistema virtual (como las zonas). • **<device-group>** (solo Panorama): el nombre del grupo de dispositivos en el que se definen los objetos o reglas de la política.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **<template>**: (solo Panorama) el nombre de la plantilla o pila de plantillas en la que se definen los ajustes. • **<log-collector-group>**: (solo Panorama) el nombre del grupo de recopiladores en el que se definen los ajustes. • **<log-collector>**: (solo Panorama) el nombre del recopilador de logs en el que se definen los ajustes.
Tipo de ubicación	Esta columna categoriza las ubicaciones donde se realizaron los cambios: • **Virtual Systems (Sistemas Virtuales)**: (solo cortafuegos) configuraciones definidas en un sistema virtual específico. • **Device Group (Grupo de dispositivos)**: (solo Panorama) configuraciones definidas en un grupo de dispositivos específico. • **Template (Plantilla)**: (solo Panorama) configuraciones definidas en una plantilla o pila de plantillas específica. • **Log Collector Group (Grupo de recopiladores de log)**: (solo Panorama) ajustes específicos de una configuración de grupo de recopiladores. • **Log Collector (Recopiladores de log)**: (solo Panorama) ajustes específicos de una configuración de recopiladores de log. • **Other Changes (Otros cambios)**: ajustes que no son específicos de ninguna de las áreas de configuración anteriores (como los objetos compartidos).
Include in Revert (reversión parcial únicamente)	Permite seleccionar los cambios que desea revertir. De manera predeterminada, se seleccionan todos los cambios en **Revert Scope (Ámbito de reversión)**. Esta columna solo se muestra tras elegir revertir los cambios realizados por administradores específicos (**Revert Changes Made By**). *Es posible que haya dependencias que afecten los cambios que incluye cuando revierte. Por ejemplo, si añade un objeto y otro administrador, a continuación, modifica ese objeto, no puede revertir su cambio sin revertir el cambio del otro administrador.*
Group by Location Type	Agrupa la lista de cambios de configuración en **Revert Scope (Ámbito de reversión)** por **Location Type (Tipo de ubicación)**.
Vista previa de cambios	Permite comparar las configuraciones seleccionadas en **Revert Scope (Ámbito de reversión)** con la configuración en ejecución. La ventana de vista previa utiliza codificación de colores para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo). Para ayudarle a comparar los cambios con las secciones de la interfaz web, puede configurar la ventana de vista previa para que muestre **Lines of Context (Líneas de contexto)** antes y después de cada cambio. Este contexto proviene de los archivos de las configuraciones candidata y en ejecución que está comparando.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	Debido a que los resultados de previsualización se muestran en una ventana nueva, su navegador debe permitir ventanas emergentes. Si la ventana de previsualización no se abre, consulte la documentación de su navegador para ver los pasos para desbloquear las ventanas emergentes.
Cambiar resumen	Enumera los ajustes individuales en los que está revirtiendo cambios. La lista **Change Summary (Resumen de los cambios)** muestra la siguiente información para cada ajuste: • **Object Name (Nombre de objeto)**: el nombre que identifica la política, el objeto, el ajuste de red o la configuración del dispositivo. • **Type (Tipo)**: el tipo de ajuste (como Dirección, Regla de seguridad o Zona). • **Location Type (Tipo de ubicación)**: indica si el ajuste está definido en **Virtual Systems (Sistemas virtuales)**. • **Location (Ubicación)**: el nombre del sistema virtual donde se define el ajuste. La columna muestra **Shared (Compartido)** en los ajustes que no son específicos a un sistema virtual. • **Operations (Operaciones)**: indica todas las operaciones (crear, editar o eliminar) realizadas en la configuración desde la última compilación. • **Owner (Propietario)**: el administrador que realizó el último cambio en el ajuste. • **Will Be Reverted (Se revertirá)**: indica si la reversión incluirá el ajuste. • **Previous Owners (Propietarios anteriores)**: administradores que realizaron cambios en el ajuste antes del último cambio. Opcionalmente, puede agrupar por nombre de columna con **Group By (Agrupar por)** (como, por ejemplo, **Type [Tipo]**).
Revertir	Revierte los cambios seleccionados.

© 2020 Palo Alto Networks, Inc.

Bloquear configuraciones

Para ayudarle a coordinar las tareas de configuración con otros administradores de cortafuegos durante las sesiones de inicio de sesión simultáneas, la interfaz web le permite aplicar un bloqueo de configuración o confirmación para impedir que otros administradores cambien la configuración o confirmen cambios hasta que se retire el bloqueo.

En la parte superior derecha de la interfaz web, un candado cerrado ( ) indica que se estableció uno o más candados (con el número de bloqueos entre paréntesis); un candado abierto ( ) indica que no se establecieron bloqueos. Si hace clic en cualquier candado se abre el diálogo Locks, el cual brinda los siguientes campos y opciones.

Para que el cortafuegos establezca automáticamente un bloqueo de confirmación cada vez que un administrador cambie la configuración candidata, seleccione Device (Dispositivo) > Setup (Configuración) > Management (Gestión), edite la configuración general, habilite Automatically Acquire Commit Lock (Adquirir bloqueo de confirmación automáticamente) y haga clic en OK (Aceptar) y Commit (Confirmar).

Cuando revierte los cambios (Config [Configuración] > Revert Changes [Revertir cambios]), el cortafuegos bloquea automáticamente la configuración en uso y la configuración candidata para impedir que otros administradores editen la configuración o confirmen cambios. Una vez que se han terminado de revertir los cambios, el cortafuegos levanta automáticamente el bloqueo.

Campo/Botón	Description (Descripción)
administración	El nombre de usuario del administrador que estableció el bloqueo.
Ubicación	En un cortafuegos con más de un sistema virtual (vsys), el alcance del bloqueo puede ser un vsys específico o la ubicación compartida.
Tipo	Los tipos de bloqueo son los siguientes: • **Config Lock**: bloquea la realización de cambios en la configuración candidata por parte de otros administradores. Solo un superusuario o el administrador que estableció el bloqueo puede quitarlo. • **Commit Lock (Bloqueo de compilación)**: impide que otros administradores compilen cambios en la configuración candidata. La cola de confirmaciones no acepta nuevas confirmaciones hasta que se quiten todos los bloqueos. Este bloqueo evita las colisiones que pueden ocurrir cuando múltiples administradores realizan cambios durante los inicios de sesión simultáneos y un administrador finaliza e inicia una confirmación antes de que otros administradores hayan finalizado. El cortafuegos quita automáticamente el bloqueo luego de completar la confirmación para la que el administrador estableció el bloqueo. Un superusuario o el administrador que estableció el bloqueo también puede quitarlo manualmente.
Comentarios	Introduzca hasta 256 caracteres de texto. Esto es útil para otros administradores que desea conocer el motivo del bloqueo.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
Creado el	La fecha y hora cuando un administrador estableció el bloqueo.
Conectado	Indica si el administrador que estableció el bloqueo está conectado en este momento.
Aplicación de un bloqueo	Para establecer un bloqueo, elija **Take a Lock (Aplicación de un bloqueo)**, seleccione **Type (Tipo)**, **Location (Ubicación)** (solo para cortafuegos de sistemas virtuales múltiples), escriba los comentarios que desee en **Comments (Comentarios)**, haga clic en **OK (Aceptar)** y, por último, en **Close (Cerrar)**.
Eliminar bloqueo	Para quitar un bloqueo, selecciónelo, haga clic en **Remove Lock (Eliminar bloqueo)**, **OK (Aceptar)** y luego en **Close (Cerrar)**.

© 2020 Palo Alto Networks, Inc.

Búsqueda global

Global Find le permite buscar en la configuración candidata de un cortafuegos o Panorama una cadena específica, como una dirección IP, un nombre de objeto, un nombre de política, un ID de amenaza, un identificador único universal (Universal Unique Identifier, UUID) de regla o un nombre de aplicación. 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 encuentra la cadena o se hace referencia a la misma.

Para iniciar Global Find, haga clic en el icono Search **Search (Búsqueda)** que se encuentra en la esquina superior derecha de la interfaz web. Global Find está disponible en todas las páginas y ubicaciones de la interfaz web. A continuación tiene una lista de funciones de búsqueda global que le ayudarán a realizar búsquedas correctamente:

- Si inicia una búsqueda en un cortafuegos que tiene varios sistemas virtuales habilitados o si hay funciones administrativas definidas, Global Find solamente devolverá resultados de las áreas del cortafuegos para las que tenga permisos. Lo mismo se aplica a los grupos de dispositivos Panorama; verá los resultados de búsqueda sólo para los grupos de dispositivos a los que tiene acceso administrativo.
- Los espacios del texto de búsqueda se tratan como operaciones AND. Por ejemplo, si busca en **`corp policy`**, ambos **Corp** y **policy (política)** deben existir en el elemento de configuración para que se incluya en los resultados de búsqueda.
- Para encontrar una frase exacta, indíquela entre comillas.
- Para volver a ejecutar una búsqueda anterior, haga clic en Global Find y se mostrará una lista de las últimas 20 búsquedas. Haga clic en cualquier elemento de la lista para volver a ejecutar dicha búsqueda. La lista del historial de búsqueda es exclusiva de cada cuenta de administrador.

Global Find está disponible para todos los campos que permitan la búsqueda. Por ejemplo, en el caso de una política de seguridad, puede buscar en los campos siguientes: Name (Nombre), Tags (Etiquetas), Zone (Zona), Address (Dirección), User (Usuario), HIP Profile (Perfil HIP), Application (Aplicación), UUID y Service (Servicio). Para realizar una búsqueda, haga clic en la lista desplegable situada junto a cualquiera de estos campos y haga clic en **Global Find**. Por ejemplo, si hace clic en **Global Find** en una zona denominada l3-vlan-trust, este buscará en toda la configuración de ese nombre de zona y devolverá resultados de cada ubicación donde se haga referencia a la zona. Los resultados de búsqueda se agrupan por categoría y puede pasar el cursor por encima de cualquier elemento para ver información detallada o hacer clic en un elemento para desplazarse a su página de configuración.

Global Find no buscará contenido dinámico que el cortafuegos asigna a los usuarios (como logs, intervalos de direcciones o direcciones DHPC individuales). En el caso de DHCP, puede buscar un atributo de servidor DHCP, como la entrada DNS, pero no puede buscar direcciones individuales emitidas para usuarios. Otro ejemplo son los nombres de usuario que el cortafuegos recopila cuando habilita la característica User-ID™. En este caso, un nombre de usuario o un grupo de usuarios que exista en la base de datos de User-ID solamente se puede buscar si el nombre o el grupo existe en la configuración, como cuando el nombre de un grupo de usuarios se define en una política. Por lo general, solamente puede buscar contenido que el cortafuegos escribe en la configuración.

¿Busca más información?

Obtenga más información sobre el Uso de Global Find para buscar en el cortafuegos o en la configuración de Panorama.

© 2020 Palo Alto Networks, Inc.

Detalles de amenaza

- Monitor > Logs > Threat
- ACC > Threat Activity
- Objects > Security Profiles > Anti-Spyware/Vulnerability Protection

Utilice el cuadro de diálogo Detalles de amenaza para obtener más información sobre las firmas de amenazas con las que está equipado el cortafuegos y los eventos que activan dichas firmas. Se proporcionan detalles de amenazas para:

- Logs de amenazas que registran las amenazas detectadas por el cortafuegos (**Monitor [Supervisar]** > **Logs [Logs]** > **Threat [Amenaza]**)
- Las principales amenazas que se encuentran en su red (**ACC** > **Threat Activity [Actividad de la amenaza]**)
- Firmas de amenazas que desea modificar o excluir de la aplicación (**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware/Vulnerability Protection (Protección Anti-Spyware / Vulnerabilidad)**)

Cuando encuentre una firma de amenaza sobre la que desee obtener más información, pase sobre **Threat Name (Nombre de la amenaza)** o sobre la **ID** de la amenaza y haga clic **Exception (Excepción)** para revisar los detalles de la amenaza. Los detalles de la amenaza le permiten verificar fácilmente si una firma de amenaza está configurada como excepción a su política de seguridad y encontrar la información más reciente de Threat Vault sobre una amenaza específica. La base de datos de Palo Alto Networks Threat Vault está integrada con el cortafuegos, lo que le permite ver detalles ampliados sobre las firmas de amenazas en el contexto del cortafuegos, o bien iniciar una búsqueda Threat Vault en una nueva ventana del navegador para detectar una amenaza registrada.

Dependiendo del tipo de amenaza que esté viendo, los detalles incluirán todos o algunos de los detalles de la amenaza descritos en la siguiente tabla.

Detalles de amenaza	Description (Descripción)
Nombre	Nombre de firma de amenaza
ID	ID único de firma de amenaza. Seleccionar **View in Threat Vault (Ver en Threat Vault)** para abrir una búsqueda Threat Vault en una nueva ventana del navegador y buscar la información más reciente que tiene la base de datos de amenazas de Palo Alto Networks para esta firma. La entrada de Threat Vault para la firma de amenaza podría incluir detalles adicionales, incluyendo la primera y última versión de contenido para incluir actualizaciones de la firma y la versión PAN-OS mínima requerida para admitir la firma.
Description (Descripción)	Información sobre la amenaza que desencadena la firma.
Gravedad	El nivel de gravedad de la amenaza: informativo, bajo, medio, alto o crítico.
CVE	Vulnerabilidades de seguridad conocidas públicamente asociadas con la amenaza. El identificador de vulnerabilidades y exposiciones comunes (CVE) es el identificador más útil para encontrar información sobre vulnerabilidades singulares, ya que los identificadores específicos del proveedor suelen abarcar varias vulnerabilidades.
Bugtraq ID (ID de Bugtraq)	El Bugtraq ID asociado con la amenaza.

© 2020 Palo Alto Networks, Inc.

Detalles de amenaza	Description (Descripción)
ID de proveedor	Identificador específico del proveedor para una vulnerabilidad. Por ejemplo, MS16-148 es el ID de proveedor para una o más vulnerabilidades de Microsoft, y APBSB16-39 es el ID de proveedor para una o más vulnerabilidades de Adobe.
Referencia	Fuentes de investigación que puede utilizar para obtener más información sobre la amenaza.
Perfiles de exención	Perfiles de seguridad que definen una acción de cumplimiento para la firma de amenaza diferente a la acción de firma predeterminada. La excepción de amenaza sólo está activa cuando se agregan perfiles exentos a una regla de política de seguridad (compruebe si la excepción es Se utiliza en la regla de seguridad actual).
Utilizado en la regla de seguridad actual	Excepciones de amenaza activa: una marca de verificación en esta columna indica que el cortafuegos está aplicando activamente la excepción de amenaza (los Perfiles exentos que definen la excepción de amenaza se adjuntan a una regla de política de seguridad). Si esta columna es clara, el cortafuegos está imponiendo la amenaza basándose únicamente en la acción de firma predeterminada recomendada.
Direcciones IP de exención	Direcciones IP exentas: puede agregar una dirección IP para filtrar la excepción de amenaza o ver las **Exempt IP Addresses (Direcciones IP exentas)**. Esta opción impone una excepción de amenaza sólo cuando la sesión asociada tiene una dirección IP de origen o de destino que coincide con la dirección IP exenta. Para todas las demás sesiones, la amenaza se aplica basándose en la acción de firma predeterminada.

Si tiene problemas para ver los detalles de la amenaza, compruebe las siguientes condiciones:

- *La licencia de prevención de amenazas del cortafuegos está activa (Device [Dispositivo] > Licenses [Licencias]).*
- *Están instaladas las actualizaciones más recientes de contenido de aplicaciones y protección antivirus y contra amenazas.*
- *El acceso a Threat Vault está habilitado (seleccione Device [Dispositivo] > Setup [Configuración] > Management [Gestión] y edite el ajuste Logging and Reporting (Registro e informes) en Enable Threat Vault Access (Habilitar el acceso a Threat Vault)).*
- *El valor predeterminado (o personalizado) de* Perfiles de seguridad de antivirus, antispyware y protección frente a vulnerabilidades *se aplicará a su política de seguridad.*

© 2020 Palo Alto Networks, Inc.

Resumen de inteligencia de AutoFocus

Puede ver una descripción gráfica de la información de amenazas que AutoFocus compila para ayudarle a evaluar la penetración y el riesgo de los siguientes artefactos del cortafuegos:

- Dirección IP
- URL
- Dominio
- Agente de usuario (encontrado en la columna Agente de usuario de los logs de filtrado de datos)
- Nombre de la amenaza (solo para las amenazas de los virus de subtipos y wildfire)
- Filename
- SHA-256 hash (que se encuentra en la columna File Digest (Resumen de archivo) de los logs de envíos de WildFire)

Para ver la ventana del resumen de inteligencia de AutoFocus, primero debe tener una suscripción de AutoFocus activa y habilitar la inteligencia contra amenazas de AutoFocus (seleccione **Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** y edite la configuración de AutoFocus).

Una vez que ha habilitado la inteligencia de AutoFocus, pase el cursor del ratón sobre un log o artefacto de lista dinámica externa para abrir la lista desplegable ( ) y luego haga clic en **AutoFocus**:

- Ver tráfico, amenaza, filtrado de URL, envíos de WildFire, filtrado de datos y logs unificados (**Monitor [Supervisar]** > **Logs [Logs]**).
- Ve entradas de lista dinámica externa.

También puede iniciar una búsqueda de AutoFocus desde el cortafuegos para investigar en mayor detalle los artefactos interesantes o sospechosos que encuentre.

Campo/Botón	Description (Descripción)
Buscar en AutoFocus...	Haga clic para que Autofocus inicie una búsqueda del artefacto.
Pestaña Información de análisis	
Sesiones	El número de sesiones privadas en las que WildFire detectó el artefacto. Las sesiones privadas son sesiones que se ejecutan solo en los cortafuegos asociados con su cuenta de asistencia técnica. Coloque el cursor sobre una barra de sesiones para ver el número de sesiones por mes.
Muestras	Organización y muestras globales (archivos y enlaces de correo electrónico) asociados con el artefacto y agrupados por veredicto de WildFire (benigno, grayware, malware, phishing). *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. Haga clic en un veredicto de WildFire para que Autofocus inicie una búsqueda del artefacto filtrado según ámbito (organización o global) y veredicto de WildFire.
Matching Tags	Etiquetas de AutoFocus que coinciden con el artefacto: • **Etiquetas privadas**: Visible sólo para los usuarios de Autofocus asociados con su cuenta de asistencia técnica. • **Etiquetas públicas**: Visible para todos los usuarios de AutoFocus.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Unidad 42 Etiquetas**: Identifican las amenazas y las campañas que suponen un riesgo directo de seguridad. Estas etiquetas son creadas por la Unidad 42 (el equipo de inteligencia e investigación de amenazas de Palo Alto Networks). • **Etiquetas informativas**: Etiquetas de Unit 42 que identifican las amenazas de productos. Coloque el cursor sobre una etiqueta para ver la descripción de la etiqueta y otros detalles de la etiqueta. Haga clic en una etiqueta para que Autofocus inicie una búsqueda de esa etiqueta. Para ver más etiquetas coincidentes de un artefacto, haga clic en el símbolo de elipsis (...) para que AutoFocus inicie una búsqueda de ese artefacto. La columna Etiquetas en los resultados de búsqueda AutoFocus muestra más etiquetas coincidentes para el artefacto.
Pestaña de DNS pasivo La pestaña DNS pasivo muestra el historial de DNS pasivo asociado al artefacto. Esta pestaña sólo muestra información coincidente si el artefacto es una dirección IP, dominio o URL.	
request	El dominio que envió una solicitud de DNS. Haga clic en el dominio para iniciar una búsqueda de Autofocus.
Tipo	El tipo de solicitud DNS (por ejemplo: A, NS, CNAME).
Respuesta	La dirección IP o el dominio al que se resolvió la solicitud de DNS. Haga clic en la dirección IP o dominio para iniciar una búsqueda de Autofocus. *La columna Respuesta no muestra direcciones IP privadas.*
Count	El número de veces que se realizó la solicitud.
First Seen	La fecha y la hora en que la combinación Request, Response y Type se vio por primera vez en base al historial de DNS pasivo.
Last Seen	La fecha y la hora en que la combinación Request, Response y Type se vio más recientemente en base al historial de DNS pasivo.
Pestaña Matching Hashes La pestaña de hashes coincidentes muestra las cinco muestras privadas más recientes en las que WildFire detectó el artefacto. Las muestras privadas son muestras que se detectaron únicamente en los cortafuegos asociados con su cuenta de asistencia técnica.	
SHA256	El hash SHA-256 para una muestra. Haga clic en el hash para que Autofocus inicie una búsqueda de ese hash.
File Type	El tipo de archivo de la muestra.
Create Date	La fecha y hora en que WildFire analizó una muestra y le asignó un veredicto de WildFire.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
Update Date	La fecha y hora en que WildFire actualizó el veredicto de WildFire para una muestra.
Verdict	El veredicto de WildFire para una muestra: benigno, grayware, malware o phishing.

© 2020 Palo Alto Networks, Inc.

Exportación de la tabla de configuración

Los usuarios administrativos pueden exportar los datos de la base de reglas, los objetos, los dispositivos gestionados de .a política y las interfaces en formato tabular en un archivo PDF o CSV. Los datos que se exportan son los datos visibles en la interfaz web. En el caso de los datos filtrados, solo se exportan los datos que coinciden con el filtro. Si no aplica filtros, se exportan todos los datos.

Todos los datos confidenciales, como contraseñas, se ocultan con símbolos de comodín (*).

Se genera un log del sistema y un enlace de descarga cuando la exportación de la tabla de configuración se realiza correctamente. Utilice el enlace de descarga para guardar el archivo PDF o CSV localmente. Luego de cerrar la ventana que contiene el enlace de descarga, el enlace de descarga de esa exportación ya no estará disponible.

Para exportar los datos de la tabla, haga clic en **PDF/CSV** y configure los siguientes ajustes:

Configuración de exportación	Description (Descripción)
Nombre de archivo	Introduzca un nombre (de hasta 32 caracteres) para identificar los datos exportados. Este nombre se asignará también al archivo de descarga que se genera con la exportación.
File Type	Seleccione el tipo de archivo de exportación que desea generar. Puede seleccionar el formato PDF o CSV.
Page Size (Tamaño de página)	El tamaño de página predeterminado es carta (22 cm por 28 cm). No puede cambiar el tamaño de la página. De manera predeterminada, el PDF se genera con orientación vertical y cambia la orientación horizontal para adaptarla a la cantidad máxima de columnas.
Description (Descripción) (Solo en PDF)	Introduzca una descripción (255 caracteres como máximo) para brindar contexto e información adicional sobre la exportación.
Table Data (Datos de la tabla)	Muestra la tabla de datos que se exportará. Si desea borrar los ajustes de filtrado que estableció previamente, haga clic en **Show All Columns (Mostrar todas las columnas)** para mostrar todas las reglas de la política del tipo de política seleccionado. Luego, podrá añadir o eliminar columnas, y aplicar los filtros según sea necesario.
Show All Columns (Mostrar todas las columnas)	Elimina todos los filtros y muestra todas las columnas de la tabla.

Haga clic en **Export (Exportar)** para generar el enlace de descarga de la tabla de configuración.

© 2020 Palo Alto Networks, Inc.

Dashboard (Panel)

Los widgets del Dashboard muestran información general del cortafuegos o Panorama™, como por ejemplo la versión de software, el estado de cada interfaz, la utilización de recursos y hasta 10 entradas para cada uno de varios tipos de log; los widgets de log muestran las entradas de la última hora.

El tema Widgets del Dashboard (Panel) describe cómo utilizar el panel y describe los widgets disponibles.

© 2020 Palo Alto Networks, Inc.

Widgets de panel

De manera predeterminada, **Dashboard (Panel)** muestra widgets en un **Layout (Diseño)** de **3 columns (3 columnas)** pero es posible personalizar el **Dashboard (Panel)** para mostrar solo **2 columns (2 columnas)**, en su lugar.

También puede decidir qué widgets mostrar u ocultar para ver solo los que desea supervisar. Para mostrar un widget, seleccione una categoría de widget en la lista desplegable **Widgets** y seleccione un widget para agregarlo al Dashboard (los nombres de los widgets que aparecen en el texto atenuado y atenuado ya se muestran). Para ocultar (dejar de mostrar) un widget, cierre el widget (en el encabezado del widget). Los cortafuegos y Panorama guardan la configuración de visualización de widgets en todos los inicios de sesión (por separado para cada administrador).

Consulte la **Last updated (Última actualización)** de la marca de tiempo para determinar cuándo se actualizaron por última vez los datos del Dashboard. Puede actualizar manualmente todo el **Dashboard (Panel)** (en la esquina superior derecha del Dashboard) o puede actualizar widgets individuales (dentro de cada cabecera de widget). Utilice el menú desplegable sin etiqueta junto a la opción de actualización manual del Dashboard ( ) Para seleccionar el intervalo de actualización automático para **Dashboard (Panel)** (en minutos): **1 Min**, **2 min** , o **5 min**; para desactivar la actualización automática para todo el **Dashboard (Panel)**, seleccione **Manual**.

Widgets de panel	Description (Descripción)
Widgets de aplicación	
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.
Factor de riesgo de ACC	Muestra el factor de riesgo medio (1-5) para el tráfico de red procesado la semana pasada. Los valores mayores indican un mayor riesgo.
Widgets del sistema	
Información general	Muestra el nombre y modelo del cortafuegos o Panorama, la CPU y RAM de Panorama, el modo de sistema de Panorama, la versión de software de PAN-OS® o Panorama, la información de IP de gestión de IPv4 e IPv6, el número de serie, el identificador e identificador único universal (Universal Unique Identifier, UUID) de la CPU, las versiones de definición de filtro de la aplicación, amenaza y URL, la fecha y hora actual, y el tiempo transcurrido desde el último reinicio.
Interfaces (Solo cortafuegos)	Indica si cada interfaz está activa (verde), no está operativa (rojo) o en un estado desconocido (gris).

© 2020 Palo Alto Networks, Inc.

Widgets de panel	Description (Descripción)
Recursos del sistema	Muestra el uso de CPU de gestión, el uso de plano de datos y el número de sesiones (el número de sesiones establecido a través del cortafuegos o Panorama).
High Availability	Cuando alta disponibilidad (high availability, HA) está activada, indica el estado de HA de Panorama/cortafuegos local y del peer: verde (activa), amarillo (pasiva) o negro (otro). Para obtener más información sobre HA, consulte Device > Virtual Systems o Panorama > High Availability.
Bloqueos	Muestra los bloqueos de configuración que establecieron los administradores.
Administradores registrados	Muestra la dirección IP de origen, el tipo de sesión (interfaz web o CLI) y la hora de inicio de sesión para cada administrador actualmente registrado.
Widgets de logs	
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. Muestra solo las entradas de los últimos 60 minutos.
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 Filtrado de datos	Muestra la descripción y la fecha y hora de los últimos 60 minutos en el log Filtrado de datos.
Logs de configuración	Muestra el nombre de usuario del administrador, el cliente (la interfaz web o CLI) y la fecha y hora de las 10 últimas entradas en el log Configuración. Muestra solo las entradas de los últimos 60 minutos.
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. Muestra solo las entradas de los últimos 60 minutos.*

ACC

El Centro de control de aplicaciones (ACC) es una herramienta analítica que proporciona inteligencia intuitiva sobre la actividad dentro de su red. El ACC usa los logs del cortafuegos para representar gráficamente las tendencias de su red. La representación gráfica le permite interactuar con los datos y visualizar las relaciones entre eventos en la red, incluidos los patrones de uso de la red, patrones de tráfico, actividades sospechosas y anomalías.

> Información básica sobre el ACC
> Pestañas de ACC
> Widgets de ACC
> Acciones de ACC
> Uso de las pestañas y widgets
> Uso de los filtros: Filtros locales y filtros globales

¿Busca más información?

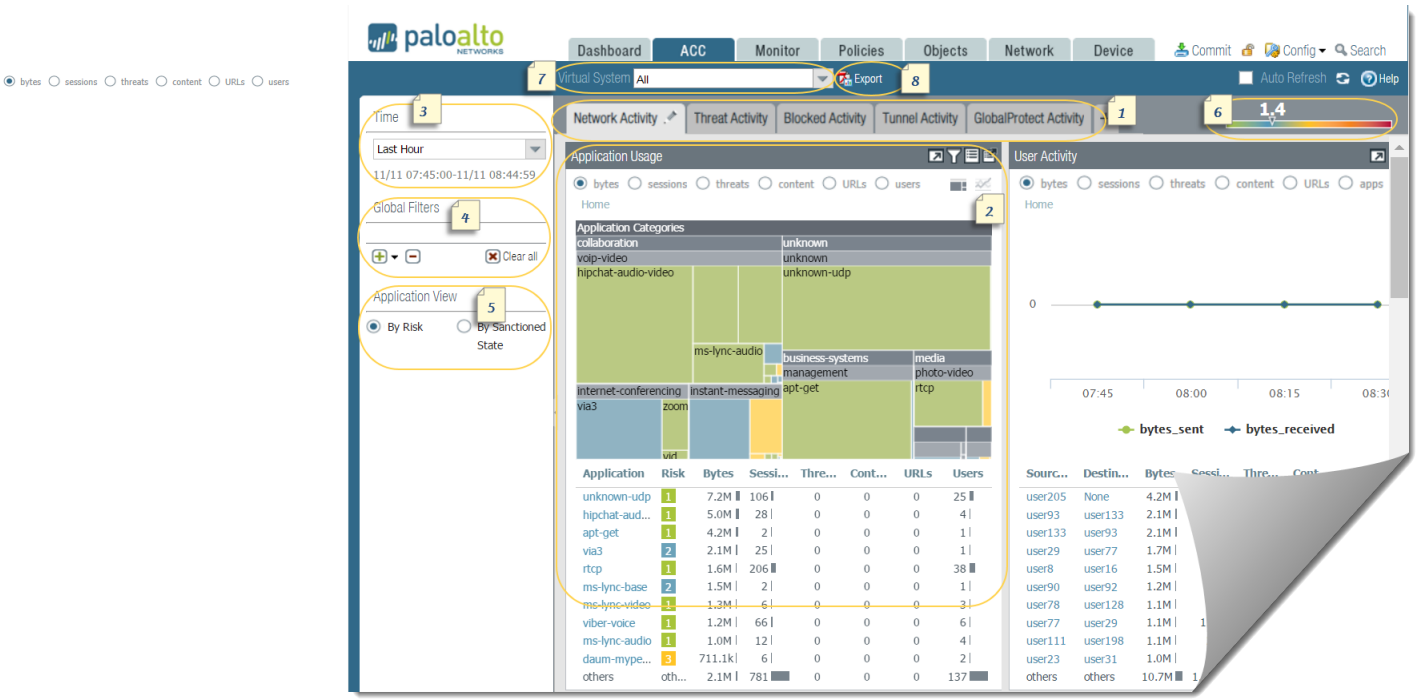
Consulte Uso del Centro de control de aplicaciones.

© 2020 Palo Alto Networks, Inc.

Información básica sobre el ACC

La siguiente tabla muestra la ficha ACC y describe cada componente.

Información básica sobre el ACC



1	**Pestañas**	El ACC incluye pestañas predefinidas que proporcionan visibilidad sobre: tráfico de red, actividad de amenaza, actividad bloqueada, actividad de túnel, activad de GlobalProtect y la actividad de la red móvil (si la seguridad GTP está habilitada). Si desea más información sobre cada pestaña, consulte Pestañas de ACC.
2	**Widgets**	Cada pestaña incluye un conjunto predeterminado de widgets que representan concretamente los eventos y tendencias asociados a la pestaña. Los widgets le permiten consultar los datos usando los siguientes filtros: bytes (entrada y salida), sesiones, contenido (archivos y datos), categorías de URL, aplicaciones, usuarios, amenazas (malintencionadas, benignas, grayware, phishing) y recuento. Si desea más información sobre cada pestaña, consulte Widgets de ACC.
3	**Time**	Los gráficos en cada widget ofrecen una vista en tiempo real y de historial. Puede elegir un intervalo personalizado o usar los periodos predefinidos que van desde 15 minutos hasta los últimos 30 días o los últimos 30 días naturales. El periodo usado de manera predeterminada para representar datos es la última hora. El intervalo de hora y fecha se muestran en la pantalla. Por ejemplo: `11/11 10:30:00-01/12 11:29:59`

© 2020 Palo Alto Networks, Inc.

Información básica sobre el ACC		
4	**Filtros globales**	Los filtros globales le permiten establecer el filtro en todas las pestañas. Los gráficos se aplican a los filtros seleccionados antes de representar los datos. Para obtener información sobre cómo utilizar los filtros, consulte Acciones de ACC.
5	**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. Verde indica aplicaciones sancionadas, azul aplicaciones no sancionadas y amarillo indica aplicaciones que tienen un estado de sanción diferente en diferentes sistemas virtuales o grupos de dispositivos.
6	**Medidor de riesgos**	El medidor de riesgos (1=más bajo; 5=más alto) indica el riesgo de seguridad relativo de su red. El medidor de riesgos usa diversos factores como el tipo de aplicaciones vistas en la red y los niveles de riesgo asociados a las aplicaciones, la actividad de las amenazas y el software malintencionado según el número de amenazas bloqueadas, así como los hosts en riesgo o el tráfico hacia hosts o dominios malintencionados.
7	**Source (Origen)**	Los datos usados para la visualización varía entre el cortafuegos y Panorama™. Tiene las siguientes opciones para seleccionar qué datos se utilizan para generar las vistas en el ACC: **Virtual System**: En un cortafuegos que 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. **Device Group**: En Panorama, puede usar el menú desplegable **Device Group (Grupo de dispositivos)** para cambiar la visualización del ACC de modo que incluya datos de todos los grupos de dispositivos o solo un grupo de dispositivos seleccionados. **Data Source**: En Panorama, también puede cambiar la visualización para usar **Panorama** o **Remote Device Data (Datos de dispositivo remoto)** (datos del cortafuegos gestionado). Si el origen de los datos es **Panorama**, puede filtrar la visualización para un grupo de dispositivos específico.
8	**Exportar**	Puede exportar los widgets que se muestran en la pestaña actual como un PDF.

© 2020 Palo Alto Networks, Inc.

Pestañas de ACC

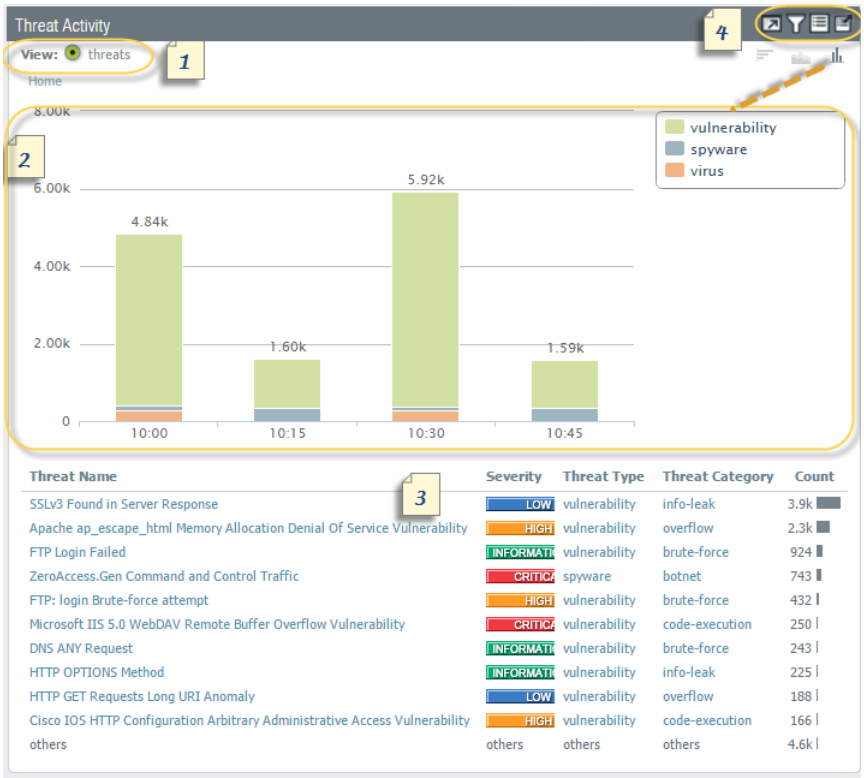
- **Network Activity (Actividad de red)**: Muestra una descripción general del tráfico y la actividad de los usuarios en su red. Esta vista se centra en las aplicaciones principales en uso, los usuarios que generan más tráfico y una descripción pormenorizada de los bytes, contenido, amenazas y direcciones URL a las que ha accedido el usuario, además de las reglas de la política de seguridad más utilizadas con las que se comparar el tráfico. Asimismo, puede ver la actividad de la red según la zona de origen o destino, región o direcciones IP, por interfaces de entrada o salida y por información del host, como los sistemas operativos de los dispositivos más usados en la red.
- **Threat Activity (Actividad de amenazas)**: Esta pestaña muestra una descripción general de las amenazas en la red. Se centra en las principales amenazas: vulnerabilidades, spyware, virus, hosts que visitan dominios o URL malintencionados, principales envíos de WildFire por tipo de archivo y aplicación y aplicaciones que usan puertos no estándar. El widget Hosts en riesgo complementa la detección con mejores técnicas de visualización. Usa la información de la pestaña de eventos correlacionados (Monitor > Automated Correlation Engine > Correlated Events) para presentar una vista agregada de hosts en riesgo en su red por usuarios o direcciones IP de origen, organizadas por nivel de gravedad.
- **Blocked Activity (Actividad bloqueada)**: Esta pestaña se centra en el tráfico bloqueado para que no entre 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 (archivos y datos) y las principales reglas de seguridad con una acción de denegación que bloquearon el tráfico.
- **Mobile Network Activity (Actividad de red móvil)**: muestra una representación visual del tráfico móvil en su red utilizando los logs GTP generados a partir de su configuración para las reglas de la política de seguridad. Esta vista incluye eventos GTP interactivos y personalizables, actividad de suscriptor móvil y widgets de causa de rechazo de GTP a los que puede aplicar filtros ACC y profundizar para aislar la información que necesita. Cuando habilita la seguridad de SCTP, los widgets en esta pestaña muestran una representación visual y detalles de los eventos ed SCTP en el cortafuegos, además de la cantidad de fragmentos enviados y recibidos por ID de asociación de SCTP.
- **Tunnel Activity (Actividad del 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 la ID del túnel, la etiqueta de inspección, el usuario y los protocolos de túnel tales como Generic Routing Encapsulation (GRE), el protocolo de túnel para datos de usuario (GTP-U) del General Packet Radio Service (GPRS) e IPSec no cifrado.
- **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.

También puede personalizar las pestañas y widgets según se describe en Uso de las pestañas y widgets*.*

© 2020 Palo Alto Networks, Inc.

Widgets de ACC

Los widgets de cada pestaña están inactivos. Puede establecer filtros y pormenorizar la visualización para personalizarla y poder centrarse en la información que necesita.



Cada widget está estructurado para mostrar la siguiente información:

1	**Ver**	Puede ordenar los datos por bytes, sesiones, amenazas, recuento, usuarios, contenido, aplicaciones, URL, malintencionados, benignos, grayware, phishing, nombre(s) de archivos, datos, perfiles, objetos. 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, y la experiencia de interacción 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 y ver información más granular de esa selección.
3	**Tabla**	La vista detallada de los datos usados para representar el gráfico se muestra en una tabla debajo del gráfico. Puede hacer clic y establecer un filtro local o un filtro global para elementos en la tabla. Con un filtro local, el gráfico se actualiza y la tabla se ordena según ese filtro.

© 2020 Palo Alto Networks, Inc.

		Con un filtro global, la vista de todo el ACC pivota para mostrar solo la información específica de su filtro.
4	**Acciones**	Las siguientes son acciones disponibles en la barra de títulos de un widget: • **Maximize view**: Le permite aumentar el widget y verlo en una pantalla más grande. En la vista maximizada, es posible ver más de los diez elementos principales que se muestran en la pantalla predeterminada del widget. • **Set up local filters**: Le permite añadir filtros que refinan la visualización dentro del widget. Consulte Uso de los filtros: filtros locales y filtros globales. • **Jump to logs (Saltar a logs)**: le permite navegar directamente a los logs (**Monitor [Supervisar]** > **Logs [Logs]** > **<log-type>**). Los logs se filtran usando el periodo que se muestra en el gráfico. Si establece 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 establecido. • **Export**: le permite exportar el gráfico como PDF.

Si quiere ver una descripción de cada widget, consulte la información sobre el uso del ACC.

© 2020 Palo Alto Networks, Inc.

Acciones de ACC

Para personalizar y refinar la visualización de ACC, puede añadir y eliminar pestañas y widgets, establecer filtros locales y globales e interactuar con los widgets.

- Uso de las pestañas y widgets
- Uso de los filtros: Filtros locales y filtros globales

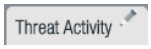
Uso de las pestañas y widgets

Las siguientes opciones describen cómo utilizar y personalizar pestañas y widgets.

- Añada una pestaña personalizada.
  1. Seleccione Add ( ) de la lista de pestañas.
  2. Añada un **View Name**. Este nombre se utilizará como el nombre de la pestaña. Puede añadir hasta 10 pestañas personalizadas.

- Modifique una pestaña.

  Seleccione la pestaña y haga clic en editar junto al nombre de la pestaña para modificarla.

  Ejemplo: 

- Establecer pestaña como predeterminada
  1. Modifique una pestaña.
  2. Seleccione para establecer la pestaña actual como predeterminada. Cada vez que inicie sesión en el cortafuegos, se mostrará esta pestaña.

- Guarde el estado de una pestaña
  1. Modifique una pestaña.
  2. Seleccione para guardar sus preferencias en la pestaña actual como predeterminada.

     El estado de la pestaña, incluidos los filtros que se hayan configurado, se sincronizan entre peers de HA.

- Exportar una pestaña:
  1. Modifique una pestaña.
  2. Seleccione para exportar la pestaña actual. La pestaña se descarga en su equipo como un archivo .txt. Debe habilitar las ventanas emergentes para descargar el archivo.

- Importar una pestaña:
  1. Añada una pestaña personalizada.
  2. Seleccione para importar una pestaña.
  3. Busque el archivo de texto (.txt) y selecciónelo.

© 2020 Palo Alto Networks, Inc.

- Vea qué widgets están incluidos en una vista.
  1. Seleccione la vista y haga clic en Modificar ( ).
  2. Seleccione el menú desplegable **Add Widgets (Añadir Widget)** para revisar los widgets seleccionados.

- 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 (Añadir grupo de widgets)**. 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 un widget o un grupo de widgets.
  - Para eliminar una pestaña personalizada, seleccione la pestaña y haga clic en eliminar ( ).

    No puede eliminar una pestaña predefinida.
  - Para eliminar un widget o grupo de widgets, edite la pestaña y luego haga clic en eliminar ([X]). Esta acción no se puede deshacer.

- Restablecer la vista predeterminada.

  En una vista predefinida, como la vista **Blocked Activity (Actividad bloqueada)**, 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)**..

Uso de los filtros: Filtros locales y filtros globales

Para depurar la información y controlar con precisión qué muestra el ACC, puede usar filtros.

- **Local Filters**: los filtros locales se aplican a un widget específico. Un filtro local le permite interactuar con el gráfico y personalizar la vista para que pueda explorar los datos y acceder a la información que quiere supervisar en un widget específico. Puede aplicar un filtro local de dos modos: haga clic en un atributo del gráfico o tabla o seleccione **Set Filter (Establecer filtro)**dentro de un widget. La opción **Set Filter (Establecer filtro)** le permite establecer un filtro local que no se elimina al reiniciar.
- **Global filters**: los filtros globales se aplican a todo el ACC. Un filtro global le permite pivotar la vista alrededor de la información que más necesita y excluir la información irrelevante para la vista actual. Por ejemplo, para ver todos los eventos relacionados con un usuario y aplicación específicos, puede aplicar la dirección IP del usuario y especificar la aplicación para crear un filtro global que muestra 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 durante inicios de sesión.

  Los filtros globales se pueden aplicar 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.

© 2020 Palo Alto Networks, Inc.

- **Añadir un filtro de widget para que sea un filtro global**: pase el cursor del ratón sobre el atributo y haga clic en el icono de 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.

- Establecer un filtro local.

  También puede hacer clic en un atributo en la siguiente tabla bajo el gráfico para aplicarlo como un filtro local.

  1. Seleccione un widget y haga clic Filtrar ( ).
  2. Añada ( ) filtros que desea aplicar.
  3. Haga clic en **Apply (Aplicar)**. Estos filtros no se eliminan al reiniciar.

  El número de filtros locales aplicado en un widget se indica junto al nombre del widget.

- Establecer un filtro global desde una tabla.

  Pase el curso del ratón sobre un atributo en una tabla y haga clic en la flecha que aparece a la derecha del atributo.

- Establezca un filtro global usando el panel Filtros globales

  Añada ( ) filtros que desea aplicar.

- Promocionar un filtro local como filtro global.
  1. En cualquier tabla de un widget, seleccione un atributo. De este modo se establece el atributo como un filtro local.
  2. Para promover el filtro a un filtro global, pase el cursor del ratón sobre el atributo y haga clic en la flecha a la derecha del atributo.

- Eliminar un filtro.

  Haga clic en Eliminar ( ) para eliminar un filtro.

  - **Global filters**: se encuentra en el panel Filtros globales.
  - **Local filters**: haga clic en Filtro ( ) para mostrar el diálogo Set Local Filters y luego seleccione el filtro y quítelo.

- Borrar todos los filtros.

  - Haga clic en **Global filters Clear All Clear all (Borrar todo)** para borrar todos los filtros globales.
  - **Local filters**: seleccione un widget y haga clic en Filter ( ). Haga clic en **Clear All Clear all (Borrar todo)** en el widget Set Local Filters.

- Invalidar filtros.

  Seleccione un atributo y haga clic en Negar ( ) un filtro.

  - **Global filters**: se encuentra en el panel Filtros globales.

© 2020 Palo Alto Networks, Inc.

- **Local filters**: haga clic en Filtro ( ) para mostrar el diálogo Set Local Filters, añada un filtro y luego niéguelo.

- Ver filtros en uso.
  - **Global filters**: el número de filtros globales aplicado se muestra en el panel izquierdo, debajo de Global Filters.
  - **Local filters**: el número de filtros locales aplicado en un widget se muestra junto al nombre del widget. Para ver los filtros, haga clic en **Set Local Filters**.

© 2020 Palo Alto Networks, Inc.

Monitor (Supervisar)

Los siguientes temas describen los informes y logs del cortafuegos que puede utilizar para supervisar la actividad en su red:

- Supervisar > Logs
- Supervisar > Logs externos
- Supervisar > Motor de correlación automatizada
- Monitor > Packet Capture
- Supervisar > Appscope
- Monitor > Session Browser
- Supervisar > Lista de direcciones IP a bloquear
- Monitor > Botnet
- Supervisar > Informes en PDF
- Monitor > Manage Custom Reports
- Monitor > Reports

© 2020 Palo Alto Networks, Inc.

Supervisar > Logs

Los siguientes temas proporcionan información adicional acerca de los logs de supervisión.

¿Qué desea saber?	Consulte:
Quiero saber sobre los diferentes tipos de logs.	Tipos de log
Filtrar logs. Exportar logs. Ver los detalles de las entradas de log individuales. Modificar la visualización del log.	Acciones de log
¿Busca más información?	Supervisar y gestionar logs.

Tipos de log

- **Monitor (Supervisar)** > **Logs (Logs)**

El cortafuegos muestra todos los logs por lo que se respetan los permisos de administración basado en función. Solo se incluye la información para la que tiene permiso de visualización, lo cual varía según los tipos de logs que está visualizando. Para obtener información acerca de los permisos de administrador, consulte Device (Dispositivo) > Admin Roles (Funciones de administrador).

Tipo de log	Description (Descripción)
Tráfico	Muestra una entrada para el inicio y el final de cada sesión. Todas las entradas incluyen la fecha y la hora, las zonas de origen y destino, las direcciones y los puertos, el nombre de la aplicación, el nombre de la regla de seguridad aplicada al flujo, la acción de la regla (**allow (permitir)**, **deny (denegar)** o **drop (descartar)**), la interfaz de entrada y salida, el número de bytes y la razón para finalizar la sesión. La columna Type (Tipo) indica si la entrada es para el inicio o el final de la sesión o si se ha denegado o descartado la sesión. Una “asignación” indica que la regla de seguridad que ha bloqueado el tráfico ha especificado una aplicación “cualquiera”, mientras que “denegación” indica que la regla ha identificado una aplicación específica. Si se asigna el tráfico antes de identificar la aplicación, como cuando una regla asigna todo el tráfico a un servicio específico, la aplicación aparece como “no aplicable”. Explore los logs de tráfico para obtener más detalles sobre las entradas y artefactos individuales.

© 2020 Palo Alto Networks, Inc.

Tipo de log	Description (Descripción)
	• Haga clic en Detalles ( ) junto a una entrada para ver detalles adicionales acerca de la sesión, por ejemplo, si una entrada ICMP agrega varias sesiones entre el mismo origen y destino (el valor **Recuento** será superior a uno). • En un cortafuegos con una licencia activa de AutoFocus™, pase el cursor del ratón junto a una dirección IP, un nombre de archivo, una URL, un agente de usuario, un nombre de amenaza o un hash de una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en Resumen de inteligencia de AutoFocus.
threat	Muestra una entrada para cada alarma de seguridad generada por el cortafuegos. Cada entrada incluye la fecha y hora, un nombre de amenaza o URL, las zonas de origen y destino, direcciones, puertos, el nombre de la aplicación, el nombre de la regla de seguridad aplicada al flujo y la acción de alarma (**allow [permitir]** o **block [bloquear]**), y la gravedad. La columna Type (Tipo) indica el tipo de amenaza, por ejemplo, "virus" o "spyware". La columna Name (Nombre) es una URL o la descripción de la amenaza, y la columna Category es la categoría de amenaza (por ejemplo, "keylogger") o categoría de URL. Explore los logs de amenazas para obtener más detalles sobre las entradas y artefactos individuales. • Haga clic en Detalles ( ) para ver detalles adicionales acerca de la amenaza, por ejemplo, si la entrada agrega varias amenazas del mismo tipo entre el mismo origen y destino (el valor **Recuento** será superior a uno). • En un cortafuegos con una licencia activa de AutoFocus, pase el cursor del ratón junto a una dirección IP, un nombre de archivo, una URL, un agente de usuario, un nombre de amenaza o un hash de una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en Resumen de inteligencia de AutoFocus. • Si las capturas de paquetes locales están activadas, haga clic en Descargar ( ) para acceder a los paquetes capturados. Para activar las capturas de paquetes locales, consulte las subdivisiones en **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)**. • Para ver más detalles sobre una amenaza o para configurar rápidamente las exenciones directamente desde los logs de amenazas, haga clic en el nombre de una amenaza en la columna **Name (Nombre)**. La lista Exempt Profiles (Perfiles de exención) muestra todos los perfiles de protección frente a antivirus, antispyware y vulnerabilidad personalizados. Para configurar una excepción de una firma de amenaza, seleccione la casilla de verificación situada a la izquierda del nombre del perfil de seguridad y guarde el cambio. Para añadir excepciones de direcciones IP (hasta 100 direcciones IP por firma), resalte

© 2020 Palo Alto Networks, Inc.

Tipo de log	Description (Descripción)
	el perfil de seguridad, añada las direcciones IP en la sección Exempt IP Addresses (Direcciones IP de exención) y haga clic en **OK (Aceptar)** para guardarlas. Para ver o modificar la excepción, vaya al perfil de seguridad asociado y haga clic en la pestaña **Exceptions (Excepciones)**. Por ejemplo, si el tipo de amenaza es una vulnerabilidad, seleccione **Objetos** > **Perfiles de seguridad** > **Protección frente a vulnerabilidades**, haga clic en el perfil asociado y, a continuación, haga clic en la pestaña **Excepciones**.
Filtrado de URLs	Muestra logs de los filtros de URL, que controlan el acceso a los sitios web y que los usuarios puedan enviar credenciales a sitios web. Seleccione Objects > Security Profiles > URL Filtering para definir la configuración de filtrado de URL, incluidas las categorías de URL que se van a bloquear o permitir y a las que desea conceder o retirar el envío de credenciales. También puede activar la creación de logs de las opciones de encabezados HTTP para la URL. En un cortafuegos con una licencia activa de AutoFocus, pase el cursor del ratón junto a una dirección IP, un nombre de archivo, una URL, un agente de usuario, un nombre de amenaza o un hash de una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en Resumen de inteligencia de AutoFocus.
Envíos a WildFire	Muestra los logs de los archivos y los enlaces de correo electrónico que el cortafuegos envió para el análisis de WildFire™. La nube de WildFire analiza la muestra y devuelve los resultados del análisis, que incluyen el veredicto de WildFire asignado a la muestra: benigno, malware, grayware o phishing. En la columna Action (Acción) puede confirmar si el cortafuegos ha permitido o bloqueado un archivo basado en reglas de la política de seguridad. En un cortafuegos con una licencia activa de AutoFocus, pase el cursor del ratón junto a una dirección IP, nombre de archivo, URL, agente de usuario, nombre de amenaza o hash (en la columna Resumen de archivo) incluido en una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en Resumen de inteligencia de AutoFocus.
Data Filtering	Muestra los logs de las políticas de seguridad con perfiles de filtrado de datos adjuntos, para ayudar a evitar que la información confidencial, como números de tarjeta de crédito o seguro social, salga del área protegida por el cortafuegos, y perfiles de bloqueo de archivos, que evitan que determinados tipos de archivos se carguen o descarguen. Para configurar la protección de contraseña para el acceso a detalles de una entrada de log, haga clic en . Introduzca la contraseña y haga clic en **OK (Aceptar)**. Consulte en Device > Response Pages las instrucciones acerca de cómo cambiar o eliminar la contraseña de protección de datos.

© 2020 Palo Alto Networks, Inc.

Tipo de log	Description (Descripción)
	El sistema le solicitará introducir la contraseña solo una vez por sesión.
Coincidencia HIP	Muestra todas las coincidencias HIP que ha identificado la puerta de enlace de GlobalProtect™ al comparar los datos HIP sin procesar que ha suministrado el agente en comparación con los objetos y los perfiles HIP. A diferencia de otros logs, se registra una coincidencia HIP incluso cuando no coincide con una política de seguridad. Para obtener más información, consulte Network > GlobalProtect > Portals.
GlobalProtect	Muestra los logs de conexión de GlobalProtect. Utilice esta información para identificar a sus usuarios de GlobalProtect y su versión de SO cliente, solucionar problemas de conexión y rendimiento e identificar el portal y las puertas de enlace a las que se conectan los usuarios.
Etiqueta IP	Muestra información sobre cómo y cuándo se aplicó una etiqueta a una dirección IP particular. Utilice esta información para determinar cuándo y por qué una dirección IP particular se colocó en un grupo de direcciones y qué reglas de política afectan a dicha dirección. El log incluye el momento de la recepción (la fecha y hora en que llegó el primer y último paquete de la sesión), el sistema virtual, la dirección IP de origen, la etiqueta, el evento, el tiempo de espera, el nombre de origen y el tipo de origen.
User-ID™	Muestra información sobre las asignaciones de dirección IP a nombres de usuario, por ejemplo, cuál es el origen de la información de asignación, cuándo realizó el agente de User-ID la asignación y cuánto tiempo queda para que venzan las asignaciones. Puede utilizar esta información para ayudar a solucionar problemas de User-ID. Por ejemplo, si el cortafuegos está aplicando la regla de política incorrecta 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.
GTP	Muestra los logs basados en eventos que incluyen información sobre la amplia gama de atributos de GTP. Estos incluyen GTP event type (Tipo de evento de GTP), GTP event message type (Tipo de mensaje de evento GTP), APN, IMSI, IMEI y End User IP address (Dirección IP de usuario final), además de la información de TCP/IP que el cortafuegos de nueva generación identifica como la dirección de aplicación, origen y destino, y la marca de tiempo.
Inspección de túnel	Muestra una entrada para el inicio y el final de cada sesión de túnel inspeccionado. El log incluye Receive Time (fecha y hora en que llegó el primero y el último paquete de la sesión), Tunnel ID (ID de túnel), Monitor Tag (Etiqueta de supervisión), Session ID (ID de sesión), la regla de seguridad aplicada al tráfico del túnel, etc. Consulte Policies > Tunnel Inspection para obtener más información.

© 2020 Palo Alto Networks, Inc.

Tipo de log	Description (Descripción)
SCTP	Muestra eventos de SCTP y asociaciones basadas en los logs generados por el cortafuegos mientras realiza inspección por estados, validación de protocolo y filtrado de tráfico SCTP. Los logs de SCTP incluyen información sobre una amplia gama de SCTP y los atributos de su protocolo de carga, como el tipo de evento de SCTP, el tipo de fragmento, el código de causa de SCTP, la ID de aplicación de diámetro, el código de comando de diámetro, y los fragmentos. Esta información de SCTP se brinda además de la información general que el cortafuegos identifica, como la dirección de origen y de destino, el puerto de origen y de destino, la regla y la marca de tiempo. Consulte Objects (Objetos) > Security Profiles (Perfiles de seguridad) > GTP Protection (Protección de GTP) para obtener más información.
Configuración	Muestra una entrada para cada cambio de configuración. Cada entrada incluye la fecha y hora, el nombre de usuario del administrador, la dirección IP desde la cual se ha realizado el cambio, el tipo de cliente (interfaz web o CLI), el tipo de comando ejecutado, si el comando se ha ejecutado correctamente o ha fallado, la ruta de configuración y los valores anteriores y posteriores al cambio.
Sistema	Muestra una entrada para cada evento del sistema. Cada entrada incluye la fecha y hora, la gravedad del evento y una descripción del evento.
Alarmas	El log Alarmas registra información detallada sobre las alarmas que genera el sistema. La información de este log también se indica en Alarms. Consulte Definir la configuración de Alarm.
Autenticación	Muestra información sobre los eventos de autenticación que ocurren cuando los usuarios finales tratan de acceder a los recursos de red el acceso a los cuales está controlado mediante 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 reglas de autenticación para Log Authentication Timeouts. 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 permiten decidir mejor si debe ajustarlos y cómo hacerlo. *Los logs del sistema registran eventos de autenticación relacionados con GlobalProtect y el acceso de los administradores a la interfaz web.*

© 2020 Palo Alto Networks, Inc.

Tipo de log	Description (Descripción)
unified	Muestra las últimas entradas de logs de tráfico, amenazas, filtrado de URL, envíos de WildFire y filtrado de datos en una sola pantalla. La vista de logs colectivos le permite investigar y filtrar estos diferentes tipos de logs juntos (en lugar de buscar cada conjunto de logs por separado). También puede elegir qué tipos de logs desea ver: haga clic en la flecha situada a la izquierda del campo de filtros y seleccione **traffic (tráfico)**, **threat (amenaza)**, **url**, **data (datos)** o **wildfire** para ver solo los tipos de logs seleccionados. En un cortafuegos con una licencia activa de AutoFocus, pase el cursor del ratón junto a una dirección IP, un nombre de archivo, una URL, un agente de usuario, un nombre de amenaza o un hash de una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en Resumen de inteligencia de AutoFocus. El cortafuegos muestra todos los logs por lo que se respetan los permisos de administración basado en función. Cuando se muestran los logs unificados, solo se incluyen los logs para los cuales dispone de permisos. 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. Para obtener información acerca de los permisos de administrador, consulte Device > Admin Roles. *Puede utilizar el conjunto de logs Unified (Unificados) con el portal de inteligencia de amenazas de AutoFocus. Configure una búsqueda de AutoFocus para añadir filtros de búsqueda de AutoFocus directamente al campo de filtro de logs unificados.*

Acciones de log

La siguiente tabla describe las acciones de log.

Acción	Description (Descripción)

Filtrar logs	Cada página de log cuenta con un campo de filtro en la parte superior de la página. Puede añadir artefactos al campo, como direcciones IP o un intervalo de tiempo, para encontrar entradas de logs coincidentes. Los iconos situados a la derecha de cada campo le permite aplicar, borrar, crear, guardar y cargar filtros.
	
	• Crear un filtro:
	  • Haga clic en un artefacto en una entrada de log para añadir ese artefacto al filtro.
	  • Haga clic en **Add (Añadir)** ( ) para definir los nuevos criterios de búsqueda. Para cada criterio, seleccione el **Connector (Conector)** que define el tipo de búsqueda (**and [y]** u **or [o]**), el **Attribute (Atributo)** en el que basar la búsqueda, un **Operator (Operador)** para definir el ámbito de la búsqueda y un **Value (Valor)** que

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)
	contrastar con las entradas de log. Haga clic en **Add (Añadir)** para añadir cada criterio al campo de filtro y luego en **Close (Cerrar)** cuando finalice. Luego, puede aplicar ( ) el filtro. *Si la cadena Value (Valor) coincide con Operator (Operador) (como has o in), encierre la cadena entre comillas para evitar un error de sintaxis. Por ejemplo, si filtra por país de destino y usa* ***`IN`*** *como Value (Valor) de India, introduzca el filtro con el formato* ***`( dstloc eq "IN" )`****.* *El filtro de logs* ***(receive_time in last-60-seconds)*** *provoca que el número de entradas de logs (y páginas de logs) mostrado aumente o disminuya con el tiempo.* • Aplicar filtros: haga clic en Apply Filter ( ) para mostrar las entradas de logs que coincidan con el filtro actual. • Borrar filtros: haga clic en Clear Filter ( ) para borrar el campo de filtro. • Guardar un filtro: haga clic en Save Filter ( ), introduzca un nombre para el filtro y haga clic en **OK (Aceptar)**. • Usar un filtro guardado: haga clic en Load Filter ( ) para añadir un filtro guardado al campo de filtro.
Exportación de logs	Haga clic en Export to CSV ( ) para exportar todos los logs que coinciden con el filtro actual en un informe con formato CSV y continúe con la descarga del archivo con **Download file (Descargar archivo)**. De manera predeterminada, el informe contiene hasta 2000 líneas de logs. Para cambiar el límite de línea de los informes CSV generados, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Logging and Reporting Settings (Configuración de log e informes)** > **Log Export and Reporting (Exportación e informes de logs)** e introduzca un nuevo valor en **Max Rows in CSV Export (Máx. de filas en exportación CSV)**.
Resaltar acciones de política	Seleccione esta opción para resaltar las entradas de log que coinciden con la acción. Los logs filtrados se resaltan en estos colores: • Verde: allow (permitir) • Amarillo: continue (continuar) u override (anular) • Rojo: deny (denegar), drop (descartar), drop-icmp (descartar icmp), rst-client (rst cliente), reset-server (restablecer servidor), reset-both (restablecer ambos), block-continue (bloquear y continuar), block-override (bloquear y anular), block-url (bloquear URL), drop-all (descartar todo), sinkhole

Cambiar la visualización de logs	Si desea personalizar la visualización de logs:
	• Cambie el intervalo de actualización automática; seleccione un intervalo del menú desplegable (**60 seconds (60seg.)**, **30 seconds (30 seg.)**, **10 seconds (10 seg.)**, or **Manual**).
	• Cambie el número y el orden de las entradas mostradas por página; las entradas de logs se brindan en bloques de 10 páginas.
	  • Utilice los controles de página en la parte inferior de la página para navegar por la lista de logs.
	  • Para cambiar el número de entradas de logs por página, seleccione el número de filas desde el menú desplegable por página (**20**, **30**, **40**, **50**, **75**, or **100**).

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)
	• Para ordenar los resultados de modo ascendente o descendente, use el menú desplegable **ASC** o **DESC**. • Resuelva direcciones IP en nombres de dominio: seleccione **Resolve Hostname (Resolver nombre de host)** para comenzar a resolver las direcciones IP externas en nombres de dominio. • Cambie el orden en el que los logs se muestran: seleccione **DESC** para mostrar logs en orden descendente empezando por las entradas de logs con la fecha de recepción más reciente. Seleccione **ASC** para mostrar los logs en orden ascendente empezado por las entradas de logs con la fecha de recepción más antiguo.
Ver detalles de entradas de log individuales	Para ver la información de las entradas de log individuales: • Para mostrar detalles adicionales, haga clic en Detalles ( ) de una entrada. Si el origen o el destino cuentan con una dirección IP para la asignación de nombre de usuario o dominio definidos en la página **Addresses (Direcciones)**, se presentará el nombre en lugar de la dirección IP. Para ver la dirección IP asociada, mueva su cursor sobre el nombre. • En un cortafuegos con una licencia activa de AutoFocus, pase el cursor del ratón junto a una dirección IP, un nombre de archivo, una URL, un agente de usuario, un nombre de amenaza o un hash de una entrada de log y haga clic en el menú desplegable ( ) para abrir el resumen de inteligencia de AutoFocus del artefacto en AutoFocus Intelligence Summary.

© 2020 Palo Alto Networks, Inc.

Supervisar > Logs externos

Utilice esta página para ver los logs ingeridos de Traps™ Endpoint Security Manager (ESM) en los recopiladores de logs gestionados por Panorama™. Para ver los logs de Traps ESM en Panorama:

- En Traps ESM Server, configure Panorama como un servidor syslog y configure los eventos de log para que se reenvíen a Panorama. Los eventos pueden incluir eventos de seguridad, cambios de política, cambios del estado del agente y ESM Server, y cambios en los ajustes de la configuración.
- En un dispositivo Panorama que se implementa en modo Panorama con uno o más recopiladores de logs gestionados, configure un perfil de ingestión de logs (Panorama > Perfil de ingestión de logs) y adjunte el perfil a un grupo de recopiladores (Panorama > Grupos de recopiladores) en el que almacenar los logs de Traps ESM.

Los logs externos no se asocian a ningún grupo de dispositivos y solo se pueden ver al seleccionar **Device Group (Grupo de dispositivos)**: **All (Todos)** porque los logs no se reenvían desde los cortafuegos.

Tipo de log	Description (Descripción)
Monitor (Supervisar) > **External Logs (Logs externos)** > **Traps ESM** > **Threat (Amenaza)**	Estos eventos de amenaza incluyen todos los eventos de prevención, notificación, provisionales y posteriores a la detección de los que los agentes Traps informan.
Monitor (Supervisar) > **External Logs (Logs externos)** > **Traps ESM** > **Sysem (Sistema)**	Los eventos de sistema de ESM Server incluyen cambios relacionados con el estado de ESM, licencias, archivos de soporte técnico de ESM y comunicación con WildFire.
Monitor (Supervisar) > **External Logs (Logs externos)** > **Traps ESM** > **Policy (Política)**	Los eventos de cambio de política incluyen cambios en reglas, niveles de protección, actualizaciones de contenido, logs de control de hash y veredictos.
Monitor (Supervisar) > **External Logs (Logs externos)** > **Traps ESM** > **Agent (Agente)**	Los eventos de cambio de agente ocurren en el endpoint e incluyen cambios a las actualizaciones de contenido, licencias, software, estado de conexión, reglas de acción de una sola vez, procesos y servicios, y archivos en cuarentena.
Monitor (Supervisar) > **External Logs (Logs externos)** > **Traps ESM** > **Config (Config.)**	Los eventos de cambio de configuración de ESM incluyen cambios generales a licencias, usuarios administrativos y funciones, procesos, configuración de restricción y condiciones.

Panorama puede correlacionar eventos de seguridad discretos en los endpoints con eventos en la red para rastrear cualquier actividad sospechosa o malintencionada entre los endpoints y el cortafuegos. Para ver los eventos correlacionados que Panorama identifica, consulte Monitor > Automated Correlation Engine > Correlated Events.

© 2020 Palo Alto Networks, Inc.

Supervisar > Motor de correlación automatizada

El motor de correlación automatizada realiza un seguimiento de los patrones de su red y correlaciona eventos que indican un aumento de los comportamientos o eventos sospechosos que se convierten en actividad malintencionada. El motor funciona como su analista de seguridad personal, que escudriña eventos aislados en los diferentes conjuntos de logs en el cortafuegos, solicita los datos de patrones específicos y analiza la información obtenida para que pueda disponer de información procesable.

El motor de correlación usa objetos de correlación que generan eventos correlacionados. Los eventos correlacionados cotejan las pruebas para ayudarle a llevar un seguimiento de eventos comunes entre eventos de red no relacionados a primera vista; además, le permite centrarse en la respuesta a incidentes.

Los siguientes modelos admiten el motor de correlación automatizado:

- Panorama: dispositivos M-Series y dispositivos virtuales.
- Cortafuegos de PA-3200 Series
- Solo cortafuegos PA-5200 Series
- Cortafuegos PA-7000 Series

¿Qué desea saber?	Consulte:
¿Qué son los objetos de correlación?	Monitor > Automated Correlation Engine > Correlation Objects
¿Qué es un evento correlacionado? ¿Dónde puedo ver una prueba de coincidencia para una coincidencia de correlación?	Monitor > Automated Correlation Engine > Correlated Events
¿Cómo puedo ver una vista gráfica de coincidencias de correlación?	Consulte información sobre el widget Compromised Hosts (Hosts en riesgo) en ACC.
¿Busca más información?	Use el motor de correlación automatizada.

Monitor > Automated Correlation Engine > Correlation Objects

Para contrarrestar los avances en los métodos de explotación y distribución de malware, los objetos de correlación amplían las funciones de detección de malware basadas en firmas en el cortafuegos. Ofrecen la inteligencia para identificar patrones de comportamiento sospechosos en diferentes conjuntos de logs y recopilan las pruebas necesarias para investigar y dar respuestas rápidas a los eventos.

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 orígenes de datos y a cada patrón se le asigna un nivel de gravedad y un umbral, que es el número de veces que se produce una coincidencia con el patrón dentro de un límite de tiempo definido. Cuando se produce una coincidencia con un patrón, se registra un evento de correlación.

© 2020 Palo Alto Networks, Inc.

Los orígenes de datos usados para realizar las búsquedas pueden incluir los siguientes logs: estadísticas de aplicación, tráfico, resumen de tráfico, resumen de amenazas, amenazas, filtrado de datos y filtrado de URL. Por ejemplo, la definición de un objeto de correlación puede incluir un conjunto de patrones que consulta los logs en busca de pruebas de hosts infectados, patrones de malware, movimiento lateral del malware en el tráfico, filtrado de URL y logs de amenazas.

Palo Alto Networks® define los objetos de correlación, que se incluyen en las actualizaciones de contenido. Debe contar con una licencia de prevención de amenazas para obtener actualizaciones de contenido.

Todos los objetos de correlación están habilitados de forma predeterminada. Para deshabilitar un objeto, selecciónelo y haga clic en **Disable**.

Campos de objetos de correlación	Description (Descripción)
Nombre y título	La etiqueta indica el tipo de actividad que detecta el objeto de correlación.
ID	Un número exclusivo que identifica el objeto de correlación. Este número pertenece a la serie 6000.
Category	Resumen del tipo de amenaza o riesgo para la red, usuario o host.
Estatal o regional	Indica si el objeto de correlación está habilitado (activo) o deshabilitado (inactivo).
Description (Descripción)	Especifica las condiciones de coincidencia con las que el cortafuegos o Panorama analizará los logs. Describe el patrón de aumento o ruta de progresión que se usará para identificar la actividad malintencionada o el comportamiento sospechoso del host.

Monitor > Automated Correlation Engine > Correlated Events

Los eventos correlacionados amplían las funciones de detección de amenazas en el cortafuegos y Panorama; los eventos correlacionados recopilan pruebas o sospechas de comportamiento inusual en los hosts en la red.

El objeto de correlación permite pivotar en ciertas condiciones o comportamientos y seguir la pista de eventos comunes en múltiples orígenes de logs. Cuando se observa un conjunto de condiciones especificadas en un objeto de correlación en la red, cada coincidencia se registra como un evento correlacionado.

El evento correlacionado incluye los detalles enumerados en la siguiente tabla.

Campo	Description (Descripción)
Hora de coincidencias	La hora a la que el objeto de correlación activó una coincidencia.
Hora de actualización	La marca de tiempo a la que se actualizó la última coincidencia.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Nombre de objeto	El nombre del objeto de correlación que activó la coincidencia.
Dirección de origen	La dirección IP del usuario desde el que se originó el tráfico.
Source User (Usuario de origen)	La información del usuario y el grupo de usuario del servidor de directorios si se habilita el User-ID™.
Gravedad	Una escala que clasifica el riesgo en función del alcance de los daños.
Resumen	Una descripción que resume las pruebas recopiladas en el evento correlacionado.

Para visualizar el log detallado, haga clic en Details ( ) en una entrada. Este log detallado incluye todas las pruebas de una coincidencia:

Pestaña	Description (Descripción)
Información de coincidencias	**Object Details**: Presenta la información del objeto de correlación que activó la coincidencia. Para obtener información sobre los objetos de correlación, consulte Monitor > Automated Correlation Engine > Correlation Objects.
	Match Details: 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	Esta pestaña incluye todas las pruebas que corroboran el evento correlacionado. Enumera la información detallada en las pruebas recopiladas de cada sesión.

Consulte una vista gráfica de la información en la pestaña **Correlated Events (Eventos correlacionados)**; consulte el widget Compromised Hosts (Hosts en riesgo) en la pestaña **ACC** > **Threat Activity (Actividad de amenazas)**. En el widget Compromised Hosts, la vista se compone de usuarios y direcciones IP de origen ordenados por nivel de gravedad.

Para configurar notificaciones cuando se registra un evento correlacionado, vaya a las pestañas **Device (Dispositivo)** > **Log Settings (Configuración de log)** o **Panorama** > **Log Settings (Configuración de log)**.

© 2020 Palo Alto Networks, Inc.

Monitor > Packet Capture

Todos los cortafuegos de Palo Alto Networks tienen integrada una función de captura de paquetes (pcap) que puede utilizar para capturar paquetes que atraviesen las interfaces de red del cortafuegos. A continuación, puede utilizar los datos capturados para solucionar problemas o para crear firmas de aplicaciones personalizadas.

La función de captura de paquetes hace un uso intensivo de la CPU y puede reducir el rendimiento del cortafuegos. Utilice esta función únicamente cuando sea necesario y asegúrese de desactivarla cuando haya recopilado los paquetes necesarios.

¿Qué desea saber?	Consulte:
¿Cuáles son los diferentes métodos que puede utilizar el cortafuegos para capturar paquetes?	Descripción general de captura de paquetes
¿Cómo puedo generar una captura de paquetes personalizada?	Componentes de una captura de paquetes personalizada
¿Cómo puedo generar capturas de paquetes cuando el cortafuegos detecte una amenaza?	Habilitación de captura de paquetes de amenazas
¿Dónde puedo descargar una captura de paquetes?	Descripción general de captura de paquetes
¿Busca más información?	
• Activar la captura de paquetes extendida para perfiles de seguridad.	Device > Setup > Content-ID
• Utilizar capturas de paquetes para escribir firmas de aplicaciones personalizadas.	Consulte Firmas personalizadas.
• Impedir que un administrador de cortafuegos visualice capturas de paquetes.	Defina el acceso de administrador a la interfaz web.
• Vea un ejemplo.	Consulte Realización de capturas de paquetes (en inglés).

Descripción general de captura de paquetes

Puede configurar un cortafuegos de Palo Alto Networks para que realice una captura de paquetes personalizada o una captura de paquetes de amenazas.

- **Custom Packet Capture (Captura de paquetes personalizada)**: capture paquetes para todo el tráfico o el tráfico basado en los filtros que defina. Por ejemplo, puede configurar el cortafuegos para que

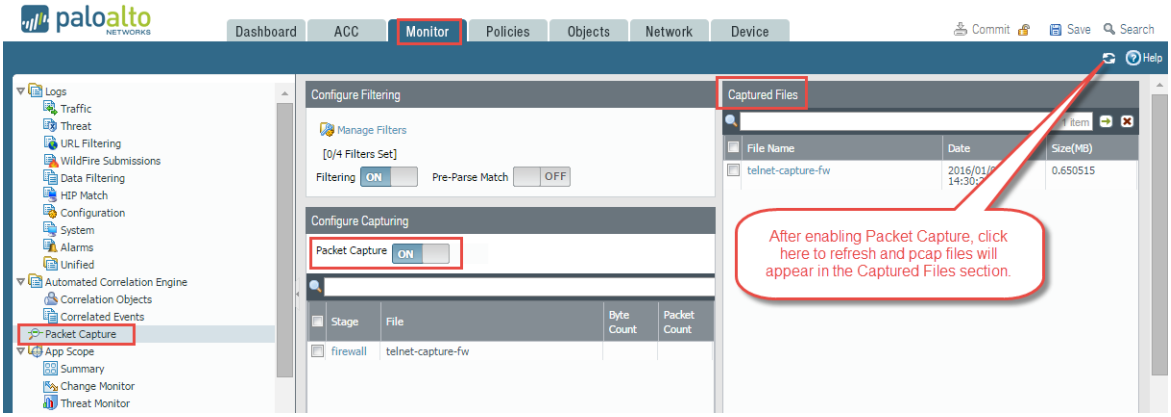
© 2020 Palo Alto Networks, Inc.

solamente capture paquetes hacia y desde una dirección IP o un puerto de origen y destino específicos. Utilice estas capturas de paquetes para solucionar problemas relacionados con el tráfico de red o para recopilar atributos de aplicación con el fin de escribir firmas de aplicaciones personalizadas (**Monitor [Supervisar]** > **Packet Capture [Captura de paquetes]**). Defina el nombre de archivo en función de la etapa (Descartar, Cortafuegos, Recepción o Transmisión) y, cuando la PCAP haya finalizado, descargue PCAP en la sección Captured Files (Archivos capturados).

- **Threat Packet Capture (Captura de paquetes de amenazas)**: capture paquetes cuando el cortafuegos detecte un virus, spyware o una vulnerabilidad. Puede habilitar esta función en los perfiles de seguridad Antivirus, Antispyware y Protección de vulnerabilidades. 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. La acción para la amenaza debe establecerse como permitir o alertar; de lo contrario, la amenaza se bloqueará y no se podrán capturar los paquetes. Puede configurar este tipo de captura de paquetes en **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)**. Para descargar ( ) pcap, seleccione **Monitor (Supervisar)** > **Threat (Amenaza)**.

Componentes de una captura de paquetes personalizada

La tabla siguiente describe los componentes de la página **Monitor (Supervisar)** > **Packet Capture (Captura de paquetes)** que se utiliza para configurar capturas de paquetes, habilitar la captura de paquetes y descargar archivos de captura de paquetes.



Componentes de captura de paquetes personalizada	Configurado en	Description (Descripción)
Gestionar filtros	Configurar filtrado	Cuando habilite capturas de paquetes personalizadas, debería definir filtros de modo que solamente se capturen los paquetes que coincidan con los filtros. Esto facilitará la localización de la información que necesita en las pcaps y reducirá la potencia de procesamiento que necesitará el cortafuegos para realizar la captura de paquetes. Haga clic en **Add (Añadir)** para añadir un nuevo filtro y configurar los campos siguientes: • **Id**: introduzca o seleccione un identificador para el filtro.

© 2020 Palo Alto Networks, Inc.

Componentes de captura de paquetes personalizada	Configurado en	Description (Descripción)
		• **Ingress Interface (Interfaz de entrada)**: seleccione la interfaz de entrada en la que quiera capturar el tráfico. • **Source (Origen)**: especifique la dirección IP de origen del tráfico que quiera capturar. • **Destination (Destino)**: especifique la dirección IP de destino del tráfico que quiera capturar. • **Src Port (Puerto orig.)**: especifique el puerto de origen del tráfico que quiera capturar. • **Dest Port (Puerto dest.)**: especifique el puerto de destino del tráfico que quiera capturar. • **Proto**: especifique el número de protocolo que desee filtrar (1-255). Por ejemplo, ICMP es el número de protocolo 1. • **Non-IP (no IP)**: seleccione cómo tratar el tráfico no IP (excluir todo el tráfico IP, incluir todo el tráfico IP, incluir solo tráfico IP o no incluir un filtro de IP). La difusión y AppleTalk son ejemplos de tráfico no IP. • **IPv6**: seleccione esta opción para incluir paquetes de IPv6 en el filtro.
Filtrado	Configurar filtrado	Tras definir los filtros, configure **Filtering (Filtrado)** como **ON (Activado)**. Si el filtrado está como **OFF (Desactivado)**, se capturará todo el tráfico.
Anterior a la coincidencia	Configurar filtrado	Esta opción se utiliza para la resolución de problemas avanzada. Cuando un paquete se introduce en el puerto de entrada, se llevan a cabo varios pasos de procesamiento antes de analizarlo en busca de coincidencias frente a filtros preconfigurados. Es posible que un paquete, debido a un fallo, no alcance la etapa de filtrado. Eso puede ocurrir, por ejemplo, si falla una búsqueda de ruta. Establezca el ajuste **Pre-Parse Match (Anterior a la coincidencia)** como **ON (Activado)** para emular una coincidencia positiva de cada paquete que entre en el sistema. Eso permite que el cortafuegos capture paquetes que no alcancen el proceso de filtrado. Si un paquete puede alcanzar la etapa de filtrado, se procesará de acuerdo con la configuración del filtro y se descartará si no consigue cumplir los criterios de filtrado.
Captura de paquetes	Configurar captura	Haga clic en el conmutador de alternancia para cambiar el estado de la captura de paquetes de **ON (Activado)** a **OFF (Desactivado)** o viceversa.

© 2020 Palo Alto Networks, Inc.

Componentes de captura de paquetes personalizada	Configurado en	Description (Descripción)

		Debe seleccionar al menos una etapa de captura. Haga clic en **Add (Añadir)** y especifique la siguiente información:
		• **Stage (Etapa)**: indique el punto en el que capturar paquetes:
		  • **drop (descartar)**: cuando el procesamiento de paquetes encuentra un error y el paquete se descarta.
		  • **firewall (cortafuegos)**: cuando el paquete tiene una coincidencia de sesión o se crea un primer paquete con una sesión correctamente.
		  • **receive (recibir)**: cuando se recibe el paquete en el procesador de plano de datos
		  • **transmit (transmitir)**: cuando se transmite el paquete en el procesador de plano de datos.
		• **File (Archivo)**: especifica el nombre del archivo de captura. El nombre del archivo debe comenzar por una letra y puede incluir letras, dígitos, puntos, guiones bajos o guiones.
		• **Packet Count (Recuento de paquetes)**: especifica el número máximo de paquetes a partir del cual se detiene la captura.
		• **Byte Count (Recuento de bytes)**: especifica el número máximo de bytes a partir del cual se detiene la captura.

Archivos capturados	Archivos capturados	Contiene una lista de capturas de paquetes personalizadas generadas previamente por el cortafuegos. Haga clic en un archivo para descargarlo en su ordenador. Para eliminar una captura de paquetes, seleccione la captura de paquetes y luego **Delete (Eliminar)**. • **File Name (Nombre de archivo)**: Enumera los archivos de capturas de paquetes. Los nombres de archivos se basan en el nombre de archivo que especifique para la etapa de captura. • **Date (Fecha)**: Fecha en la que se generó el archivo. • **Size (MB) ([Tamaño (MB)]**: Tamaño del archivo de captura. Después de activar la captura de paquetes y desactivarla a continuación, debe hacer clic en Refresh (Actualizar) ( ) para ver los nuevos archivos de pcap en esta lista.
Borrar toda la configuración	Configuración	Haga clic en **Clear All Settings (Borrar toda la configuración)** para desactivar la captura de paquetes y borrar todos los ajustes de capturas de paquetes.

© 2020 Palo Alto Networks, Inc.

Componentes de captura de paquetes personalizada	Configurado en	Description (Descripción)
		Esto no desactiva la captura de paquetes establecida en un perfil de seguridad. Para obtener información sobre cómo habilitar la captura de paquetes en un perfil de seguridad, consulte Habilitación de captura de paquetes de amenazas*.*

Habilitación de captura de paquetes de amenazas

- Objetos > Perfiles de seguridad

Para habilitar el cortafuegos para que capture paquetes cuando detecte una amenaza, habilite la opción de captura de paquetes en el perfil de seguridad.

En primer lugar, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** y, a continuación, modifique el perfil que desee como se describe en la tabla siguiente:

Opciones de captura de paquetes en perfiles de seguridad	Ubicación
Antivirus	Seleccione un perfil de antivirus personalizado y, en la pestaña **Antivirus**, seleccione **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 paquetes)**, seleccione **single-packet (paquete único)** o **extended-capture (captura extendida)**.
Protección contra vulnerabilidades	Seleccione un perfil de protección de vulnerabilidades personalizado y, en la pestaña **Rules (Reglas)**, haga clic en **Add (Añadir)** para añadir una nueva regla o seleccionar una regla existente. A continuación, seleccione la lista desplegable **Packet Capture (Captura de paquetes)** y seleccione **single-packet (paquete único)** o **extended-capture (captura extendida)**.

En los perfiles de antispyware y de protección de vulnerabilidades, también puede habilitar la captura de paquetes en excepciones. Haga clic en la pestaña Exceptions (Excepciones) y en la columna Captura de paquetes de una firma, haga clic en la lista desplegable y seleccione single-packet (paquete único) o extended-capture (captura extendida).

(Opcional) Para definir la longitud de una captura de paquetes de amenazas en función del número de paquetes capturados (que se basa en un ajuste global), seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** y, en la sección Content-ID™ Settings (Configuración de Content-ID™), modifique **Extended Packet Capture Length (packets field) (Longitud de captura de paquetes extendida [paquetes])** (el intervalo es de 1 a 50, el valor predeterminado es 5).

© 2020 Palo Alto Networks, Inc.

Tras habilitar la captura de paquetes en un perfil de seguridad, debe verificar que el perfil forme parte de una regla de seguridad. Para obtener información sobre cómo añadir un perfil de seguridad a una regla de seguridad, consulte Descripción general de política de seguridad.

Cada vez que el cortafuegos detecta una amenaza y la captura de paquetes está habilitada en el perfil de seguridad, puede descargar ( ) o exportar el paquete con la captura.

© 2020 Palo Alto Networks, Inc.

Supervisar > Appscope

Los siguientes apartados describen las funciones de Appscope

- Descripción general de Appscope
- Informe de resumen de Appscope
- Informe del supervisor de cambios de Appscope
- Informe del supervisor de amenazas de Appscope
- Informe de mapa de amenazas de Appscope
- Informe del supervisor de red de Appscope
- Informe del mapa de tráfico de Appscope

Descripción general de Appscope

Los informes de Appscope proporcionan visibilidad gráfica en los siguientes aspectos de la red:

- Cambios en el uso de la aplicación y la actividad del usuario
- Los usuarios y las aplicaciones que absorben la mayor parte del ancho de banda de la red
- Amenazas de red

Con los informes de Appscope, puede ver rápidamente si se produce algún comportamiento inusual o inesperado y que la detección de cualquier comportamiento problemático sea más sencilla; cada informe proporciona una ventana dinámica y personalizable por el usuario en la red. Los informes incluyen opciones para seleccionar los datos e intervalos para mostrar. En Panorama puede seleccionar también **Data Source (Origen de datos)** para la información que se muestra. El origen de datos predeterminado (en instalaciones nuevas de Panorama) usa la base de datos local de Panorama que almacena los logs enviados por los cortafuegos gestionados; en una actualización, el origen de datos predeterminado es **Remote Device Data (Datos de dispositivo remoto)** (datos de cortafuegos gestionados). Para recuperar y visualizar una vista agregada de los datos directamente desde los cortafuegos gestionados tendrá que cambiar el origen de **Panorama** a **Remote Device Data (Datos de dispositivo remoto)**.

Al pasar el ratón por encima y hacer clic en las líneas o barras de los gráficos, se pasa al ACC y se proporciona información detallada sobre la aplicación específica, la categoría de la aplicación, el usuario o el origen.

Gráficos del Centro de control de aplicaciones	Description (Descripción)
Resumen	Informe de resumen de Appscope
Supervisor de cambios	Informe del supervisor de cambios de Appscope
Supervisor de amenazas	Informe del supervisor de amenazas de Appscope
Mapa de amenazas	Informe de mapa de amenazas de Appscope
Supervisor de red	Informe del supervisor de red de Appscope
Mapa de tráfico	Informe del mapa de tráfico de Appscope

© 2020 Palo Alto Networks, Inc.

Informe de resumen de Appscope

El informe Resumen muestra gráficos de los cinco principales ganadores, perdedores, aplicaciones de consumo de ancho de banda, categorías de aplicación, usuarios y orígenes.

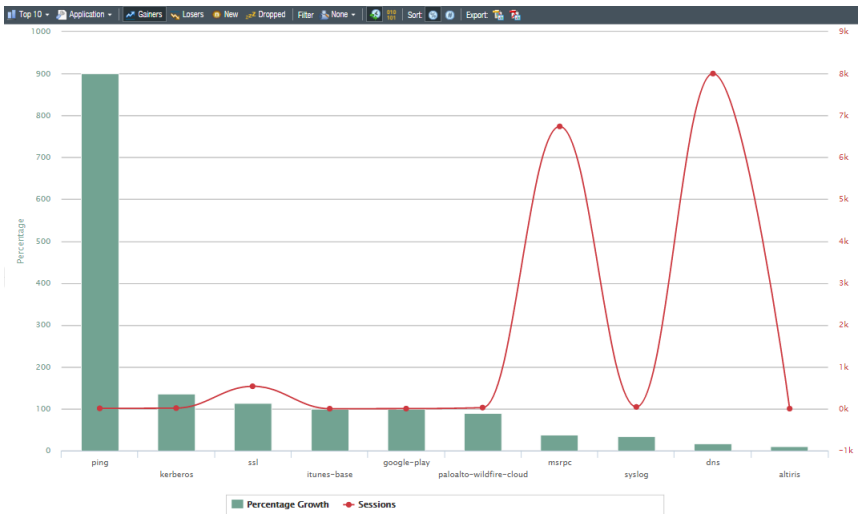
Para exportar los gráficos en el informe de resumen como un PDF, haga clic en **Export (Exportar)** (Export:). Cada gráfico se guarda como una página en el PDF creado.

Informe de resumen de Appscope

Informe del supervisor de cambios de Appscope

El informe del supervisor de cambios muestra cambios realizados en un período de tiempo específico. Por ejemplo, la figura a continuación 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.

Informe del supervisor de cambios de Appscope



Este informe contiene las siguientes opciones.

© 2020 Palo Alto Networks, Inc.

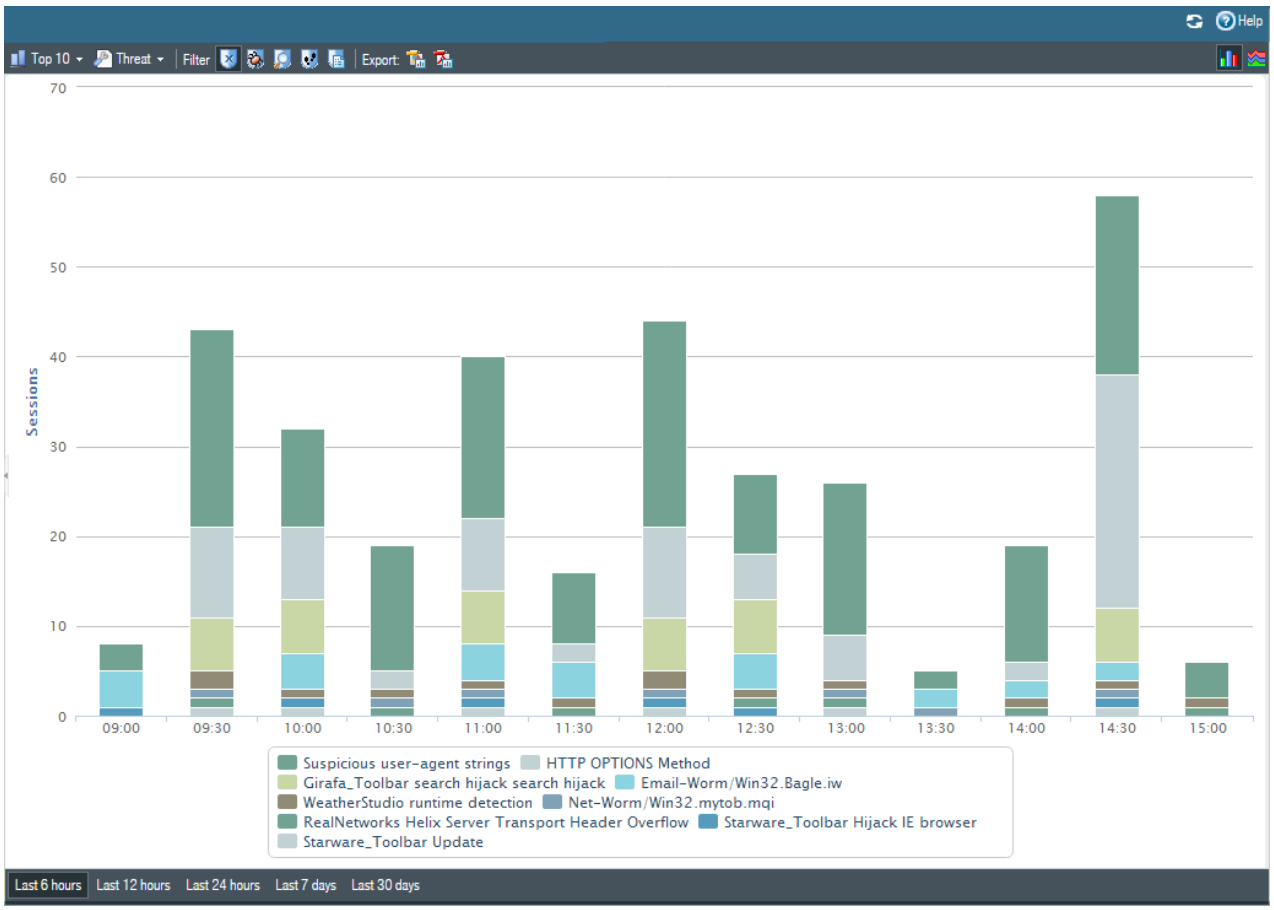
Opciones del informe del supervisor de cambios	Description (Descripción)
Barra superior	
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Application (Aplicación)	Determina el tipo de elemento indicado: Aplicación, Categoría de aplicación, Origen o Destino.
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 período de medición.
Descartado	Muestra mediciones de elementos que se han suspendido durante el período de medición.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el elemento seleccionado. None (Ninguno) muestra todas las entradas.
Contar sesiones y contar bytes	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.
Barra inferior	
Comparar (intervalo)	Especifica el periodo durante el que se realizaron las mediciones de cambio.

Informe del supervisor de amenazas de Appscope

El informe del supervisor de amenazas muestra un recuento de las principales amenazas durante el período de tiempo seleccionado. Por ejemplo, la figura a continuación muestra los 10 principales tipos de amenaza en las últimas 6 horas.

Informe del supervisor de amenazas de Appscope

© 2020 Palo Alto Networks, Inc.



Cada tipo de amenaza está indicado con colores como se indica en la leyenda debajo del gráfico. Este informe contiene las siguientes opciones.

Opciones del informe del supervisor de amenazas	Description (Descripción)
Barra superior	
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
threat	Determina el tipo de elemento medido: Amenaza, Categoría de amenaza, Origen o Destino.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el 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.
Barra inferior	

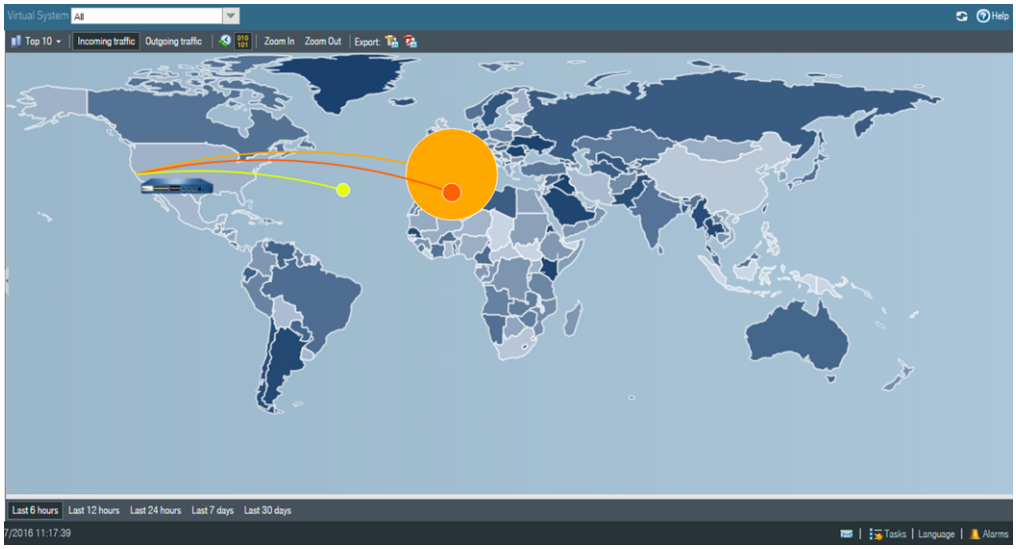
© 2020 Palo Alto Networks, Inc.

Opciones del informe del supervisor de amenazas	Description (Descripción)
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Especifica el periodo durante el que se realizaron las mediciones.

Informe de mapa de amenazas de Appscope

El informe del mapa de amenazas muestra una vista geográfica de amenazas, incluyendo la gravedad.

Informe de mapa de amenazas de Appscope



Cada tipo de amenaza está indicado con colores como se indica en la leyenda debajo del gráfico. Haga clic en un país del mapa para acercarse con **Zoom In (Acercar)** y luego alejarse con **Zoom Out (Alejar)** según sea necesario. Este informe contiene las siguientes opciones.

Opciones del informe del mapa de amenazas	Description (Descripción)
Barra superior	
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.
Filter (Filtro)	Aplica un filtro para mostrar únicamente el elemento seleccionado.
Acercar y alejar	Acerque y aleje el mapa.
Exportar	Exporta el gráfico como imagen .png o PDF.

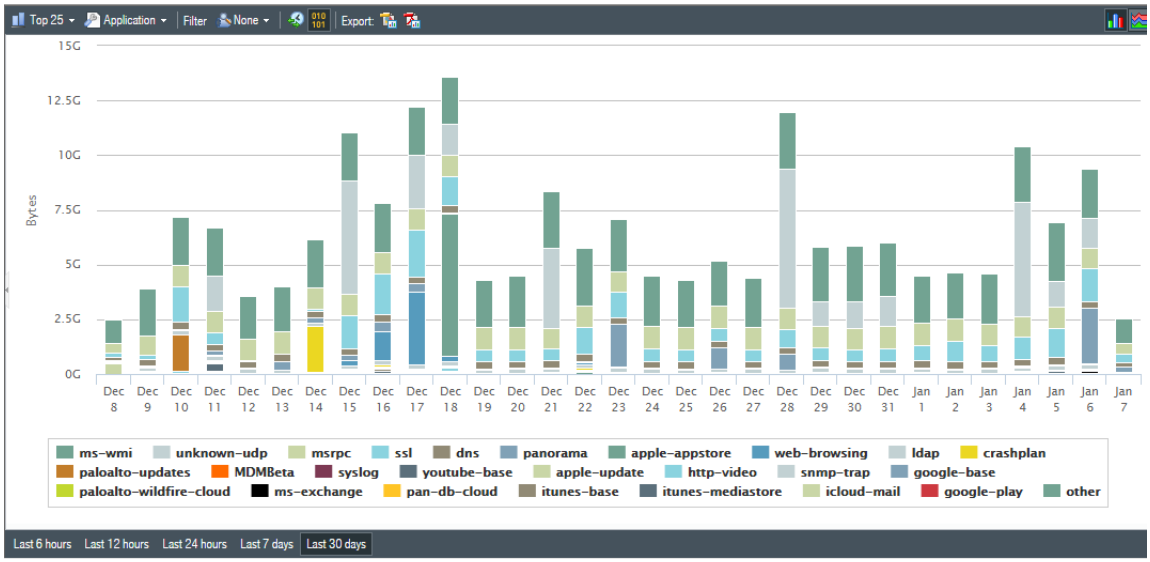
© 2020 Palo Alto Networks, Inc.

Opciones del informe del mapa de amenazas	Description (Descripción)
Barra inferior	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indica el periodo durante el que se realizaron las mediciones.

Informe del supervisor de red de Appscope

El informe del 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.

Informe del supervisor de red de Appscope



El informe contiene las siguientes opciones.

Opciones del informe del supervisor de red	Description (Descripción)
Barra superior	
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.
Contar sesiones y contar bytes	Determina si mostrar información de sesión o byte.

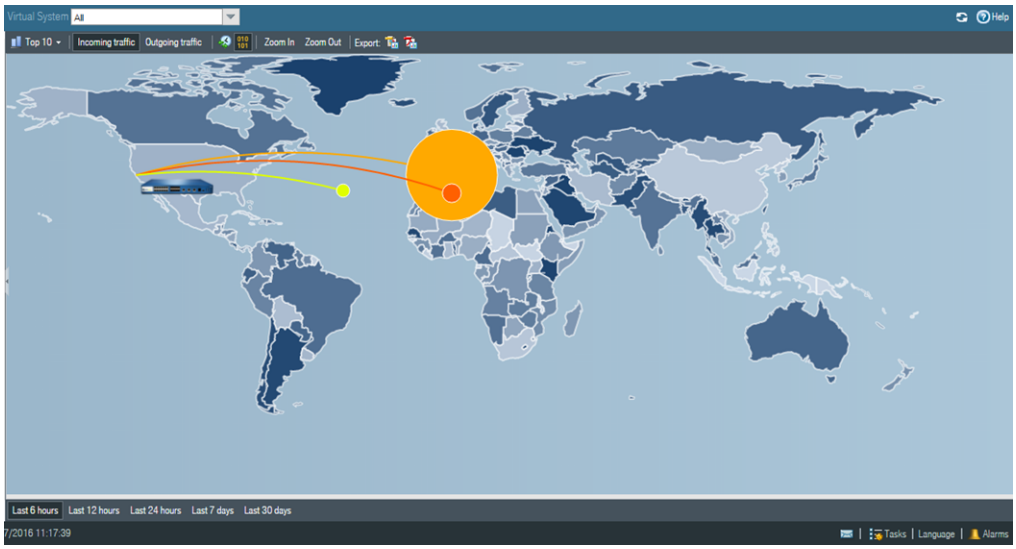
© 2020 Palo Alto Networks, Inc.

Opciones del informe del supervisor de red	Description (Descripción)
	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.
Barra inferior	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indica el periodo durante el que se realizaron las mediciones de cambio.

Informe del mapa de tráfico de Appscope

El informe del mapa de tráfico muestra una vista geográfica de los flujos de tráfico según las sesiones o los flujos.

Informe del mapa de tráfico de Appscope



Cada tipo de tráfico está indicado con colores como se indica en la leyenda debajo del gráfico. Este informe contiene las siguientes opciones.

Opciones del informe del mapa de tráfico	Description (Descripción)
Barra superior	
PRINCIPALES 10	Determina el número de registros con la mayor medición incluidos en el gráfico.
Tráfico entrante	Muestra el tráfico entrante.
Tráfico saliente	Muestra el tráfico saliente.

© 2020 Palo Alto Networks, Inc.

Opciones del informe del mapa de tráfico	Description (Descripción)
Contar sesiones y contar bytes	Determina si mostrar información de sesión o byte.
Acercar y alejar	Acerque y aleje el mapa.
Exportar	Exportar el gráfico como imagen .png o PDF.
Barra inferior	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indica el periodo durante el que se realizaron las mediciones de cambio.

© 2020 Palo Alto Networks, Inc.

Monitor > Session Browser

Seleccione **Monitor (Supervisar)** > **Session Browser (Navegador de sesión)** para explorar y filtrar sesiones actualmente en ejecución en el cortafuegos. Para obtener información acerca de las opciones de filtrado en esta página, consulte Acciones de log.

© 2020 Palo Alto Networks, Inc.

Supervisar > Lista de direcciones IP a bloquear

Puede configurar el cortafuegos para que coloque direcciones IP en la lista de bloqueo de varias formas:

- Configure una regla de políticas de protección DoS con la acción **Protect (Proteger)** y aplicar a la regla un perfil de protección DoS clasificado. El perfil incluye la duración del bloqueo.
- Configure una regla de la política de seguridad con un perfil de protección frente a vulnerabilidades que utilice una regla con la acción **Block IP (Bloquear IP)** y aplíquela a una zona.

La lista Bloquear IP se admite en los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series.

¿Qué desea saber?	Consulte:
¿Qué indican los campos de la lista Block IP?	Entradas de lista de direcciones IP a bloquear
¿Cómo puedo filtrar, navegar o eliminar entradas de la lista Block IP?	Ver o eliminar entradas de lista de direcciones IP a bloquear
¿Busca más información?	Configuración de antivirus, antispyware y protección frente a vulnerabilidades Protección DoS contra inundaciones de nuevas sesiones Supervisión de direcciones IP bloqueadas

Entradas de lista de direcciones IP a bloquear

- **Supervisión de > lista IP de bloqueo**

La tabla siguiente explica la entrada en la lista de bloqueadas para una dirección IP de origen que el cortafuegos ha bloqueado.

Campo	Description (Descripción)
Tiempo de bloqueo	Mes/día y horas: minutos: segundos cuando la dirección IP entró en la lista de IP bloqueadas.
Tipo	Tipo de acción de bloqueo: si el hardware (hw) o el software (sw) bloquearon la dirección IP. Cuando configura una polçitica de protección DoS o una política de seguridad que utiliza un perfil de protección contra vulnerabilidades para bloquear conexiones desde direcciones IPv4 de origen, el cortafuegos bloquea automáticamente ese tráfico en hardware antes de que esos paquetes usen recursos de la CPU o búfer de paquetes. Si el tráfico de ataques excede la capacidad de bloqueo del hardware, el cortafuegos utiliza software para bloquear el tráfico.
Source IP Address (Dirección IP de origen)	Dirección IP de origen del paquete que bloqueó el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Zona de entrada	Zona de seguridad asignada a la interfaz donde el paquete entró en el cortafuegos.
Tiempo restante	Número de segundos restantes para que la dirección IP esté en la lista de bloqueo de direcciones IP.
Bloquear origen	Nombre del perfil de protección de DoS clasificado o del objeto de protección de vulnerabilidad donde especificó la acción de bloqueo de direcciones IP.
Número total de IP bloqueadas: x de y (z% utilizado)	Número de direcciones IP bloqueadas (x) del número de direcciones IP bloqueadas que soporta el cortafuegos (y) y el porcentaje correspondiente de direcciones IP bloqueadas utilizadas (z).

Ver o eliminar entradas de lista de direcciones IP a bloquear

Vaya a la lista de entradas de Block IP, vea información detallada y elimine una entrada si lo desea.

Ver o eliminar entradas de lista de direcciones IP a bloquear	
Busque información específica de la lista de block IP	Seleccione un valor en una columna, que introduce un filtro en el campo **Filters (Filtros)** y haga clic en la flecha derecha para iniciar la búsqueda de entradas con ese valor. Haga clic en X para quitar el filtro.
Vea las entradas de la lista Block IP más allá de la pantalla actual	Introduzca un número de página en el campo **Page (Página)** o haga clic en las flechas individuales para ver la página siguiente o la página anterior de las entradas. Haga clic en las flechas dobles para ver la última página o primera página de las entradas.
Consulte información detallada sobre una dirección IP en la lista de Block IP	Haga clic en una dirección IP de origen de una entrada, que enlaza con Network Solutions WhoIs con información sobre la dirección.
Elimine entradas en la lista de Block IP	Seleccione una entrada y haga clic en **Delete (Eliminar)**. *Solo la eliminación de entradas de hardware es compatible en la interfaz web. Sin embargo, es posible eliminar las entradas de hardware y software desde la CLI.*
Borrar todo el contenido de la lista Block IP	Haga clic en **Clear all (Borrar todo)** para eliminar permanentemente todas las entradas, lo que significa que esos paquetes ya no están bloqueados. *Solo se puede borrar la lista de bloqueo de entradas de hardware en la interfaz web. Sin embargo, es posible borrar las entradas de hardware y de software desde la CLI.*

© 2020 Palo Alto Networks, Inc.

Monitor > Botnet

El Informe de Botnet le permite utilizar mecanismos basados en el comportamiento para identificar posibles hosts potencialmente infectados por Botnet o por malware en su red. El informe le asigna a cada host una puntuación de confianza del 1 al 5 que indica la probabilidad de infección por Botnet, 5 indica la mayor probabilidad. Antes de programar el informe o ejecutarlo bajo demanda, debe configurarlo para que identifique los tipos de tráfico sospechosos. La Guía del administrador de PAN-OS® proporciona información detallada sobre la interpretación de los informes de Botnet.

- Configuración de informe de Botnet
- Ajustes de configuración de Botnet

Configuración de informe de Botnet

- Monitor > Botnet > Report Setting

Antes de generar un informe de Botnet, debe especificar los tipos de tráfico que indican una actividad de Botnet potencial (consulte Configuración del informe de Botnet). Para programar un informe diario o ejecutarlo bajo demanda, haga clic en **Report Setting (Configuración de informes)** y complete los siguientes campos. Para exportar un informe, selecciónelo y elija **Export to PDF (Exportar a PDF)**, **Export to CSV (Exportar a CSV)** o **Export to XML (Exportar a XML)**.

Configuración de informe de Botnet	Description (Descripción)
Test Run Time Frame (Período de ejecución de la prueba)	Seleccione el intervalo de tiempo del informe: **Last 24 Hours (Últimas 24 horas)** (predeterminado) o **Last Calendar Day (Último día natural)**.
Ejecutar ahora	Haga clic en **Run Now (Ejecutar ahora)** para generar un informe de manera manual e inmediata. El informe muestra una nueva pestaña dentro del cuadro de diálogo de Informe de Botnet.
N.º de filas	Especifique el número de filas que mostrar en el informe (de forma predeterminada está el número 100).
Programado	Seleccione esta opción para generar el informe diariamente de manera automática. De manera predeterminada, esta opción está habilitada.
Generador de consultas	(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 sabe que el tráfico iniciado desde la dirección 192.0.2.0 no contiene ninguna actividad potencial de Botnet, puede añadir `not (addr.src in 192.0.2.0)` como una consulta para excluir al host del informe. • **Connector (Conector)**: seleccione un conector lógico (**and** o bien **or**). Si selecciona **Negate (Negar)**, el informe excluirá a los hosts que especifica la consulta. • **Attribute (Atributo)**: seleccione una zona, dirección o usuario asociado con los hosts que el contrafuegos evalúa en busca de actividad de Botnet.

© 2020 Palo Alto Networks, Inc.

Configuración de informe de Botnet	Description (Descripción)
	• **Operator (Operador)**: seleccione un operador para relacionar el **Attribute (Atributo)** a un **Value (Valor)**. • **Value (Valor)**: Escriba un valor para que coincida con la consulta.

Ajustes de configuración de Botnet

- Monitor > Botnet > Configuration

Para especificar los tipos de tráfico que indican actividad potencial de Botnet, haga clic en **Configuration (Configuración)** a la derecha de la página **Botnet** y complete los siguientes campos. Después de configurar el informe, puede ejecutarlo según petición o programarlo diariamente (consulte Monitor > PDF Reports > Manage PDF Summary).

La configuración predeterminada del informe de Botnet es la óptima. Si considera que los valores predeterminados identifican falsos positivos, cree un vale de soporte para que Palo Alto Networks pueda reexaminar los valores.

Ajustes de configuración de Botnet	Description (Descripción)
Tráfico HTTP	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 **Count (Recuento)** que introduzca corresponden a la cantidad mínima de eventos de cada tipo de tráfico que deben producirse para que el informe indique al host asociado con una puntuación de confianza mayor (mayor probabilidad de una infección por Botnet). Si la cantidad de eventos es menor al valor **Count (Recuento)**, el informe mostrará una puntuación de confianza menor o (en determinados tipos de tráfico) no mostrará una entrada para el host. • **Malware URL visit (Visita a URL de malware)** (intervalo de 2-1000; el valor predeterminado es 5): Identifica a los usuarios que se están comunicando con URL con malware conocidas basándose en las categorías de filtrado de URL de software malintencionado y Botnet. • **Use of dynamic DNS (Uso de DNS dinámica)** (intervalo de 2-1000; el valor predeterminado es 5): Busca tráfico de consulta DNS dinámico que pueda indicar malware, comunicaciones de Botnet o kits de vulnerabilidad de seguridad. Generalmente, utilizar dominios DNS dinámicos es muy arriesgado. El malware a menudo usa DNS dinámico para evitar estar en listas negras de IP. Considere utilizar un filtrado de URL para bloquear dicho tráfico. • **Browsing to IP domains (Navegación por dominios IP)** (intervalo de 2-1000; el valor predeterminado es 10): Identifica a los usuarios que examinan dominios IP en lugar de URL. • **Browsing to recently registered domains (Navegación en dominios registrados recientemente)** (intervalo de 2-1000; el valor predeterminado es 5): Busca tráfico en dominios que se registraron en los últimos 30 días. Los atacantes, malware y los exploits kits a menudo usan dominios recientemente registrados.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de Botnet	Description (Descripción)
	• **Executable files from unknown sites (Archivos ejecutables de sitios desconocidos)** (intervalo de 2-1000; el valor predeterminado es 5): Identifica los archivos ejecutables descargados desde URL desconocidas. Los archivos ejecutables son una parte de muchas infecciones y, cuando se combinan con otros tipos de tráfico sospechoso, pueden ayudar a priorizar las investigaciones de hosts.
Aplicaciones desconocidas	Defina los umbrales que determinan si el informe incluirá tráfico asociado con las aplicaciones de TCP desconocido o UDP desconocido sospechosas. • **Sessions Per Hour (Sesiones por hora)** (intervalo es 1-3600; el valor predeterminado es 10): El informe incluye tráfico que incluye hasta la cantidad especificada de sesiones de aplicación por hora. • **Destinations Per Hour (destinos por hora)** (intervalo es 1-3600; el valor predeterminado es 10): El informe incluye tráfico que incluye hasta la cantidad especificada de destinos de aplicación por hora. • **Minimum Bytes (Bytes mínimos)** (intervalo es 1-200; el valor predeterminado es 50): El informe incluye tráfico para el que la carga de aplicaciones es igual o excede el tamaño especificado. • **Maximum Bytes (Bytes máximos)** (intervalo es 1-200; el valor predeterminado es 100): El informe incluye tráfico para el que la carga de aplicaciones es igual o menor al tamaño especificado.
IRC	Seleccione esta opción para incluir tráfico que incluye servidores IRC.

© 2020 Palo Alto Networks, Inc.

Supervisar > Informes en PDF

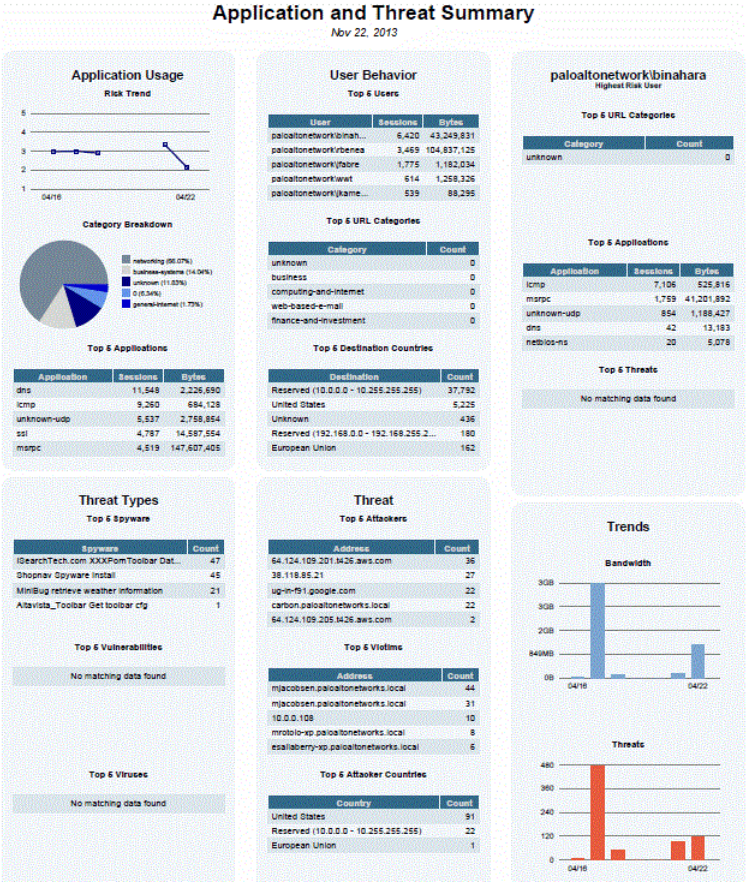
Los siguientes temas describen los informes en PDF.

- Monitor > PDF Reports > Manage PDF Summary
- Monitor > PDF Reports > User Activity Report
- Monitor > PDF Reports > SaaS Application Usage
- Monitor > PDF Reports > Report Groups
- Monitor > PDF Reports > Email Scheduler

Monitor > PDF Reports > Manage PDF Summary

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.

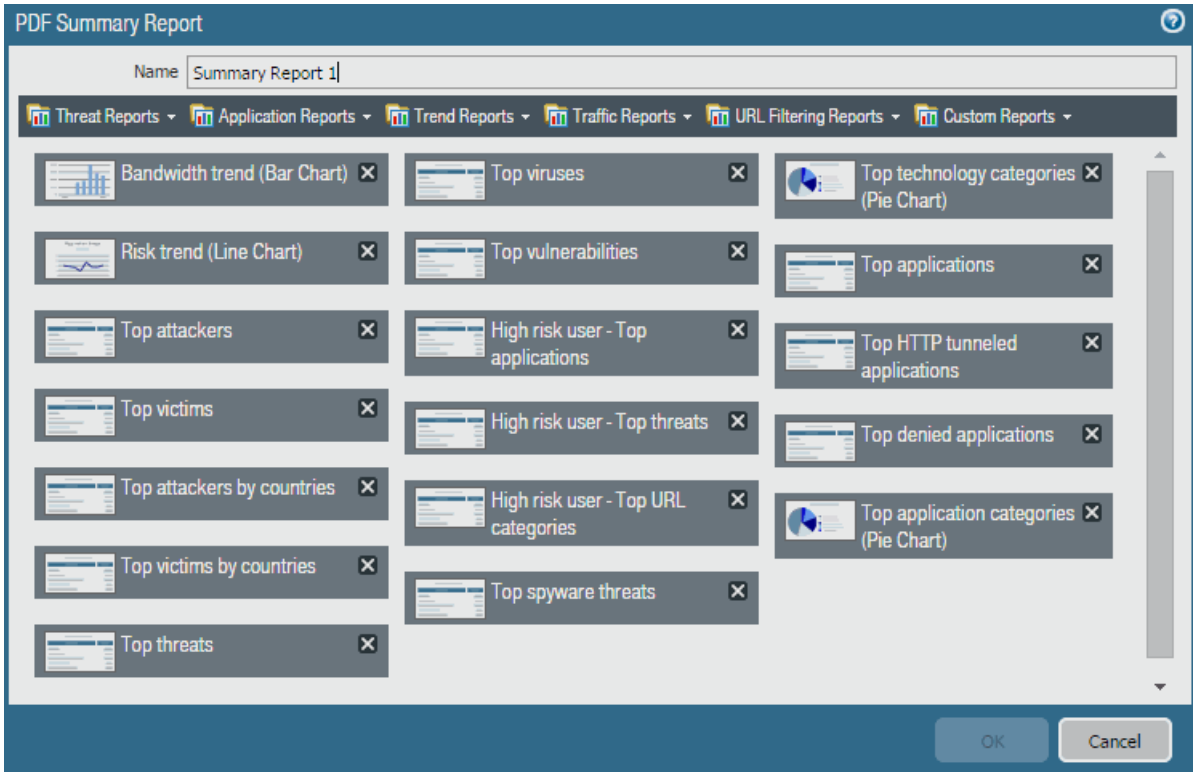
Informe de resumen en PDF



Para crear informes de resumen en PDF, haga clic en **Add (Añadir)**. Se abre la página **PDF Summary Report (Informe de resumen en PDF)** para mostrar todos los elementos de informe disponibles.

Gestión de informes en PDF

© 2020 Palo Alto Networks, Inc.



Diseñe el informe con una o varias de estas opciones:

- Para eliminar un elemento del informe, haga clic en el botón de las aspas ([X]) o borre el artículo en el menú desplegable correspondiente.
- Seleccione elementos adicionales desde la lista desplegable correspondiente.
- Arrastre y suelte un elemento para desplazarlo a otra área del informe.

Se permite un máximo de 18 elementos de informe. Si ya tiene 18, debe eliminar elementos existentes para poder añadir más.

Para guardar el informe (**Save [Guardar]**), introduzca un nombre para el informe y haga clic en **OK (Aceptar)**.

Para mostrar informes en PDF, seleccione **Supervisar** > **Informes**, haga clic en **Informe de resumen en PDF** para seleccionar un informe y haga clic en un día del calendario para descargar un informe de ese día.

Los nuevos informes de resumen en PDF no aparecerán hasta después de que se ejecute el informe, que se producirá automáticamente cada 24 horas a las 2:00 de la madrugada.

Monitor > PDF Reports > User Activity Report

Utilice esta página para crear informes que resumen la actividad de usuarios individuales o grupos de usuarios. Haga clic en **Add (Añadir)** y especifique la siguiente información.

Configuración de User/ Group Activity Report	Description (Descripción)
Nombre	Introduzca un nombre para el informe (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Configuración de User/ Group Activity Report	Description (Descripción)
Tipo	Para informe de actividad de usuario: Seleccione **User (Usuario)** e introduzca el **Username (Nombre de usuario)**o **IP address (Dirección IP)** (IPv4 o IPv6) del usuario que será el asunto del informe.
	Para informe de actividad de grupo: Seleccione **Group (Grupo)** e introduzca el **Group Name (Nombre de grupo)**.
Additional Filters (Filtros adicionales)	Seleccione **Filter Builder (Generador de filtro)** para crear filtros para el informe de actividad de usuario/grupo.
Periodo de tiempo	Seleccione el período de tiempo para el informe en el menú desplegable.
Incluir navegación detallada	(Opcional) Seleccione esta opción para incluir logs de URL detallados en el informe. *La información de navegación detallada puede incluir un gran volumen de logs (miles) para el usuario o grupo de usuarios seleccionado y puede hacer que el informe sea muy extenso.*

El informe de actividad de grupo no incluye Resumen de navegación por categoría de URL; el resto de información es común para el informe de actividad de usuarios y el informe de actividad de grupo.

Para ejecutar el informe a petición, haga clic en **Run Now (Ejecutar ahora)**. Para cambiar el máximo de filas que se muestran en el informe, consulte Logging and Reporting Settings.

Para guardar el informe, haga clic en **OK (Aceptar)**. A continuación, puede programar el envío del informe por correo electrónico (Monitor > PDF Reports > Email Scheduler).

Añadir un filtro de log

Cree filtros de log para los informes de actividad del usuario y actividad del grupo para personalizar los informes. Puede filtrar los informes de actividad en función de la aplicación, las características de la aplicación, etc. Por ejemplo, si le interesa una aplicación de SaaS que no posea certificaciones, puede crear un filtro con esta característica de aplicación.

Campo de Añadir filtro de log	Description (Descripción)
Cuadro de texto Log Filter (Filtro de log)	Introduzca el filtro que desea aplicar al log. Puede introducir múltiples filtros.
Conector	Añada una opción de filtrado adicional al filtro. Seleccione la opción **Negate (Negar)** para no aplicar un conector al filtro que introdujo.
Atributo	Seleccione el atributo que desea añadir desde el menú.

© 2020 Palo Alto Networks, Inc.

Campo de Añadir filtro de log	Description (Descripción)
Operador	Seleccione si Attribute (Atributo) debe ser igual o no a Value (Valor).
Valor	Establezca el valor para el atributo. Cuando esté disponible, aparecerá un menú desplegable con los valores posibles.

Seleccione **Apply (Aplicar)** para aplicar el filtro creado al informe de actividad de usuario o de actividad de grupo.

Monitor > PDF Reports > SaaS Application Usage

Utilice esta página para generar un informe de utilización de aplicación de SaaS que resuma los riesgos de seguridad asociados a las aplicaciones de SaaS que atraviesan su red. El informe predefinido presenta una comparación de las aplicaciones no sancionadas frente a las sancionadas, resume las aplicaciones de SaaS riesgosas con características de host desfavorables, y destaca la actividad, la utilización y el cumplimiento de las aplicaciones enumerando las principales aplicaciones de cada categoría en las páginas con información detallada. Puede utilizar esta información detalladas de riesgo para aplicar políticas para aplicaciones de SaaS que desee permitir o bloquear en su red.

Para generar un informe preciso e informativo, debe etiquetar las aplicaciones sancionadas en su red (consulte Generar el informe de utilización de aplicaciones de SaaS). El cortafuegos y Panorama consideran cualquier aplicación sin esta etiqueta predefinida como no aprobada para usar en la red. Es importante saber acerca de las aplicaciones sancionadas y las no sancionadas que son frecuentes en su red, ya que las aplicaciones SaaS no sancionadas son una amenaza potencial a la seguridad de la información; no están aprobadas para uso en su red y pueden causar una exposición a amenazas y pérdidas de datos privados y confidenciales.

Asegúrese de etiquetar las aplicaciones de forma coherente en todos los cortafuegos o grupos de dispositivos. Si la misma aplicación está etiquetada como sancionada en un sistema virtual y como no sancionada en otro, o en Panorama, si una aplicación es no sancionada en un grupo de dispositivos primarios, pero está etiquetada como sancionada en un grupo de dispositivos secundarios (o viceversa), el informe de uso de la aplicación SaaS producirá resultados superpuestos.

En el ACC, defina Application View (Vista de la aplicación) en By Sanctioned State (Por estado sancionado) para identificar visualmente las aplicaciones que tienen diferentes estados sancionados en todos los sistemas virtuales o grupos de dispositivos. El color verde, indica aplicaciones sancionadas, azul, aplicaciones no sancionadas y amarillo, aplicaciones con un estado sancionado diferente en distintos sistemas virtuales o grupos de dispositivos.

Para configurar el informe, haga clic en **Add (Añadir)** y especifique la siguiente información:

Configuración del informe de SaaS Application Usage	Description (Descripción)
Nombre	Introduzca un nombre para el informe (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Configuración del informe de SaaS Application Usage	Description (Descripción)
Periodo de tiempo	Seleccione el período de tiempo para el informe en la lista desplegable: **Last 7 Days (Últimos 7 días)**, **Last 30 Days (Últimos 30 días)** o **Last 90 Days (Últimos 90 días)**. El informe incluye datos del presente día en que se genera el informe.
Incluir logs de	En el menú desplegable, seleccione si desea generar el informe en un grupo de usuarios seleccionado, en una zona seleccionada o en todos los grupos de usuarios y zonas configurados en el cortafuegos o en Panorama. • **Para un grupo de usuarios seleccionado**: seleccione el **User Group (Grupo de usuarios)** cuyos logs filtrará el cortafuegos o Panorama. • **Para una zona seleccionada**: seleccione la **Zone (Zona)** cuyos logs filtrará el cortafuegos o Panorama. • **Para todos los grupos de usuarios y zonas**: puede generar informes de todos los grupos o elegir hasta 25 grupos de usuarios de los que desea visibilidad. Si tiene más de 25 grupos, el cortafuegos o Panorama mostrarán los 25 grupos principales en el informe y asignará todos los grupos de usuarios restantes al grupo Others (Otros).
Incluir información de grupos de usuarios en el informe (No disponible si elige generar el informe en un **Selected User Group [Grupo de usuarios seleccionado]**).	Esta opción filtra los logs de los grupos de usuarios que desea incluir en el informe. Seleccione el enlace **manage groups (Gestionar grupos)** o **manage groups for the selected zone (Gestionar grupos de la zona seleccionada)** para elegir hasta 25 grupos de usuarios de los que desea visibilidad. Cuando genera un informe para grupos de usuarios específicos en una zona seleccionada, los usuarios que no son miembros de ninguno de los grupos seleccionados se asignan a un grupo denominado Others (Otros).
User group (Grupo de usuarios)	Seleccione los grupos de usuarios de los que desea generar informes. Esta opción solo se muestra cuando elige **Selected User Group (Grupo de usuarios seleccionado)** en el menú desplegable **Include logs from (Incluir logs de)**.
Zona	Seleccione la zona de la que desea generar un informe. Esta opción solo se muestra cuando elige **Selected Zone (Zona seleccionada)** en el menú desplegable **Include logs from (Incluir logs de)**. Por lo tanto, puede incluir información de grupo de usuarios en el informe.
Incluir la información detallada de la categoría de la aplicación en el informe	El Informe de uso de la aplicación SaaS en PDF es un informe de dos partes. De manera predeterminada, se generan ambas partes de informe. La primera parte del informe (10 páginas) se centra en las aplicaciones SaaS utilizadas en su red durante el periodo del informe. Borre esta opción si no desea la segunda parte del informe que incluye información detallada para las aplicaciones SaaS y no SaaS para cada subcategoría de aplicación enumerada en la primera parte del informe. Esta segunda parte del informe incluye los nombres de las aplicaciones principales en cada subcategoría e información acerca de los usuarios, grupos de usuarios, archivos, bytes transferidos y amenazas generadas a partir de estas aplicaciones.

© 2020 Palo Alto Networks, Inc.

Configuración del informe de SaaS Application Usage	Description (Descripción)
	Sin la información detallada, el informe tiene diez páginas.
Limitar subcategorías máximas del informe a	Seleccione si desea utilizar todas las subcategorías en el informe SaaS Application Usage (Uso de aplicación SaaS) o si desea limitar el máximo a 10, 15, 20 o 25 subcategorías. Al reducir el máximo de subcategorías, el informe detallado es más corto porque limita la información de la actividad de la aplicación SaaS y no SaaS incluida en el informe.

Haga clic en **Run Now (Ejecutar ahora)** para generar el informe a petición.

Puede generar este informe bajo demanda o programarlo para que se genere a diario, semanalmente o mensualmente. Para programar el informe, consulte Programar informes para la entrega de correos electrónicos.

En los contrafuegos PA-220 y PA-220R, el informe SaaS Application Usage no se envía como PDF adjunto PDF en el correo electrónico. En lugar de eso, el correo electrónico incluye un enlace para abrir el informe en un navegador web.

Para obtener más información acerca de los informes, consulte Gestión de informes (en inglés).

Monitor > PDF Reports > Report Groups

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.

Configuración de Report Group	Description (Descripción)
Nombre	Introduzca un nombre para el grupo de informe (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Página de título	Seleccione esta opción para incluir una página de título en el informe.
Title	Introduzca el nombre que aparecerá como el título del informe.
Selección de informe / widgets	Para que se incluya en el grupo, seleccione el informe en la columna izquierda y haga clic en **Add (Añadir)** para añadirlo a la columna derecha. Puede seleccionar los siguientes tipos de informe: • Informe predefinido • Informe personalizado • Informe de resumen en PDF • Csv • Log View (Vista de log): siempre que cree un informe personalizado, el cortafuegos crea automáticamente un informe Log View con el mismo nombre. Este informe Log View mostrará los logs que el cortafuegos ha utilizado para crear el contenido del informe personalizado. Para incluir

© 2020 Palo Alto Networks, Inc.

Configuración de Report Group	Description (Descripción)
	los datos de la vista de logs, al crear un grupo de informes, añada sus **Custom Reports (Informes personalizados)** y añada los informes de **Log View (Vista de log)** coincidentes. El informe agregado que se ha generado para el grupo de informes muestra los datos de informe personalizados seguidos de los datos de log. Después de guardar el grupo de informes, la columna Widgets de la página Report Groups (Grupos de informes) muestra los informes que ha añadido al grupo.

Para utilizar el grupo de informes, consulte Monitor > PDF Reports > Email Scheduler.

Monitor > PDF Reports > Email Scheduler

Utilice el programador de correo electrónico para programar informes para la entrega de correo electrónico. Antes de agregar un programa, debe definir grupos de informe y un perfil de correo electrónico. Consulte Monitor > PDF Reports > Report Groups y Device > Server Profiles > Email.

Los informes programados comienzan a ejecutarse a las 2:00 AM y el reenvío de correo electrónico se produce después de que finalice la ejecución de todos los informes programados.

Configuración de Email Scheduler	Description (Descripción)
Nombre	Indique un nombre para la planificación (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Grupo de informes	Seleccione el grupo de informes (Monitor > PDF Reports > Report Groups) o el informe de uso de la aplicación SaaS (Monitor > PDF Reports > SaaS Application Usage) que desea programar.
Perfil de correo electrónico	Seleccione el perfil que define los ajustes de correo electrónico. Consulte Device > Server Profiles > Email para obtener información sobre la definición de perfiles de correo electrónico.
Periodicidad	Seleccione la frecuencia con la que generar y enviar el informe.
Cancelar direcciones de correo electrónico	Introduzca una dirección de correo electrónico opcional para utilizar en lugar del destinatario especificado en el perfil de correo electrónico.
Enviar correo electrónico de prueba	Haga clic para enviar un correo electrónico de prueba a la dirección de correo electrónico definida en el **Email Profile (Perfil de correo electrónico)**.

© 2020 Palo Alto Networks, Inc.

Monitor > Manage Custom Reports

Puede crear informes personalizados que se ejecuten a petición o según una planificación (cada noche). Para los informes predefinidos, seleccione **Monitor (Supervisar)** > **Reports (Informes)**.

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.

Haga clic en **Add (Añadir)** para añadir un informe personalizado para crear uno nuevo. Para basar el informe en una plantilla existente, haga clic en **Load Template (Cargar plantilla)** y selecciónela. Para generar un informe a petición, en lugar o además del que se genera a la hora programada (**Scheduled [Programado]**), haga clic **Run Now (Ejecutar ahora)**. Especifique los siguientes ajustes para definir el informe.

Configuración de los informes personalizados	Description (Descripción)
Nombre	Introduzca un nombre para el informe (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción para el informe personalizado.
Base de datos	Seleccione la base de datos para utilizar como el origen de datos para el informe.
Programado	Seleccione esta opción para ejecutar el informe cada noche. El informe estará disponible en **Monitor (Supervisar)** > **Reports (Informes)**.
Time Frame (Período de tiempo)	Seleccione un período de tiempo fijo o seleccione **Custom (Personalizar)** y especifique un intervalo de fecha y hora.
Ordenar por	Seleccione las opciones de clasificación para organizar el informe, así como la cantidad de información que desea incluir en el informe. Las opciones disponibles dependen de la elección de la base de datos.
Agrupar por	Seleccione las opciones de agrupación para organizar el informe, así como la cantidad de información que desea incluir en el informe. Las opciones disponibles dependen de la elección de la base de datos.
Columnas	Seleccione Available Columns para incluir en el informe personalizado y añádalas (⊞) a Selected Columns. Seleccione **Up (Hacia arriba)**, **Down (Hacia abajo)**, **Top (A la parte superior)** y **Bottom (A la parte inferior)** para reordenar las columnas seleccionadas. Según sea necesario, también puede seleccionar y eliminar (⊟) las columnas previamente seleccionadas.
Generador de consultas	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.

© 2020 Palo Alto Networks, Inc.

Configuración de los informes personalizados	Description (Descripción)
	• **Connector (Conector)**: seleccione el conector (**and** o **or**) para preceder la expresión que está agregando. • **Negate (Negar)**: seleccione esta opción para interpretar la consulta como una negativa. En el ejemplo anterior, la opción negar causa una coincidencia en entradas que no se han producido en las últimas 24 horas o que no son de 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.

Para obtener más información, consulte Generación de informes personalizados (en inglés).

© 2020 Palo Alto Networks, Inc.

Monitor > Reports

El cortafuegos proporciona diversos informes de los “50 principales” de las estadísticas de tráfico del día anterior o un día seleccionado de la semana anterior.

Para ver un informe, expanda una categoría de informe (por ejemplo, Informes personalizados) en el lado derecho de la página y seleccione un nombre de informe. La página enumera los informes en secciones. Puede visualizar la información en cada informe del período de tiempo seleccionado.

De forma predeterminada, el cortafuegos muestra todos los informes del día de calendario anterior. Para ver informes de otras fechas, seleccione una fecha de creación de informe en el calendario de la parte inferior derecha de la página.

Para ver los informes en un sistema que no sea el cortafuegos, seleccione una opción de exportación:

- **Exportar a PDF**
- **Exportar a CSV**
- **Exportar a XML**

Políticas

Los siguientes temas describen tipos de políticas de cortafuegos, cómo mover o duplicar políticas y la configuración de las políticas:

> Tipos de políticas
> Traslado o duplicación de una regla de política
> Auditar archivo de comentarios
> Consulta de recuento de resultado de uso de regla
> Políticas > Seguridad
> Políticas > NAT
> Políticas > QoS
> Políticas > Reenvío basado en políticas
> Políticas > Descifrado
> Políticas> Inspección de túneles
> Policies > Application Override
> Políticas > Autenticación
> Políticas > Protección DoS
> Políticas > SD-WAN

© 2020 Palo Alto Networks, Inc.

Tipos de políticas

Las políticas permiten controlar el funcionamiento del cortafuegos al aplicar reglas y automatizar acciones. El cortafuegos admite los siguientes tipos de políticas:

- Políticas de seguridad básicas para bloquear o permitir una sesión de red basada en la aplicación, las zonas y direcciones de origen y destino y, opcionalmente, el servicio (puerto y protocolo). Las zonas identifican interfaces físicas o lógicas que envían o reciben tráfico. Consulte Policies > Security.
- Políticas de traducción de direcciones de red (NAT) para traducir direcciones y puertos. Consulte Policies > NAT.
- Políticas de calidad de servicio (QoS) para determinar la forma en la que se clasifica el tráfico para su tratamiento, cuando pasa por una interfaz con QoS activado. Consulte Policies > QoS.
- Políticas de reenvío basado en políticas para cancelar la tabla de enrutamiento y especificar una interfaz de salida para el tráfico. Consulte Policies > Policy Based Forwarding.
- Políticas de descifrado para especificar el descifrado del tráfico de las políticas de seguridad. Cada una de las políticas puede especificar las categorías de las URL del tráfico que desea descifrar. El descifrado SSH se utiliza para identificar y controlar los túneles SSH, así como el acceso SSH (Secure Shell). Consulte Policies > Decryption.
- Políticas de inspección de túneles para aplicar las políticas de seguridad, protección DoS y QoS en el tráfico de túneles y para ver la actividad del túnel. Consulte Policies > Tunnel Inspection.
- Políticas de cancelación para anular las definiciones de la aplicación proporcionadas por el cortafuegos. Consulte Policies > Application Override.
- Políticas de autenticación para definir la autenticación para los usuarios finales que acceden a los recursos de red. Consulte Policies > Authentication.
- Políticas de denegación de servicio (DoS) para proteger de ataques DoS y tomar las medidas de protección en respuesta que coincidan con las reglas. Consulte Policies > DoS Protection.
- Políticas de SD-WAN para determinar la gestión de la ruta de enlace entre las zonas de origen y destino cuando el estado de la ruta de enlace se degrada por debajo de las métricas de estado configuradas y aprobadas. Consulte Políticas > SD-WAN.

Las políticas compartidas enviadas desde Panorama™ se muestran en naranja en la interfaz web del cortafuegos. Solo puede editar estas políticas compartidas en Panorama; no se pueden editar en el cortafuegos.

Ver base de reglas como grupos para ver todos los grupos de etiquetas utilizados en una base de reglas. En las bases de reglas con numerosas reglas, la visualización de la base de reglas como grupos simplifica la visualización al presentar las etiquetas, el código de color y la cantidad de reglas en cada grupo, a la vez que mantiene la jerarquía de reglas establecida.

© 2020 Palo Alto Networks, Inc.

Traslado o duplicación de una regla de política

Al trasladar o duplicar políticas, puede asignar un **Destination (Destino)** (un sistema virtual en un cortafuegos o un grupo de dispositivos en Panorama) para el que cuenta con permisos de acceso, incluida la ubicación compartida.

Para mover una regla de políticas, seleccione la regla en la pestaña **Policies (Políticas)**, haga clic en **Move (Mover)**, seleccione **Move to other vsys (Mover a otros sistemas virtuales)** (solo cortafuegos) o **Move to different rulebase or device group (Mover a una base de reglas o grupo de dispositivos diferente)** (solo Panorama), complete los campos de la tabla siguiente y, a continuación, haga clic en **OK (Aceptar)**.

Para duplicar una regla de política, seleccione la regla en la pestaña **Policies (Políticas)**, haga clic en **Clone (Duplicar)**, complete los campos de la tabla siguiente y, a continuación, haga clic en **OK (Aceptar)**.

Configuración de traslado/ duplicación	Description (Descripción)
Reglas seleccionadas	Muestra el nombre y la ubicación actual (sistema virtual o grupo de dispositivos) de las reglas de políticas que ha seleccionado para la operación.
IP Destino	Seleccione la nueva ubicación de la política u objeto: un sistema virtual, un grupo de dispositivos o una ubicación compartida. El valor predeterminado es el **Virtual System (Sistema virtual)** o **Device group (Grupo de dispositivos)** que seleccionó en la pestaña **Policies (Políticas)** u **Objects (Objetos)**.
Orden de la regla	Seleccione la posición de regla con respecto a otras reglas: • **Move top (Mover a la parte superior)**: la regla precederá al resto de reglas. • **Move bottom (Mover a la parte inferior)**: la regla seguirá al resto de reglas. • **Before rule (Regla anterior)**: en la lista desplegable adyacente, seleccione la regla posterior. • **After rule (Regla posterior)**: en la lista desplegable adyacente, seleccione la regla anterior.
Error en el primer error detectado en la validación	Seleccione esta opción (seleccionada de manera predeterminada) para que el cortafuegos o Panorama muestre el primer error que encuentre y deje de buscar más errores. Por ejemplo, se produce un error si el **Destination (Destino)** no incluye un objeto al que se haga referencia en la regla de política que está moviendo. Si borra esta selección, el cortafuegos o Panorama buscará todos los errores antes de mostrarlos.

© 2020 Palo Alto Networks, Inc.

Auditar archivo de comentarios

Seleccione **Audit Comment Archive (Archivo de comentario de auditoría)** para ver el historial de comentarios de auditoría, los logs de configuración y el historial de cambios de la regla seleccionada.

- Comentarios de auditoría
- Logs de configuración (entre confirmaciones)
- Cambios de la regla

Comentarios de auditoría

Vea el historial de **Audit Comment (Comentario de auditoría)** para una regla de política seleccionada. Aplique y guarde los filtros para identificar rápidamente comentarios de auditoría específicos y exportar en formato CSV los comentarios de auditoría que se muestran.

Campo	Description (Descripción)
Hora de confirmación	Hora en que se confirmó el comentario de auditoría.
Auditar comentario	Contenido del comentario de auditoría.
Administrador	Usuario que añadió o modificó el comentario de auditoría.
Configurar versión	Versión de revisión de la configuración. 0 indica que la regla de política se creó por primera vez y se confirmó en Panorama.

Logs de configuración (entre confirmaciones)

Vea el log de configuración generado por la regla de política seleccionada entre confirmaciones. Aplique y guarde los filtros para identificar rápidamente los logs de configuración específicos y exportar en formato CSV los logs de configuración que se muestran.

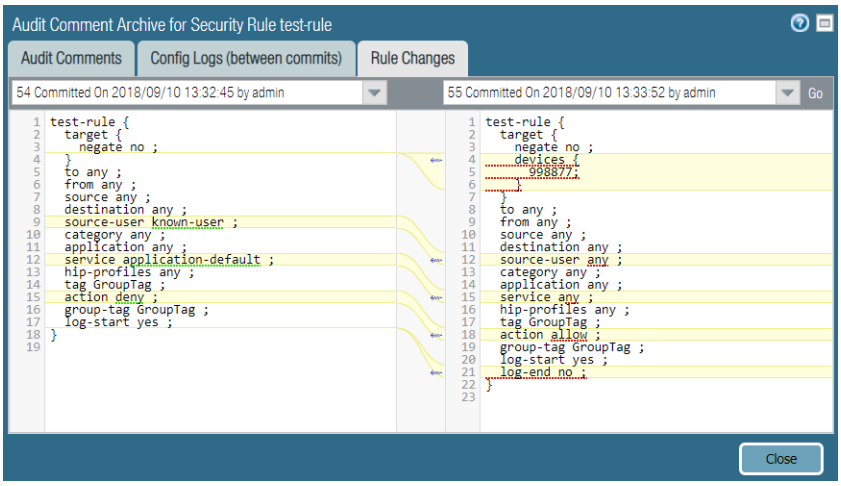
Campo	Description (Descripción)
Time	Hora en que se confirmó el comentario de auditoría.
Administrador	Contenido del comentario de auditoría.
Comando	Tipo de comando ejecutado.
Antes del cambio	Información de la regla antes de que se produjera el cambio. Por ejemplo, si cambia el nombre de una regla, se muestra el nombre anterior.
Después del cambio	Información de la regla después de que se produjera el cambio. Por ejemplo, si cambia el nombre de una regla, se muestra el nombre nuevo.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Device Name (Nombre del dispositivo)	Nombre del dispositivo antes del cambo de comentario de auditoría.

Cambios de la regla

Vea y compare la versión de configuración de la regla de política seleccionada para analizar los cambios que se han producido. En la lista desplegable, seleccione las dos versiones de configuración de regla de política que desea comparar.



© 2020 Palo Alto Networks, Inc.

Consulta de recuento de resultado de uso de regla

- **Policies (Políticas)** > **Rule Usage (Uso de reglas)**

Utilice la consulta de uso de reglas para filtrar la base de reglas seleccionada en un periodo especificado. La consulta de uso de reglas le permite filtrar rápidamente su base de reglas de política para identificar reglas no utilizadas para eliminarlas y así reducir los puntos de entrada abiertos para un atacante. Haga clic en **PDF/CSV** para exportar las reglas filtradas en formato PDF o CSV. Para usar la consulta de recuento de resultados de uso de regla, debe habilitar el ajuste **Policy Rule Hit Count (Recuento de resultados de regla de política)** (Device (Dispositivo) > Setup (Configuración) > Management (Gestión)).

De manera predeterminada, las columnas **Name (Nombre)**, **Location (Ubicación)**, **Created (Creación)**, **Modified (Modificación)** y **Rule Usage (Uso de regla)** se muestran cuando consulta el uso de la regla en su base de reglas de política. Puede añadir más columnas para ver información adicional sobre las reglas de políticas.

Tarea	Description (Descripción)
Hit Count (Recuento de resultados)	
Intervalo de tiempo	Indica el periodo para realizar la consulta en la base de reglas seleccionada. Seleccione entre las opciones de periodos predeterminados o configure un periodo **Custom (Personalizado)**.
Uso	Seleccione el uso de la regla que desea consultar: **Any (Cualquiera)**, **Unused (No utilizada)**, **Used (Utilizada)** o **Partially Used (Parcialmente utilizada)** (solo Panorama).
Desde	(Solo periodo personalizado) Seleccione la fecha y hora desde las cuales consultar la base de reglas de política.
Exclude rules reset during the last _ days (Excluir el restablecimiento de reglas durante los últimos _ días)	Seleccione esta opción para excluir las reglas que un usuario restableció manualmente en la cantidad especificada de días.

Uso de regla de dispositivo para la consulta de recuento de resultados de regla

Puede ver el uso de las reglas del dispositivo y el sistema virtual al ver el uso de una regla de política en el servidor de gestión de Panorama. Seleccione **Reset Rule Hit Counter (Restablecer el recuento de resultados de regla)** para restablecer el recuento de resultados, el primer resultado y el último resultado.

Haga clic en **PDF/CSV** para exportar las reglas filtradas en formato PDF o CSV.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Grupo de dispositivos	Grupo de dispositivo al que pertenece el dispositivo o sistema virtual.
Device Name (Nombre del dispositivo)/ Virtual System (Sistema virtual)	Nombre del grupo de dispositivos o sistema virtual.
Hit Count (Recuento de resultados)	Cantidad total de coincidencias de tráfico para la regla de política.
Last Hit (Último resultado)	Fecha y hora de la última coincidencia de tráfico para la regla de política.
First Hit (Primer resultado)	Fecha y hora de la primera coincidencia de tráfico para la regla de política.
Last Update Received (Última actualización recibida)	Fecha y hora de la última información de uso recibida del dispositivo en el servidor de gestión de Panorama.
Creado	Fecha y hora de creación de la regla de política.
Modificado	Fecha y hora de la última modificación de la regla de política. La columna está vacía si la regla de política no se ha modificado.
Estatal o regional	Estado de conexión del dispositivo: `Connected (Conectado)` o `Disconnected (Desconectado)`.

© 2020 Palo Alto Networks, Inc.

Políticas > Seguridad

Las reglas de políticas de seguridad hacen referencia a zonas de seguridad y gracias a ellas puede permitir, restringir y realizar un seguimiento del tráfico de su red basándose en la aplicación, el usuario o grupo de usuarios, y el servicio (puerto y protocolo). De manera predeterminada, el cortafuegos incluye una regla de seguridad denominada *regla1* que permite todo el tráfico desde la zona fiable a la zona no fiable.

¿Qué desea saber?	Consulte:
¿Qué es una política de seguridad?	Descripción general de las políticas de seguridad Para Panorama, consulte Traslado o duplicación de una regla de política
¿Qué campos están disponibles para crear una regla de política de seguridad?	Componentes de una regla de política de seguridad
¿Cómo puedo utilizar la interfaz web para gestionar reglas de políticas de seguridad?	Creación y gestión de políticas Cancelación o reversión de una regla de política de seguridad Aplicaciones y uso Optimizador de política de seguridad
¿Busca más información?	Política de seguridad

Descripción general de las políticas de seguridad

Las políticas de seguridad le permiten aplicar reglas y realizar acciones, y pueden ser todo lo general o específicas como sea necesario. Las reglas de política se comparan con el tráfico entrante en secuencia y al aplicar la primera regla que coincida con el tráfico, las reglas más específicas deben anteceder a las reglas más generales. Por ejemplo, una regla de una aplicación simple debe anteceder a una regla para todas las aplicaciones si el resto de configuraciones de tráfico son las mismas.

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. Para obtener más información, consulte Policies > Authentication.

Para el tráfico que no coincide con ninguna regla definida por el usuario, se aplican las reglas predeterminadas. Las reglas predeterminadas (que aparecen en la parte inferior de la base de reglas de seguridad) se predefinen para permitir todo el tráfico de intrazona (en la zona) y denegar todo el tráfico interzona (entre zonas). Aunque estas reglas son parte de la configuración predefinida y son de solo lectura de forma predeterminada, puede **Override (Cancelar)** y cambiar un número limitado de ajustes, incluidas las etiquetas, acción (permitir o denegar) configuración de log y perfiles de seguridad.

La interfaz incluye las siguientes pestañas para definir las reglas de la política de seguridad.

- **General**: seleccione la pestaña **General** para configurar un nombre y una descripción para la regla de la política de seguridad.
- **Source (Origen)**: seleccione la pestaña **Source (Origen)** para definir la zona o dirección de origen donde se origina el tráfico.
- **User (Usuario)**: seleccione la pestaña **User (Usuario)** para aplicar una política para usuarios individuales o un grupo de usuarios. Si está utilizando GlobalProtect™ con perfil de información del host (host

© 2020 Palo Alto Networks, Inc.

information profile, HIP) habilitado, también puede basar la política en información recopilada por GlobalProtect. Por ejemplo, el nivel de acceso del usuario puede estar determinado por un HIP que informe al cortafuegos acerca de la configuración local del usuario. La información HIP se puede utilizar para un control de acceso granular basado en los programas de seguridad en ejecución en el host, los valores de registro y muchas más comprobaciones si el host tiene instalado software antivirus.

- **Destination (Destino)**: seleccione la pestaña **Destination (Destino)** para definir la zona o dirección de destino para el tráfico.
- **Application (Aplicación)**: seleccione la pestaña **Application (Aplicación)** para que la acción de la política se produzca basándose en una aplicación o un grupo de aplicaciones. Un administrador también puede usar una firma de App-ID™ existente y personalizarla para detectar aplicaciones de propiedad reservada o para detectar atributos específicos de una aplicación existente. Las aplicaciones personalizadas se definen en **Objects (Objetos)** > **Applications (Aplicaciones)**.
- **Service/URL Category (Categoría de URL/servicio)**: seleccione la pestaña **Service/URL Category (Categoría de URL/servicio)** para especificar un número de puerto TCP o UDP específico o una categoría de URL como criterios de coincidencia en la política.
- **Action (Acciones)**: seleccione la pestaña **Action (Acciones)** para determinar la acción que se realizará basándose en el tráfico que coincida con los atributos de la política definida.
- **Usage (Utilización)**: seleccione la pestaña **Usage** para ver la utilización de una regla, incluida la cantidad de aplicaciones vistas en una regla, cuándo se vieron las últimas aplicaciones nuevas en la regla, los datos del recuento de resultados, el tráfico en los últimos 30 días y cuándo se creó y editó por última vez la regla.

Componentes de una regla de política de seguridad

- Políticas > Seguridad

La sección siguiente describe cada Componente en una regla de política de seguridad. Cuando crea una regla de la política de seguridad, podrá configurar las opciones descritas aquí.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
Número de regla	n/c	El cortafuegos numera automáticamente cada regla y el orden cambia a medida que las reglas se mueven. Al filtrar reglas para que coincidan con filtros específicos, cada regla se muestra con su número en el contexto del conjunto de reglas completo de la base de reglas y su puesto en el orden de evaluación. Panorama numera de manera independiente las reglas previas y las reglas posteriores. Cuando las reglas se envían desde Panorama hacia un cortafuegos gestionado, la numeración de reglas incorpora la jerarquía en las reglas previas, reglas del cortafuegos y reglas posteriores dentro de una base de reglas, y refleja la secuencia de reglas y su orden de evaluación.
Nombre	**General**	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
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.
Description (Descripción)		Introduzca una descripción de la política (hasta 1024 caracteres).
Etiquetas		Especifique la etiqueta para la política. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas reglas con palabras específicas como descifrado y sin descifrado, o utilizar el nombre de un centro de datos específico para políticas asociadas a esa ubicación. También puede añadir etiquetas a las reglas predeterminadas.
Agrupar reglas por etiquetas		El valor predeterminado es **None (Ninguna)**.
Auditar comentario		
Auditar archivo de comentarios		

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
Logs de configuración (entre confirmaciones)		
Cambios de la regla		
Zona de origen	**Source (Origen)**	Seleccione **Add (Añadir)** para añadir zonas de origen (el valor predeterminado es **Any [Cualquiera]**). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.
Dirección de origen		Seleccione **Add (Añadir)** para añadir direcciones de origen, grupos de direcciones o regiones (la opción predeterminada es **Any [Cualquiera]**). Seleccione entre las opciones del menú desplegable o seleccione el objeto **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** (en la parte inferior del menú desplegable) para especificar los ajustes. Objects (Objetos) >Addresses (Direcciones) y Objects (Objetos) >AddressGroups (Grupos de direcciones) describen los tipos de objetos de direcciones y grupos de direcciones, respectivamente, que admiten una regla de política de seguridad. Al seleccionar la opción **Negate (Negar)**, la regla se aplicará a las direcciones de origen de la zona especificada, con la excepción de las direcciones especificadas.
Source User (Usuario de origen)	**Usuario**	Seleccione **Add (Añadir)** para añadir los usuarios de origen o grupos de usuarios que están sujetos a la política: • **any**: incluye todo el tráfico independientemente de los datos de usuario. • **pre-logon**: incluye a usuarios remotos conectados a la red mediante GlobalProtect pero que no han iniciado sesión en su sistema. Cuando se configura la opción Pre-logon (anterior al inicio de sesión) en el portal de endpoints de GlobalProtect, cualquier usuario que no esté registrado en su equipo en ese momento se identificará con el nombre de usuario anterior al inicio de sesión. Puede crear estas políticas para usuarios anteriores al inicio de sesión y, aunque el usuario no haya iniciado sesión directamente, sus equipos estarán autenticados en el dominio como si hubieran iniciado sesión completamente. • **known-user (usuario conocido)**: Incluye a todos los usuarios autenticados, es decir, cualquier dirección IP con

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		datos de usuario asignados. Esta opción es equivalente al grupo de usuarios del dominio en un dominio. • **unknown (desconocido)**: incluye a todos los usuarios desconocidos, es decir, las direcciones IP que no estén asignadas a un usuario. Por ejemplo, podría utilizar **unknown (desconocido)** para el acceso de invitados a alguna parte porque tendrán una dirección IP en su red, pero no se autenticarán en el dominio y no tendrán ninguna información de asignación de dirección IP a nombre de usuario en el cortafuegos. • **Select (Seleccionar)**: incluye los usuarios seleccionados en esta ventana. Por ejemplo, puede que quiera añadir a un usuario, una lista de individuos, algunos grupos o añadir usuarios manualmente. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*
Perfil HIP de origen	**Usuario**	**Añada** perfiles de información de host (HIP) para recopilar información sobre el estado de seguridad de sus hosts de extremo, como por ejemplo si tienen instalados los parches de seguridad y las definiciones de antivirus más recientes. El uso de los perfiles de información del host para la aplicación de políticas posibilita una seguridad granular que garantiza que los hosts remotos que acceden a sus recursos críticos posean un mantenimiento adecuado y conforme a sus normas de seguridad antes de que se les permita acceder a los recursos de su red. Los siguientes perfiles de origen HIP son compatibles: • **any (cualquiera)**: Incluye cualquier endpoint, independientemente de la informacion HIP. • **select (selecto)**: incluye perfiles HIP seleccionados según lo determina su configuración. Por ejemplo, puede añadir un perfil HIP, una lista de perfiles HIP o añadir perfiles HIP manualmente. • **no-hip (sin hip)**: No se requiere información HIP. Esta configuración permite el acceso desde clientes de terceros que no pueden recopilar o enviar información HIP.
Zona de destino	**IP Destino**	Haga clic en **Add (Añadir)** para añadir zonas de destino (el valor predeterminado es **Any [Cualquiera]**). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing,

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases. *En las reglas de intrazona, no puede definir una zona de destino porque estos tipos de reglas solo pueden hacer coincidir tráfico con un origen y un destino dentro de la misma zona. Para especificar las zonas que coincidan con una regla de intrazona, solo debe especificar la zona de origen.*
Dirección de destino		Haga clic en **Add (Añadir)** para añadir direcciones de destino, grupos de direcciones o regiones (la opción predeterminada es **Any [Cualquiera]**). Seleccione entre las opciones del menú desplegable o seleccione el objeto **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** (en la parte inferior del menú desplegable) para especificar los ajustes de dirección. Objects (Objetos) >Addresses (Direcciones) y Objects (Objetos) >AddressGroups (Grupos de direcciones) describen los tipos de objetos de direcciones y grupos de direcciones, respectivamente, que admiten una regla de política de seguridad. Al seleccionar la opción **Negate (Negar)**, la regla se aplicará a las direcciones de destino de la zona especificada, con la excepción de las direcciones especificadas.
Application (Aplicación)	**Application (Aplicación)**	Haga clic en **Add (Añadir)** para añadir aplicaciones específicas a la regla de la política de seguridad. Si una aplicación tiene múltiples funciones, puede seleccionar una aplicación general o aplicaciones individuales. Si selecciona la aplicación general, se incluirán todas las funciones y la definición de la aplicación se actualizará automáticamente a medida que se añadan futuras funciones. Si utiliza grupos de aplicaciones, filtros o contenedores en la regla de la política de seguridad, podrá ver la información detallada de estos objetos pasando el ratón por encima del objeto en la columna Application (Aplicación), abriendo el menú desplegable y seleccionando **Value (Valor)**. De esta forma podrá ver miembros de la aplicación directamente desde la política, sin tener que desplazarse a las pestañas **Object**. *Siempre especifique una o más aplicaciones para que solo se permitan en la red las aplicaciones que usted desea, lo cual reduce la superficie de ataque y le brinda mayor control sobre el tráfico de la red No configure la aplicación en any (cualquiera), lo que permite el tráfico de cualquier*

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		aplicación y aumenta la superficie de ataque.
service	**Categoría de URL/servicio**	Seleccione los servicios que desea limitar a números de puertos TCP o UDP concretos. Seleccione una de las siguientes opciones de la lista desplegable: • **Any (Cualquiera)**: las aplicaciones seleccionadas se permiten o deniegan en cualquier protocolo o puerto. • **application-default (valor predeterminado de aplicación)**: las aplicaciones seleccionadas se permiten o deniegan únicamente según sus **puertos definidos por Palo Alto Networks** predeterminados. Esta opción se recomienda para políticas de permiso porque impide que las aplicaciones se ejecuten en puertos y protocolos no habituales, que si no es a propósito, puede ser una señal de comportamiento y uso de aplicaciones no deseados. *Al utilizar esta opción, el cortafuegos sigue comprobando todas las aplicaciones en todos los puertos, pero las aplicaciones solo tienen permiso en sus puertos y protocolos predeterminados.* *Para la mayoría de las aplicaciones, utilice application-default (predeterminado-de-aplicación) para evitar que la aplicación utilice puertos no estándar o que exhiba otros comportamientos evasivos.* *Si el puerto predeterminado para la aplicación cambia, el cortafuegos actualiza automáticamente la regla con el puerto predeterminado correcto. Para las aplicaciones que usan puertos no estándar, tal como aplicaciones personalizadas internas, modifique la aplicación o cree una regla que especifique los puertos no estándares, y aplique la regla únicamente al tráfico que requiera la aplicación.* • **Select (Selecto)**: haga clic en **Add (Añadir)** para añadir un servicio existente o seleccione **Service (Servicio)** o **Service Group (Grupo de servicios)** para especificar una nueva entrada. (O seleccione Objects > Services y Objects > Service Groups).
URL Category (Categoría de URL)		Seleccione las categorías URL de la regla de seguridad. • Seleccione **any (cualquiera)** para permitir o denegar todas las sesiones, con independencia de la categoría URL. • Para especificar una categoría, haga clic en **Add (Añadir)** y seleccione una o varias categorías concretas (incluso

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		categorías personalizadas) de la lista desplegable. Selecione Objects > External Dynamic Lists Para definir categorías personalizadas.
Configuración de acción	**Acciones**	En **Action (Acción)**, seleccione la acción que el cortafuegos llevará a cabo sobre el tráfico que coincida con los atributos definidos en una regla: • **Allow (Permitir)**: (predeterminado) permite el tráfico coincidente. • **Deny (Denegar)**: bloquea el tráfico coincidente y aplica la acción predeterminada *Deny (Denegar)* definida para la aplicación denegada. Para ver la acción de denegación definida de manera predeterminada para una aplicación, consulte la información detallada de la aplicación (**Objects [Objetos]** > **Applications [Aplicaciones]**). Dado que la acción de denegación predeterminada varía según la aplicación, el cortafuegos podría bloquear la sesión y enviar un restablecimiento para una aplicación, mientras que podría descartar la sesión silenciosamente para otra aplicación. • **Drop (Descartar)**: descarta la aplicación silenciosamente. No se envía un restablecimiento de TCP al host o la aplicación, a menos que seleccione **Send ICMP Unreachable (Enviar ICMP inalcanzable)**. • **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. • **Send ICMP Unreachable (Enviar ICMP inalcanzable)**: solo disponible en interfaces de capa 3. Cuando configura una regla de seguridad para descartar tráfico o restablecer la conexión, el tráfico no alcanza el host de destino. En dichos casos, para todo el tráfico de UDP y para el tráfico de TCP descartado, puede habilitar el cortafuegos para enviar una respuesta inalcanzable de ICMP a la dirección IP de origen donde se originó el tráfico. Habilitar este ajuste permite que el origen cierre o borre la sesión correctamente y evita que las aplicaciones fallen. Para ver la tasa de paquetes inalcanzables de ICMP configurada en el cortafuegos, consulte Session Settings (Configuración de sesión) (**Device [Dispositivo]** > **Setup [Configuración]** > **Session [Sesión]**).

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		Para anular la acción predeterminada definida en las reglas de interzona e intrazona predefinidas, consulte Cancelación o reversión de una regla de la política de seguridad.
Ajuste de perfil	**Acciones**	Para especificar la comprobación adicional que realiza el cortafuegos en los paquetes que coinciden con la regla del perfil de seguridad, seleccione los perfiles individuales de antivirus, antispyware, protección contra vulnerabilidades, filtrado de URL, bloqueo de archivos, filtrado de datos, análisis de WildFire, protección de GTP y protección de SCTP. Para especificar un grupo de perfiles en lugar de perfiles individuales, seleccione **Profile Type Group (Grupo de tipos de perfil)** y, a continuación, seleccione **Group Profile (Perfil de grupo)**. Para definir nuevos perfiles o grupos de perfiles, haga clic en **New (Nuevo)** junto al perfil o grupo adecuado (consulte Objects > Security Profiles > GTP Protection). También puede adjuntar perfiles de seguridad (o grupos de perfiles) a las reglas predeterminadas.
Configuración del log y otras configuraciones	**Acciones**	Para generar entradas de tráfico en el log de tráfico local que cumplan esta regla, seleccione las siguientes opciones: • **Log At Session Start (Log al iniciar sesión)** (opción deshabilitada de manera prederminada): genera una entrada en el log de tráfico para el inicio de una sesión. *No habilite Log at Session Start (Log al iniciar sesión), excepto para fines de solución de problemas o para que los logs de sesión de túnel muestren túneles GRE activos en el ACC. La creación de logs al final de la sesión consume menos recursos e identifica la aplicación exacta si la aplicación cambia después de algunos paquetes; por ejemplo, de la base de Facebook al chat de Facebook.* • **Log At Session End (Log al finalizar sesión)** (opción deshabilitada de manera prederminada): genera una entrada en el log de tráfico para el final de una sesión. *Si las entradas de inicio o fin de la sesión se registran, también lo harán las entradas de colocación y denegación.* • **Log Forwarding (Reenvío de logs)**: para reenviar el log de tráfico local y las entradas de log de amenazas a destinos remotos, como servidores de Panorama y Syslog, seleccione **Log Forwarding Profile (Perfil de reenvío de logs)**.

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		La generación de entradas de log de amenazas está determinada por los perfiles de seguridad. Para definir nuevos perfiles de log, haga clic en New (Nuevo) como sea necesario (consulte Objects [Objetos] > Log Forwarding [Reenvío de logs]*).* *Cree y habilite los perfiles de reenvío de logs para enviar logs a dispositivos de almacenamiento externo específicos. Esto permite conservar los logs, debido a que el cortafuegos posee espacio de almacenamiento limitado para logs y, cuando el espacio se agota, el cortafuegos descarta los logs más antiguos.* También puede cambiar la configuración del log en las reglas predeterminadas. Especifique cualquier combinación de las siguientes opciones: • **Schedule (Programar)**: Para limitar los días y horas en los que la regla está en vigor, seleccione una programación de la lista desplegable. Para definir nuevos programas, haga clic en **New (Nuevo)** según sea necesario (consulte Configuración para controlar el tráfico SSL descifrado). • **QoS Marking (Marca de QoS)**: para cambiar el ajuste de Calidad de servicio (Quality of Service, QoS) en paquetes que coincidan con la regla, seleccione **IP DSCP** o **IP Precedence (Precedencia de IP)** e introduzca el valor de QoS en formato binario o seleccione un valor predeterminado de la lista desplegable. Para obtener más información sobre QoS, consulte Calidad del servicio. • **Disable Server Response Inspection (Deshabilitar inspección de respuesta de servidor)**: deshabilita la inspección de paquetes desde el servidor hacia el cliente. La opción está deshabilitada de manera predeterminada. *Para obtener una mejor postura de seguridad, no habilite Disable Server Response Inspection (Deshabilitar inspección de respuesta de servidor). Si selecciona esta opción, el cortafuegos solo inspecciona los flujos de cliente a servidor. No inspecciona los flujos de servidor a cliente y, por lo tanto, no puede identificar si existen amenazas en esos flujos de tráfico.*
Básicas	**Rule Usage (Uso de reglas)**	• **Rule Created (Regla creada)**: fecha y hora de creación de la regla.

© 2020 Palo Alto Networks, Inc.

Bloques de creación de una regla de seguridad	Configurado en	Description (Descripción)
		• **Last Edited (Última edición)**: última fecha y hora en que la regla fue editada.
Actividad	**Rule Usage (Uso de reglas)**	• **Hit Count (Recuento de resultados)**: la cantidad total de veces que el tráfico coincidió con la regla (cada vez que se obtuvo un resultado). • **First Hit (Primer resultado)**: hora de la primera coincidencia con la regla. • **Last Hit (Último resultado)**: hora de la última coincidencia con la regla.
applications	**Rule Usage (Uso de reglas)**	• **Applications Seen (Aplicaciones vistas)**: la cantidad de aplicaciones que admite la regla. • **Last App Seen (Última aplicación vista)**: la cantidad de días desde que se vio en la regla la última aplicación nueva (una aplicación que no se había visto antes). • **Compare Applications & Applications Seen (Comparar aplicaciones y aplicaciones vistas)**: haga clic en esta opción para comparar las aplicaciones configuradas en la regla con las aplicaciones vistas en la regla. Utilice esta herramienta para descubrir las aplicaciones que coinciden con la regla y para añadir aplicaciones a la regla.
Tráfico (últimos 30 días)	**Rule Usage (Uso de reglas)**	• **Bytes**: la cantidad de tráfico en la regla en los últimos 30 días, en bytes. *Un periodo mayor a 30 días haría que las reglas más antiguas quedaran al principio de la lista, ya que probablemente sean las que tengan más tráfico acumulado. Esto puede hacer que las reglas más nuevas se enumeren a continuación de las más antiguas, incluso si las reglas más nuevas observan un tráfico intenso.*

Creación y gestión de políticas

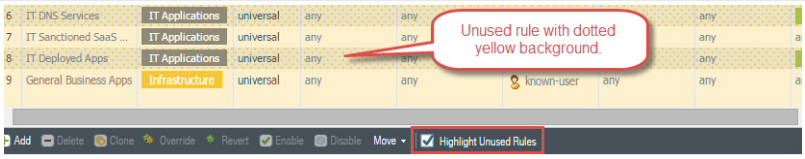
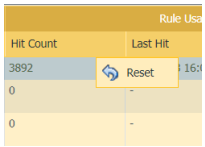
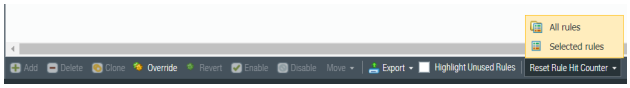
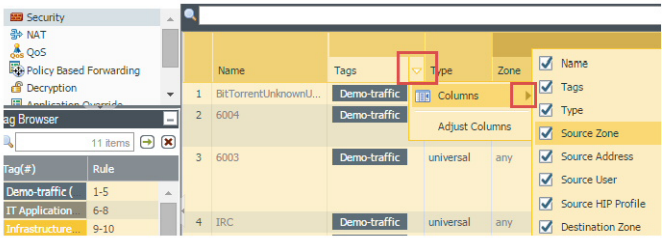
Seleccione la página **Policies (Políticas)** > **Security (Seguridad)** para añadir, modificar y gestionar políticas de seguridad:

Tarea	Description (Descripción)
Añadir	Seleccione **Add (Añadir)** para añadir una nueva regla de política o seleccionar una regla sobre la cual basar una regla nueva y, a continuación, **Clone Rule (Duplicar regla)**. La regla copiada, "regla *n*" se inserta debajo de la regla seleccionada, donde *n*es el siguiente número entero disponible que hace que el nombre de la regla sea único. Para obtener más información sobre la duplicación, consulte Traslado o duplicación de una regla de política.

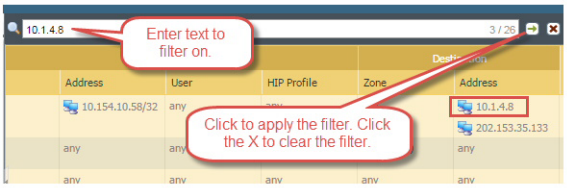
© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Modificar	Seleccione una regla para modificar su configuración. Si la regla se ha enviado desde Panorama, la regla será de solo lectura en el cortafuegos y no podrá editarse de forma local.
	Las acciones **Override (Cancelar)** y **Revert (Revertir)** únicamente pertenecen a las reglas predeterminadas que se muestran en la parte inferior de la base de reglas de seguridad. Estas reglas predefinidas (que permiten todo el tráfico de intrazona y rechazan todo el tráfico de interzona) indican al cortafuegos cómo debe gestionar el tráfico que no coincida con ninguna otra regla de la base de reglas. Como son parte de la configuración predefinida, debe cancelarlas con la opción **Override (Cancelar)** para editar la configuración de política seleccionada. Si utiliza Panorama, también puede **Override (Anular)** las reglas predeterminadas y, a continuación, enviarlas a los cortafuegos de un grupo de dispositivos o contexto compartido. También puede **Revert (Revertir)** las reglas predeterminadas, lo que restaura la configuración predefinida o la configuración enviada a Panorama. Para obtener más información, consulte Cancelación o reversión de una regla de política de seguridad.
Movimiento	Las reglas se evalúan de manera descendente y en orden en la página **Policies (Políticas)**. Para cambiar el orden en el que las reglas se evalúan con respecto al tráfico de red, seleccione una regla y haga clic en **Move Up (Mover hacia arriba)**, **Move Down (Mover hacia abajo)**, **Move Top (Mover a la parte superior)**, **Move Bottom (Mover a la parte inferior)** o **Move to a different rulebase or device group (Mover a una base de reglas o grupo de dispositivos diferente)**. Para obtener más información, consulte Traslado o duplicación de una regla de política.
Copiar UUID	Copie el identificador único universal (Universal Unique Identifier, UUID) en el portapapeles para usarlo al buscar la configuración o los logs.
delete	Seleccione y haga clic en **Delete (Eliminar)** para eliminar una regla existente.
Habilitar/ deshabilitar	Para deshabilitar una regla, selecciónela y haga clic en **Disable (Deshabilitar)** para deshabilitarla. Para habilitar una regla que está deshabilitada, selecciónela y haga clic en **Enable (Habilitar)**.
Monitor Rule Usage (Supervisar el uso de las reglas)	Para identificar las reglas que no se utilizan desde la última vez que el cortafuegos se reinició, seleccione **Highlight Unused Rules (Resaltar reglas no utilizadas)**. A continuación, podrá decidir si desea **Disable (Deshabilitar)** una regla o **Delete (Eliminar)** dicha regla. Las reglas que actualmente no están en uso se muestran con un fondo amarillo. Cuando el recuento de resultados de la regla de la política está habilitado, los datos del recuento de resultados se utilizan para determinar si una regla no se utiliza. *Cada cortafuegos mantiene una marca de tráfico para las reglas que tienen una coincidencia. Dado que la marca se restablece cuando se produce un restablecimiento del plano de datos al reiniciar, la práctica recomendada es supervisar esta lista periódicamente para determinar si la regla ha tenido una coincidencia desde la última comprobación, antes de eliminarla o deshabilitarla.*

© 2020 Palo Alto Networks, Inc.

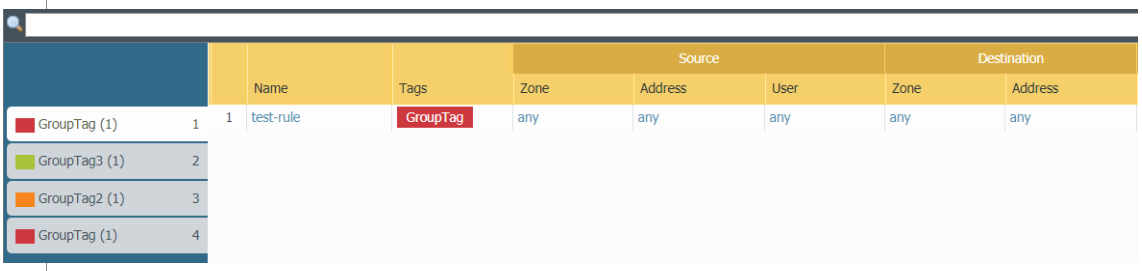
Tarea	Description (Descripción)
	
Reset rule Hit Count (Restablecer recuento de resultados de regla)	El valor de **Hit Count (Recuento de resultados)** registra el valor total de resultados de tráfico en la regla de la política. El recuento total de resultados de tráfico permanece tras el reinicio, la actualización y el reinicio del plano de datos. Para restablecer el recuento de resultados de una regla concreta, expanda la lista desplegable y haga clic en **Reset (Restablecer)** para restablecer el recuento.  O bien, seleccione **Reset Rule Hit Counter (Restablecer recuento de resultados de regla)** (menú de la parte inferior). Para borrar las estadísticas de recuento de resultados, seleccione **All Rules (Todas las reglas)** o seleccione reglas concretas y restablezca las estadísticas de recuento de resultados solo para las **Selected rules (Reglas seleccionadas)**.  Vea el primer valor en **First Hit (Primer resultado)** para identificar el primer resultado de la política de seguridad. La fecha se introduce con el formato fecha hh:mm:ss año. No puede restablecer este valor. Vea el último valor en **Last Hit (Último resultado)** para identificar la última utilización de la política de seguridad. La fecha se introduce con el formato fecha hh:mm:ss año. No puede restablecer este valor.
Mostrar/ ocultar columnas	Muestre u oculte las columnas que se muestran en **Policies (Políticas)**. Seleccione el nombre de la columna para alternar la visualización. 
Apply filters (Aplicar filtros)	Para aplicar un filtro a la lista, selecciónelo de la lista desplegable **Filter Rules (Reglas de filtro)**. Para definir un filtro, elija **Filter (Filtro)** en la lista desplegable de elementos. *Las reglas predeterminadas no son parte del filtro de la base de reglas y siempre aparecen en la lista de reglas filtradas.*

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	Para ver las sesiones de red registradas como coincidencias con respecto a la política, seleccione **Log Viewer (Visor de log)** en la lista desplegable del nombre de regla.
	Para visualizar el valor actual, elija **Value (Valor)** en la lista desplegable de la entrada. También puede editar, filtrar o eliminar elementos directamente desde el menú de la columna. Por ejemplo, para ver las direcciones incluidas en un grupo de direcciones, pase el cursor por encima del objeto en la columna **Address (Dirección)** y seleccione **Value (Valor)** en la lista desplegable. Esto le permitirá ver rápidamente los miembros y las direcciones IP correspondientes del grupo de direcciones sin tener que navegar a la pestaña **Object (Objeto)**.
	Para buscar objetos utilizados dentro de una política basándose en su nombre o dirección IP, utilice el filtro. Luego de aplicar el filtro, verá solo los elementos que coinciden con el filtro. El filtro también funciona con objetos incrustados. Por ejemplo, cuando filtra con 10.1.4.8, solo se muestra la política que contiene esa dirección: 
Reglas de vista previa (únicamente Panorama)	Utilice **Preview Rules (Vista previa de las reglas)** para ver una lista de las reglas antes de enviarlas a los cortafuegos gestionados. En cada base de reglas, la jerarquía de las mismas se marca visualmente para cada grupo de dispositivos (y cortafuegos gestionado), lo que permite revisarlas entre un gran número de reglas.
Export Configuration Table (Exportar la tabla de configuración)	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la base de la regla de la política como **PDF/CSV**. Puede aplicar filtros para crear resultados más específicos de la configuración de la tabla cuando sea necesario; por ejemplo, para las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.
Resaltar regla no utilizada	Resalte una regla de política sin coincidencias de tráfico en la columna **Rule Usage (Utilización de regla)**.
Grupo	Gestione grupos de etiquetas cuando tenga la casilla **View Rulebase as Groups (Ver base de reglas como grupos)** marcada. Puede realizar las siguientes acciones: • **Move rules in group to different rulebase or device group (Mover reglas del grupo a una base de reglas o grupo de dispositivos diferente)**: traslade el grupo de etiquetas seleccionado a un grupo de dispositivos diferente. • **Change group of all rules (Cambiar grupo de todas las reglas)**: mueva las reglas del grupo de etiquetas seleccionado a un grupo de etiquetas diferente de la base de reglas. • **Delete all rules in group (Eliminar todas las reglas en el grupo)**: elimine todas las reglas dentro del grupo de etiquetas seleccionado. • **Delete all rules in group (Eliminar todas las reglas en el grupo)**: elimine todas las reglas dentro del grupo de etiquetas seleccionado.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Ver base de reglas como grupos	Seleccione **View Rulebase as Groups (Ver base de reglas como grupos)** para visualizar la base de reglas de política usando la etiqueta utilizada en **Group Rules by Tag (Agrupar reglas por etiquetas)**. Las reglas de política visibles son aquellas que pertenecen al grupo de etiquetas seleccionado.
Coincidencia de política de pruebas	Realice una prueba de las políticas de protección para la base de reglas de política seleccionada para comprobar que se ha rechazado y permitido el tráfico correspondiente.



Cancelación o reversión de una regla de política de seguridad

Las reglas de seguridad predeterminadas, predeterminada entre zonas y predeterminada intrazona, tienen ajustes predefinidos que puede cancelar en un cortafuegos o en Panorama. Si un cortafuegos recibe las reglas predeterminadas de un grupo de dispositivos, también puede cancelar los ajustes del grupo de dispositivos. El cortafuegos o sistema virtual donde realice la cancelación almacena una versión local de la regla en su configuración. Los ajustes que puede cancelar son un subconjunto del conjunto completo (la tabla siguiente indica el subconjunto de reglas de seguridad). Para obtener información acerca de las reglas de seguridad predeterminadas, consulte Policies > Security.

Para cancelar una regla, seleccione **Policies (Políticas)** > **Security (Seguridad)** en un cortafuegos o **Policies (Políticas)** > **Security (Seguridad)** > **Default Rules (Reglas predeterminadas)** en Panorama. La columna Name muestra el icono de herencia ( ) de las reglas que puede cancelar. Seleccione la regla, haga clic en **Override (Cancelar)** y edite los ajustes en la tabla siguiente.

Para revertir una regla anulada a sus ajustes predefinidos o a los ajustes introducidos desde un grupo de dispositivos de Panorama, seleccione **Policies (Políticas)** > **Security (Seguridad)** en un cortafuegos o **Policies (Políticas)** > **Security (Seguridad)** > **Default Rules (Reglas predeterminadas)** en Panorama. La columna Name muestra el icono de cancelación ( ) de las reglas que tienen valores cancelados. Seleccione la regla, haga clic en **Revert (Revertir)** y haga clic en **Sí** para confirmar la operación.

Campos para cancelar una regla de seguridad predeterminada	Description (Descripción)
Pestaña General	
Nombre	El **Name (Nombre)** que identifica la regla es de solo lectura; no puede cancelarlo.
Tipo de regla	El **Rule Type (Tipo de regla)** es de solo lectura; no puede cancelarlo.
Description (Descripción)	La **Description (Descripción)** es de solo lectura; no puede cancelarla.

© 2020 Palo Alto Networks, Inc.

Campos para cancelar una regla de seguridad predeterminada	Description (Descripción)
Tag (Etiqueta)	Seleccione **Tags (Etiquetas)** en la lista desplegable. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de descifrado específicas de etiqueta con las palabras descifrado y sin descifrado o utilizar el nombre de un centro de datos específico para políticas asociadas a esa ubicación.
Pestaña Acciones	
Configuración de acción	Seleccione la opción **Action (Acción)** adecuada para el tráfico que coincida con la regla. • **Allow (Permitir)**: (predeterminado) permite el tráfico. • **Deny (Denegar)**: bloquea el tráfico y aplica la acción predeterminada Denegar que se define para la aplicación que el cortafuegos está denegando. Para ver la acción de denegación definida de manera predeterminada para una aplicación, consulte la información detallada de la aplicación en **Objects (Objetos)** > **Applications (Aplicaciones)**. • **Drop (Descartar)**: descarta la aplicación silenciosamente. El cortafuegos no envía un mensaje de restablecimiento de TCP al host o la aplicación. • **Reset client (Restablecer cliente)**: envía un mensaje de restablecimiento de TCP al dispositivo de la parte del cliente. • **Reset server (Restablecer servidor)**: envía un mensaje de restablecimiento de TCP al dispositivo de la parte del servidor. • **Reset both (Restablecer ambos)**: envía un mensaje de restablecimiento de TCP tanto al dispositivo de la parte del cliente como al de la parte del servidor.
Ajuste de perfil	**Profile Type (Tipo de perfil)**: asigne perfiles o grupos de perfiles a la regla de seguridad: • Para especificar la comprobación que realizan los perfiles de seguridad predeterminados, seleccione **Profiles** y, a continuación, seleccione uno o más perfiles individuales de **Antivirus**, **Vulnerability Protection**, **Anti-Spyware**, **URL Filtering**, **File Blocking**, **Data Filtering** y **WildFire Analysis**. • Para asignar un grupo de perfiles, en lugar de perfiles individuales, seleccione **Group (Grupo)** y, a continuación, seleccione un **Group Profile (Perfil de grupo)** en la lista desplegable. • Para definir nuevos perfiles (Objects > Security Profiles) o grupos de perfiles (Objects > Security Profiles > GTP Protection), haga clic en **New (Nuevo)** en el menú desplegable del grupo o perfil correspondiente.
Ajuste de log	Especifique cualquier combinación de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

Campos para cancelar una regla de seguridad predeterminada	Description (Descripción)

	• **Log Forwarding (Reenvío de logs)**: Para enviar el log del tráfico local y las entradas del log de amenazas a destinos remotos, como servidores de Panorama y Syslog, seleccione un perfil de **Log forwarding (Reenvío de logs)** de la lista desplegable. Los perfiles de seguridad determinan la generación de entradas en el log Amenaza. Para definir un nuevo perfil de **Log Forwarding (Reenvío de logs)**, seleccione **Profile (Perfil)** en el menú desplegable (consulte Objects > Log Forwarding).
	• Para generar entradas de tráfico en el log de tráfico local que cumplan esta regla, seleccione las siguientes opciones:
	  • **Log at Session Start (Log al iniciar sesión)**: genera una entrada en el log de tráfico al inicio de la sesión (seleccionado de manera predeterminada).
	  • **Log at Session End (Log al finalizar sesión)**: genera una entrada en el log de tráfico al final de la sesión (no seleccionado de manera predeterminada).
	  Si configura el cortafuegos para incluir entradas al inicio o al final de una sesión en el log de tráfico, también incluirá entradas de descarte y denegación.

Aplicaciones y uso

- Políticas > Seguridad > Optimizador de políticas > Sin aplicación especificada > Comparar (o haga clic en el número en **Aplicaciones vistas)**
- Políticas > Seguridad > Optimizador de políticas > Aplicaciones no usadas > Comparar (o haga clic en el número en **Aplicaciones vistas)**
- Seleccione Políticas > Seguridad y haga clic en el número en **Aplicaciones vistas**.

En la pestaña Uso de la regla de política de seguridad, puede entrar también en **Comparar aplicaciones y aplicaciones vistas** para acceder a las herramientas que le ayudan a migrar desde reglas de la política de seguridad basadas en puertos hacia reglas de política de seguridad basadas en aplicaciones, y a eliminar de las reglas las aplicaciones no usadas en **Aplicaciones y uso**.

Campo	Description (Descripción)
Intervalo de tiempo	El periodo para la información de la aplicación: • **Anytime (En cualquier momento)**: muestra las aplicaciones vistas durante la vigencia de la regla. • **Past 7 days (Últimos 7 días)**: muestra únicamente las aplicaciones vistas en los últimos 7 días. • **Past 15 days (Últimos 15 días)**: muestra únicamente las aplicaciones vistas en los últimos 7 días. • **Past 30 days (Últimos 30 días)**: muestra únicamente las aplicaciones vistas en los últimos 30 días.
Aplicaciones en regla	Las aplicaciones configuradas en la regla o **cualquiera**, si no hubiera aplicaciones específicas configuradas en la regla. Para las

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	aplicaciones, puede seleccionar **Browse (Examinar)**, **Add (Añadir)** y **Delete (Eliminar)**, según fuera necesario, y las aplicaciones se configuran en una regla; el número encerrado en un círculo junto a Apps on Rule (Aplicaciones en regla) indica cuántas hay. El añadir aplicaciones desde esta ubicación es igual que añadir aplicaciones en la pestaña **Application (Aplicación)** de la regla de política de seguridad.
Aplicaciones vistas	Todas las aplicaciones vistas y permitidas en el cortafuegos que coincidan con la regla. El número en el círculo junto a Apps Seen (Aplicaciones vistas) indica cuántas aplicaciones se vieron en la regla. • **Applications (Aplicaciones)**: las aplicaciones vistas en la regla. Por ejemplo, si una regla permite el tráfico de navegación web (aplicaciones en regla), puede ver numerosas aplicaciones en la lista debido a que hay numerosas aplicaciones de navegación web. • **Subcategory (Subcategoría)**: la subcategoría de la aplicación. • **Risk (Riesgo)**: la calificación de riesgo de la aplicación. • **First Seen (Primera vez vista)**: el primer día que la aplicación se vio en la red. • **Last Seen (Última vez vista)**: el día más reciente que la aplicación se vio en la red. *La granularidad de la medición para la primera y última visualización es un día, por lo cual, el día que define una regla, el primer día y el último día son el mismo día.* • **Traffic (30 days) (Tráfico [30 días])**: la cantidad de tráfico en bytes que se vio en los últimos 30 días. *Un periodo más prolongado haría que las reglas más antiguas quedaran al principio de la lista, ya que probablemente sean las que tengan más tráfico acumulado. Esto puede hacer que las reglas más nuevas se enumeren a continuación de las más antiguas, incluso si las reglas más nuevas observan un tráfico intenso.*
Acciones para las aplicaciones vistas	Acciones que puede realizar en **Apps Seen (Aplicaciones vistas)**: • **Create Cloned Rule (Crear regla duplicada)**: duplica la regla actual. Al migrar desde reglas basadas en puertos a reglas basadas en aplicaciones, duplique primero la regla basada en puertos y luego edite la duplicación para crear la regla de lista de permitidos basada en aplicaciones. La regla duplicada se inserta por encima de la regla basada en puertos en la lista de políticas. Use este método de migración para garantizar que no se deniegue accidentalmente el tráfico que desea permitir; si la regla duplicada no permite todas las aplicaciones que necesita, la regla basada en puertos que sigue sí las permite.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Supervise la regla basada en puertos y ajuste la regla basada en aplicaciones (duplicada), según fuera necesario. Una vez que se haya asegurado de que la regla basada en aplicaciones permite el tráfico que desea y que solo el tráfico no deseado se filtra a través de la regla basada en puertos, puede eliminar de manera segura la regla basada en puertos. • **Añadir a esta regla**: Añade aplicaciones desde Aplicaciones vistas en la regla. El añadir aplicaciones a la regla transforma una regla configurada para coincidir con **cualquier** aplicación (una regla basada en puertos) en una regla basada en aplicaciones que permita las aplicaciones que usted especifica (la nueva regla basada en aplicaciones reemplaza a la regla basada en puertos). Las aplicaciones que no añade a la regla son denegadas, al igual que cualquier otra regla de lista de permitidos basada en aplicaciones. Asegúrese de identificar todas las aplicaciones que desea permitir y añadirlas a la regla, para no denegar accidentalmente una aplicación. • **Añadir a regla existente**: Añade aplicaciones desde Aplicaciones vistas a una regla basada en aplicaciones (App-ID). Esto le permite duplicar una regla basada en App-ID a partir de una regla basada en puerto y, a continuación, añadir más aplicaciones vistas en reglas basadas en puerto a la regla de App-ID más adelante. • **Match Usage (Hacer coincidir el uso)**: mueve todas las aplicaciones vistas en la regla (se enumeran en Apps on Rule [Aplicaciones en regla] después de que usted **hace coincidir el uso**). Si tiene la certeza de que la regla debe permitir *todas* las aplicaciones enumeradas, **Match Usage (Hacer coincidir el uso)** es muy conveniente. Sin embargo, no debe ninguna duda de que todas las aplicaciones enumeradas son aplicaciones que desea permitir en la red. Si se han visto numerosas aplicaciones en la regla (por ejemplo, en una regla que permite la navegación web), es mejor duplicar la regla y cambiar a una regla basada en aplicaciones. **Match Usage (Hacer coincidir el uso)** funciona correctamente para las reglas simples con aplicaciones conocidas. Por ejemplo, si una regla basada en puertos para el puerto 22 solo ha visto tráfico SSH (que es lo único que debería ver), es seguro **hacer coincidir el uso**.

Cuadro de diálogo Clone (Duplicar)
Cuadro de Añadir a esta regla
Cuadro de diálogo Añadir aplicaciones a regla existente
	Cuando selecciona las aplicaciones en **Apps Seen (Aplicaciones vistas)** y **Create Cloned Rule (Crear regla duplicada)** o **Add to Rule (Añadir a regla)** que tienen aplicaciones relacionadas, estos cuadros de diálogo detallan lo siguiente:
	• **Nombre** (solo cuadros de diálogo para Duplicar y Añadir aplicaciones a regla existente).
	  • Duplicar: Introduzca el nombre de la nueva regla duplicada.
	  • Añadir aplicaciones a regla existente: Seleccione la regla a la que añadir aplicaciones en el menú desplegable o especifique el nombre de la regla.
	• **Applications (Aplicaciones)**

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• Añadir aplicación de contenedor (predeterminado): Active casillas de verificación de todas las aplicaciones de contenedor, las aplicaciones vistas en la regla y las aplicaciones en el contenedor que no han sido vistas en la regla. • Añadir aplicaciones específicas vistas: Permite seleccionar solo las aplicaciones que realmente se ven en la regla y anula la selección de todo lo demás. Puede seleccionar manualmente aplicaciones de contenedor y otras aplicaciones. • **Aplicación**: • Las aplicaciones seleccionadas que se ven en la regla, resaltadas en verde. • Las aplicaciones de contenedor, resaltadas en gris, con sus aplicaciones individuales indicadas a continuación. • Las aplicaciones individuales en un contenedor que se ven en la regla, pero que no se seleccionaron en **Aplicaciones y uso** (texto normal). • Las aplicaciones individuales en un contenedor que no se han visto en la regla (*cursiva*). • La fecha en la que se **vieron por última vez** las aplicaciones en la regla. • **Aplicaciones dependientes**: • La casilla de verificación para añadir dependencias de aplicaciones está marcada de manera predeterminada, debido a que estas aplicaciones son necesarias para que se ejecute la aplicación seleccionada. • **Depends On (Depende de)**: lista de las aplicaciones dependientes para las aplicaciones seleccionadas. Las aplicaciones que seleccionó requieren estas aplicaciones dependientes para funcionar. • **Required By (Exigida por)**: indica la aplicación que necesita la aplicación dependiente (**Depends On [Depende de]**). (En ocasiones, una aplicación dependiente, a su vez, requiere otra aplicación dependiente). Los cuadros de diálogo **Duplicar**, **Añadir a regla** y **Añadir aplicaciones a regla existente** ayudan a garantizar que las aplicaciones no se interrumpan y le permite asegurarse de que las aplicaciones funcionen en el futuro, al incluir aplicaciones individuales relevantes que estén relacionadas con las aplicaciones que está duplicando o añadiendo a una regla.

Optimizador de política de seguridad

- Policies (Políticas) > Security (Seguridad) > Policy Optimizer (Optimizador de política)

Policies (Políticas) > **Security (Seguridad)** > **Policy Optimizer (Optimizador de política)** muestra lo siguiente:

© 2020 Palo Alto Networks, Inc.

- **No App Specified (Sin aplicación especificada)**: reglas que tienen la aplicación configurada como **any (cualquiera)**, de manera que pueda identificar las reglas basadas en puertos para convertirlas en reglas basadas en aplicaciones.
- **Unused Apps (Aplicaciones no utilizadas)**: reglas que incluyen aplicaciones que nunca coincidieron con la regla.

Campo	Description (Descripción)
Nombre	El nombre de la regla de política de seguridad.
service	Cualquier servicio asociado con la regla de política de seguridad.
Tráfico (Bytes, 30 días)	**Traffic (30 days) (Tráfico [30 días])**: la cantidad de tráfico en bytes que se vio en los últimos 30 días. *Un periodo más prolongado haría que las reglas más antiguas quedaran al principio de la lista, ya que probablemente sean las que tengan más tráfico acumulado. Esto puede hacer que las reglas más nuevas se enumeren a continuación de las más antiguas, incluso si las reglas más nuevas observan un tráfico intenso.*
Aplicaciones permitidas	Las aplicaciones que permite la regla. Abra el cuadro de diálogo **Application (Aplicación)**, en el cual puede añadir y eliminar aplicaciones sobre la regla.
Aplicaciones vistas	La cantidad de aplicaciones vistas en la regla. Haga clic en el número para abrir el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**, que le permite comparar las aplicaciones configuradas en la regla con las aplicaciones vistas en la regla y modificar las aplicaciones.
Day with No New Apps (Días sin aplicaciones nuevas)	Cantidad de días desde que la última aplicación nueva se vio en la regla.
Comparar	Abre el cuadro de diálogo **Applications & Usage (Aplicaciones y uso)**, para comparar las aplicaciones configuradas en la regla con las aplicaciones vistas en la regla y modificar las aplicaciones.
Last Hit (Último resultado)	Última vez que el tráfico coincidió con la regla.
First Hit (Primer resultado)	Primera vez que el tráfico coincidió con la regla.
Modificado	La fecha y hora de la última modificación de la regla.
Creado	La fecha y hora de creación de la regla.

© 2020 Palo Alto Networks, Inc.

Políticas > NAT

Si define interfaces de capa 3 en el cortafuegos, puede configurar una política de traducción de direcciones de red (NAT) para especificar si los puertos y las direcciones IP de origen y destino se convierten entre puertos y direcciones públicos y privados. Por ejemplo, las direcciones de origen privadas se pueden traducir a direcciones públicas en el tráfico enviado desde una zona interna (fiable) a una zona pública (no fiable). NAT también es compatible en interfaces de cable virtual.

Las reglas NAT se basan en las zonas de origen y destino, en las direcciones de origen y destino, y en el servicio de aplicación (como HTTP). Al igual que las políticas de seguridad, las reglas de política NAT se comparan con el tráfico entrante en secuencia, y se aplica la primera regla que coincida con el tráfico.

A medida que sea necesario, añada rutas estáticas al enrutador local para enrutar el tráfico a todas las direcciones públicas hacia el cortafuegos. Es posible que también necesite añadir reglas estáticas a la interfaz de destino en el cortafuegos para reducir el tráfico en la dirección privada.

Las tablas siguientes describen los ajustes de NAT y NPTv6 (traducción de prefijo de red de IPv6 a IPv6):

- Pestaña General de políticas NAT
- Pestaña Paquete original de NAT
- Pestaña Paquete traducido de NAT
- Pestaña Enlace HA Activo/Activo de NAT

¿Busca más información?

Consulte NAT.

Pestaña General de políticas NAT

- **Policies (Políticas)** > **NAT** > **General (General)**

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política NAT o NPTv6. También puede configurar una etiqueta para que le permita ordenar o filtrar políticas cuando existan numerosas políticas. Seleccione el tipo de política NAT que está creando, lo que influirá en los campos que estarán disponibles en las pestañas **Original Packet (Paquete original)** y **Translated Packet (Paquete traducido)**.

Regla NAT: Configuración de General	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la regla (hasta 1024 caracteres).
Tag (Etiqueta)	Si desea añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta.

© 2020 Palo Alto Networks, Inc.

Regla NAT: Configuración de General	Description (Descripción)
	Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
NAT Type (Tipo de NAT)	Especifique el tipo de traducción: • **ipv4**: la traducción entre direcciones IPv4. • **nat64**: la traducción entre direcciones IPv6 y IPv4. • **nptv6**: la traducción entre prefijos IPv6. No puede combinar intervalos de direcciones IPv4 e IPv6 en una única regla NAT.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.

Pestaña Paquete original de NAT

- Policies > NAT > Original Packet

Utilice la pestaña **Original Packet (Paquete original)** para definir las zonas de origen y destino de los paquetes que el cortafuegos traducirá y, de manera opcional, especifique la interfaz de destino y el tipo de servicio. Puede configurar múltiples zonas de origen y destino del mismo tipo y puede aplicar la regla a redes específicas o direcciones IP específicas.

Regla NAT: Configuración de Original Packet	Description (Descripción)
Source Zone / Destination Zone	Seleccione una o más zonas de origen y destino para el paquete original (no NAT). (El valor predeterminado es **Any (Cualquiera)**.) Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede especificar múltiples zonas para simplificar la gestión. Por ejemplo, puede configurar los ajustes para que múltiples direcciones NAT internas se dirijan a la misma dirección IP externa.
Interfaz de destino	Especifique la interfaz de destino de los paquetes que traduce el cortafuegos. Puede usar la interfaz de destino para traducir direcciones IP de manera diferente en caso de que la red esté conectada a dos proveedores de Internet con grupos diferentes de direcciones IP.

© 2020 Palo Alto Networks, Inc.

Regla NAT: Configuración de Original Packet	Description (Descripción)
service	Especifique el servicio para el cual el cortafuegos traduce las direcciones de origen o destino. Para definir un nuevo grupo de servicios, seleccione Objects > Service Groups.
Source Address / Destination Address	Especifique una combinación de direcciones de origen y destino que traducirá el cortafuegos. Para NPTv6, los prefijos configurados para **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)** deben tener el formato xxxx:xxxx::/yy. La dirección no puede tener definida una parte de identificador de interfaz (host). El intervalo admitido de longitudes de prefijo es de /32 a /64.

Pestaña Paquete traducido de NAT

- Policy > NAT > Translated Packet

Para la traducción de la dirección de origen, seleccione la pestaña **Translated Packet (Paquete traducido)** para determinar el tipo de traducción que se realizará en el origen, la dirección y posiblemente el puerto al cual se traducirá el origen.

También puede habilitar la traducción de dirección de destino de un host interno para permitir el acceso a él desde una dirección IP pública. En este caso, usted define una dirección de origen pública y una dirección de destino en la pestaña **Original Packet (Paquete original)** para un host interno, y en la pestaña **Translated Packet (Paquete traducido)**, configura la **Static IP (IP estática)** o **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesión])** e introduce la **Translated Address (Dirección traducida)**. Luego, cuando se acceda a la dirección pública, se traducirá a la dirección interna (de destino) del host interno.

Regla NAT: Configuración de Translated Packet	Description (Descripción)
Traducción de dirección de origen	Seleccione el **Translation Type (Tipo de traducción)** (grupo de direcciones dinámicas o estáticas) e introduzca una dirección IP o un intervalo de direcciones IP (dirección1 a dirección2) a las que se traducirá la dirección de origen (**Translated Address [Dirección traducida]**). El tamaño del intervalo de direcciones está limitado por el tipo del grupo de direcciones: • **Dynamic IP And Port (IP dinámica y puerto)**: la selección de direcciones se basa en un hash de la dirección de IP de origen. Para una dirección de IP de origen, el cortafuegos utiliza la misma dirección de origen traducida para todas las sesiones. La NAT de origen de IP dinámica y puerto (Dynamic IP and Port, DIPP) admite aproximadamente 64 000 sesiones simultáneas en cada dirección IP del grupo de NAT. Algunos modelos admiten un exceso de suscripciones, lo que permite a una única IP albergar más de 64 000 sesiones simultáneas. La NAT de DIPP de Palo Alto Networks® admite más sesiones de NAT que las admitidas por el número de puertos y direcciones IP disponibles. Con una suscripción excesiva, el cortafuegos puede usar combinaciones de puertos y direcciones IP dos veces simultáneamente en los cortafuegos PA-220, PA-820, PA-850, VM-50, VM-300 y VM-1000-HV, cuatro veces simultáneamente en

© 2020 Palo Alto Networks, Inc.

Regla NAT: Configuración de Translated Packet	Description (Descripción)
	los cortafuegos PA-5220 y PA-3200 Series, y ocho veces simultáneamente en los cortafuegos PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-500 y VM-700 cuando las direcciones IP de destino son únicas. • **Dynamic IP (IP dinámica)**: se traduce en la siguiente dirección disponible en el intervalo especificado, pero el número de puerto permanece sin cambios. Se admiten hasta 32 000 direcciones IP consecutivas. Un grupo de direcciones IP dinámicas puede contener varias subredes, por lo que podrá traducir sus direcciones de red internas a dos o más subredes públicas diferentes. • **Advanced (Dynamic IP/Port Fallback) (Avanzado [método alternativo de IP dinámica/puerto])**: utilice esta opción para crear un grupo alternativo que ejecutará la traducción de IP y puerto, y que se utilizará si el grupo principal agota sus direcciones. Puede definir las direcciones del grupo utilizando la opción **Dirección traducida** o **Dirección de interfaz**; la última opción es para interfaces que reciben una dirección IP dinámica. Cuando cree un grupo alternativo, asegúrese de que las direcciones no se solapen con las direcciones del grupo principal.
Traducción de la dirección de origen (continuación)	• **Static IP (IP estática)**: siempre se utiliza la misma dirección para la traducción y el puerto permanece inalterable. Por ejemplo, si el intervalo de origen es de 192.168.0.1 a 192.168.0.10 y el intervalo de traducción es de 10.0.0.1 a 10.0.0.10, la dirección 192.168.0.2 siempre se traduce a 10.0.0.2. El intervalo de dirección es casi ilimitado. Debe utilizar la traducción de **Static IP (IP estática)** para la traducción de dirección de origen de NPTv6. En NPTv6, los prefijos configurados para **Translated Address (Dirección traducida)** deben estar en formato xxxx:xxxx::/aa y la dirección no puede tener una porción de identificador de interfaz (host) definida. El intervalo admitido de longitudes de prefijo es de /32 a /64. • **None (Ninguna)**: La traducción no se ejecuta.
Bidireccional	(Opcional) Habilite la traducción bidireccional para una traducción de dirección de origen de **IP estática** si quiere que el cortafuegos cree una traducción correspondiente (NAT o NPTv6) en la dirección opuesta de la traducción que configure. *Si habilita la traducción bidireccional, debe asegurarse de tener establecidas políticas de seguridad para controlar el tráfico en ambas direcciones. Sin tales políticas, la función bidireccional permite que se traduzcan paquetes automáticamente en ambas direcciones.*
Traducción de dirección de destino	Configure las siguientes opciones para que cortafuegos realicen la NAT de destino. Por lo general, la NAT de destino se utiliza para permitir que un servidor interno, como un servidor de correo electrónico, sea accesible desde la red pública.
Translation Type and Translated Address (Tipo de traducción	Seleccione el tipo de traducción que realiza el cortafuegos en la dirección de destino: • **None (Ninguno)** (predeterminado)

© 2020 Palo Alto Networks, Inc.

Regla NAT: Configuración de Translated Packet	Description (Descripción)
y dirección traducida)	• **Static IP (IP estática)**: introduzca una **Dirección traducida** como una dirección IP o un intervalo de direcciones IP y un número de **Puerto traducido** (de 1 a 65535) al que la dirección de destino y el número de puerto originales se traducirán. Si el campo **Translated Port (Puerto traducido)** se deja en blanco, el puerto de destino no se modifica. Para NPTv6, los prefijos configurados para **Translated Address (Dirección traducida)** del prefijo de destino deben tener el formato xxxx:xxxx::/aa. La dirección no puede tener definida una parte de identificador de interfaz (host). El intervalo admitido de longitudes de prefijo es de /32 a /64. *El puerto traducido no es compatible con NPTv6 porque esta es una traducción de prefijo estricta. La sección de direcciones de puerto y host sencillamente se reenvía sin cambios.* *La traducción de IP estática para IPv4 también le permite habilitar la reescritura de DNS (que se describe a continuación).* • **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])**: seleccione o introduzca una **Translated Address (Dirección traducida)** que sea un FQDN, un objeto de dirección o un grupo de direcciones desde las cuales el cortafuegos selecciona la translated address (Dirección traducida). Si el servidor DNS devuelve más de una dirección para un FQDN o si el objeto de dirección o el grupo de direcciones se traducen en más de una dirección IP, el cortafuegos distribuye las sesiones entre esas direcciones utilizando el **Session Distribution Method (Método de distribución de sesiones)** especificado.
Session Distribution Method (Método de distribución de sesiones)	Si selecciona la traducción NAT de destino para que sea **IP dinámica (con distribución de sesión)**, es posible que la dirección traducida de destino (a un FQDN, objeto de dirección o grupo de direcciones) pueda resolverse en más de una dirección. Puede elegir cómo el cortafuegos distribuye (asigna) las sesiones entre esas direcciones para proporcionar una distribución de sesiones más equilibrada: • **Round Robin (Operación por turnos)**: (valor predeterminado) asigna nuevas sesiones a las direcciones IP de forma rotativa. A menos que su entorno le exija elegir uno de los demás métodos de distribución, utilice ese método. • **Source IP Hash (Hash IP de origen)**: asigna nuevas sesiones en función de un hash de direcciones IP de origen. Si tiene tráfico entrante de una única dirección IP dde origen, seleccione un método que no sea **Source IP Hash (Hash IP de origen)**. • **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**: asigna sesiones nuevas usando un hash de las direcciones IP de origen y destino. • **Least Sessions (Últimas sesiones)**: asigna sesiones nuevas a la dirección IP que tiene la menor cantidad de sesiones simultáneas. Si tiene numerosas sesiones de corta duración, **Últimas sesiones** le proporcionará una distribución más equilibrada de las sesiones.

© 2020 Palo Alto Networks, Inc.

Regla NAT: Configuración de Translated Packet	Description (Descripción)
Habilitar reescritura DNS	En PAN-OS 9.0.2 y versiones 9.0 posteriores, si el tipo de regla de políticas de NAT de destino es **ipv4** y el tipo de traducción de la dirección de destino es **IP estática**, la opción **Habilitar reescritura de DNS** está disponible. Puede habilitar la reescritura de DNS si usa la NAT de destino y también usa los servicios de DNS en un lado del cortafuegos para resolver los FQDN para un cliente en el otro lado del cortafuegos. Cuando la respuesta de DNS atraviesa el cortafuegos, este reescribe la dirección IP en la respuesta de DNS, en relación con la dirección de destino original o la dirección de destino traducida que coincide con la respuesta de DNS en la regla de políticas de NAT. Una sola regla de políticas de NAT hace que el cortafuegos aplique NAT en paquetes que coincidan con la regla y en las direcciones IP en respuestas de DNS que coincidan con la regla. Debe especificar cómo el cortafuegos ejecuta NAT en la dirección IP en la respuesta de DNS relacionada con la regla de NAT: inverso o directo. • **inverso**: (predeterminado) si el paquete es una respuesta de DNS que 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 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. • **directo**: (predeterminado) 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 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.

Pestaña Enlace HA Activo/Activo de NAT

- Policies > NAT > Active/Active HA Binding

La pestaña Active/Active HA Binding solo está disponible si el cortafuegos está en una configuración activa o activa de alta disponibilidad (HA). En esta configuración, debe enlazar cada regla de NAT de origen (tanto si se trata de NAT estático como dinámico) a los ID de dispositivo 0 o 1; debe enlazar cada regla de NAT de destino al ID de dispositivo **0**, **1**, **both (ambos)** (ID de dispositivo 0 y 1) o bien al cortafuegos active-**primary (activo-principal)**.

Seleccione una configuración **Active/Active HA Binding (Enlace HA activo/activo)** para enlazar la regla de NAT a un cortafuegos de HA de la siguiente manera:

- **0**: enlaza la regla de NAT al cortafuegos que tiene un ID de dispositivo 0 de HA.
- **1**: enlaza la regla de NAT al cortafuegos que tiene un ID de dispositivo 1 de HA.
- **both (ambos)**: enlaza la regla NAT al cortafuegos que tiene el ID de dispositivo 0 de HA y al cortafuegos que tiene el ID de dispositivo 1 de HA. Esta configuración no admite la IP dinámica ni la IP dinámica y NAT de puerto.
- **primary (primario)**: enlaza la regla de NAT al cortafuegos que está en estado activo-primario de HA. Esta configuración no admite la IP dinámica ni la IP dinámica y NAT de puerto.

En general, configurará las reglas de NAT específicas para un dispositivo cuando los dos peers HA tienen grupos únicos de direcciones IP de NAT.

Cuando el cortafuegos crea una nueva sesión, el enlace HA determina qué regla de NAT puede coincidir con la sesión. El enlace debe incluir al propietario de la sesión para que la regla coincida. El cortafuegos de la configuración de sesión realiza la coincidencia de regla de NAT pero la sesión se compara a las reglas

© 2020 Palo Alto Networks, Inc.

de NAT que están enlazadas con el propietario de sesión y traducidas de acuerdo a una de las reglas. En el caso de reglas específicas de dispositivo, un cortafuegos salta todas las reglas de NAT que no están enlazadas con el propietario de sesión. Por ejemplo, el cortafuegos con ID de dispositivo 1 es el propietario de la sesión y el cortafuegos de configuración de sesión. Cuando ID de dispositivo 1 intenta que la sesión coincida con una regla de NAT, este ignora todas las reglas enlazas al ID de dispositivo 0.

Si un peer falla, el segundo peer continúa procesando el tráfico para las sesiones sincronizadas del peer que falló, incluidas las traducciones de NAT. Palo Alto Networks recomienda crear un duplicado de la regla de NAT que esté asocoada al segundo ID de dispositivo. De esta manera, existirán dos reglas de NAT con las mismas direcciones de traducción de origen y de destino; una regla enlazada a cada ID de dispositivo. Esta configuración le permite al peer de HA llevar a cabo la nueva configuración de sesión y realizar la coincidencia de la regla de NAT para las reglas de NAT que están enlazas a su ID de dispositivo. Sin un duplicado de la regla de NAT, el peer en funcionamiento intentará realizar la coincidencia de política de NAT, pero la sesión no coincidirá con las propias reglas específicas del dispositivo del cortafuegos y este omitirá todas las demás reglas de NAT que no estén enlazas con su ID de dispositivo.

¿Busca más información?

Consulte NAT en modo HA activo/activo

© 2020 Palo Alto Networks, Inc.

Políticas > QoS

Añada reglas de políticas de QoS para definir el tráfico que recibe un tratamiento específico de QoS y asignar una clase de QoS para cada regla de política de QoS con el fin de especificar que la clase de servicio asignada se aplica a todo el tráfico que coincida con la regla asociada cuando sale de una interfaz habilitada para QoS.

Las reglas de política de QoS introducidas a un cortafuegos desde Panorama aparecen en naranja y no se pueden modificar a nivel del cortafuegos.

Además, para habilitar completamente el cortafuegos para que proporcione QoS:

- Establezca los límites de ancho de banda para cada clase de servicio QoS (seleccione Network > Network Profiles > QoS para añadir o modificar un perfil de QoS).
- Active QoS en una interfaz (seleccione Network > QoS).

Consulte Calidad de servicio para obtener los flujos de trabajo completos, los conceptos y los casos de uso de QoS.

Añada una nueva regla o duplique una regla existente y, a continuación, defina los siguientes campos.

Configuración de regla de política de QoS	
Pestaña General	
Nombre	Introduzca un nombre para identificar la regla (hasta 63 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción opcional.
Tag (Etiqueta)	Si necesita añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de descifrado con las palabras descifrado y sin descifrado, o usar el nombre de un centro de datos específico para políticas asociadas con esa ubicación.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.

© 2020 Palo Alto Networks, Inc.

Configuración de regla de política de QoS	
Pestaña Origen	
Zona de origen	Seleccione una o más zonas de origen (el valor predeterminado es **any [cualquiera]**). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire).
Dirección de origen	Especifique una combinación de direcciones IPv4 o IPv6 de origen para las que se puede sobrescribir la aplicación identificada. Para seleccionar direcciones específicas, elija **select (sleccionar)** en la lista desplegable y realice cualquiera de las siguientes acciones: • Seleccione esta opción junto a las direcciones o grupos de direcciones pertinentes en la columna Available, y haga clic en **Add (Añadir)** para añadir sus selecciones a la columna Selected. • Introduzca los primeros caracteres de un nombre en el campo de búsqueda para mostrar todas las direcciones y todos los grupos de direcciones que comienzan con esos caracteres. Si selecciona un elemento de la lista, se habilita esta opción en la columna Available. Repita este proceso tantas veces como sea necesario y luego haga clic en **Add (Añadir)**. • Introduzca una o más direcciones IP (una por línea), con o sin máscara de red. El formato general es: *<ip_address>/<mask>* • Para eliminar direcciones, selecciónelas (columna Selected) y haga clic en **Delete (Eliminar) (Eliminar)** o seleccione **Any (Cualquiera)** para borrar todas las direcciones y los grupos de direcciones. Para añadir nuevas direcciones que se puedan utilizar en esta u otras políticas, haga clic en **New Address (Nueva dirección)**. Para definir nuevos grupos de direcciones, seleccione Objects > Address Groups.
Source User (Usuario de origen)	Especifique los grupos y usuarios de origen a los que se aplicará la política de QoS.
Negar	Seleccione esta opción para que esta política se aplique si la información especificada en esta pestaña no coincide.
Pestaña Destino	
Zona de destino	Seleccione una o más zonas de destino (el valor predeterminado es **any [cualquiera]**). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire).
Dirección de destino	Especifique una combinación de direcciones IPv4 o IPv6 de origen para las que se puede sobrescribir la aplicación identificada. Para seleccionar direcciones específicas, elija **select (sleccionar)** en la lista desplegable y realice cualquiera de las siguientes acciones: • Seleccione esta opción junto a las direcciones o grupos de direcciones pertinentes en la columna Available, y haga clic en **Add (Añadir)** para añadir sus selecciones a la columna Selected.

© 2020 Palo Alto Networks, Inc.

Configuración de regla de política de QoS	
	• Introduzca los primeros caracteres de un nombre en el campo de búsqueda para mostrar todas las direcciones y todos los grupos de direcciones que comienzan con esos caracteres. Si selecciona un elemento de la lista, se habilita esta opción en la columna Available. Repita este proceso tantas veces como sea necesario y luego haga clic en **Add (Añadir)**. • Introduzca una o más direcciones IP (una por línea), con o sin máscara de red. El formato general es: *<ip_address>/<mask>*. • Para eliminar direcciones, selecciónelas (columna Selected) y haga clic en **Delete (Eliminar) (Eliminar)** o seleccione **Any (Cualquiera)** para borrar todas las direcciones y los grupos de direcciones. Para añadir nuevas direcciones que se puedan utilizar en esta u otras políticas, haga clic en **New Address (Nueva dirección)**.
Negar	Seleccione esta opción para que esta política se aplique si la información especificada en esta pestaña no coincide.
Pestaña Application	
Application (Aplicación)	Seleccione aplicaciones específicas para la regla de QoS. Para definir nuevas aplicaciones o grupos de aplicaciones, seleccione **Objects (Objetos)** > **Applications (Aplicaciones)**. Si una aplicación tiene múltiples funciones, puede seleccionar una aplicación general o aplicaciones individuales. Si selecciona una aplicación general se incluirán todas las funciones y la definición de la aplicación se actualizará automáticamente a medida que se añadan futuras funciones. Si utiliza grupos de aplicaciones, filtros o un contenedor en la regla de QoS, podrá ver los detalles de estos objetos al pasar el ratón por encima del objeto en la columna Application, haciendo clic en la flecha hacia abajo y seleccionando **Value (Valor)**. De esta forma podrá ver fácilmente los miembros de la aplicación directamente desde la política, sin tener que ir a la pestaña **Objects (Objetos)**.
Pestaña Service/URL Category	
service	Seleccione los servicios para limitar números de puertos TCP y/o UDP concretos. Seleccione una de las siguientes opciones de la lista desplegable: • **Any (Cualquiera)**: las aplicaciones seleccionadas se permiten o deniegan en cualquier protocolo o puerto. • **application-default (valor predeterminado de aplicación)**: las aplicaciones seleccionadas se permiten o deniegan únicamente en los **puertos predefinidos por Palo Alto Networks**. Esta opción es la recomendada para políticas de permiso. • **Select (Seleccionar)**: haga clic en **Add (Añadir)**. Seleccione un servicio existente o seleccione **Service (Servicio)** o **Service Group (Grupo de servicios)** para especificar una nueva entrada.
URL Category (Categoría de URL)	Seleccione las categorías URL de la regla de QoS.

© 2020 Palo Alto Networks, Inc.

Configuración de regla de política de QoS	
	• Seleccione **Any (Cualquiera)** para garantizar que una sesión puede coincidir con esta regla de QoS independientemente de la categoría de URL. • Para especificar una categoría, haga clic en **Add (Añadir)** y seleccione una categoría específica (incluyendo una categoría personalizada) de la lista desplegable. Puede añadir varias categorías. Consulte Objects > External Dynamic Lists para obtener información sobre la definición de categorías personalizadas.
Pestaña DSCP/TOS	
Cualquiera	Seleccione la opción **Any (Cualquiera)** (predeterminada) para que la política coincida con el tráfico independientemente del valor Differentiated Services Code Point (DSCP) o la precedencia de IP/el tipo de servicio (Type of Service, ToS) definido para el tráfico.
Puntos de código	Seleccione **Codepoints (Puntos de código)** para permitir que el tráfico reciba un tratamiento de QoS basándose en el valor de DSCP o ToS definido en el encabezado IP de un paquete. Los valores de DSCP y ToS se utilizan para indicar el nivel de servicio solicitado para el tráfico, como la prioridad alta o la entrega de la mejor opción. El uso de codepoints como criterios de coincidencia en una política de QoS permite que una sesión reciba un tratamiento de QoS basándose en el codepoint detectado al inicio de la sesión. A continuación, seleccione **Add (Añadir)** para añadir codepoints con el fin de que el tráfico coincida con la política de QoS: • Otorgue a las entradas codepoint un **Name (Nombre)** descriptivo. • Seleccione el **Tipo** codepoint que desee utilizar como criterio de coincidencia para la política de QoS y, a continuación, seleccione un valor de **Codepoint (Punto de código)** específico. También puede crear un **Custom Codepoint (Punto de código personalizado)** introduciendo un **Codepoint name (Nombre de punto de código)** y un **Binary Value (Valor binario)**.
Pestaña Other Settings	
Clase	Seleccione la clase de QoS para asignar a la regla y haga clic en **OK (Aceptar)**. Las características de clase se definen en el perfil de QoS. Consulte Network > Network Profiles > QoS para obtener información acerca de la configuración de ajustes para clases de QoS.
Programa	• Seleccione **None (Ninguno)** para que la regla de política permanezca activa en todo momento. • Desde el menú desplegable, seleccione **Schedule [Programación]** (icono del calendario) para configurar un intervalo de tiempo único o un intervalo de tiempo recurrente durante el cual la regla estará activa.

© 2020 Palo Alto Networks, Inc.

Políticas > Reenvío basado en políticas

Normalmente, cuando el tráfico entra en el cortafuegos, el enrutador virtual de la interfaz de entrada indica la ruta que determina la interfaz de salida y la zona de seguridad de destino según la dirección IP de destino. Al crear una regla de reenvío basado en políticas (PBF), puede especificar otra información para determinar la interfaz de salida, incluida la zona, dirección y usuario de origen, así como la dirección, aplicación y servicio de destino. La sesión inicial de una dirección IP y puerto de destino concretos asociados con una aplicación no coincidirá con una regla de aplicación específica y se reenviarán de acuerdo con reglas PBF subsiguientes (que no especifican ninguna aplicación) o la tabla de reenvío del enrutador virtual. El resto de sesiones de esa dirección IP y puerto de destino de la misma aplicación coincidirán con una regla específica de aplicación. Para garantizar el reenvío mediante reglas PBF, no se recomienda el uso de reglas específicas de la aplicación.

Cuando sea necesario, las reglas PBF se pueden utilizar para forzar el tráfico mediante un sistema virtual adicional con la acción de reenvío Reenviar a Vsys. En este caso, es necesario definir una regla PBF adicional que reenvíe el paquete desde el sistema virtual de destino mediante una interfaz de salida concreta en el cortafuegos.

Las siguientes tablas describen la configuración de reenvío basado en políticas:

- Pestaña general de reenvío basado en políticas
- Pestaña de origen de reenvío basado en políticas
- Pestaña de Destino/Aplicación/Servicio de reenvío basado en políticas
- Pestaña de reenvío de reenvío basado en políticas

¿Busca más información?

Consulte Reenvío basado en políticas.

Pestaña general de reenvío basado en políticas

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política PBF. También puede configurar una pestaña para que le permita ordenar o filtrar políticas cuando estas son muy numerosas.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la política (hasta 1024 caracteres).
Tag (Etiqueta)	Si necesita añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de descifrado con las palabras descifrado y sin descifrado,

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	o usar el nombre de un centro de datos específico para políticas asociadas con esa ubicación.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.

Pestaña de origen de reenvío basado en políticas

Seleccione la pestaña **Source (Origen)** para definir la zona de origen o la dirección de origen que define el tráfico de origen entrante al que se aplicará la política de reenvío.

Campo	Description (Descripción)
Zona de origen	Para elegir zonas de origen (el valor predeterminado es cualquiera), haga clic en **Add (Añadir)** y seleccione una opción del menú desplegable. Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases. *Solo se admiten zonas de tipo Capa 3 para reenvío basado en políticas.*
Dirección de origen	Haga clic en **Add (Añadir)** para añadir las direcciones, direcciones de grupos o regiones de origen (la opción predeterminada es Cualquiera). Seleccione desde el menú desplegable o haga clic en **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** en la parte inferior del menú desplegable y especifique la configuración.
Source User (Usuario de origen)	Haga clic en **Add (Añadir)** para seleccionar los usuarios o grupos de usuarios de origen sometidos a la política. Los siguientes tipos de usuarios de origen son compatibles: • **Any (cualquiera)**: incluye todo el tráfico independientemente de los datos de usuario. • **pre-logon (anterior al inicio de sesión)**: incluye a usuarios remotos conectados a la red mediante GlobalProtect™, pero que no han iniciado sesión en su sistema. Cuando se configura la opción anterior al inicio de sesión en el portal de aplicaciones de GlobalProtect, cualquier usuario

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	que no esté registrado en su equipo en ese momento se identificará con el nombre de usuario anterior al inicio de sesión. Puede crear estas políticas para usuarios anteriores al inicio de sesión y, aunque el usuario no haya iniciado sesión directamente, sus equipos estarán autenticados en el dominio como si hubieran iniciado sesión completamente. • **known-user (usuario conocido)**: incluye a todos los usuarios autenticados, es decir, cualquier IP con datos de usuario asignados. Esta opción es equivalente al grupo "usuarios del dominio" en un dominio. • **unknown (desconocido)**: incluye a todos los usuarios desconocidos, es decir, las direcciones IP que no estén asignadas a un usuario. Por ejemplo, podría utilizar desconocido para acceso de invitados a alguna parte porque tendrán una IP en su red, pero no se autenticarán en el dominio y no tendrán ninguna información de asignación de dirección IP a usuario en el cortafuegos. • **Select (Seleccionar)**: incluye los usuarios seleccionados en esta ventana. Por ejemplo, puede que quiera añadir a un usuario, una lista de individuos, algunos grupos o añadir usuarios manualmente. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*

Pestaña de Destino/Aplicación/Servicio de reenvío basado en políticas

Seleccione la pestaña **Destination/Application/Service** para definir la configuración de destino que se aplicará al tráfico que coincida con la regla de reenvío.

Campo	Description (Descripción)
Dirección de destino	Haga clic en **Add (Añadir)** para añadir las direcciones o grupos de direcciones de destino (la opción predeterminada es any [cualquiera]). De manera predeterminada, esta regla se aplica a **cualquier** dirección IP. Seleccione en la lista desplegable o haga clic en **Address (Dirección)** o **Address Group (Grupo de direcciones)** en la parte inferior de la lista desplegable y especifique la configuración.
Aplicación/servicio	Seleccione aplicaciones o servicios específicos para la regla de PBF. Para definir nuevas aplicaciones, consulte Definición de aplicaciones. Para definir grupos aplicaciones, consulte Objects > Application Groups. *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.*

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Puede ver los detalles de estas aplicaciones al pasar el ratón por encima del objeto en la columna **Aplicación**, haciendo clic en la flecha hacia abajo y seleccionando **Valor**. De esta forma podrá ver fácilmente la información de la aplicación directamente desde la política, sin tener que ir hasta las pestañas de objetos. *No puede utilizar aplicaciones personalizadas, filtros de aplicaciones o grupos de aplicaciones en las reglas de PBF.*

Pestaña de reenvío de reenvío basado en políticas

Seleccione la pestaña **Forwarding (Reenvío)** para definir la acción y la información de red que se aplicará al tráfico que coincida con la política de reenvío. El tráfico se puede reenviar a una dirección IP de siguiente salto o un sistema virtual, o bien se puede interrumpir el tráfico.

Campo	Description (Descripción)
Acción	Seleccione una de las siguientes opciones: • **Forward (Reenviar)**: especifique la dirección IP del próximo salto y la interfaz de salida (egress) (la interfaz que toma el paquete para el siguiente salto especificado). • **Forward To VSYS (Reenviar a VSYS)**: seleccione el sistema virtual de reenvío en la lista desplegable. • **Discard (Descartar)**: descarta el paquete. • **No PBF (No hay ningún PBF)**: no altera la ruta que tomará el paquete. Esta opción excluye los paquetes que coincidan con los criterios de origen/destino/aplicación/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. *Utilice Forward (Reenviar) o Forward to VSYS (Reenviar al sistema virtual) como la acción, para aplicar un perfil de supervisión al tráfico. (No puede aplicar un perfil de supervisión cuando la acción no reenvía el tráfico). Los perfiles de supervisión supervisan la dirección IP. Si la conectividad con la dirección IP falla, los perfiles de supervisión especifican la acción.*
Interfaz de salida	Dirige el paquete a una interfaz de salida específica.
siguiente salto	Si dirige el paquete a una interfaz específica, especifique el próximo salto del paquete de alguna de las siguientes maneras: • **IP Address (Dirección IP)**: seleccione la dirección IP y seleccione un objeto de dirección (o cree un nuevo objeto de dirección) que utilice una dirección IPv4 o IPv6.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **FQDN**: seleccione FQDN y seleccione un objeto de dirección (o cree un nuevo objeto de dirección) que utilice un FQDN. • **None (Ninguno)**: no hay próximo salto; el paquete se descarta.
Monitor (Supervisar)	Habilite la monitorización para comprobar la conectividad con una **IP Address (Dirección IP)** de destino o con la dirección IP de **Next Hop (Siguiente salto)**. Seleccione **Monitor** y adjunte un **Profile (Perfil)** de supervisión (predeterminado o personalizado, **Network [Red]** > **Network Profiles [Perfiles de red]** > **Monitor [Supervisar]**) que especifique la acción cuando no se pueda alcanzar la dirección IP. *Configure perfiles de supervisión y habilite la supervisión para que, si la interfaz de salida o la ruta se desactivan, el cortafuegos realice la acción en el perfil y minimice o prevenga la interrupción del servicio.*
Forzar vuelta simétrica	(Necesario para entornos de enrutamiento asimétrico) Seleccione **Enforce Symmetric Return (Forzar vuelta simétrica)** e introduzca una o más direcciones IP en la lista **Next Hop Address (Dirección 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.
Programa	Para limitar los días y horas en los que la regla está en vigor, seleccione una programación del menú desplegable. Para definir nuevas programaciones, consulte Configuración para controlar el tráfico SSL descifrado.

© 2020 Palo Alto Networks, Inc.

Políticas > Descifrado

Puede configurar el cortafuegos para descifrar el tráfico con el fin de ganar visibilidad, control y seguridad granular. Las políticas de descifrado se pueden aplicar a una capa de sockets seguros (SSL), incluidos protocolos SSL encapsulados como IMAP(S), POP3(S), SMTP(S) y FTP(S), y a tráfico Secure Shell (SSH). El descifrado SSH se puede utilizar para descifrar el tráfico SSH entrante y saliente para asegurar que los protocolos no se están utilizando para túneles de aplicaciones y contenido no permitido.

Añada una regla de política de descifrado para definir el tráfico que desea descifrar (por ejemplo, puede descifrar el tráfico basado en la categorización de URL). Las reglas de política de descifrado se comparan con el tráfico en secuencias, por lo que las reglas más específicas deben preceder a las reglas más generales.

El descifrado de proxy de reenvío SSL requiere que se le presente al usuario la configuración de un certificado de confianza, si el servidor al que se conecta el usuario posee un certificado firmado por una CA de confianza del cortafuegos. Cree un certificado en la página **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** y, a continuación, haga clic en el nombre del certificado y seleccione **Forward Trust Certificate (Certificado de reenvío fiable)**.

El cortafuegos no descifra las aplicaciones que rompen el descifrado técnicamente; por ejemplo, debido a que usan certificados anclados o autenticación de cliente.

Consulte la Lista de aplicaciones excluidas del descifrado SSL.

Las siguientes tablas describen la configuración de políticas de descifrado:

- Pestaña general de descifrado
- Pestaña Origen de descifrado
- Pestaña de destino de descifrado
- Pestaña Categoría de URL/Servicio de descifrado
- Pestaña Opciones de descifrado

¿Busca más información?

Consulte Descifrado

Pestaña general de descifrado

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política de descifrado. También puede configurar una etiqueta para que le permita ordenar o filtrar políticas cuando exista una gran cantidad de políticas.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la regla (hasta 1024 caracteres).
Tag (Etiqueta)	Si necesita añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de descifrado con las palabras descifrado y sin descifrado, o usar el nombre de un centro de datos específico para políticas asociadas con esa ubicación.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.

Pestaña Origen de descifrado

Seleccione la pestaña **Source (Origen)** para definir la zona de origen o dirección de origen que define el tráfico de origen entrante al que se aplicará la política de descifrado.

Campo	Description (Descripción)
Zona de origen	Haga clic en **Add (Añadir)** para seleccionar las zonas de origen (la opción predeterminada es Cualquiera). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.
Dirección de origen	Haga clic en **Add (Añadir)** para añadir las direcciones, direcciones de grupos o regiones de origen (la opción predeterminada es Cualquiera). Seleccione desde el menú desplegable o haga clic en **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** en la parte inferior del menú desplegable y especifique la configuración. Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las configuradas.
Source User (Usuario de origen)	Haga clic en **Add (Añadir)** para seleccionar los usuarios o grupos de usuarios de origen sometidos a la política. Los siguientes tipos de usuarios de origen son compatibles: • **Any (cualquiera)**: incluye todo el tráfico independientemente de los datos de usuario.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **pre-logon (anterior al inicio de sesión)**: Incluye a usuarios remotos conectados a la red mediante GlobalProtect pero que no han iniciado sesión en su sistema. Cuando se configura la opción anterior al inicio de sesión en el portal de aplicaciones de GlobalProtect, cualquier usuario que no esté registrado en su equipo en ese momento se identificará con el nombre de usuario anterior al inicio de sesión. Puede crear estas políticas para usuarios anteriores al inicio de sesión y, aunque el usuario no haya iniciado sesión directamente, sus equipos estarán autenticados en el dominio como si hubieran iniciado sesión completamente. • **known-user (usuario conocido)**: incluye a todos los usuarios autenticados, es decir, cualquier IP con datos de usuario asignados. Esta opción es equivalente al grupo "usuarios del dominio" en un dominio. • **unknown (desconocido)**: incluye a todos los usuarios desconocidos, es decir, las direcciones IP que no estén asignadas a un usuario. Por ejemplo, podría usar desconocido para acceso de invitados a alguna parte porque tendrán una IP en su red, pero no se autenticarán en el dominio y no tendrán ninguna IP en la información de asignación de usuarios en el cortafuegos. • **Select (Seleccionar)**: incluye los usuarios seleccionados en esta ventana. Por ejemplo, puede que quiera añadir a un usuario, una lista de individuos, algunos grupos o añadir usuarios manualmente. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*

Pestaña de destino de descifrado

Seleccione la pestaña **Destination (Destino)** para definir la zona de destino o dirección de destino que define el tráfico de destino al que se aplicará la política.

Campo	Description (Descripción)
Zona de destino	Haga clic en **Add (Añadir)** para seleccionar las zonas de destino (la opción predeterminada es Cualquiera). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.
Dirección de destino	Haga clic en **Add (Añadir)** para añadir las direcciones, direcciones de grupos o regiones de destino (la opción predeterminada es Cualquiera). Seleccione desde el menú desplegable o haga clic en **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** en la parte inferior del menú desplegable

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	y especifique la configuración. Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las configuradas.

Pestaña Categoría de URL/Servicio de descifrado

Seleccione la pestaña **Service/URL Category (Categoría de URL/servicio)** para aplicar la política de descifrado al tráfico en función del número de puerto TCP o a cualquier categoría de URL (o una lista de categorías).

Campo	Description (Descripción)
service	Aplique la política de descifrado al tráfico en función de números de puertos TCP específicos. Seleccione una de las siguientes opciones de la lista desplegable: • **Any (Cualquiera)**: las aplicaciones seleccionadas se permiten o deniegan en cualquier protocolo o puerto. • **application-default (valor predeterminado de aplicación)**: las aplicaciones seleccionadas se descifrarán (o estarán exentas de descifrado) únicamente en los puertos predeterminados definidos para las aplicaciones por Palo Alto Networks. • **Select (Seleccionar)**: haga clic en **Add (Añadir)**. Seleccione un servicio existente o especifique un nuevo **Service (Servicio)** o **Service Group (Grupo de servicios)**. (O seleccione Objetos > Servicios y Objetos > Grupos de servicios).
Pestaña Categoría de URL	Seleccione las categorías URL de la regla de descifrado. • Seleccione **Any (Cualquiera)** para buscar en todas las sesiones, con independencia de la categoría URL. • Para especificar una categoría, haga clic en **Add (Añadir)** y seleccione una categoría específica (incluyendo una categoría personalizada) de la lista desplegable. Puede añadir varias categorías. Consulte la para obtener más información sobre cómo definir categorías personalizadas.

Pestaña Opciones de descifrado

Seleccione la pestaña **Options (Opciones)** para determinar si el tráfico coincidente debería descifrarse o no. Si se ha definido **Decrypt (Descifrar)**, especifique el tipo de descifrado. También puede añadir funciones de descifrado adicionales configurando o seleccionando un perfil de descifrado.

Campo	Description (Descripción)
Acción	Seleccione **Decrypt (descifrar)** o **No-decrypt (No descifrar)** para el tráfico.
Tipo	Seleccione el tipo de tráfico para descifrar del menú desplegable:

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **SSL Forward Proxy (Proxy SSL de reenvío)**: Especifique que la política descifrará el tráfico del cliente destinado a un servidor externo. • **SSH Proxy (Proxy SSH)**: Especifique que la política descifrará el tráfico SSH. Esta opción permite controlar los túneles SSH en políticas, especificando el ID de aplicación (App-ID) de túnel ssh. • **SSL Inbound Inspection (Inspección de entrada SSL)**: Especifique que la política descifrará el tráfico de inspección entrante SSL.
Perfil de descifrado	Adjunte un perfil de descifrado a la regla de la política para bloquear y controlar determinados aspectos del tráfico. Para obtener información acerca de la creación de un perfil de descifrado, seleccione Objetos > Perfil de descifrado.

© 2020 Palo Alto Networks, Inc.

Políticas> Inspección de túneles

Puede configurar el cortafuegos para que inspeccione el contenido del tráfico de los siguientes protocolos de túnel de texto no cifrado:

- Generic Routing Encapsulation (GRE)
- Protocolo de túneles de servicio general de paquetes vía radio (General Packet Radio Service, GPRS) para datos de usuario (GTP-U); solo se admite en los cortafuegos compatibles con GTP.
- Tráfico IPSec no codificado (algoritmo de cifrado nulo para IPSec y modo de transporte AH IPSec)
- Virtual Extensible LAN (VXLAN)

Puede utilizar la inspección del contenido del túnel para aplicar las políticas de seguridad, protección DoS y QoS en el tráfico en estos tipos de túneles y en el tráfico anidado dentro de otro túnel de texto no cifrado (por ejemplo, IPSec con cifrado nulo dentro de un túnel GRE).

Cree una política de inspección de túneles que, al comparar un paquete entrante, determine qué protocolos de túnel del paquete inspeccionará el cortafuegos y que especifique las condiciones en las que el cortafuegos descarta o continúa procesando el paquete. 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.

El cortafuegos admite la inspección de contenido de túnel en interfaces y subinterfaces Ethernet, interfaces AE, interfaces VLAN y túneles VPN y LSVPN. La función 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.

¿Qué desea saber?	Consulte:
¿Qué campos están disponibles para crear una política de inspección de túneles?	Componentes básicos de una política de inspección de túnel
¿Cómo puedo ver los logs de inspección del túnel?	Tipos de logs y niveles de gravedad
¿Busca más información?	Inspección del contenido del túnel

Componentes básicos de una política de inspección de túnel

Seleccione **Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** para añadir una regla de política de inspección de túnel. Puede utilizar el cortafuegos para inspeccionar el contenido de los protocolos de túnel de texto no cifrado (GRE, GTP-U, IPSec no cifrado y VXLAN) y aprovechar la inspección del contenido de túnel para aplicar políticas de seguridad, protección DoS y QoS en el tráfico de ese tipo de túneles. Todos los modelos de cortafuegos admiten la inspección de contenido de túnel de túneles GRE e IPSec no cifrados, pero solo los cortafuegos que admiten GTP admiten la inspección del contenido de túnel de túneles GTP-U. La tabla siguiente se describen los campos que se configuran para una política de inspección de túneles.

© 2020 Palo Alto Networks, Inc.

Componentes básicos de una política de inspección de túnel	Configurado en	Description (Descripción)
Nombre	**General**	Introduzca un nombre para la política de inspección de túneles que comience con un carácter alfanumérico y que contenga cero u otros caracteres alfanuméricos, guion bajo, guion, punto o espacio.
Description (Descripción)		(Opcional): introduzca una descripción para la política de inspección de túnel.
Etiquetas		(Opcional) Introduzca una o más etiquetas para informar y registrar que identifiquen los paquetes que están sujetos a la política de inspección de túneles.
Agrupar reglas por etiquetas		Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario		Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios		Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.
Zona de origen	**Source (Origen)**	Haga clic en **Add (Añadir)** para añadir una o varias zonas de paquetes a las que se aplica la política de inspección de túneles (el valor predeterminado es **Any [Cualquiera]**).
Dirección de origen		(Opcional) Para **Add (Añadir)** direcciones IPv4 o IPv6 de origen, grupos de direcciones u objetos de direcciones de georegiones de paquetes a los que se aplica la política de inspección de túneles (predeterminada es **Any (Cualquiera)**).
Source User (Usuario de origen)		(Opcional) Haga clic en **Add (Añadir)** para añadir usuarios de paquetes de origen a los que se aplica la política de inspección de túneles (el valor predeterminado es Any [Cualquiera]).
Negar		(Opcional) Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las especificadas.
Zona de destino	**IP Destino**	Seleccione **Add (Añadir)** para añadir una o varias zonas de paquetes de destino a los que se aplica la política de inspección de túneles (el valor predeterminad es **Any [Cualquiera]**).

© 2020 Palo Alto Networks, Inc.

Componentes básicos de una política de inspección de túnel	Configurado en	Description (Descripción)
Dirección de destino		(Opcional) Haga clic en **Add (Añadir)** para añadir direcciones IPv4 o IPv6 de destino, grupos de direcciones u objetos de direcciones de regiones geográficas de los paquetes a los que se aplica la política de inspección de túneles (el valor predeterminado es Any [Cualquiera]).
Negar		(Opcional) Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las especificadas.
Protocolo de túnel	**Inspección**	**Add (Añadir)** uno o más **Protocols (Protocolos)** de túnel que desea que el cortafuegos inspeccione: • **GRE**: El cortafuegos inspecciona los paquetes que utilizan Generic Route Encapsulation 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 no cifrado)**: El cortafuegos inspecciona los paquetes que usan IPSec no cifrado (Null Encrypted IPSec o IPSec AH en modo Transporte) en el túnel. • **VXLAN**: el cortafuegos inspecciona una carga VXLAN para encontrar el contenido encapsulado o las aplicaciones dentro del túnel. Para eliminar un protocolo de la lista, selecciónelo y haga clic en **Delete (Eliminar)**.
Niveles máximos de inspección de túnel	**Inspection (Inspección)** > **Inspect Options (Opciones de inspección)**	Especifique si el cortafuegos inspeccionará **One Level (Un nivel)** (predeterminado) o **Two Levels (Tunnel In Tunnel) (Dos niveles [túnel en túnel])** de encapsulación. Para VXLAN, seleccione **One Level (Un nivel)**, ya que la inspección solo se produce en la capa externa.
Descartar paquete si está por encima del nivel de inspección máximo del túnel		(Opcional) Descarte paquetes que contengan más niveles de encapsulación que los especificados para los niveles máximos de inspección de túnel.
Descartar paquete si el protocolo de túnel falla en la comprobación de cabecera estricta.		(Opcional) Descarte paquetes que contienen un protocolo de túnel que utiliza un encabezado que no es compatible con la RFC para ese protocolo. Los encabezados no compatibles pueden indicar paquetes sospechosos. Esta opción hace que el cortafuegos verifique los encabezados GRE contra RFC 2890. *No habilite esta opción si su cortafuegos utiliza túneles GRE con un dispositivo*

© 2020 Palo Alto Networks, Inc.

Componentes básicos de una política de inspección de túnel	Configurado en	Description (Descripción)
		que implementa una versión de GRE anterior a RFC 2890.
Descartar paquete si hay protocolo desconocido en el túnel		(Opcional) Descarte paquetes que contienen un protocolo dentro del túnel que el cortafuegos no puede identificar.
Devolución del túnel VXLAN escaneado al origen		(Opcional) Habilite esta opción para regresar el tráfico al endpoint de túnel VXLAN de origen (VTEP). Por ejemplo, utilice esta opción para regresar el paquete encapsulado al VTEP de origen. Solo es compatible en la capa 3, la subinterfaz de la capa 3, la capa 3 de interfaz agregada y VLAN.
Habilitar opciones de seguridad	**Inspection (Inspección) > Security Options (Opciones de seguridad)**	(Opcional) **Enable Security Options (Habilitar opciones de seguridad)** para asignar zonas de seguridad para el tratamiento independiente de la política de seguridad del contenido del túnel. El origen del contenido interno pertenecerá a la **Tunnel Source Zone (Zona de origen de túnel)** que especifique y el destino de contenido interno pertenecerá a la **Tunnel Destination Zone (Zona de destino del túnel)** que especifique. Si no selecciona **Enable Security Options (Habilitar opciones de seguridad)**, de manera predeterminada, el origen de contenido interno pertenece a la misma zona que el origen de túnel exterior y el destino de contenido interno pertenece a la misma zona que el destino del túnel exterior. Por lo tanto, tanto el origen de contenido interno como el de destino están sujetos a las mismas políticas de seguridad que se aplican a esas zonas de origen y de destino del túnel externo.
Tunnel Source Zone		Si selecciona la opción **Enable Security Options (Habilitar opciones de seguridad)**, seleccione una zona de túnel que creo y el contenido interno utilizará esta zona de origen para aplicar la política. De lo contrario, el origen de contenido interno predeterminado pertenece a la misma zona que el origen del túnel externo y las políticas de la zona de origen del túnel externo también aplican a la zona de origen de contenido interno.
Zonas de destino de túnel		Si selecciona la opción **Enable Security Options (Habilitar opciones de seguridad)**, seleccione una zona de túnel que creo y el contenido interno utilizará esta zona de destino para aplicar la política. De lo contrario, el destino de contenido interno predeterminado pertenece a la misma zona que el

© 2020 Palo Alto Networks, Inc.

Componentes básicos de una política de inspección de túnel	Configurado en	Description (Descripción)
		destino del túnel externo y las políticas de la zona de destino del túnel externo también aplican a la zona de destino de contenido interno.
Supervisar nombre	**Inspection (Inspección) > Monitor Options (Opciones de supervisión)**	(Opcional) Introduzca un nombre de supervisión para agrupar tráfico similar para supervisar el tráfico en logs e informes.
Supervisar etiqueta (número)		(Opcional) Introduzca un número de etiqueta de supervisión que puede agrupar tráfico similar para registrar e informar (intervalo 1 a 16.777.215). El número de etiqueta se define globalmente. *Este campo no se aplica al protocolo VXLAN. Los logs VXLAN usan automáticamente el identificador de red VXLAN (VXLAN Network Identifier, VNI) del encabezado VXLAN.*
Log al iniciar sesión		(Opcional) Seleccione esta opción para generar un log al inicio de la sesión de un túnel de texto no cifrado que coincida con la política de inspección del túnel. Esta configuración anula la configuración de log al iniciar sesión en la regla de la política de seguridad que aplica a la sesión. Los logs del túnel y los logs de tráfico se almacenan por separado. La información con la sesión de túnel externo (GRE, IPSec no cifrado o GTP-U) se almacena en los logs del túnel y los flujos de tráfico interno se almacenan en los logs de tráfico. Esta separación le permite informar con facilidad la actividad del túnel (a diferencia de la actividad de contenido interno) con las funciones de ACC y creación de informes. *La práctica recomendada para los logs de túnel es crear un log al inicio de la sesión y al final de la sesión debido a que en el caso de la creación de logs, 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 selecciona la opción Log at Session Start (Log al iniciar sesión), nunca verá si existe un túnel de GRE activo en el ACC.*
Log al finalizar sesión		(Opcional) Seleccione esta opción para capturar un log al final de una sesión de túnel de texto no cifrado que

© 2020 Palo Alto Networks, Inc.

Componentes básicos de una política de inspección de túnel	Configurado en	Description (Descripción)
		coincida con la política de inspección del túnel. Esta configuración anula la configuración de log al finalizar sesión en la regla de la política de seguridad que aplica a la sesión.
Log Forwarding		(Opcional) Seleccione un perfil de reenvío de logs de la lista desplegable para especificar adónde se reenvían los logs de inspección de túnel. (Esta configuración está separada de la configuración de reenvío de logs en una regla de la política de seguridad, que se aplica a los logs de tráfico).
Nombre	**ID de túnel** De manera predeterminada, si **no** configura un identificador VXLAN, se inspeccionará todo el tráfico. Si configura un identificador VXLAN, puede usarlo como criterio de coincidencia para restringir la inspección del tráfico a VNI específicos.	(**Opcional**) Un nombre que comience con un carácter alfanumérico y que contenga cero u otros caracteres alfanuméricos, guion bajo, guion, punto o espacio. El **nombre** describe los VNI que está agrupando. El nombre es un factor para mayor comodidad, no para la creación de logs, la supervisión o la creación de informes.
ID de VXLAN (VNI)		(Opcional) Introduzca un VNI único, una lista de VNI separados por coma, un intervalo de hasta 16 millones de VNI (usando el guion como separador) o una combinación de estas opciones. Por ejemplo: 1-54,1024,1677011-1677038,94 La cantidad máxima de identificadores VXLAN por política es 4096. Para conservar la memoria de configuración, use intervalos siempre que sea posible.

© 2020 Palo Alto Networks, Inc.

Policies > Application Override

Para cambiar la forma en la que el cortafuegos clasifica el tráfico de red en las aplicaciones, puede especificar políticas de cancelación de aplicación. Por ejemplo, si desea controlar una de sus aplicaciones personalizadas, puede utilizar una política de application override para identificar el tráfico de esa aplicación en función de la zona, dirección de origen y destino, puerto y protocolo. Si tiene aplicaciones de red clasificadas como "desconocidas", puede crear nuevas definiciones de aplicaciones (consulte Definición de aplicaciones).

Si fuera posible, evite el uso de políticas de cancelación de aplicaciones, ya que impiden que el cortafuegos utilice App-ID para identificar aplicaciones y que realicen inspecciones de capa 7 para detectar amenazas. Para admitir las aplicaciones exclusivas internas, se recomienda crear aplicaciones personalizadas *que incluyan la firma de aplicación, de manera que el cortafuegos realice una inspección de capa 7 y examine el tráfico de la aplicación en busca de amenazas. Si una aplicación comercial no tiene App-ID,* envíe una solicitud de un nuevo App-ID. *Si una definición de aplicación pública (firma o puertos predeterminados) cambia de manera que el cortafuegos ya no identifica la aplicación correctamente, cree un vale de soporte para que Palo Alto Networks pueda actualizar la definición. Mientras tanto, cree una aplicación para que el cortafuegos continúe realizando una inspección de capa 7 del tráfico.*

Al igual que las políticas de seguridad, las políticas de de cancelación de aplicación pueden ser tan generales o específicas como sea necesario. Las reglas de las políticas se comparan con el tráfico en secuencias, por lo que las reglas más específicas deben preceder a las reglas más generales.

Como el motor App-ID de PAN-OS clasifica el tráfico mediante la identificación del contenido específico de la aplicación en el tráfico de red, la definición de aplicación personalizada no puede utilizar un número de puerto para identificar una aplicación. La definición de la aplicación también debe incluir el tráfico (restringido por zona y dirección IP de origen, y zona y dirección IP de destino).

Para crear una aplicación personalizada con cancelación de aplicaciones:

- Creación de una aplicación personalizada (consulte Definición de aplicaciones). No es necesario especificar firmas para la aplicación si la aplicación se utiliza únicamente para reglas de application override.
- Defina una política de application override que especifique si la aplicación personalizada se debe activar. Una política suele incluir la dirección IP del servidor que ejecuta la aplicación personalizada y un conjunto restringido de direcciones IP o una zona de origen.

Use las siguientes tablas para configurar una regla de cancelación de aplicaciones.

- Pestaña general de anulación de aplicación
- Pestaña de origen de anulación de aplicación
- Pestaña de destino de anulación de aplicación
- Pestaña de aplicación/protocolo de anulación de aplicación

¿Busca más información?

Consulte Uso de objetos de aplicación en la política

Pestaña general de anulación de aplicación

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política de anulación de aplicación. También puede configurar una pestaña para que le permita ordenar o filtrar políticas cuando estas son muy numerosas.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la regla (hasta 1024 caracteres).
Tag (Etiqueta)	Si necesita añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de descifrado con las palabras descifrado y sin descifrado, o usar el nombre de un centro de datos específico para políticas asociadas con esa ubicación.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede optar por agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. El archivo de comentario de auditoría se puede exportar en formato CSV.

Pestaña de origen de anulación de aplicación

Seleccione la pestaña **Source (Origen)** para definir la zona de origen o dirección de origen que define el tráfico de origen entrante al que se aplicará la política de cancelación de aplicación.

Campo	Description (Descripción)
Zona de origen	Seleccione **Add (Añadir)** para añadir zonas de origen (el valor predeterminado es **Any [Cualquiera]**). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Dirección de origen	Seleccione **Add (Añadir)** para añadir direcciones de origen, grupos de direcciones o regiones (la opción predeterminada es **Any [Cualquiera]**). Seleccione desde el menú desplegable o haga clic en **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** en la parte inferior del menú desplegable y especifique la configuración. Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las configuradas.

Pestaña de destino de anulación de aplicación

Seleccione la pestaña **Destination (Destino)** para definir la zona de destino o dirección de destino que define el tráfico de destino al que se aplicará la política.

Campo	Description (Descripción)
Zona de destino	Haga clic en **Add (Añadir)** para seleccionar las zonas de destino (la opción predeterminada es Cualquiera). Las zonas deben ser del mismo tipo (capa 2, capa 3 o de cable virtual, Virtual Wire). Para definir nuevas zonas, consulte Network > Zones. Puede utilizar múltiples zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.
Dirección de destino	Haga clic en **Add (Añadir)** para añadir las direcciones, direcciones de grupos o regiones de destino (la opción predeterminada es Cualquiera). Seleccione desde el menú desplegable o haga clic en **Address (Dirección)**, **Address Group (Grupo de direcciones)** o **Regions (Regiones)** en la parte inferior del menú desplegable y especifique la configuración. Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las configuradas.

Pestaña de aplicación/protocolo de anulación de aplicación

Seleccione la pestaña **Protocol/Application (Protocolo/Aplicación)** para definir el protocolo (TCP o UDP), puerto y aplicación que definen con mayor exactitud los atributos de la aplicación para la coincidencia de la política.

Campo	Description (Descripción)
PROTOCOL	Seleccione el protocolo (**TCP** o **UDP**) para el cual permitir una anulación de la aplicación.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Puerto	Introduzca el número de puerto (0 a 65535) o el intervalo de números de puerto (puerto1-puerto2) de las direcciones de destino especificadas. Si especifica varios puertos o intervalos, deben estar separados por comas.
Application (Aplicación)	Seleccione la aplicación de cancelación de los flujos de tráfico que coincidan con los criterios de la regla anterior. Si cancela una aplicación personalizada, no se realizará una inspección de amenazas. La excepción es si cancela una aplicación predeterminada que admite la inspección de amenazas. Para definir nuevas aplicaciones, consulte Objetos > Aplicaciones).

© 2020 Palo Alto Networks, Inc.

Políticas > Autenticación

Su política de autenticación le permite autenticar a los usuarios finales antes de que puedan acceder a los recursos de la red.

¿Qué desea saber?	Consulte:
¿Qué campos están disponibles para crear una regla de autenticación?	Componentes básicos de una regla de política de autenticación
¿Cómo puedo utilizar la interfaz web para gestionar políticas de autenticación?	Crear y gestionar la política de autenticación Para Panorama, consulte Traslado o duplicación de una regla de política
¿Busca más información?	Política de autenticación

Componentes básicos de una regla de política de autenticación

Cada vez que un usuario solicita un recurso (como al visitar una página web), el cortafuegos evalúa la política de autenticación. Según la regla de política de coincidencia, el cortafuegos le pide al usuario que responda a uno o más desafíos de diferentes factores (tipos), como autenticación de inicio de sesión y contraseña, voz, SMS, envío o autenticación de contraseñas de una sola vez (OTP). Después de que el usuario responda a todos los factores, el cortafuegos evaluará la política de seguridad (consulte Policies > Security) para determinar si se debe permitir el acceso al recurso.

El cortafuegos no pide a los usuarios que se autenticen si acceden a recursos no basados en web (como una impresora) mediante una puerta de enlace de GlobalProtect ™ que sea interna o en modo de túnel. En su lugar, los usuarios verán mensajes de error de conexión. Para garantizar que los usuarios puedan acceder a estos recursos, configure un portal de autenticación y forme a los usuarios para visitarlo cuando vean fallos de conexión. Consulte con su departamento de TI para configurar un portal de autenticación.

La tabla siguiente describe cada elemento o componente de una regla de política de autenticación. Antes de añadir una regla, complete los requisitos previos descritos en Crear y administrar la política de autenticación.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
Número de regla	n/c	Cada regla se numera automáticamente y el orden cambia a medida que se mueven las reglas. Al filtrar reglas para que coincidan con filtros específicos, la página **Policies (Políticas)** > **Authentication (Autenticación)** enumere cada regla con su número en el contexto del conjunto de reglas completo de la base de reglas y su puesto en el orden de evaluación. Para

© 2020 Palo Alto Networks, Inc.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
		obtener más información, consulte secuencia de reglas y su orden de evaluación.
Nombre	**General**	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)		Introduzca una descripción de la regla (hasta 1024 caracteres).
Tag (Etiqueta)		Seleccione una etiqueta para las reglas de clasificación y filtrado (consulte Objects > Tags).
Agrupar reglas por etiquetas		Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario		Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios		Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.
Zona de origen	**Source (Origen)**	**Add (Añadir)** zonas para aplicar la regla únicamente al tráfico procedente de interfaces de las zonas que especifique (el valor predeterminado es **any (cualquiera)**). Para definir nuevas zonas, consulte Network > Zones.
Dirección de origen		**Add (Añadir)** direcciones o grupos de direcciones para aplicar la regla únicamente al tráfico procedente de los orígenes que especifique (el valor predeterminado es **any (cualquiera)**). Seleccione **Negate (Negar)** para elegir cualquier dirección excepto las seleccionadas. Para definir una nueva dirección o grupos de direcciones, consulte Objects > Addresses y Objects > Address Groups.

© 2020 Palo Alto Networks, Inc.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
Source User (Usuario de origen)	**Usuario**	Seleccione los usuarios de origen o los grupos de usuarios a los que se aplica la regla: • **any (cualquiera)**: incluye todo el tráfico independientemente de los datos de usuario. • **pre-logon (pre-inicio de sesión)**: incluye usuarios remotos que no han iniciado sesión en sus sistemas cliente pero cuyos sistemas cliente se conectan a la red a través de la función de pre-inicio de sesión de GlobalProtect. • **known-user (usuario conocido)**: incluye todos los usuarios para los que el cortafuegos ya tiene asignaciones de dirección IP a nombre de usuario antes de que la norma evoque la autenticación. • **unknown (desconocido)**: incluye todos los usuarios para los que el cortafuegos no cuente con asignaciones de dirección IP a nombre de usuario. Después de que la norma evoque la autenticación, el cortafuegos creará asignaciones de usuarios para usuarios desconocidos basándose en los nombres de usuario que introdujeron. • **Select (Seleccionar)**: incluye sólo los usuarios y grupos de usuarios que añadió con **Add (Añadir)** a la lista de usuarios de origen. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*
Perfil HIP de origen		**Añada** perfiles de información de host (HIP) para recopilar información sobre el estado de seguridad de sus hosts de extremo, como por ejemplo si tienen los parches de seguridad y las definiciones de antivirus más recientes. Para obtener más información y definir nuevos HIP, consulte Objects > GlobalProtect > HIP Profiles.
Zona de destino	**IP Destino**	**Añadir (Add)** zonas para aplicar la regla únicamente al tráfico que va a las interfaces en las zonas que especifique (el valor predeterminado es **any (cualquiera)**). Para definir nuevas zonas, consulte Network > Zones.

© 2020 Palo Alto Networks, Inc.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
Dirección de destino		**Add (Añadir)** direcciones o grupos de direcciones para aplicar la regla sólo a los destinos que especifique (el valor predeterminado es **any (cualquiera)**). Seleccione **Negate (Negar)** para elegir cualquier dirección excepto las seleccionadas. Para definir una nueva dirección o grupos de direcciones, consulte Objects > Addresses y Objects > Address Groups.
service	**Categoría de URL/servicio**	Seleccione entre las siguientes opciones para aplicar la regla sólo a servicios en números de puerto TCP y UDP específicos: • **any (cualquiera)**: especifica servicios en cualquier puerto y usando cualquier protocolo. • **default (predeterminado)**: especifica los servicios sólo en los puertos predeterminados que define Palo Alto Networks. • **Select (Seleccionar)**: le permite **Add (Añadir)** servicios o grupos de servicios. Para crear nuevos servicios y grupos de servicios, consulte Objects > Services y Objects > Service . *La selección predeterminada es service-http. Cuando utilice la política de autenticación para Captive Portal, habilite también service-https, para asegurarse de que el cortafuegos obtenga la asignación de usuarios a dirección IP para todo el tráfico.*
URL Category (Categoría de URL)		Seleccione las categorías de URL a las que se aplicará la regla. • Seleccione **any (cualquiera)** para especificar todo el tráfico , con independencia de la categoría URL. • **Add (Añadir)** categorías. Para definir categorías personalizadas, consulte Objects > Custom Objects > URL Category.
Aplicación de la autenticación	**Acciones**	Seleccione el objeto de cumplimiento de autenticación (Objects > Authentication) que especifique el método (por ejemplo, Captive Portal o desafío del navegador) y el perfil de autenticación que el cortafuegos utilice para autenticar usuarios. El perfil de autenticación define si los usuarios responden a un solo desafío o a una autenticación de múltiples factores (consulte Device > Authentication Profile). Puede seleccionar un objeto de aplicación de autenticación predefinido o personalizado.

© 2020 Palo Alto Networks, Inc.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
		Si debe excluir los hosts o servidores de una política de Captive Portal, añádalos al perfil de autenticación que especifica no-captive-portal (portal diferente a Captive Portal) como Authentication Enforcement (Aplicación de la autenticación). Sin embargo, las políticas de Captive Portal ayudan al cortafuegos a obtener la asignación de usuario a dirección IP, y deberían usarse siempre que fuera posible.
Tiempo de espera		Para reducir la frecuencia de los desafíos de autenticación que interrumpen el flujo de trabajo del usuario, puede especificar el intervalo en minutos (el valor predeterminado es 60) cuando el cortafuegos solicite al usuario que se autentique sólo una vez para obtener acceso repetido a los recursos. Si el objeto **Authentication Enforcement (Aplicación de la autenticación)** especifica la autenticación de múltiples factores, el usuario debe autenticar una vez para cada factor. El cortafuegos registrará una marca de tiempo y volverá a emitir un desafío sólo cuando expire el tiempo de espera de un factor. La redistribución de las marcas de tiempo de otros cortafuegos le permitirá aplicar el tiempo de espera incluso si el cortafuegos que inicialmente permitió el acceso para un usuario no es el mismo cortafuegos que más tarde controla el acceso para ese usuario. *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.* *Para los recursos del perímetro, configure el valor en 480 minutos (8 horas) y para los recursos del centro de datos y sistemas críticos, configure*

© 2020 Palo Alto Networks, Inc.

Componentes de una regla de autenticación	Configurado en	Description (Descripción)
		un valor más bajo, tal como 60 minutos, para reforzar la seguridad. Supervise y ajuste los valores según sea necesario.
Tiempos de espera de autenticación de log		Seleccione esta opción (deshabilitada de forma predeterminada) si desea que el cortafuegos genere logs de autenticación siempre que el **Timeout (Tiempo de espera)** asociado con un factor de autenticación caduque. Habilitar esta opción proporciona más datos para solucionar problemas de acceso. Junto con los objetos de correlación, también puede utilizar registros de autenticación para identificar actividad sospechosa en su red (como ataques de fuerza bruta). *Habilitar esta opción aumenta el tráfico de log.*
Log Forwarding		Seleccione un perfil de Reenvío de logs si desea que el cortafuegos reenvíe logs de autenticación a Panorama o a servicios externos como un servidor syslog (consulte Objects > Log Forwarding).

Crear y gestionar la política de autenticación

Seleccione la página **Policies (Políticas)** > **Authentication (Autenticación)** para crear y gestionar reglas de la política de autenticación:

Tarea	Description (Descripción)
Añadir	Realice los siguientes requisitos previos antes de crear reglas de política de autenticación: ❑ Configure los ajustes del portal cautivo de User-ID™ (consulte Device > User Identification > Captive Portal Settings). El cortafuegos utiliza el portal cautivo para mostrar el primer factor de autenticación que requiere la regla de Autenticación. Captive Portal también permite que el cortafuegos registre las marcas de tiempo asociadas a los períodos de Timeout (Tiempo de espera) de autenticación y que actualice las asignaciones de usuario. ❑ Configure un perfil de servidor que especifique cómo puede acceder el cortafuegos al servicio que autenticará a los usuarios (consulte Device [Dispositivo] > Server Profiles [Perfiles de servidor]). ❑ Asigne el perfil de servidor a un perfil de autenticación que especifique la configuración de autenticación (consulte Device [Dispositivo] > Authentication Profile [Perfil de autenticación]). ❑ Asigne el perfil de autenticación a un objeto de aplicación de autenticación que especifique el método de autenticación (consulte Objects [Objectos] > Authentication [Autenticación]).

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	Para crear una regla, realice uno de los pasos siguientes y complete los campos descritos en Componentes de una regla de política de autenticación: • Haga clic en **Add (Añadir)**. • Seleccione una regla enla que se base la nueva regla y haga clic en **Clone Rule (Duplicar regla)**. El cortafuegos inserta la regla copiada, denominada <rulename>#, debajo de la regla seleccionada, donde # es el siguiente número entero disponible que hace que el nombre de la regla sea único, y genera un nuevo identificador único universal (Universal Unique Identifier, UUID) para la regla duplicada. Para obtener más información, consulte Traslado o duplicación de una regla de política.
Modificar	Para modificar una regla, haga clic en el nombre de la regla y edite los campos descritos en Componentes de una regla de política de autenticación. *Si el cortafuegos recibió la regla de Panorama, la regla es de solo lectura; solo puede editarlo en Panorama.*
Movimiento	Cuando busca coincidencias para el tráfico, el cortafuegos evalúa las reglas de arriba a abajo en el orden que la página **Policies (Políticas)** > **Authentication (Autenticación)** las enumera. Para cambiar el orden de evaluación, seleccione una regla y seleccione **Move Up (Mover hacia arriba)**, **Move Down (Mover hacia abajo)**, **Move Top (Mover a la parte superior)** o **Move Bottom (Mover a la parte inferior):**. Para obtener más información, consulte Traslado o duplicación de una regla de política.
delete	Para eliminar una regla existente, seleccione **Delete (Eliminar)** regla.
Habilitar/ deshabilitar	Para deshabilitar una regla, seleccione y haga clic en **Disable (Deshabilitar)**. Para volver a habilitar una regla deshabilitada, seleccione y haga clic en **Enable (Habilitar)**.
Resaltar reglas no utilizadas	Para identificar las reglas que no se utilizan desde la última vez que el cortafuegos se reinició, seleccione **Highlight Unused Rules (Resaltar reglas no utilizadas)**. A continuación, podrá decidir si desea deshabilitar o eliminar las reglas no utilizadas. La página Resaltar reglas no utilizadas con un fondo amarillo punteado.
Reglas de vista previa (únicamente Panorama)	Haga clic en **Preview Rules (Reglas de vista previa)** para ver una lista de las reglas antes de enviarlas a los cortafuegos gestionados. Dentro de cada base de reglas, la página demarca visualmente la jerarquía de reglas para cada grupo de dispositivos (y cortafuegos gestionado) para facilitar el escaneado de numerosas reglas.

© 2020 Palo Alto Networks, Inc.

Políticas > Protección DoS

La política de protección DoS le permite proteger recursos críticos individuales contra los ataques DoS al especificar si se debe denegar o permitir paquetes que coincidan con una interfaz, zona, dirección o usuario de origen, o con una interfaz, zona o usuario de destino.

Opcionalmente, puede elegir la acción Protect (Proteger) y especificar un perfil DoS donde establezca los umbrales (sesiones o paquetes por segundo) que generarán una alarma, activar una acción de protección e indicar la frecuencia máxima por encima de la cual se descartarán las nuevas conexiones. Por tanto, puede controlar el número de sesiones entre interfaces, zonas, direcciones y países, en función de sesiones agregadas o direcciones IP de origen o destino. Por ejemplo, puede controlar el tráfico desde y hacia determinadas direcciones o grupos de direcciones o desde determinados usuarios y para servicios concretos.

El cortafuegos aplica las reglas de la política de protección DoS antes que las reglas de política de seguridad para garantizar que el cortafuegos utiliza sus recursos de la manera más eficiente. Si una regla de la política de protección DoS rechaza un paquete, ese paquete nunca alcanza una regla de política de seguridad.

Las siguientes tablas describen la configuración del perfil de la política de protección DoS:

- Pestaña general de protección DoS
- Pestaña de origen de protección DoS
- Pestaña de destino de protección DoS
- Pestaña de protección/opción de protección DoS

¿Busca más información?

Consulte Perfiles de protección DoS y Objects > Security Profiles > DoS Protection.

Pestaña general de protección DoS

- **Policies (Políticas)** > **DoS Protection (Protección DoS)** > **General (General)**

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política de DoS Protection. También puede configurar una etiqueta para que le permita ordenar o filtrar políticas cuando existen numerosas políticas.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla de política de DoS Protection. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la regla (hasta 1024 caracteres).
Etiquetas	Si desea añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Una etiqueta es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, tal vez quiera etiquetar determinadas políticas de seguridad con Entrante en DMZ, políticas de

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	descifrado con las palabras descifrado o sin descifrado, o usar el nombre de un centro de datos específico para políticas asociadas con esa ubicación.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. Puede exportar el archivo de comentarios de auditoría en formato CSV.

Pestaña de origen de protección DoS

Selecciona la pestaña **Source (Origen)** para definir la o las interfaces de origen o zonas de origen y, opcionalmente, las direcciones de origen y usuarios de origen que definen el tráfico entrante al que se aplica la regla de política DoS.

Campo	Description (Descripción)
Tipo	Seleccione el tipo de origen al que se aplica la regla de política de protección DoS: • **Interface (Interfaz)**: Aplica la regla al tráfico procedente de la interfaz o grupo de interfaces especificado. • **Zone (Zona)**: aplica la regla al tráfico procedente de cualquier interfaz en una zona especificada. Haga clic en **Add (Añadir)** para seleccionar múltiples interfaces o zonas.
Dirección de origen	Seleccione **Any (Cualquiera)** o **Add (Añadir)** y especifique una o más direcciones de origen a las que se aplica la regla de política de protección de DoS. (Opcional) Seleccione **Negate (Negar)** para especificar que la regla se aplica a cualquier dirección excepto las especificadas.
Source User (Usuario de origen)	Especifique uno o más usuarios de origen a los que se aplica la regla de política de Protección de DoS: • **any (cualquiera)**: incluye paquetes independientemente del usuario de origen. • **pre-logon (anterior al inicio de sesión)**: incluye paquetes de usuarios remotos conectados a la red mediante GlobalProtect pero que no han iniciado sesión en su sistema. Cuando se configura la opción **Pre-logon (Anterior al inicio de sesión)** en el portal de aplicaciones de GlobalProtect, cualquier usuario que no esté registrado en su equipo en ese momento será identificado con el nombre de usuario anterior al inicio de sesión. Puede crear estas políticas para usuarios anteriores al inicio de sesión y, aunque el usuario no haya iniciado sesión directamente, sus equipos estarán autenticados en el dominio como si hubieran iniciado sesión completamente.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **known-user (usuario conocido)**: Incluye a todos los usuarios autenticados, es decir, cualquier dirección IP con datos de usuario asignados. Esta opción es equivalente al grupo “usuarios del dominio” en un dominio. • **unknown (desconocido)**: incluye a todos los usuarios desconocidos, es decir, las direcciones IP que no estén asignadas a un usuario. Por ejemplo, podría utilizar **unknown (desconocido)** para acceso de invitados a alguna parte porque tendrán una dirección IP en su red, pero no se autenticarán en el dominio y no tendrán ninguna información de asignación de dirección IP a nombre de usuario en el cortafuegos. • **Select (Seleccionar)**: incluye usuarios especificados en esta ventana. Por ejemplo, puede seleccionar un usuario, una lista de individuos, algunos grupos o añadir usuarios manualmente. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*

Pestaña de destino de protección DoS

Seleccione la pestaña **Destination (Destino)** para definir la zona o interfaz de destino y la dirección de destino que define el tráfico de destino al que se aplicará la política.

Campo	Description (Descripción)
Tipo	Seleccione el tipo de destino al que se aplicará la regla de política de protección DoS: • **Interface** (Interfaz): Aplica la regla a los paquetes que van a la interfaz especificada o grupo de interfaces. Haga clic en **Add (Añadir)** y seleccione una o más interfaces. • **Zone** (Zona): Aplica la regla a los paquetes que van a cualquier interfaz en la zona especificada. Haga clic en **Add (Añadir)** y seleccione una o más zonas.
Dirección de destino	Seleccione **Any (Alguna)** o **Add (Añadir)** y especifique una o más direcciones de destino a las que se aplica la regla de política de Protección DoS. (Opcional) Seleccione **Negate (Negar)** para especificar que la regla se aplica a cualquier dirección excepto las especificadas.

Pestaña de protección/opción de protección DoS

Seleccione la pestaña **Option/Protection (Opción/Protección)** para configurar opciones de la regla de política de protección DoS, como el tipo de servicio al que se aplica la regla o la acción que se realizará con los paquetes que coinciden con la regla, y para decidir si se activará o no un reenvío de log para el tráfico coincidente. Puede definir un programa para cuando la regla está activa.

También puede seleccionar un perfil de protección DoS agregado y/o un perfil de protección DoS clasificado que determinan las tasas de umbral que, cuando se superan, provocan que el cortafuegos tome acciones protectoras, como activar una alarma, activar una acción como Random Early Drop , y descartar paquetes que exceden el umbral de tasa máxima.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
service	Haga clic en **Add (Añadir)** y seleccione uno o más servicios a los que se aplica la política de protección DoS. El valor predeterminado es **Any (Cualquier)** servicio. Por ejemplo, si la política DoS protege servidores web, especifique HTTP, HTTPS y otros puertos de servicio apropiados para las aplicaciones web. *Para los servidores críticos, cree reglas de protección DoS separadas para proteger los puertos de servicio no utilizados y ayudar a prevenir los ataques dirigidos.*
Acción	Seleccione la acción que el cortafuegos realiza en los paquetes que coinciden con la regla de política de protección DoS: • **Negate (Negar)**: descartar todos los paquetes que coinciden con la regla. • **Allow (Permitir)**: permite todos los paquetes que coinciden con la regla. • **Protect (Proteger)**: aplique las protecciones especificadas en el perfil de protección DoS especificado en los paquetes que coinciden con la regla. Los paquetes que coinciden con la regla se contabilizan hacia las tasas del umbral en el perfil DoS Protection, que a su vez activan una alarma, activan otra acción y Activan el descarte de paquetes cuando se excede la tasa máxima. *El objeto de la aplicación de la protección DoS es proteger contra ataques de DoS; por ende, habitualmente debería usar Protect (Proteger). Deny (Denegar) descarta el tráfico legítimo, junto con el tráfico DoS y Allow (Permitir) no detiene los ataques de DoS. Utilice Deny (Denegar) y Allow (Permitir) únicamente para hacer excepciones dentro de un grupo. Por ejemplo, puede denegar el tráfico de la mayoría de los elementos de un grupo, pero permitir un subconjunto de ese tráfico, o permitir el tráfico de la mayoría de los elementos de un grupo, pero denegar un subconjunto de ese tráfico.*
Programa	Especifica el horario cuando la regla de política de Protección DoS está en vigor. El ajuste predeterminado de **None (Ninguno)** indica que no hay horario; la política está siempre en efecto. Como alternativa, seleccione una planificación o cree una nueva programación para controlar cuándo está en vigor la regla de la política de protección DoS. Introduzca un **Name (Nombre)** para la programación. Seleccione **Shared (Compartido)** para compartir esta programación con todos los sistemas virtuales en un cortafuegos de múltiples sistemas virtuales. Seleccione una **Recurrence (Periodicidad)** de **Daily (Diariamente)**, **Weekly (Semanal)** o **Non-recurring (Sin periodicidad)**. Añada una **Start Time (Hora de inicio)** y **End Time (Hora de finalización)** en horas: minutos, basado en un formato de hora de 24 horas.
Log Forwarding	Si quiere activar el reenvío de entradas de logs de amenazas para tráfico coincidente a un servicio externo, como un servidor syslog o Panorama, seleccione un perfil de reenvío de logs o haga clic en **Profile (Perfil)** para crear uno nuevo. *El cortafuegos crea logs y reenvía solo el tráfico que coincide con una acción de la regla.*

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Para lograr una gestión más sencilla, reenvíe por separado los logs DoS de los demás logs de amenazas directamente a los administradores por correo electrónico y a un servidor de logs.
Agregado	Agrupe los umbrales establecidos en los perfiles de protección DoS que se aplican al grupo combinado de dispositivos especificados en la regla de protección DoS para proteger dichos grupos de servidores. Por ejemplo, un umbral de frecuencia de alarma de 10 000 CPS significa que cuando la CPS nueva total para el grupo completo supera 10 000 CPS, el cortafuegos activa un mensaje de alarma. Seleccione un perfil de protección DoS agregado que especifique las tasas del umbral en las que las conexiones entrantes por segundo activan una alarma, activan una acción y superan una tasa máxima. Todas las conexiones entrantes (el agregado) cuentan hacia los umbrales especificados en un perfil de Protección DoS agregada. Una configuración de perfil de agregado de **None (Ninguna)** significa que no hay ninguna configuración de umbral establecida para el tráfico agregado. Consulte Objects > Security Profiles > DoS Protection.
Clasificado	Los umbrales establecidos en los perfiles de protección DoS clasificados que se aplican a cada dispositivo individual especificado en la regla de protección DoS para proteger grupos individuales o pequeños de servidores críticos. Por ejemplo, un umbral de frecuencia de alarma de 10 000 CPS significa que cuando la CPS nueva total para un servidor individual especificado supera 10 000 CPS, el cortafuegos activa un mensaje de alarma. Seleccione esta opción y especifique lo siguiente: • **Profile (Perfil)**: seleccione un perfil de protección DoS clasificado para aplicar a esta regla. • **Address (Dirección)**: seleccione si las conexiones entrantes cuentan para los umbrales del perfil, si coinciden con las **Source-ip-only (Solo IP de origen)**, **destination-ip-only (Solo PI de destino)** o **Src-dest-ip-both (IP de origen y de destino)**. *El cortafuegos consume más recursos para registrar los contadores src-dest-ip-both (IP de origen y de destino) que para registrar solo el contador de IP de origen o IP de destino.* Si especifica un perfil de protección DoS clasificado, solo las conexiones entrantes que coincidan con la dirección IP de origen, la dirección IP de destino o ambas direcciones IP de origen y destino cuentan hacia los umbrales especificados en el perfil. Por ejemplo, puede especificar un perfil de protección DoS clasificado con una **Max Rate (Frecuencia máx.)** de 100 cps y especificar un ajuste de **Address (Dirección)** de **source-ip-only (solo IP de origen)** en la regla. El resultado sería un límite de 100 conexiones por segundo para esa dirección IP de origen en particular. *No utilice src-ip-only (Solo IP de origen) o src-dest-ip-both (IP de origen y de destino) para zonas accesibles desde Internet, porque el cortafuegos no puede almacenar contadores para todas las direcciones IP posibles de Internet. Use destination-ip-only (Solo IP de destino) en las zonas del perímetro.* *Use destination-ip-only (Solo IP de destino) para proteger los dispositivos individuales críticos.*

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Use source-ip-only (Solo IP de origen) y el umbral Alarm (Alarma) para supervisar hosts sospechosos en zonas no accesibles desde Internet. Consulte Objects > Security Profiles > DoS Protection.

© 2020 Palo Alto Networks, Inc.

Políticas > SD-WAN

Cree una regla de políticas de SD-WAN con criterios de coincidencia, incluidas las aplicaciones y un perfil de calidad de ruta que especifique las métricas de vibración, latencia y pérdida de paquetes que especifique. Cuando las rutas entre el origen y el destino de aplicaciones críticas y sensibles experimenten una degradación, la regla de políticas de SD-WAN utilizará el perfil de distribución de tráfico asociado para seleccionar dinámicamente una nueva ruta óptima para las aplicaciones. La regla de políticas de SD-WAN también especifica los dispositivos de destino a los que Panorama aplica la regla.

- Pestaña General de SD-WAN
- Pestaña Origen de SD-WAN
- Pestaña Destino de SD-WAN
- Pestaña Aplicación/Servicio de SD-WAN
- Pestaña Selección de ruta de SD-WAN
- (Solo Panorama) Pestaña Destino de SD-WAN

Pestaña General de SD-WAN

- **Políticas** > **SD-WAN** > **General**

Seleccione la pestaña **General** para configurar un nombre y una descripción de la política de SD-WAN. También puede configurar una pestaña para que le permita ordenar o filtrar políticas cuando estas son muy numerosas.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar la regla. El nombre distingue entre mayúsculas y minúsculas y puede tener hasta 63 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos. El nombre debe ser exclusivo en un cortafuegos y, en Panorama, exclusivo dentro de su grupo de dispositivos y cualquier grupo de dispositivos antecesor o descendiente.
Description (Descripción)	Introduzca una descripción de la regla (hasta 1024 caracteres).
Tag (Etiqueta)	Si necesita añadir una etiqueta a la política, haga clic en **Add (Añadir)** para especificar la etiqueta. Una etiqueta de política es una palabra clave o frase que le permite ordenar o filtrar políticas. Es útil cuando ha definido muchas políticas y desea revisar las que están etiquetadas con una palabra clave específica. Por ejemplo, es posible que desee etiquetar determinadas políticas de SD-WAN con etiquetas únicas que identifiquen centrales o sucursales específicas a los que se aplican las reglas.
Agrupar reglas por etiquetas	Introduzca una etiqueta con la que desee agrupar reglas de política similares. La etiqueta del grupo le permite ver la base de reglas de política en función de las etiquetas. Puede optar por agrupar las reglas en función de una **etiqueta**.
Auditar comentario	Introduzca un comentario para auditar la creación o edición de la regla de política. El comentario de auditoría distingue entre mayúsculas y

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	minúsculas, y puede tener hasta 256 caracteres, que pueden ser letras, números, espacios, guiones y guiones bajos.
Auditar archivo de comentarios	Ver los **Comentarios de auditoría** de la regla de política. El archivo de comentario de auditoría se puede exportar en formato CSV.

Pestaña Origen de SD-WAN

- **Políticas** > **SD-WAN** > **Origen**

Seleccione la pestaña **Origen** para definir las zonas de origen, las direcciones de origen y los usuarios de origen que definen los paquetes entrantes a los que se aplica la política de SD-WAN.

Campo	Description (Descripción)
Zona de origen	Para especificar una zona de origen, seleccione **Añadir** y seleccione una o más zonas, o seleccione **cualquier** zona. La especificación de varias zonas puede simplificar la gestión. Por ejemplo, si tiene tres sucursales en diferentes zonas y desea que los criterios de coincidencia restantes y la selección de ruta sean los mismos para las tres, puede crear una regla de SD-WAN y especificar las tres zonas de origen para cubrir las tres. *Solo las zonas de tipo capa 3 son compatibles con las reglas de políticas de SD-WAN.*
Dirección de origen	Para especificar direcciones de origen, **añada** direcciones de origen o listas dinámicas externas (EDL), seleccione en el menú desplegable o seleccione **Dirección** y cree un nuevo objeto de dirección. Alternativamente, seleccione **cualquier** dirección de origen (valor predeterminado).
Source User (Usuario de origen)	Para especificar ciertos usuarios, seleccione **Añadir** (el tipo indica **seleccionar**) e introduzca un usuario, una lista de usuarios o grupos de usuarios. También puede seleccionar un tipo de usuario: • **cualquiera** (valor predeterminado): incluye cualquier usuario, independientemente de sus datos. • **pre-logon**: incluye a usuarios remotos conectados a la red mediante GlobalProtect™, pero que no han iniciado sesión en su sistema. Cuando se configura la opción anterior al inicio de sesión en el portal de aplicaciones de GlobalProtect, cualquier usuario que no esté registrado en su equipo en ese momento se identificará con el nombre de usuario anterior al inicio de sesión. Puede crear estas políticas para usuarios anteriores al inicio de sesión y, aunque el usuario no haya iniciado sesión directamente, sus equipos estarán autenticados en el dominio como si hubieran iniciado sesión completamente. • **known-user (usuario conocido)**: Incluye a todos los usuarios autenticados, es decir, cualquier dirección IP con datos de usuario asignados. Esta opción es equivalente al grupo “usuarios del dominio” en un dominio.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **unknown (desconocido)**: incluye a todos los usuarios desconocidos, es decir, las direcciones IP que no estén asignadas a un usuario. Por ejemplo, podría utilizar **unknown (desconocido)** para el acceso de invitados a alguna parte porque tendrán una dirección IP en su red, pero no se autenticarán en el dominio y no tendrán ninguna información de asignación de dirección IP a nombre de usuario en el cortafuegos. *Si el cortafuegos recopila información del cliente de un servidor proveedor de identidad RADIUS, TACACS+, o SAML y no del agente de User-ID™, la lista de usuarios no se muestra y deberá introducir la información del usuario manualmente.*

Pestaña Destino de SD-WAN

- **Políticas** > **SD-WAN** > **Destino**

Seleccione la pestaña **Destino** para definir las zonas de destino o las direcciones de destino que definen el tráfico al que se aplicará la regla de políticas de SD-WAN.

Campo	Description (Descripción)
Zona de destino	**Añada** zonas de destino (el valor predeterminado es Cualquiera). Las zonas deben ser de capa 3. Para definir nuevas zonas, consulte Network > Zones. Añada varias zonas para simplificar la gestión. Por ejemplo, si tiene tres zonas internas diferentes (Marketing, Ventas y Relaciones públicas) que se dirigen todas a la zona de destino no fiable, puede crear una regla que cubra todas las clases.
Dirección de destino	**Añada** direcciones de destino, grupos de direcciones, listas dinámicas externas (EDL) o regiones (el valor predeterminado es **Cualquiera**). Seleccione en la lista desplegable o haga clic en **Address (Dirección)** o **Address Group (Grupo de direcciones)** en la parte inferior de la lista desplegable y especifique la configuración. Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las configuradas.

Pestaña Aplicación/Servicio de SD-WAN

- **Políticas** > **SD-WAN** > **Aplicación/Servicio**

Seleccione la pestaña **Aplicación/Servicio** para especificar las aplicaciones o servicios a los que se aplica la regla de políticas de SD-WAN.

Campo	Description (Descripción)
Perfil de calidad de ruta	Seleccione un perfil de calidad de ruta que determine los umbrales máximos de vibración, latencia y porcentaje de pérdida de paquetes

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	que desee aplicar a las aplicaciones y servicios especificados. Si aún no se ha creado un perfil de calidad de ruta, puede crear un perfil **Nueva calidad de ruta de SD-WAN** desde esta pestaña.
applications	**Añada** aplicaciones específicas a la regla de políticas de SD-WAN o seleccione **Cualquiera**. Si una aplicación tiene múltiples funciones, seleccione una aplicación general o aplicaciones individuales. Si selecciona la aplicación general, se incluirán todas las funciones y la definición de la aplicación se actualizará automáticamente a medida que se añadan futuras funciones. Si utiliza grupos de aplicaciones, filtros o contenedores en la regla de la política de SD-WAN, vea la información detallada de estos objetos pasando el ratón por encima del objeto en la columna Aplicación, abriendo el menú desplegable y seleccionando **Valor**. De esta forma podrá ver miembros de la aplicación directamente desde la política, sin tener que desplazarse a las pestañas **Object**. *Añada solo aplicaciones críticas para la empresa que se vean afectadas por la latencia, la vibración o la pérdida de paquetes. Evite añadir categorías o subcategorías de aplicaciones, ya que son demasiado amplias y no permiten el control por aplicación.*
service	**Añada** servicios específicos para la regla de políticas de SD-WAN y seleccione en qué puertos se permiten o deniegan los paquetes de estos servicios: • **Cualquiera**: los servicios seleccionados se permiten o deniegan en cualquier protocolo o puerto. • **valor predeterminado de aplicación**: los servicios seleccionados se permiten o deniegan únicamente según sus **puertos definidos de forma predeterminada por Palo Alto Networks** Esta opción se recomienda para políticas que especifican la acción **permitir** porque evita que los servicios se ejecuten en puertos y protocolos inusuales que, si no son intencionales, pueden ser una señal de un comportamiento y uso no deseados del servicio. *Cuando usa esta opción, solo el puerto predeterminado coincide con la política de SD-WAN y se aplica la acción. Es posible que se permitan otros servicios que no estén en el puerto predeterminado según la regla de la política de seguridad, pero que no coincidan con la política de SD-WAN y no se realicen acciones con la regla de la política de SD-WAN.* *Para la mayoría de los servicios, utilice predeterminado-de-aplicación para evitar que el servicio utilice puertos no estándar o que exhiba otros comportamientos evasivos. Si el puerto predeterminado para el servicio cambia, el cortafuegos actualiza automáticamente la regla con el puerto predeterminado correcto. Para los servicios que usan*

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	puertos no estándar, tal como servicios personalizados internos, modifique el servicio o cree una regla que especifique los puertos no estándares, y aplique la regla únicamente al tráfico que requiera el servicio. • **Select (Selecto)**: haga clic en **Add (Añadir)** para añadir un servicio existente o seleccione **Service (Servicio)** o **Service Group (Grupo de servicios)** para especificar una nueva entrada. (O seleccione Objects > Services y Objects > Service Groups).

Pestaña Selección de ruta de SD-WAN

- **Políticas** > **SD-WAN** > **Selección de ruta**

Seleccione la pestaña **Selección de ruta** para especificar el perfil de distribución de tráfico que controla cómo el cortafuegos selecciona una nueva ruta para el tráfico de aplicaciones o servicios que usar cuando una de las métricas de estado de la ruta para la ruta preferida excede el umbral configurado en el perfil de calidad de la ruta para la regla de políticas de SD-WAN.

Campo	Description (Descripción)
Perfil de distribución de tráfico	En el menú desplegable, seleccione un perfil de distribución de tráfico, que determina cómo el cortafuegos selecciona una ruta alternativa para el tráfico de la aplicación o del servicio cuando una de las métricas de estado de la ruta para la ruta preferida excede el umbral configurado en el perfil de calidad de la ruta para la regla.

Pestaña Destino de SD-WAN

- **Políticas** > **SD-WAN** > **Destino**

Seleccione la pestaña **Destino** para seleccionar los dispositivos gestionados a los que Panorama enviará la regla de políticas de SD-WAN. Esta pestaña solo es compatible con el servidor de gestión Panorama.

Campo	Description (Descripción)
Cualquiera (apuntar a todos los dispositivos)	Habilite (marque) esta opción para enviar la regla de políticas de SD-WAN a todos los dispositivos gestionados por el servidor de gestión Panorama.
Dispositivos	1. En la pestaña Dispositivos, en el lado izquierdo, seleccione opcionalmente uno o más filtros para filtrar qué elementos aparecen en el lado derecho en la sección **Nombre**. 2. En la sección **Nombre**, seleccione uno o más dispositivos a los que Panorama inserta la regla de políticas de SD-WAN. 3. Habilite (marque) **Filtro seleccionado** para mostrar solo los dispositivos seleccionados y el recuento.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Etiquetas	En la pestaña Etiquetas, **añada** una o más **etiquetas** que se aplicaron a los dispositivos. Panorama enviará la regla de SD-WAN a los dispositivos etiquetados con las etiquetas especificadas. *Puede utilizar la pestaña Dispositivos o la pestaña Etiquetas para especificar dónde envía Panorama la regla, pero no ambas.*
Dirigirse a todos menos a estos dispositivos y etiquetas especificados	Habilite (marque) esta opción para enviar la regla de políticas de SD-WAN a todos los dispositivos excepto a los **dispositivos** seleccionados o los dispositivos con las **etiquetas** especificadas.

© 2020 Palo Alto Networks, Inc.

Objetos

Los objetos son elementos que le permiten construir, programar y buscar reglas de política, y los perfiles de seguridad brindan protección contra las amenazas en las reglas de política.

Esta sección describe cómo configurar los perfiles de seguridad y objetos que puede utilizar con Políticas:

- Mover, clonar, anular o revertir objetos
- Objects(Objetos) > Addresses (Direcciones)
- Objects (Objetos) > Address Groups (Grupos de direcciones)
- Objects (Objetos) > Regions (Regiones)
- Objects (Objetos) > Applications (Aplicaciones)
- Objects (Objetos) > Application Groups (Grupos de aplicaciones)
- Objects (Objetos) > Application Filters (Filtros de aplicaciones)
- Objects (Objetos) > Services (Servicios)
- Objects (Objetos) > Service Groups (Grupos de servicios)
- Objects (Objetos) > Tags (Etiquetas)
- Objects (Objetos) > GlobalProtect > HIP Objects (Objetos HIP)
- Objects (Objetos) > GlobalProtect > HIP Profiles (Perfiles HIP)
- Objects (Objetos) > External Dynamic Lists (Listas dinámicas externas)
- Objects (Objetos) > Custom Objects (Objetos personalizados)
- Objects (Objetos) > Security Profiles (Perfiles de seguridad)
- Objects (Objetos) > Security Profiles (Perfiles de seguridad) > GTP Protection (Protección de GTP)
- Objetos > Perfiles de seguridad > Protección SCTP
- Objects (Objetos) > Security Profile Groups (Grupos de perfiles de seguridad)
- Objects (Objetos) > Log Forwarding (Reenvío de logs)
- Objects (Objetos) > Authentication (Autenticación)
- Objects (Objetos) > Decryption Profile (Perfil de descifrado)
- Objects (Objetos) > Schedules (Programaciones)

© 2020 Palo Alto Networks, Inc.

Mover, clonar, cancelar o revertir objetos

Consulte los siguientes temas para obtener opciones para modificar objetos existentes:

- «Mover o duplicar un objeto»
- Cancelación o reversión de un objeto

«Mover o duplicar un objeto»

Al trasladar o duplicar objetos, puede asignar un **Destination (Destino)** (un sistema virtual en un cortafuegos o un grupo de dispositivos en Panorama™) para el que cuenta con permisos de acceso, incluida la ubicación compartida.

Para trasladar un objeto, seleccione el objeto en la pestaña **Objects (Objetos)**, haga clic en **Move (Mover)**, seleccione **Move to other vsys (Mover a otros vsys)** (únicamente cortafuegos) o **Move to other device group (Mover a otro grupo de dispositivos)** (únicamente Panorama), complete los campos de la tabla siguiente y, a continuación, haga clic en **OK (Aceptar)**.

Para duplicar un objeto, seleccione el objeto en la pestaña **Objects (Objetos)**, haga clic en **Clone (Duplicar)**, complete los campos de la tabla siguiente y, a continuación, haga clic en **OK (Aceptar)**.

Configuración de traslado/ duplicación	Description (Descripción)
Objetos seleccionados	Muestra el nombre y la ubicación actual (sistema virtual o grupo de dispositivos) de las políticas u objetos que ha seleccionado para la operación.
IP Destino	Seleccione la nueva ubicación de la política u objeto: un sistema virtual, un grupo de dispositivos o una ubicación compartida. El valor predeterminado es el **Virtual System (Sistema virtual)** o **Device group (Grupo de dispositivos)** que seleccionó en la pestaña **Policies (Políticas)** u **Objects (Objetos)**.
Error en el primer error detectado en la validación	Seleccione esta opción (seleccionada de manera predeterminada) para que el cortafuegos o Panorama muestre el primer error que encuentre y deje de buscar más errores. Por ejemplo, se produce un error si el **Destination (Destino)** no incluye un objeto al que se haga referencia en la regla de política que está moviendo. Si borra esta selección, el cortafuegos o Panorama buscará todos los errores antes de mostrarlos.

Cancelación o reversión de un objeto

En Panorama, puede anidar grupos de dispositivos en una jerarquía de árbol de hasta cuatro niveles. En el nivel inferior, un grupo de dispositivos puede tener grupos de dispositivos primarios, primarios principales y primarios principales superiores en niveles sucesivamente mayores (lo que en conjunto se denomina *antecesores*), de los cuales el grupo de dispositivos de nivel inferior hereda políticas y objetos. En el nivel superior, un grupo de dispositivos puede tener grupos de dispositivos secundarios, secundarios de segundo nivel y secundarios de tercer nivel (lo que en conjunto se denomina *descendientes*). Puede cancelar un objeto en un descendiente de modo que sus valores difieran de los de un antecesor. Esta capacidad de cancelación está habilitada de manera predeterminada. Sin embargo, no puede cancelar

© 2020 Palo Alto Networks, Inc.

objetos compartidos o predeterminados (preconfigurados). La interfaz web muestra el icono para indicar que un objeto tiene valores heredados y muestra el icono para indicar que un objeto heredado tiene valores cancelados.

- **Cancelar un objeto**: seleccione la pestaña **Objects (Objetos)**, seleccione el **Device Group (Grupo de dispositivos)** descendiente que tendrá la versión cancelada, seleccione el objeto, haga clic en **Override (Cancelar)** y edite los ajustes. No puede cancelar los ajustes **Name (Nombre)** o **Shared (Compartido)** del objeto.
- **Revertir un objeto cancelado a sus valores heredados**: seleccione la pestaña **Objects (Objetos)**, seleccione el **Device Group (Grupo de dispositivos)** que tiene la versión cancelada, seleccione el objeto, haga clic en **Revert (Revertir)** y haga clic en **Yes (Sí)** para confirmar la operación.
- **Deshabilitar las cancelaciones de un objeto**: seleccione la pestaña **Objects (Objetos)**, seleccione el **Device Group (Grupo de dispositivos)** donde reside el objeto, haga clic en el nombre del objeto para editarlo, seleccione **Disable override (Deshabilitar cancelación)** y haga clic en **OK (Aceptar)**. Las cancelaciones de ese objeto se deshabilitarán en todos los grupos de dispositivos que hereden el objeto del **Device Group (Grupo de dispositivos)** seleccionado.
- **Sustituir todas las cancelaciones de objetos en Panorama con los valores heredados de la ubicación compartida o los grupos de dispositivos antecesores**: seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)**, modifique los ajustes de Panorama, seleccione **Ancestor Objects Take Precedence (Los objetos antecesores tienen prioridad)** y haga clic en **OK (Aceptar)**. A continuación debe compilar en Panorama y en los grupos de dispositivos que contengan cancelaciones para introducir los valores heredados.

© 2020 Palo Alto Networks, Inc.

Objetos > Direcciones

Un objeto de dirección puede incluir direcciones IPv4 o IPv6 (una dirección IP simple, un intervalo de direcciones o una subred), un FQDN o una dirección comodín (dirección IPv4 seguida por una barra diagonal y una máscara comodín). Un objeto de dirección le permite volver a utilizar la misma dirección o grupo de direcciones como direcciones de origen o destino en las reglas de política, filtros y otras funciones del cortafuegos, sin añadir cada dirección manualmente para cada instancia. Usted crea un objeto de dirección utilizando la interfaz web o el CLI y el cambio requiere una confirmación para que el objeto forme parte de la configuración.

Primero, haga clic en **Add (Añadir)** para añadir un nuevo objeto de dirección y especifique los siguientes valores:

Configuración de un objeto de dirección	Description (Descripción)
Nombre	Introduzca un nombre (hasta 63 caracteres) que describa las direcciones que incluirá como parte de este objeto. Este nombre aparece en la lista de direcciones cuando se definen las reglas de política de seguridad. El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos.
Lugar	Seleccione esta opción si desea compartir este objeto de dirección con: • **Every virtual system (vsys) on a multi-vsys firewall (Cada sistema virtual [vsys] en un cortafuegos de varios vsys)**: si no selecciona esta opción, el objeto de dirección estará disponible solo para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • **Every device group on Panorama (Cada grupo de dispositivos en Panorama):** si no selecciona esta opción, el objeto de dirección estará disponible solo para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores anulen la configuración de este objeto de dirección en los grupos de dispositivos que lo heredan. De manera predeterminada, esta opción está deshabilitada, lo que significa que los administradores pueden anular la configuración de cualquier grupo de dispositivos que hereda el objeto.
Description (Descripción)	Introduzca una descripción del objeto (hasta 1.023 caracteres).

Tipo	Especifique el tipo de objeto de dirección y la entrada:
	• **IP Netmask (Máscara de red IP)**: introduzca la dirección IPv4 o IPv6, o el intervalo de dirección IP con la siguiente notación: *ip_address/mask* o *ip_address*, donde la mask (máscara) es el número de dígitos binarios significativos utilizados para la parte de red de la dirección. En el caso de las direcciones IPv6, lo ideal es que especifique solo la parte de red, no la de host. Por ejemplo:
	  • **192.168.80.150/32:** indica una dirección.
	  • **192.168.80.0/24:** abarca todas las direcciones desde 192.168.80.0 hasta 192.168.80.255.
	  • **2001:db8::/32**

© 2020 Palo Alto Networks, Inc.

Configuración de un objeto de dirección	Description (Descripción)
	• **2001:db8:123:1::/64** • **IP Range (Intervalo IP)**: introduzca un intervalo de direcciones usando el siguiente formato: *ip_address–ip_address*, donde ambos extremos del intervalo son direcciones IPv4 o IPv6. Por ejemplo: 2001:db8:123:1::1-2001:db8:123:1::22 • **IP Wildcard Mask (Máscara comodín IP)**: introduzca una dirección comodín IP con el formato de una dirección IPv4 seguida por una barra diagonal y una máscara (que debe comenzar con cero); por ejemplo, 10.182.1.1/0.127.248.0. En la máscara comodín, un bit cero (0) indica que el bit que se está comparando debe coincidir con el bit de la dirección IP cubierta por el 0. Un bit uno (1) en la máscara es un bit comodín, lo que significa que el bit que se está comparando no necesita coincidir con el bit de la dirección IP cubierta por el 1. Convierta la dirección IP y la máscara comodín en binarias. Para ilustrar la coincidencia: con el fragmento de código binario 0011, una máscara comodín de 1010 da como resultado cuatro coincidencias (0001, 0011, 1001 y 1011). *Puede usar un objeto de dirección del tipo máscara comodín IP únicamente en una regla de política de seguridad.* • **FQDN**: introduzca el nombre de dominio. FQDN se resuelve inicialmente en el momento de la compilación. Una entrada FQDN se actualiza de manera subsiguiente según el TTL del FQDN si el TTL es mayor o igual que el tiempo mínimo de actualización de FQDN; de lo contrario, la entrada de FQDN se actualiza con el tiempo mínimo de actualización de FQDN. El FQDN se resuelve mediante el servidor DNS del sistema o un objeto proxy DNS, si se configura un proxy.
Resolver	Después de seleccionar el tipo de dirección e introducir una dirección IP o FQDN, haga clic en **Resolve (Resolver)** para ver los FQDN o direcciones IP asociados, respectivamente (en función de la configuración de DNS del cortafuegos o Panorama). Usted puede cambiar un objeto de dirección de un FQDN a una máscara de red IP o viceversa. Para cambiar de un FQDN a una máscara de red IP, haga clic en **Resolve (Resolver)** para ver las direcciones IP que determina el FQDN, seleccione una y haga clic en **Use this address (Utilizar esta dirección)**. El tipo de objeto de dirección cambia dinámicamente a máscara de red IP y la dirección IP que seleccionó aparece en el campo de texto. De manera alternativa, para cambiar un objeto de dirección de una máscara de red IP a un FQDN, haga clic en **Resolve (Resolver)** para ver el nombre DNS que determina la máscara de red IP, seleccione el FQDN y haga clic en **Use this FQDN (Utilizar este FQDN)**. El tipo cambia de FQDN y el FQDN aparece en el campo de texto.
Etiquetas	Seleccione o introduzca las etiquetas que desee aplicar a este objeto de dirección. Puede definir una etiqueta aquí o usar la pestaña Objects (Objetos) > Tags (Etiquetas) para crear etiquetas nuevas.

© 2020 Palo Alto Networks, Inc.

Objetos > Grupos de direcciones

Para simplificar la creación de políticas de seguridad, las direcciones que requieren la misma configuración de seguridad se pueden combinar en grupos de direcciones. Un grupo de direcciones puede ser estático o dinámico.

- Grupos de direcciones dinámicas: Un grupo de direcciones dinámicas cumplimenta sus miembros dinámicamente usando búsquedas de etiquetas y filtros basados en etiquetas. Los grupos de direcciones dinámicas son muy útiles si tiene una infraestructura virtual amplia con cambios frecuentes en la ubicación de la máquina virtual o la dirección IP. Por ejemplo, si tiene una configuración de conmutación por error o incluye nuevas máquinas virtuales con frecuencia y le gustaría aplicar una política al tráfico que va o que procede de la nueva máquina sin modificar la configuración o las reglas del cortafuegos.

  Para usar un grupo de direcciones dinámicas en la política, debe realizar las siguientes tareas:

  - Defina un grupo de direcciones dinámicas y haga referencia al mismo en la regla de política.
  - Indique al cortafuegos las direcciones IP y las etiquetas correspondientes para que puedan formarse los grupos de direcciones dinámicas. Esto se puede hacer usando secuencias de comandos externas que usen la XML API en el cortafuegos o un entorno basado en VMware configurando **Device (Dispositivo)** > **VM Information Sources (Orígenes de información de VM)** en el cortafuegos.

  Los grupos de direcciones dinámicas también pueden incluir objetos de direcciones definidas estáticamente. Si crea un objeto de dirección y aplica las mismas etiquetas que ha asignado al grupo de direcciones dinámicas, este incluirá todos los objetos estáticos y dinámicos que coincidan con las etiquetas. Por lo tanto, puede usar etiquetas para agrupar objetos tanto dinámicos como estáticos en el mismo grupo de direcciones.
- Grupos de direcciones estáticas: Un grupo de direcciones estáticas puede incluir objetos de dirección que sean estáticas, grupos de direcciones dinámicas o puede ser una combinación de objetos de dirección y grupos de direcciones dinámicas.

  Para crear un grupo de direcciones, haga clic en **Add (Añadir)** y cumplimente los siguientes campos.

Configuración de un grupo de direcciones	Description (Descripción)
Nombre	Introduzca un nombre que describe el grupo de direcciones (de hasta **63** caracteres). Este nombre aparece en la lista de direcciones cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Lugar	Seleccione esta opción si desea que el grupo de direcciones esté disponible para: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el grupo de direcciones únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el grupo de direcciones únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de grupo de direcciones en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de

© 2020 Palo Alto Networks, Inc.

Configuración de un grupo de direcciones	Description (Descripción)
	manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Description (Descripción)	Introduzca una descripción del objeto (hasta 1.023 caracteres).
Tipo	Seleccione **Static (Estático)** o **Dynamic (Dinámico)**. Para usar un grupo de direcciones dinámicas, use el criterio de coincidencia para incluir los miembros en el grupo. Defina el criterio **Match (Coincidencia)** usando los operadores **AND** u **OR**. *Para ver la lista de atributos del criterio de coincidencia, debe haber configurado el cortafuegos para acceder y recuperar los atributos desde el origen/host. Cada máquina virtual en el origen de información configurado se registra en el cortafuegos, que puede realizar un sondeo de la máquina para recuperar cambios en direcciones IP o en la configuración sin modificaciones en el cortafuegos.* Para un grupo de direcciones estáticas, haga clic en **Add (Añadir)** y seleccione una o más **Addresses (Direcciones)**. Haga clic en **Add (Añadir)** para añadir un objeto o un grupo de direcciones al grupo de direcciones. El grupo puede contener objetos de direcciones y grupos de direcciones tanto estáticas como dinámicas.
Etiquetas	Seleccione o introduzca etiquetas que desee aplicar a este grupo de direcciones. Si desea más información sobre etiquetas, consulte Objects > Tags.

Members Count and Address	Después de añadir un grupo de direcciones, la columna Members Count (Conteo de miembros) de la página **Objects (Objetos)** > **Address Groups (Grupos de direcciones)** indica si los objetos del grupo se propagan de forma dinámica o estática.
	
	• En el caso de un grupo de direcciones estáticas, puede ver el recuento de los miembros en el grupo de direcciones.
	• En un grupo de direcciones que utiliza etiquetas para rellenar dinámicamente miembros o tiene miembros estáticos y dinámicos, haga clic en el enlace **More... (Más...)** de la columna Address (Dirección) para verlos. Ya puede ver las direcciones IP registradas en el grupo de direcciones.
	  • Type (Tipo) indica si la dirección IP es un objeto de dirección estática o se está registrando dinámicamente y muestra la dirección IP.
	  • Action (Acción) le permite **Unregister (Borrar) Tags (Etiquetas)** de una dirección IP. Haga clic en el enlace **Add (Añadir)** para añadir el origen del registro y especificar las etiquetas que desea borrar.

© 2020 Palo Alto Networks, Inc.

Objetos > Regiones

El cortafuegos permite crear reglas de políticas que se apliquen a países concretos y otras regiones. La región está disponible como una opción si especifica el origen y el destino de las políticas de seguridad, políticas de descifrado y políticas DoS. Puede elegir entre una lista estándar de países o utilizar los ajustes de región que se describen en esta sección para definir las regiones personalizadas que se incluirán como opciones de las reglas de la política de seguridad.

Las siguientes tablas describen la configuración regional:

Configuración de región	Description (Descripción)
Nombre	Seleccione un nombre que describa la región. Este nombre aparece en la lista de direcciones cuando se definen políticas de seguridad.
Ubicación geográfica	Para especificar la latitud y la longitud, seleccione esta opción y especifique los valores (formato xxx.xxxxxx). Esta información se utiliza en los mapas de tráfico y amenazas de Appscope. Consulte Monitor > Logs.
addresses	Especifique una dirección IP, un intervalo de direcciones IP o una subred para identificar la región, utilizando cualquiera de los siguientes formatos: x.x.x.x x.x.x.x-a.a.a.a x.x.x.x/n

© 2020 Palo Alto Networks, Inc.

Objectos > Grupos de usuarios dinámicos

Para crear un grupo de usuarios dinámicos, seleccione **Objetos** > **Grupos de usuarios dinámicos** y **añada** un nuevo grupo de usuarios dinámicos y, a continuación, establezca las siguientes configuraciones:

Configuración de grupo de usuarios dinámicos	Description (Descripción)
Nombre	Introduzca un **nombre** que describa a grupo de usuarios dinámicos (hasta 63 caracteres). Este nombre aparece en la lista de usuarios de origen cuando se definen las reglas de la política de seguridad. El nombre ser exclusivo y utilizar únicamente caracteres alfanuméricos, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una **descripción** del objeto (hasta 1023 caracteres).
Lugar (Solo en Panorama)	Seleccione esta opción si desea que los criterios de coincidencia del grupo de usuarios dinámicos estén disponibles para todos los grupos de dispositivos en Panorama. *Panorama no comparte los miembros del grupo con grupos de dispositivos.* Si desactiva esta opción, los criterios de coincidencia del grupo de usuarios dinámicos están disponibles solo para el **grupo de dispositivos** seleccionado en la pestaña **Objetos**.
Deshabilitar anulación (Solo en Panorama)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este grupo de usuarios dinámicos en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Coincidencia	**Añada criterios de coincidencia** para definir los miembros en el grupo de usuarios dinámicos mediante los operadores **AND** o **OR** para incluir varias etiquetas. *Cuando añada criterios de coincidencia, solo se mostrarán las etiquetas existentes. Puede seleccionar una etiqueta existente o crear etiquetas nuevas.*
Etiquetas	(Opcional) Seleccione o especifique las etiquetas de objeto estático que desee aplicar al objeto de grupo de usuarios dinámicos. De esta forma, se etiqueta el objeto del grupo de usuarios dinámicos en sí y no los miembros del grupo. Las etiquetas que seleccione le permiten agrupar elementos relacionados y no son relativos a los criterios de coincidencia. Si desea más información sobre etiquetas, consulte Objects > Tags.

Después de añadir un grupo de usuarios dinámicos, puede ver la siguiente información para el grupo:

© 2020 Palo Alto Networks, Inc.

Columna de grupos de usuarios dinámicos	Description (Descripción)
Ubicación (Solo en Panorama)	Identifica si los criterios de coincidencia para el grupo de usuarios dinámicos están disponibles para cada grupo de dispositivos en Panorama (**Compartido**) o para el grupo de dispositivos seleccionado.
Usuarios	Seleccione **más** para ver la lista de usuarios en el grupo de usuarios dinámicos. • Para añadir etiquetas a los usuarios para su inclusión en el grupo, **registre los usuarios** y luego seleccione el **origen del registro** y las **etiquetas** que desee aplicar al usuario. Cuando las etiquetas del usuario coinciden con los criterios del grupo, el cortafuegos añade el usuario al grupo de usuarios dinámicos. • (Opcional) Especifique un **tiempo de espera** en minutos (el valor predeterminado es 0; el intervalo es de 0 a 43 200) para eliminar usuarios del grupo cuando expire el tiempo especificado. • (Opcional) **Añada usuarios** al grupo o **elimine** usuarios del grupo. • Para eliminar las etiquetas de los usuarios y evitar que se conviertan en miembros del grupo, seleccione los usuarios y **anule el registro de usuarios** y, después, seleccione el **origen del registro** y las **etiquetas**. • Cuando termine de revisar o modificar la lista de usuarios dinámica del grupo de usuarios, haga clic en **Cerrar**.

© 2020 Palo Alto Networks, Inc.

Objetos > Aplicaciones

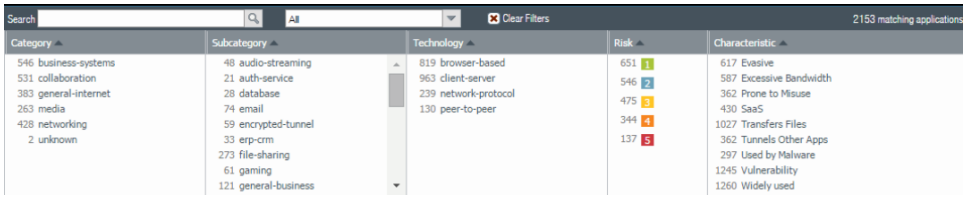
Los siguientes apartados describen la página de **Aplicaciones**.

¿Qué está buscando?	Consulte
Comprender los ajustes y atributos de aplicaciones que aparecen en la página Aplicaciones.	Descripción general de aplicaciones Acciones admitidas en aplicaciones
Añadir una nueva aplicación o modificar una existente.	Definición de aplicaciones

Descripción general de aplicaciones

La página Aplicaciones muestra los diferentes atributos de cada definición de aplicación, como el riesgo de seguridad relativo de la aplicación (1 a 5). El valor del riesgo se basa en criterios como si la aplicación puede compartir archivos, si es proclive a un uso incorrecto o a intentos de evasión de cortafuegos. Los valores mayores indican un mayor riesgo.

El área superior de navegación de la aplicación de la página muestra los atributos que puede utilizar para filtrar la vista de la manera siguiente. El número a la izquierda de cada entrada representa el número total de aplicaciones con ese atributo.



Las publicaciones semanales de contenido incluyen periódicamente nuevos descodificadores y contextos para los que puede desarrollar firmas.

La siguiente tabla describe los detalles de la aplicación: es posible que las aplicaciones personalizadas y las aplicaciones de Palo Alto® Networks muestren algunos o todos estos campos.

Detalles de la aplicación	Description (Descripción)
Nombre	Nombre de la aplicación.
Description (Descripción)	Descripción de la aplicación (hasta 255 caracteres).
Información adicional	Enlaces a sitios web (Wikipedia, Google o Yahoo!) que contienen más información sobre la aplicación.
Puertos estándar	Puertos que utiliza la aplicación para comunicarse con la red.
Depende de	Lista de otras aplicaciones necesarias para el funcionamiento de esta aplicación. Al crear una regla de política para permitir la aplicación

© 2020 Palo Alto Networks, Inc.

Detalles de la aplicación	Description (Descripción)
	seleccionada, también debe asegurarse de permitir otras aplicaciones de las que dependa la aplicación.
Usa implícitamente	Otras aplicaciones de las que depende la aplicación seleccionada pero que no necesita añadir a sus reglas de política de seguridad para permitir la aplicación seleccionada porque dichas aplicaciones son compatibles de manera implícita.
Identificado anteriormente como	Para un nuevo App-ID™ o App-ID que se cambian, esto indica cómo se identificaba anteriormente la aplicación. Esto le ayuda a evaluar si se requieren cambios de política en función de los cambios en la aplicación. Si un App-ID está deshabilitado, las sesiones asociadas a esa aplicación coincidirán con la política como la anteriormente identificada como aplicación. De igual modo, los App-ID deshabilitados aparecerán en los logs como la aplicación como se identificaban anteriormente.
Denegar acción	Los App-ID se desarrollan con una acción de denegación predeterminada que determina cómo responde el cortafuegos cuando la aplicación se incluye en una regla de política de seguridad con una acción deny. La acción de denegación predeterminada puede especificar un descarte silencioso o un restablecimiento de TCP. Puede anular esta acción predeterminada en la política de seguridad.
Características	
Evasiva	Utiliza un puerto o protocolo para cualquier cosa menos su propósito inicial con la intención de atravesar un cortafuegos.
Ancho de banda excesivo	Consume al menos 1 Mbps con regularidad en uso normal.
Prone to Misuse (Propenso al uso indebido)	Habitualmente utilizada para fines nefarios o fácilmente establecida para llegar más allá de las intenciones del usuario.
SaaS	En el cortafuegos, el software como servicio (SaaS) se caracteriza como un servicio en el que el software y la infraestructura son propiedad y están gestionados por el proveedor de servicios de aplicaciones pero en el que conserva el control completo sobre los datos, incluido quién puede crear, compartir y transferir los datos, así como acceder a ellos. Recuerde que en el contexto de cómo se caracteriza una aplicación, las aplicaciones SaaS difieren de los servicios web. Los servicios web son aplicaciones alojadas en las que el usuario no posee los datos (por ejemplo, Pandora) o donde el servicio está compuesto principalmente de datos compartidos proporcionados por numerosos suscriptores con fines sociales (por ejemplo, LinkedIn, Twitter o Facebook).
Capaz de transferir archivos	Tiene la capacidad de transferir un archivo de un sistema a otro a través de una red.
Tuneliza otras aplicaciones	Puede incluir otras aplicaciones en su protocolo.

© 2020 Palo Alto Networks, Inc.

Detalles de la aplicación	Description (Descripción)
Used by Malware (Utilizado por software malintencionado)	El software malintencionado es conocido por utilizar la aplicación con fines de propagación, ataque o robo de datos o se distribuye con software malintencionado.
Tiene vulnerabilidades conocidas	Ha informado públicamente de vulnerabilidades.
Generalizado	Probablemente cuente con más de 1.000.000 de usuarios.
Continue Scanning for Other Applications (Continuar buscando otras aplicaciones)	Indica al cortafuegos que debe seguir intentando buscar coincidencias con otras firmas de aplicaciones. Si no selecciona esta opción, el cortafuegos dejará de buscar coincidencias de aplicaciones adicionales después de la primera firma coincidente.
Características de SaaS	
Filtraciones de datos	Aplicaciones que podrían haber divulgado información segura a una fuente no fiable en los últimos tres años.
Condiciones del servicio insuficientes	Aplicaciones con términos de servicio desfavorables que pueden comprometer los datos empresariales.
Sin certificados	Aplicaciones que no cumplen con los programas o certificaciones actuales de la industria como SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA o FEDRAMP.
Viabilidad financiera insuficiente	Aplicaciones con probabilidad de salir del mercado en los próximos 18 a 24 meses.
Sin restricciones IP	Aplicaciones sin restricciones IP para el acceso de los usuarios.
Clasificación	
Category	La categoría de la aplicación será una de las siguientes: • sistemas empresariales • collaboration (colaboración) • internet general • media (medios) • Conexión a red • unknown
subcategory	Subcategoría en la que se clasifica la aplicación. Las diferentes categorías tienen diferentes subcategorías asociadas a ellas. Por ejemplo, las subcategorías de la categoría de colaboración incluyen correo electrónico, intercambio de archivos, mensajería instantánea, vídeoconferencia por internet, empresas sociales, redes sociales, voip y vídeo, y publicación web. No obstante, las subcategorías de la categoría sistemas empresariales incluyen servicio de autenticación, base de datos, erp-crm, empresa general, gestión, programas

© 2020 Palo Alto Networks, Inc.

Detalles de la aplicación	Description (Descripción)
	de oficina, actualización de software y copia de seguridad de almacenamiento.
Tecnología	La tecnología de la aplicación será una de las siguientes: • cliente-servidor: Una aplicación que utiliza un modelo de servidor cliente donde uno o más clientes se comunican con un servidor en la red. • Protocolo de red: Una aplicación que se utiliza generalmente para la comunicación entre sistemas y que facilita la operación de red. Eso incluye la mayoría de los protocolos de IP. • peer-to-peer: Una aplicación que se comunica directamente con otros clientes para transferir información en vez de basarse en un servidor central para facilitar la comunicación. • Basado en el navegador: Una aplicación que se basa en un explorador web para funcionar.
Riesgo	Riesgo asignado de la aplicación. Para personalizar este ajuste, haga clic en el enlace **Customize (Personalizar)**, introduzca un valor (1 a 5) y haga clic en **OK (Aceptar)**.
Etiquetas	Etiquetas asignadas a una aplicación. **Edite las etiquetas** para añadir o eliminar etiquetas para una aplicación.
Opciones	
Tiempo de espera de sesión	Período de tiempo, en segundos, necesario para agotar el tiempo de espera por inactividad (el intervalo es de 1-604800 segundos). Este tiempo de espera es para protocolos diferentes a TCP o UDP. En el caso de TCP y UDP, consulte las siguientes filas de esta tabla. Para personalizar este ajuste, haga clic en el enlace **Customize (Personalizar)** introduzca un valor y haga clic en **OK (Aceptar)**.
Tiempo de espera de TCP (segundos)	Tiempo de espera, en segundos, para finalizar un flujo de aplicación TCP (el intervalo es de 1-604800). Para personalizar este ajuste, haga clic en el enlace **Customize (Personalizar)** introduzca un valor y haga clic en **OK (Aceptar)**. Un valor de 0 indica que se utilizará el temporizador de sesión global, que es 3600 segundos para TCP.
Tiempo de espera de UDP (segundos):	Tiempo de espera, en segundos, para finalizar un flujo de aplicación UDP (el intervalo es de 1-604800 segundos). Para personalizar este ajuste, haga clic en el enlace **Customize (Personalizar)** introduzca un valor y haga clic en **OK (Aceptar)**.
TCP semicerrado (segundos)	Tiempo máximo, en segundos, que una sesión permanece en la tabla de la sesión entre la recepción del primer paquete FIN y la recepción del segundo paquete FIN o RST. Cuando el temporizador caduca, la sesión se cierra (el intervalo es de 1-604800).

© 2020 Palo Alto Networks, Inc.

Detalles de la aplicación	Description (Descripción)
	Default: Si este temporizador no está configurado en el nivel de aplicación, se utiliza el ajuste global. Si este valor se configura en el nivel de aplicación, cancela el ajuste global **TCP semicerrado**.
Tiempo de espera TCP (segundos)	Tiempo máximo, en segundos, que una sesión permanece en la tabla de la sesión después de la recepción del segundo paquete FIN o un paquete RST. Cuando el temporizador caduca, la sesión se cierra (el intervalo es de 1-600). Default: Si este temporizador no está configurado en el nivel de aplicación, se utiliza el ajuste global. Si este valor se configura en el nivel de aplicación, cancela el ajuste global **Tiempo de espera TCP**.
App-ID habilitado	Indica si App-ID está habilitado o deshabilitado. Si un App-ID está deshabilitado, el tráfico de esa aplicación se tratará como el App-ID **Previously Identified As (Identificado anteriormente como)** tanto en la política de seguridad como en los logs. En el caso de aplicaciones añadidas tras la versión de publicación de contenido 490, tendrá la capacidad de deshabilitarlos mientras revisa el impacto de la política de la nueva aplicación. Tras revisar la política, puede decidir **enable (habilitar)** el App-ID. También tiene la capacidad de **disable (deshabilitar)** una aplicación que haya habilitado anteriormente. En un cortafuegos de vsys múltiples, puede deshabilitar varios App-ID por separado en cada sistema virtual.

Si el cortafuegos no puede identificar una aplicación utilizando el App-ID, el tráfico se clasifica como desconocido: TCP desconocido o UDP desconocido. Este comportamiento se aplica a todas las aplicaciones desconocidas, excepto aquellas que emulan HTTP completamente. Para obtener más información, consulte Monitor > Botnet.

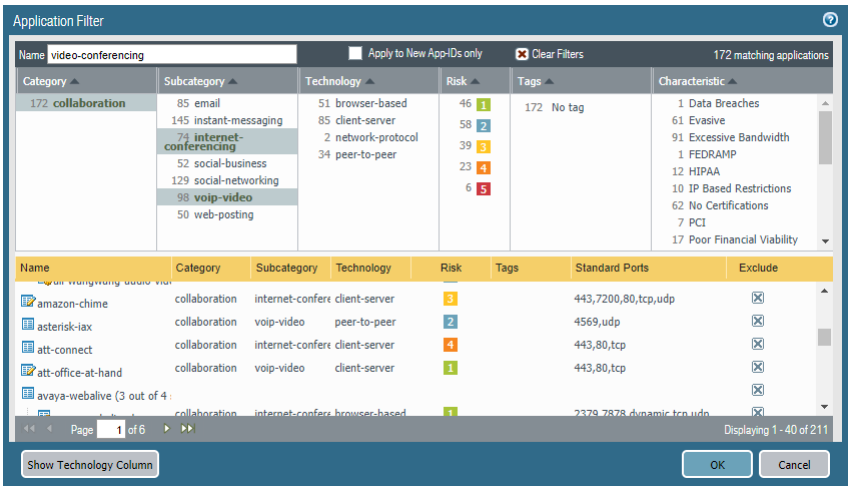
Puede crear nuevas definiciones para aplicaciones desconocidas y a continuación, definir políticas de seguridad para las nuevas definiciones de la aplicación. Además, las aplicaciones que requieren los mismos ajustes de seguridad se pueden combinar en grupos de aplicaciones para simplificar la creación de políticas de seguridad.

Acciones admitidas en aplicaciones

Puede realizar cualquiera de las siguientes acciones en esta página:

Acciones admitidas para aplicaciones	Description (Descripción)
Filtrar por aplicación	• Para buscar una aplicación concreta, introduzca el nombre o descripción de la aplicación en el campo **Search (Buscar)** y pulse **Enter (Intro)**. La lista desplegable le permite buscar o filtrar una aplicación específica o ver **All (Todas)** las aplicaciones, **Custom applications (Aplicaciones personalizadas)**, **Disabled applications (Aplicaciones deshabilitadas)**, o **Tagged applications (Aplicaciones etiquetadas)**

© 2020 Palo Alto Networks, Inc.

Acciones admitidas para aplicaciones	Description (Descripción)
	Se mostrará la aplicación y las columnas de filtrado se actualizarán con las estadísticas de las aplicaciones que coinciden con la búsqueda. Una búsqueda incluye cadenas parciales. Cuando defina políticas de seguridad, puede escribir reglas que se aplicarán a todas las aplicaciones que coincidan con un filtro guardado. Estas reglas se actualizan dinámicamente cuando se añade una nueva aplicación mediante una actualización de contenido que coincida con el filtro. • Para filtrar por atributos de aplicación mostrados en la página, haga clic en un elemento que desee utilizar como base para el filtrado. Por ejemplo, para restringir la lista a la categoría de colaboración, haga clic en **collaboration (colaboración)** y la lista solo mostrará las aplicaciones de esta categoría.  • Para filtrar por más columnas, seleccione una entrada en las otras columnas. El filtrado es sucesivo: En primer lugar, se aplican los filtros de categoría, luego, los filtros de subcategoría, los filtros de tecnología, los filtros de riesgo y, finalmente, los filtros de característica. Por ejemplo, si aplica un filtro de categoría, subcategoría y riesgo, la columna Technology (Tecnología) se restringe automáticamente a las tecnologías que cumplen los requisitos de la categoría y subcategoría seleccionadas, aunque no se haya aplicado un filtro de tecnología de manera explícita. Cada vez que aplique un filtro, la lista de aplicaciones se actualiza automáticamente. Para crear un nuevo filtro de aplicación, consulte Objects > Application Filters.
Añada una nueva aplicación.	To add a new application, consulte Defining Applications.
Visualice o personalice los detalles de la aplicación.	Haga clic en el enlace del nombre de la aplicación para ver la descripción de la aplicación, incluido el puerto estándar y las características de la aplicación, el riesgo, entre otros detalles. Para obtener detalles sobre la configuración de la aplicación, consulte Defining Applications. Un lápiz amarillo ( ) sobre el icono que aparece a la izquierda del nombre de la aplicación significa que la aplicación se ha personalizado.

© 2020 Palo Alto Networks, Inc.

Acciones admitidas para aplicaciones	Description (Descripción)
Deshabilitar una aplicación	Puede **Disable (Deshabilitar)** una aplicación (o varias aplicaciones) para que la firma de aplicación no coincida con el tráfico. Las reglas de seguridad definidas para bloquear, permitir o forzar una aplicación coincidente no se aplican al tráfico de la aplicación cuando la aplicación está deshabilitada. Puede decidir deshabilitar una aplicación que esté incluida con una nueva versión de publicación de contenido porque la implementación de la política de la aplicación podría cambiar cuando la aplicación esté identificada de manera exclusiva. Por ejemplo, el cortafuegos permite una aplicación identificada como tráfico de navegación web antes de una nueva instalación de versión de contenido; después de instalar la actualización de contenido, la aplicación identificada de manera exclusiva ya no coincide con la regla de seguridad que permite el tráfico de navegación web. En este caso, podría decidir deshabilitar la aplicación para que el tráfico que coincida con la firma de aplicación siga estando clasificado como tráfico de exploración web y esté permitido.
Habilitar una aplicación	Seleccione una aplicación deshabilitada y seleccione **Enable (Habilitar)** de modo que el cortafuegos pueda gestionar la aplicación en función de sus políticas de seguridad configuradas.
Importar una aplicación	Para importar una aplicación, haga clic en **Import (Importar)**. Navegue y seleccione el archivo y el sistema virtual de destino en el menú desplegable **Destination (Destino)**.
Exportar una aplicación	Para exportar una aplicación, seleccione esta opción de la aplicación y haga clic en **Export (Exportar)**. Siga las instrucciones para guardar el archivo.
Export an application configuration table (Exporte la tabla de configuración de aplicaciones)	Exporte la información de todas las aplicaciones en formato **PDF/CSV**. Solo se exportan las columnas visibles en la interfaz web. Consulte Datos de la tabla de configuración de exportación.
Evalúe el impacto de la política después de instalar una nueva versión de contenido.	Seleccione **Review Policies (Revisar políticas)** para evaluar la implementación basada en políticas para aplicaciones antes y después de instalar una versión de publicación de contenido. Utilice el cuadro de diálogo Políticas de revisión para revisar el impacto de la política en las nuevas aplicaciones incluidas en una versión de publicación de contenido descargada. El cuadro de diálogo Revisión de políticas le permite añadir o eliminar una aplicación pendiente (una aplicación que se descarga con una versión de publicación de contenido pero no se instala en el cortafuegos) desde o hacia una regla de política de seguridad existente; los cambios en políticas para aplicaciones pendientes no tienen efecto hasta que no se instala la versión de publicación de contenido correspondiente. También puede acceder al cuadro de diálogo Revisión de políticas al descargar e instalar versiones de publicación de contenido en la página **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**.
Etiquete una aplicación.	Una etiqueta predefinida nombrada **sanctioned (sancionada)** está disponible para que etiquete aplicaciones SaaS. Mientras la aplicación

© 2020 Palo Alto Networks, Inc.

Acciones admitidas para aplicaciones	Description (Descripción)
	SaaS es una aplicación que se identifica como **Saas=yes** en los detalles de las características de la aplicación, puede usar la etiquetada sancionada en cualquier aplicación. *Etiquete las aplicaciones como sanctioned (sancionadas) para facilitar la diferenciación del tráfico sancionado de la aplicación SaaS del tráfico de la aplicación SaaS sin sancionar; por ejemplo, al examinar el Informe de utilización de aplicaciones de SaaS o evaluar las aplicaciones de la red.* Seleccione una aplicación, haga clic en **Editar etiquetas** y, desde el menú desplegable, seleccione la etiquetada predefinida **Sancionada** para identificar cualquier aplicación que desee explícitamente permitir en su red. Cuando genere el Informe de uso de la aplicación Saas (consulte Monitor > PDF Reports > SaaS Application Usage), podrá comparar las estadísticas en la aplicación que sancionó con aplicaciones SaaS no sancionadas que se utilizan en su red. Cuando etiqueta una aplicación como sancionada, se aplican las siguientes restricciones: • La etiqueta sancionada no puede aplicarse en un grupo de aplicaciones. • La etiqueta sancionada no puede aplicarse en el nivel **Shared (Compartido)**; puede etiquetar solo una aplicación por grupo de dispositivos o por sistema virtual. • La etiqueta sancionada no puede utilizarse para etiquetar aplicaciones incluidas en una aplicación de contenedor, como el correo de Facebook, el cual es parte de la aplicación de contenedor de Facebook. También puede quitar la etiqueta con **Remove tag (Eliminar etiqueta)** o cancelar la etiqueta con **Override tag (Cancelat etiqueta)**. La opción de cancelar solo está disponible en un cortafuegos que tiene configuraciones heredadas de un grupo de dispositivos de Panorama.

Definición de aplicaciones

Seleccione la página **Objects (Objetos)** > **Applications (Aplicaciones)** para **Add (Añadir)** una nueva aplicación a la evaluación del cortafuegos cuando aplique políticas.

Configuración de nuevas aplicaciones	Description (Descripción)
Pestaña Configuración	
Nombre	Introduzca el nombre de la aplicación (hasta 31 caracteres). Este nombre aparece en la lista de aplicaciones cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser

© 2020 Palo Alto Networks, Inc.

Configuración de nuevas aplicaciones	Description (Descripción)
	exclusivo. Utilice únicamente letras, números, espacios, puntos, guiones y guiones bajos. El primer carácter debe ser una letra.
Lugar	Seleccione esta opción si desea que la aplicación esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, la aplicación únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, la aplicación únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores cancelen la configuración de este objeto de aplicación en los grupos de dispositivos que heredan el objeto. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Description (Descripción)	Introduzca una descripción de la aplicación como referencia general (hasta 255 caracteres).
Category	Seleccione la categoría de la aplicación, como **email (correo electrónico)** o **database (base de datos)**. Esta categoría se utiliza para generar el gráfico Diez categorías de aplicación principales y está disponible para su filtrado (consulte ACC).
subcategory	Seleccione la subcategoría de la aplicación, como **email (correo electrónico)** o **database (base de datos)**. La subcategoría se utiliza para generar el gráfico Diez categorías de aplicación principales y está disponible para su filtrado (consulte ACC).
Tecnología	Seleccione la tecnología de la aplicación.
Aplicación primaria	Especifique una aplicación principal para esta aplicación. Este ajuste se aplica cuando en una sesión coinciden las aplicaciones principal y personalizadas; sin embargo, se registra la aplicación personalizada porque es más específica.
Riesgo	Seleccione el nivel de riesgo asociado con esta aplicación (1= el más bajo a 5= el más alto).
Características	Seleccione las características de la aplicación que pueden poner en riesgo la aplicación. Para ver una descripción de cada característica, consulte Características.
Pestaña Avanzada	

© 2020 Palo Alto Networks, Inc.

Configuración de nuevas aplicaciones	Description (Descripción)
Puerto	Si el protocolo que utiliza la aplicación es TCP y/o UDP, seleccione **Port (Puerto)** e introduzca una o más combinaciones del protocolo y número de puerto (una entrada por línea). El formato general es: *<protocol>/<port>* donde *<port> (puerto)* es un número de puerto único; o **dynamic (dinámica)** para una asignación dinámica de puertos. Ejemplos: TCP/dinámica o UDP/32. Este ajuste se aplica si utiliza **app-default** en la columna Service de una regla de seguridad.
Protocolo IP	Especifique un protocolo IP diferente a TCP o UDP, seleccionando **IP Protocol (Protocolo IP)** e introduciendo el número del protocolo (1 a 255).
Tipo de ICMP	Especifique un tipo de protocolo de mensajes de control de Internet versión 4 (ICMP) seleccionando **ICMP Type (Tipo ICMP)** e introduciendo el número (intervalo 0-255).
Tipo de ICMP6	Especifique un tipo de protocolo de mensajes de control de Internet versión 6 (ICMPv6) seleccionando **ICMP6 Type (Tipo ICMP6)** e introduciendo el número (intervalo 0-255).
ninguno	Especifique firmas independientes de protocolo, seleccionando **None (Ninguno)**.
Tiempo de espera	Introduzca el número de segundos antes de finalizar un flujo de inactividad de una aplicación (intervalo 0-604800 segundos). Un valor de cero indica que se utilizará el tiempo de espera predeterminado de la aplicación. Este valor se utiliza para protocolos diferentes de TCP y UDP en todos los casos y para tiempos de espera TCP y UDP cuando no se especifican los tiempos de espera TCP y UDP.
Tiempo de espera de TCP	Introduzca el número de segundos antes de finalizar un flujo de inactividad de una aplicación TCP (intervalo 0-604800 segundos). Un valor de cero indica que se utilizará el tiempo de espera predeterminado de la aplicación.
Tiempo de espera de UDP	Introduzca el número de segundos antes de finalizar un flujo de inactividad de una aplicación UDP (intervalo 0-604800 segundos). Un valor de cero indica que se utilizará el tiempo de espera predeterminado de la aplicación.
TCP semicerrado	Introduzca el tiempo máximo que una sesión permanece en la tabla de la sesión entre la recepción del primer FIN y la recepción del segundo FIN o RST. Cuando el temporizador caduca, la sesión se cierra. Default: Si este temporizador no está configurado en el nivel de aplicación, se utiliza el ajuste global (el intervalo es 1-604800 segundos). Si este valor se configura en el nivel de aplicación, cancela el ajuste global TCP semicerrado.

© 2020 Palo Alto Networks, Inc.

Configuración de nuevas aplicaciones	Description (Descripción)
Tiempo de espera TCP	Introduzca el tiempo máximo que una sesión permanece en la tabla de la sesión después de la recepción del segundo FIN o RST. Cuando el temporizador caduca, la sesión se cierra. Default: Si este temporizador no está configurado en el nivel de aplicación, se utiliza el ajuste global (el intervalo es 1-600 segundos). Si este valor se configura en el nivel de aplicación, cancela el ajuste global Tiempo de espera TCP.
Analizando	Seleccione los tipos de análisis que desee permitir, en función de los perfiles de seguridad (tipos de archivos, patrones de datos y virus).
Pestaña Firmas	

Firmas	Haga clic en **Add (Añadir)** para agregar una firma nueva y especificar la siguiente información:
	
	• **Signature Name (Nombre de firma)**: Introduzca un nombre para identificar la firma.
	• **Comment (Comentarios)**: introduzca una descripción opcional.
	• **Ordered Condition Match (Importa el orden de las condiciones)**: seleccione si el orden en que se definen las condiciones de la firma es importante.
	• **Scope (Ámbito)**: seleccione si desea aplicar esta firma a la transacción actual en **Transaction (Transacción)** únicamente o a la sesión completa del usuario en **Session (Sesión)**.
	
	Especifique las condiciones que identifican la firma. Estas condiciones se usan para generar la firma que el cortafuegos usa para hacer coincidir los patrones de la aplicación con el tráfico de control:
	
	• Para añadir una condición, seleccione **Añadir condición** o **Añadir condición O**. Para añadir una condición en un grupo, seleccione el grupo y haga clic en **Add Condition (Añadir condición)**.
	• Seleccione un operador en **Operator (Operador)** desde el menú despegable. Las opciones son **Pattern Match (Coincidencia de patrones)**, **Greater Than (Mayor que)**, **Less Than (Menor que)** y **Equal To (Igual a)** y especifique las siguientes opciones:
	
	(Solo para Coincidencia de patrones)
	
	  • **Context (Contexto)**: seleccione uno de los contextos disponibles. Estos contextos se actualizan usando actualizaciones de contenido dinámico.
	  • **Pattern (Patrón)**: indique una expresión regular para especificar valores de contexto de cadena que se aplican a la aplicación personalizada.
	
	  Realice una captura del paquete para identificar el contexto. Consulte Sintaxis de reglas de patrones para ver las reglas de patrones de expresiones regulares.

© 2020 Palo Alto Networks, Inc.

Configuración de nuevas aplicaciones	Description (Descripción)
	(Para mayor que, menor que) • **Context (Contexto)**: seleccione uno de los contextos disponibles. Estos contextos se actualizan usando actualizaciones de contenido dinámico • **Value (Valor)**: especifique un valor para coincidir (el intervalo es 0-4294967295). • **Qualifier and Value (Calificador y valor)**: (Opcional): puede añadir pares de calificador/valor. (Para Igual a únicamente) • **Context (Contexto)**: seleccione de respuestas y solicitudes desconocidas para TCP o UDP (por ejemplo, unknown-req-tcp) o contexto adicionales que están disponibles mediante actualizaciones de contenido dinámico (por ejemplo, dnp3-req-func-code) Para solicitudes y respuestas desconocidas para TCP o UDP, especifique lo siguiente: • **Position (Posición)**: seleccione los primeros cuatro bytes o los segundos cuatro en la carga. • **Mask (Máscara)**: especifique un valor hexadecimal de 4 bytes, por ejemplo, 0xffffff00. • **Value (Valor)**: especifique un valor hexadecimal de 4 bytes, por ejemplo, 0xaabbccdd. Para todos los demás contextos, especifique un valor en **Value (Valor)** que sea pertinente a la aplicación. Para mover una condición dentro de un grupo, seleccione la condición y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. Para mover un grupo, seleccione el grupo y haga clic en el flecha **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. No puede mover condiciones de un grupo a otro.

No es necesario especificar firmas para la aplicación si la aplicación se utiliza únicamente para reglas de application override.

© 2020 Palo Alto Networks, Inc.

Objetos > Grupos de aplicaciones

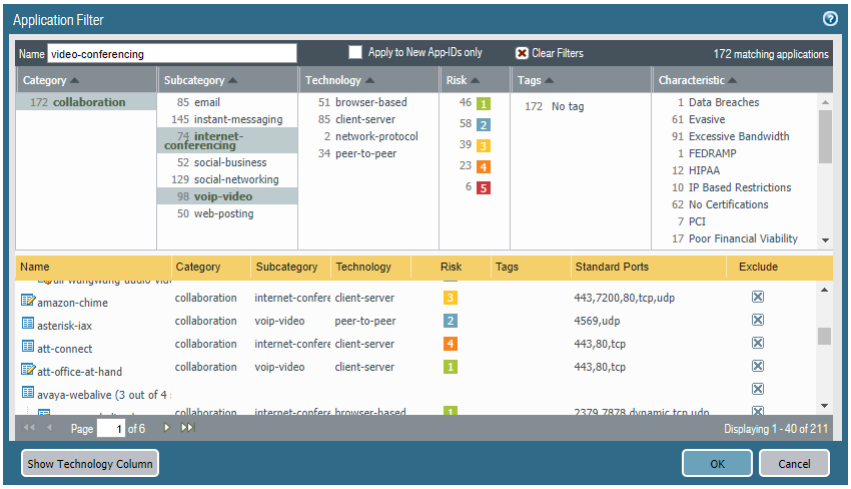
Para simplificar la creación de políticas de seguridad, las aplicaciones que requieren la misma configuración de seguridad se pueden combinar creando un grupo de aplicaciones. Para definir nuevas aplicaciones, consulte Definición de aplicaciones.

Configuración de un nuevo grupo de aplicaciones	Description (Descripción)
Nombre	Introduzca un nombre que describe el grupo de aplicaciones (de hasta 31 caracteres). Este nombre aparece en la lista de aplicaciones cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Lugar	Seleccione esta opción si desea que el grupo de aplicaciones esté disponible para lo siguiente: Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el grupo de aplicaciones únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. Cada grupo de dispositivos en Panorama. Si cancela esta selección, el grupo de aplicaciones únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de grupo de aplicaciones en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
applications	Haga clic en **Add (Añadir)** y seleccione las aplicaciones, filtros de aplicaciones y/o grupos de aplicaciones diferentes que se incluirán en este grupo.

© 2020 Palo Alto Networks, Inc.

Objetos > Filtros de aplicaciones

Los filtros de aplicación ayudan a simplificar las búsquedas repetidas. Para definir un filtro de aplicaciones, haga clic en **Add (Añadir)** e introduzca un nombre para su nuevo filtro. En el área superior de la ventana, haga clic en un elemento que desee utilizar como base para el filtrado. Por ejemplo, para restringir la lista a la categoría de colaboración, haga clic en **collaboration**.



Para filtrar por más columnas, seleccione una entrada en las columnas. El filtrado es sucesivo: se aplican los filtros de categoría primero, a continuación los filtros de subcategoría, tecnología y riesgo, etiquetas y, finalmente, los filtros de característica.

A medida que selecciona los filtros, la lista de aplicaciones que se muestra en la página se actualiza automáticamente.

© 2020 Palo Alto Networks, Inc.

Objetos > Servicios

Cuando define políticas de seguridad de aplicaciones específicas, puede seleccionar uno o más servicios para limitar el número de puertos que las aplicaciones pueden utilizar. El servicio predeterminado es **any (cualquiera)**, que permite todos los puertos TCP y UDP. Los servicios HTTP y HTTPS son los predefinidos, pero puede agregar más definiciones de servicios. Los servicios que se suelen asignar juntos se pueden combinar en grupos de servicios para simplificar la creación de políticas de seguridad (consulte Objects [Objetos] > Service Groups [Grupos de servicio]).

Además, puede utilizar objetos de servicio para especificar períodos de tiempo de espera de sesión basados en el servicio. Esto significa que puede aplicar diferentes valores de tiempo de espera a diferentes grupos de usuarios incluso cuando estos grupos utilizan el mismo servicio TCP o UDP, o que si migra de una política de seguridad basada en puertos con aplicaciones personalizadas a una política de seguridad basada en aplicaciones, podrá conservar con facilidad los valores de tiempo de espera de aplicación personalizados.

La siguiente tabla describe la configuración del servicio:

Configuración de servicios	Description (Descripción)
Nombre	Introduzca el nombre del servicio (de hasta **63** caracteres). Este nombre aparece en la lista de servicios cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del servicio (hasta 1023 caracteres).
Lugar	Seleccione esta opción si desea que el objeto de servicio esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el objeto de servicio únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el objeto de servicio únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de servicio en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
PROTOCOL	Seleccione el protocolo que utiliza el servicio (**TCP** o **UDP**).
Puerto de destino	Introduzca el número de puerto de destino (0 a 65535) o el intervalo de números de puerto (puerto1-puerto2) que utiliza el servicio. Si especifica varios puertos o intervalos, deben estar separados por comas. El puerto de destino es obligatorio.
Puerto de origen	Introduzca el número de puerto de origen (0 a 65535) o el intervalo de números de puerto (puerto1-puerto2) que utiliza el servicio. Si especifica

© 2020 Palo Alto Networks, Inc.

Configuración de servicios	Description (Descripción)
	varios puertos o intervalos, deben estar separados por comas. El puerto de origen es opcional.
Tiempo de espera de sesión	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; se aplica el tiempo de espera de la aplicación. • **Override (Anular)**: defina un tiempo de espera de sesión personalizado para el servicio. Continúe rellenando los campos TCP Timeout (Tiempo de espera de TCP), TCP Half Closed (TCP semicerrado) y TCP Wait Time (Tiempo de espera de TCP).
Los siguientes ajustes muestran solo si selecciona anular los tiempo de espera de la aplicación o crear tiempos de espera de sesión personalizados para un servicio:	
Tiempo de espera de TCP	Establezca 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 de 3600 segundos.
TCP semicerrado	Establezca el tiempo máximo en los segundos que una sesión permanece abierta cuando solo un extremo de la conexión ha intentado cerrar la conexión. Esta configuración se aplica a lo siguiente: • El período de tiempo después de que el cortafuegos recibe el primer paquete FIN (indica que un extremo de la conexión intenta cerrar la sesión), pero antes de que reciba el segundo paquete FIN (indica que el otro extremo de la conexión cierra sesión). • El período de tiempo antes de recibir un paquete RST (indica el intento de restablecer la conexión). Cuando el temporizador expira, la sesión se cierra. El intervalo es de 1 a 604800. El valor predeterminado es de 120 segundos.
TCP Wait Time (Tiempo de espera de TCP)	Configure el tiempo máximo en los segundos que una sesión permanece abierta después de recibir el segundo de dos paquetes FIN necesarios para finalizar una sesión, o después de recibir un paquete RST para restablecer una conexión. Cuando el temporizador expira, la sesión se cierra. El intervalo es de 1 a 600. El valor predeterminado es de 15 segundos.

© 2020 Palo Alto Networks, Inc.

Objetos > Grupos de servicios

Para simplificar la creación de políticas de seguridad, puede combinar los servicios con los mismos ajustes de seguridad en grupos de servicios. Para definir nuevos servicios, consulte Objects > Services.

La siguiente tabla describe la configuración del grupo de servicios:

Configuración de grupos de servicios	Description (Descripción)
Nombre	Introduzca el nombre del grupo de servicios (de hasta **63** caracteres). Este nombre aparece en la lista de servicios cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Lugar	Seleccione esta opción si desea que el grupo de servicio esté disponible para: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el grupo de servicio únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el grupo de servicio únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto del grupo de servicios en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
service	Haga clic en **Add (Añadir)** para agregar servicios al grupo. Seleccione desde el menú desplegable o haga clic en **Service (Servicio)**, en la parte inferior del menú desplegable y especifique la configuración. Consulte Objects > Services para obtener una descripción de la configuración.

© 2020 Palo Alto Networks, Inc.

Objetos > Etiquetas

Las etiquetas le permiten agrupar objetos usando palabras clave o frases. Puede aplicar etiquetas a objetos de dirección, grupos de direcciones (estáticas y dinámicas), aplicaciones, zonas, servicios, grupos de servicios y reglas de políticas. Puede usar un perfil de interfaz de SD-WAN para aplicar una etiqueta de enlace a una interfaz Ethernet. Puede utilizar etiquetas para ordenar o filtrar objetos, y para distinguir objetos visualmente por color. Al aplicar un color a una etiqueta, la pestaña **Policy (Política)** muestra el objeto con un color de fondo.

Debe crear una etiqueta para poder agrupar las reglas usando la etiqueta. Después de asignar las reglas agrupadas por etiqueta, seleccione **View Rulebase as Groups (Ver base de reglas como grupos)** para ver una representación visual de su base de regla de políticas en las etiquetas asignadas. Mientras visualiza su base de reglas como grupos, se mantiene el orden y la prioridad de las políticas. En esta vista, seleccione la etiqueta de grupo para ver todas las reglas agrupadas en función de esa etiqueta.

Hay disponible una etiqueta predefinida denominada **Sanctioned (Autorizada)** para etiquetar aplicaciones (**Objects [Objetos]** > **Applications [Aplicaciones]**). Estas etiquetas son necesarias para fines de precisión (Monitor [Supervisar] > PDF Reports [Informes en PDF] > SaaS Application Usage [Uso de aplicación SaaS]).

¿Qué desea saber?	Consulte:
¿Cómo puedo crear etiquetas?	Crear etiquetas
¿Cómo visualizo la base de reglas como grupos?	Ver base de reglas como grupos
Buscar reglas que estén etiquetadas. Agrupar reglas utilizando etiquetas. Ver etiquetas usadas en una política. Aplique etiquetas a una política.	Gestión de etiquetas
¿Busca más información?	Consulte Política. Consulte Creación de una etiqueta de enlace para un enlace de SD-WAN.

Crear etiquetas

- **Objects (Objetos)** > **Tags (Etiquetas)**

Seleccione **Tags (Etiquetas)** para crear una etiqueta, asignar un color o eliminar, cambiar el nombre y duplicar etiquetas. Cada objeto puede tener hasta 64 etiquetas; cuando un objeto tiene varias etiquetas, muestra el color de la primera etiqueta aplicada.

En el cortafuegos, la pestaña **Tags (Etiquetas)** muestra las etiquetas que usted define de forma local en el cortafuegos o envía desde Panorama al cortafuegos. En Panorama, la pestaña **Tags (Etiquetas)** muestra las etiquetas que usted define en Panorama. Esta pestaña no muestra las etiquetas que se recuperan de forma dinámica de las fuentes de información de VM definidas en el cortafuegos para formar grupos de direcciones dinámicas, ni muestra etiquetas que se definen utilizando la API XML o REST.

© 2020 Palo Alto Networks, Inc.

Cuando crea una nueva etiqueta, la etiqueta se crea automáticamente en el sistema virtual o grupo de dispositivos seleccionado actualmente en el cortafuegos o Panorama.

Configuración de etiqueta	Description (Descripción)
Nombre	Introduzca un nombre de etiqueta exclusivo (de hasta 127 caracteres). El nombre no distingue entre mayúsculas y minúsculas.
Lugar	Seleccione esta opción si desea que la etiqueta esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, la etiqueta únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si desactiva (desmarca) esta opción, la etiqueta únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores cancelen la configuración de esta etiqueta en los grupos de dispositivos que heredan la etiqueta. Esta selección se borra de forma predeterminada, lo que significa que los administradores pueden cancelar la configuración de cualquier grupo de dispositivos que hereda la etiqueta.
Color	Seleccione un color de la paleta de colores en la lista desplegable (el valor predeterminado es ninguno).
Comentarios	Añada una etiqueta o una descripción para describir para qué se usa la etiqueta.

- Añada una etiqueta: Seleccione **Add (Añadir)** para añadir una etiqueta en los siguientes campos:

  También puede crear una nueva etiqueta cuando cree o edite una política en la pestaña **Policies (Políticas)**. La etiqueta se crea automáticamente en el grupo de dispositivos o sistema virtual seleccionado actualmente.
- Edite una etiqueta: Haga clic en una etiqueta para editarla, cambiar el nombre o asignar un color a una etiqueta.
- Elimine una etiqueta: Haga clic en **Delete (Eliminar)** y seleccione la etiqueta. No puede eliminar una etiqueta predefinida.
- Traslade o duplique una etiqueta: Las opciones de trasladar o duplicar una etiqueta le permiten copiar una etiqueta o trasladarla a un grupo de dispositivos o sistema virtual diferente en cortafuegos habilitados para varios sistemas virtuales.

  Mueva o duplique y seleccione la etiqueta. Seleccione la ubicación de **Destination (Destino)** (grupo de dispositivos o sistema virtual). Desactive (desmarque) esta opción para **Error out on first detected error in validation (Error en el primer error detectado en la validación)**, si desea que el proceso de validación detecte todos los errores del objeto antes de mostrar los errores. Esta opción está habilitada de manera predeterminada y el proceso de validación se detiene cuando se detecta el primer error y solo muestra ese error.
- Cancele o revierta una etiqueta (solo Panorama): La opción **Override (Cancelar)** está disponible solo si no seleccionó la opción **Disable override (Deshabilitar cancelación)** al crear la etiqueta. La opción **Override (Cancelar)** le permite cancelar el color asignado a la etiqueta heredado de un grupo de dispositivos compartido o antecesor. El campo **Location (Ubicación)** corresponde al grupo de dispositivos actual.

© 2020 Palo Alto Networks, Inc.

También puede seleccionar la opción **Disable override (Desactivar cancelación)**, para evitar futuros intentos de cancelación.

Seleccione la opción **Revert (Revertir)** para revertir los cambios para deshacer las modificaciones recientes. Cuando revierte una etiqueta, el campo **Location (Ubicación)** muestra el grupo de dispositivos o sistema virtual del que se heredó la etiqueta.

Ver base de reglas como grupos

- **Policies (Políticas)** > **<Rulebase Type (Tipo de base de reglas)>**

Seleccione **View Rulebase as Groups (Ver base de reglas como grupos)** para ver la base de reglas de política usando la etiqueta de grupo. Mientras visualiza su base de reglas como grupos, se mantiene el orden y la prioridad de las políticas. En esta vista, seleccione la etiqueta de grupo para ver todas las reglas agrupadas en función de esa etiqueta.

Al ver la base de reglas como grupos, haga clic en **Group (Grupo)** para mover, cambiar, eliminar o duplicar todas las reglas del grupo de etiquetas seleccionado. La siguiente tabla describe las opciones de gestión de reglas disponible al ver la base de reglas como grupos.

Opción	Description (Descripción)
Mover reglas del grupo a una base de reglas o grupo de dispositivos diferente	Mueva todas las reglas de política del grupo de etiquetas seleccionado a una base de reglas o grupo de dispositivos diferente.
Cambiar grupo de todas las reglas	Mueva todas las reglas del grupo de etiquetas seleccionado a un grupo de etiquetas diferente.
Mover todas las reglas en el grupo	Mueva todas las reglas del grupo de etiquetas seleccionado dentro de la base de reglas.
Eliminar todas las reglas en el grupo	Elimine todas las reglas en el grupo de etiquetas seleccionado.
Duplicar todas las reglas en el grupo	Duplique todas las reglas en el grupo de etiquetas seleccionado.

Mover reglas del grupo a una base de reglas o grupo de dispositivos diferente

Si necesita organizar su base de reglas, seleccione el grupo de etiquetas que contenga las reglas que desea mover y seleccione **Move Rules in Group to Different Rulesbase or Device Group (Mover reglas del grupo a una base de reglas o grupo de dispositivos diferente)** para reasignarlas a una base de reglas o grupo de dispositivos diferente (en lugar de mover cada regla de forma individual). El grupo de dispositivos ya debe existir desde antes del traspaso (no se puede crear durante el traspaso) de las reglas de un grupo de etiquetas a un grupo de dispositivos diferente. Además, puede mover las reglas de un grupo de etiquetas a una base de reglas diferente dentro del mismo grupo de dispositivos.

Para mover las reglas a una base de reglas o grupo de dispositivos diferente, introduzca lo siguiente:

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
IP Destino	El grupo de dispositivos de destino al cual mover las reglas de política.
(Solo Panorama) Tipo de destino	Seleccione si moverá las reglas a la **Pre-Rulebase (Base de reglas previa)** o a la **Post-Rulebase (Base de reglas posterior)** del grupo de dispositivos de destino.
Orden de regla	Seleccione la ubicación de la base de reglas a la cual moverá las reglas. Puede elegir entre lo siguiente: • **Move Top (Mover a la parte superior)**: mueve las reglas al comienzo de la base de reglas del grupo de dispositivos de destino. • **Move Bottom (Mover a la parte inferior)**: mueve las reglas al final de la base de reglas del grupo de dispositivos de destino. • **Before Rule (Antes de la regla)**: mueve las reglas antes de la regla seleccionada en la base de reglas del grupo de dispositivos de destino. • **After Rule (Después de la regla)**: mueve las reglas después de la regla seleccionada en la base de reglas del grupo de dispositivos de destino.
Error en el primer error detectado en la validación	Marque esta casilla para determinar cómo se mostrarán los errores que se encuentren durante la validación. Si está marcada, cada error se mostrará de forma individual. Si está desmarcada, los errores se agruparán y se mostrarán como un único error. Los errores detectados durante la validación impiden la tarea de traspaso de reglas, por lo cual no se moverá ninguna regla al grupo de dispositivos de destino.

Cambiar grupo de todas las reglas

En lugar de editar cada regla, seleccione **Change Group of All Rules (Cambiar grupo de todas las reglas)** para mover un conjunto de reglas de política completo de un grupo de etiquetas a otro grupo de etiquetas existente. El orden de las reglas del grupo de etiquetas se mantiene al pasar al nuevo grupo de etiquetas, pero usted tiene la opción de colocar las reglas nuevas antes de las reglas en el grupo de etiquetas de destino, o después.

Para mover las reglas a un grupo de etiquetas diferente, especifique el grupo de etiquetas de destino y dónde desea ubicar las reglas movidas.

Campo	Description (Descripción)
Seleccionar un grupo por su orden de aparición	Seleccione el grupo de etiquetas.
Mover a la parte superior	**Move Top (Mover a la parte superior)** inserta las reglas al comienzo del grupo de etiquetas de destino.
Mover a la parte inferior	**Move bottom (Mover a la parte inferior)** inserta las reglas al final del grupo de etiquetas de destino.

© 2020 Palo Alto Networks, Inc.

Mover todas las reglas en el grupo

En lugar de reordenar cada regla individualmente, seleccione **Move All Rules in Group (Mover todas las reglas en el grupo)** para mover todas las reglas del grupo de etiquetas seleccionado hacia arriba o hacia abajo en la jerarquía de reglas. El orden de las reglas que se movieron en el grupo de etiquetas se mantiene al pasar al nuevo grupo de etiquetas, pero usted tiene la opción de colocar las reglas nuevas antes de las reglas del grupo de etiquetas de destino, o después.

Para mover las reglas, especifique el grupo de etiquetas de destino y dónde ubicar las reglas movidas.

Campo	Description (Descripción)
Seleccionar un grupo por su orden de aparición	Seleccione el grupo de etiquetas.
Mover a la parte superior	**Move Top (Mover a la parte superior)** inserta las reglas antes del grupo de etiquetas de destino.
Mover a la parte inferior	**Move bottom (Mover a la parte inferior)** inserta las reglas después del grupo de etiquetas de destino.

Eliminar todas las reglas en el grupo

Para simplificar la gestión de reglas, puede seleccionar la opción **Delete All Rules in Group (Eliminar todas las reglas en el grupo)** para reducir sus riesgos de seguridad y mantener su base de reglas de política organizada al eliminar reglas no utilizadas o indeseadas que estén asociadas con un grupo de etiquetas seleccionado.

Duplicar todas las reglas en el grupo

En lugar de volver a crear manualmente las reglas de política existentes en un grupo de etiquetas, **duplique todas las reglas en el grupo** para copiar rápidamente las reglas en el grupo de etiquetas seleccionado del grupo de dispositivos y la base de reglas que desee. El grupo de dispositivos ya debe existir desde antes de la duplicación de reglas (no se puede crear durante la duplicación) de un grupo de etiquetas a un grupo de dispositivos diferente. Además, puede duplicar las reglas de un grupo de etiquetas a una base de reglas diferente dentro del mismo grupo de dispositivos.

Las reglas duplicadas se anexan con el nombre de regla y el siguiente formato: `<Rule Name>-1`. Si una regla se duplica en la misma ubicación que la primera regla duplicada y el nombre no se modifica, se anexará el nombre. Por ejemplo, `<Rule Name>-2`, `<Rule Name>-3`, y así sucesivamente.

Para duplicar reglas, configure los siguientes campos.

Campo	Description (Descripción)
IP Destino	El grupo de dispositivos de destino de las reglas de política duplicadas.
(Solo Panorama) Tipo de destino	Seleccione si duplicará las reglas en la **Pre-Rulebase (Base de reglas previa)** o en la **Post-Rulebase (Base de reglas posterior)** del grupo de dispositivos de destino.
Orden de regla	Seleccione la ubicación de la base de reglas donde desea duplicar las reglas. Puede elegir entre lo siguiente:

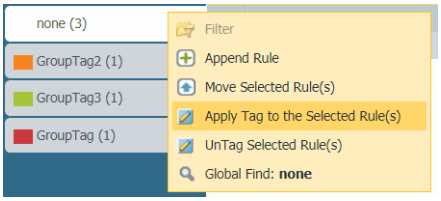
© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **Move Top (Mover a la parte superior)** inserta las reglas duplicadas al comienzo de la base de reglas del grupo de dispositivos de destino. • **Move Bottom (Mover a la parte inferior)** inserta las reglas duplicadas al final de la base de reglas del grupo de dispositivos de destino. • **Before Rule (Antes de la regla)** inserta las reglas duplicadas antes de la regla seleccionada en la base de reglas del grupo de dispositivos de destino. • **After Rule (Después de la regla)** inserta las reglas duplicadas después de la regla seleccionada en la base de reglas del grupo de dispositivos de destino.
Error en el primer error detectado en la validación	Seleccione esta opción para determinar cómo se mostrarán los errores que se encuentren durante la validación. Si está habilitada, cada error se mostrará de forma individual. Si está deshabilitada (desmarcada), los errores se agruparán y se mostrarán como un único error. Los errores detectados durante la validación impiden la tarea de duplicación de reglas, por lo cual no se duplicará ninguna regla en el grupo de dispositivos de destino.

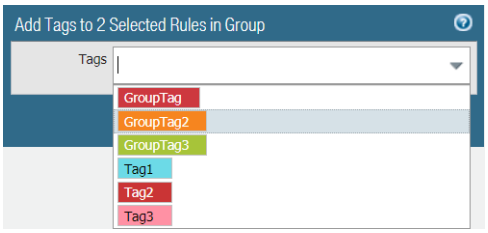
Gestión de etiquetas

La siguiente tabla enumera las acciones que puede realizar al agrupar las reglas según las etiquetas del grupo.

- Etiquete una regla.
  1. Seleccione **View Rules as Groups (Ver reglas como grupos)**.
  2. Seleccione una o varias reglas en el panel derecho.
  3. En la lista desplegable de etiquetas, seleccione **Apply Tag to the Selected Rules (Aplicar etiqueta a las reglas seleccionadas)**.



  4. Añada etiquetas a las reglas seleccionadas.

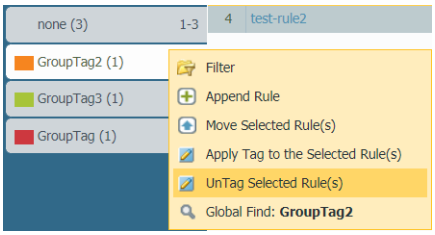


- Vea las reglas asignadas a una etiqueta de grupo.
  1. Seleccione **View Rulebase as Groups (Ver base de reglas como grupos)** para ver las etiquetas del grupo a las que están asignadas sus reglas.

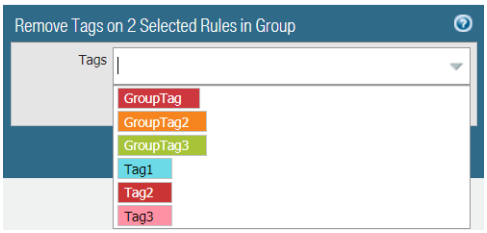
© 2020 Palo Alto Networks, Inc.

2. El panel derecho se actualiza para mostrar las reglas de etiquetas de grupo que tienen cualquiera de las etiquetas seleccionadas.
3. Seleccione la etiqueta del grupo para ver las reglas asignadas al grupo. Las reglas que no tienen asignada una etiqueta de grupo se enumeran en el grupo **none (ninguna)**.

- Elimine la etiqueta de una regla.
  1. Seleccione **View Rulebase as Groups (Ver base de reglas como grupos)** para ver las etiquetas del grupo a las que están asignadas sus reglas.
  2. Seleccione una o varias reglas en el panel derecho.
  3. En la lista desplegable de etiquetas, seleccione **Apply Tag to the Selected Rules (Aplicar etiqueta a las reglas seleccionadas)**.

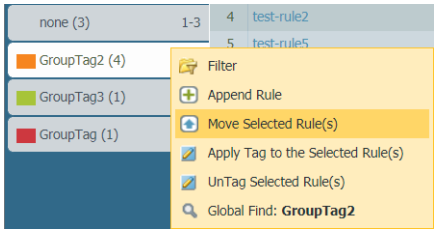


  4. Elimine etiquetas de las reglas seleccionadas. Además, puede seleccionar **Delete All (Eliminar todo)** para eliminar todas las etiquetas asignadas a la regla.



- Reordene una regla utilizando etiquetas.

  Cuando seleccione **View Rulebase as Groups (Ver base de reglas como grupos)**, seleccione una o varias reglas en una etiqueta de grupo, desplace el cursor sobre el número de regla y seleccione **Move Selected Rule(s) (Mover reglas seleccionadas)** en la lista desplegable. No seleccione ninguna regla si desea mover todas las reglas en la etiqueta de grupo seleccionada.



  Seleccione una etiqueta de grupo en la lista desplegable de la ventana para mover reglas y seleccione si desea aplicar la opción **Move Before (Mover antes de)** o **Move After (Mover después de)** con respecto a la etiqueta seleccionada en la lista desplegable.

- Añada una nueva regla que aplique las etiquetas seleccionadas.

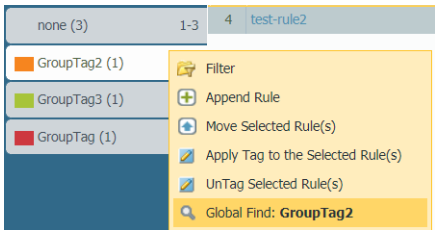
  Cuando seleccione **View Rulebase as Groups (Ver base de reglas como grupos)**, desplace el cursor sobre la etiqueta de grupo y seleccione **Append Rule (Anexar regla)** en la lista desplegable.

  La nueva regla se anexa al final de la lista de reglas asignadas a la etiqueta del grupo.

© 2020 Palo Alto Networks, Inc.

- Busque una etiqueta de grupo.

  Cuando seleccione **View Rulebase as Groups (Ver base de reglas como grupos)**, desplace el cursor sobre la etiqueta de grupo y, en la lista desplegable, seleccione **Global Find (Búsqueda global)**.



- Exporte la tabla de configuración de etiquetas

  Las funciones administrativas pueden exportar la tabla de configuración de etiquetas en formato **PDF/CSV** y pueden aplicar filtros para personalizar el resultado, de modo que solo incluya las columnas que desea. Únicamente las columnas visibles en el cuadro de diálogo Export (Exportación) se exportan. Consulte Datos de la tabla de configuración de exportación.

© 2020 Palo Alto Networks, Inc.

Objects > External Dynamic Lists

Una lista dinámica externa es un objeto de dirección basado en una lista importada de direcciones IP, URL o nombres de dominio que pueden usarse en las reglas de la política para bloquear o permitir tráfico. Esta lista debe estar un archivo de texto guardado en un servidor web al que el cortafuegos pueda acceder. El cortafuegos utiliza la interfaz de gestión (MGT) de forma predeterminada para recuperar esta lista.

Con una licencia de prevención de amenazas activa, Palo Alto Networks® proporciona varias listas IP dinámicas incorporadas que puede usar para bloquear hosts malintencionados Las listas se actualizan diariamente según nuestra investigación de amenazas más reciente.

Puede usar una lista de direcciones IP como objeto de dirección en el origen y destino de sus reglas de política; puede usar una lista de URL en un perfil de filtrado de URL (Objects [Objetos] > Security Profiles [Perfiles de seguridad] > URL Filtering [Filtrado de URL]) o como criterio de coincidencia en las reglas de política de seguridad; y puede usar una lista de dominios en Objects (Objetos) > Security Profiles (Perfiles de seguridad) > Anti-Spyware Profile (Perfil antispyware) para realizar el sinkhole de nombres de dominio especificados.

En cada modelo de cortafuegos, puede utilizar hasta 30 listas dinámicas externas con fuentes únicas en todas las reglas de política de seguridad. El máximo de entradas que admite el cortafuegos en cada tipo de lista varía en función del modelo de cortafuegos (consulte los diferentes límites de cortafuegos de cada tipo de lista externa dinámica). Las entradas de lista solo cuentan para el límite máximo si se utiliza la lista dinámica externa en la política. Si supera la cantidad máxima de entradas que se admiten en un modelo, el cortafuegos genera un log del sistema y omite las entradas que superan el límite. Para comprobar la cantidad de direcciones IP, dominios y direcciones URL que se utilizan actualmente en la política y el número total admitido en el cortafuegos, haga clic en **List Capacities (Capacidades de lista)** (solo cortafuegos).

Las listas dinámicas externas se muestran en orden descendente de evaluación. Use los controles de dirección (parte inferior de la página) para cambiar el orden de la lista. Esto le permite reordenar las listas para asegurarse de que las entradas más importantes de un EDL se confirmen antes de alcanzar los límites de capacidad.

No puede cambiar el orden de EDL cuando las listas se agrupan por tipo.

Para recuperar la última versión de la lista dinámica externa del servidor que la aloja, seleccione una lista dinámica externa y haga clic en **Import Now (Importar ahora)**.

No puede eliminar, copiar ni editar la configuración de las fuentes de las direcciones IP maliciosas Palo Alto Networks.

Haga clic en **Add (Añadir)** para añadir una nueva lista dinámica externa y configurar los ajustes que se describen en la tabla siguiente.

Configuración de una lista dinámica externa	Description (Descripción)
Nombre	Introduzca un nombre para identificar la lista de dinámica externa (de hasta 32 caracteres). Este nombre identifica la lista cuando la utiliza para aplicar la política.
Lugar	Seleccione esta opción si desea que la lista dinámica externa esté disponible para lo siguiente:

© 2020 Palo Alto Networks, Inc.

Configuración de una lista dinámica externa	Description (Descripción)
	• Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, la lista dinámica externa solo estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, la lista dinámica externa solo estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de lista dinámica externa en los grupos de dispositivos que lo heredan. Esta opción está deshabilitada (desmarcada) de manera predeterminada, lo que significa que los administradores pueden invalidar la configuración de cualquier grupo de dispositivos que herede el objeto.
Test Source URL (solo cortafuegos)	Haga clic para verificar que el cortafuegos se puede conectar al servidor que aloja la lista dinámica externa. *Esta prueba no comprueba si el servidor se autentica correctamente.*
Pestaña Create List	

Tipo
No puede mezclar direcciones IP, URL y nombres de dominio en una sola lista. Cada lista debe incluir entradas de solo un tipo.
	Seleccione los tipos de dispositivos de listas dinámicas externas:
	• **Predefined IP List (Lista de IP predefinida)**: las listas de este tipo utilizan una fuente de direcciones IP de alto riesgo o maliciosas de Palo Alto Networks como fuente de entradas de listas (se requiere una licencia activa de Threat Prevention).
	• **IP List (Lista de IP)**: cada lista puede incluir intervalos y subredes de IP en el espacio de direcciones de IPv4 e IPv6. La lista solo debe contener una dirección IP, intervalo o subred por línea. Ejemplo:
	`192.168.80.150/32`
	`2001:db8:123:1::1 or 2001:db8:123:1::/64`
	`192.168.80.0/24 (this indicates all addresses from 192.168.80.0 through 192.168.80.255)`
	`2001:db8:123:1::1 - 2001:db8:123:1::22`
	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.
	• **Domain List (Lista de dominios)**: cada lista puede tener solo una entrada de nombre de dominio por línea. Ejemplo:
	`www.p301srv03.paloalonetworks.com`
	`ftp.example.co.uk`
	`test.domain.net`

© 2020 Palo Alto Networks, Inc.

Configuración de una lista dinámica externa	Description (Descripción)

	Para la lista de dominios incluidos en la lista dinámica externa, el cortafuegos crea un conjunto de firmas personalizadas de spyware normal y de gravedad promedio, de manera que pueda usar la medida de sinkhole para una lista personalizada de dominios.
	• **URL List (Lista de URL)**: cada lista puede tener solo una entrada de URL por línea. Ejemplo:
	`financialtimes.co.in`
	`www.wallaby.au/joey`
	`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`
	`*.example.com/*`
	Para cada lista de URL, la medida predeterminada está configurada como permitir. Para editar la acción predeterminada, consulte Objects (Objetos) > Security Profiles (Perfiles de seguridad) > URL Filtering (Filtrado de URL).

Description (Descripción)	Introduzca una descripción de la lista dinámica externa (hasta 255 caracteres).
Source (Origen)	Introduzca una ruta URL HTTP o HTTPS que contenga el archivo de texto. Por ejemplo, http://192.0.2.20/myfile.txt. • Si la lista dinámica externa es una lista de IP predefinida, seleccione **Palo Alto Networks - High risk IP addresses (Direcciones IP de alto riesgo)** o **Palo Alto Networks - Known malicious IP addresses (Direcciones IP malintencionadas conocidas)** como origen de la lista. • Si la lista dinámica externa es una lista de dominio, el ajuste predeterminado es **Automatically expand to include subdomains (Expandir automáticamente para incluir subdominios)**. Esta opción habilita PAN-OS para evaluar todos los componentes de nivel inferior de los nombres de dominio enumerados en el archivo EDL. *Si su EDL contiene subdominios, estas entradas expandidas se tienen en cuenta para el recuento de capacidad del modelo de su dispositivo. Puede deshabilitar esta función si desea definir manualmente los subdominios. Sin embargo, los subdominios que no se definen explícitamente en la lista no son evaluados por las reglas de política.*
Perfil del certificado	Si la lista dinámica externa tiene una dirección URL HTTPS, seleccione un perfil de certificado existente (cortafuegos y Panorama) o cree un nuevo **Certificate Profile (Perfil del certificado)** (solo cortafuegos) para autenticar el servidor web que aloja la lista. Para obtener más información sobre cómo configurar un perfil de certificado, consulte Device > Certificate Management > Certificate Profile. Default: **None (Disable Cert profile)**

© 2020 Palo Alto Networks, Inc.

Configuración de una lista dinámica externa	Description (Descripción)
	Para maximizar la cantidad de listas dinámicas externas que puede utilizar para aplicar la política, utilice el mismo perfil de certificado para autenticar aquellas listas dinámicas externas que utilizan la misma dirección URL de origen de modo que las listas cuenten como una sola lista dinámica externa. Las listas dinámicas externas de la misma URL de origen que utilizan distintos perfiles de certificados cuentan como listas dinámicas externas únicas.
Autenticación de cliente	Seleccione esta opción (deshabilitada de forma predeterminada) para añadir un nombre de usuario y una contraseña para que el cortafuegos los utilice al acceder a un origen de lista dinámica externa que requiera autenticación HTTP básica. Esta opción solo está disponible cuando la dirección URL de la lista dinámica externa es HTTPS. • **Username (Nombre de usuario)**: indique un nombre de usuario válido para acceder a la lista. • **Password/Confirm Password (Contraseña/Confirmar contraseña)**:introduzca y confirme la contraseña asociada al nombre de usuario.
Buscar actualizaciones	Especifique la frecuencia en la que el cortafuegos recupera la lista del servidor web. Puede establecer un intervalo **Hourly (Por hora)** (predeterminado) , **Five Minute (Cinco minutos)**, **Daily (Diario)**, **Weekly (Semanal)** o **Monthly (Mensual)**, que el cortafuegos respeta para recuperar la lista. El cortafuegos confirma automáticamente los cambios de configuración de inmediato si la última confirmación no se realizó en los últimos 15 minutos; si se realizaron cambios en los últimos 15 minutos, la confirmación se realiza a los 15 minutos de la última confirmación. Cualquier regla de política que haga referencia a la lista está actualizada de modo que el cortafuegos pueda aplicar la política de manera correcta. *No tiene que configurar una frecuencia para una lista IP predefinida porque el cortafuegos recibe dinámicamente actualizaciones de contenido con una licencia activa de Threat Prevention.*
Pestaña List Entries and Exceptions	
Entradas de lista	Muestra las entradas de la lista dinámica externa. • Añadir una entrada como una excepción de lista: seleccione hasta 100 entradas y haga clic en Submit (Enviar) ( ). • Ver un resumen de inteligencia de amenazas de AutoFocus™ de un elemento: pasee el cursor por una entrada, haga clic en el menú desplegable y en **AutoFocus**. Debe tener una licencia de AutoFocus y habilitar la inteligencia contra amenazas de AutoFocus para ver un resumen del elemento (seleccione **Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** y edite los ajustes de **AutoFocus**).

© 2020 Palo Alto Networks, Inc.

Configuración de una lista dinámica externa	Description (Descripción)
	• Comprobar si una dirección IP, un dominio o una URL están en la lista dinámica externa: introduzca un valor en el campo de filtro y aplique el filtro ( ). Restablezca el filtro ([X]) para volver a ver la lista completa.
Excepciones manuales	Muestra excepciones de la lista dinámica externa. • Editar una excepción: haga clic en una excepción y realice los cambios que desee. • Introducir manualmente una excepción: haga clic en **Add (Añadir)** para añadir una nueva excepción manualmente. • Eliminar una excepción de la lista de excepciones manuales: seleccione la excepción que desee y haga clic en **Delete (Eliminar)** para eliminarla. • Comprobar si una dirección IP, un dominio o una URL están en la lista de excepciones manuales: introduzca un valor en el campo de filtro y aplique el filtro ( ). Restablezca el filtro ([X]) para volver a ver la lista completa. No puede guardar los cambios de la lista dinámica externa si tiene entradas duplicadas en la lista de excepciones manuales.

© 2020 Palo Alto Networks, Inc.

Objetos > Objetos personalizados

Cree patrones de datos personalizados, firmas de spyware y vulnerabilidad, y categorías URL para usar con las políticas:

- Objetos > Objetos personalizados > Patrones de datos
- Objetos > Objetos personalizados > Spyware/vulnerabilidad
- Objetos > Objetos personalizados > Categoría de URL

Objetos > Objetos personalizados > Patrones de datos

Los siguientes temas describen los patrones de datos.

¿Qué está buscando?	Consulte:
Crear un patrón de datos.	Configuración de patrones de datos
Obtener más información sobre la sintaxis de los patrones de datos de expresiones regulares y vea algunos ejemplos.	Sintaxis para patrones de datos de expresiones regulares Ejemplos de patrones de datos de expresiones regulares

Configuración de patrones de datos

Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **Data Patterns (Patrones de datos)** para definir las categorías de información confidencial que desea filtrar. Para obtener información sobre la definición de perfiles de filtrado de datos, seleccione Objects > Security Profiles > Data Filtering.

Puede crear tres tipos de patrones de datos para el cortafuegos que se utilizarán al analizar en busca de información confidencial:

- **Predefined (Predefinido)**: Utilice los patrones de datos predefinidos para analizar archivos en busca de números de la seguridad social y de tarjetas de crédito.
- **Regular Expression (Expresión regular)**: Cree patrones de datos personalizados usando expresiones regulares.
- **File Properties (Propiedades de archivo)**: Analice archivos en busca de propiedades y valores de archivos específicos.

Configuración de patrones de datos	Description (Descripción)
Nombre	Introduzca el nombre de patrón de datos (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del patrón de datos (hasta 255 caracteres).
Lugar	Seleccione esta opción si desea que el patrón de datos esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el patrón de datos únicamente estará disponible

© 2020 Palo Alto Networks, Inc.

Configuración de patrones de datos	Description (Descripción)
	para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el patrón de datos únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores cancelen la configuración de este objeto de patrón de datos en los grupos de dispositivos que heredan el objeto. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Tipo de patrón	Seleccione el tipo de patrón de datos que desea crear: • Patrón predefinido • Expresión regular • Propiedades de archivo
Patrón predefinido	Palo Alto Networks proporciona patrones de datos predefinidos para analizar ciertos tipos de información en archivos, por ejemplo, para números de tarjetas de crédito o números de la seguridad social. Para configurar el filtrado de datos basado en un patrón predefinido, seleccione **Add (Añadir)** un patrón y seleccione lo siguiente: • **Name (Nombre)**: Seleccione un patrón predefinido para usar para filtrar datos sensibles. Cuando selecciona un patrón predefinido, la **Description (Descripción)** se rellena automáticamente. • Selecciona el **File Type (Tipo de archivo)** en el que desea detectar el patrón predefinido.
Expresión regular	**Add (Añadir)** un patrón de datos personalizado. Dé al patrón un **Name (Nombre)** descriptivo, establezca el **File Type (Tipo de archivo)** que desea buscar en el patrón de datos e introduzca la expresión regular que define el **Data Pattern (Patrón de datos)**. Para detalles y ejemplos de sintaxis de patrones de datos de expresión regular, consulte: • Sintaxis para patrones de datos de expresiones regulares • Ejemplos de patrones de datos de expresiones regulares
Propiedades de archivo	Genere un patrón de datos para buscar las propiedades del archivo y los valores asociados. Por ejemplo, seleccione **Add (Añadir)** un patrón de datos para filtrar documentos de Microsoft Word y PDF donde el título del documento incluya las palabras "privado", "interno" o "confidencial". • Dé al patrón de datos un **Name (Nombre)** descriptivo. • Seleccione el **File Type (Tipo de archivo)** que desea analizar. • Seleccione la **File Property (Propiedad de archivo)** en la que desea buscar un valor específico. • Introduzca el **Property Value (Valor de la propiedad)** para el que desea analizar.

© 2020 Palo Alto Networks, Inc.

Sintaxis para patrones de datos de expresiones regulares

Cuando se crea un patrón de datos de expresión regular, se aplican los siguientes requisitos generales:

- El patrón debe tener una cadena de al menos 7 bytes con valores fijos. Los 7 bytes no pueden contener punto (`.`), asterisco (`*`), signo más (`+`) o un intervalo (`[a-z]`).
- Cuando necesite que los valores distingan entre mayúsculas y minúsculas, defina patrones para todas las cadenas posibles para que coincidan con todas las variaciones de un término. Por ejemplo, si encontrar documentos denominados como confidenciales, debe crear un patrón que incluya "confidencial", "Confidencial" y "CONFIDENCIAL".

La sintaxis de expresión regular en PAN-OS® es similar a la de los motores de expresiones regulares tradicionales, pero cada motor es único. La tabla siguiente describe la sintaxis compatible con PAN-OS.

Sintaxis de reglas de patrones	Description (Descripción)
.	Busca cualquier carácter único.
?	Busca el carácter o la expresión anterior 0 o 1 veces. Debe incluir la expresión general entre paréntesis. Ejemplo: (abc)?
*	Busca el carácter o la expresión anterior 0 o más veces. Debe incluir la expresión general entre paréntesis. Ejemplo: (abc)*
+	Busca el carácter o la expresión anterior una o más veces. Debe incluir la expresión general entre paréntesis. Ejemplo: (abc)+
|	Especifique uno "or" otro. Ejemplo: ((bif)|(scr)|(exe)) coincide con "bif", "scr" or "exe". *Debe incluir subcadenas alternativas entre paréntesis.*
-	Especifique un intervalo. Ejemplo: [c-z] busca cualquier carácter entre c y z, ambos inclusive.
[ ]	Busque cualquier carácter especificado. Ejemplo: [abz]: coincide con cualquiera de los caracteres a, b o z.
^	Busque cualquier carácter, excepto los especificados. Ejemplo: [^abz] busca cualquier carácter excepto a, b, o z.
{ }	Busque una cadena que contenga un mínimo y un máximo.

© 2020 Palo Alto Networks, Inc.

Sintaxis de reglas de patrones	Description (Descripción)
	Ejemplo: {10-20} busca cualquier cadena entre 10 y 20 bytes (incluidas esas cifras). Debe especificar esto directamente delante de una cadena fija y solo podrá usar guiones (–).
\	Realice una coincidencia literal en cualquier carácter anterior. Debe especificar una barra invertida (\) antes del carácter especificado.
&amp	El ampersand (&) es un carácter especial, por lo que para buscar & en una cadena, debe utilizar **&amp**.

Ejemplos de patrones de datos de expresiones regulares

A continuación se incluyen algunos ejemplos de patrones personalizados válidos:

- .*((Confidencial)|(CONFIDENCIAL))
  - Busca la palabra “Confidencial” o “CONFIDENCIAL” en cualquier parte
  - “.*” al principio especifica que se debe buscar en cualquier parte en la secuencia
  - Dependiendo de los requisitos de distinción entre mayúsculas y minúsculas del descodificador, puede que esto no coincida con “confidencial” (todo en minúsculas)
- .*((Privado &amp Confidencial)|(Privado y Confidencial))
  - Busca “Privado & Confidencial” o “Privado y Confidencial”
  - Es más preciso que buscar “Confidencial”
- .*(Comunicado de prensa).*((Borrador)|(BORRADOR)|(borrador))
  - Busca “Comunicado de prensa” seguido de las diferentes formas de la palabra borrador, lo que puede indicar que el comunicado de prensa no está preparado aún para ser emitido.
- .*(Trinidad)
  - Busca un nombre de código de proyecto, como “Trinidad”

© 2020 Palo Alto Networks, Inc.

Objetos > Objetos personalizados > Spyware/ vulnerabilidad

El cortafuegos permite crear firmas de spyware y vulnerabilidades personalizadas con el motor de amenazas del cortafuegos. Puede escribir patrones de expresiones regulares para identificar comunicaciones de llamada a casa de spyware o intentos de explotar las vulnerabilidades. Los patrones de spyware y vulnerabilidades resultantes están disponibles para su uso en cualquier perfil de vulnerabilidad personalizado. El cortafuegos busca los patrones definidos de forma personalizada en el tráfico de la red y toma las medidas especificadas para la explotación de la vulnerabilidad.

Las publicaciones semanales de contenido incluyen periódicamente nuevos descodificadores y contextos para los que puede desarrollar firmas.

También puede incluir un atributo temporal cuando defina firmas personalizadas especificando un umbral por intervalo para activar posibles acciones en respuesta a un ataque. Las acciones solo se activan una vez alcanzado el umbral.

Utilice la página **Custom Spyware Signature (Firma de spyware personalizada)** para definir firmas de perfiles de antispyware. Utilice la página **Custom Vulnerability Signature (Firma de vulnerabilidad personalizada)** para definir firmas de perfiles de protección frente a vulnerabilidades.

Configuración de firmas de spyware y vulnerabilidades personalizadas	Description (Descripción)
Pestaña Configuración	
ID de amenaza	Ingrese un identificador de número para la configuración (el intervalo de firmas de spyware es 15.000-18.000; el intervalo de firmas de vulnerabilidad es 41.000-45.000).
Nombre	Especifique el nombre de la amenaza.
Lugar	Seleccione esta opción si desea que la firma personalizada esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, la firma personalizada únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, la firma personalizada únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de esta firma en los grupos de dispositivos que heredan la firma. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda la firma.
Comentarios	Introduzca un comentario opcional.

© 2020 Palo Alto Networks, Inc.

Configuración de firmas de spyware y vulnerabilidades personalizadas	Description (Descripción)
Gravedad	Asigne un nivel que indique la gravedad de la amenaza.
Acción predeterminada	Asigne la acción predefinida que se activará si se cumplen las condiciones de la amenaza. Para ver una lista de las acciones, consulte Acciones en los perfiles de seguridad.
DIRECTION	Indique si la amenaza se evaluará desde el cliente al servidor, desde el servidor al cliente, o ambos.
Sistema afectado	Indique indicar si la amenaza afecta al cliente, servidor, a uno de ellos o a ambos. Se aplica a las firmas de vulnerabilidades, pero no a las firmas de spyware.
CVE	Especifique las vulnerabilidades y exposiciones comunes (CVE) como una referencia externa de información y análisis adicional.
Proveedor	Especifique el identificador del proveedor de la vulnerabilidad como una referencia externa de información y análisis adicional.
Bugtraq	Especifique la bugtraq (similar a CVE) como una referencia externa de información y análisis adicional.
Referencia	Añada vínculos a la información o al análisis. La información se muestra cuando un usuario hace clic en la amenaza desde ACC, logs o el perfil de vulnerabilidad.
Pestaña Firmas	
Firma estándar	Seleccione **Standard (Estándar)** y luego **Add (Añadir)** para añadir una nueva firma. Especifique la siguiente información: • **Standard (Estándar)**: introduzca un nombre para identificar la firma. • **Comment (Comentarios)**: introduzca una descripción opcional. • **Ordered Condition Match (Importa el orden de las condiciones)**: seleccione si el orden en que se definen las condiciones de la firma es importante. • **Scope (Ámbito)**: seleccione si desea aplicar esta firma a la transacción actual únicamente o a la sesión completa del usuario. Añada una condición haciendo clic en **Add Or Condition (Añadir condición OR)** o **Add And Condition (Añadir condición AND)**. Para añadir una condición en un grupo, seleccione el grupo y haga clic en **Add Condition (Añadir condición)**. Añada una condición a una firma para que la firma se genere para el tráfico cuando los parámetros que defina para la condición sean verdaderos. Seleccione un operador en **Operator (Operador)** desde el menú despegable. El operador define el tipo de condición que debe ser verdadera para que la firma personalizada coincida con el tráfico. Seleccione un operador de entre **Less Than (Inferior a)**, **Equal To (Igual que)**, **Greater Than (Mayor que)** o **Pattern Match (Coincidencia de patrones)**.

© 2020 Palo Alto Networks, Inc.

Configuración de firmas de spyware y vulnerabilidades personalizadas	Description (Descripción)
	• Cuando seleccione un operador **Coincidencia de patrones**, especifique que lo siguiente sea verdadero para que la firma coincida con el tráfico: • **Context (Contexto)**: seleccione uno de los contextos disponibles. • **Pattern (Patrón)**: especifique una expresión regular. Consulte Sintaxis de reglas de patrones para ver las reglas de patrones de expresiones regulares. • **Qualifier and Value (Calificador y Valor)**: puede añadir pares de calificador/valor. • **Negate (Negar)**: seleccione **Negate (Negar)**para que la firma personalizada coincida con el tráfico únicamente cuando la condición Coincidencia de patrones definida no sea verdadera. Esto le permite garantizar que la firma personali b zada no se active en ciertas circunstancia. *Una firma personalizada no se puede crear únicamente con condiciones Negar; se debe incluir al menos una condición positiva para poder especificar una condición Negar. Asimismo, si el ámbito de la firma se establece como Sesión, no se podrá configurar una condición Negar como la última condición que debe coincidir con el tráfico.* Podrá definir excepciones para firmas de vulnerabilidades o spyware personalizadas utilizando la nueva opción para negar la generación de firmas cuando el tráfico coincida tanto con una firma como con la excepción de la firma. Utilice esta opción para permitir determinado tráfico en su red que de otro modo se clasificaría como spyware o una explotación de la vulnerabilidad. En este caso, la firma se ha generado para el tráfico que coincide con el patrón; el tráfico que coincide con el patrón pero que también coincide con la excepción del patrón se excluye de la generación de firmas y cualquier acción de política asociada (como su bloqueo o denegación). Por ejemplo, puede definir una firma para que se genere para URL redirigidas; sin embargo, ahora también puede crear una excepción cuando la firma no se genere para URL que redirijan a un dominio de confianza.
	• Cuando seleccione un operador **Equal To (Igual que)**, **Less Than (Inferior a)** o **Greater Than (Mayor que)**, especifique que lo siguiente sea verdadero para que la firma coincida con el tráfico: • **Context (Contexto)**: seleccione entre solicitudes desconocidas y respuestas de TCP o UDP. • **Position (Posición)**: seleccione los primeros cuatro bytes o los segundos cuatro en la carga. • **Mask (Máscara)**: especifique un valor hexadecimal de 4 bytes, por ejemplo, 0xffffff00. • **Value (Valor)**: especifique un valor hexadecimal de 4 bytes, por ejemplo, 0xaabbccdd.

© 2020 Palo Alto Networks, Inc.

Configuración de firmas de spyware y vulnerabilidades personalizadas	Description (Descripción)
Firma de combinación	Seleccione **Combination (Combinación)** y especifique la siguiente información: Seleccione **Combination Signatures (Firmas de combinación)** para especificar las condiciones que definirán las firmas: • Añada una condición haciendo clic en **Add AND Condition (Añadir condición AND)** o **Add OR Condition (Añadir condición OR)**. Para añadir una condición en un grupo, seleccione el grupo y haga clic en **Add Condition (Añadir condición)**. • Para mover una condición dentro de un grupo, seleccione la condición y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. Para mover un grupo, seleccione el grupo y haga clic en el flecha **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. No puede mover condiciones de un grupo a otro. Seleccione **Time Attribute (Atributo de fecha y hora)** para especificar la siguiente información: • **Number of Hits (Número de resultados)**: especifique el umbral que activará una acción basada en una política como un número de resultados (1-1000) en un número especificado de segundos (1-3600) • **Aggregation Criteria (Criterios de agregación)**: especifique si los resultados los supervisará la dirección IP de origen, la dirección IP de destino o una combinación de las direcciones IP de origen y destino. • Para mover una condición dentro de un grupo, seleccione la condición y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. Para mover un grupo, seleccione el grupo y haga clic en el flecha **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. No puede mover condiciones de un grupo a otro.

© 2020 Palo Alto Networks, Inc.

Objetos > Objetos personalizados > Categoría de URL

Use la página de categoría de URL para crear su lista personalizada de URL y usarla en un perfil de filtrado de URL o como criterio de coincidencia en reglas de política. En una categoría de URL personalizada, puede añadir entradas URL individualmente o importar un archivo de texto que contenga una lista de URL.

Las entradas URL añadidas a las categorías personalizadas no distinguen entre mayúsculas y minúsculas.

La siguiente tabla describe la configuración de URL personalizada.

Configuración de categorías de URL personalizadas	Description (Descripción)
Nombre	Introduzca un nombre para identificar la categoría de URL personalizada (de hasta 31 caracteres). Este nombre se muestra en la lista de categoría al definir políticas de filtrado de URL y en los criterios de coincidencia para las categorías de URL en las reglas de políticas. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción de la categoría URL (hasta 255 caracteres).
Tipo	Seleccione el tipo de categoría: • **Coincidencia de categoría**—: seleccione **Coincidencia de categoría** para definir una nueva categoría personalizada que contengan las URL que coincidan con todas las categorías de URL especificadas (una URL debe coincidir con todas las categorías de la lista). Especifique entre 2 y 4 categorías. • **Lista de URL**: seleccione **Lista de URL** para añadir o importar una lista de URL para la categoría. Este tipo de categoría también contiene URL añadidas antes de PAN-OS 9.0.
Lugar	Seleccione esta opción si desea que la categoría URL esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si deshabilita (desmarca) esta opción, la categoría URL únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si deshabilita (desmarca) esta opción, la categoría URL únicamente estará disponible para el **Device Group (Grupo de dispositivos** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de URL personalizada en los grupos de dispositivos que lo heredan. Esta selección está

© 2020 Palo Alto Networks, Inc.

Configuración de categorías de URL personalizadas	Description (Descripción)
	deshabilitada de manera predeterminada, lo que significa que los administradores pueden invalidar la configuración de cualquier grupo de dispositivos que herede el objeto.
Sitios	Gestione sitios para la categoría de URL personalizada (cada URL añadida o importada puede tener un máximo de 255 caracteres). • **Add (Añadir)**: **añada** URL (solo una por fila). Cada URL puede tener el formato "www.ejemplo.com" o puede incluir caracteres comodín, como "*.ejemplo.com". Para obtener información adicional en formatos compatibles, consulte la lista de bloqueo en Objetos > Perfiles de seguridad > Filtrado de URL. • **Import (Importar)**: **importe** y explore para seleccionar el archivo de texto que contenga la lista de URL. Introduzca solo una URL por fila. Cada URL puede tener el formato "www.ejemplo.com" o puede incluir caracteres comodín, como "*.ejemplo.com". Para obtener información adicional en formatos compatibles, consulte la lista de bloqueo en Objetos > Perfiles de seguridad > Filtrado de URL. • **Export (Exportar)**: **exporte** entradas de URL personalizadas incluidas en la lista (exportadas como archivo de texto). • **Delete (Eliminar)**: **elimine** una entrada para quitar la URL de la lista. *Para eliminar una categoría personalizada que utilizó en un perfil de filtrado de URL, debe establecer la acción en None (Ninguna) para poder borrar la categoría personalizada. Consulte las acciones de categoría en* Objetos > Perfiles de seguridad > Filtrado de URL.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad

Los perfiles de seguridad proporcionan protección frente a amenazas en la política de seguridad. Cada regla de la política de seguridad puede incluir uno o varios perfiles de seguridad. Los tipos de perfil disponibles son los siguientes:

- Perfiles de antivirus para proteger contra gusanos, virus y troyanos y bloquear descargas de spyware. Consulte Objects > Security Profiles > Antivirus.
- Perfiles de antispyware para bloquear los intentos del spyware en hosts comprometidos para realizar llamadas a casa o balizamiento a servidores externos de comando y control (C2). Consulte Objects > Security Profiles > Anti-Spyware Profile.
- Perfiles de protección de vulnerabilidades para detener los intentos de explotación de fallos del sistema y de acceso no autorizado a los sistemas. Consulte Objects > Security Profiles > Vulnerability Protection.
- Perfiles de filtrado de URL para restringir el acceso de los usuarios a sitios web específicos y/o categorías de sitios web, como compras o apuestas. Consulte Objects > Security Profiles > URL Filtering.
- Perfiles de bloqueo de archivo para bloquear tipos de archivos seleccionados y en la dirección de flujo de sesión especificada (entrante/saliente/ambas). Consulte Objects > Security Profiles > File Blocking.
- Perfiles de análisis de WildFire™ para especificar que se realice un análisis de archivos localmente en el dispositivo WildFire o en la nube de WildFire. Consulte Objects > Security Profiles > WildFire Analysis.
- Perfiles de filtrado de datos que ayudan a evitar que la información confidencial, como los números de tarjetas de crédito o de la seguridad social, salga de una red protegida. Consulte Objects > Security Profiles > Data Filtering.
- Los perfiles de protección DoS se utilizan con las reglas de la política de protección DoS para proteger el cortafuegos frente a los ataques de gran volumen de sesión única y múltiple. Consulte Objects > Security Profiles > DoS Protection.
- Los perfiles de protección de GTP permiten al cortafuegos inspeccionar, validar y filtrar el tráfico de GTP. Consulte Objects > Security Profiles > GTP Protection

Además de los perfiles individuales, puede combinar perfiles que a menudo se aplican en conjunto y crear grupos de perfiles de seguridad (**Objects [Objetos]** > **Security Profile Groups [Grupos de perfiles de seguridad]**).

Acciones en perfiles de seguridad

La acción especifica cómo responde un cortafuegos ante un evento de amenaza. Cada firma de amenaza o virus definida por Palo Alto Networks incluye una acción predeterminada, que suele establecerse como **Alerte (Alerta)**, que le informa del uso de la opción que ha habilitado para que se realice una notificación, o como **Reset Both (Restablecer ambos)**, que restablece ambas partes de la conexión. No obstante, puede definir o cancelar la acción en el cortafuegos. Las siguientes acciones son aplicables al definir perfiles de antivirus, perfiles de antispyware, perfiles de protección de vulnerabilidades, objetos de spyware personalizados, objetos de vulnerabilidades personalizados o perfiles de protección DoS.

Acción	Description (Descripción)	Perfil de antivirus	Perfil de antispyware	perfil de protección frente a vulnerabilida	Objeto personalizado spyware y vulnerabilidad	perfil de protección DoS
predeterminado	Realiza la acción predeterminada especificada internamente para	✓	✓	✓	—	Descarte aleatorio temprano

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)	Perfil de antivirus	Perfil de antispyware	perfil de protección frente a vulnerabilida	Objeto personalizado spyware y vulnerabilidad	perfil de protección DoS
	cada firma de amenaza. Para perfiles de antivirus, realiza la acción predeterminada para la firma de virus.					
Permitir	Permite el tráfico de la aplicación. *La acción Permitir no genera logs relacionados con firmas o perfiles.*	✓	✓	✓	✓	—
Alerta	Genera una alerta para el flujo de tráfico de cada aplicación. La alerta se guarda en el log de amenazas.	✓	✓	✓	✓	✓ Genera una alerta cuando el volumen de ataque (cps) alcanza el umbral de alarma establecido en el perfil.
Descartar	Descarta el tráfico de la aplicación.	✓	✓	✓	✓	—
Restablecer cliente	Para TCP, restablece la conexión de la parte del cliente. Para UDP, descarta la conexión.	✓	✓	✓	✓	—
Restablecer servidor	Para TCP, restablece la conexión de la parte del servidor.	✓	✓	✓	✓	—

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)	Perfil de antivirus	Perfil de antispyware	perfil de protección frente a vulnerabilida	Objeto personalizado spyware y vulnerabilidad	perfil de protección DoS
	Para UDP, descarta la conexión.					
Restablecer ambos	Para TCP, restablece la conexión tanto en el extremo del cliente como en el del servidor. Para UDP, descarta la conexión.	✓	✓	✓	✓	—
Bloquear IP	Bloquea el tráfico de un origen o un par de origen-destino; configurable durante un período de tiempo especificado.	—	—	—	—	✓
Sinkhole	Esta medida redirige las consultas de DNS de dominios maliciosos a una dirección IP de sinkhole. La acción está disponible para las firmas DNS de Palo Alto Networks y para los dominios personalizados incluidos en Objects > External Dynamic Lists.	—	—	—	—	—
Descarte aleatorio temprano	Provoca que el cortafuegos descarte paquetes aleatoriamente cuando las conexiones por segundo alcanzan el umbral de frecuencia de activación en un perfil de protección DoS aplicado a una regla de protección DoS.	—	—	—	—	✓

© 2020 Palo Alto Networks, Inc.

Acción	Description (Descripción)	Perfil de antivirus	Perfil de antispyware	perfil de protección frente a vulnerabilida	Objeto personalizado spyware y vulnerabilidad	perfil de protección DoS
Sincronizar cookies	Provoca que el cortafuegos genere SYN cookies para autenticar un SYN desde un cliente cuando las conexiones por segundo alcancen el umbral de tasa de activación en un perfil de protección DoS aplicado a una regla de protección DoS.	—	—	—	—	✓

No puede eliminar un perfil que se utiliza en una regla de política; Primero debe quitar el perfil de la regla de política.

© 2020 Palo Alto Networks, Inc.

Objects > Security Profiles > Antivirus

En la página **Antivirus Profiles (Perfiles de antivirus)** puede configurar opciones para que el cortafuegos busque virus mediante análisis del tráfico definido. Defina en qué aplicaciones se buscarán virus mediante inspecciones y la acción que se llevará a cabo si se encuentra uno. El perfil predeterminado busca virus en todos los descodificadores de protocolo enumerados, genera alertas de Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP), y Post Office Protocol Version 3 (POP3), y toma las medidas predeterminadas para el resto de las aplicaciones (alerta o denegación), dependiendo del tipo de virus detectado. El perfil se adjuntará después a una regla de la política de seguridad para determinar la inspección del tráfico que atraviesa zonas específicas.

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.

Para añadir un perfil de antivirus nuevo, seleccione Add (Añadir) y realice los siguientes ajustes:

Campo	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de antivirus cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, puntos, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Lugar (Solo en Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este perfil de antivirus 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.
Pestaña Antivirus Especifique la acción para los diferentes tipos de tráfico, como FTP y HTTP.	
Captura de paquetes	Seleccione esta opción si desea capturar paquetes identificados.
Descodificadores y acciones	Para cada tipo de tráfico en el que desee buscar virus, seleccione una acción del menú desplegable. Puede definir diferentes acciones para firmas de antivirus estándar (columna Acción) y firmas generadas por el sistema WildFire (Acción de WildFire).

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Algunos entornos pueden requerir pruebas de estabilidad más largas para firmas de antivirus, por lo que esta opción permite definir distintas acciones para los dos tipos de firmas de antivirus ofrecidos por Palo Alto Networks. Por ejemplo, las firmas de antivirus estándar pasan pruebas de estabilidad más largas (24 horas) en comparación con las firmas de WildFire, que se pueden generar y emitir en 15 minutos o menos tras la detección de la amenaza. Por ello, tal vez prefiera elegir la acción de alerta en las firmas de WildFire en lugar del bloqueo. *Para lograr la máxima seguridad, duplique el perfil de antivirus predeterminado y configure la acción y acción de WildFire Action para todos los descodificadores en reset-both (restablecer ambos), y adjunte el perfil a todas las reglas de política de seguridad que permiten el tráfico.*
Applications Exceptions y Actions	La tabla **Applications Exception (Excepción de aplicaciones)** le permite definir las aplicaciones que no serán inspeccionadas. Por ejemplo, para bloquear todo el tráfico HTTP excepto el de una aplicación específica, puede definir un perfil de antivirus para el que la aplicación es una excepción. **Block (Bloquear)** es la acción del descodificador HTTP, y **Allow (Permitir)** es la excepción de la aplicación. Para cada excepción de la aplicación, seleccione la acción que se adoptará cuando se detecte la amenaza. Para ver una lista de las acciones, consulte Acciones en los perfiles de seguridad. Para buscar una aplicación, comience escribiendo el nombre de la aplicación en el cuadro de texto. Se mostrará una lista con las aplicaciones coincidentes, en la que podrá realizar una selección. *Si considera que se identificó por error una aplicación legítima como portadora de un virus (falso positivo), abra un caso de soporte con TAC para que Palo Alto Networks pueda analizar y resolver el virus identificado erróneamente. Cuando el problema se resuelva, elimine la excepción del perfil.*

Pestaña Excepción de virus

Utilice la pestaña **Virus Exception (Excepción de virus)** para definir una lista de amenazas que serán ignoradas por el perfil de antivirus.

Cree una excepción de virus únicamente si tiene la certeza de que el virus identificado no es una amenaza (falso positivo). Si considera que detectó un falso positivo, abra un caso de soporte con TAC para que Palo Alto Networks pueda analizar y resolver la firma de virus identificada por error. Cuando el problema se resuelva, elimine la excepción del perfil inmediatamente.

ID de amenaza	para añadir amenazas específicas que desee ignorar, introduzca el ID de amenaza y haga clic en **Add (Añadir)**. Los ID de amenaza se presentan como parte de la información del log de amenaza. Consulte Monitor > Logs.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Perfil de antispyware

Puede adjuntar un perfil de antispyware a una regla de política de seguridad para detectar conexiones iniciadas por spyware y malware de comando y control (C2) que se encuentra instalado en sistemas de su red. Puede elegir entre dos perfiles de antispyware predefinidos para adjuntar a una regla de política de seguridad. Cada uno de estos perfiles tiene un conjunto de reglas predefinidas (con firmas de amenazas) organizadas según su gravedad; cada firma de amenaza incluye una acción *predeterminada* especificada por Palo Alto Networks.

- Predeterminado: el perfil predeterminado utiliza la acción predeterminada para cada firma, tal como especifica Palo Alto Networks al crear la firma.
- Estricto: el perfil estricto cancela la acción definida en el archivo de firma para amenazas de gravedad crítica, alta y media, y la establece como la acción de **reset-both (restablecer ambos)**. La acción predeterminada se utiliza con amenazas de gravedad baja e informativa.
- También puede crear perfiles personalizados. Por ejemplo, puede reducir el rigor de la inspección del antispyware del tráfico entre zonas de seguridad de confianza y aprovechar al máximo la inspección del tráfico recibido de Internet o del tráfico enviado a activos protegidos, como granjas de servidores.

Las siguientes tablas describen la configuración del perfil de antispyware:

Configuración de perfil de antispyware	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles antispyware cuando se definen las políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, puntos, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este perfil de antispyware 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.

Pestaña Reglas

Las reglas de antispyware le permiten definir una gravedad personalizada y la medida que se debe adoptar ante cualquier amenaza, un nombre de amenaza específico que contiene el texto que el usuario introduce, o una categoría de amenaza, como adware.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de antispyware	Description (Descripción)
Haga clic en **Add (Añadir)** para añadir una regla nueva, o bien seleccione una existente y seleccione **Find Matching Signatures (Buscar firmas coincidentes)** para filtrar firmas de amenazas basadas en esa regla.	
Nombre de regla	Especifique el nombre de la regla.
Nombre de la amenaza	Introduzca **Any (Cualquiera)** para buscar todas las firmas o introduzca el texto para buscar cualquier firma con el texto indicado como parte del nombre de la firma.
Category	Elija una categoría o seleccione **any** (cualquiera) para buscar coincidencias con todas las categorías.
Acción	Seleccione una acción para cada amenaza. Para ver una lista de las acciones, consulte Acciones en los perfiles de seguridad. *Para lograr la máxima seguridad, utilice la configuración de la acción en el perfil strict (estricto) predefinido.*
Captura de paquetes	Seleccione esta opción si desea capturar paquetes identificados. Seleccione **single-packet (paquete único)** para capturar un paquete cuando se detecte una amenaza o seleccione la opción **extended-capture (captura extendida)** para capturar de 1 a 50 paquetes (el valor predeterminado es 5 paquetes). La captura extendida ofrece mucho más contexto sobre la amenaza al analizar los logs de amenazas. Para ver la captura de paquetes, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)**, busque la entrada del log de su interés y haga clic en la flecha verde hacia abajo, en la segunda columna. Para definir el número de paquetes que deben capturarse, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** y edite la configuración de Content-ID™. Solo se producirá captura de paquetes si la acción es **allow (permitir)** o **alert (alertar)**. Si está definida la opción **block (bloquear)**, la sesión finaliza inmediatamente. *Habilite la captura extendida para los eventos de gravedad crítica, alta y media. Utilice el valor de captura extendida predeterminado de 5 paquetes, lo cual proporciona información suficiente para analizar la amenaza en la mayoría de los casos. (Un tráfico demasiado alto de captura de paquetes puede derivar en la interrupción de las capturas de paquetes). No habilite la captura extendida para eventos informativos y de gravedad baja, debido a que no resulta muy útil en comparación con la captura de información sobre eventos de gravedad mayor, y crea un volumen relativamente alto de tráfico de bajo valor.*
Gravedad	Seleccione un nivel de gravedad [**critical (crítico)**, **high (alto)**, **medium (medio)**, **low (bajo)** o **informational (informativo)**].

Pestaña Excepciones

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de antispyware	Description (Descripción)
Le permiten cambiar la acción de una firma específica. Por ejemplo, puede generar alertas para un conjunto específico de firmas y bloquear todos los paquetes que coincidan con el resto de firmas. Las excepciones de amenazas se suelen configurar cuando se producen falsos positivos. Para facilitar aún más la gestión de amenazas, puede añadir excepciones de amenazas directamente desde la lista **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)**. Asegúrese de obtener las actualizaciones de contenido más recientes para estar protegido ante las nuevas amenazas y contar con nuevas firmas para cualquier falso positivo.	
Excepciones	Seleccione **Enable (Habilitar)** para cada amenaza a la que desee asignar una acción o seleccione **All (Todas)** para responder a todas las amenazas enumeradas. La lista depende del host, categoría y gravedad seleccionada. Si la lista está vacía, no hay amenazas en las selecciones actuales. Utilice excepciones de dirección IP para añadir filtros de dirección IP a una excepción de amenaza. Si las direcciones IP se añaden a una excepción de amenaza, la acción de excepción de amenaza de esa firma cancelará la acción de la regla solo si la firma se activa mediante una sesión con la dirección IP de origen o de destino que coincida con una dirección IP en la excepción. Puede añadir hasta 100 direcciones IP por firma. Con esta opción no tiene que crear una nueva regla de política y un nuevo perfil de vulnerabilidad para crear una excepción para una dirección IP concreta. *Cree una excepción únicamente si tiene la certeza de que una firma identificada como spyware no es una amenaza (es un falso positivo). Si considera que detectó un falso positivo, abra un caso de soporte con TAC para que Palo Alto Networks pueda analizar y resolver la firma identificada por error. Tan pronto como se resuelva el problema, elimine la excepción del perfil.*
Pestaña Firmas DNS El ajuste de **DNS Signatures (Firmas DNS)** proporciona un método adicional de identificación de hosts infectados en una red. Estas firmas detectan búsquedas DNS concretas de nombres de host asociados con malware.	
Pestaña Políticas y configuración Las **DNS Signature Policies (Políticas de firma DNS)** le permiten seleccionar y configurar orígenes de política de firma DNS para permitir, alertar, realizar un sinkhole o bloquear cuando se observen estas consultas, al igual que las firmas de antivirus habituales. Los hosts que realizan consultas DNS en dominios malware aparecerán en el informe de botnet. Asimismo, puede especificar IP de sinkhole en **DNS Sinkhole Settings (Configuración de sinkhole de DNS)** si está realizando un sinkhole de consultas DNS de malware.	
Origen de firma DNS	Le permite seleccionar las listas en las cuales desea ejecutar una acción cuando ocurra una consulta DNS. Existen dos opciones de política de firma DNS predeterminada: • **Firmas DNS de contenido de Palo Alto Networks:** una lista de firmas local para descargar que se actualiza a través de actualizaciones de contenido dinámico. • Seguridad DNS de **Palo Alto Networks:** un servicio de seguridad DNS basado en la nube que realiza análisis proactivos de datos DNS y proporciona acceso total a la base de datos de firmas DNS de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de antispyware	Description (Descripción)
	Este servicio requiere la compra y activación de la licencia de seguridad DNS además de una licencia de prevención de amenazas. De manera predeterminada, las firmas DNS de contenido de Palo Alto Networks a las que se accede de forma local son sometidas al sinkhole, mientras que la seguridad DNS basada en la nube se configura en allow (permitir). Si desea habilitar el sinkhole usando la seguridad DNS, debe configurar la acción en las consultas DNS para que se realice el sinkhole. La dirección predeterminada utilizada para realizar el sinkhole pertenece a Palo Alto Networks (sinkhole.paloaltonetworks.com). Esta dirección no es estática y puede modificarse con actualizaciones de contenido en el cortafuegos o Panorama. Haga clic en **Add (Añadir)** para añadir una lista nueva y seleccione la lista dinámica externa del tipo de dominio que creó. Para crear una nueva lista, consulte Objects > External Dynamic Lists.
Acción para consultas de DNS	Elija una acción que adoptará cuando se realicen búsquedas DNS en sitios conocidos de malware. Las opciones son **alert (alertar)**, **allow (permitir)**, **block (bloquear)** o **sinkhole**. La acción predeterminada para las firmas DNS de Palo Alto Networks es **sinkhole**. La acción DNS sinkhole proporciona a los administradores un método para identificar hosts infectados en la red usando tráfico DNS, incluso aunque el cortafuegos esté antes de un servidor de DNS local (por ejemplo, si el cortafuegos no puede ver el originador de una solicitud de DNS). Si tiene instalada una licencia de prevención de amenazas y tiene habilitado un perfil antispyware en un perfil de seguridad, las firmas basadas en DNS se activarán en las solicitudes de DNS destinadas a dominios de malware. En una implementación típica, donde el cortafuegos está antes del servidor DNS local, el log de amenaza identificará la resolución DNS local como el origen del tráfico, en lugar del host infectado. Las consultas DNS de software malintencionado falsificadas resuelven este problema de visibilidad generando respuestas erróneas a las consultas dirigidas a dominios malintencionados, de modo que los clientes que intenten conectarse a dominios malintencionados (mediante comando y control, por ejemplo) intenten conectarse en su lugar a una dirección IP especificada por el administrador. Los hosts infectados pueden identificarse fácilmente en los logs de tráfico porque cualquier host que intente conectarse a la IP sinkhole está infectado casi con toda seguridad con software malintencionado. *Habilite el sinkhole DNS cuando el cortafuegos no pueda detectar el originador de la consulta DNS (generalmente, cuando el cortafuegos está antes del servidor DNS local), de modo que pueda identificar los hosts infectados. Si no puede realizar el sinkhole del tráfico, bloquéelo.*
Captura de paquetes	Seleccione esta opción para un origen dado si desea capturar paquetes identificados.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de antispyware	Description (Descripción)
	Habilite la captura de paquetes en el tráfico al que se le realizó sinkhole, para que pueda analizarlo y obtener información sobre el host infectado.
Configuración de DNS sinkhole	Después de definir la acción de sinkhole para un origen de firma DNS, especifique una dirección IPv4 o IPv6 que se utilizará para realizar el sinkhole. De manera predeterminada, la dirección IP del sinkhole se configura en un servidor de Palo Alto Networks. Puede usar los logs de tráfico o crear un informe personalizado que filtre las direcciones IP de sinkhole e identifique los clientes afectados. A continuación se detalla la secuencia de eventos que se producirán al realizar un sinkhole en una solicitud de DNS: El software malintencionado en el ordenador de un cliente infectado envía una consulta DNS para resolver un host malintencionado en Internet. La consulta DNS del cliente se envía a un servidor DNS interno, que a su vez realiza una consulta al servidor de DNS público al otro lado del cortafuegos. La consulta DNS coincide con una entrada DNS en el origen de la base de datos de firmas DNS, de modo que la acción sinkhole se llevará a cabo en la consulta. El cliente infectado intenta entonces iniciar una sesión en el host, pero usa la dirección IP falsificada en su lugar. La dirección IP falsificada es la dirección definida en la pestaña Firmas DNS del perfil Antispyware al seleccionar la acción sinkhole. Se alerta al administrador de la consulta DNS malintencionada en el log de amenazas, quien puede entonces buscar en los logs de tráfico la dirección IP sinkhole y localizar fácilmente la dirección IP del cliente que intenta iniciar una sesión con la dirección IP sinkhole.
Pestaña Excepciones La firma DNS **Exceptions (Excepciones)** le permite excluir ID de amenazas específicas de la aplicación de la política. Para añadir amenazas específicas que desee excluir de la política, seleccione o busque un **Threat ID (ID de amenaza)** y haga clic en **Enable (Habilitar)**. Cada entrada proporciona el **ID** de la amenaza, el **Name (Nombre)** y el **FQDN** del objeto.	

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Protección de vulnerabilidades

Una regla de política de seguridad puede incluir especificaciones de un perfil de protección frente a vulnerabilidades que determine el nivel de protección contra desbordamiento de búfer, ejecución de código ilegal y otros intentos de explotar las vulnerabilidades del sistema. Hay dos perfiles predefinidos disponibles para la función de protección de vulnerabilidades:

- El perfil **default (predeterminado)** aplica la acción predeterminada a todas las vulnerabilidades de gravedad crítica, alta y media del servidor y del cliente. No detecta los eventos de protección de vulnerabilidad informativos y bajos.
- El perfil **strict (estricto)** aplica la respuesta de bloqueo a todos los eventos de spyware de gravedad crítica, alta y media y utiliza la acción predeterminada para los eventos de protección de vulnerabilidad bajos e informativos.

Los perfiles personalizados se pueden utilizar para minimizar la comprobación de vulnerabilidades para el tráfico entre zonas de seguridad fiables y para maximizar la protección del tráfico recibido de zonas no fiables, como Internet; y el tráfico enviado a destinos altamente sensibles, como granjas de servidores. Para aplicar los perfiles de protección frente a vulnerabilidades a las políticas de seguridad, consulte Policies > Security.

Aplique un perfil de protección de vulnerabilidad a cada regla de política de seguridad que permita el tráfico para proteger contra los desbordamientos de búfer, la ejecución de código ilegal y otros intentos de aprovechar vulnerabilidades del lado del cliente y del lado del servidor.

Los parámetros de Reglas especifican conjuntos de firmas para habilitar, así como las medidas que se deben adoptar cuando se active una firma de un conjunto.

Los ajustes de Excepciones permiten cambiar la respuesta a una firma concreta. Por ejemplo, puede bloquear todos los paquetes coincidentes con una firma, excepto el del paquete seleccionado, que genera una alerta. La pestaña **Exception (Excepción)** admite funciones de filtrado.

La página **Vulnerability Protection (Protección de vulnerabilidades)** muestra un conjunto predeterminado de columnas. Existen más columnas de información disponibles en el selector de columnas. Haga clic en la flecha a la derecha de un encabezado de columna y seleccione las columnas en el submenú Columnas.

Las siguientes tablas describen la configuración del perfil de protección frente a vulnerabilidades:

Configuración del perfil de protección de vulnerabilidades	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de protección frente a vulnerabilidades cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, puntos, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente:

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de vulnerabilidades	Description (Descripción)
	• Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban 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.
Pestaña Reglas	
Nombre de regla	Especifique un nombre para identificar la regla.
Nombre de la amenaza	Especifique una cadena de texto para buscar. El cortafuegos aplica un conjunto de firmas a la regla buscando nombres de firmas para esta cadena de texto.
Lista CVE	Especifique las vulnerabilidades y exposiciones comunes (CVE) si desea limitar las firmas a las que también coinciden con las CVE especificadas. Cada CVE tiene el formato CVE-aaaa-xxxx, donde aaaa es el año y xxxx es un identificador único. Puede realizar una búsqueda de cadenas en este campo. Por ejemplo, para buscar las vulnerabilidades del año 2011, introduzca “2011”.
Tipo de host	Especifique si desea limitar las firmas de la regla a las del lado del cliente, lado del servidor o (**Any (Cualquiera)**).
Gravedad	Seleccione el nivel de gravedad (**informational (informativo)**, **low (bajo)**, **medium (medio)**, **high (alto)** o **critical (crítico)**) si desea limitar las firmas a las coincidentes con los niveles de gravedad especificados.
Acción	Seleccione la acción que deberá realizarse cuando se active la regla. Para ver una lista de las acciones, consulte Acciones en los perfiles de seguridad. La acción **Default (Predeterminada)** se basa en la acción por defecto que forma parte de cada firma proporcionada por Palo Alto Networks. Para ver la acción predeterminada de una firma, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Vulnerability Protection (Protección frente a vulnerabilidades)** y haga clic en **Add (Añadir)** o seleccione un perfil existente. 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)** asociada.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de vulnerabilidades	Description (Descripción)
	Para obtener máxima seguridad, configure la acción para los eventos de gravedad crítica, alta y media del cliente y del servidor en reset-both (restablecer ambos) y use la acción predeterminada para los eventos de gravedad baja e informativos.
Captura de paquetes	Seleccione esta opción si desea capturar paquetes identificados. Seleccione **single-packet (paquete único)** para capturar un paquete cuando se detecte una amenaza o seleccione la opción **extended-capture (captura extendida)** para capturar de 1 a 50 paquetes (el valor predeterminado es 5 paquetes). La captura extendida ofrece mucho más contexto sobre la amenaza al analizar los logs de amenazas. Para ver la captura de paquetes, seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)** y busque la entrada de log que le interese y haga clic en la flecha verde hacia abajo de la segunda columna. Para definir el número de paquetes que deben capturarse, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** y, a continuación, edite la configuración de Content-ID. Solo se producirá captura de paquetes si la acción es **allow (permitir)** o **alert (alertar)**. Si está definida la opción **block (bloquear)**, la sesión finaliza inmediatamente. *Habilite la captura extendida para los eventos de gravedad crítica, alta y media, y la captura de paquetes únicos para los eventos de gravedad baja. Utilice el valor de captura extendida predeterminado de 5 paquetes, lo cual proporciona información suficiente para analizar la amenaza en la mayoría de los casos. (Un tráfico demasiado alto de captura de paquetes puede derivar en la interrupción de las capturas de paquetes). No habilite la captura de paquetes para eventos informativos, debido a que no resulta muy útil en comparación con la captura de información sobre eventos de gravedad mayor, y crea un volumen relativamente alto de tráfico de bajo valor.* *Aplique la captura extendida de paquetes usando la misma lógica que usa para decidir qué tráfico registrará; tome las capturas extendidas del tráfico que registra, incluido el tráfico que bloquea.*
Pestaña Excepciones	
Threats (Amenazas)	*Cree una excepción de amenaza únicamente si tiene la certeza de que la amenaza identificada no es una amenaza (falso positivo). Si considera que detectó un falso positivo, abra un caso de soporte con TAC para que Palo Alto Networks pueda analizar y resolver la amenaza identificada por error. Cuando el problema se resuelva, elimine la excepción del perfil inmediatamente.*

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de vulnerabilidades	Description (Descripción)
	Seleccione **Enable (Habilitar)** para cada amenaza a la que desee asignar una acción, o seleccionar **All (Todas)** para responder a todas las amenazas indicadas. La lista depende del host, categoría y gravedad seleccionada. Si la lista está vacía, no hay amenazas en las selecciones actuales. Seleccione una acción del menú desplegable o seleccione una opción de la lista desplegable **Action (Acción)** en la parte superior de la lista para aplicar la misma acción a todas las amenazas. Si seleccionó **Show All (Mostrar todas)**, entonces todas las firmas están en la lista. Si no es así, solo las firmas que son excepciones están en la lista. Seleccione **Packet Capture (Captura de paquetes)** si desea capturar paquetes identificados. La base de datos de firma de vulnerabilidad contiene firmas que indican un ataque de fuerza bruta; por ejemplo, el ID de amenaza 40001 se activa en un ataque de fuerza bruta de FTP. Las firmas de fuerza bruta se activan cuando se produce una condición en un determinado umbral temporal. Los umbrales están preconfigurados para firmas de fuerza bruta y se pueden modificar haciendo clic en editar ( ) junto al nombre de la amenaza de la pestaña **Vulnerability (Vulnerabilidad)** (con la opción **Custom (Personalizar)** seleccionada). Puede especificar el número de resultados por unidad de tiempo y si se aplicarán los umbrales de origen, destino u origen-destino. Los umbrales se pueden aplicar en una IP de origen, IP de destino o una combinación de IP de origen y destino. La acción predeterminada se muestra entre paréntesis. La columna CVE muestra los identificadores de vulnerabilidades y exposiciones comunes (CVE). Estos identificadores únicos y comunes son para vulnerabilidades de seguridad de información públicamente conocidas. Utilice la columna IP Address Exemptions (Excepciones de dirección IP) para **Add (Añadir)** filtros de dirección IP a una excepción de amenaza. Cuando añade direcciones IP a una excepción de amenaza, la acción de excepción de la amenaza de esa firma tendrá prioridad sobre la acción de la regla solamente si la firma se activa mediante una sesión con la dirección IP de origen o de destino que coincida con una dirección IP en la excepción. Puede añadir hasta 100 direcciones IP por firma. Debe introducir una dirección IP de unidifusión (es decir, una dirección sin una máscara de red), como 10.1.7.8 o 2001:db8:123:1::1. Al añadir excepciones de dirección IP, no es necesario crear una nueva regla de políticas y un nuevo perfil de vulnerabilidad con el fin de crear una excepción para una dirección IP concreta.
ID de proveedor	Especifique el ID del proveedor si desea limitar las firmas a las coincidentes con la de los Id de los proveedores especificados. Por ejemplo, los ID de proveedor de Microsoft tienen el formato MSaa-xxx, donde aa es el año en formato de dos dígitos y xxx es el identificador único. Por ejemplo, para buscar Microsoft en el año 2009, introduzca “MS09” en el campo Search (Búsqueda).

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de vulnerabilidades	Description (Descripción)
Category	Seleccione una categoría de vulnerabilidad si desea limitar las firmas a las que coinciden con esa categoría.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Filtrado de URL

Puede usar los perfiles de filtrado de URL no solo para controlar el acceso al contenido web, sino también para controlar la manera en que los usuarios interactúan con el contenido web.

¿Qué está buscando?	Consulte:
Controle el acceso a sitios web según la categoría de URL.	Categorías de filtrado de URL
Detecte los envíos de credenciales corporativas y, a continuación, decida las categorías de URL a las que los usuarios pueden enviar credenciales.	Detección de credencial de usuario Categorías de filtrado de URL
Bloquee resultados de búsqueda si el usuario final no está usando la configuración de búsqueda segura más estricta.	Configuración de filtrado URL
Active la creación de logs de encabezados HTTP.	Configuración de filtrado URL
Controlar el acceso a los sitios web utilizando encabezados HTTP personalizados.	Inserción del encabezado HTTP
¿Busca más información?	• Obtenga más información sobre cómo configurar el filtrado de URL. • Utilice las categorías URL para evitar el phishing de credenciales. • Para crear categorías de URL personalizadas, seleccione Objects (Objetos) > Custom Objects (Objetos personalizados) > URL Category (Categoría de URL). • Para importar una lista de URL que desee aplicar, seleccione Objects > External Dynamic Lists.

Configuración general del filtrado de URL

La siguiente tabla describe la configuración general de filtrado de URL:

Configuración general	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de filtrado de URL cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Configuración general	Description (Descripción)
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Lugar	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores anulen la configuración de este perfil de filtrado de URL en grupos de dispositivos que heredan el perfil. 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.

Categorías de filtrado de URL

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** > **Categories (Categorías)** para controlar el acceso a los sitios web basado en las categorías URL.

Ajustes de categorías	Description (Descripción)
Category	Muestra las categorías URL e indica en cuáles puede definir el acceso web y la política de uso. De forma predeterminada, los permisos del **Site Access (Acceso al sitio)** y el **User Credential Submission (Envío de credencial de usuario)** para todas las categorías se establecen en **Allow (Permitir)**. Las categorías y listas de URL se agrupan en tres menús desplegables: • **Custom URL Categories (Categorías URL personalizadas)**: seleccione Objetos > Objetos personalizados > Categoría de URL para definir una categoría de URL personalizada. Puede basar las categorías URL personalizadas en una lista de URL o en numerosas categorías predefinidas. • **External Dynamic URL Lists (Listas de URL dinámicas externas)**: seleccione Objects > External Dynamic Lists para habilitar el cortafuegos para importar una lista de URL desde un servidor web. • **Pre-defined Categories (Categorías predefinidas)**: enumera todas las categorías de URL definidas por PAN-DB, la URL de Palo Alto Networks y la base de datos IP en la nube. *Seleccione Bloquear para bloquear todas las categorías de URL peligrosas conocidas y proteger contra las infiltraciones de exploits, la descarga de malware, la actividad de comando y control y la filtración de datos: comando y control, infracción de derechos de autor, DNS dinámico, extremismo, malware, phishing, evasión de*

© 2020 Palo Alto Networks, Inc.

Ajustes de categorías	Description (Descripción)
	proxy y anonimizadores, desconocido, dominio recién registrado, grayware y parked . *Para introducir gradualmente una política de bloqueo, configure las categorías en continue (continuar) y* cree una página de respuesta personalizada *para informar a los usuarios sobre sus políticas de uso y alertarlos sobre el hecho de que están ingresando en un sitio que puede suponer una amenaza. Después de un tiempo adecuado, realice la transición a la política que bloquea estos sitios potencialmente malintencionados.*
Acceso a sitio	Para cada categoría de URL, seleccione la acción que se adoptará cuando un usuario intente acceder a una URL de esa categoría: • **alert (alerta)**: le permite acceder al sitio web pero añade una alerta al log de la URL cada vez que un usuario accede a la URL. *Configure alert (alertar) como la acción para las categorías de tráfico que no bloquea, para que se registre el intento de acceso y se proporcione visibilidad sobre el tráfico.* • **allow (permitir)**: permite el acceso a los sitios web. *Debido a que allow (permitir) no registra el tráfico no bloqueado, configure alert (alertar) como la acción para las categorías de tráfico que no bloquea, si desea registrar los intentos de acceso y ofrecer visibilidad sobre el tráfico.* • **block (bloquear)**: bloquea el acceso al sitio web. Si el acceso al sitio a una categoría de URL está configurado como block (bloquear), los permisos de envío de credencial de usuario también se establecen automáticamente como block (bloquear). • **continue (continuar(**: muestra una página de advertencia a los usuarios, para recomendarles que no ingresen en el sitio web. Luego el usuario deberá elegir **Continue (Continuar)** para ingresar en el sitio web si decide ignorar la advertencia. *Las páginas Continue (advertencia) no se mostrarán correctamente en equipos cliente configurados para usar un servidor proxy.* • **override (cancelar)**: muestra una página de respuesta que le solicita al usuario que introduzca una contraseña válida para poder acceder al sitio. Configure los ajustes de cancelación de administrador de URL (**Device [Dispositivo]** > **Setup [Configuración]** > **Content ID**) para gestionar la configuración de la contraseña y otros ajustes de cancelación. (Consulte la tabla de configuración de gestión en Device > Setup > Content-ID) *Las páginas Override no se mostrarán correctamente en equipos cliente configurados para usar un servidor proxy.* • **none (ninguna)**(solo URL de categoría personalizada): si tiene categorías de URL personalizadas, establezca la acción en **none (ninguna)** para permitir

© 2020 Palo Alto Networks, Inc.

Ajustes de categorías	Description (Descripción)
	que el cortafuegos herede la asignación de la categoría de filtrado de URL del proveedor de la base de datos de URL. El configurar la acción en **none (ninguna)** le brinda la flexibilidad de ignorar las categorías personalizadas en un perfil de filtrado de URL, a la vez que le permite usar la categoría de URL personalizada como un criterio de coincidencia en las reglas de políticas (seguridad, descifrado y QoS) para realizar excepciones o aplicar acciones diferentes. Para eliminar una categoría de URL personalizada, debe establecer la medida en **none (ninguna)** en cualquier perfil donde se utilice la categoría personalizada. Si desea más información sobre las categorías URL personalizadas, consulte Objects > Custom Objects > URL Category.
Envío de credencial de usuario	Para cada categoría de URL, seleccione **User Credential Submissions (Envíos de credenciales de usuario)** para permitir o impedir que los usuarios envíen credenciales corporativas válidas a una URL de esa categoría. Antes de poder controlar los envíos de credenciales de usuario basados en la categoría de URL, debe habilitar la detección de envío de credenciales (seleccione la pestaña **User Credential Detection (Detección de credencial de usuario)**). Las categorías de URL con el **Site Access (Acceso al sitio)** configurado en block (bloquear) se establecen para bloquear también automáticamente los envíos de credenciales de usuario. • **alert (alertar)**: permite que los usuarios envíen sus credenciales al sitio web, pero generan un log de filtrado de URL cada vez que un usuario envía credenciales a sitios de esta categoría. • **allow (permitir)** (predeterminado): permite que los usuarios envíen sus credenciales al sitio web. • **block (bloquear)**: impide que usuarios envíen credenciales al sitio web. Una página predeterminada de respuesta anti-phishing bloquea los envíos de credenciales de usuario. • **continue (continuar)**: muestra una página de respuesta a los usuarios que les solicita seleccionar **Continue (Continuar)** para enviar credenciales al sitio. De forma predeterminada, se muestra una página de continuación de anti-phishing para advertir a los usuarios cuando intentan enviar credenciales a sitios a los que se recomienda no enviar credenciales. Puede elegir crear una página de respuesta personalizada para advertir a los usuarios contra los intentos de phishing o para educarlos contra la reutilización de credenciales corporativas válidas en otros sitios web.
Comprobar categoría de URL	Haga clic para acceder a la base de datos de filtrado de URL de PAN-DB donde podrá introducir una URL o dirección IP para ver información de categorización.
Dynamic URL Filtering (Filtrado de URL dinámicas) (deshabilitado de forma predeterminada) (configurable solo para BrightCloud)	Seleccione para activar las búsquedas en la nube y categorizar la URL. Esta opción se activa si la base de datos local no puede categorizar la URL. Si la URL no se resuelve después del tiempo de espera de 5 segundos, la respuesta aparece como `Not resolved URL (URL no resuelta)`. *Con PAN-DB, esta opción está habilitada de forma predeterminada y no es configurable.*

© 2020 Palo Alto Networks, Inc.

Configuración de filtrado URL

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** > **URL Filtering Settings (Configuración de filtrado de URL)** para aplicar los ajustes de búsqueda segura y para habilitar la creación de logs del encabezado de HTTP.

Configuración de filtrado URL	Descripciones
Log container page only Solo página de contenedor de log Default: Habilitado	Seleccione esta opción para incluir en el log únicamente las URL que coinciden con el tipo de contenido especificado. El cortafuegos no registra los enlaces web relacionados durante la sesión, tales como los anuncios y los enlaces de contenido, lo cual reduce la creación de logs y la carga de la memoria, a la vez que permite continuar la creación de logs de las URL relevantes. *Si utiliza proxies que ocultan la dirección IP original del origen, habilite la opción de Creación de logs de encabezado HTTP X-Forwarded-For para mantener la dirección IP original del usuario que inicia la solicitud de página web.*
Enable Safe Search Enforcement Default: Disabled (Deshabilitado) No se requiere licencia de filtrado de URL para usar esta función.	Seleccione esta opción para forzar el filtrado de búsquedas seguras estricto. 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. Cuando selecciona el ajuste para Habilitar la aplicación forzada de búsquedas seguras, el cortafuegos bloquea los resultados de la búsqueda si el usuario final no está usando la configuración de búsqueda segura más estricta en la consulta de búsqueda. El cortafuegos puede aplicar forzar la búsqueda segura para los siguientes proveedores de búsquedas: Google, Yahoo, Bing, Yandex y YouTube. Este ajuste es la mejor opción, si bien los proveedores de búsquedas no garantizan que funcione con todos los sitios web. Para utilizar la aplicación forzada de búsqueda segura debe habilitar esta configuración y, a continuación, adjuntar la regla de política de seguridad del perfil de filtrado de URL. A continuación, el cortafuegos bloquea el tráfico de devolución de consultas de búsqueda al que no se aplique la configuración de búsqueda segura más estricta. *Si está realizando una búsqueda en Yahoo Japan (yahoo.co.jp) mientras está registrado en su cuenta de Yahoo!, la opción de bloqueo para el ajuste de búsqueda también debe estar habilitada.* *Para evitar que los usuarios omitan esta función usando otros proveedores de búsquedas, configure el perfil de filtrado de URL para que bloquee la categoría de los motores de búsqueda y que se puedan permitir Bing, Google, Yahoo, Yandex y YouTube.*
Creación de logs del encabezado HTTP	La activación del logging de la cabecera HTTP proporciona visibilidad sobre los atributos incluidos en la solicitud de HTTP enviada a un servidor. Cuando

© 2020 Palo Alto Networks, Inc.

Configuración de filtrado URL	Descripciones
	están activados, uno o varios de los siguientes pares de valores de atributos se graban en el log de filtrado de URL: • Agente-usuario (User-Agent): El navegador web que utilizaba el usuario para acceder a la URL. Esta información se envía en la solicitud de HTTP al servidor. Por ejemplo, el agente-usuario puede ser Internet Explorer o Firefox. El valor Agente-usuario del log admite hasta 1024 caracteres. • Sitio de referencia: URL de la página web que enlazaba el usuario a otra página web; se trata del origen que ha redirigido (referencia) al usuario a la página web que se está solicitando. El valor del sitio de referencia en el log admite hasta 256 caracteres. • X-Forwarded-For: Opción del campo de encabezado que conserva la dirección IP del usuario que ha solicitado la página web. Le permite identificar la dirección IP del usuario. Es especialmente útil si tiene un servidor proxy en su red o ha implementado NAT de origen, algo que enmascara la dirección IP del usuario de tal forma que todas las solicitudes parecen originarse desde la dirección IP del servidor proxy o una dirección IP común. El valor de x reenviado para en el log admite hasta 128 caracteres.

Detección de credencial de usuario

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** > **User Credential Detection (Detección de credenciales de usuario)** para permitir que el cortafuegos detecte cuando los usuarios envían credenciales corporativas.

Configure la detección de credenciales de usuario para que los usuarios puedan enviar credenciales únicamente a los sitios de categorías URL especificadas, lo cual reduce la superficie de ataque al prevenir el envío de credenciales a sitios de categorías no fiables. Si bloquea todas las categorías de URL en un perfil de filtrado de URL para el envío de credenciales de usuario, no necesita verificar las credenciales.

El cortafuegos utiliza uno de entre tres métodos para detectar credenciales válidas enviadas a páginas web. Cada método requiere una User-ID™, que permite al cortafuegos comparar los envíos de nombre de usuario y contraseña a páginas web con credenciales empresariales válidas. Seleccione uno de estos métodos para después continuar y Evitar el phishing de credenciales basado en la categoría de URL.

Debe configurar el cortafuegos para descifrar el tráfico que quiera supervisar para las credenciales de usuario.

Configuración de la detección de credenciales de usuario	Description (Descripción)
Usuario IP	Este método de detección de credenciales comprueba los envíos de nombre de usuario válidos. Puede utilizar este método para detectar envíos de credenciales que incluyan un nombre de usuario corporativo válido (independientemente de la contraseña que lo acompaña). El cortafuegos determina una coincidencia de nombre de usuario al verificar que el nombre de usuario coincide con el usuario registrado en la dirección IP de origen de

© 2020 Palo Alto Networks, Inc.

Configuración de la detección de credenciales de usuario	Description (Descripción)
	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 este método puede emplear cualquiera de los métodos de asignación de usuarios descritos en Asignar direcciones IP a los usuarios.
Asignación de grupos	El cortafuegos determina 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 grupo para detectar cuándo los usuarios envían un nombre de usuario corporativo a un sitio en una categoría restringida. 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. Debe habilitar la asignación de grupos para utilizar este método.
Credencial de dominio	Este método de detección de credenciales permite al cortafuegos comprobar si hay un nombre de usuario corporativo válido y la contraseña asociada. El cortafuegos determina 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 comparar 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 usuario con sesión iniciada. Este modo sólo se admite con el agente de User-ID basado en Windows y requiere que el agente de User-ID esté instalado en un controlador de dominio de sólo lectura (RODC), y esté equipado con el Complemento de servicio de credenciales de identificación de usuario. Para utilizar este método, también debe activar User-ID para Asignar direcciones IP a los usuarios utilizando cualquiera de los métodos de asignación de usuarios admitidos, incluida la Política de autenticación y Captive Portal y GlobalProtect™. Consulte Evitar el phishing de credenciales para obtener información detallada sobre cada uno de los métodos que el cortafuegos puede utilizar para verificar los envíos de credenciales corporativas válidas y los pasos para habilitar la prevención del phishing.
Gravedad de log detectada en nombre de usuario válido	Establezca la gravedad de los logs que indiquen que el cortafuegos detectó un envío de nombre de usuario válida a un sitio web. Esta gravedad del log está asociada a eventos en los que se envía un nombre de usuario válido a sitios web con permisos de envío de credenciales para alertar, bloquear o continuar. Los logs que registran cuando un usuario envía un nombre de usuario válido a un sitio web para el que se permite el envío de credenciales tienen una severidad de información. Seleccionar **Categories (Categorías)** para revisar o ajustar las categorías de URL en las que se permiten y bloquean los envíos de credenciales.

© 2020 Palo Alto Networks, Inc.

Configuración de la detección de credenciales de usuario	Description (Descripción)
	Configure la gravedad de logs en media o superior.

Inserción del encabezado HTTP

Para permitir que el cortafuegos gestione el acceso a la aplicación web insertando encabezados HTTP y sus valores en solicitudes HTTP, seleccione **Objetos** > **Perfiles de seguridad** > **Filtrado de URL** > **Inserción de encabezado HTTP**.

El cortafuegos admite la inserción de encabezados solo para tráfico HTTP/1.x; el cortafuegos no admite la inserción de encabezados para el tráfico HTTP/2.

Puede crear entradas de inserción basadas en un tipo de inserción de encabezado HTTP predefinido o puede crear su propio tipo personalizado. Por lo general, la inserción de encabezados se realiza con encabezados HTTP personalizados, pero también puede insertar encabezados HTTP estándar.

La inserción de encabezados sucede cuando se producen lo siguiente:

1. Una solicitud HTTP coincide con una regla de la política de seguridad con una o más entradas de inserción de encabezado HTTP configuradas.
2. Un dominio específico coincide con el dominio que se detectó en el encabezado de host HTTP.
3. La acción es diferente a `Bloquear`.

El cortafuegos puede realizar la inserción de encabezado HTTP solo con los métodos GET, POST, PUT y HEAD.

Si habilita la inserción de encabezados HTTP y el encabezado identificado no se encuentra en una solicitud, el cortafuegos inserta el encabezado. Si el encabezado identificado existe en la solicitud, el cortafuegos sobreescribe los valores del encabezado con los valores que especifique.

Haga clic en **Add (Añadir)** para añadir una entrada de inserción o seleccione una entrada de inserción existente para modificarla. Cuando sea necesario, también podrá seleccionar una entrada de inserción **eliminarla**.

La acción predeterminada de la lista de bloqueo para una nueva entrada de inserción de encabezado HTTP es Block (Bloquear). Si desea una acción diferente, vaya a Categorías de filtrado de URL y seleccione la acción apropiada. De manera alternativa, añada la entrada de inserción a un perfil configurado con la acción deseada.

Configuración de inserción de encabezados HTTP	Description (Descripción)
Nombre	El **nombre** de esta entrada de inserción de encabezado HTTP.
Tipo	El **tipo** de entrada que desea crear. Las entradas pueden ser predefinidas o personalizadas. El cortafuegos usa actualizaciones de contenido para completar y mantener entradas predefinidas.

© 2020 Palo Alto Networks, Inc.

Configuración de inserción de encabezados HTTP	Description (Descripción)
	Si desea incluir el nombre de usuario en el encabezado HTTP, seleccione **Campos dinámicos**.
Dominios	La inserción de encabezados se produce cuando un dominio en esta lista coincide con el encabezado host de la solicitud de HTTP. Si desea crear una entrada predefinida, la lista de dominio se predefine en una actualización de contenido. En la mayoría de los casos, es suficiente, pero puede añadir o eliminar dominios según sea necesario. Para crear una entrada personalizada, **añada** al menos un dominio a esta lista. Cada nombre de dominio puede tener hasta 256 caracteres y puede identificar, como máximo, 50 dominios para cada entrada. Puede utilizar un asterisco (*) como carácter comodín, que buscará cualquier solicitud con el dominio especificado (por ejemplo, *.etrade.com).
Encabezado	Cuando crea una entrada predefinida, la lista de encabezados se rellena previamente con una actualización de contenido. En la mayoría de los casos, es suficiente, pero puede añadir o eliminar encabezados según sea necesario. Cuando cree una entrada personalizada, añada uno o más encabezados (hasta un total de cinco) a esta lista. Los nombres de encabezados pueden tener hasta 100 caracteres, pero no pueden incluir espacios. Si desea incluir el nombre de usuario en el encabezado HTTP, seleccione **X-Authenticated-User** y luego seleccione el **valor** o **añada** un nuevo encabezado.
Valor	Configure el **valor** con un máximo de 512 caracteres. El valor del encabezado varía según la información que desee incluir en el encabezado HTTP para los dominios especificados. Por ejemplo, gestione el acceso de los usuarios a las aplicaciones SaaS mediante la selección de tipos predefinidos o con entradas personalizadas. Para incluir el nombre de usuario en el encabezado HTTP, seleccione el dominio y el formato de nombre de usuario que requiere el dispositivo de seguridad: • **`($domain)\($user)`** • **`WinNT://($domain)/($user)`** Alternativamente, especifique un formato personalizado con los tokens dinámicos **`($user)`** y **`($domain)`** (por ejemplo, **`($user)@($domain)`**). El cortafuegos completa los tokens dinámicos de usuario y dominio mediante el nombre de usuario principal en el perfil de asignación de grupos. *Utilice cada token dinámico **`($user)`** y **`($domain)`** solo una vez por valor.*

© 2020 Palo Alto Networks, Inc.

Configuración de inserción de encabezados HTTP	Description (Descripción)
Log	Seleccione **Log** para habilitar la creación de logs para esta entrada de inserción de encabezados.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Bloqueo de archivo

Puede adjuntar un perfil de bloqueo de archivos a una regla de la política de seguridad (Policies > Security) para impedir que los usuarios carguen o descarguen los tipos de archivos indicados, o para lanzar una alerta cuando un usuario intente subir o descargar tipos de archivos indicados.

Para lograr la máxima seguridad, aplique el perfil predefinido strict (estricto). Si necesita aplicaciones críticas de soporte que utilizan un tipo de archivo que el perfil strict bloquea, duplique el perfil strict e incluya solo las excepciones de tipo de archivo que necesita. Aplique el perfil duplicado a una regla de política de seguridad que restrinja la excepción solo a los orígenes, destinos y usuarios que deben usar el tipo de archivo. También puede usar Direction (Dirección) para restringir la excepción a la carga o descarga.

Si no bloquea todos los archivos de Windows PE, envíe todos los archivos desconocidos a WildFire para analizarlos. Para las cuentas de usuario, configure la acción en continue (continuar) para ayudar a evitar descargas ocultas en las que sitios web, correos electrónicos o ventanas emergentes malintencionadas provoquen que los usuarios descarguen archivos malintencionados accidentalmente. Informe a sus usuarios que si les aparece un mensaje que les indica continuar con la transferencia de un archivo que no iniciaron intencionadamente, pueden quedar sujetos a una descarga malintencionada.

Las siguientes tablas describen la configuración del perfil de bloqueo de archivos:

Configuración de perfil de bloqueo de archivo	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de bloqueo de archivos cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban 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.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de bloqueo de archivo	Description (Descripción)

Reglas	Defina una o más reglas para especificar la medida que se adoptará (si se especifica alguna) para los tipos de archivos seleccionados. Para añadir una regla, especifique los siguientes ajustes y haga clic en **Add (Añadir)**:
	• **Name (Nombre)**: introduzca un nombre para la regla (hasta 31 caracteres).
	• **Applications (Aplicaciones)**: seleccione las aplicaciones a las que afectará la regla o seleccione **Any (Cualquiera)**.
	• **File Types (Tipos de archivo)**: haga clic en los tipos de archivos y luego en **Add (Añadir)** para ver una lista de los tipos de archivos compatibles. Haga clic en un tipo de archivo para agregarlo al perfil y continuar agregando tipos de archivos adicionales según sea necesario. Si selecciona **Any (Cualquiera)**, la medida definida se toma en todos los tipos de archivos compatibles.
	• **Direction (Dirección)**: seleccione la dirección de la transferencia de archivos [**Upload (Cargar)**, **Download (Descargar)** o **Both (Ambos)**].
	• **Action (Acción)**: seleccione la medida que se adoptará cuando se detecten archivos de los tipos seleccionados:
	  • **Alert (Alertar)**: se añade una entrada al log de amenazas.
	  • **Continue (Continuar)**: aparecerá un mensaje para el usuario indicando que se ha solicitado una descarga y le pide confirmación para continuar. El propósito es advertir al usuario de una posible descarga desconocida (también se conocen como descargas drive-by) y darle al usuario la opción de continuar o detener la descarga.
	  Cuando crea un perfil de bloqueo de archivos con la acción **continue (continuar)**, únicamente puede elegir la aplicación **web-browsing (navegación web)**. Si elige cualquier otra aplicación, el tráfico que coincida con la regla de la política de seguridad no pasará por el cortafuegos debido a que los usuarios no verán ninguna página que les pregunte si desean continuar.
	  • **Block (Bloquear)**: el archivo se bloquea.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Análisis de WildFire

Utilice un perfil de análisis de WildFire para especificar que se realice un análisis de archivos de WildFire localmente en el dispositivo WildFire o en la nube de WildFire. Puede especificar que el tráfico se reenvíe a la nube pública o a la nube privada en función del tipo de archivo, la aplicación o la dirección de transmisión del archivo (carga o descarga). Después de crear un perfil de análisis de WildFire, añadir el perfil a una política (**Policies [Políticas]** > **Security [Seguridad]**) le permite aplicar los ajustes de perfil a cualquier tráfico que coincida con esa política (por ejemplo, una categoría de URL definida en la política).

Use el perfil predeterminado definido previamente para reenviar todos los archivos desconocidos a WildFire para su análisis. Además, configure las actualizaciones de contenido en el dispositivo WildFire para que se descarguen e instalen automáticamente, de modo que siempre tenga el soporte más reciente.

Configuración de perfil de análisis de WildFire	
Nombre	Introduzca un nombre descriptivo para el perfil de análisis de WildFire (hasta 31 caracteres). Este nombre aparecerá en la lista de perfiles de análisis de WildFire entre los que puede elegir al definir una regla de política de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Opcionalmente, puede describir las reglas de perfil o el uso previsto del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban 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.
Reglas	Defina una o más reglas para especificar que el tráfico se reenvíe a la nube pública de WildFire o al dispositivo WildFire (nube privada) para su análisis. • Introduzca un **Name (Nombre)** descriptivo para cada regla que añada al perfil (hasta 31 caracteres).

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de análisis de WildFire	

	• Añada una **Application (Aplicación)** para que el tráfico de cualquier aplicación coincida con la regla y se reenvíe al destino de análisis especificado.
	• Seleccione un **File Type (Tipo de archivo)** para su análisis en el destino de análisis definido para la regla.
	
	La nube privada de WildFire (alojada en un dispositivo WildFire) no admite el análisis de archivos APK, Mac OS X y Linux.
	
	• Aplique la regla al tráfico dependiendo de la **Direction (Dirección)** de la transmisión. Puede aplicar la regla para cargar tráfico, descargar tráfico o ambas acciones.
	• Seleccione el **Destination (Destino)** del tráfico que se reenviará para su análisis:
	  • Seleccione la nube pública para que todo el tráfico que coincida con la regla se reenvíe a la nube pública de WildFire para su análisis.
	  • Seleccione la nube privada para que todo el tráfico que coincida con la regla se reenvíe al dispositivo de WildFire para su análisis.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Filtrado de datos

El filtrado de datos permite al cortafuegos detectar información confidencial —como números de tarjeta de crédito o de seguridad social, o documentos corporativos internos— e impedir que salga de una red segura. Antes de habilitar el filtrado de datos, vaya a Objects > Custom Objects > Data Patterns para definir el tipo de datos que desea filtrar (como números de seguridad social o nombres de documentos que contengan la palabra "confidencial"). Puede añadir varios objetos de patrón de datos a un solo perfil de filtrado de datos; cuando se adjunta a una regla de la política de seguridad, el cortafuegos escanea el tráfico permitido de cada patrón de datos y bloquea el tráfico que coincide con la configuración del perfil de filtrado de datos.

Configuración de perfiles de filtrado de datos	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de reenvío de logs cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este perfil de filtrado de datos en los grupos de dispositivos que heredan el perfil. 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.
Captura de datos	Seleccione esta opción 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. Consulte* Device > Setup > Management*.*

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de filtrado de datos	Description (Descripción)
Patrón de datos	Añada un patrón de datos existente con el que filtrar o seleccione **New (Nuevo)** para configurar un nuevo objeto de patrón de datos (Objects > Custom Objects > Data Patterns).
applications	Especifique las aplicaciones que se incluirán en la regla de filtrado: • Seleccione **Any (Cualquiera)** para aplicar el filtro a todas las aplicaciones enumeradas. Esta selección no bloquea todas las aplicaciones posibles, solo las enumeradas. • Haga clic en **Add (Añadir)** para especificar aplicaciones individuales.
Tipos de archivos	Especifique los tipos de archivos que se incluirán en la regla de filtrado: • Seleccione **Any (Cualquiera)** para aplicar el filtro a todos los tipos de archivos enumerados. Esta selección no bloquea todos los posibles tipos de archivo, solo los enumerados. • Haga clic en **Add (Añadir)** para especificar tipos de archivos individuales.
DIRECTION	Especifique si desea aplicar el filtro en la dirección de la carga, descarga o ambas.
Umbral de alerta	Especifique las veces que el patrón de datos debe detectarse en un archivo antes de que se active una alerta.
Umbral de bloqueo	Bloquee archivos que contengan al menos esta cantidad de instancias del patrón de datos.
Gravedad de logs	Defina la gravedad de logs registrada para eventos que coinciden con esta regla del perfil de filtrado de datos.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Protección DoS

Los perfiles de protección DoS están diseñados para una selección muy precisa y mejoran los perfiles de protección de zona. Un perfil de protección DoS especifica los límites de la tasa a los que las nuevas conexiones por segundo (CPS) activan una alarma y una acción (especificada en la política de protección DoS). El perfil de protección DoS también especifica la tasa máxima de CPS y el tiempo que una dirección IP bloqueada permanece en la lista Block IP (Bloquear IP). Usted especifica un perfil de protección DoS en una regla de política de protección DoS, donde indica los criterios para que los paquetes coincidan con la regla, y la regla de política determina los dispositivos a los cuales se aplica el perfil.

Cree perfiles de protección DoS y políticas para proteger dispositivos individuales críticos o grupos pequeños de dispositivos, especialmente los dispositivos accesibles desde Internet, tales como servidores web y servidores de base de datos.

Puede configurar Perfiles de protección DoS agregados y clasificados. Puede aplicar un perfil agregado, un perfil clasificado o uno de cada tipo a una regla de política de protección DoS. Si aplica ambos tipos de perfil a una regla, el cortafuegos aplica el perfil agregado primero y luego aplica el perfil clasificado, si fuera necesario.

- Un perfil de protección DoS clasificado tiene la opción **Classified (Clasificado)** seleccionada como el **Type (Tipo)**. Cuando aplica un perfil de protección DoS clasificado a una regla de protección DoS cuya acción es **Protect (Proteger)**, el cortafuegos cuenta las conexiones para los límites CPS del perfil si el paquete cumple el tipo de dirección especificado: source-ip-only, destination-ip-only o src-dest-ip-both.
- Un perfil de protección DoS agregado tiene la opción **Aggregate (Agregado)** seleccionada como el **Type (Tipo)**. Cuando aplica un perfil de protección DoS agregado a una regla de protección DoS cuya acción es **Protect (Proteger)**, el cortafuegos cuenta para los límites de CPS del perfil todas las conexiones (el número combinado de conexiones para el grupo de dispositivos especificado en la regla) que reúnen los criterios para la regla.

Para aplicar un perfil de protección DoS a una política de protección DoS, consulte Policies > DoS Protection.

Si tiene un entorno de sistemas virtuales múltiples (multi-vsys) y ha configurado lo siguiente:

- *zonas externas para permitir la comunicación entre sistemas virtuales, y*
- *puertas de enlace compartidas para permitir que los sistemas virtuales compartan una interfaz común y una única dirección IP para las comunicaciones externas, entonces*

los siguientes mecanismos de protección DoS y de zona se desactivarán en la zona externa:

- *Cookies de sincronización*
- *Fragmentación de IP*
- *ICMPv6*

Para habilitar la fragmentación IP y la protección ICMPv6, cree un perfil de protección de zona independiente para la puerta de enlace compartida.

Para protegerse frente a inundaciones SYN en una puerta de enlace compartida, puede aplicar un perfil de protección de inundaciones SYN con Random Early Drop (Descarte aleatorio temprano) o SYN Cookies (Cookies SYN). En una zona externa, solo Random Early Drop está disponible para la protección frente a inundaciones SYN.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección DoS	
Nombre	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de reenvío de logs cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres).
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este perfil de protección DoS en los grupos de dispositivos que heredan el perfil. 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.
Tipo	Seleccione uno de los tipos de perfil siguientes: • **Aggregate (Agregado)**: aplica los límites DoS que se han configurado en el perfil a todas las conexiones que coinciden con los criterios de la regla en la que se aplica el perfil. Por ejemplo, una regla agregada con un umbral de **Alarm Rate (Tasa de alarma)** para inundación SYN de 10 000 CPS cuenta las conexiones combinadas de todos los dispositivos que coinciden con la regla DoS. Cuando el total de CPS del grupo supera las 10 000 CPS se activa la alarma, independientemente de la manera en que las CPS se extienden por los dispositivos. • **Classified (Clasificado)**: aplica los límites DoS configurados en el perfil a todas las conexiones individuales que cumplen el criterio de clasificación (dirección IP de origen, dirección IP de destino o par de direcciones IP de origen y destino). Por ejemplo, una regla clasificada con un umbral de **Alarm Rate (Tasa de alarma)** para inundación SYN de 10 000 CPS permite hasta 10 000 CPS por dispositivo, y activa una alarma cuando un dispositivo individual especificado en la regla DoS supera las 10 000 CPS.
Pestaña Protección contra inundaciones	
Pestaña Inundación SYN Pestaña Inundación UDP Pestaña Inundación ICMP Pestaña Inundación ICMPv6	Seleccione esta opción para habilitar en la pestaña el tipo de protección frente a inundaciones y realice los siguientes ajustes: • **Action (Acción)**: (solo **SYN Flood [Inundación SYN]**) acción que lleva a cabo el cortafuegos si la acción de la política de protección DoS es **Protect (Proteger)** y si las CPS entrantes alcanzan la **Activate Rate (Tasa de activación)**. Elija una de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección DoS	
Pestaña Otra inundación IP	• **Random Early Drop (Descarte aleatorio temprano)**: descarta paquetes al azar cuando las conexiones por segundo alcanzan el límite de la **Activate Rate (Tasa de activación)**. • **SYN cookies (Cookies SYN)**: elija esta opción para generar confirmaciones de forma que no sea necesario descartar conexiones durante un ataque de inundación SYN. *Comience con cookies SYN, que tratan al tráfico legítimo de manera equitativa, pero consumen más recursos del cortafuegos. Supervise la utilización de la CPU y la memoria, y si las cookies SYN consumen demasiados recurso, cambie a RED. Siempre utilice RED si no tiene un dispositivo de prevención DDoS dedicado en el perímetro de la red (Internet) para proteger contra ataques DoS de grandes volúmenes.* • **Alarm Rate (Tasa de alarma)**: seleccione la frecuencia límite (CPS) para generar una alarma DoS (el intervalo es de 0 a 2 000 000 cps; el valor predeterminado es 10 000 cps). Para los perfiles clasificados, se recomienda configurar el umbral un 15-20 % por encima de la frecuencia de CPS promedio del dispositivo para contemplar las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas. Para los perfiles agregados, se recomienda configurar el umbral un 15-20 % por encima de la frecuencia CPS promedio del grupo. Supervise y ajuste los umbrales según sea necesario. • **Activate Rate (Tasa de activación)**: especifique la tasa límite (cps) en la que se activa una respuesta DoS. La respuesta DoS se configura en el campo **Action (Acción)** del perfil de protección DoS (Random Early Drop o SYN cookies). El intervalo de **Activate Rate (Tasa de activación)** es de 0 a 2 000 000 cps; el valor predeterminado es 10 000 cps. Si el perfil **Action (Acción)** es **Random Early Drop (Descarte aleatorio temprano)** (RED), cuando las conexiones entrantes por segundo alcanzan el límite **Activate Rate (Tasa de activación)**, se produce el descarte aleatorio temprano. Si la tasa de CPS aumenta, la tasa de RED aumenta según un algoritmo. El cortafuegos continúa con RED hasta que la tasa de CPS alcanza el límite **Max Rate (Tasa máxima)**. Los perfiles clasificados aplican los límites de CPS exactos a los dispositivos individuales y usted configura estos límites de acuerdo con la capacidad de los dispositivos protegidos, de modo que no tenga que limitar las CPS gradualmente y pueda configurar la **Activate Rate (Tasa de activación)** en el mismo umbral que 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 comenzar a descartar tráfico en un servidor individual antes de que llegue a la **Max Rate (Tasa máxima)**. En los perfiles agregados, configure el umbral por encima de la tasa de CPS pico del grupo. Supervise y ajuste los umbrales según sea necesario. • **Max Rate (Tasa máxima)**: especifique la tasa límite de las conexiones entrantes por segundo que el cortafuegos permite. En el límite **Max Rate (Tasa máxima)**, el cortafuegos pierde el 100 % de las conexiones nuevas

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección DoS	
	(el intervalo es de 2 a 2 000 000 cps; el valor predeterminado es 40 000 cps). En los perfiles clasificados, configure la **Max Rate (Tasa máxima)** de acuerdo con la capacidad de los dispositivos que protege, de modo que no se produzca una congestión. En los perfiles agregados, configure la **Max Rate (Tasa máxima)** del 80 al 90 % de la capacidad del grupo. Supervise y ajuste los umbrales según sea necesario. • **Block Duration (Duración del bloqueo)**: especifique el tiempo (en segundos) durante el que la dirección IP infractora debe permanecer en la lista Block IP (Bloquear IP) y las conexiones con la dirección IP, bloqueadas. El cortafuegos no cuenta los paquetes que llegan durante el bloqueo para los límites de tasa de alarma, de activación o máxima (el intervalo es de 1 a 21 600 segundos; el valor predeterminado es 300 segundos).
Pestaña Protección de recursos	
Sesiones	Seleccione esta opción para habilitar la protección de recursos.
Máx. de límites simultáneos	Especifique el número máximo de sesiones simultáneas. • En el caso del tipo de perfil **Aggregate (Agregado)**, este límite se aplica a todo el tráfico que cumple la regla de protección DoS en la que se aplica el perfil de protección DoS. • En el caso del tipo de perfil **Classified (Clasificado)**, este límite se aplica a todo el tráfico clasificado (IP de origen, IP de destino o IP de origen y destino) que cumple la regla de protección DoS a la que se aplica el perfil de protección DoS.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Protección GTP

El perfil de protección de GTP permite al cortafuegos inspeccionar el tráfico de GTP. Para ver este perfil, debe habilitar GTP Security (Seguridad de GTP) en Device > Setup > Management.

Las opciones del perfil le permiten habilitar la inspección por estados de GTP v1-C, GTP v2-C y GTP-U, la validación de protocolos para GTPv1-C, GTP v2-C y GTP-U, y la inspección de contenido de GTP-U para escanear datos de usuarios dentro de los túneles GTP-U. También le permite filtrar las sesiones de GTP basadas en APN, IMSI-Prefix y RAT, y evitar que la suplantación de direcciones IP de usuarios finales proteja a los abonados móviles frente a los excesos de facturación.

Configuración del perfil de inspección GTP	
Inspección GTP	

GTP-C	• Seleccione **Stateful Inspection (Inspección por estados)** para habilitar el cortafuegos e inspeccionar **GTPv1-C** o **GTPv2-C**, o ambos. Al habilitar la inspección por estados, el cortafuegos utiliza la IP de origen, el puerto de origen, la IP de destino, el puerto de destino, el protocolo y los ID de endpoints de túnel (TEID) para realizar el seguimiento de una sesión de GTP. También comprueba y valida el orden de los diferentes tipos de mensajes de GTP que se emplean para crear un túnel de GTP. El TEID identifica de forma exclusiva los endpoints del túnel de GSN. Los túneles para un enlace de subida y uno de bajada están separados y utilizan un TEID diferente.
	• Seleccione la **Action (Acción)**—**Block (Bloquear)** o **Alert (Alertar)**— que el cortafuegos adopta tras una comprobación de validez fallida. La acción de alerta permite el tráfico, pero genera un log; la acción de bloqueo niega el tráfico y genera un log.
	• Especifique las comprobaciones de validez que el cortafuegos debe realizar en un encabezado de GTP y los elementos de información (IE) en una carga útil. El cortafuegos utiliza la acción de bloqueo o alerta que seleccione a continuación para gestionar el error. Puede configurar el cortafuegos para validar:
	  • **Reserved IE (IE reservado)**: comprueba los mensajes de GTPv1-C o GTPv2-C que usan valores de IE reservados.
	  • **Out of Order IE (IE averiado)** (solo GTPv1-C): comprueba que el orden de los IE en los mensajes de GTPv1-C es preciso.
	  • **Length of IE (Longitud de IE)**: comprueba los mensajes de GTPv1-C o GTPv2-C con una longitud de IE no válida.
	  • **Reserved field in header (Campo reservado en encabezado)**: comprueba que no existen paquetes malformados que usan valores no válidos o valores reservados en un encabezado.
	  • **Unsupported message type (Tipo de mensaje no compatible)**: comprueba que no haya tipos de mensajes desconocidos o incorrectos.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de inspección GTP	
GTP-U	Habilitar la inspección por estados para GTPv1-C o GTPv20C habilita automáticamente la inspección por estados de GTPU-U. Puede especificar las siguientes comprobaciones de validez de las cargas útiles de GTP-U. • **Reserved IE (IE reservado)**: comprueba los mensajes de GTP-U que usan valores IE reservados en la carga. • **Out of Order IE (IE averiado)**: comprueba que el orden de los IE en los mensajes de GTP-U es correcto. • **Length of IE (Longitud de IE)**: comprueba que no existan mensajes con una longitud de IE no válida. • **Reserved field in header (Campo reservado en encabezado)**: comprueba que no existen paquetes malformados que usan valores no válidos o valores reservados en un encabezado. • **Unsupported message type (Tipo de mensaje no compatible)**: comprueba que no haya tipos de mensajes desconocidos o incorrectos. También puede configurar una acción de permiso, bloqueo o alerta para: • **End User IP Address Spoofing (Replicación de dirección IP de usuario final)**: configure el cortafuegos para que bloquee o emita una alerta cuando la dirección IP de origen de un paquete de GTP-U del equipo del usuario abonado no sea la misma que la dirección IP del mensaje de GTP-C correspondiente intercambiado durante la configuración del túnel. • **GTP-in-GTP (GTP en GTP)**: puede configurar el cortafuegos para que bloquee o emita una alerta cuando detecte un mensaje de GTP en GTP. Al detectarlo, el cortafuegos genera un log de GTP con gravedad crítica. • Habilite **GTP-U Content Inspection (Inspección de contenido de GTP-U)** si desea inspeccionar y aplicar la política a la carga útil de datos de usuario en un paquete de GTP-U. La inspección del contenido de GTP-U le permite relacionar la información IMSI e IMEI aprendida de los mensajes de GTP-C con el tráfico de IP encapsulado en paquetes de GTP-U.
Opciones de filtrado	
Filtrado RAT	De forma predeterminada, están permitidas todas las tecnologías de acceso por radio (RAT). Los mensajes GTP-C Create-PDP-Request y Create-Session-Request se filtran o se permiten según el filtro de RAT. Puede especificar si desea permitir, bloquear o emitir alertar en las siguientes tecnologías de acceso por radio (RAT) que el equipo del usuario utiliza para acceder a la red móvil central: • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **Evolución HSPA** • **EUTRAN** • **Virtual**

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de inspección GTP	
	• **EUTRAN-NB-IoT**
Filtrado IMSI	IMSI (identidad internacional de abonado móvil) es una identificación única asociada a un abonado en las redes GSM, UMTS y LTE que se incluye en la tarjeta SIM (módulo de identificación del abonado). Generalmente, una IMSI es un número de 15 dígitos (8 bytes), pero puede ser más corto. La IMSI se compone de tres partes: • El código móvil de país (MCC) consta de tres dígitos. El MCC identifica de forma exclusiva el país de residencia del abonado móvil. • El código de la red móvil (Mobile Network Code, MNC) consta de dos o tres dígitos: dos si pertenece al estándar europeo o tres, si pertenece al de América del Norte. El MNC identifica la RMTP (red móvil terrestre pública) de origen del abonado móvil. • Número de identificación de abonado móvil (MSIN) que identifica al abonado móvil en una RMTP. El **IMSI Prefix (Prefijo IMSI)** combina el MCC y el MNC, y con él puede **allow (permitir)**, **block (bloquear)** o **alert (alertar)** del tráfico de GTP de una RMTP específica. De forma predeterminada, todas las IMSI están habilitadas. Puede introducir manualmente o importar un archivo csv con prefijos IMSI o IMSI en el cortafuegos. La IMSI puede incluir caracteres comodín, por ejemplo, 310* o 240011*. El cortafuegos admite un máximo de 5000 IMSI o prefijos IMSI.
Filtrado de APN	El nombre de punto de acceso (APN) es una referencia a un GGSN/PGW que un equipo de usuario requiere para conectarse a Internet. El APN se compone de dos partes: • El identificador de red APN, que define la red externa a la que está conectado el GGSN/PGW y opcionalmente un servicio solicitado por la estación móvil. Esta parte del APN es obligatoria. • El identificador de operador de APN, que define en qué área troncal de GPRS/EPS de RMTP se encuentra el GGSN/PGW. Esta parte del APN es opcional. De forma predeterminada, todos los APN están habilitados. Con el filtro de APN puede permitir, bloquear o emitir alertas de tráfico de GTP basado en el valor APN. Los mensajes GTP-C Create-PDP-Request y Create-Session-Request se filtran o se permiten según la reglas definidas para el filtrado de APN. Puede añadir o importar manualmente una lista de filtrado de APN al cortafuegos. El valor del APN debe incluir el ID de red o el nombre de dominio de la red (por ejemplo, ejemplo.com) y, opcionalmente, el ID del operador. Para el filtrado de APN, el comodín "*" le permite una coincidencia para todas las APN. Una combinación de "*" y otros caracteres no es compatible como comodines. Por ejemplo, "internet.mnc*" se considera una APN regular y no servirá para filtrar todas las entradas que comienzan con internet.mnc...

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de inspección GTP	
	El cortafuegos admite un máximo de 1000 filtros de APN.
Límites de túnel de GTP	
Túneles máximos concurrentes permitidos por destino	Le permite limitar el máximo de túneles de GTP-U a una dirección IP de destino, por ejemplo, al GGSN. Intervalo: de 0 a 100 000 000 túneles.
Alertar en máximo de túneles simultáneos por destino	Especifica el límite en el que el cortafuegos activa una alerta cuando se ha establecido el máximo de túneles de GTP-U a un destino. Se genera un mensaje de log de GTP de gravedad alta cuando se alcanza el límite de túnel configurado.
Logging frequency	La cantidad de eventos que el cortafuegos cuenta antes de generar un log cuando se superan los límites del túnel de GTP configurados. Esta configuración le permite reducir el volumen de los mensajes de log. Default: 100; intervalo: 1/-100000000
Protección de sobrefacturación	Seleccione el sistema virtual que sirve como cortafuegos Gi/SGi en su cortafuegos. El cortafuegos Gi/SGi inspecciona el tráfico IP de los abonados móviles que atraviesa la interfaz Gi/SGi desde el PGW/GGSN hasta la red PDN externa (red de datos de paquetes), como Internet, y asegura el acceso a Internet a los abonados móviles. Se pueden producir excesos en la facturación cuando un GGSN asigna a un abonado móvil una dirección IP del grupo de direcciones IP del usuario final previamente utilizada. Cuando un servidor malicioso de Internet sigue enviando paquetes a esta dirección IP, ya que no cerró la sesión iniciada del anterior abonado y la sesión sigue abierta en el cortafuegos de Gi. Para impedir que los datos se entreguen, cada vez que se elimine un túnel de GTP (que se detecta mediante los mensajes delete-PDP o delete-session) o se agote su tiempo de espera, el cortafuegos habilitado para la protección frente al exceso de facturación notifica al cortafuegos de Gi/SGi que elimine todas las sesiones que pertenecen al abonado de la tabla de sesiones. La seguridad de GTP y el cortafuegos de SGi/Gi deben configurarse en el mismo cortafuegos físico, pero pueden estar en diferentes sistemas virtuales. Para eliminar las sesiones basadas en eventos de GTP-C, el cortafuegos requiere toda la información de sesión relevante, que solo es posible si gestiona el tráfico desde las interfaces SGi + S11 o S5 para GTPv2, y las interfaces Gi + Gn para GTPv1 en la red móvil central.
Otros ajustes de log	
De forma predeterminada, el cortafuegos no registra los mensajes de GTP permitidos. Puede habilitar de forma selectiva la creación de logs de los mensajes de GTP permitidos para solucionar problemas cuando sea necesario, ya que generará un elevado volumen de logs. Además de los mensajes de log permitidos, esta pestaña también le permite habilitar de forma selectiva la creación de logs de la información de ubicación del usuario.	
Mensajes admitidos de GTPv1-C	Le permite habilitar de forma selectiva los logs de los mensajes de GTPv1-C permitidos, si ha habilitado la inspección por estados para GTPv1?C. Estos

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de inspección GTP	
	mensajes generan logs para ayudarle a solucionar problemas según sea necesario. De forma predeterminada, el cortafuegos no registra los mensajes permitidos. Las opciones de creación de logs de los mensajes de GTPv1-C permitidos son: • **Tunnel Management (Gestión de túnel)**: estos mensajes GTPv1-C se utilizan para gestionar los túneles de GTP-U que llevan paquetes IP encapsulados y mensajes de señalización entre un par dado de nodos de red, como SGSN y GGSN. Incluye mensajes tales como Create PDP Context Request (Crear solicitud de contexto de PDP), Create PDP Context Response (Crear respuesta de contexto de PDP), Update PDP Context Request (Actualizar solicitud de contexto de PDP), Update PDP Context Response (Actualizar respuesta de contexto de PDP), Delete PDP Context Request (Eliminar solicitud de contexto de PDP) y Delete PDP Context Response (Eliminar respuesta de contexto de PDP). • **Path Management (Gestión de ruta)**: estos mensajes de GTPv1?C normalmente se envían mediante el GSN o el controlador de red radioeléctrica (Radio Network Controller, RNC) al otro GSN o RNC para averiguar si el par está activo. Incluye mensajes como Echo Request/Response (Solicitud/respuesta de eco). • **Others (Otros)**: estos mensajes incluyen la gestión de ubicación, gestión de movilidad, gestión de información RAN y mensajes de servicio de multidifusión multimedia (MBMS).
Ubicación de usuario de logs	Le permite incluir la información de ubicación del usuario, como prefijos telefónicos e ID de celda, en los logs de GTP.
Captura de paquetes	Le permite capturar eventos de GTP.
Mensajes admitidos de GTPv2-C	Le permite habilitar de forma selectiva los logs de los mensajes de GTPv2-C permitidos, si ha habilitado la inspección por estados para GTPv2-C. Estos mensajes generan logs para ayudarle a solucionar problemas según sea necesario. De forma predeterminada, el cortafuegos no registra los mensajes permitidos. Las opciones de creación de logs de los mensajes de GTPv2-C permitidos son: • **Tunnel Management (Gestión de túnel)**: estos mensajes GTPv2-C se utilizan para gestionar los túneles de GTP-U que llevan paquetes IP encapsulados y mensajes de señalización entre un par dado de nodos de red, como el SGW y el PGW. Incluye los siguientes tipos de mensajes: Create Session Request (Crear solicitud de sesión), Create Session Response (Crear respuesta de sesión), Create Bearer Request (Crear solicitud de portador), Create Bearer Response (Crear respuesta de portador), Modify Bearer Request (Modificar solicitud de portador), Modify Bearer Response (Modificar respuesta de portador), Delete Session Request (Eliminar solicitud de sesión), Delete Session Response (Eliminar respuesta de sesión). • **Path Management (Gestión de rutas)**: estos mensajes de GTPv2-C suelen enviarse por nodos de red como el SGW o PGW al otro PGW y

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de inspección GTP	
	SGW, para averiguar si el par está activo. Incluye mensajes como Echo Request/Response (Solicitud/respuesta de eco). • **Others (Otros)**: estos mensajes incluyen la gestión de la movilidad y los mensajes relacionados con el acceso no 3GPP.
Mensajes admitidos de GTP-U	Le permite habilitar de forma selectiva los logs de los mensajes de GTP-U permitidos, si ha habilitado la inspección por estados para GTPv2?C o GTPv1-C. Estos mensajes generan logs para ayudarle a solucionar problemas según sea necesario. Las opciones de creación de logs de los mensajes de GTP-U permitidos son: • **Tunnel Management (Gestión de túnel)**: son mensajes de señalización de GTP-U, tales como Error Indication (Indicación de error). • **Path Management (Gestión de ruta)**: estos mensajes de GTP-U se envían mediante un nodo de red (como eNodeB) a otro nodo de red (como SGW), para averiguar si el par está activo. Incluye mensajes como Echo Request/Response (Solicitud/respuesta de eco). • **G-PDU**: G-PDU (GTP-U PDU) se utiliza para transportar paquetes de datos de usuarios en los nodos de la red móvil central; consta de un encabezado GTP y una T-PDU.
Paquetes de G-PDU registrados por nuevo túnel GTP-U	Habilite esta opción para verificar que el cortafuegos está inspeccionando las PDU de GTP-U. El cortafuegos genera un log para el número especificado de paquetes de G-PDU en cada nuevo túnel de GTP-U. Default: 1; intervalo: 1-10.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfiles de seguridad > Protección SCTP

Cree un perfil de protección de Protocolo de transmisión de control de secuencias (Stream Control Transmission Protocol, SCTP) para especificar cómo desea que el cortafuegos valide y filtre los fragmentos del SCTP. Primero, debe habilitar la seguridad del SCTP (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]** > **General Settings [Configuración general]**) para ver este tipo de perfil en Security Profiles (Perfiles de seguridad). También puede limitar la cantidad de direcciones IP por endpoint de SCTP en un entorno de múltiples bases y puede especificar cuándo el cortafuegos registra los eventos de SCTP. Tras crear un perfil de protección de SCTP, deberá aplicar el perfil a una regla de la política de seguridad para una zona.

Los modelos de cortafuegos compatibles con la seguridad de SCTP cuentan con un perfil de protección de SCTP predefinido (*default-ss7*) disponible para que lo utilice como es o puede clonar el perfil default-ss7 como base para un nuevo perfil de protección de SCTP. Seleccione **Object (Objeto)** > **Security Profiles (Perfiles de seguridad)** > **SCTP Protection (Protección de SCTP)** y seleccione **default-ss7** para ver los códigos de operación que causan una alerta para este perfil predefinido.

Configuración del perfil de protección de SCTP	
Nombre	Introduzca un nombre para el perfil de protección de SCTP.
Description (Descripción)	Introduzca una descripción para el perfil de protección de SCTP.
SCTP Inspection (Inspección de SCTP)	
Unknown Chunk (Fragmento desconocido)	Seleccione la acción del cortafuegos cuando recibe un paquete de SCTP con un fragmento desconocido (el fragmento no se define en RFC3758, RFC4820, RFC4895, RFC4960, RFC5061 o RFC 6525): • **allow (permitir)** (predeterminado): permite que el paquete pase sin modificaciones. • **alert (alertar)**: permite que el paquete pase sin modificaciones y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]). • **block (bloquear)**: anula al fragmento antes de pasar el paquete y generar un log de SCTP.
Chunk Flags (Indicadores de fragmentos)	Seleccione la acción del cortafuegos cuando recibe un paquete de SCTP con un indicador de fragmentos inconsistente con RFC4960: • **allow (permitir)** (predeterminado): permite que el paquete pase sin modificaciones. • **alert (alertar)**: permite que el paquete pase sin modificaciones y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]).

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de SCTP	
	• **block (bloquear)**: descarta el paquete y genera un log de SCTP.
Invalid Length (Longitud inválida)	Seleccione la acción del cortafuegos cuando recibe un fragmento de SCTP con una longitud inválida: • **allow (permitir)** (predeterminado): permite que el paquete o fragmento pasen sin modificaciones. • **block (bloquear)**: descarta el paquete y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs]).
IP address limit for multihoming (Límite de direcciones IP para múltiples bases)	Introduzca el número máximo de direcciones IP que puede configurar para un endpoint de SCTP antes de que el cortafuegos genere un mensaje de alerta (el intervalo es de 1 a 8; el valor predeterminado es 4). Las bases múltiples de SCTP es la capacidad que tiene un endpoint de admitir más de una dirección IP para la asociación con un peer. Si una ruta hacia un endpoint falla, SCTP selecciona una de las otras direcciones IP de destino que se proporcionaron para esa asociación.
Configuración de log	Seleccione cualquier combinación de ajustes para generar logs de SCTP para fragmentos permitidos, inicio y fin de la asociación, y eventos de fallo del estado: • **Log al inicio de la asociación** • **Log al final de la asociación** • **Fragmentos de inicialización de asociación permitidos del log** • **Fragmentos de heartbeat permitido del log** • **Fragmentos de finalización de asociación permitidos del log** • **Todos los fragmentos de control del log** • **Eventos de fallo del estado del log** Para que el cortafuegos almacene logs de SCTP, debe asignar el almacenamiento de logs de SCTP (consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]).
Opciones de filtrado	
Filtrado de SCTP	
Nombre	Introduzca un nombre para el filtro de SCTP.
PPID	Especifique un PPID para el filtro de SCTP. • **any (cualquiera)**: el cortafuegos realiza la acción que especifica en todos los fragmentos de datos de SCTP que contienen un PPID. • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA**

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de SCTP	
	• **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • Introduzca un valor de PPID válido (uno que no aparezca en el menú desplegable). Por ejemplo, el valor de PPID de H.323 es 13. Cada filtro de SCTP puede especificar solo un PPID, pero puede especificar múltiples filtros de SCTP para un perfil de protección de SCTP.
Acción	Especifique la acción que realiza el cortafuegos en los fragmentos de datos que contienen el PPID especificado: • **allow (permitir)** (predeterminado): permite que el fragmento pase sin modificaciones. • **alert (alertar)**: permite que el fragmento pase sin modificaciones y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]). • **block (bloquear)**: anula el fragmento antes de pasar el paquete y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]).
Los paquetes de SCTP coinciden con los filtros en la lista de manera descendente. Si crea más de un filtro de SCTP para un perfil, el orden de los filtros de SCTP es importante. Seleccione un filtro y **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar su prioridad relativa en la lista de filtrado de SCTP.	
Filtrado de diámetro	
Nombre	Introduzca un nombre para el filtro de diámetro.
Acción	Especifique la acción que realiza el cortafuegos en los fragmentos de diámetro que contienen ID de aplicación, código de comando y AVP del diámetro. Si el fragmento inspeccionado incluye la ID de aplicación especificado del diámetro *y* cualquiera de los códigos de comando especificados del diámetro *y* cualquiera de los AVP especificados del diámetro: • **allow (permitir)** (predeterminado): permite que el fragmento pase sin modificaciones. • **alert (alertar)**: permite que el fragmento pase sin modificaciones y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de SCTP	
	de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]). • **block (bloquear)**: anula el fragmento antes de pasar el paquete y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]).
Diameter Application ID (ID de aplicación del diámetro)	Especifique la ID de aplicación del diámetro para un fragmento en el cual el cortafuegos realiza la acción especificada. • **any (cualquiera)** • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • **Diameter Base Accounting (Contabilidad de la base del diámetro)** • **Diameter Common Messages (Mensajes comunes del diámetro)** • **Diameter Credit Control (Control de crédito del diámetro)** De manera alternativa, puede introducir un valor numérico de una ID de aplicación del diámetro (el intervalo es de 0 a 4 294 967 295). Un filtro de diámetro solo puede tener una ID de aplicación
Diameter Command Code (Código de comando del diámetro)	Especifique los códigos de comando del diámetro para un fragmento en el cual el cortafuegos realiza la acción especificada. Seleccione **any (cualquiera)**, seleccione uno de los códigos de comando del diámetro de la lista desplegable o introduzca un valor concreto (el intervalo es de 0 a 16 777 215). La lista desplegable incluye solo los códigos de comando que aplican a la ID de aplicación del diámetro seleccionada. Puede añadir múltiples códigos de comando del diámetro en un filtro de diámetro.
Diameter AVP (AVP del diámetro)	Especifique los códigos de Par de valor de atributo (Attribute-Value Pair, AVP) del diámetro para un fragmento en el cual el cortafuegos realiza la acción especificada. Introduzca uno o más códigos o valores AVP (el intervalo es de 1 a 16 777 215).
Si crea más de un filtro de diámetro para un perfil, el orden de los filtros de diámetro es importante. Seleccione un filtro y **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para ajustar su prioridad relativa en la lista de filtrado de diámetro.	
Filtrado de SS7	
Nombre	Introduzca un nombre para el filtro SS7.
Acción	Especifique la acción que realiza el cortafuegos en los fragmentos de SS7 que contienen los elementos de filtro SS7 especificados: Si el fragmento que se inspecciona contiene los valores de SSN del emisor

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de SCTP	
	de la llamada de SCCP *y* cualquiera de los valores de título global (Global Title, GT) del emisor de la llamada de SCCP *y* cualquiera de los códigos de operación especificados: • **allow (permitir)** (predeterminado): permite que el fragmento pase sin modificaciones. • **alert (alertar)**: permite que el fragmento pase sin modificaciones y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]). • **block (bloquear)**: anula el fragmento antes de pasar el paquete y genera un log de SCTP (debe asignar el almacenamiento de logs para estos logs, consulte la pestaña Log Storage [Almacenamiento de logs] en Logging and Reporting Settings [Configuración de creación de logs e informes]: Device [Dispositivo] > Setup [Configuración] > Management [Gestión]).
SCCP Calling Party SSN (SSN del emisor de la llamada de SCCP)	Especifique el SSN del emisor de la llamada de SCCP de un fragmento en el cual el cortafuegos realiza la acción especificada. Seleccione **any (cualquiera)** o haga clic en **Add (Añadir)** para añadir uno de los SSN del emisor de la llamada de SCCP de la lista desplegable: • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **SCCP Management (Gestión de SCCP)** Un filtro SS7 solo puede tener un SSN del emisor de la llamada de SCCP.
SCCP Calling Party GT (GT del emisor de la llamada de SCCP)	Especifique el valor de GT del emisor de la llamada de SCCP de un fragmento en el cual el cortafuegos realiza la acción especificada. Seleccione **Any (Cualquiera)** o haga clic en **Add (Añadir)** para añadir un valor numérico de hasta 15 dígitos. También puede introducir un grupo de valores de GT del emisor de la llamada de SCCP utilizando un prefijo. Por ejemplo: 876534*. Puede añadir múltiples valores de GT del emisor de la llamada de SCCP en un filtro SS7. En SCCP Calling Party SSN (SSN del emisor de la llamada de SCCP): **INAP** y **SCCP Management (Gestión de SCCP)**, esta opción está deshabilitada.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de SCTP	
Operation Code (Código de operación)	Especifique los códigos de operación de un fragmento en el cual el cortafuegos realiza la acción especificada: En los siguientes SSN del emisor de la llamada de SCCP, seleccione **any (cualquiera)**, o un código de operación de la lista desplegable, o introduzca un valor concreto (el intervalo es 1 a 255): • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** En SCCP Calling Party SSN (SSN del emisor de la llamada de SCCP): **CAP**, introduzca un valor (el intervalo es de 1 a 255). En SCCP Calling Party SSN (SSN del emisor de la llamada de SCCP): **INAP** y **SCCP Management (Gestión de SCCP)**, esta opción está deshabilitada. Puede añadir múltiples códigos de operación en un filtro SS7.
Si crea más de un filtro SS7 para un perfil, el orden de los filtros SS7 es importante. Seleccione un filtro y **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para ajustar su prioridad relativa en la lista de filtrado de SS7.	

© 2020 Palo Alto Networks, Inc.

Objetos > Grupos de perfiles de seguridad

El cortafuegos permite crear grupos de perfiles de seguridad, que especifican los conjuntos que se pueden tratar como una unidad y añadirse posteriormente a las políticas de seguridad. Por ejemplo, puede crear un grupo de perfiles de seguridad *threats (amenazas)* que incluya perfiles de antivirus, antispyware y protección frente a vulnerabilidades, y después crear una regla de la política de seguridad que incluya el perfil "threats".

Los perfiles de antivirus, antispyware, protección frente a vulnerabilidades, filtrado de URL y bloqueo de archivos que se suelen asignar juntos pueden combinarse en grupos de perfiles para simplificar la creación de las políticas de seguridad.

Para definir un nuevo perfil de seguridad, seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)**.

La siguiente tabla describe la configuración de los perfiles de seguridad:

Configuración de grupos de perfiles de seguridad	Description (Descripción)
Nombre	Introduzca el nombre del grupo (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Compartido (solo Panorama)	Seleccione esta opción si desea que el grupo de perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el grupo de perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el grupo perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de grupo de perfiles de seguridad en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Perfiles	Seleccione un perfil de antivirus, antispyware, protección de vulnerabilidades, filtrado URL o bloqueo de archivos que se incluirá en este grupo. Los perfiles de filtrado de datos también se pueden especificar en los grupos de perfiles de seguridad. Consulte Objects > Security Profiles > Data Filtering.

© 2020 Palo Alto Networks, Inc.

Objetos > Reenvío de logs

De forma predeterminada, los logs que genera el cortafuegos solo se guardan en su almacenamiento local. Sin embargo, puede utilizar Panorama™, el servicio de creación de logs o los servicios externos (como un servidor syslog) para supervisar de forma centralizada la información de logs definiendo un perfil de reenvío de logs y asignándolo a las reglas de la política de seguridad, autenticación, protección DoS e inspección del túnel. Los perfiles de reenvío de logs definen destinos de reenvío para los siguientes tipos de log: Authentication (Autenticación), Data Filtering (Filtrado de datos), GTP, SCTP, Threat (Amenaza), Traffic (Tráfico), Tunnel (Túnel), URL Filtering (Filtrado de URL) y logs de envíos de WildFire®.

Debe reenviar los logs a Panorama o a un almacenamiento externo por muchos motivos, incluidos los siguientes: cumplimiento, redundancia, análisis de ejecución, supervisión centralizada y revisión de conductas de amenazas, y patrones a largo plazo. Además, el cortafuegos posee una capacidad de almacenamiento de logs limitada y elimina los logs más antiguos cuando el espacio de almacenamiento se agota. Asegúrese de reenviar los logs de amenazas y los logs de WildFire.

Para reenviar otros tipos de log, consulte Device > Log Settings.

Para permitir que el cortafuegos serie PA-7000 reenvíe logs o archivos a WildFire®, debe configurar una Log Card Interface (Interfaz de tarjeta de log) en el cortafuegos serie PA-7000. En cuanto configure esta interfaz, el cortafuegos utilizará automáticamente este puerto; no se requiere una configuración especial. Solamente debe configurar el puerto de datos en una de las Tarjetas de procesamiento de red (Network Processing Cards, NPC) de la serie PA-7000 como un tipo de interfaz de tarjeta de log y comprobar que la red que utiliza pueda establecer contacto con sus servidores de logs. Para el reenvío de WildFire, la red se debe comunicar correctamente con la nube de WildFire o con el dispositivo WildFire (o ambos).

La siguiente tabla describe la configuración del perfil de reenvío de logs:

Configuración de perfiles de reenvío de logs	Description (Descripción)
Nombre	Introduzca un nombre (hasta 64 caracteres) para identificar el perfil. Este nombre aparece en la lista de perfiles de reenvío de logs al definir políticas de seguridad. El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos.
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil 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 deshabilita (desmarca) esta opción, el perfil está disponible solo para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • **Every device group on Panorama** (Cada grupo de dispositivos en Panorama): si deshabilita (desmarca) esta opción, el perfil está disponible solo para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de reenvío de logs	Description (Descripción)
Habilitar la creación de logs de aplicaciones mejorada para el Servicio envío de Logs (incluido el tráfico y los logs de url)	Los Logs de aplicación mejorados para los servicios en la nube de Palo Alto Networks están disponibles a través de la suscripción al Servicio de creación de logs. La creación mejorada de logs de aplicaciones permite que el cortafuegos recopile datos que, específicamente, tienen como objetivo aumentar la visibilidad de la actividad de la red para las aplicaciones que se ejecutan en el entorno de los servicios en la nube de Palo Alto Networks.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este perfil de reenvío de logs en los grupos de dispositivos que lo heredan. Esta opción está deshabilitada (desmarcada) de manera predeterminada, lo que significa que los administradores pueden anular la configuración de cualquier grupo de dispositivos que herede el perfil.
Description (Descripción)	Introduzca una descripción que explique el propósito de este perfil de reenvío de logs.
Match List (sin etiquetar)	Haga clic en **Add (Añadir)** para añadir uno o más perfiles de lista de coincidencias (hasta 64) que especifiquen destinos de reenvío, filtros basados en atributos para controlar qué logs reenvía el cortafuegos, y qué acciones se deben realizar en los logs (por ejemplo, etiquetado automático). Complete los dos campos siguientes (Name [Nombre] y Description [Descripción]) de cada perfil de la lista de coincidencias.
Name (perfil de lista de coincidencias)	Introduzca un nombre (hasta 31 caracteres) para el perfil de la lista de coincidencias.
Description (perfil de lista de coincidencias)	Introduzca una descripción (hasta 1023 caracteres) para explicar el propósito de este perfil de lista de coincidencias.
Tipo de log	Seleccione el tipo de log al que desea que se aplique el perfil de la lista de coincidencias: autenticación (**auth**), **data (datos)**, **gtp**, **sctp**, **threat (amenaza)**, **traffic (tráfico)**, **tunnel (túnel)**, **URL** o **WildFire**.
Filter (Filtro)	De forma predeterminada, el cortafuegos reenvía **All Logs (Todos los logs)** del **Log Type (Tipo de log)** seleccionado. Para reenviar un subconjunto de los logs, seleccione un filtro existente en el menú desplegable o seleccione **Filter Builder (Generador de filtro)** para añadir un nuevo filtro. En cada nueva aplicación de filtro, especifique los siguientes campos y haga clic en **Add (Añadir)** para incluir la consulta: • **Connector (Conector)**: seleccione la lógica del conector (y/o) para la consulta. Seleccione **Negate (Negar)** si desea aplicar la negación a la lógica. Por ejemplo, para evitar el reenvío de logs desde una zona no fiable, seleccione **Negate (Negar)**, **Zone (Zona)** como atributo, **equal (igual)** como operador e introduzca el nombre de la zona no fiable en la columna Value (Valor). • **Attribute (Atributo)**: seleccione un atributo de log. Los atributos disponibles dependen del **Log Type (Tipo de log)**. • **Operator (Operador)**: seleccione el criterio para determinar si se aplica el atributo (como **equal [igual]**). Los criterios disponibles dependen del **Log Type (Tipo de log)**.

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de reenvío de logs	Description (Descripción)
	• **Value (Valor)**: Especifique el valor del atributo para coincidir. Para mostrar o exportar los logs que coinciden con el filtro, haga clic en **Ver logs filtrados**, que brinda las mismas opciones que las páginas de la pestaña **Supervisión** (como **Supervisión** > **Logs** > **Tráfico**).
Panorama Panorama/Logging Service (Servicio de creación de logs)	Seleccione **Panorama** si desea reenviar logs a los recopiladores de logs o al servidor de gestión Panorama, o para reenviar logs al servicio de creación de logs. Si habilita esta opción, debe configurar el reenvío de logs a Panorama. Para utilizar el servicio de creación de logs, también debe **Enable (Habilitar)** el servicio de creación de logs en Device (Dispositivo) > Setup (Configuración) > Management (Gestión).
SNMP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de trampas SNMP para reenviar logs como trampas SNMP (consulte Device > Server Profiles > SNMP Trap).
EMAIL	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de correo electrónico para reenviar logs como notificaciones de correo electrónico (consulte Device > Server Profiles > Email).
Syslog	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor Syslog para reenviar logs como mensajes de syslog (consulte Device > Server Profiles > Syslog).
HTTP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor HTTP para reenviar logs como solicitudes HTTP (consulte Device > Server Profiles > HTTP).
Acciones integradas	Haga clic en **Add (Añadir)** para añadir la acción que se debe realizar. Puede seleccionar entre dos tipos: Tagging (Etiquetado) e Integration (Integración). • **Tagging (Etiquetado)**: añada o elimine automáticamente una etiqueta en la dirección IP de origen o destino de una entrada de log, y registre la dirección IP y la asignación de etiquetas en un agente de User-ID en el cortafuegos o Panorama, o en un agente de User-ID remoto, para poder responder a un evento y aplicar dinámicamente la política de seguridad. La capacidad de etiquetar una dirección IP y de aplicar dinámicamente la política mediante grupos de direcciones dinámicos le otorga mayor visibilidad, más contexto y mejor control para aplicar la política de seguridad de forma homogénea, independientemente de por dónde se mueva la dirección IP en su red. Configure los siguientes ajustes: • Haga clic en **Add (Añadir)** para añadir una acción e introduzca un nombre que la describa. • Seleccione la dirección IP de destino que desea etiquetar: **Source Address (Dirección de origen)** o **Destination Address (Dirección de destino)**.

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de reenvío de logs	Description (Descripción)
	Puede realizar una acción con todos los tipos de log que incluyen una dirección IP de origen o de destino en la entrada de log. Solo puede etiquetar la dirección IP de origen en los logs de correlación y en los logs de coincidencias HIP. No puede configurar una acción para los logs del sistema y los de configuración porque el tipo de log no incluye una dirección IP en la entrada del log. • Seleccione la acción: **Add Tag (Añadir etiqueta)** o **Remove Tag (Eliminar etiqueta)**. • Seleccione si desea registrar la dirección IP y la asignación de etiquetas en el agente de **Local User-ID (User-ID local)** en este cortafuegos o en Panorama, o a un agente de **Remote User-ID (User-ID remoto)**. • Para registrar la dirección IP y la asignación de etiquetas en un agente **Remote User-ID (User-ID remoto)**, seleccione el perfil del servidor HTTP (Device > Server Profiles > HTTP) que habilitará el reenvío. • Configure la opción **Timeout (Tiempo de espera)** de la etiqueta IP para configurar, en minutos, el tiempo durante el que se mantendrá la asignación de dirección IP a etiqueta. Una configuración de tiempo de espera en 0 significa que el tiempo de espera de la asignación de la etiqueta IP no se agotará (el intervalo es de 0 a 43 200 [30 días]; el valor predeterminado es 0). *Solo puede configurar un tiempo de espera con la acción Add Tag (Añadir etiqueta).* • Introduzca o seleccione las **Tags (Etiquetas)** que desea aplicar o quitar de la dirección IP objetivo de origen o de destino. • **Integration (Integración):** solo disponible en el cortafuegos serie VM en Azure. Esta opción le permite reenviar los logs seleccionados al centro de seguridad de Azure utilizando la acción **Azure-Security-Center-Integration**.

© 2020 Palo Alto Networks, Inc.

Objetos > Autenticación

Un objeto de aplicación de la autenticación especifica el método y el servicio que se utilizará para autenticar a los usuarios finales que acceden a sus recursos de red. Asigne el objeto a las reglas de la política de autenticación, que invocan el método de autenticación y el servicio cuando el tráfico coincide con una regla (consulte Políticas > Autenticación).

El cortafuegos tiene los siguientes objetos predefinidos y de solo lectura de aplicación de la autenticación:

- **default-browser-challenge (Reto del navegador predeterminado)**: el cortafuegos obtiene de forma transparente las credenciales de autenticación del usuario. Si selecciona esta acción, debe habilitar el inicio de sesión único (SSO) de Kerberos o la autenticación NT LAN Manager (NTLM) al configurar el portal cautivo. Si la autenticación SSO de Kerberos falla, el cortafuegos volverá a la autenticación de NTLM. Si no configuró NTLM o la autenticación NTLM falla, el cortafuegos vuelve al método de autenticación especificado en el objeto **default-web-form (Formato web predeterminado)** predefinido.
- **default-web-form (Formato web predeterminado)**: para autenticar usuarios, el cortafuegos utiliza el perfil de certificado o el de autenticación que especificó al configurar el portal cautivo. Si especificó un perfil de autenticación, el cortafuegos hará caso omiso de cualquier configuración de SSO de Kerberos del perfil y presentará una página del portal cautivo para que el usuario introduzca las credenciales de autenticación.
- **default-no-captive-portal (Portal no cautivo predeterminado)**: el cortafuegos evalúa la política de seguridad sin autenticar a los usuarios.

Antes de crear un objeto personalizado de aplicación de la autenticación:

- ❑ Configure un perfil de servidor que indique cómo conectarse al servicio de autenticación (consulte Dispositivo > Perfiles de servidor > Netflow).
- ❑ Asigne el perfil de servidor a uno de autenticación que indique la configuración de autenticación, como los parámetros de inicio de sesión único de Kerberos (consulte Device > Authentication Profile).

Para crear un objeto personalizado de aplicación de la autenticación, haga clic en **Add (Añadir)** y rellene los siguientes campos:

Configuración de aplicación de la autenticación	Description (Descripción)
Nombre	Al definir las reglas de autenticación, introduzca un nombre descriptivo (hasta 31 caracteres) para facilitar la identificación del objeto. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Compartido (solo Panorama)	Seleccione esta opción si desea que el objeto esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si desmarca esta opción, el objeto únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el objeto únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.

© 2020 Palo Alto Networks, Inc.

Configuración de aplicación de la autenticación	Description (Descripción)
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de este objeto de aplicación de la autenticación en los grupos de dispositivos que lo heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda el objeto.
Authentication Method	Seleccione un método: • **browser-challenge (Reto del navegador)**: el cortafuegos obtiene de forma transparente las credenciales de autenticación del usuario. Si selecciona esta acción, el **Authentication Profile (Perfil de autenticación)** que seleccione debe tener el inicio de sesión único de Kerberos habilitado o NTLM configurado en la configuración de portal cautivo. Si la autenticación SSO de Kerberos falla, el cortafuegos volverá a la autenticación de NTLM. Si no ha configurado NTLM o si la autenticación NTLM falla, el cortafuegos volverá a la autenticación de **web-form** (Formato web). • **web-form (Formato web)**: para autenticar usuarios, el cortafuegos utiliza el perfil de certificado especificado al configurar el portal cautivo o el **Authentication Profile (Perfil de autenticación)** que seleccione en el objeto de aplicación de la autenticación. Si selecciona un **Authentication Profile (Perfil de autenticación)**, el cortafuegos hará caso omiso de cualquier configuración de SSO de Kerberos del perfil y presentará una página del portal cautivo para que el usuario introduzca las credenciales de autenticación. • **no-captive-portal (Portal no cautivo)**: el cortafuegos evalúa la política de seguridad sin autenticar a los usuarios.
Perfil de autenticación	Seleccione el perfil de autenticación que el servicio especifica para utilizarlo en la validación de las identidades de los usuarios.
Mensaje	Dé instrucciones a los usuarios para que sepan responder al primer desafío de autenticación que vean cuando su tráfico active la regla de autenticación. El mensaje se muestra en la **Captive Portal Comfort Page (Página de comodidad de portal cautivo)**. Si no escribe ningún mensaje, se mostrará el predeterminado, **Captive Portal Comfort Page (Página de comodidad de Captive Portal)** (consulte Dispositivo > Páginas de respuesta). *El cortafuegos muestra la Captive Portal Comfort Page (Página de comodidad de Captive Portal) solo para el primer desafío de autenticación (factor), que debe definir en la pestaña Authentication (Autenticación) del Authentication Profile (Perfil de autenticación) (consulte Device > Authentication Profile). Para desafíos de autenticación de múltiples factores (MFA), que debe definir en la pestaña Factors (Factores) del perfil, el cortafuegos muestra la MFA Login Page (Página de inicio de sesión de MFA).*

© 2020 Palo Alto Networks, Inc.

Objetos > Perfil de descifrado

Los perfiles de descifrado le permiten bloquear y controlar aspectos específicos del tráfico SSL y SSH que ha especificado para el descifrado, además del tráfico que excluyó explícitamente del descifrado. Después de crear un perfil de descifrado, podrá añadir dicho perfil a una política de descifrado; cualquier tráfico que coincida con la política de descifrado se aplicará de acuerdo con los ajustes de perfil.

Un perfil de descifrado predeterminado se configura en el cortafuegos y se incluye automáticamente en las nuevas políticas de descifrado (no puede modificar el perfil de descifrado predeterminado). Haga clic en **Add (Añadir)** para crear un nuevo perfil de descifrado, o seleccione un perfil existente para duplicarlo mediante **Clone (Duplicar)** o modificarlo.

¿Qué está buscando?	Consulte:
Añadir un perfil de descifrado nuevo. Habilitar el reflejo del puerto para el tráfico descifrado.	Configuración general de perfiles de descifrado
Bloquear y controlar el tráfico SSL descifrado.	Configuración para controlar el tráfico SSL descifrado
Bloquear y controlar el tráfico que ha excluido del descifrado (por ejemplo, tráfico clasificado como salud y medicina, o servicios financieros).	Configuración para controlar el tráfico que no está descifrado
Bloquear y controlar el tráfico SSH descifrado.	Configuración para controlar el tráfico SSH descifrado

Configuración general de perfiles de descifrado

La tabla siguiente describe los ajustes generales de perfiles de descifrado:

Perfiles de descifrado: Configuración general	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta **31** caracteres). Este nombre aparece en la lista de perfiles de descifrado cuando se definen políticas de descifrado. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Compartido (solo Panorama)	Seleccione esta opción si desea que el perfil esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, el perfil únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.

© 2020 Palo Alto Networks, Inc.

Perfiles de descifrado: Configuración general	Description (Descripción)
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores cancelen la configuración de este perfil de descifrado en los grupos de dispositivos que heredan el perfil. 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.
Interfaz de reflejo de descifrado (Admitido en todos los modelos, excepto por el cortafuegos serie VM en AWS, Azure, edición NSX y Citrix SDX).	Seleccione una **Interface (Interfaz)** que debe utilizarse para el reflejo del puerto de descifrado. *Antes de poder habilitar el reflejo del puerto de descifrado, debe obtener una licencia de reflejo del puerto de descifrado, instalar la licencia y reiniciar el cortafuegos.*
Reenviado solo (Admitido en todos los modelos, excepto por el cortafuegos serie VM en AWS, Azure, edición NSX y Citrix SDX).	Seleccione **Forwarded Only (Reenviado solo)** si desea reflejar el tráfico descifrado solamente después de la aplicación de la política de seguridad. 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). Si cancela esta selección (el ajuste predeterminado), 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.

Configuración para controlar el tráfico SSL descifrado

La tabla siguiente describe los ajustes que puede utilizar para controlar el tráfico SSL que se ha descifrado mediante descifrado del proxy SSL de reenvío o inspección entrante SSL. Puede utilizar estos ajustes para limitar o bloquear sesiones SSL en función de los criterios, incluidos el estado del certificado del servidor externo, el uso de conjuntos de cifras o versiones de protocolos no compatibles o la disponibilidad de los recursos del sistema para procesar el descifrado.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
PESTAÑA PROXY DE REENVÍO SSL Seleccione las opciones para limitar o bloquear el tráfico SSL descifrado mediante Proxy SSL de reenvío.	
Validación de certificado de servidor seleccione las opciones para controlar certificados de servidor para el tráfico SSL descifrado.	
Bloquear sesiones con certificados caducados	Finalice la conexión SSL si el certificado del servidor está caducado. Esto evita que los usuarios acepten certificados caducados y continúen con una sesión SSL.

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
	Bloquee las sesiones con certificados caducados para evitar el acceso a sitios potencialmente peligrosos.
Bloquear sesiones con emisores no fiables	Finalice la sesión SSL si el emisor del certificado del servidor no es fiable. *Bloquee las sesiones con emisores no fiables, debido a que un emisor no fiable puede indicar un ataque de tipo "man-in-the-middle", un ataque de reproducción u otro ataque.*
Bloquear sesiones con estado de certificado desconocido	Finalice la sesión SSL si un servidor devuelve un estado de revocación de certificado "Desconocido". El estado de revocación de certificado indica si se ha revocado o no la fiabilidad del certificado. *Bloquee las sesiones con estado de certificado desconocido para obtener máxima seguridad. Sin embargo, debido a que el estado del certificado puede ser desconocido por diversos motivos, esto quizás sea una medida de seguridad excesiva. Si el bloqueo del estado de certificado desconocido afecta a los sitios que necesita usar para fines comerciales, no bloquee las sesiones con estado de certificado desconocido.*
Bloquear sesiones al agotar el tiempo de espera de comprobación de estado de certificado	Finalice la sesión SSL si el estado del certificado no se puede recuperar en la cantidad de tiempo que el cortafuegos tiene configurado antes de dejar de esperar una respuesta de un servicio de estado de certificado. Puede configurar el valor de **Certificate Status Timeout (Tiempo de espera del estado del certificado)** al crear o modificar un perfil de certificado (**Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**). El bloqueo de las sesiones cuando se agota el tiempo de espera de la comprobación de estado es una compensación entre una seguridad más estricta y una mejor experiencia del usuario. Si los servidores de revocación del certificado responden lentamente, el bloqueo tras el tiempo de espera puede bloquear sitios con certificados válidos. Puede aumentar el valor del tiempo de espera para la comprobación de revocación de certificado (Certificate Revocation Checking, CRL) y el protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) si le preocupa que se agote el tiempo de espera con certificados válidos.
Restringir extensiones de certificados	Limita las extensiones de certificados utilizados en el certificado de servidor dinámico al uso de claves y claves extendidas. *Restrinja las extensiones de certificados si su implementación no requiere otras extensiones de certificado.*
Append certificate's CN value to SAN extension	Permita que el cortafuegos añada una extensión de Nombre alternativo del asunto (Subject Alternative Name, SAN) al certificado de personificación

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
(Adjuntar el valor de CN del certificado a la extensión SAN)	que presenta a los clientes como parte del descifrado de proxy de reenvío de SSL. Cuando un certificado de servidor solo contiene un Nombre común (Common Name, CN), el cortafuegos añade una extensión de SAN al certificado de personificación basado en el CN del certificado de servidor. Esta opción es útil en casos donde los navegadores requieren que los certificados de servidor utilicen un SAN y ya no admiten la coincidencia de los certificados basada en el CN. Esto garantiza que los usuarios finales puedan continuar accediendo los recursos web solicitados y que el cortafuegos continúe descifrando sesiones incluso si un certificado de servidor solo contiene un CN. *Anexe el valor de CN del certificado a la extensión SAN para garantizar el acceso a los recursos web solicitados.*
Comprobaciones de modos no compatibles seleccione las opciones para controlar aplicaciones SSL no compatibles.	
Bloquear sesiones con versiones no compatibles	Finalice las sesiones si PAN-OS no admite el mensaje de bienvenida del cliente. PAN-OS admite SSLv3, TLS1.0, TLS1.1 y TLS1.2. *Siempre bloquee las sesiones con versiones no compatibles, para prevenir el acceso a sitios con protocolos no seguros. En la pestaña SSL Protocol Settings (Configuración del protocolo SSL), configure la versión mínima del protocolo en TLSv1.2 para bloquear los sitios con versiones de protocolo no seguros. Si un sitio al que necesita acceder por fines comerciales utiliza un protocolo menos seguro, cree un perfil de descifrado separado que permita el protocolo menos seguro y especifíquelo en una regla de política de descifrado que se aplique únicamente a los sitios para los cuales desea permitir el protocolo menos seguro.*
Bloquear sesiones con conjuntos de cifras no compatibles	Finalice la sesión si el conjunto de cifrado especificado en el protocolo de enlace SSL si no es compatible con PAN-OS. *Bloquee las sesiones que utilizan conjuntos de cifrado que usted no admite. Usted configura qué conjuntos de cifrado (algoritmos de cifrado) se permitirán en la pestaña SSL Protocol Settings (Configuración del protocolo SSL). No permita que los usuarios se conecten a los sitios con conjuntos de cifrado no seguros.*
Bloquear sesiones con autenticación de cliente	Finalice las sesiones con autenticación de cliente para el tráfico de proxy de reenvío SSL. *Bloquee sesiones con autenticación del cliente, a menos que así lo requiera una aplicación importante, en cuyo caso*

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
	debe crear un perfil de descifrado separado y aplicarlo solo en el tráfico que necesita esta autenticación.
Comprobaciones de fallos seleccione la acción que se adoptará si los recursos del sistema no están disponibles para procesar el descifrado.	
Bloquear sesiones si no hay recursos disponibles	Finalice las sesiones si los recursos del sistema no están disponibles para procesar el descifrado. La decisión de bloquear sesiones cuando los recursos no están disponibles es un punto medio entre una seguridad más estricta y una mejor experiencia del usuario. Si no bloquea las sesiones cuando los recursos no están disponibles, el cortafuegos no podrá descifrar el trafico que usted desea descifrar cuando los recursos resultan afectados. Sin embargo, el bloqueo de sesiones cuando los recursos no están disponibles puede afectar la experiencia del usuario, debido a que los sitios habitualmente disponibles pueden volverse temporalmente inaccesibles.
Bloquear sesiones si HSM no está disponible	Finalizar sesiones si no hay un módulo de seguridad de hardware (HSM) disponible para firmar certificados. La decisión de bloquear las sesiones si HSM no está disponible depende de sus reglas de cumplimiento acerca del origen de las claves privadas y la manera en que desea manejar el tráfico cifrado si HSM no está disponible.
Extensión de cliente	
Eliminar ALPN	El cortafuegos procesa e inspecciona el tráfico HTTP/2 de manera predeterminada. Sin embargo, usted puede deshabilitar la inspección de HTTP/2 al especificar la opción **Strip ALPN (Eliminar ALPN)** en el cortafuegos. Con esta opción seleccionada, el cortafuegos elimina los valores incluidos en la extensión TLS de negociación de protocolo de capa de aplicación (Application-Layer Protocol Negotiation, ALPN). Debido a que ALPN se utiliza para asegurar las conexiones HTTP/2, cuando no hay un valor especificado para esta extensión TLS, el cortafuegos regresa el tráfico HTTP/2 a la versión HTTP/1.1 o lo clasifica como tráfico TCP desconocido.

En el caso de modos no compatibles y de fallos, la información de la sesión se guarda en caché durante 12 horas, por lo que las futuras sesiones entre los mismos pares de hosts y servidor no se descifran. Habilite las opciones para bloquear esas sesiones.

PESTAÑA INSPECCIÓN DE ENTRADA SSL

Seleccione las opciones para limitar o bloquear el tráfico SSL descifrado usando la inspección de entrada SSL.

Comprobaciones de modos no compatibles: seleccione opciones para controlar sesiones si se detectan modos no compatibles en el tráfico SSL.

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
Bloquear sesiones con versiones no compatibles	Finalice las sesiones si PAN-OS no admite el mensaje de bienvenida del cliente. PAN-OS admite SSLv3, TLS1.0, TLS1.1 y TLS1.2. *Siempre bloquee las sesiones con versiones no compatibles, para prevenir el acceso a sitios con protocolos no seguros. En la pestaña SSL Protocol Settings (Configuración del protocolo SSL), configure la versión mínima del protocolo en TLSv1.2 para bloquear los sitios con versiones de protocolo no seguros. Si un sitio al que necesita acceder por fines comerciales utiliza un protocolo menos seguro, cree un perfil de descifrado separado que permita el protocolo menos seguro y especifíquelo en una regla de política de descifrado que se aplique únicamente a los sitios para los cuales desea permitir el protocolo menos seguro.*
Bloquear sesiones con conjuntos de cifras no compatibles	Finalice la sesión si el conjunto de cifrado utilizado no es compatible con PAN-OS. *Bloquee las sesiones que utilizan conjuntos de cifrado que usted no admite. Usted configura qué conjuntos de cifrado (algoritmos de cifrado) se permitirán en la pestaña SSL Protocol Settings (Configuración del protocolo SSL). No permita que los usuarios se conecten a los sitios con conjuntos de cifrado no seguros.*
Comprobaciones de fallos seleccione la acción que se adoptará si los recursos del sistema no están disponibles.	
Bloquear sesiones si no hay recursos disponibles	Finalice las sesiones si los recursos del sistema no están disponibles para procesar el descifrado. La decisión de bloquear sesiones cuando los recursos no están disponibles es un punto medio entre una seguridad más estricta y una mejor experiencia del usuario. Si no bloquea las sesiones cuando los recursos no están disponibles, el cortafuegos no podrá descifrar el trafico que usted desea descifrar cuando los recursos resultan afectados. Sin embargo, el bloqueo de sesiones cuando los recursos no están disponibles puede afectar la experiencia del usuario, debido a que los sitios habitualmente disponibles pueden volverse temporalmente inaccesibles.
Bloquear sesiones si HSM no está disponible	Finalizar sesiones si no hay un módulo de seguridad de hardware (HSM) disponible para descifrar la clave de sesión. La decisión de bloquear las sesiones si HSM no está disponible depende de sus reglas de cumplimiento acerca del origen de las claves privadas y la manera en que desea manejar el tráfico cifrado si HSM no está disponible.

PESTAÑA CONFIGURACIÓN DEL PROTOCOLO SSL

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
Seleccione los ajustes siguientes para aplicar versiones de protocolo y conjuntos de cifras al tráfico de la sesión SSL.	
Versiones de protocolo	Aplique el uso de versiones de protocolo mínima y máxima para la sesión SSL.
Versión mín.	Establezca la versión de protocolo mínima que se puede utilizar para establecer la conexión SSL. *Configure la versión mínima en TLSv1.2 para proporciona máxima seguridad. Revise los sitios que no admitan TLSv1.2 para determinar si realmente tienen un fin comercial legítimo. En el caso de los sitios a los que necesita acceder y que no admiten TLSv1.2, cree un perfil de descifrado separado que especifique la versión de protocolo más estricta que admita y aplíquelo a una regla de política de descifrado que limite el uso de la versión no segura solo para los sitios necesarios, únicamente de los orígenes necesarios (zonas, direcciones, usuarios).*
Versión máx.	Establezca la versión de protocolo máxima que se puede utilizar para establecer la conexión SSL. Puede seleccionar la opción máxima para que no se especifique ninguna versión máxima; en este caso, se admiten las versiones de protocolo que sean equivalentes o posteriores a la versión mínima seleccionada. *Configure la versión máxima en Max (Máxima) para que, a medida que el protocolo mejore, el cortafuegos lo admita automáticamente.*
Algoritmos de intercambio de clave	Fuerce el uso de los algoritmos de intercambio de clave seleccionados para la sesión SSL. Los tres algoritmos (**RSA**, **DHE** y **ECDHE**) están habilitados de manera predeterminada. **DHE** (Diffie-Hellman) y **ECDHE** (Diffie-Hellman de curva elíptica) habilitan la Confidencialidad directa total (Perfect Forward Secrecy, PFS) para el proxy de reenvío SSL o el descifrado de inspección entrante.
Algoritmos de cifrado	Aplique el uso de los algoritmos de cifrado seleccionados para la sesión SSL. *No admita los algoritmos de cifrado no seguros 3DES o RC4. (El cortafuegos automáticamente bloquea estos dos algoritmos cuando utiliza TLSv1.2 como la versión mínima del protocolo). Si debe realizar una excepción y admitir una versión de protocolo menos segura, desmarque 3DES y RC4 en el perfil de descifrado. Si hay sitios a los que debe acceder por motivos comerciales que utilicen los algoritmos de cifrado 3DES o RC4, cree un perfil de descifrado separado y aplíquelo a una regla de política de descifrado solo para esos sitios.*

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Descifrado SSL	Description (Descripción)
Algoritmos de autenticación	Aplique el uso de los algoritmos de autenticación seleccionados para la sesión SSL. *Bloquee el antiguo algoritmo MD5 no seguro (está bloqueado de manera predeterminada). Si ningún sitio necesario utiliza la autenticación SHA1, bloquee SHA1. Si algún sitio al que debe acceder por motivos comerciales utiliza SHA1, cree un perfil de descifrado separado y aplíquelo a una regla de política de descifrado solo para ese sitio.*

Configuración para controlar el tráfico que no está descifrado

Puede utilizar la pestaña **No Decryption (Sin descifrado)** para habilitar ajustes que bloqueen el tráfico que coincida con una política de descifrado configurada con la acción **No Decrypt (No descifrar)** (**Policies [Políticas]** > **Decryption [Descifrado]** > **Action [Acción]**). Utilice estas opciones para controlar los certificados de servidor de la sesión, aunque el cortafuegos no descifre e inspeccione el tráfico de la sesión.

Configuración de la pestaña No hay descifrado	Description (Descripción)
Bloquear sesiones con certificados caducados	Finalice la conexión SSL si el certificado del servidor está caducado. Esto evita que los usuarios acepten certificados caducados y continúen con una sesión SSL. *Bloquee las sesiones con certificados caducados para evitar el acceso a sitios potencialmente peligrosos.*
Bloquear sesiones con emisores no fiables	Finalice la sesión SSL si el emisor del certificado del servidor no es fiable. *Bloquee las sesiones con emisores no fiables, debido a que un emisor no fiable puede indicar un ataque de tipo “man-in-the-middle”, un ataque de reproducción u otro ataque.*

Configuración para controlar el tráfico SSH descifrado

La tabla siguiente describe los ajustes que puede utilizar para controlar el tráfico SSH entrante y saliente descifrado. Estos ajustes le permiten limitar o bloquear el tráfico SSH de túnel en función de criterios, incluidos el uso de algoritmos no compatibles, la detección de errores SSH o la disponibilidad de recursos para procesar el descifrado del proxy SSH.

© 2020 Palo Alto Networks, Inc.

Configuración de la pestaña Proxy SSH	Description (Descripción)
Comprobaciones de modos no compatibles: utilice estas opciones para controlar sesiones si se detectan modos no compatibles en el tráfico SSH. La versión SSH compatible es la versión 2.	
Bloquear sesiones con versiones no compatibles	Finalice las sesiones si el mensaje de bienvenida del cliente no es compatible con PAN-OS. *Siempre bloquee las sesiones con versiones no compatibles, para prevenir el acceso a sitios con protocolos no seguros. En la pestaña SSL Protocol Settings (Configuración del protocolo SSL), configure la versión mínima del protocolo en TLSv1.2 para bloquear los sitios con versiones de protocolo no seguros. Si un sitio al que necesita acceder por fines comerciales utiliza un protocolo menos seguro, cree un perfil de descifrado separado que permita el protocolo menos seguro y especifíquelo en una regla de política de descifrado que se aplique únicamente a los sitios para los cuales desea permitir el protocolo menos seguro.*
Bloquear sesiones con algoritmos no compatibles	Finalice las sesiones si el algoritmo especificado por el cliente o el servidor no es compatible con PAN-OS. *Siempre bloquee las sesiones con algoritmos no compatibles, para prevenir el acceso a sitios con protocolos no seguros.*
Comprobación de fallos: seleccione las medidas que se adoptarán si se producen errores de aplicación SSH y si no hay recursos del sistema disponibles.	
Bloquear sesiones con errores SSH	Finalice las sesiones si se producen errores SSH.
Bloquear sesiones si no hay recursos disponibles	Finalice las sesiones si los recursos del sistema no están disponibles para procesar el descifrado. La decisión de bloquear sesiones cuando los recursos no están disponibles es un punto medio entre una seguridad más estricta y una mejor experiencia del usuario. Si no bloquea las sesiones cuando los recursos no están disponibles, el cortafuegos no podrá descifrar el trafico que usted desea descifrar cuando los recursos resultan afectados. Sin embargo, el bloqueo de sesiones cuando los recursos no están disponibles puede afectar la experiencia del usuario, debido a que los sitios habitualmente disponibles pueden volverse temporalmente inaccesibles.

© 2020 Palo Alto Networks, Inc.

Objetos > Perfil de descifrado > Perfil de reenvío

Puede configurar un perfil de reenvío de descifrado para permitir que el cortafuegos actúe como un agente de descifrado. Un cortafuegos que sea agente de descifrado reenvía tráfico cifrado e inspeccionado a una cadena de seguridad (un conjunto de dispositivos de seguridad externos en línea) para mayor cumplimiento. También puede configurar el cortafuegos para que brinde una distribución de sesión para la cadena de seguridad y garantizar que los dispositivos de la cadena de seguridad no se suscriban en exceso. Cuando el cortafuegos recibe el tráfico de la cadena de seguridad, lo vuelve a cifrar y lo reenvía al destino apropiado.

Antes de crear un perfil de reenvío de descifrado para permitir que el cortafuegos funcione como agente de descifrado, debe realizar lo siguiente:

- Habilite el descifrado del proxy SSL de reenvío.
- Dedique al menos dos interfaces de capa 3 en el cortafuegos para reenviar tráfico descifrado a la cadena de seguridad (seleccione **Network [Red]** > **Interfaces** > **Ethernet**, edite una interfaz, seleccione **Advanced [Avanzado]** > **Other Info [Otra información]**, y habilite la opción Decrypt Forward [Reenvío de descifrado]). Repita esta tarea para habilitar una segunda interfaz como una interfaz de reenvío de descifrado.

Después de completar estas tareas, cree un perfil de reenvío de descifrado para conectar las dos interfaces y defina los ajustes para la cadena de seguridad a la que el cortafuegos reenviará el tráfico descifrado.

Consulte Agente de descifrado para obtener más información sobre el agente de descifrado y las implementaciones de cadena de seguridad admitidos, y para acceder al flujo de trabajo completo para permitir que el cortafuegos actúe como un agente de descifrado.

Configuración de reenvío de descifrado	Description (Descripción)
Nombre	Dele al perfil un nombre descriptivo.
Description (Descripción)	De manera opcional, describa la configuración del perfil.
Pestaña General	
Security Chain Type (Tipo de cadena de seguridad)	Seleccione el tipo de cadena de seguridad al que el cortafuegos reenvía el tráfico descifrado: • **Routed (Enrutado) (capa 3)**: Los dispositivos en este tipo de cadena de seguridad utilizan interfaces de capa 3 para conectarse a la red de la cadena de seguridad; cada interfaz debe tener una dirección IP y una máscara de subred asignadas. Los dispositivos de cadena de seguridad se configuran con rutas estáticas (o enrutamiento dinámico) para dirigir el tráfico entrante y saliente al próximo dispositivo en la cadena de seguridad y de vuelta al cortafuegos. • **Transparent Bridge (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 del plano de datos se configuran para funcionar en modo Transparent Bridge (Puente transparente); no se les asignan direcciones IP, máscaras de subred o puertas de enlace predeterminadas, ni poseen tablas de enrutamiento

© 2020 Palo Alto Networks, Inc.

Configuración de reenvío de descifrado	Description (Descripción)
	local. Los dispositivos de la cadena de seguridad en modo Transparent Bridge (Puente transparente) reciben tráfico en una interfaz, y analizan y aplican el tráfico antes de que salga de la otra interfaz camino al próximo dispositivo de la cadena de seguridad en la línea.
Flow Direction (Dirección de flujo)	Especifique cómo el cortafuegos dirige las sesiones descifradas entrantes y salientes a través de una cadena de seguridad: en la misma dirección (unidireccional) o en direcciones opuestas (bidireccional). La dirección de flujo que seleccione dependerá del tipo de dispositivos que componen la cadena de seguridad. Por ejemplo, si una cadena de seguridad incluye dispositivos sin estado que pueden examinar ambos lados de una sesión, debe seleccionar un flujo unidireccional.
Primary Interface (Interfaz principal)	Seleccione las interfaces principal y secundaria que utilizará el cortafuegos para reenviar tráfico a una cadena de seguridad. Las interfaces principal y secundaria forman un par de interfaces de reenvío de descifrado. Solo se muestran las interfaces que configura como interfaces de reenvío de descifrado.
Secondary Interface (Interfaz secundaria)	
Pestaña Security Chains (Cadenas de seguridad)	
Habilitación	Habilite la cadena de seguridad.
Nombre	Brinde un nombre descriptivo a la cadena de seguridad.
First Device (Primer dispositivo)	Seleccione la dirección IPv4 del primer dispositivo y el último dispositivo en la cadena de seguridad o defina un nuevo objeto de dirección para hacer referencia al dispositivo con facilidad.
Last Device (Último dispositivo)	
Session Distribution Method (Método de distribución de sesiones)	Cuando reenvíe cadenas de seguridad con múltiples rutas (capa 3), seleccione el método que el cortafuegos utilizará para distribuir las sesiones descifradas entre las cadenas de seguridad: • **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. Para que este método funcione de la manera esperada, debe habilitar la supervisión de latencia y la supervisión de HTTP (seleccione **Health Monitor [Supervisor de estado]**).
Pestaña Health Monitor (Supervisor de estado)	

© 2020 Palo Alto Networks, Inc.

Configuración de reenvío de descifrado	Description (Descripción)
On Health Check Failure (Fallo de la comprobación de estado)	Seleccione esta opción para que el cortafuegos **Bypass Security Chain (Omita la cadena de seguridad)** (permitirá tráfico de sesiones) o **Block Session (Bloquee las sesiones)** si todas las cadenas de seguridad asociadas a este perfil de reenvío de descifrado fallan una comprobación de estado. Esto significa que cuando un perfil de descifrado se configura con múltiples cadenas de seguridad, si una cadena de seguridad falla una comprobación de estado, el cortafuegos realiza la distribución de sesiones entre el resto de las cadenas de seguridad con estado aceptable en función del método especificado en la pestaña **Security Chains (Cadenas de seguridad)**; solo bloquea o permite el tráfico basado en esta configuración si cada cadena de seguridad falla.
Health Check Failed Condition (Condición fallida de la comprobación de estado)	Defina un fallo 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]**).
Monitorización de rutas Latency Monitoring (Supervisión de latencia) HTTP Monitoring (Supervisión de HTTP)	Habilite la supervisión de rutas, latencia y HTTP, o una combinación de las tres para identificar cuando las cadenas de seguridad no procesas eficazmente el tráfico descifrado. Para cada tipo de supervisión que habilite, defina los períodos de tiempo y recuentos que activarán una falla de la comprobación de estado. Habilitar: • La supervisión de rutas para comprobar la conectividad de los dispositivos. • La supervisión de latencia para comprobar la velocidad y eficiencia de procesamiento de los dispositivos. • La supervisión de HTTP para comprobar la disponibilidad y el tiempo de respuesta de los dispositivos.

© 2020 Palo Alto Networks, Inc.

Objetos > Gestión de enlaces de SD-WAN

Cree perfiles de calidad de ruta de SD-WAN y perfiles de distribución de tráfico para usar con las reglas de políticas de SD-WAN.

- Objetos > Gestión de enlaces de SD-WAN > Perfil de calidad de la ruta
- Objetos > Gestión de enlaces de SD-WAN > Perfil de distribución de tráfico

Objetos > Gestión de enlaces de SD-WAN > Perfil de calidad de la ruta

SD-WAN le permite crear un perfil de calidad de ruta para cada conjunto de aplicaciones, filtros de aplicaciones, grupos de aplicaciones, servicios, objetos de servicio y objetos de grupo de servicios que tienen requisitos de calidad de red únicos y, después, hacer referencia a ese perfil en una regla de políticas de SD-WAN. En el perfil, establezca umbrales máximos para tres parámetros: latencia, vibración y pérdida de paquetes. Cuando un enlace de SD-WAN exceda cualquiera de los umbrales, el cortafuegos seleccionará una nueva mejor ruta para los paquetes que coincidan con la regla de SD-WAN donde aplicó este perfil.

La configuración de sensibilidad para cada parámetro de calidad de ruta le permite indicar al cortafuegos qué parámetro es más importante (preferido) para las aplicaciones a las que se aplica el perfil. El cortafuegos da más importancia a un parámetro con una configuración alta que a un parámetro con una configuración media o baja. Por ejemplo, algunas aplicaciones son más sensibles a la pérdida de paquetes que a la vibración o la latencia, por lo que puede configurar la pérdida de paquetes en alta sensibilidad para el perfil asociado con esas aplicaciones, lo que hace que el cortafuegos examine primero la pérdida de paquetes.

Si deja la configuración de sensibilidad para latencia, vibración y pérdida de paquetes en la configuración predeterminada (media) o si establece los tres parámetros en la misma configuración, el orden de preferencia para el perfil es la pérdida de paquetes, luego la latencia y luego la vibración.

De forma predeterminada, el cortafuegos mide la latencia y la vibración cada 200 ms y hace una media de las últimas tres mediciones para medir la calidad de la ruta en una ventana deslizante. Puede modificar este comportamiento seleccionando la supervisión de ruta agresiva o relajada cuando configure un perfil de interfaz de SD-WAN.

	Configuración del perfil de calidad de ruta
Nombre	Especifique un **nombre** para el perfil de calidad de ruta con cualquier combinación y un máximo de 31 caracteres alfanuméricos, guiones bajos, guiones, espacios y puntos.
Latencia (ms)	**Umbral**: especifique la cantidad de milisegundos permitidos para que un paquete salga del cortafuegos, llegue al extremo opuesto del túnel de SD-WAN y el paquete de respuesta para ese paquete regrese al cortafuegos antes de que se supere el umbral (el intervalo es de 10 a 2000; el valor predeterminado es 100).
	Sensibilidad: seleccione **alta**, **media** (valor predeterminado) o **baja**.
Jitter o Vibración (ms)	**Umbral**: especifique la variación media, en milisegundos, que las latencias de los paquetes de SD-WAN pueden variar (el intervalo es de 10 a 1,000; el valor predeterminado es 100). El umbral de vibración predeterminado de

© 2020 Palo Alto Networks, Inc.

	Configuración del perfil de calidad de ruta
	100 ms significa que las mediciones de latencia pueden variar en una media de 100 ms antes de que se exceda el umbral de vibración.
	Sensibilidad: seleccione **alta**, **media** (valor predeterminado) o **baja**.
Pérdida de paquetes (%)	**Umbral**: especifique el porcentaje de paquetes perdidos en el enlace antes de que se supere el umbral (el intervalo es de 1 a 100,0; el valor predeterminado es 1).
	Sensibilidad: seleccione **alta**, **media** (valor predeterminado) o **baja**.

Objetos > Gestión de enlaces de SD-WAN > Distribución de tráfico

Para este perfil de distribución de tráfico, seleccione el método que usa el cortafuegos para distribuir sesiones y conmutar por error a una mejor ruta cuando la calidad de la ruta se deteriora. Añada las etiquetas de enlace que considera el cortafuegos al determinar el enlace por el que reenvía el tráfico de SD-WAN. Aplique un perfil de distribución de tráfico a cada regla de política de SD-WAN que cree.

	Perfil de distribución de tráfico
Nombre	Especifique un **nombre** para el perfil de distribución de tráfico con una combinación y un máximo de 31 caracteres alfanuméricos, guiones, espacios, guiones bajos y puntos.
Mejor ruta disponible	Si el coste no es un factor; permitirá que las aplicaciones usen cualquier ruta fuera de la sucursal, seleccione **Mejor ruta disponible**. El cortafuegos distribuye el tráfico y conmuta por error a un enlace de entre los enlaces que pertenecen a todas las etiquetas de enlace de la lista según las métricas de calidad de la ruta para proporcionar la mejor experiencia de aplicación a los usuarios.
Prioridad de arriba hacia abajo	Si tiene enlaces caros o de baja capacidad que desee usar solo como último recurso o como enlace de respaldo, seleccione el método de **prioridad de arriba hacia abajo** y coloque las etiquetas que incluyen esos los últimos enlaces en la lista de **etiquetas de enlaces** para este perfil. El cortafuegos primero usa la etiqueta de enlace superior en la lista para determinar los enlaces en los que se cargará el tráfico en la sesión y a los que se aplicará la conmutación por error. Si ninguno de los enlaces en la etiqueta de enlace superior es apto, el cortafuegos selecciona un enlace de la segunda etiqueta de enlace en la lista. Si ninguno de los enlaces en la segunda etiqueta de enlace es apto, el proceso continúa según sea necesario hasta que el cortafuegos encuentre uno. Si todos los enlaces asociados están sobrecargados y ningún enlace cumple con los umbrales de calidad, el cortafuegos utiliza el método Mejor ruta disponible para seleccionar un enlace sobre el que reenviar el tráfico. Si la vibración, la latencia o la pérdida de paquetes de una aplicación exceden el umbral configurado, el cortafuegos comienza en la parte superior de la lista de arriba hacia abajo de etiquetas de enlace para encontrar un enlace para la conmutación por error.

© 2020 Palo Alto Networks, Inc.

	Perfil de distribución de tráfico
Distribución de sesión ponderada	Seleccione **Distribución de sesión ponderada** si desea cargar manualmente el tráfico (que coincide con la regla) en los enlaces de su ISP y WAN, y no necesita conmutación por error durante las condiciones de caída de tensión. Especifique manualmente la carga del enlace cuando aplique un porcentaje estático de nuevas sesiones que obtendrán las interfaces agrupadas con una sola etiqueta de enlace. Por ejemplo, seleccione este método para aplicaciones que no sean sensibles a la latencia y que requieran una gran parte de la capacidad de ancho de banda del enlace, como copias de seguridad de grandes sucursales y grandes transferencias de archivos. Sin embargo, si el enlace experimenta una caída de tensión, el cortafuegos no redirige el tráfico correspondiente a un enlace diferente.
Etiquetas de enlace	Añada las **etiquetas de enlace** que desee que el cortafuegos considere durante el proceso de selección de enlace que eligió para este perfil. El orden de las etiquetas es importante si elige el método **Prioridad de arriba hacia abajo**; puede **subir** o **bajar** etiquetas para cambiar el orden.
Peso	Si eligió el método Distribución de sesión ponderada, elija un porcentaje por cada etiqueta de enlace que añadió. La suma de los valores porcentuales debe ser igual al 100 %.

© 2020 Palo Alto Networks, Inc.

Objetos > Programaciones

De manera predeterminada, las reglas de la política de seguridad siempre se aplican (en todas las fechas y horarios). Para limitar una regla de la política de seguridad a horas concretas, puede realizar programaciones y aplicarlas a las políticas que correspondan. Para cada programación puede especificar una fecha y un intervalo horario fijo, o bien una programación diaria o semanal recurrente. Para aplicar programaciones a las políticas de seguridad, consulte Policies > Security.

Cuando se activa una regla de la política de seguridad en una programación definida, solo las sesiones nuevas se verán afectadas por la regla aplicada. Las sesiones actuales no se ven afectadas por la política programada.

Ajustes de programación	Description (Descripción)
Nombre	Introduzca un nombre de la programación (de hasta 31 caracteres). Este nombre aparece en la lista de programaciones cuando se definen políticas de seguridad. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Compartido (solo Panorama)	Seleccione esta opción si desea que la programación esté disponible para lo siguiente: • Cada sistema virtual (vsys) de un cortafuegos de vsys múltiples. Si cancela esta selección, la programación únicamente estará disponible para el **Virtual System (Sistema virtual)** seleccionado en la pestaña **Objects (Objetos)**. • Cada grupo de dispositivos en Panorama. Si cancela esta selección, la programación únicamente estará disponible para el **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**.
Deshabilitar anulación (Panorama únicamente)	Seleccione esta opción para evitar que los administradores sobrescriban la configuración de esta programación en los grupos de dispositivos que la heredan. Esta opción no está seleccionada de manera predeterminada, lo que significa que los administradores pueden sobrescribir la configuración de cualquier grupo de dispositivos que hereda la programación.
Periodicidad	Seleccione la periodicidad (**Daily [Diario]**, **Weekly [Semanal]** o **Non-Recurring [Sin repetición]**).
Diario	Haga clic en **Add (Añadir)** y especifique una **Start Time (Fecha de inicio)** y una **End Time (Hora de finalización)** en formato de 24 horas (HH:MM).
Semanal	Haga clic en **Add (Añadir)**, seleccione un **Day of Week (Día de la semana)** y especifique la **Start Time (Fecha de inicio)** y la **End Time (Hora de finalización)** en formato de 24 horas (HH:MM).
Sin repetición	Haga clic en **Add (Añadir)** y especifique una **Start Date (Fecha de inicio)**, una **Start Time (Fecha de inicio)**, una **End Date (Fecha de finalización)** y una **End Time (Hora de finalización)**.

network

Los temas siguientes describen la configuración de red del cortafuegos.

- Network > Virtual Wires
- Red > Interfaces
- Network > Virtual Routers
- Network > Zones
- Network > VLANs
- Network > IPSec Tunnels
- Network (Red) > GRE Tunnels (Túneles GRE)
- Network > DHCP
- Network > DNS Proxy
- Red > QoS
- Network > LLDP
- Red > Perfiles de red

© 2020 Palo Alto Networks, Inc.

Red > Interfaces

Las interfaces de cortafuegos (puertos) permiten a un cortafuegos conectar con otros dispositivos de red y con otras interfaces del cortafuegos. En los siguientes temas se describen los tipos de interfaz y cómo configurarlos:

¿Qué está buscando?	Consulte
¿Qué son las interfaces de cortafuegos?	Resumen de las interfaces de cortafuegos
Acabo de empezar con las interfaces de cortafuegos; ¿qué componentes tienen?	Componentes comunes de las interfaces de cortafuegos Componentes comunes de interfaces de cortafuegos de la serie PA-7000
Sé bastante sobre interfaces de cortafuegos; ¿dónde puedo encontrar información sobre cómo configurar un tipo de interfaz específico?	**Interfaces físicas (Ethernet)** Interfaz de Tap Interfaz HA Interfaz de cable virtual Subinterfaz de cable virtual Interfaz de la capa 2 de la serie PA-7000 Subinterfaz de la capa 2 de la serie PA-7000 Interfaz de la capa 3 de la serie PA-7000 #unique_230 Subinterfaz de la capa 3 Interfaz de tarjeta de log Subinterfaz de tarjeta de log Interfaz de reflejo de descifrado Grupo de interfaz de Ethernet agregados (AE) Interfaz de Ethernet agregados (AE) **Interfaces lógicas** Network > Interfaces > VLAN Network > Interfaces > Loopback Network > Interfaces > Tunnel Network (Red) > Interfaces (Interfaces) > SD-WAN
¿Busca más información?	Networking

© 2020 Palo Alto Networks, Inc.

Resumen de las interfaces de cortafuegos

Las configuraciones de interfaz en los puertos de datos del cortafuegos permiten que entre y salga el tráfico del cortafuegos. Un cortafuegos de Palo Alto Networks® puede funcionar en múltiples implementaciones de forma simultánea porque puede realizar la Configuración de las interfaces para admitir distintas implementaciones. Por ejemplo, puede configurar las interfaces Ethernet en un cortafuegos para cable virtual, capa 2, capa 3 y modo TAP. Las interfaces que admite el cortafuegos son:

- **Interfaces físicas**: el cortafuegos admite dos tipos de medios, cobre y fibra óptica, que pueden enviar y recibir tráfico a distintas velocidades de transmisión. Puede configurar interfaces de Ethernet como los siguientes tipos: Tap, alta disponibilidad (HA), la tarjeta de log (interfaz y subinterfaz), el reflejo de descifrado, el cable virtual (interfaz y subinterfaz), la capa 2 (interfaz y subinterfaz), la capa 3 (interfaz y subinterfaz) y la Ethernet agregada. Los tipos de interfaz y las velocidades de transmisión disponibles pueden variar por modelo de hardware.
- **Interfaces lógicas**: esto incluye interfaces de red de área local virtual (VLAN), interfaces de bucle invertido, interfaces de túnel e interfaces de SD-WAN. Debe configurar la interfaz física antes de definir una VLAN, SD-WAN o una interfaz de túnel.

Componentes comunes de las interfaces de cortafuegos

Seleccione **Network (Red)** > **Interfaces** para mostrar y configurar los componentes que son comunes a la mayoría de los tipos de interfaz.

Para una descripción de componentes que son únicos o diferentes cuando configura interfaces en un cortafuegos serie PA-7000, o cuando usa Panorama™ para configurar interfaces en cualquier cortafuegos, consulte Componentes comunes de interfaces de cortafuegos de la serie PA-7000*.*

Componentes de interfaz de cortafuegos.	Description (Descripción)
Interfaz (nombre de interfaz)	El nombre de interfaz viene predefinido y no puede cambiarlo. Sin embargo, puede adjuntar un sufijo numérico para subinterfaces, interfaces agregadas, interfaces VLAN, interfaces de bucle invertido, interfaces de túnel e interfaces de SD-WAN.
Tipo de interfaz	Para las interfaces de Ethernet (**Network [Red]** > **Interfaces** > **Ethernet**), puede seleccionar el tipo de interfaz: • **Puntear** • **HA** • **Decrypt Mirror (Reflejo de descifrado)** (compatible con todos los cortafuegos excepto por la serie VM en NSX, Citrix SDX, AWS y Azure). • **Virtual Wire** • **Capa 2** • **Capa 3** • **Log Card (Tarjeta de log)** (solo cortafuegos de la serie PA-7000) • **Ethernet de agregación**
Perfil de gestión	Seleccione un **Management Profile (Perfil de gestión)** (**Network [Red]** > **Interfaces** > **<if-config>** > **Advanced [Avanzado]** > **Other Info [Otra información]**) que defina los protocolos (como SSH, Telnet y HTTP) que puede utilizar para gestionar el cortafuegos en esta interfaz.

© 2020 Palo Alto Networks, Inc.

Componentes de interfaz de cortafuegos.	Description (Descripción)
estado del enlace	Para interfaces Ethernet, el estado de enlace indica si la interfaz es accesible y puede recibir tráfico a través de la red: • **Verde**: configurado y funcionando • **Rojo**: configurado pero desactivado o inactivo • **Gris**: no configurado Pase el ratón sobre el estado de enlace para mostrar información sobre herramientas que indique la velocidad de enlace y los ajustes dúplex en la interfaz.
Dirección IP	(Opcional) Configure la dirección IPv4 o IPv6 de la interfaz de Ethernet, VLAN, de bucle invertido o de túnel. Para una dirección IPv4, también puede seleccionar el modo de direccionamiento (**Type (Tipo)**) para la interfaz: **Static (Estático)**, **DHCP Client (Cliente DHCP)** o **PPPoE**.
Enrutador virtual	Asigne un enrutador virtual a la interfaz o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network [Red] > Virtual Routers [Enrutadores virtuales]). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Etiqueta (solo subinterfaz)	Introduzca la etiqueta VLAN (1-4.094) para la subinterfaz.
VLAN	Seleccione **Network (Red)** > **Interfaces** > **VLAN** y modifique una **VLAN** existente o seleccione **Add (Añadir)** para añadir una nueva (consulte Network [Red] > VLANs). Seleccione **None (Ninguna)** para eliminar la asignación de dirección actual de la interfaz. Para permitir el intercambio entre las interfaces de la capa 2 o permitir el enrutamiento a través de una interfaz de VLAN, debe configurar un objeto VLAN.
Sistema virtual	Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad	Seleccione una **Security Zone (Zona de seguridad)** (**Network [Red]** > **Interfaces** > **<if-config>** > **Config [Configuración]**) para la interfaz o seleccione **Zone (Zona)** para definir una nueva. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Features	En las interfaces Ethernet, esta columna indica si se han habilitado las siguientes características: Cliente DHCP Proxy DNS Puerta de enlace de GlobalProtect™ habilitada Protocolo de control de agregación de enlaces (Link Aggregation Control Protocol, LACP)

© 2020 Palo Alto Networks, Inc.

Componentes de interfaz de cortafuegos.	Description (Descripción)
	Protocolo de detección de nivel de enlace (Link Layer Discovery Protocol, LLDP) Supervidor NDP Perfil de NetFlow Perfil de calidad de servicio (Quality of Service, QoS) SD-WAN
Comentarios	Una descripción de la función u objetivo de la interfaz.

Componentes comunes de interfaces de cortafuegos de la serie PA-7000

La siguiente tabla describe los componentes de la página **Network (Red)** > **Interfaces** > **Ethernet** que son únicos o diferentes cuando configura interfaces en un cortafuegos serie PA-7000, o cuando usa Panorama para configurar interfaces en cualquier cortafuegos. Haga clic en **Add Interface (Añadir interfaz)** para crear una interfaz nueva o seleccione una interfaz existente (ethernet1/1, por ejemplo) para editarla.

En los cortafuegos de la serie PA-7000, debe configurar una Interfaz de tarjeta de log *en un puerto de datos.*

Componentes del interfaz del cortafuegos de la serie PA-7000	Description (Descripción)
Ranura	Seleccione el número de ranura (1-12) de la interfaz. Solo los cortafuegos de la serie PA-7000 tienen múltiples ranuras. Si usa Panorama para configurar una interfaz para cualquier otro modelo de cortafuegos, seleccione la **Ranura 1**.
Interfaz (nombre de interfaz)	Seleccione el nombre de una interfaz que esté asociada con la **Slot (Ranura)** seleccionada.

Interfaz de Tap

- Network > Interfaces > Ethernet

Puede usar una interfaz de Tap para supervisar el tráfico en un puerto.

Para configurar una interfaz de Tap, haga clic en el nombre de una interfaz (ethernet1/1, por ejemplo) que no esté configurada y especifique la siguiente información.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de Tap	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz Ethernet**	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tipo de interfaz		Seleccione **Tap**.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil del servidor o haga clic en **Netflow Profile (Perfil Netflow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow (Dispositivo > Perfiles de servidor > Netflow)). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
Sistema virtual	**Ethernet Interface (Interfaz de Ethernet)** > **Config (Configuración)**	Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Velocidad de enlace	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)**	Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad.
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace		Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).

Interfaz HA

- Network > Interfaces > Ethernet

Todas las interfaces de alta disponibilidad (HA) tienen una función específica: una interfaz se utiliza para la sincronización de la configuración y latidos y la otra interfaz se utiliza para la sincronización del estado. Si se activa la alta disponibilidad activa/activa, el cortafuegos puede usar una tercera interfaz de HA para reenviar los paquetes.

Algunos cortafuegos de Palo Alto Networks incluyen puertos físicos exclusivos para su uso en implementaciones HA (uno para el enlace de control y uno para el enlace de datos). En el caso de cortafuegos que no incluyen puertos exclusivos, debe especificar los puertos de datos que se utilizarán para HA. Para obtener más información sobre HA, consulte "Dispositivo > Sistemas virtuales".

© 2020 Palo Alto Networks, Inc.

Para configurar una interfaz de HA, haga clic en el nombre de una interfaz (ethernet1/1, por ejemplo) que no esté configurada y especifique la siguiente información.

Configuración de interfaz HA	Description (Descripción)
Nombre de interfaz	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios	Introduzca una descripción opcional para la interfaz.
Tipo de interfaz	Seleccione **HA**.
Velocidad de enlace	Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad.
Dúplex de enlace	Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace	Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).

Interfaz de cable virtual

- Network > Interfaces > Ethernet

Un cable virtual une dos interfaces Ethernet, lo que permite que pase todo el tráfico entre las interfaces, o solo el tráfico con etiquetas VLAN selectas (no hay disponible ningún otro servicio de enrutamiento o conmutación). También puede crear subinterfaces de cable virtual para clasificar el tráfico en función de una dirección IP, un intervalo IP o una subred. Un cable virtual no requiere ningún tipo de cambio en los dispositivos de red adyacentes. Un cable virtual puede unir dos interfaces Ethernet del mismo tipo (ambos de cobre o de fibra óptica) o unir una interfaz de cobre a una interfaz de fibra óptica.

Para configurar un cable virtual, decida cuál de las dos interfaces se unirá (**Network [Red]** > **Interfaces [Interfaces]** > **Ethernet**) y configúrelas como se describe en la siguiente tabla.

Si está utilizando una interfaz existente para el cable virtual, quite primero la interfaz de cualquier zona de seguridad asociada.

Configuración de interfaces de cable virtual	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz Ethernet**	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		Introduzca una descripción opcional para la interfaz.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaces de cable virtual	Configurado en	Description (Descripción)
Tipo de interfaz		Seleccione **Virtual Wire (Cable virtual)**.
Virtual Wire	**Ethernet Interface (Interfaz de Ethernet)** > **Config (Configuración)**	Seleccione un cable virtual o haga clic en **Virtual Wire (Cable virtual)** para definir uno nuevo (consulte Network [Red] > Virtual Wires [Cables virtuales]). Seleccione **None (Ninguno)** para eliminar la asignación del cable virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Velocidad de enlace	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)**	Seleccione una velocidad de interfaz concreta en Mbps o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad. Ambas interfaces en el cable virtual deben tener la misma velocidad.
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**). Ambas interfaces en el cable virtual deben tener el mismo modo de transmisión.
estado del enlace		Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).
Habilitar LLDP	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **LLDP**	Seleccione esta opción para habilitar Protocolo de detección de nivel de enlace (LLDP) en la interfaz. Funciones LLDP en la capa de enlace para descubrir dispositivos vecinos y sus capacidades.
Perfil		Si LLDP está habilitado, seleccione un perfil LLDP para asignar a la interfaz o haga clic en **LLDP Profile (Perfil de LLDP)** para crear un nuevo perfil (consulte Network > Network Profiles > LLDP Profile). Seleccione **None (Ninguno)** para configurar al cortafuegos para que use los valores predeterminados globales.
Habilite en el estado pasivo de HA		Si LLDP está habilitado, seleccione esta opción para configurar un cortafuegos pasivo HA para prenegociar LLDP con su peer antes de que se active el cortafuegos. Si LLDP no está habilitado, seleccione configurar un cortafuegos pasivo HA para pasar los paquetes LLDP por el cortafuegos.

Subinterfaz de cable virtual

- Network > Interfaces > Ethernet

© 2020 Palo Alto Networks, Inc.

Las subinterfaces de cable virtual (Virtual Wire) le permiten separar el tráfico según las etiquetas VLAN o una combinación de etiqueta VLAN y clasificador IP, asignar el tráfico etiquetado a una zona y sistema virtual diferentes y, a continuación, aplicar políticas de seguridad para el tráfico que coincida con los criterios definidos.

Para añadir un Interfaz de cable virtual, seleccione la fila para esa interfaz, haga clic en **Add Subinterface (Añadir subinterfaz)** y especifique la siguiente información.

Configuración de subinterfaz de Virtual Wire	Description (Descripción)
Nombre de interfaz	El campo **Interface Name (Nombre de la interfaz)** de solo lectura muestra el nombre de la interfaz vwire que ha seleccionado. En el campo adyacente, introduzca un sufijo numérico (1-9.999) para identificar la subinterfaz.
Comentarios	Introduzca una descripción opcional para la subinterfaz.
Tag (Etiqueta)	Introduzca la Tag (Etiqueta) VLAN (0-4.094) para la subinterfaz.
Perfil de NetFlow	Si quiere exportar el tráfico IP unidireccional que atraviesa una subinterfaz de entrada a un servidor NetFlow, seleccione el perfil del servidor o haga clic en **Netflow Profile (Perfil Netflow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow (Dispositivo > Perfiles de servidor > Netflow)). Si selecciona **None (Ninguno)**, se elimina la asignación de servidor NetFlow actual de la subinterfaz.
Clasificador IP	Haga clic en **Add (Añadir)** para introducir una dirección IP, intervalo IP o subred para clasificar el tráfico en esta subinterfaz de cable virtual.
Virtual Wire	Seleccione un cable virtual o haga clic en **Virtual Wire (Cable virtual)** para definir uno nuevo (consulte Network > Virtual Wires). Seleccione **None** para eliminar la asignación del cable virtual actual de la subinterfaz.
Sistema virtual	Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la subinterfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad	Seleccione una zona de seguridad para la subinterfaz o haga clic en **Zone** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la subinterfaz.

Interfaz de la capa 2 de la serie PA-7000

- Network > Interfaces > Ethernet

Seleccione **Network (Red)** > **Interfaces** > **Ethernet** para configurar una interfaz de capa 2. Haga clic en el nombre de una interfaz (ethernet1/1, por ejemplo) que no esté configurada y especifique la siguiente información.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 2	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz Ethernet**	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tipo de interfaz		Seleccione **Layer2 (Capa 2)**.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
VLAN	**Ethernet Interface (Interfaz de Ethernet)** > **Config (Configuración)**	Para permitir el cambio entre las interfaces de capa 2 o para permitir el enrutamiento a través de una interfaz VLAN, seleccione una VLAN existente, o haga clic en **VLAN** para definir una nueva VLAN (consulte Network > VLANs). Seleccione **None (Ninguna)** para eliminar la asignación de dirección actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una **Security Zone (Zona de seguridad)** para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Velocidad de enlace	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)**	Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad.
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace		Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).
Habilitar LLDP	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **LLDP**	Seleccione esta opción para habilitar Protocolo de detección de nivel de enlace (LLDP) en la interfaz. Funciones LLDP en la capa de enlace para descubrir dispositivos vecinos y sus capacidades.
Perfil		Si LLDP está habilitado, seleccione un perfil LLDP para asignar a la interfaz o haga clic en **LLDP Profile (Perfil de LLDP)** para crear un nuevo perfil (consulte Network > Network Profiles > LLDP Profile).

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 2	Configurado en	Description (Descripción)
		Seleccione **None (Ninguno)** para configurar al cortafuegos para que use los valores predeterminados globales.
Habilite en el estado pasivo de HA		Si LLDP está habilitado, seleccione esta opción para permitir que un cortafuegos pasivo HA prenegocie LLDP con su peer antes de que se active el cortafuegos.

Subinterfaz de la capa 2 de la serie PA-7000

- Network > Interfaces > Ethernet

Para cada puerto Ethernet configurado con una interfaz física de capa 2, puede definir una interfaz lógica de capa 2 adicional (subinterfaz) para cada etiqueta VLAN asignada al tráfico que recibe el puerto. Para permitir el intercambio entre subinterfaces de capa 2, asígneles el mismo objeto VLAN a las subinterfaces.

Para configurar una interfaz de capa 2 PA-7000 Series, seleccione la fila asociada a dicha interfaz física, haga clic en **Add Subinterface (Añadir subinterfaz)** y especifique la siguiente información.

Configuración de la subinterfaz de capa 2	Description (Descripción)
Nombre de interfaz	El campo Interface Name de solo lectura muestra el nombre de la interfaz física que ha seleccionado. En el campo adyacente, introduzca un sufijo numérico (1-9.999) para identificar la subinterfaz.
Comentarios	Introduzca una descripción opcional para la subinterfaz.
Tag (Etiqueta)	Introduzca la etiqueta VLAN (1-4.094) para la subinterfaz.
Perfil de NetFlow	Si quiere exportar el tráfico IP unidireccional que atraviesa una subinterfaz de entrada a un servidor NetFlow, seleccione el perfil del servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (Ninguna)** para eliminar la asignación actual del servidor NetFlow de la subinterfaz.
VLAN	Para permitir el cambio entre las interfaces de capa 2 o para permitir el enrutamiento a través de una interfaz VLAN, seleccione una VLAN o haga clic en **VLAN** para definir una nueva VLAN (consulte Network > VLANs). Seleccione **None (Ninguna)** para eliminar la asignación de dirección actual de la subinterfaz.
Sistema virtual	Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la subinterfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad	Seleccione una zona de seguridad para la subinterfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la subinterfaz.

© 2020 Palo Alto Networks, Inc.

Interfaz de la capa 3 de la serie PA-7000

- Network > Interfaces > Ethernet

Para configurar una interfaz de capa 3, seleccione una interfaz (ethernet1/1, por ejemplo) y especifique la siguiente información.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz Ethernet**	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tipo de interfaz		Seleccione **Layer3 (Capa 3)**.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
Enrutador virtual	**Ethernet Interface (Interfaz de Ethernet)** > **Config (Configuración)**	Asigne un enrutador virtual o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network > Virtual Routers). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Velocidad de enlace	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)**	Seleccione la velocidad de la interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)**.
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace		Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).
Perfil de gestión	**Ethernet Interface (Interfaz de Ethernet)** > **Advanced (Avanzado)** >	Seleccione un perfil que defina los protocolos (por ejemplo, SSH, Telnet y HTTP) que puede usar para gestionar el cortafuegos en esta interfaz. Seleccione **None (Ninguna)** para eliminar la asignación de perfil actual de la interfaz.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
MTU	**Other Info (Otra información)**	Introduzca la unidad máxima de transmisión (MTU) en bytes para los paquetes enviados en esta interfaz (576 a 9192, la opción predeterminada es 1500). Si las máquinas de ambos extremos del cortafuegos ejecutan un descubrimiento de MTU de ruta (PMTUD) y la interfaz recibe un paquete que supera la MTU, el cortafuegos envía al origen un mensaje de *necesidad de fragmentación del ICMP* que indica que el paquete es demasiado grande.
Ajustar TCP MSS		Seleccione esta opción para ajustar el tamaño de segmento máximo (MSS) de forma que se pueda albergar bytes de cualquier encabezado dentro del tamaño de byte MTU de la interfaz. El tamaño de byte MTU menos el tamaño de ajuste MSS es igual al tamaño de byte MSS, que varía según el protocolo de IP: • **IPv4 MSS Adjustment Size (Tamaño de ajuste IPv4 MSS)**: el intervalo es de 40 a 300; el valor predeterminado es 40. • **IPv6 MSS Adjustment Size (Tamaño de ajuste IPv6 MSS)**: el intervalo es de 60 a 300; el valor predeterminado es 60. Utilice esta configuración para tratar los casos en los que un **tunnel (túnel)** en la red necesita un MSS más pequeño. Si un paquete tiene más bytes que el MSS sin fragmentación, este parámetro permite ajustarlo. La encapsulación les añade longitud a los encabezados, por lo que es útil para configurar el tamaño de ajuste MSS para habilitar bytes para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.
Subinterfaz no etiquetada		Especifica que todas las interfaces que pertenecen a esta interfaz de capa 3 no se etiqueten. PAN-OS® selecciona una subinterfaz sin etiquetar como la interfaz de entrada basada en el destino del paquete. Si el destino es la dirección IP de una subinterfaz sin etiquetar, se asignará a la subinterfaz. Esto también significa que un paquete que va en dirección inversa debe tener su dirección de origen traducida a la dirección IP de la subinterfaz sin etiquetar. Otra variable de esta forma de clasificación es que todos los paquetes de multidifusión y difusión se asignarán a la interfaz de base en lugar de a cualquiera de las subinterfaces. Como OSPF utiliza multidifusión, no es compatible con subinterfaces sin etiquetar.
Dirección IP Dirección MAC	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **ARP Entries**	Para añadir una o más entradas estáticas del protocolo de resolución de dirección (ARP), haga clic en **Add (Añadir)** y, a continuación, introduzca una dirección IP y la dirección del hardware asociado (MAC). Para eliminar una entrada, selecciónela y haga clic en **Delete (Eliminar)**. Las entradas ARP estáticas reducen el procesamiento ARP e impiden los ataques de man in the middle de las direcciones especificadas.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
	(Entradas de ARP)	
Dirección IPv6 Dirección MAC	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **ND Entries (Entradas de ND)**	Para proporcionar información sobre vecinos para el protocolo de detección de vecinos (NDP), haga clic en **Add (Añadir)** y, a continuación, introduzca la dirección IP y MAC del vecino.
Habilitar proxy NDP	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **NDP Proxy (Proxy NDP)**	Seleccione para habilitar el proxy de protocolo de detección de vecinos (NDP) para la interfaz. El cortafuegos no responderá a los paquetes ND que solicitan direcciones MAC para direcciones IPv6 en esta lista. En la respuesta ND, el cortafuegos envía su propia dirección MAC para la interfaz para indicar que funcionará como proxy respondiendo a los paquetes destinados para estas direcciones. Se recomienda que seleccione **Enable NDP Proxy (Habilitar proxy NDP)** si usa Traducción de prefijo de red IPv6 (NPTv6). Si **Enable NDP Proxy (Habilitar proxy NDP)** está seleccionado, puede filtrar varias cantidades de direcciones ingresando una cadena de búsqueda y haciendo clic en Apply Filter ( ).
Dirección		Haga clic en **Add (Añadir)** para introducir una o más direcciones IPv6, intervalos de IP, subredes IPv6 u objetos de direcciones para las que el cortafuegos actuará como el proxy NDP. Idealmente, una de estas direcciones es la misma que la traducción de origen en NPTv6. El orden de las direcciones es indiferente. Si la dirección es una subred, el cortafuegos enviará una respuesta ND para todas las direcciones de la subred, por lo que le recomendamos que agregue también los vecinos IPv6 del cortafuegos y seleccione **Negate (Negar)** para indicar al cortafuegos que no responda a estas direcciones IP.
Negar		Seleccione **Negate (Negar)** junto a una dirección para evitar el proxy NDP de esa dirección. Puede negar un subconjunto del intervalo de dirección IP o subred IP especificado.
Habilitar LLDP	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **LLDP**	Seleccione esta opción para habilitar Protocolo de detección de nivel de enlace (LLDP) en la interfaz. Funciones LLDP en la capa de enlace para descubrir dispositivos vecinos y sus capacidades.
Perfil de LLDP		Si LLDP está habilitado, seleccione un perfil LLDP para asignar a la interfaz o haga clic en **LLDP Profile (Perfil de LLDP)** para crear un nuevo perfil (consulte Network > Network Profiles >

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		LLDP Profile). Seleccione **None (Ninguno)** para configurar al cortafuegos para que use los valores predeterminados globales.
Habilite en el estado pasivo de HA		Si LLDP está habilitado, seleccione esta opción para permitir que el cortafuegos, como cortafuegos pasivo HA, prenegocie LLDP con su peer antes de que se active el cortafuegos.
Tipo	**Ethernet Interface (Interfaz Ethernet)** > **IPv4**	Seleccione el método para asignar un tipo de dirección IPv4 a la interfaz: • **Static (Estática)**: debe especificar manualmente la dirección IP. • **PPPoE**: el cortafuegos utilizará la interfaz para el protocolo punto a punto sobre Ethernet (PPPoE). • **DHCP Client (Cliente DHCP)**: permite a la interfaz actuar como cliente del protocolo de configuración de host dinámico (DHCP) y recibir una dirección IP dinámicamente asignada. *Los cortafuegos que están con una configuración de alta disponibilidad (High Availability, HA) activa/activa no admiten el cliente PPPoE o DHCP.* Las opciones que se muestran en la pestaña variarán según su selección de método de dirección IP.
Configuración	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)** > **DDNS**	Seleccione **Settings (Configuración)** para poner los campos DDNS a disposición para la configuración.
Habilitación		Habilitar DDNS en la interfaz. Debe habilitar inicialmente DDNS para configurarlo. (Si la configuración de su DDNS no está terminada, puede guardarla sin habilitarla, para no perder los ajustes parciales).
Intervalo de actualización (días)		Introduzca el intervalo (en días) entre las actualizaciones que el cortafuegos envía al servidor DDNS para actualizar las direcciones IP asignadas a los FQDN (el intervalo es de 1 a 30; el valor predeterminado es 1). *El cortafuegos también actualiza el DDNS tras recibir una dirección IP nueva para la interfaz desde el servidor DHCP.*
Perfil del certificado		Cree un perfil de certificado para verificar el servicio DDNS. El servicio DDNS presenta el cortafuegos con un certificado firmado por la autoridad de certificación (Certificate Authority, CA).
Nombre de host		Introduzca un nombre de host para la interfaz, que esté registrado con el servidor DDNS (por ejemplo, host123.domain123.com o host123). El cortafuegos no valida

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		el nombre de host, excepto para confirmar que la sintaxis utilice caracteres válidos permitidos por DNS para un nombre de dominio.
Proveedor		Seleccione el proveedor DDNS (y la versión) que proporcione el servicio DDNS a esta interfaz: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si selecciona una versión anterior de un servicio DDNS que el cortafuegos indica que se retirará antes de cierta fecha, pase a la versión más reciente.* Los campos **Name (Nombre)** y **Value (Valor)** que siguen al nombre del proveedor son específicos del proveedor. Los campos de solo lectura le notifican los parámetros que el cortafuegos utiliza para conectarse con el servicio DDNS. Configure los demás campos, como la contraseña que el servicio DDNS le proporciona y un tiempo de espera para que el cortafuegos utilice si no recibe respuesta del servidor DDNS.
Pestaña IPv4 - IP		Añada las direcciones IPv4 configuradas en la interfaz y luego selecciónelas. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Pestaña IPv6 - IPv6		Añada las direcciones IPv6 configuradas en la interfaz y luego selecciónelas. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Mostrar información de tiempo de ejecución		Muestra el registro DDNS: Proveedor DDNS, FQDN resuelto y las direcciones IP asignadas, con un asterisco (*) que indica la dirección IP principal. Cada proveedor DDNS posee sus propios códigos de retorno para indicar el estado de la actualización del nombre de host y una fecha de retorno para fines de solución de problemas.
Dirección IPv4 **Type (Tipo)** = **Static (Estático)**		
IP	**Ethernet Interface (Interfaz Ethernet)** > **IPv4**	Haga clic en **Add (Añadir)** y, a continuación, realice uno de los siguientes pasos para especificar una dirección IP y una máscara de red para la interfaz. • Escriba la entrada en la notación de enrutamiento entre dominios sin clases (CIDR): *dirección_ip/máscara* (por ejemplo, 192.168.2.0/24). • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		• Haga clic en **Address (Dirección)** para crear un objeto de dirección de tipo **IP netmask (Máscara de red IP)**. Puede introducir múltiples direcciones IP para la interfaz. La base de información de reenvío (FIB) que utiliza su cortafuegos determina el número máximo de direcciones de IP. Para eliminar una dirección IP, seleccione la dirección y haga clic en **Delete (Eliminar)**.
Dirección IPv4 **Type (Tipo)** = **PPPoE**		
Habilitación	**Ethernet Interface (Interfaz de Ethernet)** > **IPv4** > **PPPoE** > **General (General)**	Seleccione esta opción para activar la interfaz para la terminación PPPoE.
Nombre de usuario		Introduzca el nombre de usuario de la conexión de punto a punto.
Contraseña/ Confirmar contraseña		Introduzca y confirme la contraseña del nombre de usuario.
Mostrar información de tiempo de ejecución de cliente PPPoE		(Opcional) Abre un cuadro de diálogo que muestra los parámetros que el cortafuegos ha negociado con el proveedor de servicios de Internet (ISP) para establecer una conexión. La información específica depende del ISP.
Autenticación	**Ethernet Interface (Interfaz de Ethernet)** > **IPv4** > **PPPoE** > **Advanced (Avanzado)**	Seleccione el protocolo de autenticación para las comunicaciones PPPoE: **CHAP** (Protocolo de autenticación por desafío mutuo), **PAP** (Protocolo de autenticación de contraseña) o, de forma predeterminada, **Auto (Automático)** (el cortafuegos determina el protocolo). Seleccione **None (Ninguno)** para eliminar la asignación de protocolo actual de la interfaz.
Dirección estática		Realice uno de los siguientes pasos para especificar la dirección IP que ha asignado el proveedor de servicios de Internet (no predeterminado): • Escriba la entrada en la notación de enrutamiento entre dominios sin clases (CIDR): *dirección_ip/máscara* (por ejemplo, 192.168.2.0/24). • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**. • Haga clic en **Address (Dirección)** para crear un objeto de dirección de tipo **IP netmask (Máscara de red IP)**. • Seleccione **Ninguno** para eliminar la asignación de dirección actual de la interfaz.
Automatically create default route pointing to peer (Crear		Seleccione esta opción para crear automáticamente una ruta predeterminada que señale al peer PPPoE cuando se conecta.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
automáticamente una ruta predeterminada que apunte al peer)		
Métrica de ruta predeterminada		(Opcional) Para la ruta entre el cortafuegos y el proveedor de servicios de Internet, introduzca una métrica de ruta (nivel prioritario) que se asocie a la ruta predeterminada y que se utilice para la selección de ruta (el intervalo es de 1 a 65 535). El nivel de prioridad aumenta conforme disminuye el valor numérico.
Acceder a concentrador		(Opcional) Introduzca el nombre del concentrador de acceso, en el proveedor de servicios de Internet, al que se conecta el cortafuegos (no predeterminado).
service		(Opcional) Introduzca la cadena de servicio (no predeterminado).
Pasivo		Seleccione esta opción para utilizar el modo pasivo. En modo pasivo, un extremo PPPoE espera a que el concentrador de acceso envíe la primera trama.
Dirección IPv4 **Type (Tipo)** = **DHCP**		
Habilitación	**Ethernet Interface (Interfaz Ethernet)** > **IPv4**	Seleccione esta opción para activar el cliente DHCP en la interfaz.
Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor		Seleccione esta opción para que se cree automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada que proporciona el servidor DHCP.
Enviar nombre de host		Seleccione que el cortafuegos (como un cliente DHCP) envíe el nombre de host de la interfaz (opción 12) al servidor DHCP. Si envía el nombre de host, el nombre de host del cortafuegos será la opción predeterminada en el campo de nombre de host. Puede enviar ese nombre o introducir un nombre de host personalizado (64 caracteres como máximo, incluidas letras mayúsculas y minúsculas, números, puntos, guiones y guiones bajos.
Métrica de ruta predeterminada		Para la ruta entre el cortafuegos y el servidor DHCP, introduzca de forma optativa una métrica de ruta (nivel prioritario) que se asocie a la ruta predeterminada y que se utilice para la selección de ruta (el intervalo es de 1 a 65 535, no hay valor predeterminado). El nivel de prioridad aumenta conforme disminuye el valor numérico.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
Mostrar información de tiempo de ejecución de cliente DHCP		Seleccione que se muestren todos los ajustes recibidos desde el servidor DHCP, incluidos el estado de concesión de DHCP, la asignación de IP dinámica, la máscara de subred, la puerta de enlace y la configuración del servidor (DNS, NTP, dominio, WINS, NIS, POP3 y SMTP).
Habilitar IPv6 en la interfaz	**Ethernet Interface (Interfaz Ethernet)** > **IPv6**	Seleccione esta opción para habilitar las direcciones IPv6 en esta interfaz.
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.

Dirección		Haga clic en **Add (Añadir)** y configure los siguientes parámetros para cada una de las direcciones IPv6:
		• **Address (Dirección)**: escriba una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear un objeto de dirección.
		• **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz.
		• **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6.
		• **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.
		• **Send Router Advertisement (Enviar anuncio de enrutador)**: seleccione esta opción para habilitar el anuncio de enrutador (RA) de esta dirección IP. (También puede activar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** de forma global en la interfaz). Si desea información sobre el RA, consulte Enable Router Advertisement.
		Los campos restantes solo se aplican si habilita el RA.
		  • **Valid Lifetime (Duración válida)**: duración (en segundos) que el cortafuegos considera válida la dirección. La duración válida debe ser igual o superar la **Preferred Lifetime (Duración preferida)** (el valor predeterminado es 2 592 000).
		  • **Preferred Lifetime (Duración preferida)**: duración (en segundos) en la que se prefiere la dirección válida, lo que significa que el cortafuegos la puede utilizar para enviar

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		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). • **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador. • **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
Habilitar detección de direcciones duplicadas	**Ethernet Interface (Interfaz Ethernet)** > **IPv6** > **Address Resolution (Resolución de dirección)**	Seleccione esta opción para habilitar la detección de dirección duplicada (DAD) y configure los otros campos de esta sección.
Intentos DAD		Especifique el número de intentos DAD en el intervalo de solicitación de vecinos (**Neighbor Solicitation [NS] Interval**) antes de que falle el intento de identificar vecinos (el intervalo es de 1 a 10; el valor predeterminado es 1).
Tiempo alcanzable		Especifique la duración, en segundos, durante la que se puede establecer comunicación con un vecino tras una consulta y una respuesta correctas (el intervalo es de 10 a 36 000; el valor predeterminado es 30).
Intervalo NS (intervalo de solicitación de vecinos)		Especifique el número de segundos de intentos DAD antes de indicar el fallo (el intervalo es de 1 a 10; el valor predeterminado es 1).
Habilitar supervisión NDP		Seleccione esta opción para habilitar la supervisión del protocolo de detección de vecinos (NDP). Cuando está habilitada, puede seleccionar NDP Monitor (Supervisor NDP) (en la columna Features [Características]) y ver información acerca de un vecino detectado por el cortafuegos, como la dirección IPv6, la dirección MAC correspondiente y el User-ID (según el mejor de los casos).
Habilitar anuncio de enrutador	**Ethernet Interface (Interfaz Ethernet)** > **IPv6** > **Router Advertisement (Anuncio del enrutador)**	Para poder llevar a cabo la configuración automática de direcciones sin estado (SLAAC) en interfaces IPv6, seleccione esta opción y configure los otros campos de esta sección. Los clientes DNS IPv6 que reciben mensajes de anuncio de enrutador (RA, por sus siglas en inglés) utilizan esta información. El RA permite al cortafuegos actuar como una puerta de enlace predeterminada para hosts IPv6 que no estén configurados estáticamente y proporcionar al host un prefijo IPv6 que se puede utilizar para la configuración de direcciones. Puede utilizar

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		un servidor DHCPv6 independiente junto con esta función para proporcionar DNS y otros ajustes a los clientes. Esta opción es un ajuste global de la interfaz. Si desea establecer las opciones de RA para direcciones IP individuales, haga clic en **Add (Añadir)** en la tabla de direcciones IP y configure la opción Address. Si establece las opciones de RA para cualquier dirección IP, debe seleccionar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz.
Mín. de intervalo (segundos)		Especifique el intervalo mínimo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 3 a 1350; el valor predeterminado es 200). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Máx. de intervalo (segundos)		Especifique el intervalo máximo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 4 a 1800; el valor predeterminado es 600). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Límite de salto		Especifique el 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.
MTU de enlace		Especifique la unidad máxima de transmisión (MTU) del enlace que se debe aplicar a los clientes. Seleccione **unspecified (no especificado)** si no desea ninguna MTU de enlace (intervalo es de 1280 a 9192; el valor predeterminado es no especificado).
Tiempo alcanzable (ms)		Especifique 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 no especificado).
Tiempo de retransmisión (ms)		Especifique el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente (en milisegundos) antes de retransmitir los mensajes de solicitación 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 no especificado).
Duración de enrutador (segundos)		Especifique por cuánto tiempo 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

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
		cortafuegos de la lista de ruta predeterminada y utiliza otro enrutador como puerta de enlace predeterminada.
Preferencia de enrutador		Si el segmento de la red tiene múltiples enrutadores de IPv6, el cliente utiliza este campo para seleccionar un enrutador preferido. Seleccione si el RA publica el enrutador del cortafuegos con prioridad **High (Alta)**, **Medium (Media)** (predeterminada) o **Low (Baja)** en relación con otros enrutadores del segmento.
Configuración gestionada		Seleccione esta opción para indicar al cliente que las direcciones están disponibles en DHCPv6.
Comprobación de coherencia	**Ethernet Interface (Interfaz Ethernet)** > **IPv6** > **Router Advertisement (Anuncio del enrutador) (cont.)**	Seleccione esta opción si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos registra cualquier incoherencia en un log del sistema de tipo **ipv6nd**.
Otras configuraciones		Seleccione esta opción para indicar al cliente que hay disponible otra información de dirección (por ejemplo, configuración relacionada con DNS) en DHCPv6.
Incluir información DNS en anuncio de enrutador	**Ethernet Interface (Interfaz Ethernet)** > **IPv6** > **DNS Support (Asistencia DNS)**	Seleccione esta opción para que el cortafuegos envíe información de DNS en los mensajes de anuncios del enrutador NDP (RA) de esta interfaz Ethernet IPv6. El resto de campos de DNS Support (Asistencia DNS) de esta tabla solo pueden verse al seleccionar esta opción.
Servidor		Haga clic en **Add (Añadir)** para añadir una o más direcciones recursivas de servidor DNS (RDNS) a fin de que el cortafuegos envíe anuncios de enrutador NDP desde esta interfaz Ethernet IPv6. Los servidores RDNS envían una serie de solicitudes de búsqueda de DNS a los servidores DNS raíz y servidores DNS autoritativos para finalmente proporcionar una dirección IP al cliente DNS. Puede configurar un número máximo de ocho servidores RDNS que el cortafuegos envía (en orden descendente) en un anuncio del enrutador NDP al destinatario, que luego utiliza esas direcciones en el mismo orden. Seleccione un servidor y utilice las opciones **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar el orden de los servidores, o **Delete (Eliminar)** para quitar un servidor de la lista cuando ya no lo necesite.
Duración		Introduzca la cantidad máxima de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar los servidores RDNS para resolver nombres de dominio (el intervalo es del valor de Max Interval [sec] al doble del intervalo máximo; el valor predeterminado es 1200).

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de capa 3	Configurado en	Description (Descripción)
Sufijo		Pulse **Add (Añadir)** para añadir uno o varios nombres de dominio (sufijos) a la lista de búsqueda DNS (DNSSL) y configúrelos. La longitud máxima es de 255 bytes. Una lista de búsqueda de DNS es una lista de sufijos de dominio que un enrutador de cliente DNS anexa (uno a la vez) a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, utilizando de ese modo un nombre de dominio completo en la consulta DNS. Por ejemplo, si un cliente DNS trata de enviar una consulta DNS de “calidad” sin sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda DNS al nombre, y luego transmite la 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 enrutador agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El enrutador prueba sufijos DNS hasta que una búsqueda de DNS sea correcta (omite 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 detección de vecinos; el cliente DNS que recibe la opción DNSSL utiliza los sufijos en sus consultas DNS no calificadas. Puede configurar hasta ocho nombres de dominio (sufijos) para una lista de búsqueda de DNS que el cortafuegos envía (en orden descendente) en un anuncio del enrutador NDP al destinatario, que luego utiliza dichas direcciones en el mismo orden. Seleccione un sufijo y utilice las opciones **Move Up (Subir)** o **Move Down (Bajar)** para cambiar el orden, o **Delete (Eliminar)** para quitar un sufijo de la lista cuando ya no lo necesite.
Duración		Introduzca el máximo de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar un nombre de dominio (sufijo) en la lista de búsqueda DNS (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).

Subinterfaz de la capa 3

- Network > Interfaces > Ethernet

Para cada puerto Ethernet configurado como interfaz física de capa 3, puede definir interfaces adicionales lógicas de capa 3 (subinterfaces).

Para configurar una interfaz de capa 3 de la seria PA-7000, seleccione una interfaz física, haga clic en **Add Subinterface (Añadir subinterfaz)** y especifique la siguiente información.

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz de capa3**	El campo **Interface Name (Nombre de interfaz)** de solo lectura muestra el nombre de la interfaz física que ha seleccionado. En el campo adyacente, introduzca un sufijo numérico (de 1 a 9999) para identificar la subinterfaz.
Comentarios		Introduzca una descripción opcional para la subinterfaz.
Tag (Etiqueta)		Introduzca la etiqueta VLAN (de 1 a 4094) para la subinterfaz.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una subinterfaz de entrada a un servidor NetFlow, seleccione el perfil del servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (Ninguna)** para eliminar la asignación actual del servidor NetFlow de la subinterfaz.
Enrutador virtual	**Layer3 Subinterface (Subinterfaz de capa 3) > Config (Configuración)**	Asigne un enrutador virtual a la interfaz o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network > Virtual Routers). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la subinterfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la subinterfaz o haga clic en **Zone** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la subinterfaz.
Tipo	**Layer3 Subinterface (Subinterfaz de capa 3) > IPv4**	Seleccione el método para asignar un tipo de dirección IPv4 a la subinterfaz: • **Static (Estática)**: debe especificar manualmente la dirección IP. • **DHCP Client (Cliente DHCP)**: permite a la subinterfaz actuar como cliente del protocolo de configuración de host dinámico (DHCP) y recibir una dirección IP dinámicamente asignada. *Los cortafuegos que están con una configuración de alta disponibilidad (High Availability, HA) activa/activa no admiten el cliente DHCP.* Las opciones que se muestran en la pestaña variarán según su selección de método de dirección IP.
IP	**Layer3 Subinterface (Subinterfaz**	Haga clic en **Add** y lleve a cabo uno de los siguientes pasos a fin de especificar una dirección IP estática y una máscara de red para la interfaz.

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
	de capa 3) > IPv4, Type = Static (IPv4, Tipo = Estático)	• Escriba la entrada en la notación de enrutamiento entre dominios sin clases (CIDR): *dirección_ip/máscara* (por ejemplo, 192.168.2.0/24). • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**. • Cree un objeto **Address (Dirección)** de tipo **IP netmask (Máscara de red IP)**. Puede introducir múltiples direcciones IP para la interfaz. La base de información de reenvío (FIB) que utiliza su sistema determina el número máximo de direcciones IP. Seleccione **Delete (Borrar)** para borrar una dirección IP cuando ya no la necesite.
Habilitación	**Layer3 Subinterface (Subinterfaz de capa 3) > IPv4, Type = DHCP (IPv4, Tipo = DHCP)**	Seleccione esta opción para activar el cliente DHCP en la interfaz.
Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor		Seleccione esta opción para que se cree automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada que proporciona el servidor DHCP.
Enviar nombre de host		Seleccione que el cortafuegos (como un cliente DHCP) envíe el nombre de host de la interfaz (opción 12) al servidor DHCP. Si envía el nombre de host, de manera predeterminada, el nombre de host del cortafuegos será la opción predeterminada en el campo de nombre de host. Puede enviar ese nombre o introducir un nombre de host personalizado (64 caracteres como máximo, incluidas letras mayúsculas y minúsculas, números, puntos, guiones y guiones bajos.
Métrica de ruta predeterminada		(Opcional) Para la ruta entre el cortafuegos y el servidor DHCP, puede introducir una métrica de ruta (nivel prioritario) que se asocie a la ruta predeterminada y que se utilice para la selección de ruta (el intervalo es de 1a 65 535, no hay valor predeterminado). El nivel de prioridad aumenta conforme disminuye el valor numérico.
Mostrar información de tiempo de ejecución de cliente DHCP		Seleccione **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)** para mostrar todos los ajustes recibidos desde el servidor DHCP, incluidos el estado de concesión de DHCP, la asignación de IP dinámica, la máscara de subred, la puerta de enlace, la configuración del servidor (DNS, NTP, dominio, WINS, NIS, POP3 y SMTP).

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
Habilitar IPv6 en la interfaz	**Layer3 Subinterface (Subinterfaz de capa 3)** > **IPv6**	Seleccione esta opción para habilitar las direcciones IPv6 en esta interfaz.
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.

Dirección		Haga clic en **Add (Añadir)** y configure los siguientes parámetros para cada una de las direcciones IPv6:
		• **Address (Dirección)**: escriba una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear un objeto de dirección.
		• **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz.
		• **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6.
		• **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.
		• **Send Router Advertisement (Enviar anuncio de enrutador)**: seleccione esta opción para habilitar el anuncio de enrutador (RA) de esta dirección IP. (También puede activar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** de forma global en la interfaz). Si desea información sobre el RA, consulte Enable Router Advertisement en esta tabla.
		Los campos restantes solo se aplican si habilita el RA.
		  • **Valid Lifetime (Duración válida)**: duración (en segundos) que el cortafuegos considera válida la dirección. La duración válida debe ser igual o superar la **duración preferida**. El valor predeterminado es de 2.592.000.
		  • **Preferred Lifetime (Duración preferida)**: duración (en segundos) en 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.

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
		• **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador. • **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
Habilitar detección de direcciones duplicadas	**Layer3 Subinterface (Subinterfaz de capa 3)** > **IPv6** > **Address Resolution (Resolución de dirección)**	Seleccione esta opción para habilitar la detección de dirección duplicada (DAD) y configure los otros campos de esta sección.
Intentos DAD		Especifique el número de intentos DAD en el intervalo de solicitación de vecinos (**Neighbor Solicitation [NS] Interval**) antes de que falle el intento de identificar vecinos (el intervalo es de 1 a 10; el valor predeterminado es 1).
Tiempo alcanzable		Especifique la duración, en segundos, durante la que se puede establecer comunicación con un vecino tras una consulta y una respuesta correctas (el intervalo es de 1 a 36 000 s; el valor predeterminado es 30).
Intervalo NS (intervalo de solicitación de vecinos)		Especifique el número de segundos de intentos DAD antes de indicar el fallo (el intervalo es de 1 a 10; el valor predeterminado es 1).
Habilitar supervisión NDP		Seleccione esta opción para habilitar la supervisión del protocolo de detección de vecinos (NDP). Cuando está habilitada, puede seleccionar NDP (en la columna Features [Características]) para ver la información sobre un vecino detectado por el cortafuegos, como la dirección IPv6, la dirección MAC correspondiente y el User-ID (en el mejor de los casos).
Habilitar anuncio de enrutador	**Layer3 Subinterface (Subinterfaz de capa 3)** > **IPv6** > **Router Advertisement (Anuncio del enrutador)**	Para poder llevar a cabo la detección de vecinos en interfaces IPv6, seleccione esta opción y configure los otros campos de esta sección. Los clientes DNS IPv6 que reciben mensajes de anuncio de enrutador (RA, por sus siglas en inglés) utilizan esta información. El RA permite al cortafuegos actuar como una puerta de enlace predeterminada para hosts IPv6 que no estén configurados estáticamente y proporcionar al host un prefijo IPv6 que se puede utilizar para la configuración de direcciones. Puede utilizar un servidor DHCPv6 independiente junto con esta función para proporcionar DNS y otros ajustes a los clientes. Esta opción es un ajuste global de la interfaz. Si desea configurar las opciones de RA para direcciones IP individuales, seleccione **Add (Añadir)** y configure una Address en la tabla de direcciones IP. Si establece las opciones de RA para cualquier dirección

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
		IP, debe seleccionar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz.
Mín. de intervalo (segundos)		Especifique el intervalo mínimo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 3 a 1350; el valor predeterminado es 200). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Máx. de intervalo (segundos)		Especifique el intervalo máximo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 4 a 1800; el valor predeterminado es 600). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Límite de salto		Especifique el 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.
MTU de enlace		Especifique la unidad máxima de transmisión (MTU) del enlace que se debe aplicar a los clientes. Seleccione **unspecified (no especificado)** si no desea ninguna MTU de enlace (intervalo es de 1280 a 9192; el valor predeterminado es no especificado).
Tiempo alcanzable (ms)		Especifique 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 no especificado).
Tiempo de retransmisión (ms)		Especifique el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente (en milisegundos) antes de retransmitir los mensajes de solicitación 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 no especificado).
Duración de enrutador (segundos)		Especifique la duración, en segundos, por la que 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.
Preferencia de enrutador		Si el segmento de la red tiene múltiples enrutadores de IPv6, el cliente utiliza este campo para seleccionar un enrutador

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
		preferido. Seleccione si el RA publica el enrutador del cortafuegos con prioridad **High (Alta)**, **Medium (Media)** (predeterminada) o **Low (Baja)** en relación con otros enrutadores del segmento.
Configuración gestionada		Seleccione esta opción para indicar al cliente que las direcciones están disponibles en DHCPv6.
Otras configuraciones		Seleccione esta opción para indicar al cliente que hay disponible otra información de dirección (por ejemplo, configuración relacionada con DNS) en DHCPv6.
Comprobación de coherencia	**Layer3 Subinterface (Subinterfaz de capa 3)** > **IPv6** > **Router Advertisement (cont) (Anuncio del enrutador [cont.])**	Seleccione esta opción si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos registra cualquier incoherencia en un log del sistema de tipo **ipv6nd**.
Incluir información DNS en anuncio de enrutador	**Layer3 Subinterface (Subinterfaz de capa 3)** > **IPv6** > **DNS Support (Asistencia DNS)**	Seleccione esta opción para que el cortafuegos incluya información de DNS en los anuncios del enrutador NDP de esta subinterfaz Ethernet IPv6. El resto de campos de DNS Support (Asistencia DNS) de esta tabla solo pueden verse al seleccionar esta opción.
Servidor		Haga clic en **Add (Añadir)** para añadir una o más direcciones recursivas de servidor DNS (RDNS) a fin de que el cortafuegos envíe anuncios de enrutador NDP desde esta interfaz Ethernet IPv6. Los servidores RDNS envían una serie de solicitudes de búsqueda de DNS a los servidores DNS raíz y servidores DNS autoritativos para finalmente proporcionar una dirección IP al cliente DNS. Puede configurar hasta ocho servidores RDNS que el cortafuegos envía (en orden descendente) en un anuncio del enrutador NDP al destinatario, que luego los utiliza en el mismo orden. Seleccione un servidor y utilice las opciones **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar el orden de los servidores, o **Delete (Eliminar)** para quitar un servidor de la lista cuando ya no lo necesite.
Duración		Introduzca la cantidad máxima de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar un servidor RDNS para resolver nombres de dominio (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
Sufijo	**Subinterfaz de capa 3** > **IPv6** > **Soporte DNS (continuación)**	Pulse **Add (Añadir)** para añadir uno o varios nombres de dominio (sufijos) a la lista de búsqueda DNS (DNSSL). La longitud máxima es de 255 bytes. Una lista de búsqueda de DNS es una lista de sufijos de dominio que un enrutador de cliente DNS anexa (uno a la vez) a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, con lo cual utiliza un nombre de dominio completo en la consulta. Por ejemplo, si un cliente DNS trata de enviar una consulta DNS del nombre "calidad" sin sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda DNS al nombre y transmite la consulta DNS. Si el primer sufijo DNS de la lista es "empresa.com", la consulta DNS resultante del enrutador se realizará con el nombre de dominio completo "calidad.empresa.com". Si la consulta DNS falla, el enrutador agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El enrutador utiliza los sufijos DNS hasta que una búsqueda de DNS sea correcta (omite 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 detección de vecinos; el cliente DNS que recibe la opción DNSSL utiliza los sufijos en sus consultas DNS no calificadas. Puede configurar hasta ocho nombres de dominio (sufijos) para una opción de lista de búsqueda de DNS que el cortafuegos envía (en orden descendente) en un anuncio del enrutador NDP al destinatario, que luego los utiliza en el mismo orden. Seleccione un sufijo y utilice las opciones **Move Up (Subir)** o **Move Down (Bajar)** para cambiar el orden, o **Delete (Eliminar)** para quitar un sufijo de la lista cuando ya no lo necesite.
Duración	**Subinterfaz de capa 3** > **IPv6** > **Soporte DNS (continuación)**	Introduzca el máximo de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar un nombre de dominio (sufijo) en la lista de búsqueda DNS (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).
Perfil de gestión	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **Other Info (Otra información)**	**Management Profile (Perfil de gestión)**: seleccione un perfil que defina los protocolos (por ejemplo, SSH, Telnet y HTTP) que puede usar para gestionar el cortafuegos en esta interfaz. Seleccione **None (Ninguna)** para eliminar la asignación de perfil actual de la interfaz.
MTU		Introduzca la unidad máxima de transmisión (maximum transmission unit, MTU) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 9.192 y el valor predeterminado, 1.500). Si las máquinas de ambos extremos

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
		del cortafuegos ejecutan un descubrimiento de MTU de ruta (PMTUD) y la interfaz recibe un paquete que supera la MTU, el cortafuegos envía al origen un mensaje de *necesidad de fragmentación del ICMP* que indica que el paquete es demasiado grande.
Ajustar TCP MSS	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **Other Info (Otra información)**	Seleccione esta opción para ajustar el tamaño de segmento máximo (MSS) de forma que se pueda albergar bytes de cualquier encabezado dentro del tamaño de byte MTU de la interfaz. El tamaño de byte MTU menos el tamaño de ajuste MSS es igual al tamaño de byte MSS, que varía según el protocolo de IP: • **IPv4 MSS Adjustment Size (Tamaño de ajuste IPv4 MSS)**: el intervalo es de 40 a 300; el valor predeterminado es 40. • **IPv6 MSS Adjustment Size (Tamaño de ajuste IPv6 MSS)**: el intervalo es de 60 a 300; el valor predeterminado es 60. Utilice esta configuración para tratar los casos en los que un **tunnel (túnel)** en la red necesita un MSS más pequeño. Si un paquete tiene más bytes que el MSS sin fragmentación, este parámetro permite ajustarlo. La encapsulación les añade longitud a los encabezados, por lo que es útil para configurar el tamaño de ajuste MSS para habilitar bytes para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.
Dirección IP Dirección MAC	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **ARP Entries (Entradas de ARP)**	Para añadir una o más entradas estáticas del protocolo de resolución de dirección (ARP), **Add (Añada)** una dirección IP y la dirección del hardware asociado (Media Access Control o MAC). Para eliminar una entrada, selecciónela y haga clic en **Delete (Eliminar)**. Las entradas de ARP estáticas reducen el procesamiento de ARP.
Dirección IPv6 Dirección MAC	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **ND Entries (Entradas ND)**	Para proporcionar información sobre vecinos para el protocolo de detección de vecinos (Neighbor Discovery Protocol, NDP), **Add (Añada)** la dirección IP y MAC del vecino.
Habilitar proxy NDP	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced**	Habilite el proxy del protocolo de detección de vecinos (NDP) de la interfaz. El cortafuegos no responderá a los paquetes ND que solicitan direcciones MAC para direcciones IPv6 en esta lista. En la respuesta ND, el cortafuegos envía su propia dirección MAC

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
	(Avanzado) > **NDP Proxy (Proxy NDP)**	para la interfaz, de modo que el cortafuegos recibirá paquetes dirigidos a las direcciones en la lista. Se recomienda que habilite el proxy NDP si usa traducción de prefijo de red IPv6 (NPTv6). Si se seleccionó **Enable NDP Proxy (Habilitar proxy NDP)**, puede filtrar numerosas entradas **Address (Dirección)** introduciendo un filtro y haciendo clic en Apply Filter (la flecha gris).
Dirección		Haga clic en **Add (Añadir)** para añadir una o más direcciones IPv6, intervalos de IP, subredes IPv6 u objetos de direcciones con las que el cortafuegos ejercerá como proxy NDP. Idealmente, una de estas direcciones es la misma que la traducción de origen en NPTv6. El orden de las direcciones es indiferente. Si la dirección es una subred, el cortafuegos enviará una respuesta ND para todas las direcciones de la subred, por lo que le recomendamos que agregue también los vecinos IPv6 del cortafuegos y haga clic en **Negate (Negar)** para indicar al cortafuegos que no responda a estas direcciones IP.
Negar		Seleccione **Negate (Negar)**, junto a cualquier dirección, para evitar el proxy NDP de dicha dirección. Puede negar un subconjunto del intervalo de dirección IP o subred IP especificado.
Configuración	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **DDNS**	Seleccione **Settings (Configuración)** para poner los campos DDNS a disposición para la configuración.
Habilitación		Habilitar DDNS en la interfaz. Debe habilitar inicialmente DDNS para configurarlo. (Si la configuración de su DDNS no está terminada, puede guardarla sin habilitarla, para no perder los ajustes parciales).
Intervalo de actualización (días)	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **DDNS**	Introduzca el intervalo (en días) entre las actualizaciones que el cortafuegos envía al servidor DDNS para actualizar las direcciones IP asignadas a los FQDN (el intervalo es de 1 a 30; el valor predeterminado es 1). *El cortafuegos también actualiza el DDNS tras recibir una dirección IP nueva para la interfaz desde el servidor DHCP.*
Perfil del certificado		Cree un perfil de certificado para verificar el servicio DDNS. El servicio DDNS presenta el cortafuegos con un certificado firmado por la autoridad de certificación (Certificate Authority, CA).
Nombre de host		Introduzca un nombre de host para la interfaz, que esté registrado con el servidor DDNS (por ejemplo,

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de capa 3	Configurado en	Description (Descripción)
		host123.domain123.com o host123). El cortafuegos no valida el nombre de host, excepto para confirmar que la sintaxis utilice caracteres válidos permitidos por DNS para un nombre de dominio.
Proveedor	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **DDNS**	Seleccione el proveedor DDNS (y la versión) que proporcione el servicio DDNS a esta interfaz: • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si selecciona una versión anterior de un servicio DDNS que el cortafuegos indica que se retirará antes de cierta fecha, pase a la versión más reciente.* Los campos **Name (Nombre)** y **Value (Valor)** que siguen al nombre del proveedor son específicos del proveedor. Los campos de solo lectura le notifican los parámetros que el cortafuegos utiliza para conectarse con el servicio DDNS. Configure los demás campos, como la contraseña que el servicio DDNS le proporciona y un tiempo de espera para que el cortafuegos utilice si no recibe respuesta del servidor DDNS.
Pestaña IPv4 - IP		Añada las direcciones IPv4 configuradas en la interfaz y luego selecciónelas. Puede seleccionar solo la cantidad de direcciones IPv4 que permita el proveedor DDNS. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Pestaña IPv6 - IPv6		Añada las direcciones IPv6 configuradas en la interfaz y luego selecciónelas. Puede seleccionar solo la cantidad de direcciones IPv6 que permita el proveedor DDNS. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Mostrar información de tiempo de ejecución	**Layer3 Subinterface (Subinterfaz de capa 3)** > **Advanced (Avanzado)** > **DDNS**	Muestra el registro DDNS: Proveedor DDNS, FQDN resuelto y las direcciones IP asignadas, con un asterisco (*) que indica la dirección IP principal. Cada proveedor DDNS posee sus propios códigos de retorno para indicar el estado de la actualización del nombre de host y una fecha de retorno para fines de solución de problemas.

Interfaz de tarjeta de log

- Network > Interfaces > Ethernet

© 2020 Palo Alto Networks, Inc.

Si configura el reenvío de logs en un cortafuegos de la serie PA-7000 con una tarjeta de procesamiento de logs (Log Processing Card, LCP), debe configurar un puerto de datos de tipo **Log Card (Tarjeta de log)**. Esto se debe a que las funciones de tráfico y logs de este modelo de cortafuegos superan a las de la interfaz de gestión (MGT). Un puerto de datos de tarjeta de log realiza el reenvío de logs para syslog, el correo electrónico, el protocolo simple de administración de redes (SNMP), el reenvío de logs de Panorama y el de archivos WildFire™.

En el cortafuegos, solo puede configurar un puerto de tipo Log Card (Tarjeta de log). Si habilita el reenvío de logs, pero no configura ninguna interfaz con el tipo Log Card (Tarjeta de log), se produce un error al tratar de compilar los cambios.

Para configurar una interfaz de tarjeta de log, seleccione una interfaz que no esté configurada (por ejemplo, Ethernet1/16) y configure los parámetros que se describen en la siguiente tabla.

Configuración de la interfaz de Log Card	Configurado en	Description (Descripción)
Ranura	**Interfaz Ethernet**	Seleccione el número de ranura (1-12) de la interfaz.
Nombre de interfaz		El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tipo de interfaz		Seleccione **Log card (Tarjeta de log)**.
IPv4	**Ethernet Interface (Interfaz Ethernet)** > **Log Card Forwarding (Reenvío de tarjeta de log)**	Si su red use IPv4, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv4 del puerto. • **Netmask Máscara de red)**: la máscara de red para la dirección IPv4 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv4 del puerto de enlace predeterminado al puerto.
IPv6		Si su red use IPv6, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv6 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv6 del puerto de enlace predeterminado al puerto.
Velocidad de enlace	**Ethernet Interface (Interfaz Ethernet)** > **Advanced (Avanzado)**	Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** (por defecto) para que el cortafuegos determine automáticamente la velocidad según la conexión. Para interfaces que tienen una velocidad que no puede configurarse, **auto (automático)** es la única opción. *La velocidad mínima recomendada para la conexión es 1000 (Mbps).*
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**)

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz de Log Card	Configurado en	Description (Descripción)
		o negociado automáticamente según la conexión (**auto (automático)**). El valor predeterminado es **auto**.
estado del enlace		Seleccione si el estado de la interfaz es activada (**up (activada)**), desactivada (**down (desactivada)**) o determinado automáticamente según la conexión (**auto (automático)**). El valor predeterminado es **auto**.

Subinterfaz de tarjeta de log

- Network > Interfaces > Ethernet

Para añadir una Interfaz de tarjeta de log, seleccione la fila de dicha interfaz, haga clic en **Add Subinterface (Añadir subinterfaz)** e indique la siguiente información.

Configuración de la subinterfaz de Log Card	Configurado en	Description (Descripción)
Nombre de interfaz	**Subinterfaz LPC**	El campo **Interface Name (Nombre de interfaz)** (solo lectura) muestra el nombre de la interfaz de tarjeta log que ha seleccionado. En el campo adyacente, introduzca un sufijo numérico (1-9.999) para identificar la subinterfaz.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tag (Etiqueta)		Introduzca la **Tag (Etiqueta)** VLAN (0-4.094) para la subinterfaz. *Por comodidad, lo recomendable es que el número de la etiqueta sea igual que el de la subinterfaz.*
Sistema virtual	**Subinterface LPC (Subinterfaz LCP)** > **Config (Configuración)**	Seleccione el sistema virtual (vsys) al que se asigna la subinterfaz de tarjeta de procesamiento de log (LPC). Alternativamente, puede hacer clic en **Virtual Systems (Sistemas virtuales)** para añadir un nuevo vsys. Cuando una subinterfaz LPC se asigna a vsys, esa interfaz se usa como interfaz fuente para todos los servicios que envía logs (syslog, correo electrónico, SNMP) desde la tarjeta de log.
IPv4	**Ethernet Interface (Interfaz Ethernet)** > **Log Card Forwarding (Reenvío de tarjeta de log)**	Si su red use IPv4, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv4 del puerto. • **Netmask Máscara de red)**: la máscara de red para la dirección IPv4 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv4 del puerto de enlace predeterminado al puerto.
IPv6		Si su red use IPv6, defina lo siguiente:

© 2020 Palo Alto Networks, Inc.

Configuración de la subinterfaz de Log Card	Configurado en	Description (Descripción)
		• **IP address (Dirección IP)**: dirección IPv6 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv6 del puerto de enlace predeterminado al puerto.

Interfaz de reflejo de descifrado

- Network > Interfaces > Ethernet

Para utilizar la función Reflejo de puerto de descifrado, debe seleccionar el tipo de la interfaz **Decrypt Mirror (Reflejo de descifrado)**. Esta función permite crear una copia del tráfico descifrado desde un cortafuegos y enviarla a una herramienta de recopilación de tráfico que pueda recibir capturas de paquetes sin formato (como NetWitness o Solera) 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 (DLP) necesitan esta función. Para permitir la función, debe adquirir e instalar la licencia gratuita.

El reflejo del puerto de descifrado no está disponible en la serie VM para las plataformas de nube pública (AWS, Azure, Google Cloud Platform), VMware NSX y Citrix SDX.

Para configurar una interfaz de reflejo de descifrado, haga clic en el nombre de una interfaz (ethernet1/1, por ejemplo) que no esté configurada y especifique la siguiente información.

Configuración de interfaz de reflejo de descifrado	Description (Descripción)
Nombre de interfaz	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios	Introduzca una descripción opcional para la interfaz.
Tipo de interfaz	Seleccione **Decrypt Mirror (Reflejo de descifrado)**.
Velocidad de enlace	Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad.
Dúplex de enlace	Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace	Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).

Grupo de interfaz de Ethernet agregados (AE)

- Network > Interfaces > Ethernet

Un grupo de interfaz AE utiliza 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 a otro

© 2020 Palo Alto Networks, Inc.

cortafuegos. Un grupo de interfaz AE aumenta el ancho de banda entre peers cargando tráfico de balance en las interfaces combinadas. También proporciona redundancia; cuando una interfaz falla, las interfaces restantes continúan manteniendo el tráfico.

Antes de configurar un grupo de interfaz AE, 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 (1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps) y el tipo de interfaz (HA3, cable virtual, capa 2 o capa 3) deben ser los mismos. Puede añadir hasta ocho grupos de interfaz AE por cortafuegos, y cada grupo puede tener hasta ocho interfaces.

Todos los cortafuegos de Palo Alto Networks, excepto los modelos de la serie VM, admiten los grupos de interfaz AE.

Puede agregar las interfaces HA3 (reenvío de paquetes) en una configuración activa/activa de alta disponibilidad (HA), pero solo los siguientes cortafuegos de cortafuegos:

- *PA-220*
- *Serie PA-800*
- *Serie PA-3200*
- *Serie PA-5200*

Para configurar un grupo de interfaz AE, **Add Aggregate Group (Añadir grupo de agregación)**, configure los ajustes descritos en la siguiente tabla y asigne interfaces al grupo (consulte Interfaz Ethernet de agregación (AE)).

Configuración de grupo de interfaces de agregación	Configurado en	Description (Descripción)
Nombre de interfaz	**Agregar interfaz Ethernet**	El campo **Interface Name (Nombre de interfaz)** de solo lectura se define como **ae**. En el campo adyacente, introduzca un sufijo numérico (1 a 8) para identificar el grupo de interfaz AE.
Comentarios		Introduzca una descripción opcional para la interfaz.
Tipo de interfaz		Seleccione el tipo de interfaz, que controla los requisitos de configuración y opciones que quedan: • **HA**: Solo seleccione si la interfaz es un enlace de HA3 entre dos cortafuegos en una implementación activa/activa. También puede seleccionar un **Netflow Profile (Perfil de flujo de red)** y configurar la pestaña **LACP** (consulte Habilitar LACP). • **Virtual Wire**: También puede seleccionar un **Netflow Profile (Perfil de flujo de red)**, y configurar las pestañas **Config** y **Advanced (Avanzado)** tal y como se describe en Configuración de Virtual Wire. • **Layer 2 (Capa 2)**: Puede seleccionar de manera opcional un **Netflow Profile (Perfil de flujo de red)**; configurar las pestañas **Config** y **Advanced (Avanzado)** como se describe en Configuración de interfaz de capa 2 ; también puede configurar la pestaña **LACP** (consulte Habilitar LACP). • **Layer 3 (Capa 3)**: Puede seleccionar de manera opcional un **Netflow Profile (Perfil de flujo de red)**; configurar las pestañas **Config**, **IPv4** o **IPv6** y **Advanced (Avanzado)**, como se describe

© 2020 Palo Alto Networks, Inc.

Configuración de grupo de interfaces de agregación	Configurado en	Description (Descripción)
		en Configuración de interfaz de capa 3 ; y, de forma opcional, puede configurar la pestaña **LACP** (consulte Habilitar LACP).
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (Ninguna)** para eliminar la asignación actual del servidor NetFlow del grupo de interfaz AE.
Habilitar LACP	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación) > LACP**	Seleccione esta opción si desea habilitar el Protocolo de control de agregación de grupo (LACP) para el grupo de interfaz AE. LACP está deshabilitada de manera predeterminada. Si habilita LACP, la detección de fallas de la interfaz es automática en las capas física y de enlace de datos, sin importar si el cortafuegos y su peer LACP están conectados directamente. (Sin LACP, la detección de fallas de interfaz es automática solo en la capa física, entre peers conectados directamente). LACP también habilita una conmutación por error automática a interfaces en espera si se configuran reservas activas (consulte Puertos máx.).
Modo		Seleccione el modo de LACP del cortafuegos. Entre cualquier par de peers LACP, se recomienda que uno sea activo y otro pasivo. LACP no puede funcionar si los dos peers son pasivos. • **Active (Activo)**: el cortafuegos consulta de forma activa el estado del LACP (disponible o sin respuesta) de dispositivos de peer. • **Passive (Pasivo)** (predeterminado): el cortafuegos responde pasivamente a las consultas de estado del LACP procedentes de los dispositivos peer.
Velocidad de transmisión		Seleccione la velocidad con la que el cortafuegos intercambia consultas y responde a los dispositivos peer. • **Fast (Rápido)**: cada segundo • **Slow (Lento)**: cada 30 segundos (este es el ajuste predeterminado)
Conmutación rápida		Seleccione esta opción si, cuando una interfaz tiene un fallo, desea que el cortafuegos cambie a una interfaz operativa en 1 segundo. De lo contrario, el fallo se produce a la velocidad estándar definida en IEEE 802.1AX (al menos tres segundos).
Prioridad del sistema	**Aggregate Ethernet Interface (Interfaz de Ethernet de**	Número que determina si el cortafuegos o su peer sobrescribe el otro con respecto a las prioridades del puerto (consulte la descripción del campo **Max Ports (Puertos máx.)** que aparece a continuación).

© 2020 Palo Alto Networks, Inc.

Configuración de grupo de interfaces de agregación	Configurado en	Description (Descripción)
	agregación) > LACP (cont.)	*Cuanto más bajo sea el número, más alta sera la prioridad (intervalo 1-65.535; predeterminado 32.768).*
Puertos máx.		Número de interfaces (1-8) que pueden ser activas en cualquier momento en un grupo de agregación del LACP. El valor no puede superar el número de interfaces asignadas al grupo. Si el número de interfaces asignadas supera el número de interfaces activas, el cortafuegos utiliza las prioridades del puerto LACP de las interfaces para determinar cuáles están en modo de espera. Puede establecer prioridades de puerto LACP al configurar interfaces individuales para el grupo (consulte Interfaz Ethernet de agregación (AE)).
Habilite en el estado pasivo de HA		Para cortafuegos implementados en una configuración activa/pasiva de alta disponibilidad (HA), seleccione permitir que el cortafuegos pasivo prenegocie LACP con su peer activo antes de que ocurra una conmutación por error. La prenegociación agiliza la conmutación ya que el cortafuegos pasivo no tiene que negociar el LACP antes de volverse activo.
Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para modo activo-pasivo de HA)		Esta opción solo aplica a cortafuegos implementados en una configuración activa/pasiva de alta disponibilidad (HA); los cortafuegos en una configuración activa/pasiva requieren direcciones MAC únicas. Los peers de cortafuegos HA tienen el mismo valor de prioridad del sistema. Sin embargo, en una implementación activa/pasiva, el ID del sistema de cada uno puede ser igual o distinto, dependiendo de si asigna o no la misma dirección MAC. *Cuando los peers del LACP (también en modo de HA) se virtualizan (y aparecen para la red como un dispositivo único), usando la misma dirección MAC del sistema para los cortafuegos minimiza la latencia durante la conmutación. Cuando los peers del LACP no se virtualizan, utilizar la dirección MAC única de cada cortafuegos minimiza la latencia de la conmutación.* LACP utiliza la dirección MAC para derivar un ID de sistema a cada peer del LACP. Si el par del cortafuegos y el par de peers tienen valores de prioridad del sistema idénticos, el LACP utiliza los valores de ID del sistema para determinar qué cancela al otro con respecto a las prioridades del puerto. Si ambos cortafuegos tienen la misma dirección MAC, ambos tendrán el mismo ID del sistema, que será mayor o menor que el ID del sistema de los peers del LACP. Si los cortafuegos de HA tienen direcciones MAC únicas, es posible que uno tenga un ID del sistema mayor que los peers del LACP y el otro un ID del sistema menor. En este caso, cuando el fallo se produzca

© 2020 Palo Alto Networks, Inc.

Configuración de grupo de interfaces de agregación	Configurado en	Description (Descripción)
		en los cortafuegos, la prioridad de puerto cambia entre los peers del LACP y el cortafuegos que se activa.
Dirección MAC		Si ha activado **Use Same System MAC Address (Usar la misma dirección MAC del sistema)**, seleccione una dirección MAC generada por el sistema, o introduzca la suya propia, para ambos cortafuegos del par de alta disponibilidad activa/pasiva (HA). Debe verificar que la dirección es única globalmente.

Interfaz de Ethernet agregados (AE)

- Network > Interfaces > Ethernet

Para configurar una Interfaz Ethernet de agregación (AE), primero configure un Grupo de interfaces Ethernet de agregación (AE) y haga clic en el nombre de la interfaz que asignará al grupo. Entre las interfaces que asignó a cualquier grupo 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 (como de capa 3) deben ser los mismos. La interfaz que seleccione debe ser del mismo tipo que la definida para el grupo de interfaz AE, pero cambiará el tipo a **Aggregate Ethernet (Ethernet de agregación)** cuando configure cada interfaz. Especifique la siguiente información para cada interfaz que asigna al grupo.

Si activa el protocolo de control de agregación de enlaces (LACP) para el grupo de interfaz AE, se recomienda seleccionar la misma Link Speed (Velocidad de enlace) y Link Duplex (Dúplex de enlace) para cada interfaz del grupo. Para los valores que no coinciden, la operación de compilación muestra un aviso y PAN-OS activa el valor predeterminado de la velocidad más alta y dúplex completo.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
Nombre de interfaz	**Agregar interfaz Ethernet**	El nombre de interfaz viene predefinido y no puede cambiarlo.
Comentarios		(Opcional): introduzca una descripción para la interfaz.
Tipo de interfaz		Seleccione **Aggregate Ethernet (Agregar Ethernet)**.
Grupo de agregados		Asigne la interfaz a un grupo de agregación.
Velocidad de enlace		Seleccione la velocidad de interfaz en Mbps (**10**, **100** o **1000**) o seleccione **auto (automático)** para que el cortafuegos determine automáticamente la velocidad.

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
Dúplex de enlace		Seleccione si el modo de transmisión de la interfaz es dúplex completo (**full (completo)**), dúplex medio (**half (medio)**) o negociado automáticamente (**auto (automático)**).
estado del enlace		Seleccione si el estado de la interfaz es (**up (activada)**), (**down (desactivada)**) o determinado de forma (**auto (automática)**).
Prioridad de puerto LACP		El cortafuegos solo utiliza este campo si ha activado el Protocolo de control de agregación de grupo (LACP) para el grupo de agregación. Si el número de interfaces que asigna al grupo supera el número de interfaces activas (el campo Max Ports [Puertos máx.]), el cortafuegos utiliza las prioridades del puerto LACP de las interfaces para determinar cuáles están en modo de espera. Cuanto más bajo es el número, más alta es la prioridad (intervalo 1-65.535; predeterminado 32.768).
Enrutador virtual	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **Config (Configuración)**	Seleccione el enrutador virtual al que asigna la interfaz Ethernet de agregación.
Zona de seguridad		Seleccione la zona de seguridad a la que asigna la interfaz de Ethernet de agregación
Habilitar IPv6 en la interfaz	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6**	Seleccione esta opción para habilitar IPv6 en esta interfaz.
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 ID de interfaz como parte de host)** cuando añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.
Dirección		**Add (Añada)** una dirección IPv6 y configure los siguientes parámetros: • **Address (Dirección)**: introduzca una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear uno. • **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz. • **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6.

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)

		• **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.
		• **Send RA (Enviar RA)**: seleccione esta opción para habilitar el anuncio de enrutador (RA) de esta dirección IP. Al seleccionar esta opción, también debe **Enable Router Advertisement (Habilitar anuncio de enrutador)** de manera global en la interfaz. Si desea información sobre el RA, consulte Enable Router Advertisement.
		
		Los campos restantes solo serán visibles después de habilitar el RA:
		
		  • **Valid Lifetime (Duración válida)**: duración (en segundos) que el cortafuegos considera válida la dirección. La duración válida debe ser igual o superar la **duración preferida**. El valor predeterminado es de 2.592.000.
		  • **Preferred Lifetime (Duración preferida)**: duración (en segundos) en 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 vence la **Valid Lifetime (Duración válida)**. El valor predeterminado es 604.800.
		  • **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones IP en el prefijo publicado sin un enrutador.
		  • **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.

Habilitar detección de direcciones duplicadas	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6** > **Address Resolution (Resolución de direcciones)**	Seleccione esta opción para habilitar la detección de direcciones duplicadas (DAD), que le permite especificar el número de **Attempts (Intentos)** de **DAD**.
Intentos DAD		Especifique el número de intentos DAD en el intervalo de solicitación de vecinos (**NS Interval [Intervalo NS]**) antes de que falle el intento de identificar vecinos (el intervalo es 1-10, el predeterminado es 1).
Tiempo alcanzable		Especifique la duración (en segundos) durante la que se puede establecer comunicación con un vecino tras una consulta y una respuesta correctas (el intervalo es de 1 a 36 000 s; el valor predeterminado es de 30 s).
Intervalo NS (intervalo de solicitación de vecinos)		Especifique la duración de tiempo, en segundos, antes de que se indique un fallo de intento de detección de direcciones duplicadas (el intervalo es 1-10 segundos, el predeterminado es 1).

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
Habilitar supervisión NDP		Seleccione esta opción para habilitar la supervisión del protocolo de detección de vecinos. Cuando está habilitado, puede seleccionar el NDP (en la columna Features [Funciones]) y acceder a información como la dirección IPv6 de un vecino cuyo cortafuegos ha descubierto, la dirección MAC correspondiente y el User-ID (en el mejor de los casos).
Habilitar anuncio de enrutador	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6** > **Router Advertisement (Anuncio de enrutador)**	Seleccione esta opción para poder llevar a cabo la detección de vecinos en interfaces IPv6 y configure los otros campos de esta sección. Los clientes DNS IPv6 que reciben mensajes de anuncio de enrutador (RA, por sus siglas en inglés) utilizan esta información. El RA permite al cortafuegos actuar como una puerta de enlace predeterminada para hosts IPv6 que no estén configurados estáticamente y proporcionar al host un prefijo IPv6 que se puede utilizar para la configuración de direcciones. Puede utilizar un servidor DHCPv6 independiente junto con esta función para proporcionar DNS y otros ajustes a los clientes. Esta opción es un ajuste global de la interfaz. Si desea configurar las opciones de RA para direcciones IP individuales, seleccione **Add (Añadir)** y configure una Address en la tabla de direcciones IP. Si establece las opciones de RA para cualquier dirección IP, debe seleccionar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz.
Mín. de intervalo (segundos)		Especifique el intervalo mínimo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 3 a 1350 y el valor predeterminado, 200). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Máx. de intervalo (segundos)		Especifique el intervalo máximo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 4 a 1800 y el valor predeterminado, 600). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Límite de salto		Especifique el límite de salto que se debe aplicar a los clientes en los paquetes salientes (intervalo 1-255, predeterminado 64). Introduzca **0** si no desea ningún límite de salto.
MTU de enlace		Especifique la unidad máxima de transmisión (MTU) del enlace que se debe aplicar a los clientes. Seleccione **unspecified (no especificado)** si no desea ninguna MTU de enlace (intervalo 1.280-9.192, predeterminado no especificado).
Tiempo alcanzable (ms)		Especifique 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

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
		de tiempo alcanzable (intervalo 0-3.600.000, predeterminado no especificado).
Tiempo de retransmisión (ms)		Especifique el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente, en milisegundos, antes de retransmitir los mensajes de solicitación de vecinos. Seleccione **unspecified (no especificado)** si no desea ningún tiempo de retransmisión (intervalo 0-4.294.967.295, predeterminado no especificado).
Duración de enrutador (segundos)		Especifique la duración (en segundos) que el cliente utilizará el cortafuegos como puerta de enlace predeterminada (el intervalo es de 0 a 9000 y el valor predeterminado, 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.
Preferencia de enrutador		Si el segmento de la red tiene múltiples enrutadores de IPv6, el cliente utiliza este campo para seleccionar un enrutador preferido. Seleccione si el RA publica el enrutador del cortafuegos con prioridad **High (Alta)**, **Medium (Media)** (predeterminada) o **Low (Baja)** en relación con otros enrutadores del segmento.
Configuración gestionada		Seleccione esta opción para indicar al cliente que las direcciones están disponibles en DHCPv6.
Otras configuraciones		Seleccione esta opción para indicar al cliente que hay disponible otra información de dirección (por ejemplo, ajustes relacionados con DNS) a través de DHCPv6.
Comprobación de coherencia	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6** > **Router Advertisement (Anuncio de enrutador) (cont.)**	Seleccione esta opción si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos registra cualquier incoherencia en un log del sistema de tipo **ipv6nd**.
Incluir información DNS en anuncio de enrutador	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6** > **DNS Support**	Seleccione para que el cortafuegos envíe información de DNS en mensajes de anuncio de enrutador NDP (RA) de esta interfaz Ethernet de agregación IPv6. El resto de campos de DNS Support (Asistencia DNS) de esta tabla solo pueden verse al seleccionar esta opción.

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
Servidor	**(Asistencia DNS)**	**Add (Añadir)** una o más direcciones de servidor DNS (RDNS) recursivas para que el cortafuegos envíe anuncios de enrutador NDP desde esta interfaz Ethernet de agregación IPv6. Los servidores RDNS envían una serie de solicitudes de búsqueda de DNS a los servidores DNS raíz y servidores DNS autorizados para finalmente proporcionar una dirección IP al cliente DNS. Puede configurar hasta ocho servidores RDNS que el cortafuegos envía —en orden descendente según figuren en la lista— en un anuncio del enrutador NDP al destinatario, que luego utiliza esas direcciones en el mismo orden. Seleccione un servidor y **Move Up (Ascender)** o **Move Down (Mover hacia abajo)** para cambiar el orden de los servidores o **Delete (Eliminar)** un servidor cuando ya no lo necesite.
Duración		Introduzca el número máximo de segundos, después de que el cliente DNS IPv6 reciba el anuncio del enrutador, para que puede usar los servidores RDNS para resolver los nombres de dominio (el intervalo va del valor de Intervalo máximo (seg.) a dos veces el intervalo máximo; 1.200 es predeterminado).
Sufijo		Pulse **Add (Añadir)** para añadir uno o varios nombres de dominio (sufijos) a la lista de búsqueda DNS (DNSSL) y configúrelos. La longitud máxima del sufijo es de 255 bytes. Una lista de búsqueda de DNS es una lista de sufijos de dominio que un enrutador de cliente DNS anexa (uno a la vez) a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, utilizando de ese modo un nombre de dominio completo en la consulta DNS. Por ejemplo, si un cliente DNS trata de enviar una consulta DNS del nombre "calidad" sin sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda DNS al nombre y transmite la consulta DNS. Si el primer sufijo DNS de la lista es "empresa.com", la consulta DNS resultante del enrutador se realizará con el nombre de dominio completo "calidad.empresa.com". Si la consulta DNS falla, el enrutador agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El enrutador prueba los sufijos DNS hasta que una búsqueda de DNS sea correcta (omite 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 detección de vecinos; el cliente DNS que recibe la opción DNSSL utiliza los sufijos en sus consultas DNS no calificadas. Puede configurar un máximo de ocho nombres de dominio (sufijos) para una lista de búsqueda de DNS que el cortafuegos envía, en orden de arriba a abajo, en un anuncio del enrutador NDP al destinatario, que a su vez los usa en el mismo orden. Seleccione un sufijo y utilice las opciones **Move Up (Subir)** o **Move Down (Bajar)**

© 2020 Palo Alto Networks, Inc.

Agregar configuración de interfaz	Configurado en	Description (Descripción)
		para cambiar el orden de los sufijos, o **Delete (Eliminar)** para quitar un sufijo de la lista cuando ya no lo necesite.
Duración	**Aggregate Ethernet Interface (Interfaz de Ethernet de agregación)** > **IPv6** > **DNS Support (Asistencia DNS) (cont.)**	Introduzca el máximo de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar un nombre de dominio (sufijo) en la lista de búsqueda DNS (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).

© 2020 Palo Alto Networks, Inc.

Network > Interfaces > VLAN

Una interfaz VLAN puede proporcionar enrutamiento a una red de capa 3 (IPv4 e IPv6). Puede añadir uno o más puertos de Ethernet de capa 2 (consulte Interfaz de capa 2 de PA-7000 Series) a una interfaz VLAN.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz de VLAN**	El campo **Interface Name (Nombre de interfaz)** de solo lectura se define como **vlan**. En el campo adyacente, introduzca un sufijo numérico (de 1 a 9999) para identificar la interfaz.
Comentarios		Introduzca una descripción opcional para la interfaz.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
VLAN	**VLAN Interface (Interfaz VLAN)** > **Config (Config.)**	Seleccione una VLAN o haga clic en **VLAN** para definir una nueva (consulte Network > VLANs). Seleccione **None (Ninguna)** para eliminar la asignación de dirección actual de la interfaz.
Enrutador virtual		Asigne un enrutador virtual a la interfaz o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network > Virtual Routers). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Perfil de gestión	**VLAN Interface (Interfaz VLAN)** > **Advanced (Avanzado)** > **Other Info (Otra información)**	**Management Profile (Perfil de gestión)**: seleccione un perfil que defina los protocolos (por ejemplo, SSH, Telnet y HTTP) que puede usar para gestionar el cortafuegos en esta interfaz. Seleccione **None (Ninguna)** para eliminar la asignación de perfil actual de la interfaz.
MTU		Introduzca la unidad máxima de transmisión (maximum transmission unit, MTU) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 9.192 y el valor predeterminado, 1.500). Si las máquinas de ambos extremos del cortafuegos ejecutan un descubrimiento de MTU de ruta (PMTUD) y la interfaz recibe un paquete que supera la MTU, el cortafuegos envía al origen un

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
		mensaje de *necesidad de fragmentación del ICMP* que indica que el paquete es demasiado grande.
Ajustar TCP MSS		Seleccione esta opción para ajustar el tamaño de segmento máximo (MSS) de forma que se pueda albergar bytes de cualquier encabezado dentro del tamaño de byte MTU de la interfaz. El tamaño de byte MTU menos el tamaño de ajuste MSS es igual al tamaño de byte MSS, que varía según el protocolo de IP: • **IPv4 MSS Adjustment Size (Tamaño de ajuste IPv4 MSS)**: el intervalo es de 40 a 300; el valor predeterminado es 40. • **IPv6 MSS Adjustment Size (Tamaño de ajuste IPv6 MSS)**: el intervalo es de 60 a 300; el valor predeterminado es 60. Utilice esta configuración para tratar los casos en los que un **tunnel (túnel)** en la red necesita un MSS más pequeño. Si un paquete tiene más bytes que el MSS sin fragmentación, este parámetro permite ajustarlo. La encapsulación les añade longitud a los encabezados, por lo que es útil para configurar el tamaño de ajuste MSS para habilitar bytes para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.
Dirección IP Dirección MAC Interface (Interfaz)	**VLAN Interface (Interfaz de VLAN)** > **Advanced (Avanzado)** > **ARP Entries (Entradas de ARP)**	Para añadir una o más entradas de protocolo de resolución de direcciones (ARP) estáticas, haga clic en **Add (Añadir)** e introduzca una dirección IP y la dirección (Media Access Control o MAC) de su hardware asociado y seleccione una interfaz de capa 3 que pueda acceder a la dirección del hardware. Para eliminar una entrada, selecciónela y haga clic en **Delete (Eliminar)**. Las entradas ARP estáticas reducen el procesamiento ARP e impiden los ataques de man in the middle de las direcciones especificadas.
Dirección IPv6 Dirección MAC	**VLAN Interface (Interfaz de VLAN)** > **Advanced (Avanzado)** > **ND Entries (Entradas de ND)**	Para proporcionar información sobre vecinos para el protocolo de detección de vecinos (NDP), haga clic en **Add (Añadir)** e introduzca la dirección IPv6 y MAC del vecino.
Habilitar proxy NDP	**VLAN Interface (Interfaz de VLAN)** > **Advanced (Avanzado)** > **NDP Proxy (Proxy NDP)**	Seleccione para habilitar el proxy de protocolo de detección de vecinos (NDP) para la interfaz. El cortafuegos no responderá a los paquetes ND que solicitan direcciones MAC para direcciones IPv6 en esta lista. En la respuesta ND, el cortafuegos envía su propia dirección MAC para la interfaz y básicamente solicita todos los paquetes destinados para estas direcciones. (**Recomendado**) Habilita el proxy NDP si usa traducción de prefijo de red IPv6 (NPTv6).

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
		Si se seleccionó **Enable NDP Proxy (Habilitar proxy NDP)**, puede filtrar numerosas entradas **Address (Dirección)**: primero introduzca un filtro y luego aplíquelo (la flecha verde).
Dirección		Haga clic en **Add (Añadir)** para introducir una o más direcciones IPv6, intervalos de IP, subredes IPv6 u objetos de direcciones para las que el cortafuegos actuará como el proxy NDP. Idealmente, una de estas direcciones es la misma que la traducción de origen en NPTv6. El orden de las direcciones es indiferente. Si la dirección es una subred, el cortafuegos enviará una respuesta ND para todas las direcciones de la subred, por lo que le recomendamos que agregue también los vecinos IPv6 del cortafuegos y haga clic en **Negate (Negar)** para indicar al cortafuegos que no responda a estas direcciones IP.
Negar		Seleccione **Negate (Negar)** junto a una dirección para evitar el proxy NDP de esa dirección. Puede negar un subconjunto del intervalo de dirección IP o subred IP especificado.
Configuración	**VLAN Interface (Interfaz VLAN)** > **Advanced (Avanzado)** > **DDNS**	Seleccione Settings (Configuración) para poner los campos DDNS a disposición para la configuración.
Habilitación		Habilitar DDNS en la interfaz. Debe habilitar inicialmente DDNS para configurarlo. (Si la configuración de su DDNS no está terminada, puede guardarla sin habilitarla, para no perder los ajustes parciales).
Intervalo de actualización (días)		Introduzca el intervalo (en días) entre las actualizaciones que el cortafuegos envía al servidor DDNS para actualizar las direcciones IP asignadas a los FQDN (el intervalo es de 1 a 30; el valor predeterminado es 1). *El cortafuegos también actualiza el DDNS tras recibir una dirección IP nueva para la interfaz desde el servidor DHCP.*
Perfil del certificado		Seleccione un Perfil de certificado que haya creado (o cree uno nuevo) para verificar el servicio DDNS. El servicio DDNS presenta el cortafuegos con un certificado firmado por la autoridad de certificación (Certificate Authority, CA).
Nombre de host		Introduzca un nombre de host para la interfaz, que esté registrado con el servidor DDNS (por ejemplo, host123.domain123.com o host123). El cortafuegos no valida el nombre de host, excepto para confirmar que la sintaxis utilice caracteres válidos permitidos por DNS para un nombre de dominio.
Proveedor		Seleccione el proveedor DDNS (y el número de versión) que proporcione el servicio DDNS a esta interfaz:

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
		• **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si selecciona una versión anterior de un servicio DDNS que el cortafuegos indica que se retirará antes de cierta fecha, pase a la versión más reciente.* Los campos **Name (Nombre)** y **Value (Valor)** que siguen al nombre del proveedor son específicos del proveedor. Algunos campos son de solo lectura y le indican los parámetros que el cortafuegos utiliza para conectarse con el servicio DDNS. Configure los demás campos, como la contraseña que el servicio DDNS le proporciona y un tiempo de espera para que el cortafuegos utilice si no recibe respuesta del servidor DDNS.
Pestaña IPv4 - IP		Añada las direcciones IPv4 configuradas en la interfaz y luego selecciónelas. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Pestaña IPv6 - IPv6	**VLAN Interface (Interfaz VLAN)** > **Advanced (Avanzado)** > **DDNS**(cont.)	Añada las direcciones IPv6 configuradas en la interfaz y luego selecciónelas. Todas las direcciones IP seleccionadas se registran con el proveedor DDNS.
Mostrar información de tiempo de ejecución		Muestra el registro DDNS: Proveedor DDNS, FQDN resuelto y las direcciones IP asignadas, con un asterisco (*) que indica la dirección IP principal. Cada proveedor DDNS posee sus propios códigos de retorno para indicar el estado de la actualización del nombre de host y una fecha de retorno para fines de solución de problemas.
For an IPv4 address		
Tipo	**VLAN Interface (Interfaz VLAN)** > **IPv4**	Seleccione el método para asignar un tipo de dirección IPv4 a la interfaz: • **Static (Estática)**: debe especificar manualmente la dirección IP. • **DHCP Client (Cliente DHCP)**: permite a la interfaz actuar como cliente del protocolo de configuración de host dinámico (DHCP) y recibir una dirección IP dinámicamente asignada. *Los cortafuegos que están con una configuración de alta disponibilidad (High Availability, HA) activa/activa no admiten el cliente DHCP.* Las opciones que se muestran en la pestaña variarán según su selección de método de dirección IP.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
• Dirección IPv4 **Type (Tipo)** = **Static (Estático)**		
IP	**VLAN Interface (Interfaz VLAN)** > **IPv4**	Haga clic en **Add (Añadir)** y, a continuación, realice uno de los siguientes pasos para especificar una dirección IP y una máscara de red para la interfaz. • Escriba la entrada en la notación de enrutamiento entre dominios sin clases (CIDR): *dirección_ip/máscara* (por ejemplo, 192.168.2.0/24). • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**. • Cree un objeto **Address (Dirección)** de tipo **IP netmask (Máscara de red IP)**. Puede introducir múltiples direcciones IP para la interfaz. La base de información de reenvío (FIB) que utiliza su sistema determina el número máximo de direcciones IP. Seleccione **Delete (Borrar)** para borrar una dirección IP cuando ya no la necesite.
Dirección IPv4 **Type (Tipo)** = **DHCP**		
Habilitación	**VLAN Interface (Interfaz VLAN)** > **IPv4**	Seleccione esta opción para activar el cliente DHCP en la interfaz.
Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor		Seleccione esta opción para que se cree automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada que proporciona el servidor DHCP.
Enviar nombre de host		Configure el cortafuegos (como un cliente HCP) para que envíe el nombre de host de la interfaz (opción 12) al servidor DHCP. Si envía el nombre de host, de manera predeterminada, el nombre de host del cortafuegos será la opción en el campo de nombre de host. Puede enviar ese nombre o introducir un nombre de host personalizado (64 caracteres como máximo, incluidas letras mayúsculas y minúsculas, números, puntos, guiones y guiones bajos.
Métrica de ruta predeterminada		Para la ruta entre el cortafuegos y el servidor DHCP, introduzca de forma optativa una métrica de ruta (nivel prioritario) que se asocie a la ruta predeterminada y que se utilice para la selección de ruta (el intervalo es de 1 a 65 535; no existe ningún valor predeterminado). El nivel de prioridad aumenta conforme disminuye el valor numérico.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
Mostrar información de tiempo de ejecución de cliente DHCP		Seleccione que se muestren todos los ajustes recibidos desde el servidor DHCP, incluidos el estado de concesión de DHCP, la asignación de IP dinámica, la máscara de subred, la puerta de enlace y la configuración del servidor (DNS, NTP, dominio, WINS, NIS, POP3 y SMTP).
Para una dirección IPv6		
Habilitar IPv6 en la interfaz	**VLAN Interface (Interfaz VLAN)** > **IPv6**	Seleccione esta opción para habilitar las direcciones IPv6 en esta interfaz.
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.

Dirección	**VLAN Interface (Interfaz VLAN)** > **IPv6 (cont.)**	Haga clic en **Add (Añadir)** y configure los siguientes parámetros para cada una de las direcciones IPv6:
		• **Address (Dirección)**: introduzca una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear un objeto de dirección.
		• **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz.
		• **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6.
		• **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.
		• **Send RA (Enviar RA)**: seleccione esta opción para habilitar el anuncio de enrutador (RA) de esta dirección IP. Al seleccionar esta opción, también debe **Enable Router Advertisement (Habilitar anuncio de enrutador)** de manera global en la interfaz. Si desea información sobre el RA, consulte Enable Router Advertisement.
		Los campos restantes solo se aplican si habilita el RA.
		  • **Valid Lifetime (Duración válida)**: duración (en segundos) que el cortafuegos considera válida la dirección. La duración válida debe ser igual o superar la **duración preferida**. El valor predeterminado es de 2.592.000.
		  • **Preferred Lifetime (Duración preferida)**: duración (en segundos) en 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

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
		cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que vence la **Valid Lifetime (Duración válida)**. El valor predeterminado es 604.800. • **On-link (Enlace activo)**: seleccione esta opción si se puede establecer comunicación con los sistemas con direcciones IP en el prefijo publicado sin un enrutador. • **Autonomous (Autónomo)**: seleccione esta opción si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
Habilitar detección de direcciones duplicadas	**VLAN Interface (Interfaz de VLAN)** > **IPv6** > **Address Resolution (Resolución de dirección)**	Seleccione esta opción para habilitar la detección de direcciones duplicadas (DAD), que le permite especificar el número de **Attempts (Intentos)** de **DAD**.
Intentos DAD		Especifique el número de intentos DAD en el intervalo de solicitación de vecinos (**Neighbor Solicitation [NS] Interval**) antes de que falle el intento de identificar vecinos (el intervalo es de 1 a 10; el valor predeterminado es 1).
Tiempo alcanzable		Especifique la duración, en segundos, durante la que se puede establecer comunicación con un vecino tras una consulta y una respuesta correctas (el intervalo es de 1 a 36 000 s; el valor predeterminado es 30).
Intervalo NS (intervalo de solicitación de vecinos)		Especifique el número de segundos de intentos DAD antes de indicar el fallo (el intervalo es de 1 a 10; el valor predeterminado es 1).
Habilitar supervisión NDP		Seleccione esta opción para habilitar la supervisión del protocolo de detección de vecinos. Cuando está habilitado, puede seleccionar el NDP (en la columna Features [Funciones]) y acceder a información como la dirección IPv6 de un vecino cuyo cortafuegos ha descubierto, la dirección MAC correspondiente y el User-ID (en el mejor de los casos).
Habilitar anuncio de enrutador	**VLAN Interface (Interfaz de VLAN)** > **IPv6** > **Router Advertisement (Anuncio del enrutador)**	Seleccione esta opción para poder llevar a cabo la detección de vecinos en interfaces IPv6 y configure los otros campos de esta sección. Los clientes DNS IPv6 que reciben mensajes de anuncio de enrutador (RA, por sus siglas en inglés) utilizan esta información. El RA permite al cortafuegos actuar como una puerta de enlace predeterminada para hosts IPv6 que no estén configurados estáticamente y proporcionar al host un prefijo IPv6 que se puede utilizar para la configuración de direcciones. Puede utilizar un servidor DHCPv6 independiente junto con esta función para proporcionar DNS y otros ajustes a los clientes.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
		Esta opción es un ajuste global de la interfaz. Si desea configurar las opciones de RA para direcciones IP individuales, seleccione **Add (Añadir)** para añadir una dirección (Address) en la tabla de direcciones IP y configurarla. Si establece las opciones de RA para cualquier dirección IP, debe seleccionar la opción **Enable Router Advertisement (Habilitar anuncio de enrutador)** para la interfaz.
Mín. de intervalo (segundos)		Especifique el intervalo mínimo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 3 a 1350; el valor predeterminado es 200). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Máx. de intervalo (segundos)		Especifique el intervalo máximo, en segundos, entre los RA que el cortafuegos enviará (el intervalo es de 4 a 1800; el valor predeterminado es 600). El cortafuegos enviará los RA en intervalos aleatorios entre los valores mínimo y máximo que configure.
Límite de salto		Especifique el 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.
MTU de enlace		Especifique la unidad máxima de transmisión (MTU) del enlace que se debe aplicar a los clientes. Seleccione **unspecified (no especificado)** si no desea ninguna MTU de enlace (intervalo es de 1280 a 9192; el valor predeterminado es no especificado).
Tiempo alcanzable (ms)		Especifique 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 no especificado).
Tiempo de retransmisión (ms)		Especifique el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente (en milisegundos) antes de retransmitir los mensajes de solicitación 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 no especificado).
Duración de enrutador (segundos)		Especifique la duración, en segundos, por la que 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.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
Preferencia de enrutador		Si el segmento de la red tiene múltiples enrutadores de IPv6, el cliente utiliza este campo para seleccionar un enrutador preferido. Seleccione si el RA publica el enrutador del cortafuegos con prioridad **High (Alta)**, **Medium (Media)** (predeterminada) o **Low (Baja)** en relación con otros enrutadores del segmento.
Configuración gestionada		Seleccione esta opción para indicar al cliente que las direcciones están disponibles en DHCPv6.
Otras configuraciones		Seleccione esta opción para indicar al cliente que hay disponible otra información de dirección (por ejemplo, configuración relacionada con DNS) en DHCPv6.
Comprobación de coherencia	**VLAN Interface (Interfaz VLAN)** > **IPv6** > **Router Advertisement (Anuncio de enrutador) (cont.)**	Seleccione esta opción si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos registra cualquier incoherencia en un log del sistema de tipo **ipv6nd**.
Incluir información DNS en anuncio de enrutador	**VLAN Interface (Interfaz VLAN)** > **IPv6** > **DNS Support (Asistencia DNS)**	Seleccione esta opción para que el cortafuegos incluya información de DNS en los anuncios del enrutador NDP de esta interfaz de VLAN IPv6. El resto de campos de DNS Support (Asistencia DNS) de esta tabla solo pueden verse al seleccionar esta opción.
Servidor		Haga clic en **Add (Añadir)** para añadir una o más direcciones recursivas de servidor DNS (RDNS) a fin de que el cortafuegos envíe anuncios de enrutador NDP desde esta interfaz VLAN IPv6. Los servidores RDNS envían una serie de solicitudes de búsqueda de DNS a los servidores DNS raíz y servidores DNS autorizados para finalmente proporcionar una dirección IP al cliente DNS. Puede configurar hasta ocho servidores RDNS que el cortafuegos envía —en orden descendente según figuren en la lista— en un anuncio del enrutador NDP al destinatario, que luego los utiliza en el mismo orden. Seleccione un servidor y utilice las opciones **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar el orden de los servidores, o **Delete (Eliminar)** para quitar un servidor de la lista cuando ya no lo necesite.
Duración		Introduzca el máximo de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar los servidores RDNS para resolver nombres de dominio (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz VLAN	Configurado en	Description (Descripción)
Sufijo		Pulse **Add (Añadir)** para añadir uno o varios nombres de dominio (sufijos) a la lista de búsqueda DNS (DNSSL) y configúrelos. La longitud máxima del sufijo es de 255 bytes. Una lista de búsqueda de DNS es una lista de sufijos de dominio que un enrutador de cliente DNS anexa (uno a la vez) a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, utilizando de ese modo un nombre de dominio completo en la consulta DNS. Por ejemplo, si un cliente DNS trata de enviar una consulta DNS del nombre "calidad" sin sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda DNS al nombre y transmite la consulta DNS. Si el primer sufijo DNS de la lista es "empresa.com", la consulta DNS resultante del enrutador se realizará con el nombre de dominio completo "calidad.empresa.com". Si la consulta DNS falla, el enrutador agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El enrutador prueba los sufijos DNS hasta que una búsqueda de DNS sea correcta (omite 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 detección de vecinos; el cliente DNS que recibe la opción DNSSL utiliza los sufijos en sus consultas DNS no calificadas. Puede configurar hasta ocho nombres de dominio (sufijos) para una lista de búsqueda de DNS que el cortafuegos envía —en orden descendente según figuren en la lista— en un anuncio del enrutador NDP al destinatario, que luego utiliza dichas direcciones en el mismo orden. Seleccione un sufijo y utilice las opciones **Move Up (Subir)** o **Move Down (Bajar)** para cambiar el orden de los sufijos, o **Delete (Eliminar)** para quitar un sufijo de la lista cuando ya no lo necesite.
Duración		Introduzca el máximo de segundos desde que el cliente DNS IPv6 recibe el anuncio del enrutador hasta que puede utilizar un nombre de dominio (sufijo) en la lista de búsqueda DNS (el intervalo es el valor de Max Interval [sec] hasta el doble del intervalo máximo; el valor predeterminado es 1200).

© 2020 Palo Alto Networks, Inc.

Network > Interfaces > Loopback

Utilice los siguientes campos para configurar las interfaces de bucle invertido:

Configuración de interfaz de bucle invertido	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz de bucle invertido**	El campo **Interface Name (Nombre de interfaz)** de solo lectura se define como **loopback**. En el campo adyacente, escriba un sufijo numérico (1-9999) para identificar la interfaz.
Comentarios		Introduzca una descripción opcional para la interfaz.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
Enrutador virtual	**Loopback Interface (Interfaz de bucle invertido) > Config (Configuración)**	Asigne un enrutador virtual a la interfaz o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network > Virtual Routers). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Perfil de gestión	**Tunnel Interface (Interfaz de túnel) > Advanced (Avanzado) > Other Info (Otra información)**	**Management Profile (Perfil de gestión)**: seleccione un perfil que defina los protocolos (por ejemplo, SSH, Telnet y HTTP) que puede usar para gestionar el cortafuegos en esta interfaz. Seleccione **None (Ninguna)** para eliminar la asignación de perfil actual de la interfaz.
MTU		Introduzca la unidad máxima de transmisión (MTU) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 9.192; el valor predeterminado es 1.500). Si las máquinas de ambos extremos del cortafuegos ejecutan un descubrimiento de MTU de ruta (PMTUD) y la interfaz recibe un paquete que supera la MTU, el cortafuegos envía al origen un mensaje de *necesidad de fragmentación del ICMP* que indica que el paquete es demasiado grande.
Ajustar TCP MSS		Seleccione esta opción para ajustar el tamaño de segmento máximo (MSS) de forma que se pueda albergar bytes de cualquier encabezado dentro del tamaño de byte MTU de la interfaz. El

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de bucle invertido	Configurado en	Description (Descripción)
		tamaño de byte MTU menos el tamaño de ajuste MSS es igual al tamaño de byte MSS, que varía según el protocolo de IP: • **IPv4 MSS Adjustment Size (Tamaño de ajuste IPv6 MSS)**: el rango es 40-300; la opción predeterminada es 40. • **IPv6 MSS Adjustment Size (Tamaño de ajuste IPv6 MSS)**: el rango es 60-300; la opción predeterminada es 60. Utilice esta configuración para tratar los casos en los que un **tunnel (túnel)** en la red necesita un MSS más pequeño. Si un paquete tiene más bytes que el MSS sin fragmentación, este parámetro permite ajustarlo. La encapsulación les añade longitud a los encabezados, por lo que es útil para configurar el tamaño de ajuste MSS para habilitar bytes para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.
For an IPv4 address		
IP	**Loopback Interface (Interfaz de bucle invertido)** > **IPv4**	Haga clic en **Add (Añadir)** y, a continuación, realice uno de los siguientes pasos para especificar una dirección IP y una máscara de red para la interfaz. • Especifique una dirección IPv4 con una máscara de subred de /32; por ejemplo, 192.168.2.1/32. Solo se admite una máscara de subred /32. • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**. • Haga clic en **Address (Dirección)** para crear un objeto de dirección de tipo **IP netmask (Máscara de red IP)**. Puede introducir múltiples direcciones IP para la interfaz. La base de información de reenvío (FIB) que utiliza su sistema determina el número máximo de direcciones IP. Para eliminar una dirección IP, seleccione la dirección y haga clic en **Delete (Eliminar)**.
Para una dirección IPv6		
Habilitar IPv6 en la interfaz	**Loopback Interface (Interfaz de bucle invertido)** > **IPv6**	Seleccione esta opción para habilitar las direcciones IPv6 en esta interfaz.
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.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de bucle invertido	Configurado en	Description (Descripción)
Dirección		Haga clic en **Add (Añadir)** y configure los siguientes parámetros para cada una de las direcciones IPv6: • **Address (Dirección)**: introduzca una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear un objeto de dirección. • **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz. • **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6. • **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.

© 2020 Palo Alto Networks, Inc.

Network > Interfaces > Tunnel

Utilice los siguientes campos para configurar una interfaz de túnel:

Configuración de interfaz de túnel	Configurado en	Description (Descripción)
Nombre de interfaz	**Interfaz túnel**	El campo **Interface Name (Nombre de interfaz)** de solo lectura se define como **tunnel**. En el campo adyacente, escriba un sufijo numérico (1-9.999) para identificar la interfaz.
Comentarios		Introduzca una descripción opcional para la interfaz.
Perfil de NetFlow		Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o haga clic en **Netflow Profile (Perfil de NetFlow)** para definir un nuevo perfil (consulte Device > Server Profiles > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
Enrutador virtual	**Tunnel Interface (Interfaz de túnel)** > **Config (Config.)**	Asigne un enrutador virtual a la interfaz o haga clic en **Virtual Router (Enrutador virtual)** para definir uno nuevo (consulte Network > Virtual Routers). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual		Si el cortafuegos admite múltiples sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o haga clic en **Virtual System (Sistema virtual)** para definir un nuevo vsys.
Zona de seguridad		Seleccione una zona de seguridad para la interfaz o haga clic en **Zone (Zona)** para definir una nueva zona. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz.
Perfil de gestión	**Tunnel Interface (Interfaz de túnel)** > **Advanced (Avanzado)** > **Other Info (Otra información)**	**Management Profile (Perfil de gestión)**: seleccione un perfil que defina los protocolos (por ejemplo, SSH, Telnet y HTTP) que puede usar para gestionar el cortafuegos en esta interfaz. Seleccione **None (Ninguna)** para eliminar la asignación de perfil actual de la interfaz.
MTU		Introduzca la unidad máxima de transmisión (MTU) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 9192; el valor predeterminado es 1500). Si las máquinas de ambos extremos del cortafuegos ejecutan un descubrimiento de MTU de ruta (PMTUD) y la interfaz recibe un paquete que supera la MTU, el cortafuegos envía al origen un mensaje de *necesidad de fragmentación del ICMP* que indica que el paquete es demasiado grande.
For an IPv4 address		

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz de túnel	Configurado en	Description (Descripción)
IP	**Tunnel Interface (Interfaz de túnel)** > **IPv4**	Haga clic en **Add (Añadir)** y, a continuación, realice uno de los siguientes pasos para especificar una dirección IP y una máscara de red para la interfaz. • Escriba la entrada en la notación de enrutamiento entre dominios sin clases (CIDR): dirección_ip / máscara (por ejemplo, 192.168.2.0/24). • Seleccione un objeto de dirección existente de tipo **IP netmask (Máscara de red IP)**. • Haga clic en **Address (Dirección)** para crear un objeto de dirección de tipo **IP netmask (Máscara de red IP)**. Puede introducir múltiples direcciones IP para la interfaz. La base de información de reenvío (FIB) que utiliza su sistema determina el número máximo de direcciones IP. Para eliminar una dirección IP, seleccione la dirección y haga clic en **Delete (Eliminar)**.
Para una dirección IPv6		
Habilitar IPv6 en la interfaz	**Tunnel Interface (Interfaz de túnel)** > **IPv6**	Seleccione esta opción para habilitar las direcciones IPv6 en esta interfaz.
ID de interfaz	**Tunnel Interface (Interfaz de túnel)** > **IPv6**	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.
Dirección		Haga clic en **Add (Añadir)** y configure los siguientes parámetros para cada una de las direcciones IPv6: • **Address (Dirección)**: introduzca una dirección IPv6 y la longitud del prefijo (p. ej., 2001:400:f00::1/64). También puede seleccionar un objeto de dirección IPv6 existente o hacer clic en **Address (Dirección)** para crear un objeto de dirección. • **Enable address on interface (Habilitar dirección en interfaz)**: seleccione esta opción para habilitar la dirección IPv6 en la interfaz. • **Use interface ID as host portion (Usar ID de interfaz como parte de host)**: seleccione esta opción para utilizar el **Interface ID (ID de interfaz)** como parte de host de la dirección IPv6. • **Anycast (Difusión por proximidad)**: seleccione esta opción para incluir el enrutador mediante el nodo más cercano.

© 2020 Palo Alto Networks, Inc.

Network (Red) > Interfaces (Interfaces) > SD-WAN

Cree una interfaz de SD-WAN virtual y añada uno o más miembros de la interfaz Ethernet física que vayan al mismo destino.

Configuración de interfaz VLAN	
Nombre de interfaz	El campo **Nombre de interfaz** de solo lectura se define como **sdwan**. En el campo adyacente, introduzca un sufijo numérico (de 1 a 9999) para identificar la interfaz SD-WAN virtual.
Comentarios	Especifique una descripción fácil de usar para la interfaz, como **`a Internet`** o **`(a la central del Oeste de EEUU.`**. Sus comentarios facilitarán la identificación de interfaces en lugar de intentar descifrar nombres generados automáticamente en registros e informes.
Perfil de NetFlow	Si quiere exportar el tráfico IP unidireccional que atraviesa una interfaz de entrada a un servidor NetFlow, seleccione el perfil de servidor o defina un nuevo **perfil de NetFlow** (consulte Dispositivo > Perfiles de servidor > NetFlow). Seleccione **None (ninguno)** para eliminar la asignación actual del servidor NetFlow de la interfaz.
Pestaña Configuración	
Enrutador virtual	Asigne un enrutador virtual a la interfaz o defina un nuevo **enrutador virtual** (consulte Red > Enrutadores virtuales). Si selecciona **None (Ninguna)**, se elimina la asignación del enrutador virtual actual de la interfaz.
Sistema virtual	Si el cortafuegos admite varios sistemas virtuales y la capacidad se ha habilitado, seleccione un sistema virtual (vsys) para la interfaz o defina un nuevo **sistema virtual**.
Zona de seguridad	Seleccione una zona de seguridad para la interfaz o defina una nueva **zona**. Seleccione **None (Ninguna)** para eliminar la asignación de zona actual de la interfaz. La interfaz virtual de SD-WAN y todos sus miembros de interfaz deben estar en la misma zona de seguridad. De esa forma, se asegura de se apliquen las mismas reglas de la política de seguridad a todas las rutas desde la sucursal hasta el mismo destino.
Pestaña Avanzada	
Interfaces	Seleccione las interfaces Ethernet de capa 3 (para acceso directo a Internet (DIA)) o las interfaces de túnel VPN virtuales (para la central) que constituyen esta interfaz de SD-WAN virtual. El enrutador virtual del cortafuegos utiliza esta interfaz de SD-WAN virtual para enrutar el tráfico de SD-WAN a una ubicación de la central o DIA. Las interfaces pueden tener diferentes etiquetas. Sin embargo, si especifica más de una interfaz, todas deben ser del mismo tipo (túnel VPN o DIA).

© 2020 Palo Alto Networks, Inc.

Network > Zones

Los siguientes apartados describen las zonas de seguridad de la red:

¿Qué está buscando?	Consulte:
¿Cuál es el objetivo de una zona de seguridad?	Descripción general de zona de seguridad
¿Qué campos están disponibles para configurar zonas de seguridad?	Componentes de las zonas de seguridad
¿Busca más información?	Segmentar su red con interfaces y zonas

Descripción general de zona de seguridad

Las zonas de seguridad son una forma lógica de agrupar interfaces físicas y virtuales en el cortafuegos para poder controlar y registrar el tráfico que atraviesa interfaces específicas en su red. Una interfaz en el cortafuegos debe estar asignada a una zona de seguridad antes de que la interfaz pueda procesar tráfico. Una zona puede tener múltiples interfaces del mismo tipo asignadas (por ejemplo, interfaces de tap, capa 2 o capa 3), pero una interfaz solo puede pertenecer a una zona.

Las reglas de política en el cortafuegos usan zonas de seguridad para identificar de dónde proviene el tráfico y hacia dónde va. El tráfico puede circular libremente dentro de una zona, pero no puede circular entre diferentes zonas hasta que defina una regla de política de seguridad que lo permita. Para permitir o denegar el tráfico entre zonas, las reglas de política de seguridad deben hacer referencia a una zona de origen y de destino (no a interfaces) y las zonas deben ser del mismo tipo. Es decir, una regla de política de seguridad puede permitir o denegar el tráfico de una zona de capa 2 solo a otra zona de capa 2.

Componentes de las zonas de seguridad

Para definir una zona de seguridad, haga clic en **Add (Añadir)** y especifique la siguiente información:

Configuración de zona de seguridad	Description (Descripción)
Nombre	Introduzca un nombre de una zona (hasta 31 caracteres). Este nombre aparece en la lista de zonas cuando se definen políticas de seguridad y se configuran interfaces. El nombre distingue entre mayúsculas y minúsculas y debe ser exclusivo dentro del enrutador virtual. Utilice solamente letras, números, espacios, puntos, guiones y guiones bajos.
Ubicación	Este campo solo aparece si el cortafuegos admite varios sistemas virtuales (vsys) y esa función está activada. Seleccione los vsys a los cuales se aplica esta zona.

© 2020 Palo Alto Networks, Inc.

Configuración de zona de seguridad	Description (Descripción)
Tipo	Seleccione un tipo de zona (**Tap**, **Virtual Wire**, **Layer2**, **Layer3**, **External (Externa)** o **Tunnel (Túnel)**) para ver todas las **Interfaces** de ese tipo que no tengan una zona asignada. Los tipos de zona de capa 2 y capa 3 enumeran todas las interfaces y subinterfaces Ethernet de ese tipo. Haga clic en **Add (Añadir)** para añadir las interfaces que desea asignar a la zona. La zona externa se utiliza para controlar el tráfico entre los múltiples sistemas virtuales en un único cortafuegos. Solo se muestra en los cortafuegos que admiten múltiples sistemas virtuales y solo si **Multi Virtual System Capability (Capacidad para múltiples sistemas virtuales)** está habilitada. Para obtener información sobre las zonas externas, consulte Tráfico inter-VSYS que permanece dentro del cortafuegos. Una interfaz puede pertenecer a solo una zona en un sistema virtual.
Interfaces	Añada una o más interfaces a esta zona.
Perfiles de protección de zonas	Seleccione un perfil que especifica cómo el cortafuegos responderá a ataques desde esta zona. Para crear un nuevo perfil, consulte Network > Network Profiles > Zone Protection. Se recomienda proteger cada zona con el perfil de protección de zonas.
Habilitar protección de búfer de paquetes	Configure la protección de búfer de paquetes (Device [Dispositivo] > Setup [Configuración] > Session [Sesión]) a nivel global y aplíquela a cada zona. El cortafuegos aplica la protección de búfer de paquetes únicamente a la zona de entrada. Si bien la protección del búfer de paquetes está deshabilitada de manera predeterminada, se recomienda habilitarla en cada zona para proteger los búferes del cortafuegos.
Ajuste de log	Seleccione un perfil de reenvío de logs para reenviar logs de protección de zona a un sistema externo. Si tiene un perfil de Reenvío de logs denominado predeterminado, este se seleccionará automáticamente para esta lista desplegable cuando defina una nueva zona de seguridad. Puede cancelar esta configuración predeterminada en cualquier momento seleccionado un perfil de reenvío de logs diferente cuando establezca una nueva zona de seguridad. Para definir o añadir un nuevo perfil de Reenvío de logs (y para denominar a un perfil predeterminado de forma que la lista desplegable se rellene automáticamente), haga clic en **New (Nuevo)** (consulte Objects > Log Forwarding). *Si está configurando la zona en una plantilla Panorama, las listas desplegablesLog Setting (Configuración del registro) solo comparten perfiles de Reenvío de registros; para especificar un perfil no compartido, debe escribir el nombre.*
Habilitar identificación de usuarios	Si ha configurado User-ID™ para realizar una asignación de dirección IP a nombre de usuario (detección), se recomienda **habilitar la identificación de usuarios** para aplicar la información de asignación al tráfico en esta zona.

© 2020 Palo Alto Networks, Inc.

Configuración de zona de seguridad	Description (Descripción)
	Si deshabilita esta opción, los logs de cortafuegos, informes y políticas excluirán la información de asignación de usuario del tráfico de la zona. Por defecto, si selecciona esta opción, el cortafuegos aplica información de asignación de usuario al tráfico de todas las subredes de la zona. Para limitar la información a subredes específicas de la zona, use la **Include List (Lista de permitidos)** y la **Exclude List (Lista de excluidos)**. *Habilite User-ID solo en zonas de confianza. Si habilita User-ID y sondeo de clientes en una zona no fiable externa (como Internet), las sondas podrían enviarse fuera de su red protegida, lo que resulta en una divulgación de información del nombre de cuenta de servicio del agente User-ID, nombre de dominio y hash de contraseña cifrado, lo que podría permitir a un atacante obtener acceso no autorizado a recursos protegidos.* *User-ID realiza una detección de la zona solo si cae dentro del intervalo de red que supervisa el ID de usuario. Si la zona está fuera del intervalo, el cortafuegos no aplicará la información de asignación de usuario al tráfico de la zona aunque seleccione Enable User Identification (Habilitar identificación de usuarios). Para obtener más información, consulte* Incluir o excluir subredes para la asignación de usuarios*.*
Lista de inclusión ACL de identificación de usuarios	Por defecto, si no especifica las subredes en esta lista, el cortafuegos aplica la información de asignación de usuario que detecte a todo el tráfico de la zona para usarla en logs, informes y políticas. Para limitar la aplicación de información de asignación de usuario a subredes específicas en la zona después, para cada subred, haga clic en **Add (Añadir)** y seleccione un objeto de dirección (o grupo de direcciones) o escriba el intervalo de direcciones IP (por ejemplo, 10.1.1.1/24). La exclusión de todas las demás subredes está implícita, ya que **Include List (Lista de permitidos)** es una lista de inclusión, por lo que no necesita añadirlas a la **Exclude List (Lista de excluidos)**. Añada entradas a la **Exclude List (Lista de excluidos)** únicamente para excluir información de asignación de usuario para un subconjunto de redes en la **Lista de permitidos**. Por ejemplo, si añade 10.0.0.0/8 a la **Include List (Lista de permitidos)** y 10.2.50.0/22 a la **Exclude List (Lista de excluidos)**, el cortafuegos incluirá la información de asignación de usuario a todas las subredes de zona de 10.0.0.0/8 excepto 10.2.50.0/22, y excluye información de todas las subredes de zona fuera de 10.0.0.0/8. *Solo puede incluir subredes que caigan dentro del intervalo de red que supervise el User-ID. Para obtener más información, consulte* Incluir o excluir subredes para la asignación de usuarios*.*

© 2020 Palo Alto Networks, Inc.

Configuración de zona de seguridad	Description (Descripción)
Lista de exclusión ACL de identificación de usuarios	Para excluir la información de asignación de usuario para un subconjunto de subredes en la **Include List (Lista de permitidos)**, haga clic en **Add (Añadir)** y seleccione un objeto de dirección (o grupo de direcciones) o escriba el intervalo de direcciones IP para cada subred que va a excluir. *Si añade entradas a la Exclude List (Lista de excluidos) pero no la Include List (Lista de permitidos), el cortafuegos excluye la información de asignación de usuarios para todas las subredes de la zona, no solo las subredes que ha añadido.*

© 2020 Palo Alto Networks, Inc.

Network > VLANs

El cortafuegos admite redes VLAN que cumplan la normativa IEEE 802.1Q estándar. Cada una de las interfaces de capa 2 definidas en el cortafuegos debe tener una red VLAN asociada. La misma VLAN se puede asignar a varias interfaces de capa 2, pero cada interfaz solo puede pertenecer a una VLAN.

Configuración de VLAN	Description (Descripción)
Nombre	Introduzca un nombre de VLAN (de hasta 31 caracteres). Este nombre aparece en la lista de redes VLAN cuando se configuran interfaces. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Interfaz de VLAN	Seleccione una Red > Interfaces > VLAN para permitir enrutar el tráfico fuera de la VLAN.
Interfaces	Especifique interfaces del cortafuegos para VLAN.
Configuración de MAC estática	Especifique la interfaz mediante la que una dirección MAC es alcanzable. Sustituye a todas las asignaciones obtenidas de interfaz a MAC.

© 2020 Palo Alto Networks, Inc.

Network > Virtual Wires

Seleccione **Network (Red)** > **Virtual Wires (Cables virtuales)** para definir cables virtuales después de especificar dos interfaces de cable virtual en el cortafuegos (Network [Red] > Interfaces [Interfaces]).

Configuración de cable virtual	Description (Descripción)
Nombre de cable virtual	Introduzca un nombre para el cable virtual (Virtual Wire) (de hasta **31** caracteres). Este nombre aparece en la lista de cables virtuales cuando se configuran interfaces. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Interfaces	Seleccione dos interfaces Ethernet de la lista de configuración de cable virtual. Las interfaces aparecen en esta lista si tienen el tipo de interfaz de cable virtual y no se han asignado a otro cable virtual. Si desea más información sobre cómo configurar esta interfaz, consulte Interfaces de cable virtual.
Tags permitidos	Introduzca el número de etiqueta (0 a 4094) o el intervalo de números de etiqueta (tag1-tag2) del tráfico permitido en el cable virtual. Un valor de etiqueta 0 (predeterminado) indica tráfico sin etiquetar. Si especifica varias etiquetas o intervalos, deben estar separados por comas. El tráfico que se excluye del valor de la etiqueta se descarta. *Los valores de etiqueta no se cambian en los paquetes de entrada o de salida.* Si utiliza subinterfaces de cable virtual, la lista **Tag Allowed (Etiquetas permitidas)** causará que todo el tráfico con las etiquetas de la lista se clasifique en el cable virtual principal. Las subinterfaces de cable virtual deben utilizar etiquetas que no existen en la lista principal **Tags Allowed (Etiquetas permitidas)**.
Cortafuegos de multidifusión	Seleccione esta opción si desea poder aplicar reglas de seguridad al tráfico de multidifusión. Si este ajuste no está activado, el tráfico de multidifusión se reenvía por el cable virtual.
Envío del estado del enlace	Seleccione esta opción si desea desactivar la otra interfaz en un cable virtual cuando se detecta un estado de enlace no operativo. Si no selecciona o deshabilita esta opción, el estado del enlace no se propaga por el cable virtual.

© 2020 Palo Alto Networks, Inc.

Network > Virtual Routers

El cortafuegos requiere enrutadores virtuales para obtener rutas a otras subredes utilizando rutas estáticas que define de forma manual o mediante la participación en protocolos de enrutamiento de Capa 3 (rutas dinámicas). Todas las interfaces de capa 3, de bucle invertido y VLAN definidas en el cortafuegos se deben asociar con un enrutador virtual. Cada interfaz solo puede pertenecer a un único enrutador virtual.

Definir un enrutador virtual requiere una configuración general y cualquier combinación de protocolos de rutas estáticas o enrutamiento dinámico, como lo requiere su red. También puede configurar otras funciones como redistribución de rutas y ECMP.

¿Qué está buscando?	Consulte
¿Cuáles son los elementos requeridos de un enrutador virtual?	Ajustes generales de un enrutador virtual
Configurar:	Rutas estáticas Redistribución de ruta RIP OSPF OSPFv3 BGP IP de multidifusión ECMP
Consulte información sobre un enrutador virtual.	Más estadísticas de tiempo de ejecución para un enrutador virtual
¿Busca más información?	Networking

Ajustes generales de un enrutador virtual

- Network > Virtual Routers > Router Settings > General

Todos los enrutadores virtuales exigen que añada interfaces de Capa 3 y cifras de distancia administrativa según se describe en la siguiente tabla.

Configuración general del enrutador virtual.	Description (Descripción)
Nombre	Especifique un nombre para identificar el enrutador virtual (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Configuración general del enrutador virtual.	Description (Descripción)
Interfaces	Seleccione las interfaces que desea incluir en el enrutador virtual. Por lo tanto, pueden utilizarse como interfaces de salida en el enrutador virtual de la tabla de enrutamiento. Para especificar el tipo de interfaz, consulte Network > Interfaces. Cuando añade una interfaz, sus rutas conectadas se añaden automáticamente.
Distancias administrativas	Especifique las siguientes distancias administrativas: • **Static routes (Rutas estáticas)**: intervalo 10-240; predeterminado 10. • **OSPF Int**: intervalo 10-240; predeterminado 30. • **OSPF Ext**: intervalo 10-240; predeterminado 110. • **IBGP**: intervalo 10-240; predeterminado 200. • **EBGP**: intervalo 10-240; predeterminado 20. • **RIP**: intervalo 10-240; predeterminado 120.

Rutas estáticas

- Network > Virtual Routers > Static Routes

Opcionalmente puede introducir una o más rutas estáticas. Haga clic en la pestaña **IP** o **IPv6** para especificar la ruta mediante direcciones IPv4 o IPv6. Aquí suele ser necesario configurar las rutas predefinidas (0.0.0.0/0). Las rutas predefinidas se aplican a destinos que de otro modo no se encontrarían en la tabla de enrutamiento del enrutador virtual.

Configuración de ruta estática	Description (Descripción)
Nombre	Introduzca un nombre para identificar la ruta estática (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
IP Destino	Introduzca una dirección IP y una máscara de red en la notación de enrutamiento entre dominios sin clases (CIDR): *dirección_ip/máscara* (por ejemplo, 192.168.2.0/24 para IPv4 o 2001:db8::/32 para IPv6). O bien, puede crear un objeto de dirección de tipo máscara de red IP.
Interface (Interfaz)	Seleccione la interfaz para reenviar paquetes al destino o configure el siguiente salto, o ambos.
siguiente salto	Seleccione una de las siguientes opciones: • **IP Address (Dirección IP)**: seleccione esta opción para introducir una dirección IP de enrutador de próximo salto o seleccione o cree un objeto de dirección de tipo máscara de red IP. El objeto de dirección debe tener una máscara de red de /32 para IPv4 o /128 para IPv6.

© 2020 Palo Alto Networks, Inc.

Configuración de ruta estática	Description (Descripción)
	• **Next VR (Siguiente VR)**: seleccione para elegir un enrutador virtual en el cortafuegos como el siguiente salto. Esta opción permite configurar rutas internamente entre enrutadores virtuales en un único cortafuegos. • **FQDN**: seleccione esta opción para identificar el próximo salto mediante un FQDN. Luego seleccione un objeto de dirección de tipo FQDN o cree un nuevo objeto de dirección de tipo FQDN. • **Discard (Descartar)**: Seleccione esta opción si desea descartare l tráfico que se dirige a este destino. • **None (Ninguno)**: seleccione esta opción si no existe el siguiente salto en la ruta.
Distancia administrativa	Especifique la distancia administrativa de la ruta estática (10-240; opción predefinida 10).
Métrica	Especifique una medida para la ruta estática (1 - 65535).
Tabla de enrutamiento	Seleccione la tabla de rutas en la que el cortafuegos instala la ruta estática: • **Unicast (Unidifusión)**: instala la ruta en la tabla de rutas unidifusión • **Multicast (Multidifusión)**: instala la ruta en la tabla de rutas de multidifusión. • **Both (Ambas)**: instala la ruta en las tablas de rutas tanto unidifusión como multidifusión. • **No Install (No instalar)**: no instala la ruta en la tabla de rutas (RIB); el cortafuegos conserva la ruta estática para referencia futura hasta que elimine la ruta.
Perfil BFD	Para habilitar la detección de reenvío bidireccional (BFD) para una ruta estática en un cortafuegos PA-3200 Series, PA-5200 Series, PA-7000 Series o VM-Series, seleccione una de las siguientes opciones: • **default (predeterminada)** (configuración BFD predeterminada) • un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. Seleccione **None (Disable BFD) [Ninguno (deshabilitar BFD)]** para deshabilitar BFD para la ruta estática. Para utilizar BFD en una ruta estática: • el cortafuegos y el peer en el otro extremo de la ruta estática deben admitir las sesiones BFD. • La ruta estática del tipo **Next Hop (Siguiente salto)** debe ser **IP Address (Dirección de IP)** y debe ingresar una dirección de IP válida. • El ajuste de **Interfaz (Interface)** no puede ser **None (Ninguna)**; debe seleccionar una interfaz (incluso si utiliza una dirección DHCP).
Monitorización de rutas	Seleccione esta opción para habilitar la supervisión de la ruta estática.
Condición de fallo	Seleccione la condición bajo la cual el cortafuegos considerará la ruta supervisada hacia abajo y, por lo tanto, la ruta estática hacia abajo:

© 2020 Palo Alto Networks, Inc.

Configuración de ruta estática	Description (Descripción)
	• **Any (Alguna)**: Si uno de los destinos supervisados para la ruta estática es inaccesible por ICMP, el cortafuegos eliminará la ruta estática del RIB y FIB y agregará la ruta dinámica o estática que tenga la siguiente métrica más baja que vaya al mismo destino al FIB. • **All (Todas)**: si todos los destinos supervisados para la ruta estática son inaccesibles por ICMP, el cortafuegos elimina la ruta estática de la RIB y FIB y agrega la ruta dinámica o estática que tenga la siguiente métrica más baja y vaya al mismo destino a la FIB. Seleccionar **All (Todas)** para evitar la posibilidad de que un solo destino supervisado designe un fallo de ruta estática cuando, por ejemplo, ese destino supervisado esté simplemente fuera de línea para el mantenimiento.
Tiempo de espera preemptive (min)	Introduzca el número de minutos que un supervisor de ruta de acceso descendido debe permanecer en el estado Up (Activado): el supervisor de ruta evalúa todos sus destinos supervisados por miembros y debe permanecer en Up antes de que el cortafuegos reinstale la ruta estática en el RIB. Si el temporizador caduca sin que el enlace se desactive o fluctúe, el enlace se considera estable, el supervisor de ruta puede permanecer activo y el cortafuegos puede agregar la ruta estática de nuevo al RIB. Si el enlace se desactiva o fluctúa durante el tiempo de espera, el supervisor de ruta fallará y el temporizador se reiniciará cuando el monitor desactivado regrese al estado activado. Un **Preemptive Hold Time (Tiempo de retención preventiva)** de cero hace que el cortafuegos vuelva a instalar la ruta estática en el RIB inmediatamente después de que el monitor de trayecto se active. El intervalo es 0-1.440; el valor por defecto es 2.
Nombre	Introduzca un nombre para el destino supervisado (de hasta 31 caracteres).
Habilitación	Seleccione esta opción para habilitar la supervisión de rutas de este destino específico para la ruta estática; el cortafuegos enviará pings ICMP a este destino.
IP de origen	Seleccione la dirección IP que el cortafuegos utilizará como origen en el ping ICMP al destino supervisado: • 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.
IP de destino	Introduzca una dirección IP sólida y estable o un objeto de dirección para el que el cortafuegos supervisará la ruta. El destino supervisado y el destino de la ruta estática deben utilizar la misma familia de direcciones (IPv4 o IPv6)

© 2020 Palo Alto Networks, Inc.

Configuración de ruta estática	Description (Descripción)
Intervalo de ping (segundos)	Especifique el intervalo de ping ICMP en segundos para determinar con qué frecuencia el cortafuegos supervisará la ruta (enviará pings al destino supervisado; el intervalo es 1-60 y el predeterminado es 3).
Recuento de pings	Especifique el número de paquetes de ping ICMP consecutivos que no regresarán del destino supervisado antes de que el cortafuegos considere que el enlace no está activo. Basándose en la condición de fallo **Any (Alguna)** o **All (Todas)**, si la supervisión de rutas está en estado fallido, el cortafuegos eliminará la ruta estática del RIB (el intervalo es 3-10; el valor predeterminado es 5). Por ejemplo, un Intervalo de ping de 3 segundos y un Recuento de pings de 5 pings perdidos (el cortafuegos no recibe ningún ping en los últimos 15 segundos) significa que la supervisión de rutas detecta un fallo de enlace. Si la supervisión de rutas está en estado fallido y el cortafuegos recibe un ping después de 15 segundos, se considerará que el enlace está activo; basándose en la condición de fallo **Any (Alguna)** o **All (Todas)**, la supervisión de rutas a los destinos supervisados **Any (Alguna)** o **(All) Todas** puede considerarse activa, y se iniciará el Tiempo de retención preventiva.

Redistribución de ruta

- Network > Virtual Router > Redistribution Profiles

Los perfiles de redistribución dirigen el cortafuegos para filtrar, establecer la prioridad y realizar acciones basadas en el comportamiento de red deseado. La redistribución de rutas permite a las rutas estáticas y a las rutas adquiridas por otros protocolos anunciarse mediante protocolos de enrutamiento específicos.

Los perfiles de redistribución se deben aplicar a los protocolos de enrutamiento para que surtan efecto. Sin las reglas de redistribución, cada uno de los protocolos se ejecuta de forma separada y no se comunican fuera de su ámbito. Los perfiles de redistribución se pueden añadir o modificar después de configurar todos los protocolos de enrutamiento y de establecer la topología de red resultante.

Aplique perfiles de redistribución a los protocolos RIP y OSPF definiendo reglas de exportación. Aplique perfiles de redistribución a BGP en la pestaña **Redistribution Rules (Reglas de redistribución)**. Consulte la tabla siguiente.

Configuración de perfil de redistribución	Description (Descripción)
Nombre	Haga clic en **Add (Añadir)** en **Redistribution Profile (Perfil de redistribución)** e introduzca el nombre del perfil.
Prioridad	Introduzca un nivel de prioridad (intervalo 1-255) para este perfil. Los perfiles se muestran en orden (con los números más bajos primero).
Redistribuir	Seleccione si la redistribución de la ruta se realizará según los ajustes de esta ventana. • **Redist (Redistr.)**: Seleccione si la redistribución se realizará con rutas de candidato coincidentes. Si selecciona esta opción, introduzca un nuevo valor métrico. Un valor métrico inferior significa una ruta más preferible.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de redistribución	Description (Descripción)
	• **No Redist (No redistr.)**: Seleccione si no se realizará ningún tipo de redistribución.
Pestaña Filtro general	
Tipo	Seleccione los tipos de ruta de la ruta del candidato.
Interface (Interfaz)	Seleccione las interfaces para especificar las interfaces de reenvío de la ruta de candidato.
IP Destino	Para especificar el destino de la ruta de candidato, introduzca la dirección IP o la subred de destino (con el formato x.x.x.x o x.x.x.x/n) y haga clic en **Add (Añadir)**. Para eliminar una entrada, haga clic en Eliminar (⊖).
siguiente salto	Para especificar la puerta de enlace de la ruta de candidato, introduzca la dirección IP o la subred (con el formato x.x.x.x o x.x.x.x/n) que represente el siguiente salto y haga clic en **Add (Añadir)**. Para eliminar una entrada, haga clic en Eliminar (⊖).
Pestaña Filtro OSPF	
Tipo de ruta	Seleccione los tipos de ruta de la ruta OSPF.
Área	Especifique el identificador de área de la ruta de candidato OSPF. Introduzca el **OSPF area ID (ID de área OSPF)** (con el formato x.x.x.x), y haga clic en **Add (Añadir)**. Para eliminar una entrada, haga clic en Eliminar (⊖).
Tag (Etiqueta)	Especifique los valores de etiqueta OSPF. Introduzca un valor de etiqueta numérica (1-255) y haga clic Añadir. Para eliminar una entrada, haga clic en Eliminar (⊖).
Pestaña Filtro BGP	
Comunidad	Especifique una comunidad para la política de enrutamiento BGP.
Comunidad extendida	Especifique una comunidad extendida para la política de enrutamiento BGP.

RIP

- Network > Virtual Routers > RIP

La configuración del protocolo de información de enrutamiento (Routing Information Protocol, RIP) incluye los siguientes ajustes generales:

Configuración de RIP	Description (Descripción)
Habilitación	Seleccione esta opción para activar RIP.

© 2020 Palo Alto Networks, Inc.

Configuración de RIP	Description (Descripción)
Rechazar ruta por defecto	(Recomendado) Seleccione esta opción si no desea obtener ninguna de las rutas predeterminadas mediante RIP.
BFD	Para habilitar la detección de reenvío bidireccional (BFD) para RIP de forma global para un enrutador virtual en cortafuegos PA-5200 Series, PA-7000 Series y VM-Series, seleccione una de las siguientes opciones: • **default (predeterminado)** (perfil con la configuración BFD predeterminada) • un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. Seleccione **None (Disable BFD) [Ninguno (Deshabilitar BFD)]** para deshabilitar BFD para todas las interfaces RIP en el enrutador virtual; no puede habilitar BFD para una sola interfaz RIP.

Además, se deben configurar los ajustes RIP en las siguientes pestañas:

- **Interfaces**: Consulte Pestaña Interfaces de RIP.
- **Timers (Temporizadores)**: Consulte Pestaña Timers de RIP.
- **Auth Profiles (Perfiles de autenticación)**: Consulte Pestaña Auth Profiles de RIP.
- **Export Rules (Reglas de exportación)**: Consulte Pestaña Export Rules de RIP.

Pestaña Interfaces de RIP

- Network > Virtual Routers > RIP > Interfaces

Utilice los siguientes campos para configurar las interfaces de RIP:

RIP: Configuración de interfaz	Description (Descripción)
Interface (Interfaz)	Seleccione la interfaz que ejecuta el protocolo RIP.
Habilitación	Seleccione esta opción para habilitar estos ajustes.
Anunciar	Seleccione para habilitar el anuncio de una ruta predefinida a peers RIP con el valor métrico especificado.
Métrica	Especifique un valor métrico para el anuncio del enrutador. Este campo es visible solo si habilita **Advertise (Anuncio)**.
Perfil de autenticación	Seleccione el perfil.
Modo	Seleccione **Normal**, **passive (pasivo)** o **send-only (solo enviar)**.
BFD	Para habilitar BFD para una interfaz RIP (y por lo tanto sobrescribir la configuración BFD por RIP, siempre que BFD no esté deshabilitado para RIP a nivel del enrutador virtual), seleccione una de las siguientes opciones: • **default (predeterminado)** (perfil con la configuración BFD predeterminada)

© 2020 Palo Alto Networks, Inc.

RIP: Configuración de interfaz	Description (Descripción)
	• un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. Seleccione **None (Disable BFD) [Ninguno (deshabilitar BFD)]** para deshabilitar BFD para la interfaz RIP.

Pestaña Temporizadores de RIP

- Network > Virtual Router > RIP > Timers

La siguiente tabla describe los temporizadores que controlan las actualizaciones y vencimientos de la ruta RIP.

RIP: Configuración de temporizadores	Description (Descripción)
Sincronización de RIP	
Segundos del intervalo (seg)	Defina la duración del intervalo de tiempo en segundos. Esta duración se utiliza para el resto de los campos de temporización de RIP (el intervalo es 1-60).
Intervalo de actualizaciones	Introduzca el número de intervalos entre los anuncios de actualización de rutas (el intervalo es 1-3.600).
Intervalos de vencimiento	Introduzca el número de intervalos entre la última hora de actualización de la ruta hasta su vencimiento (el intervalo es 1-3.600).
Intervalo de eliminación	Introduzca el número de intervalos entre la hora de vencimiento de la ruta hasta su eliminación (el intervalo es 1-3.600).

Pestaña Perfiles de autenticación de RIP

- Network > Virtual Router > RIP > Auth Profiles

Por defecto, el cortafuegos no autentica los mensajes RIP entre vecinos. Para autenticar los mensajes RIP entre vecinos, cree un perfil de autenticación y aplíquelo a una interfaz que ejecute RIP en un enrutador virtual. La tabla siguiente describe los ajustes de la pestaña **Auth Profiles (Perfiles de autenticación)**.

RIP: Configuración de perfil de autenticación	Description (Descripción)
Nombre de perfil	Introduzca un nombre para el perfil de autenticación para autenticar los mensajes RIP.
Tipo de contraseña	Seleccione el tipo de contraseña (simple o MD5). • Si selecciona **Simple**, introduzca la contraseña sencilla y, a continuación, confirme.

© 2020 Palo Alto Networks, Inc.

RIP: Configuración de perfil de autenticación	Description (Descripción)
	• Si selecciona **MD5**, introduzca una o más entradas de contraseña, incluyendo **Key-ID (ID de clave)** (0-255), **Key (Clave)** y, opcionalmente, el estado **Preferred (Preferido)**. Haga clic en **Add (Añadir)** en cada entrada y, a continuación, haga clic en **OK (Aceptar)**. Para especificar la clave que se debe utilizar para autenticar el mensaje saliente, seleccione la opción **Preferred (Preferido)**.

Pestaña Reglas de exportación de RIP

- Network > Virtual Router > RIP > Export Rules

Las reglas de exportación RIP le permiten controlar qué rutas el enrutador virtual envía a los peers.

RIP: Configuración de reglas de exportación	Description (Descripción)
Permitir redistribución de ruta predeterminada	Seleccione para permitir que el cortafuegos redistribuya su ruta predeterminada a los peers.
Perfil de redistribución	Haga clic en **Add (Añadir)** y seleccione o cree un perfil de redistribución que le permita modificar la redistribución de la ruta, el filtro, la prioridad y la acción, en función del comportamiento de red deseado. Consulte la Redistribución de rutas.

OSPF

- Network > Virtual Router > OSPF

La configuración del protocolo OSPF (Open Shortest Path First) requiere que configure los siguientes ajustes generales (excepto BFD, que es opcional):

Configuración de OSPF	Description (Descripción)
Habilitación	Seleccione esta opción para habilitar el protocolo OSPF.
Rechazar ruta por defecto	(Recomendado) Seleccione esta opción si no desea obtener ninguna de las rutas predeterminadas mediante OSPF.
ID del enrutador	Especifique el ID del enrutador asociado con la instancia OSPF en este enrutador virtual. El protocolo OSPF utiliza el ID del enrutador para identificar de manera única la instancia OSPF.
BFD	Para habilitar la detección de reenvío bidireccional (BFD) para OSPF de forma global para un enrutador virtual en cortafuegos PA-5200 Series, PA-7000 Series, o VM-Series, seleccione una de las siguientes opciones: • **default (predeterminada)** (configuración BFD predeterminada) • un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo.

© 2020 Palo Alto Networks, Inc.

Configuración de OSPF	Description (Descripción)
	Seleccione **None (Disable BFD)** para deshabilitar BFD para todas las interfaces OSPF en el enrutador virtual; no puede habilitar BFD para una sola interfaz OSPF.

Además, debe configurar los ajustes de OSPF en las siguientes pestañas:

- **Areas (Áreas)**: Consulte Pestaña Areas de OSPF.
- **Auth Profiles (Perfiles de autenticación)**: Consulte Pestaña Auth Profiles de OSPF.
- **Export Rules (Reglas de exportación)**: Consulte Pestaña Export Rules de OSPF.
- **Advanced (Avanzado)**: Consulte Pestaña Advanced de OSPF.

Pestaña Áreas de OSPF

- Network > Virtual Router > OSPF > Areas

Los siguientes campos describen la configuración del área OSPF:

OSPF: Configuración de áreas	Description (Descripción)
Áreas	
ID de área	Configure el área en el que los parámetros OSPF se pueden aplicar. Introduzca un identificador del área en formato x.x.x.x. Es el identificador que cada vecino debe aceptar para formar parte de la misma área.
Tipo	Seleccione una de las siguientes opciones. • **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, seleccione **Accept Summary (Aceptar resumen)** si desea aceptar este tipo de anuncio de estado de enlace (LSA) de otras áreas. También puede especificar si desea incluir una ruta LSA predeterminada en los anuncios al área de código auxiliar, junto con el valor métrico asociado (el intervalo es de 1 a 255). Si la opción **Accept Summary (Aceptar resumen)** de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está desactivada, el área OSPF se comportará como un área totalmente de código auxiliar (TSA) y ABR no propagará ninguno de los LSA de resumen. • **NSSA** (Not-So-Stubby Area, Área no totalmente de código auxiliar): es posible salir del área directamente, pero solo mediante rutas que no sean OSPF. Si selecciona esta opción, seleccione **Accept Summary (Aceptar resumen)** si desea aceptar este tipo de LSA. Seleccione **Advertise Default Route (Anunciar ruta predeterminada)** para especificar si desea incluir una LSA de ruta predeterminada en los anuncios del área de código auxiliar, junto con el valor métrico asociado (1-255). También puede seleccionar el tipo de ruta que se utilizará para anunciar el LSA predefinido. Haga clic en **Add (Añadir)** en la sección **External Ranges (Intervalos externos)** e introduzca los intervalos si desea activar o

© 2020 Palo Alto Networks, Inc.

OSPF: Configuración de áreas	Description (Descripción)
	suprimir rutas externas de anuncios que se obtienen mediante NSSA a otras áreas.
Intervalo	Haga clic en **Add (Añadir)** para añadir direcciones de destino LSA en el área en subredes. Habilite o suprima LSA de anuncios que coincidan con la subred y haga clic en **OK (Aceptar)**. Repita esta acción para añadir intervalos adicionales.

Interface (Interfaz)	Haga clic en **Add (Añadir)** para incluir una interfaz en el área e introduzca la siguiente información:
	• **Interface (Interfaz)**: seleccione la interfaz.
	• **Enable (Habilitar)**: permite que la configuración de la interfaz OSPF surta 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. Seleccione **p2mp** (punto a multipunto) si los vecinos se deben definir manualmente. La definición manual de vecino solo se permite en modo p2mp.
	• **Metric (Métrica)**: introduzca la métrica OSPF de esta interfaz (0-65.535).
	• **Priority**: introduzca la prioridad OSPF de esta interfaz (0-255). Es la prioridad del enrutador para ser el enrutador designado (DR) o de reserva (BDR) según el protocolo OSPF. Si el valor es cero, el enrutador no se designará como DR ni BDR.
	• **Auth Profile**: seleccione un perfil de autenticación definido previamente.
	• **BFD**: para habilitar la detección de reenvío bidireccional (BFD) para una interfaz OSPF (y por lo tanto sobrescribir la configuración **BFD** por OSPF, siempre que **BFD** no esté deshabilitado para OSPF a nivel del enrutador virtual), seleccione una de las siguientes opciones:
	  • **default (predeterminada)** (configuración BFD predeterminada)
	  • un perfil BFD que creó en el cortafuegos
	  • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo.
	  • Seleccione **None (Disable BFD)** para deshabilitar BFD para la interfaz de peer OSPF.
	• **Hello Interval (sec) [Intervalo de saludo (seg)]**: intervalo, en segundos, en el que el proceso de OSPF envía paquetes de saludo a sus vecinos directamente conectados (intervalo 0-3600; predeterminado 10).
	• **Dead Counts (Recuentos fallidos)**: número de ocasiones en las que se puede producir el intervalo de saludo para un vecino sin que OSPF reciba un paquete de saludo desde el vecino, antes de que OSPF considere que ese vecino tiene un fallo. El **Hello Interval (Intervalo de saludo)** multiplicado por los **Dead Counts (Recuentos fallidos)** es igual al valor del temporizador de fallos (intervalo 3-20; predeterminado 4).

© 2020 Palo Alto Networks, Inc.

OSPF: Configuración de áreas	Description (Descripción)
	• **Retransmit Interval (sec) (Intervalo de retransmisión [s])**: tiempo, en segundos, que espera el OSPF para recibir un anuncio de estado de enlace (LSA) de un vecino antes de que el OSPF retransmita el LSA (el intervalo es de 0 a 3600; el valor predeterminado es 10). • **Transit Delay (sec) (Retraso de tránsito [s])**: tiempo, en segundos, que un LSA se retrasa antes de enviarse a una interfaz (el intervalo es de 0 a 3600; el valor predeterminado es 1).
Interface (cont.)	• **Graceful Restart Hello Delay (sec)**: se aplica a una interfaz de OSPF cuando se configura la alta disponibilidad activa/pasiva. **Graceful Restart Hello Delay (Retraso de saludo de reinicio correcto)** es el tiempo durante el cual el cortafuegos envía los paquetes de LSA de gracia en intervalos de 1 segundo. Durante este tiempo no se envían paquetes de saludo desde el cortafuegos de reinicio. Durante el reinicio, el temporizador de fallos (que es el **intervalo de saludo** multiplicado por los **recuentos fallidos**) también avanza en la cuenta regresiva. Si el temporizador de fallos es demasiado corto, la adyacencia bajará durante el reinicio correcto a causa del retraso de saludo. Por lo tanto, se recomienda que el temporizador de fallos sea al menos cuatro veces el valor del **retraso de saludo de reinicio correcto**. Por ejemplo, un **Hello Interval (Intervalo de saludo)** de 10 segundos y un valor de **Dead Counts (Recuentos fallidos)** de 4 da como resultado un valor de temporizador de fallos de 40 segundos. Si el **Graceful Restart Hello Delay (Retraso de saludo de reinicio correcto)** se establece en 10 segundos, ese retraso de 10 segundos de los paquetes de saludo se enmarca cómodamente dentro del temporizador de fallos de 40 segundos, de forma que la adyacencia no agotará su tiempo de espera durante un reinicio correcto (el intervalo es de 1 a 10; el valor predeterminado es 10).
Enlace virtual	Configure los ajustes del enlace virtual para mantener o mejorar la conectividad del área troncal. Los ajustes se deben definir para enrutadores de borde de área y se deben definir en el área troncal (0.0.0.0). Haga clic en **Add (Añadir)** e introduzca la siguiente información en enlace virtual que se incluirá en el área troncal y haga clic en **OK (Aceptar)**. • **Name**: introduzca un nombre para 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. • **Enable**: seleccione para habilitar el enlace virtual. • **Timing**: es recomendable que mantenga su configuración temporal por defecto. • **Auth Profile**: seleccione un perfil de autenticación definido previamente.

Pestaña Perfiles de autenticación de OSPF

- Network > Virtual Router > OSPF > Auth Profiles

Los siguientes campos describen la configuración de perfil de autenticación de OSPF:

© 2020 Palo Alto Networks, Inc.

OSPF: Configuración del perfil de autenticación	Description (Descripción)
Nombre de perfil	Introduzca un nombre para el perfil de autenticación. Para autenticar mensajes OSPF, primero defina los perfiles de autenticación y a continuación, aplíquelos a las interfaces en la pestaña **OSPF**.
Tipo de contraseña	Seleccione el tipo de contraseña (simple o MD5). • Si selecciona **Simple**, introduzca la contraseña. • Si selecciona **MD5**, introduzca una o más entradas de contraseña, incluyendo **Key-ID (ID de clave)** (0-255), **Key (Clave)** y, opcionalmente, el estado **Preferred (Preferido)**. Haga clic en **Add (Añadir)** en cada entrada y, a continuación, haga clic en **OK (Aceptar)**. Para especificar la clave que se debe utilizar para autenticar el mensaje saliente, seleccione la opción **Preferred (Preferido)**.

Pestaña Reglas de exportación de OSPF

- Network > Virtual Router > OSPF > Export Rules

La siguiente tabla describe los campos para exportar rutas OSPF:

OSPF: Configuración de reglas de exportación	Description (Descripción)
Permitir redistribución de ruta predeterminada	Seleccione para permitir la redistribución de las rutas predeterminadas mediante OSPF.
Nombre	Seleccione el nombre del perfil de redistribución. El valor debe ser una subred IP o un nombre de perfil de redistribución válido.
Nuevo tipo de ruta	Seleccione el tipo de métrica que se aplicará.
Nueva etiqueta	Especifique una etiqueta para la ruta que tenga un valor de 32 bits.
Métrica	(Opcional) Especifique la métrica de ruta asociada con la ruta exportada que se utilizará para seleccionar la ruta (intervalo 1-65.535).

Pestaña avanzada de OSPF

- Network > Virtual Router > OSPF > Advanced

Los siguientes campos describen la compatibilidad RFC 1583, los temporizadores OSPF y el reinicio correcto:

OSPF: Configuración avanzada	Description (Descripción)
Compatibilidad RFC 1583	Seleccione esta opción para garantizar la compatibilidad con RFC 1583 (OSPF versión 2).

© 2020 Palo Alto Networks, Inc.

OSPF: Configuración avanzada	Description (Descripción)
Temporizadores	• **SPF Calculation Delay (sec) [Retraso de cálculo SPF (seg)+**: le permite definir el retraso de tiempo entre la recepción de nueva información de topología y ejecutar un cálculo SPF. Los valores menores permiten una reconvergencia OSPF más rápida. Los enrutadores que se emparejan con el cortafuegos se deben configurar de manera similar para optimizar los tiempos de convergencia. • **LSA Interval (sec) [Intervalo LSA (seg)]**: especifica el tiempo mínimo entre las transmisiones de las 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.
Reinicio correcto	• **Enable Graceful Restart (Habilitar reinicio correcto)**: habilitado de forma predeterminada; un cortafuegos que tenga esta función activada indicará a los enrutadores vecinos que continúen usándolo como ruta cuando tenga lugar una transición que lo desactive temporalmente. • **Enable Helper Mode (Habilitar modo auxiliar)**: habilitado de forma predeterminada; un cortafuegos que tenga este modo activado continuará reenviando a un dispositivo adyacente durante el reinicio del dispositivo. • **Enable Strict LSA Checking (Habilitar comprobación de LSA estricta)**: habilitado de forma predeterminada; esta función hace que el cortafuegos que tenga habilitado el modo auxiliar de OSPF salga de este modo si se produce un cambio de topología. • **Grace Period (sec) (Periodo de gracia [s])**: periodo de tiempo, en segundos, que los dispositivos peer deben continuar reenviando a este cortafuegos mientras las adyacencias de este se están restableciendo o el enrutador se está reiniciando (el intervalo es de 5 a 1800; el valor predeterminado es 120). • **Max Neighbor Restart Time (Máx. de hora de reinicio del mismo nivel)**: periodo de gracia máximo, en segundos, que el cortafuegos aceptará como enrutador de modo auxiliar. Si los dispositivos peer ofrecen un periodo de gracia más largo en su LSA de gracia, el cortafuegos no entrará en modo auxiliar (intervalo 5-1.800; predeterminado 140).

OSPFv3

- Network > Virtual Router > OSPFv3

La configuración del protocolo OSPFv3 (Open Shortest Path First v3) requiere configurar los tres primeros ajustes en la siguiente tabla (BFD es opcional):

Configuración de OSPFv3	Description (Descripción)
Habilitación	Seleccione esta opción para habilitar el protocolo OSPF.
Rechazar ruta por defecto	Seleccione esta opción si no desea obtener ninguna de las rutas predeterminadas mediante OSPF.

© 2020 Palo Alto Networks, Inc.

Configuración de OSPFv3	Description (Descripción)
ID del enrutador	Especifique el ID del enrutador asociado con la instancia OSPF en este enrutador virtual. El protocolo OSPF utiliza el ID del enrutador para identificar de manera única la instancia OSPF.
BFD	Para habilitar la detección de reenvío bidireccional (BFD) para OSPFv3 de forma global para un enrutador virtual en cortafuegos PA-5200 Series, PA-7000 Series y VM-Series, seleccione una de las siguientes opciones: • **default (predeterminada)** (configuración BFD predeterminada) • un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. Seleccione **None (Disable BFD) (Ninguno [Deshabilitar BFD])** para deshabilitar BFD en todas las interfaces OSPFv3 del enrutador virtual; no puede habilitar BFD en una sola interfaz OSPFv3.

Además, se deben configurar los ajustes OSPFv3 en las siguientes pestañas:

- **Areas (Áreas)**: Consulte Pestaña Areas de OSPFv3.
- **Auth Profiles (Perfiles de autenticación)**: Consulte Pestaña Auth Profiles de OSPFv3.
- **Export Rules (Reglas de exportación)**: Consulte Pestaña Export Rules de OSPFv3.
- **Advanced (Avanzado)**: Consulte Pestaña Advanced de OSPFv3.

Pestaña Áreas de OSPFv3

- Network > Virtual Router > OSPFv3 > Areas

Utilice los siguientes campos para configurar las áreas OSPFv3.

OSPFv3: Configuración de áreas	Description (Descripción)
Autenticación	Seleccione el nombre del perfil de autenticación que desea especificar para esta área de OSPFarea.
Tipo	Seleccione una de las siguientes opciones: • **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, seleccione **Accept Summary (Aceptar resumen)** si desea aceptar este tipo de anuncio de estado de enlace (LSA) de otras áreas. También puede especificar si desea incluir una ruta LSA predefinida en los anuncios al área de código auxiliar, junto con el valor métrico asociado (1-255). Si la opción **Accept Summary (Aceptar resumen)** de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está desactivada, 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.

OSPFv3: Configuración de áreas	Description (Descripción)
	• **NSSA** (Not-So-Stubby Area, Área no totalmente de código auxiliar): es posible salir del área directamente, pero solo mediante rutas que no sean OSPF. Si selecciona esta opción, seleccione **Accept Summary (Aceptar resumen)** si desea aceptar este tipo de LSA. Especifique si desea incluir una ruta LSA predefinida en los anuncios al área de código auxiliar, junto con el valor métrico asociado (1-255). También puede seleccionar el tipo de ruta que se utilizará para anunciar el LSA predefinido. Haga clic en **Add (Añadir)** en la sección **External Ranges (Intervalos externos)** e introduzca los intervalos si desea activar o suprimir rutas externas de anuncios que se obtienen mediante NSSA a otras áreas.
Intervalo	Haga clic en **Add (Añadir)** para que la subred añada direcciones IPv6 de destino LSA en el área. Habilite o suprima LSA de anuncios que coincidan con la subred y haga clic en **OK (Aceptar)**. Repita esta acción para añadir intervalos adicionales.
Interface (Interfaz)	Haga clic en **Add (Añadir)** e introduzca la siguiente información en cada interfaz que se incluirá en el área y haga clic en **OK (Aceptar)**. • **Interface (Interfaz)**: seleccione la interfaz. • **Enable (Habilitar)**: permite que la configuración de la interfaz OSPF surta efecto. • **Instance ID**: introduzca un número de ID de instancia OSPFv3. • **Passive (Pasivo)**: 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. Seleccione **p2mp** (punto a multipunto) si los vecinos se deben definir manualmente. La definición manual de vecino solo se permite en modo p2mp. • **Metric (Métrica)**: introduzca la métrica OSPF de esta interfaz (0-65.535). • **Priority**: introduzca la prioridad OSPF de esta interfaz (0-255). Es la prioridad del enrutador para ser el enrutador designado (DR) o de reserva (BDR) según el protocolo OSPF. Si el valor es cero, el enrutador no se designará como DR ni BDR. • **Auth Profile**: seleccione un perfil de autenticación definido previamente. • **BFD**: para habilitar la detección de reenvío bidireccional (BFD) para una interfaz OSPFv3 (y por lo tanto sobrescribir la configuración **BFD** por OSPFv3, siempre que **BFD** no esté deshabilitado para OSPFv3 a nivel del enrutador virtual), seleccione una de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

OSPFv3: Configuración de áreas	Description (Descripción)
	• **default (predeterminada)** (configuración BFD predeterminada) • un perfil BFD que creó en el cortafuegos • **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. Seleccione **None (Disable BFD) [Ninguno (Deshabilitar BFD)]** para deshabilitar OSPFv3 para la interfaz de peer OSPF. • **Hello Interval (sec) [Intervalo de saludo (seg)]**: intervalo, en segundos, en el que el proceso de OSPF envía paquetes de saludo a sus vecinos directamente conectados (el intervalo es de 0 a 3.600; el valor predeterminado es 10). • **Dead Counts (Recuentos fallidos)**: número de ocasiones en las que se puede producir el intervalo de saludo para un vecino sin que OSPF reciba un paquete de saludo desde el vecino, antes de que OSPF considere que ese vecino tiene un fallo. El **Hello Interval (Intervalo de saludo)** multiplicado por los **Dead Counts (Recuentos fallidos)** es igual al valor del temporizador de fallos (intervalo 3-20; predeterminado 4). • **Retransmit Interval (sec) (Intervalo de retransmisión [s])**: tiempo, en segundos, que espera el OSPF para recibir un anuncio de estado de enlace (LSA) de un vecino antes de que el OSPF retransmita el LSA (el intervalo es de 0 a 3600; el valor predeterminado es 10). • **Transit Delay (sec) (Retraso de tránsito [s])**: tiempo, en segundos, que un LSA se retrasa antes de que el cortafuegos lo saque de una interfaz (el intervalo es de 0 a 3600; el valor predeterminado es 1).
Interfaz (continuación)	• **Graceful Restart Hello Delay (sec)**: se aplica a una interfaz de OSPF cuando se configura la alta disponibilidad activa/pasiva. **Graceful Restart Hello Delay (Retraso de saludo de reinicio correcto)** es el tiempo durante el cual el cortafuegos envía los paquetes de LSA de gracia en intervalos de 1 segundo. Durante este tiempo no se envían paquetes de saludo desde el cortafuegos de reinicio. Durante el reinicio, el temporizador de fallos (que es el **intervalo de saludo** multiplicado por los **recuentos fallidos**) también avanza en la cuenta regresiva. Si el temporizador de fallos es demasiado corto, la adyacencia bajará durante el reinicio correcto a causa del retraso de saludo. Por lo tanto, se recomienda que el temporizador de fallos sea al menos cuatro veces el valor del **retraso de saludo de reinicio correcto**. Por ejemplo, un **Hello Interval (Intervalo de saludo)** de 10 segundos y un valor de **Dead Counts (Recuentos fallidos)** de 4 da como resultado un valor de temporizador de fallos de 40 segundos. Si el **Graceful Restart Hello Delay (Retraso de saludo de reinicio correcto)** se establece en 10 segundos, ese retraso de 10 segundos de los paquetes de saludo se enmarca cómodamente dentro del temporizador de fallos de 40 segundos, de forma que la

© 2020 Palo Alto Networks, Inc.

OSPFv3: Configuración de áreas	Description (Descripción)
	adyacencia no agotará su tiempo de espera durante un reinicio correcto (el intervalo es de 1 a 10; el valor predeterminado es 10). • **Neighbors (Vecinos)**: en interfaces p2pmp, introduzca la dirección IP de todos los vecinos accesibles mediante esta interfaz.
Enlaces virtuales	Configure los ajustes del enlace virtual para mantener o mejorar la conectividad del área troncal. Los ajustes se deben definir para enrutadores de borde de área y se deben definir en el área troncal (0.0.0.0). Haga clic en **Add (Añadir)** e introduzca la siguiente información en enlace virtual que se incluirá en el área troncal y haga clic en **OK (Aceptar)**. • **Name**: introduzca un nombre para el enlace virtual. • **Instance ID (ID de instancia)**: introduzca un número de ID de instancia OSPFv3. • **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. • **Enable**: seleccione para habilitar el enlace virtual. • **Timing**: es recomendable que mantenga su configuración temporal por defecto. • **Auth Profile**: seleccione un perfil de autenticación definido previamente.

Pestaña Perfiles de autenticación de OSPFv3

- Network > Virtual Router > OSPFv3 > Auth Profiles

Utilice los siguientes campos para configurar la autenticación de OSPFv3.

OSPFv3: Configuración del perfil de autenticación	Description (Descripción)
Nombre de perfil	Introduzca un nombre para el perfil de autenticación. Para autenticar mensajes OSPF, primero defina los perfiles de autenticación y a continuación, aplíquelos a las interfaces en la pestaña **OSPF**.
SPI	Especifique el índice de parámetros de seguridad (SPI) para los paquetes transversales desde el cortafuegos remoto hasta el peer.
PROTOCOL	Especifique uno de los siguientes protocolos: • **ESP**: Protocolo de carga de seguridad encapsulada. • **AH**: Protocolo del encabezado de autenticación.

© 2020 Palo Alto Networks, Inc.

OSPFv3: Configuración del perfil de autenticación	Description (Descripción)
Algoritmo criptográfico	Especifique una de las siguientes opciones: • **None (Ninguno)**: No se utilizará ningún algoritmo criptográfico. • **SHA1** (predeterminado): algoritmo de hash seguro 1. • **SHA256**: Algoritmo de hash seguro 2. Conjunto de cuatro funciones de hash con un resumen de 256 bits. • **SHA384**: Algoritmo de hash seguro 2. Conjunto de cuatro funciones de hash con un resumen de 384 bits. • **SHA512**: Algoritmo de hash seguro 2. Conjunto de cuatro funciones de hash con un resumen de 512 bits. • **MD5**: Algoritmo de resumen de mensaje de MD5.
Clave/Confirmar clave	Introduzca y confirme una clave de autenticación.
Encryption (protocolo ESP únicamente)	Especifica una de las siguientes opciones: • **3des** (predeterminado): aplica el algoritmo 3DES (Triple Data Encryption Algorithm, algoritmo de cifrado de datos triple) utilizando tres claves criptográficas de 56 bits. • **aes-128-cbc**: Se aplica el estándar de cifrado avanzado (AES) usando las claves criptográficas de 128 bits. • **aes-192-cbc**: Se aplica el estándar de cifrado avanzado (AES) usando las claves criptográficas de 192 bits. • **aes-256-cbc**: Se aplica el estándar de cifrado avanzado (AES) usando las claves criptográficas de 256 bits. • **null (nulo)**: No se utiliza ningún cifrado.
Clave/Confirmar clave	Introduzca y confirme una clave de cifrado.

Pestaña Reglas de exportación de OSPFv3

- Network > Virtual Router > OSPFv3 > Export Rules

Utilice los siguientes campos para exportar rutas OSPFv3.

OSPFv3: Configuración de reglas de exportación	Description (Descripción)
Permitir redistribución de ruta predeterminada	Seleccione para permitir la redistribución de las rutas predeterminadas mediante OSPF.
Nombre	Seleccione el nombre del perfil de redistribución. El valor debe ser una subred IP o un nombre de perfil de redistribución válido.
Nuevo tipo de ruta	Seleccione el tipo de métrica que se aplicará.

© 2020 Palo Alto Networks, Inc.

OSPFv3: Configuración de reglas de exportación	Description (Descripción)
Nueva etiqueta	Especifique una etiqueta para la ruta que tenga un valor de 32 bits.
Métrica	(Opcional) Especifique la métrica de ruta asociada con la ruta exportada que se utilizará para seleccionar la ruta (intervalo 1-65.535).

Pestaña avanzada de OSPFv3

- Network > Virtual Router > OSPFv3 > Advanced

Utilice los campos siguientes para deshabilitar el enrutamiento de tránsito para los cálculos SPF, configurar los temporizadores OSPFv3 y configurar el reinicio correcto para OSPFv3.

OSPFv3: Configuración avanzada	Description (Descripción)
Deshabilitar enrutamiento de tránsito para el cálculo de SPF	Seleccione esta opción si desea establecer el R-bit en los LSA del enrutador enviados desde este cortafuegos para indicar que el cortafuegos no está activo. Cuando está en este estado, el cortafuegos participa en OSPFv3 pero ningún otro enrutador envía tráfico de tránsito. En este estado, el tráfico local seguirá reenviándose al cortafuegos. Es útil cuando se realiza mantenimiento con una red de dos bases porque el tráfico se puede volver a enrutar en el cortafuegos mientras este siga siendo accesible.
Temporizadores	• **SPF Calculation Delay (sec) (Retraso de cálculo SPF [s])**: esta opción es un temporizador que le permite definir el retraso de tiempo entre la recepción de nueva información de topología y ejecutar un cálculo SPF. Los valores menores permiten una reconvergencia OSPF más rápida. Los enrutadores que se emparejan con el cortafuegos se deben configurar de manera similar para optimizar los tiempos de convergencia. • **LSA Interval (sec) [(Intervalo LSA) (seg.)]**: esta opción especifica el tiempo mínimo entre las transmisiones de las 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.
Reinicio correcto	• **Enable Graceful Restart (Habilitar reinicio correcto)**: habilitado de forma predeterminada; un cortafuegos que tenga esta función activada indicará a los enrutadores vecinos que continúen usándolo como ruta cuando tenga lugar una transición que lo desactive temporalmente. • **Enable Helper Mode (Habilitar modo auxiliar)**: habilitado de forma predeterminada; un cortafuegos que tenga este modo

© 2020 Palo Alto Networks, Inc.

OSPFv3: Configuración avanzada	Description (Descripción)
	activado continuará reenviando a un dispositivo adyacente durante el reinicio del dispositivo. • **Enable Strict LSA Checking (Habilitar comprobación de LSA estricta)**: habilitado de forma predeterminada; esta función hace que el cortafuegos que tenga habilitado el modo auxiliar de OSPF salga de este modo si se produce un cambio de topología. • **Grace Period (sec) (Periodo de gracia [s])**: periodo de tiempo, en segundos, que los dispositivos peer continúan reenviando a este cortafuegos mientras las adyacencias de este se están restableciendo o el enrutador se está reiniciando (el intervalo es de 5 a 1800; el valor predeterminado es 120). • **Max Neighbor Restart Time (Máx. de hora de reinicio del mismo nivel)** : periodo de gracia máximo en segundos que el cortafuegos aceptará como enrutador de modo auxiliar. Si los dispositivos peer ofrecen un periodo de gracia más largo en su LSA de gracia, el cortafuegos no entrará en modo auxiliar (el intervalo es de 5 a 800; el valor predeterminado es 140).

BGP

- Network > Virtual Router > BGP

La configuración del Protocolo de puerta de enlace de borde (BGP) requiere la configuración de la Configuración básica de BGP para habilitar BGP y configurar la ID del enrutador y el número AS, como se describe en la siguiente tabla. Además, debe configurar un peer BGP como parte de un grupo de peer BGP.

Configure la configuración BGP restante en las siguientes pestañas según sea necesario para su red:

- **General**: Consulte la Pestaña General de BGP.
- **Advanced (Avanzado)**: Consulte la Pestaña avanzada de BGP.
- **Peer Group (Grupo del peer)**: Consulte la Pestaña grupo del peer de BGP.
- **Import (Importar)**: Consulte la Pestañas Importar y Exportar de BGP.
- **Export (Exportar)**: Consulte la Pestañas Importar y Exportar de BGP.
- **Conditional Adv (Anuncio condicional)**: Consulte la Pestaña Anuncio condicional de BGP.
- **Aggregate (Agregado)**: Consulte la Pestaña Agregado de BGP.
- **Redist Rules (Reglas de redistr.)**: Consulte la Pestaña Reglas de distr. de BGP.

Configuración básica de BGP

Para utilizar BGP en un enrutador virtual, debe habilitar BGP y configurar el ID del enrutador y el número AS; la habilitación de BFD es opcional.

Configuración de BGP	Configurado en	Description (Descripción)
Habilitación	**BGP**	Seleccione para habilitar BGP.
ID del enrutador		Introduzca la dirección IP para asignarla al enrutador virtual.

© 2020 Palo Alto Networks, Inc.

Configuración de BGP	Configurado en	Description (Descripción)
AS Number		Introduzca 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).
BFD		Para habilitar la detección de reenvío bidireccional (BFD) para BGP de forma global para un enrutador virtual en cortafuegos PA-5200 Series, PA-7000 Series, o VM-Series, seleccione una de las siguientes opciones: • **default (predeterminada)** (configuración BFD predeterminada) • un perfil BFD existente en el cortafuegos • creación de un **New BFD Profile (Nuevo perfil BFD)** Seleccione **None (Disable BFD) [Ninguno (Deshabilitar BFD)]** para deshabilitar BFD para todas las interfaces BGP en el enrutador virtual; no puede habilitar BFD para una sola interfaz 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, lo que puede interrumpir el tráfico BGP. Por lo tanto, habilite BFD en las interfaces BGP durante un horario de menor demanda, cuando la reconvergencia no impacte el tráfico de producción.*

Pestaña general de BGP

- Red > Enrutador virtual > BGP > General

Utilice los siguientes campos para configurar los configuración general de BGP.

Configuración general de BGP	Configurado en	Description (Descripción)
Rechazar ruta por defecto	**BGP** > **General (General)**	Seleccione esta opción para ignorar todas las rutas predeterminadas anunciadas por peers BGP.
Instalar ruta		Seleccione esta opción para instalar rutas BGP en la tabla de enrutamiento global.
Agregar MED		Seleccione esta opción para activar la agregación de rutas incluso si las rutas tienen valores diferentes de discriminador de salida múltiple (MED).
Preferencia local predeterminada		Especifica un valor que que puede utilizar el cortafuegos para determinar preferencias entre diferentes rutas.
Formato AS		Seleccione el formato de 2 (predefinido) o 4 bytes. Este ajuste es configurable por motivos de interoperabilidad.

© 2020 Palo Alto Networks, Inc.

Configuración general de BGP	Configurado en	Description (Descripción)
Comparar siempre MED		Permite comparar MED para rutas de vecinos en diferentes sistemas autónomos.
Comparación determinista de MED		Permite la comparación MED para elegir entre rutas anunciadas por peers iBGP (peers BGP en el mismo sistema autónomo).
Perfiles de autenticación		Haga clic en **Add (Añadir)** un nuevo perfil de autenticación y configurar los siguientes ajustes: • **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. Eliminar (⊖) perfiles cuando ya no los necesite.

Pestaña avanzada de BGP

- Network > Virtual Router > BGP > Advanced

La configuración avanzada de BGP incluye una variedad de capacidades. Puede ejecutar ECMP en varios sistemas autónomos BGP. Puede requerir que los peers de eBGP listen su propio AS como el primer AS en un atributo AS_PATH (para evitar los paquetes de actualización falsificados). Puede configurar reinicio correcto de BGP, un medio por el cual los peers de BGP indican si pueden conservar el estado de reenvío durante un reinicio de BGP para minimizar las consecuencias de las fluctuaciones de rutas (subidas y bajadas). Puede configurar reflectores de ruta y confederaciones AS, que son dos métodos para evitar tener una malla completa de peering de BGP en un AS. Puede configurar la amortiguación de la ruta para evitar la convergencia innecesaria del enrutador cuando una red BGP es inestable y las rutas están fluctuando.

Configuración de BGP Advanced	Configurado en	Description (Descripción)
Soporte de AS de múltiple ECMP	**BGP** > **Advanced (Avanzado)**	Seleccione si habilita ECMP para un enrutador virtual y desea ejecutar ECMP en varios sistemas BGP autónomos.
Aplicar primer AS para EBGP		Provoca que el cortafuegos elimine un paquete de actualización entrante de un peer de eBGP que no lista el propio número AS del peer de eBGP como el primer número de AS en el atributo AS_PATH. Esto evita que BGP continúe procesando un paquete de actualización falsificado o erróneo que llega de un AS distinto al AS vecino. El valor predeterminado está habilitado.
Reinicio correcto		Active la opción de reinicio correcto. • **Stale Route Time (Tiempo de ruta obsoleto)**: especifique el tiempo, en segundos, que una ruta puede permanecer inhabilitada (intervalo 1-3.600; predefinido 120). • **Local Restart Time (Hora de reinicio local)**: especifica la cantidad de tiempo, en segundos, que el cortafuegos tarda en reiniciar.

© 2020 Palo Alto Networks, Inc.

Configuración de BGP Advanced	Configurado en	Description (Descripción)
		Este valor se les comunica a los peers (intervalo 1-3.600; predefinido 120). • **Max Peer Restart Time (Máx. de hora de reinicio del peer)**: especifique el tiempo máximo, en segundos, que el cortafuegos acepta como período de gracia para reiniciar los dispositivos peer (intervalo 1-3.600; predefinido 120).
ID de clúster reflector		Especifique un identificador IPv4 para representar el clúster reflector. Un reflector de ruta (enrutador) en un AS se encarga de volver a publicar rutas que aprendió a sus peers (en lugar de requerir la conectividad de malla completa y que todos los peers envíen rutas entre sí). El reflector de ruta simplifica la configuración.
AS de miembro de confederación		Especifique el identificador de número de sistema autónomo visible solo dentro de la confederación BGP (también se denomina número de sistema subautónomo). Utilice una confederación BGP para dividir los sistemas autónomos en sistemas subautónomos y reducir el peering de malla completa.
Perfiles de amortiguación	**BGP** > **Advanced (Avanzado) (cont.)**	La amortiguación de ruta es un método que determina si se suprime el anuncio de una ruta a causa de fluctuaciones. La amortiguación de ruta puede reducir el número de veces que los enrutadores se ven obligados a converger debido a las fluctuaciones de las rutas. Entre los parámetros se incluyen: • **Profile Name**: introduzca un nombre para identificar el perfil. • **Enable**: activa el perfil. • **Cutoff (Corte)**: especifique un umbral retirada de ruta por encima del cual, se suprime un anuncio de ruta (intervalo 0,0-1.000,0; opción predefinida 1,25). • **Reuse (Reutilizar)**: especifique un umbral de retirada de ruta por debajo del cual una ruta suprimida se vuelve a utilizar (intervalo 0,0-1.000,0; opción predeterminada 5). • **Max. Hold Time (Máx. de tiempo de espera)**: especifique el tiempo máximo, en segundos, durante el que una ruta se puede suprimir, con independencia de su inestabilidad (intervalo 0-3.600; opción predeterminada 900). • **Decay Half Life Reachable (Media vida de disminución alcanzable)**: especifica el tiempo, en segundos, después del cual la métrica de estabilidad de una ruta se divide en dos si el cortafuegos considera que la ruta es alcanzable (intervalo 0-3.600; el predeterminado es 300). • **Decay Half Life Unreachable (Media vida de disminución no alcanzable)**: especifica el tiempo, en segundos, después del cual la métrica de estabilidad de una ruta se divide en dos si el cortafuegos considera que la ruta no es alcanzable (intervalo 0-3.600; el predeterminado es 300). Eliminar (⊖) perfiles cuando ya no los necesite.

© 2020 Palo Alto Networks, Inc.

Pestaña Grupo del peer de BGP

- Network > Virtual Router > BGP > Peer Group

Un grupo del peer de BGP es una colección de peers de BGP que comparten configuraciones, como el tipo de grupo del peer (EBGP, por ejemplo) o la configuración para eliminar números AS privados de la lista AS_PATH que el enrutador virtual envía en paquetes de actualización. Los grupos del peer de BGP evitan tener que configurar varios peers con la misma configuración. Debe configurar al menos un grupo del peer de BGP para configurar los peers de BGP que pertenecen al grupo.

Configuración del grupo del peer de BGP	Configurado en	Description (Descripción)
Nombre	**BGP** > **Peer Group (Grupo del peer)**	Introduzca un nombre para identificar el grupo del peer.
Habilitación		Seleccione para activar el grupo del peer.
Aggregated Confed AS Path		Seleccione para incluir una ruta a la AS de confederación agregada configurada.
Restablecimiento parcial con información almacenada		Seleccione para ejecutar un restablecimiento parcial del cortafuegos después de actualizar los ajustes del peer.

Tipo		Especifique el tipo o grupo de peer y configure los ajustes asociados (consulte la tabla siguiente para ver las descripciones de **Import Next Hop (Importar siguiente salto)** y **Export Next Hop (Exportar siguiente salto)**).
		• **IBGP**: especifique lo siguiente:
		  • **Exportar siguiente salto**
		• **EBGP Confed (EBGP confederado)**: especifique lo siguiente:
		  • **Exportar siguiente salto**
		• **IBGP Confed (IBGP confederado)**: especifique lo siguiente:
		  • **Exportar siguiente salto**
		• **EBGP**: Especifique lo siguiente:
		  • **Importar siguiente salto**
		  • **Exportar siguiente salto**
		  • **Remove Private AS (Eliminar AS privado)** (seleccione si desea forzar que BGP elimine números AS privados del atributo AS_PATH).

Importar siguiente salto		Seleccione una opción para importar el siguiente salto: • **Original**: Utilice la dirección del siguiente salto proporcionado en el anuncio de la ruta original. • **Use Peer (Utilizar peer)**: Utilice la dirección IP del peer como la dirección del siguiente salto.

© 2020 Palo Alto Networks, Inc.

Configuración del grupo del peer de BGP	Configurado en	Description (Descripción)
Exportar siguiente salto		Seleccione una opción para exportar el siguiente salto: • **Resolve (Resolver)**: Resuelve la dirección del siguiente salto mediante la base de información de reenvío (FIB). • **Original**: Utilice la dirección del siguiente salto proporcionado en el anuncio de la ruta original. • **Use Self (Utilizar automático)**: Sustituya la dirección del siguiente salto con la dirección IP del enrutador virtual para garantizar que estará en la ruta de reenvío.
Eliminar AS privado		Seleccione para eliminar sistemas autónomos privados de la lista AS_PATH.
Nombre	**BGP** > **Peer Group (Grupo del peer)** > **Peer (Peer)**	Agrega un **New (Nuevo)** peer de BGP y escriba un nombre para identificarlo.
Habilitación		Seleccione para activar el peer.
As del peer		Especifique el sistema autónomo (AS) del peer.
Activar extensiones MP-BGP	**BGP** > **Peer Group (Grupo del peer)** > **Peer (Peer)** > **Addressing (Direccionamiento)**	Permite que el cortafuegos admita el identificador de familia de direcciones BGP multiprotocolo para IPv4 e IPv6 y las opciones posteriores del identificador de familia de direcciones por RFC 4760.
Tipo de familia de dirección		Seleccione la familia de direcciones **IPv4** o **IPv6** que las sesiones de BGP con este peer admitirá.
Subsequent Address Family		Seleccione el protocolo de familia de direcciones sucesivo **Unicast (Unidifusión)** o **Multicast (Multidifusión)** que las sesiones de BGP con este peer llevarán.
Local Address —Interface		Seleccione una interfaz de cortafuegos.
Local Address —IP		Seleccione una dirección IP local.
Dirección del peer: tipo y dirección		Seleccione el tipo de dirección que identifique al peer: • **IP**: seleccione la IP y seleccione un objeto de dirección que utilice una dirección IP (o cree un nuevo objeto de dirección que utilice una dirección IP). • **FQDN**: seleccione FQDN y un objeto de dirección que utilice un FQDN (o cree un nuevo objeto de dirección que utilice un FQDN).
Perfil de autenticación	**BGP** > **Peer Group (Grupo del peer)** >	Seleccione un perfil o seleccione **Nuevo perfil de Auth (Nuevo perfil de autenticación)** desde el menú desplegable. Introduzca un

© 2020 Palo Alto Networks, Inc.

Configuración del grupo del peer de BGP	Configurado en	Description (Descripción)
	Peer (Peer) > **Connection Options (Opciones de conexión)**	**Name (Nombre)** de perfil y el **Secret (Secreto)**, y **Confirm Secret (Confirmar el secreto)**.
Keep Alive Interval		Especifique un intervalo después del cual las rutas de un peer se supriman según el parámetro de tiempo de espera (intervalo 0-1.200 segundos; opción predeterminada 30 segundos).
Multi Hop		Defina el valor del tiempo de vida (TTL) en el encabezado IP. El intervalo es de 0 a 255. El valor predeterminado de 0 significa 1 para iBGP; 255 para iBGP.
Open Delay Time		Especifique el tiempo de retraso entre la apertura de la conexión TCP del peer y el envío del primer mensaje abierto de BGP (intervalo de 0 a 240 segundos; el valor predeterminado es de 0 segundos).
Hold Time		Especifique el período de tiempo que puede transcurrir entre mensajes KEEPALIVE o UPDATE sucesivos de un peer antes de cerrar la conexión del peer (el intervalo es de 3 a 3600 segundos; el valor predeterminado es de 90 segundos).
Idle Hold Time		Especifique el tiempo de espera en estado de inactividad antes de volver a intentar la conexión con el peer (el intervalo es de 1 a 3600 segundos; el valor predeterminado es de 15 segundos).
Incoming Connections—Remote Port		Especifique el número de puerto entrante, **Allow (Permitir)** tráfico a este puerto.
Outgoing Connections—Local Port		Especifique el número de puerto saliente, **Allow (Permitir)** tráfico desde este puerto
Reflector Client	**BGP** > **Peer Group (Grupo del peer)** > **Peer (Peer)** > **Advanced (Avanzado)**	Seleccione el tipo de cliente reflector (**Non-Client (No cliente)**, **Client (Cliente)** o **Meshed Client (Cliente en malla)**). Las rutas que se reciben de los clientes reflector se comparten con todos los peers BGP internos y externos.
Peering Type		Especifique un peer bilateral o déjelo sin especificar.
Max. Prefixes		Especifique el número máximo de prefijos de IP compatibles (de 1 a 100 000 o ilimitado).
Habilitar detección de bucle en el lado del remitente		Habilite para que el cortafuegos compruebe 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 lo es, el cortafuegos lo elimina para evitar un bucle. Por lo general, el receptor realiza la detección de bucle, pero esta función de optimización hace que la detección de bucle lo realice el remitente.

© 2020 Palo Alto Networks, Inc.

Configuración del grupo del peer de BGP	Configurado en	Description (Descripción)
BFD		Para habilitar la detección de reenvío bidireccional (BFD) para el peer del BGP (y por lo tanto sobrescribir la configuración **BFD** para BGP, siempre que **BFD** no esté deshabilitado para BGP a nivel del enrutador virtual), seleccione el perfil por defecto (configuración BFD predeterminada), un perfil BFD existente, **Inherit-vr-global-setting (Heredar ajuste global de rv)** para heredar el perfil BFD global de BGP, o **New BFD Profile (Nuevo perfil BFD)** para crear un perfil BFD nuevo. **Disable BFD (Deshabilitar BFD)** deshabilita BFD para 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 reconvergencia que afecta el tráfico de producción. Por lo tanto, habilite BFD en las interfaces BGP durante un horario de menor demanda, cuando la reconvergencia no impacte el tráfico de producción.*

Pestañas Importar y Exportar de BGP

- Network > Virtual Router > BGP > Import
- Network > Virtual Router > BGP > Export

Haga clic para **Add (Añadir)** una nueva regla de importación o exportación para importar o exportar rutas BGP.

Configuración de importación y exportación de BGP	Configurado en	Description (Descripción)
Reglas	**BGP** > **Import or Export (Importar o Exportar)** > **General (General)**	Especifique un nombre para identificar la regla.
Habilitación		Seleccione para activar la regla.
Utilizado por		Seleccione los grupos de peer que utilizarán esta regla.
Expresión regular de ruta AS	**BGP** > **Import or Export (Importar o Exportar)** >	Especifique una expresión regular para el filtrado de rutas AS.

© 2020 Palo Alto Networks, Inc.

Configuración de importación y exportación de BGP	Configurado en	Description (Descripción)
Expresión regular de la comunidad	**Match (Coincidencia)**	Especifique una expresión regular para el filtrado de cadenas de comunidad.
Expresión regular de comunidad extendida		Especifique una expresión regular para el filtrado de cadenas de comunidad extendidas.
MED		Especifique un valor de Discriminador de salida múltiple para el filtrado de rutas en el rango 0-4.294.967.295.
Tabla de enrutamiento		Para una **Import Rule (Regla de importación)**, especifique en qué tabla de ruta se importarán las rutas coincidentes: **unicast (unidifusión)**, **multicast (multidifusión)** o **both (ambas)**. Para una **Export Rule (Regla de exportación)**, especifique en qué tabla de ruta se exportarán las rutas coincidentes: **unicast (unidifusión)**, **multicast (multidifusión)** o **both (ambas)**.
Prefijo de dirección		Especifique direcciones o prefijos IP para el filtrado de rutas.
siguiente salto		Especifique los enrutadores o subredes de siguiente salto para el filtrado de rutas.
Del peer		Especifique los enrutadores de peer para el filtrado de la ruta.
Acción	**BGP** > **Import or Export (Importar o Exportar)** > **Action (Acción)**	Action: Especifique una acción (**Allow (Permitir)** o **Deny (Denegar)**) que se realizará cuando se cumplan las condiciones especificadas.
Dampening		Especifique un parámetro de amortiguación, únicamente si la acción es **Allow (Permitir)**.
Local Preference		Especifique un valor de preferencia local únicamente si la acción es **Allow (Permitir)**.
MED		Especifique un valor de MED, únicamente si la acción es **Allow (Permitir)** (0- 65.535).
Peso		Especifique un valor de peso, únicamente si la acción es **Allow (Permitir)** (0- 65.535).
siguiente salto		Especifique un enrutador de siguiente salto, únicamente si la acción es **Allow (Permitir)**.
IP Origen		Especifique el tipo de la ruta de la ruta original: IGP, EGP o incompleta, únicamente si la acción es **Allow (Permitir)**.

© 2020 Palo Alto Networks, Inc.

Configuración de importación y exportación de BGP	Configurado en	Description (Descripción)
AS Path Limit		Especifique un límite de ruta AS, únicamente si la acción es **Allow (Permitir)**.
Ruta AS		Especifique una ruta AS: **None (Ninguna)**, **Remove (Eliminar)**, **Prepend (Pretender)**, **Remove and Prepend (Eliminar y Pretender)**, únicamente si la acción es **Allow (Permitir)**.
Comunidad		Especifique una opción de comunidad: **None (Ninguna)**, **Remove All (Eliminar todo)**, **Remove Regex (Eliminar Regex)**, **Append (Adjuntar)** o **Overwrite (Sobrescribir)**,, únicamente si la acción es **Allow (Permitir)**.
Comunidad extendida		Especifique una opción de comunidad: **None (Ninguna)**, **Remove All (Eliminar todo)**, **Remove Regex (Eliminar Regex)**, **Append (Adjuntar)** o **Overwrite (Sobrescribir)**,, únicamente si la acción es **Allow (Permitir)**.
		Haga clic en **Delete (Eliminar)** reglas cuando ya no las necesite o **Clone (Duplicar)** una regla cuando sea apropiado. También puede seleccionar reglas y **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar su orden.

Pestaña Anuncio condicional de BGP

- Network > Virtual Router > BGP > Conditional Adv

La función de anuncio condicional de BGP permite controlar la ruta que se anunciará en caso de que no exista ninguna ruta preferida en la tabla de enrutamiento BGP local (LocRIB), indicando un fallo de peering 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.

Para el anuncio condicional, se configura un filtro No existente que especifica las rutas preferidas (**Address Prefix (Prefijo de dirección)**) Más cualquier otro atributo que identifique la ruta preferida (como AS Path Regular Expression). Si se encuentra una ruta coincidente con el filtro No existe en la tabla de enrutamiento BGP local, solo entonces el cortafuegos permitirá el anuncio de la ruta alternativa (la ruta al otro proveedor no preferido) tal y como se especifica en su filtro de anuncio.

Para configurar el anuncio condicional, seleccione la pestaña **Condicional Adv (Anuncio condicional)** y luego **Add (Añadir)** un anuncio condicional, y configurar los valores descritos en la siguiente tabla.

Configuración de anuncios condicionales de BGP	Configurado en	Description (Descripción)
Política	**BGP** > **Conditional**	Especifique un nombre para esta regla de política de anuncio condicional.

© 2020 Palo Alto Networks, Inc.

Configuración de anuncios condicionales de BGP	Configurado en	Description (Descripción)
Habilitación	**Adv (Anuncio condicional)**	Seleccione para habilitar esta regla de política de publicidad condicional.
Utilizado por		**Add (Añada)** y seleccione los grupos de peer que utilizarán esta regla de política de anuncio condicional.
Non Exist Filter	**BGP** > **Conditional Adv (Anuncio condicional)** > **Non Exist Filters (Filtros no existentes)**	Utilice esta pestaña para especificar el prefijo de la ruta preferida. 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.) **Add (Añadir)** un filtro No existente y Especifique un nombre para identificar este filtro.
Habilitación		Seleccione para activar el filtro No existente.
Expresión regular de ruta AS		Especifique una expresión regular para el filtrado de rutas AS.
Expresión regular de la comunidad		Especifique una expresión regular para el filtrado de cadenas de comunidad.
Expresión regular de comunidad extendida		Especifique una expresión regular para el filtrado de cadenas de comunidad extendidas.
MED		Especifique un valor MED para el filtrado de rutas (el rango es 0-4,294,967,295).
Tabla de enrutamiento		Especifique la tabla de ruta (**unicast (unidifusión)**, **multicast (multidifusión)** o **both (ambos)**) en la que el cortafuegos buscará para ver si la ruta emparejada está presente. Si la ruta coincidente no está presente en esa tabla de rutas, sólo entonces el cortafuegos permitirá el anuncio de la ruta alternativa.
Prefijo de dirección		**Add (Añadir)** el prefijo de la Información de alcance de la capa de red (NLRI) exacto para la(s) ruta(s) preferida(s).
siguiente salto		Especifique enrutadores de siguiente salto o subredes para filtrar la ruta.
Del peer		Especifique los enrutadores de peer para el filtrado de la ruta.
Advertise Filter	**BGP** > **Conditional Adv (Anuncio**	Utilice esta pestaña para especificar el/los prefijo(s) de la ruta en la tabla de enrutamiento Local-RIB que anuncia si la ruta del filtro No existente no está disponible en la tabla de enrutamiento local.

© 2020 Palo Alto Networks, Inc.

Configuración de anuncios condicionales de BGP	Configurado en	Description (Descripción)
	condicional) > **Advertise Filters (Filtros de publicidad)**	Si un prefijo se va a anunciar y no coincide con un filtro No existente, el anuncio se producirá. **Add (Añadir)** un filtro de anuncio y especifique un nombre para identificar este filtro.
Habilitación		Seleccione para activar el filtro.
Expresión regular de ruta AS		Especifique una expresión regular para el filtrado de rutas AS.
Expresión regular de la comunidad		Especifique una expresión regular para el filtrado de cadenas de comunidad.
Expresión regular de comunidad extendida		Especifique una expresión regular para el filtrado de cadenas de comunidad extendidas.
MED		Especifique un valor MED para el filtrado de rutas (el rango es 0-4,294,967,295).
Tabla de enrutamiento		Especifique la tabla de rutas que el cortafuegos usa cuando se va a publicar condicionalmente una ruta coincidente: **unicast (unidifusión)**, **multidifusión (multidifusión)**, o **both (ambas)**.
Prefijo de dirección		**Add (Añadir)** el prefijo de la Información de alcance de la capa de red (NLRI) exacto para la ruta que se va a anunciar si la ruta preferida no está disponible.
siguiente salto		Especifique los enrutadores o subredes del siguiente salto para el filtrado de rutas.
Del peer		Especifique los enrutadores de peer para el filtrado de la ruta.

Pestaña Agregado de BGP

- Network > Virtual Router > BGP > Aggregate

La agregación de rutas es el acto de combinar rutas específicas (aquellas con una longitud de prefijo más larga) en una ruta única (con una longitud de prefijo más corta) para reducir los anuncios de enrutamiento que el cortafuegos debe enviar y tener menos rutas en la tabla de rutas.

© 2020 Palo Alto Networks, Inc.

Configuración de BGP Aggregate	Configurado en	Description (Descripción)
Nombre	**BGP** > **Aggregate (Agregado)**	Introduzca un nombre para la regla de agregación.
Prefijo		Introduzca un prefijo de resumen (dirección IP / longitud de prefijo) que se utilizará para agregar los prefijos más largos.
Habilitación		Seleccione esta opción para habilitar esta agregación de rutas.
Resumen		Seleccione para resumir las rutas.
Conjunto AS		Seleccione esta opción para que el cortafuegos, para esta regla de agregación, incluya el conjunto de números AS (AS Set) en la ruta AS de la ruta agregada. El conjunto AS es la lista desordenada de los números AS de origen de las rutas individuales que se agregan.
Nombre	**BGP** > **Aggregate (Agregado)** > **Suppress Filters (Filtros de supresión)**	Defina los atributos que harán que las rutas coincidentes se supriman. **Add (Añada)** y escriba un nombre para un filtro de supresión.
Habilitación		Seleccione esta opción para habilitar el Filtro de supresión.
Expresión regular de ruta AS		Especifique una expresión regular para AS_PATH para filtrar qué rutas se agregarán, por ejemplo, ^ 5000 significa rutas aprendidas de AS 5000.
Expresión regular de la comunidad		Especifique una expresión regular para que las comunidades filtran qué rutas se agregarán, por ejemplo, 500:. * coincide con comunidades con 500: x.
Expresión regular de comunidad extendida		Especifique una expresión regular para comunidades extendidas para filtrar qué rutas se agregarán.
MED		Especifique el MED que filtrará qué rutas se agregarán.
Tabla de enrutamiento		Especifique qué tabla de rutas utilizar para las rutas agregadas que se deben suprimir (no anunciadas): **unicast (unidifusión)**, **multidifusión (multidifusión)**, o **both (ambas)**.
Prefijo de dirección		Introduzca la dirección IP que desea suprimir del anuncio.
siguiente salto		Introduzca la siguiente dirección de salto del prefijo BGP que desea suprimir.
Del peer		Introduzca la dirección IP del peer desde el que se recibió el prefijo BGP (que desea suprimir).
Nombre	**BGP** > **Aggregate**	Defina los atributos de un filtro de publicidad que hace que el cortafuegos anuncie a los peers cualquier ruta que coincida con el

© 2020 Palo Alto Networks, Inc.

Configuración de BGP Aggregate	Configurado en	Description (Descripción)
	(Agregado) > Advertise Filters (Filtros de publicidad)	filtro. Haga clic en **Add (Añadir)** e introduzca un nombre para el filtro de publicidad.
Habilitación		Seleccione esta opción para activar este filtro de publicidad.
Expresión regular de ruta AS		Especifique una expresión regular para AS_PATH para filtrar qué rutas se anunciarán.
Expresión regular de la comunidad		Especifique una expresión regular para que Comunidad filtre las rutas que se anunciarán.
Expresión regular de comunidad extendida		Especifique una expresión regular para que Comunidad extendida filtre qué rutas se anunciarán.
MED		Especifique un valor MED para filtrar qué rutas se anunciarán.
Tabla de enrutamiento		Especifique qué tabla de rutas utilizar para un filtro de publicidad de rutas agregadas: **unicast (unidifusión)**, **multidifusión (multidifusión)**, o **both (ambas)**.
Prefijo de dirección		Introduzca una dirección IP que desea que BGP anuncie.
siguiente salto		Introduzca la dirección de siguiente salto de la dirección IP que desea que BGP anuncie.
Del peer		Introduzca la dirección IP del peer desde el que se recibió el prefijo, que desea que BGP anuncie.
	BGP > Aggregate (Agregado) > Aggregate Route Attributes (Atributos de rutas agregadas)	Defina los atributos de la ruta agregada.
Local Preference		Preferencia local en el rango 0-4,294,967,295.
MED		Discriminador de salida múltiple en el rango 0 - 4.294.967.295.
Peso		Peso en el rango 0-65.535.
siguiente salto		Dirección IP del siguiente salto
IP Origen		Set Origin (Establecer origen); el origen de la ruta: **igp**, **egp**, or **incomplete (incompleto)**.
AS Path Limit		Límite de ruta AS en el rango 1-255.
Ruta AS		Seleccionar tipo: **None (Ninguno)** o **Prepend (Preceder)**.

© 2020 Palo Alto Networks, Inc.

Configuración de BGP Aggregate	Configurado en	Description (Descripción)
Comunidad		Seleccionar tipo: **None (Ninguna)**, **Remove All (Eliminar todo)**, **Remove Regex (Quitar Regex)**, **Append (Adjuntar)** o **Overwrite (Sobrescribir)**.
Comunidad extendida		Seleccionar tipo: **None (Ninguna)**, **Remove All (Eliminar todo)**, **Remove Regex (Quitar Regex)**, **Append (Adjuntar)** o **Overwrite (Sobrescribir)**.

Pestaña Reglas de redistribución de BGP

- Network > Virtual Router > BGP > Redist Rules

Configure los ajustes descritos en la siguiente tabla para crear reglas para la redistribución de rutas BGP.

Configuración de reglas de redistribución BGP	Configurado en	Description (Descripción)
Permitir redistribución de ruta predeterminada	**BGP** > **Redist Rules (Reglas de redistr.)**	Permite que el cortafuegos redistribuya su ruta predefinida a los peers del BGP.
Nombre		**Add (Añade)** una subred IP o primero crea un regla de redistribución.
Habilitación		Seleccione esta opción para habilitar esta regla de redistribución.
Tabla de enrutamiento		Especifique en qué tabla de ruta se redistribuirá la ruta: **unicast (unidifusión)**, **multidifusión (multidifusión)**, o **both (ambas)**.
Métrica		Introduzca una métrica en el rango 1-65.535.
Establecer origen		Seleccione el origen de la ruta redistribuida (**Igp**, **Egp** o **incomplete (incompleto)**). El valor **incomplete (incompleto)** indica una ruta conectada.
Establecer MED		Introduzca un MED para la ruta redistribuida en el rango 0-4.294.967.295.
Establecer preferencia local		Introduzca una preferencia local para la ruta redistribuida en el rango 0-4.294.967.295.
Establecer límite de rutas AS		Introduzca un límite de ruta AS para la ruta redistribuida en el rango 1-255.

© 2020 Palo Alto Networks, Inc.

Configuración de reglas de redistribución BGP	Configurado en	Description (Descripción)
Establecer comunidad		Seleccione o introduzca un valor de 32 bits en formato decimal o hexadecimal o formato AS:VAL en el que AS y VAL estén dentro del intervalo 0 - 65.535. Introduzca un máximo de 10 comunidades.
Establecer comunidad extendida		Introduzca un valor de 64 bits en 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 comunidades extendidas.

IP de multidifusión

- Network > Virtual Router > Multicast

La configuración de protocolos de multidifusión necesita que se configuren los siguientes ajustes estándar:

Configuración de Multicast	Description (Descripción)
Habilitación	Seleccione esta opción para habilitar el enrutamiento de multidifusión.

Además, se deben configurar ajustes en las siguientes pestañas:

- **Rendezvous Point (Punto de encuentro)**: Consulte Pestaña Punto de encuentro multidifusión.
- **Interfaces**: Consulte Pestaña Interfaces de multidifusión.
- **SPT Threshold (Umbral SPT)**: Consulte Pestaña de umbral SPT de multidifusión.
- **Espacio de dirección de origen específico**: Consulte Pestaña de dirección de multidifusión de origen específico.
- **Advanced (Avanzado)**: Consulte Pestaña avanzada de multidifusión.

Pestaña Punto de encuentro multidifusión

- Network > Virtual Router > Multicast > Rendezvous Point

Utilice los siguientes campos para configurar un punto de encuentro de multidifusión de IP:

Configuración de Multicast: Rendezvous Point	Description (Descripción)
Tipo de RP	Seleccione el tipo de punto de encuentro (RP, por sus siglas en inglés) que se ejecutará en este enrutador virtual. Se debe configurar un RP estático de forma explícita en otros enrutadores PIM, mientras que se elige automáticamente un RP candidato. • **None (Ninguno)**: seleccione esta opción si no hay ningún RP ejecutándose en este enrutador virtual. • **Static (Estática)**: especifique una dirección IP estática para el RP y seleccione las opciones de **RP Interface (Interfaz de RP)** y **RP Address**

© 2020 Palo Alto Networks, Inc.

Configuración de Multicast: Rendezvous Point	Description (Descripción)

	(Dirección de RP) en las listas desplegables. Seleccione **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)** si desea utilizar el RP especificado del RP elegido para este grupo.
	• **Candidate (Candidato)**: especifique la siguiente información para el candidato del RP que se ejecuta en este enrutador virtual:
	  • **RP Interface (RP Interface (Interfaz de RP))**: seleccione una interfaz para el RP. Los tipos de interfaz válidos incluyen loopback, L3, VLAN, Ethernet agregada y túnel.
	  • **RP Address (Dirección de RP)**: seleccione una dirección IP para el RP.
	  • **Priority (Prioridad)**: especifique una prioridad para los mensajes de RP candidato (opción predefinida 192).
	  • **Advertisement interval (Intervalo de anuncio)**: especifique un intervalo entre anuncios para mensajes RP candidatos.
	• **Group list (Lista de grupo)**: si selecciona **Static (Estática)** o **Candidate (Candidata)**, haga clic en **Add (Añadir)** para especificar una lista de grupos en los que este RP candidato se propone para ser el RP.

Punto de encuentro remoto	Haga clic en **Add (Añadir)** y especifique la siguiente información: • **IP address (Dirección IP)**: especifique la dirección IP del RP. • **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)**: seleccione esta opción si desea utilizar el RP especificado del RP elegido para este grupo. • **Group (Grupo)**: especifique una lista de grupos en los que la dirección especificada actuará como RP.

Pestaña Interfaces de multidifusión

- Network > Virtual Router > Multicast > Interfaces

Utilice los siguientes campos para configurar interfaces de multidifusión que compartan ajustes de IGMP, de PIM y permisos de grupo:

Configuración de Multicast en Interfaces	Description (Descripción)
Nombre	Introduzca un nombre para identificar un grupo de interfaces.
Description (Descripción)	Introduzca una descripción opcional.
Interface (Interfaz)	Haga clic en **Add (Añadir)** para añadir una o más interfaces del cortafuegos que pertenezcan al grupo de interfaces y compartan permisos de grupo de multidifusión, ajustes IGMP y ajustes de PIM.
Permisos de grupos	Especifique grupos de multidifusión que participen en multidifusión de cualquier origen (Any-Source Multicast, ASM) de PIM o multidifusión de origen específico (Source-Specific Multicast, SSM) de PIM:

© 2020 Palo Alto Networks, Inc.

Configuración de Multicast en Interfaces	Description (Descripción)
	• **Any Source (Cualquier origen)**: haga clic en **Add (Añadir)** para añadir un **Name (Nombre)** para identificar un **Group (Grupo)** de multidifusión con permiso para recibir tráfico de multidifusión de cualquier origen en las interfaces del grupo de interfaces. De manera predeterminada, el grupo tiene la opción **Included (Incluido)** en la lista **Any Source (Cualquier origen)**. Anule la selección de **Included (Incluido)** para excluir con facilidad un grupo sin eliminarlo de la configuración del grupo. • **Source Specific (Origen específico)**: haga clic en **Add (Añadir)** para añadir un **Name (Nombre)** para un par de **Group (Grupo)** y dirección IP de **Source (Origen)** para el cual el tráfico multidifusión está permitido en las interfaces del grupo de interfaces. De manera predeterminada, el par de grupo y origen tiene la opción **Included (Incluido)** en la lista Source Specific (Origen específico). Anule la selección de **Included (Incluido)** para excluir con facilidar un par de grupo y origen sin eliminar la configuración.

IGMP	Especifique la configuración para el tráfico de IGMP. La opción IGMP debe estar habilitada para las interfaces de multidifusión orientadas al receptor.
	• **Enable (Habilitar)**: active esta opción para activar la configuración IGMP.
	• **IGMP Version (Versión IGMP)**: seleccione la versión 1, 2 o 3 que se ejecutará en la interfaz.
	• **Enforce Router-Alert IP Option (Aplicar opción de IP de enrutador-alerta)**: seleccione esta opción para solicitar la opción IP de alerta de enrutador cuando se comunique mediante IGMPv2 o IGMPv3. Esta opción se debe deshabilitar para su compatibilidad con IGMPv1.
	• **Robustness (Robustez)**: seleccione un valor entero para las cuentas de pérdida de paquete en una red (el intervalo es de 1 a 7; el valor predeterminado es 2). Si la pérdida del paquete es común, seleccione un valor mayor.
	• **Max Sources (Máx. de pertenencias de origen)**: especifique el número máximo de pertenencias de origen específico permitido en este grupo de interfaces (el intervalo es de 1 a 65 535 o **unlimited [ilimitado]**).
	• **Max Groups (Máx. de grupos)**: especifique el número máximo de grupos de multidifusión permitido en este grupo de interfaces (el intervalo es de 1 a 65 535 o **unlimited [ilimitado]**).
	• **Query Configuration (Configuración de consultas)**: especifique lo siguiente:
	  • **Query interval (Intervalo de consulta)**: especifique el intervalo con el que se envian las consultas generales a todos los receptores.
	  • **Max Query Response Time (Máx. de tiempo de respuesta de consulta)**: especifique el tiempo máximo entre una consulta general y una respuesta de un receptor.
	  • **Last Member Query Interval (Último intervalo de consulta de miembro)**:especifique el intervalo entre los mensajes de consulta entre grupos o de origen específico (incluidos los enviados en respuesta a los mensajes salientes del grupo).
	  • **Immediate Leave (Salida inmediata)**: seleccione esta opción para salir del grupo inmediatamente cuando reciba un mensaje de salida.

© 2020 Palo Alto Networks, Inc.

Configuración de Multicast en Interfaces	Description (Descripción)
Configuración PIM	Especifique los siguientes ajustes de Multidifusión independiente de protocolo (Protocol Independent Multicast, PIM): • **Enable (Habilitar)**: seleccione esta opción para permitir que esta interfaz reciba o reenvíe mensajes PIM Debe permitir que una interfaz reenvíe tráfico de multidifusión. • **Assert Interval (Imponer intervalo)**: especifique el intervalo entre mensajes de imposición de PIM para seleccionar un responsable de reenvío de PIM. • **Hello Interval (Intervalo de saludo)**: especifique el intervalo entre mensajes de saludo de PIM. • **Join Prune Interval (Intervalo de unión/reducción)**: especifique el número de segundos entre mensajes de unión de PIM (y entre mensajes de reducción de PIM). El valor predeterminado es 60. • **DR Priority (Prioridad de DR)**: especifique la prioridad del enrutador designado para esta interfaz. • **BSR Border (Borde de BSR)**: seleccione esta opción para utilizar la interfaz como borde de arranque. • **PIM Neighbors (Vecinos PIM)**: haga clic en **Add (Añadir)** para añadir la lista de vecinos que se comunicarán mediante PIM.

Pestaña de umbral SPT de multidifusión

- Network > Virtual Router > Multicast > SPT Threshold

El umbral del árbol de la ruta más corta (Shortest Path Tree, SPT) define el punto en el cual el enrutador virtual cambia el enrutamiento de multidifusión de un grupo o prefijo de multidifusión de la distribución de árbol compartido (que proviene del punto de encuentro) a la distribución de árbol de origen (también conocido como el árbol de la ruta más corta o SPT). Haga clic en **Add (Añadir)** para añadir un umbral de SPT para un grupo o prefijo de multidifusión.

Umbral SPT	Description (Descripción)
Grupo/prefijo de multidifusión	Especifique la dirección o el prefijo de multidifusión por el cual el enrutamiento de multidifusión cambia a distribución de SPT cuando el rendimiento del grupo o prefijo alcanza la configuración del umbral.
Threshold (Umbral) (kbps)	Seleccione un ajuste para especificar el punto en el cual el enrutamiento de multidifusión cambia a distribución de SPT en el grupo o prefijo de multidifusión correspondiente: • **0 (cambiar en el primer paquete de datos)** (predeterminado): cuando un paquete de multidifusión para el grupo o prefijo llega, el enrutador virtual cambia a distribución de SPT. • **never (nunca) (no cambiar a SPT):** el enrutador virtual continúa reenviando tráfico de multidifusión a este grupo o prefijo a través del árbol compartido. • Introduzca el número total de kilobits de paquetes de multidifusión que pueden llegar del grupo o prefijo de multidifusión correspondiente en cualquier interfaz y durante un período de tiempo (el intervalo es de

© 2020 Palo Alto Networks, Inc.

Umbral SPT	Description (Descripción)
	1 a 4 294 967 295). Cuando el rendimiento alcanza este número, el enrutador virtual cambia a una distribución de SPT.

Pestaña de espacio de dirección de multidifusión de origen específico

- Network > Virtual Router > Multicast > Source Specific Address Space

Haga clic en **Add** (Añadir) para añadir los grupos de multidifusión que pueden recibir paquetes de multidifusión únicamente desde una fuente específica. Son los mismos grupos y nombres de multidifusión que específico en la pestaña **Multicast (Multidifusión)** > **Interfaces (Interfaces)** > **Group Permissions (Permisos de grupo)**.

Configuración multidifusión: Espacio de dirección de origen específico	Description (Descripción)
Nombre	Identifique un grupo de multidifusión al que el cortafuegos proporcionará servicios de multidifusión de origen específico (SSM).
Grupo	Especifique una dirección de grupo de multidifusión que pueda aceptar paquetes de multidifusión únicamente desde una fuente específica.
Incluido	Seleccione esta opción para incluir el grupo especificados en el espacio de dirección de SSM.

Pestaña avanzada de multidifusión

- Network > Virtual Router > Multicast > Advanced

Configure la duración de tiempo que una ruta de multidifusión permanece en la tabla de enrutamiento una vez finalizada la sesión.

Configuración de Multicast Advanced	Description (Descripción)
Expiración de tiempo de ruta (segundos)	Le permite ajustar la duración, en segundos, para la cual una ruta multicast permanece en la tabla de rutas en el cortafuegos luego de que la sesión finaliza (el intervalo es 210-7200; el predeterminado es 210).

ECMP

- Network > Virtual Routers > Router Settings > 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

© 2020 Palo Alto Networks, Inc.

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 el ancho de banda disponible en todos los 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 esperar a que el protocolo de enrutamiento o la tabla RIB seleccione una ruta alternativa, que puede ayudar a reducir el tiempo de interrupción cuando falla un enlace..

El equilibrio de carga de ECMP se realiza a nivel de sesión, no a nivel de paquete. Esto significa que el cortafuegos selecciona una ruta de igual coste al principio de una nueva sesión, no cada vez que el cortafuegos recibe un paquete.

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.

Para configurar ECMP para un enrutador virtual, seleccione un enrutador virtual y, en **Router Settings (Configuración de enrutador)**, seleccione la pestaña **ECMP** y configure la Configuración de ECMP tal y como se describe:

¿Qué está buscando?	Consulte:
¿Cuáles son los campos disponibles para configurar ECMP?	Configuración de ECMP
¿Busca más información?	ECMP

Configuración de ECMP

- Network > Virtual Routers > Router Settings > ECMP

Utilice los siguientes campos para configurar los ajustes de varias trayectorias a igual coste

Configuración de ECMP	Description (Descripción)
Habilitación	**Enable (Habilitar)** ECMP. *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.*
Retorno simétrico	(Opcional) 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, el cortafuegos usará la interfaz de entrada a la que enviar los paquetes de retorno, en lugar de usar la interfaz ECMP, de modo que el ajuste **Symmetric Return (Retorno simétrico)** sobrescribe el equilibrio de cargas. Este comportamiento solo se produce con flujos de tráfico del servidor al cliente.

© 2020 Palo Alto Networks, Inc.

Configuración de ECMP	Description (Descripción)
Ruta máx.	Seleccione el número máximo de rutas a igual coste: (2, 3 o 4) a una red de destino que puede copiarse del RIB al FIB. El valor predeterminado es 2.

Método	Seleccione uno de los siguientes algoritmos de equilibrio de carga de ECMP para usarlo en el enrutador virtual. El equilibrio de carga de ECMP se realiza a nivel de sesión, no a nivel de paquete. Esto significa que el cortafuegos (ECMP) selecciona una ruta de igual coste al principio de una nueva sesión, no cada vez que se recibe un paquete.
	• **IP Module (Módulo IP)**: Por defecto, el enrutador virtual equilibra las cargas de sesiones mediante esta opción, que usa un hash de las direcciones IP de origen y destino en el encabezado del paquete para determinar qué ruta ECMP se puede usar.
	• **IP Hash (Hash IP)**: existen dos métodos de hash IP que determinan qué ruta ECMP se utilizará:
	  • Si selecciona **IP Hash (Hash IP)**, de manera predeterminada, el cortafuegos utiliza un hash de las direcciones IP de origen y de destino.
	  • De manera alternativa, puede seleccionar **Use Source Address Only (Utilizar solo la dirección de origen)** (disponible en PAN-OS 8.0.3 y versiones posteriores). Este método de hash IP garantiza que todas las sesiones que pertenecen a la misma dirección IP de origen tomen la misma ruta.
	  • De manera opcional, seleccione **Use Source/Destination Ports (Utilizar puertos de origen/destino)** para incluir los puertos en cualquiera de los cálculos de hash. También puede introducir un valor de **Hash Seed (Valor de inicialización de hash)** (un entero) para aleatorizar aún más el equilibrio de cargas.
	• **Weighted Round Robin (Operación por turnos ponderada)**: Este algoritmo se puede usar para tener en cuenta distintas capacidades y velocidades de enlace. Al seleccionar este algoritmo se abrirá la ventana Interfaz. Haga clic en **Add (Añadir)** y seleccione una **Interface (Interfaz)** para incluirla en el grupo de operación por turnos ponderada. En cada interfaz, escriba el **Weight (Peso)** que se usará para esa interfaz. El campo **Weight (Peso)** es de manera predeterminada 100; el intervalo 1-255. Mientras mayor sea el peso de una ruta de coste igual específica, con más frecuencia se seleccionará esa ruta de igual coste en una nueva sesión. Un enlace de mayor velocidad recibirá un peso más alto que uno más lento, para que haya más tráfico ECMP que atraviese el enlace más rápido. Haga clic en **Add (Añadir)** de nuevo para añadir otra interfaz y peso.
	• **Balanced Round Robin (Operación por turnos equilibrada)**: Distribuye las secciones de ECMP entrantes de forma homogénea entre los enlaces.

Más estadísticas de tiempo de ejecución para un enrutador virtual

Después de configurar rutas estáticas o protocolos de enrutamiento para un enrutador virtual, seleccione **Network (Red)** > **Virtual Routers (Enrutadores)** y seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)** en la última columna para ver información detallada sobre el enrutador virtual, como, por ejemplo, la tabla de rutas, la tabla de reenvío y los protocolos de enrutamiento y rutas estáticas

© 2020 Palo Alto Networks, Inc.

que configuró. Estas ventanas proporcionan más información de la que cabe en una sola pantalla para el enrutador virtual. La ventana muestra las siguientes pestañas:

- **(Routing) Enrutamiento**: Consulte la Pestaña Enrutamiento.
- **RIP**: Consulte la Pestaña RIP.
- **BGP**: Consulte la Pestaña BGP.
- **Multicast (Multidifusión)**: Consulte la Pestaña Multicast.
- **Información de resumen de BFD**: Ver Pestaña Información resumida de BFD.

Pestaña Enrutamiento

La siguiente tabla describe las estadísticas de tiempo de ejecución del enrutador virtual para las tablas Route Table, Forwarding Table y Static Route Monitoring.

Estadísticas de tiempo de ejecución	Description (Descripción)
Tabla de enrutamiento	
Tabla de enrutamiento	Seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar la tabla de rutas de unidifusión o de multidifusión.
Mostrar familia de direcciones	Seleccione **IPv4 Only (Solo IPv4)**, **IPv6 Only (Solo IPv6)** o **IPv4 and IPv6 (IPv4 e IPv6)** (predeterminado) para controlar el grupo de direcciones que se muestra en la tabla.
IP Destino	Máscara de red y dirección IPv4 o dirección IPv6 y longitud de prefijo de redes que puede alcanzar el enrutador virtual.
siguiente salto	Dirección IP del siguiente salto hacia la red de destino. Si el siguiente salto es 0.0.0.0, se indica la ruta predeterminada.
Métrica	Métrica de la ruta. Cuando un protocolo de enrutamiento tiene más de una ruta a la misma red de destino, se prefiere la ruta con el valor métrico más bajo. Cada protocolo de enrutamiento utiliza un tipo de métrica diferente (por ejemplo, RIP utiliza el recuento de saltos).
Peso	Peso de la ruta. Por ejemplo, cuando BGP tiene más de una ruta al mismo destino, preferirá la ruta con mayor peso.
Flags (Marcas)	• **A?B**: Activo y obtenido mediante BGP. • **A C**: Activo y resultado de una interfaz interna (conectada) - Destino = red. • **A H**: Activo y resultado de una interfaz interna (conectada) - Destino = solo host. • **A R**: Activo y obtenido mediante RIP. • **A S**: Activo y estático. • **S**: Inactivo (porque esta ruta tiene una métrica más alta) y estático. • **O1**: OSPF externo tipo 1. • **O2**: OSPF externo tipo 2. • **Oi**: OSPF dentro del área. • **Oo**: OSPF fuera del área.

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución	Description (Descripción)
Edad	Edad de la entrada de la ruta en la tabla de rutas. Las rutas estáticas no tienen edad.
Interface (Interfaz)	Interfaz de salida del enrutador virtual que se utiliza para llegar al siguiente salto.
Actualizar	Haga clic para actualizar las estadísticas de tiempo de ejecución en la tabla.
Tabla de desvío	

El cortafuegos elige la mejor ruta, desde la tabla de enrutamiento (RIB) hacia una red de destino, para colocarla en la FIB.

Mostrar familia de direcciones	Seleccione **IPv4 Only (Solo IPv4)**, **IPv6 Only (Solo IPv6)** o **IPv4 and IPv6 (IPv4 e IPv6)** (predeterminado) para controlar la tabla de enrutamiento que se muestra.
IP Destino	La mejor máscara de red y dirección IPv4 o dirección IPv6 y la longitud del prefijo a una red que el enrutador virtual puede alcanzar, seleccionado de la tabla de enrutamiento.
siguiente salto	Dirección IP del siguiente salto hacia la red de destino. Si el siguiente salto es 0.0.0.0, se indica la ruta predeterminada.
Flags (Marcas)	• **u**: La ruta está activa. • **h**: La ruta es a un host. • **g**: La ruta es a una puerta de enlace. • **e**: El cortafuegos selecciona esta ruta mediante ECMP (Equal Cost Multipath). • *: La ruta es la preferida hacia una red de destino.
Interface (Interfaz)	Interfaz de salida del enrutador virtual que se utiliza para llegar al siguiente salto.
MTU	Unidad máxima de transmisión (MTU); número máximo de bytes que el cortafuegos transmite en un solo paquete TCP a este destino.
Actualizar	Haga clic para actualizar las estadísticas de tiempo de ejecución en la tabla.
Monitorización de ruta estática	
IP Destino	La máscara de red y dirección IPv4 o dirección IPv6 y la longitud del prefijo de una red que el enrutador virtual puede alcanzar.
siguiente salto	Dirección IP del siguiente salto hacia la red de destino. Si el siguiente salto es 0.0.0.0, se indica la ruta predeterminada.
Métrica	Métrica de la ruta. Cuando hay más de una ruta estática a la misma red de destino, el cortafuegos prefiere la ruta con el valor métrico más bajo.
Peso	Peso de la ruta.
Flags (Marcas)	• **A?B**: Activo y obtenido mediante BGP.

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución	Description (Descripción)
	• **A C**: Activo y resultado de una interfaz interna (conectada) - Destino = red. • **A H**: Activo y resultado de una interfaz interna (conectada) - Destino = solo host. • **A R**: Activo y obtenido mediante RIP. • **A S**: Activo y estático. • **S**: Inactivo (porque esta ruta tiene una métrica más alta) y estático. • **O1**: OSPF externo tipo 1. • **O2**: OSPF externo tipo 2. • **Oi**: OSPF dentro del área. • **Oo**: OSPF fuera del área.
Interface (Interfaz)	Interfaz de salida del enrutador virtual que se utiliza para llegar al siguiente salto.
Monitorización de rutas (fallos)	Si la supervisión de rutas está habilitada para esta ruta estática, Fail On puede mostrar: • **All (Todas)**: el cortafuegos considera que la ruta estática está caída y realiza la conmutación por error si todos los destinos supervisados de la ruta estática están caídos. • **Any (Cualquiera)**: el cortafuegos considera que la ruta estática está caída y realiza la conmutación por error si cualquiera de los destinos supervisados de la ruta estática está caído. Si se desactiva la supervisión de rutas de ruta estática, Fail On se muestra **Disabled (Deshabilitado)**.
estado	Estado de la ruta estática basada en pings ICMP a los destinos supervisados: **Up (Activa)**, **Down (Caída)** o la supervisión de rutas para la ruta estática es **Disabled (Deshabilitado)**.
Actualizar	Actualiza las estadísticas de tiempo de ejecución en la tabla.

Pestaña RIP

La siguiente tabla describe las Estadísticas de tiempo de ejecución de RIP del enrutador virtual.

Estadísticas de tiempo de ejecución de RIP	Description (Descripción)
Pestaña Resumen	
Segundos del intervalo	Número de segundos en un intervalo. RIP utiliza este valor (un periodo de tiempo) para controlar sus intervalos de actualización, vencimiento y eliminación.
Intervalo de actualizaciones	Número de intervalos entre las actualizaciones de anuncio de enrutamiento RIP que el enrutador virtual envía a los peer.

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de RIP	Description (Descripción)
Intervalos de vencimiento	Número de intervalos desde que se recibió la última actualización del enrutador virtual de un peer, tras el cual el enrutador virtual marca las rutas del peer como inutilizables.
Intervalo de eliminación	Número de intervalos tras el cual una ruta se marca como inutilizable y tras el cual, si no se recibe ninguna actualización, el cortafuegos elimina la ruta de la tabla de enrutamiento.
Pestaña Interfaces	
Dirección	Dirección IP de una interfaz en el enrutador virtual donde está activado RIP.
Tipo de autenticación	Tipo de autenticación: contraseña simple, MD5 o ninguno.
Enviar permitidos	La marca de verificación indica que esta interfaz tiene permiso para enviar paquetes RIP.
Recibir permitidos	La marca de verificación indica que esta interfaz tiene permiso para recibir paquetes RIP.
Anunciar ruta predeterminada	La marca de verificación indica que RIP anunciará su ruta predeterminada a sus peers.
Métrica de ruta predeterminada	Métrica (recuento de saltos) asignada a la ruta predeterminada. Mientras menor sea el valor métrico más prioridad tendrá en la tabla de enrutamiento para su selección como ruta preferida.
ID de clave	Clave de autenticación usada con los peers.
Preferido	Clave de autenticación preferida.
Pestaña Peer	
Dirección del peer	Dirección IP de un peer hacia la interfaz RIP del enrutador virtual.
Última actualización	Fecha y hora a la que se recibió la última actualización de este peer.
Versión de RIP	Versión RIP que está ejecutando el peer.
Paquetes no válidos	Recuento de paquetes no válidos recibidos de este peer. Posibles causas por las que el cortafuegos no puede procesar el paquete RIP: x bytes por encima del límite de enrutamiento, demasiadas rutas en el paquete, subred incorrecta, dirección ilegal, fallo de autenticación o no hay suficiente memoria.
Rutas no válidas	Recuento de rutas no válidas recibidas de este peer. Causas posibles: ruta no válida, fallo de importación o memoria insuficiente.

© 2020 Palo Alto Networks, Inc.

Pestaña BGP

La siguiente tabla describe las estadísticas de tiempo de ejecución de BGP del enrutador virtual.

Estadísticas de tiempo de ejecución de BGP	Description (Descripción)
Pestaña Resumen	
ID del enrutador	Id de enrutador asignada a la instancia de BGP.
Rechazar ruta por defecto	Indica si se ha configurado la opción Rechazar ruta por defecto, que provoca que VR ignore cualquier ruta predeterminada anunciada por los peers BGP.
Redistribuir ruta por defecto	Indica si se ha configurado la opción Permitir redistribución de ruta predeterminada.
Instalar ruta	Indica si se ha configurado la opción Instalar ruta, que provoca que VR instale las rutas BGP en la tabla de enrutamiento global.
Reinicio correcto	Indica si se ha activado o no Reinicio correcto (asistencia).
Tamaño AS	Indica si el tamaño de Formato AS seleccionado es 2 Byte o 4 Byte.
AS local	Número de AS al que pertenece VR.
AS de miembro local	Número AS de miembro local (solo válido si el VR está en una confederación). El campo será 0 si VR no está en una confederación.
ID de clúster	Muestra el ID de clúster reflector configurado.
Preferencia local predeterminada	Muestra la preferencia local predeterminada configurada para el VR.
Comparar siempre MED	Indica si se ha configurado la opción Comparar siempre MED, que permite comparar entre rutas de vecinos en distintos sistemas autónomos.
Agregar MED independientemente	Indica si se ha configurado la opción Agregar MED, que permite añadir una ruta aunque las rutas tengan valores MED distintos.
Procesamiento determinista de MED	Indica si se ha configurado la opción Comparación determinista de MED, que permite a una comparación elegir entre rutas anunciadas por peers IBGP (peers BGP en el mismo AS).
Entradas salientes de RIB actuales	Número de entradas en la tabla RIB saliente.
Entradas salientes de RIB pico	Número máximo de rutas Adj-RIB-Salida que se han asignado en un momento dado.
Pestaña Peer	

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de BGP	Description (Descripción)
Nombre	Nombre del peer.
Grupo	Nombre del grupo de peers al que pertenece este peer.
IP local	Dirección IP de la interfaz BGP en el VR.
IP del peer	Dirección IP del peer.
As del peer	Sistema autónomo al que pertenece el peer.
Contraseña establecida	Sí o No indica si se ha definido la autenticación.
estado	Estado del peer, p. ej. Activo, Conectar, Establecido, Inactivo, Confirmación abierta o Enviado abierto.
Duración de estado (seg.)	Duración del estado del peer.
Pestaña Grupo del peer	
Nombre de grupo	Nombre del grupo de peers.
Tipo	Tipo del grupo de peers configurados, como EBGP o IBGP.
Agregar AS AS	Sí o No indican si se ha configurado la opción Agregar AS confederado.
Soporte de restablecimiento parcial	Sí o No indica si el grupo de peers admite un restablecimiento parcial. Cuando cambian las políticas de enrutamiento a un peer BGP, las actualizaciones de tabla de enrutamiento pueden verse afectadas. Se recomienda un restablecimiento parcial de las sesiones BGP en lugar de uno completo, el restablecimiento parcial permite que las tablas de enrutamiento se actualicen sin borrar las sesiones BGP.
Próximo salto automático	Sí o No indica si se ha configurado esta opción.
Siguiente salto de tercero	Sí o No indica si se ha configurado esta opción.
Eliminar AS privado	Indica si las actualizaciones eliminarán los números AS privados del atributo AS_PATH antes de que se envíen.
Pestaña RIB local	
Prefijo	Prefijo de red y máscara de subred en la base de información de enrutamiento local.
Marca	* indica que la ruta se seleccionó como la mejor ruta BGP.

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de BGP	Description (Descripción)
siguiente salto	Dirección IP del siguiente salto hasta el prefijo.
Peer	Nombre del peer.
Peso	Atributo de peso asignado al prefijo. Si el cortafuegos tiene más de una ruta hacia el mismo prefijo, la ruta con el peso más alto se instalará en la tabla de enrutamiento de IP.
Preferencia local.	Atributo de preferencia local para la ruta, que se usa para seleccionar el punto de salida hacia el prefijo si hay múltiples puntos de salida. Es preferible una preferencia local más alta en lugar de más baja.
Ruta AS	Lista de sistemas autónomos en la ruta hacia la red Prefijo; la lista se anuncia en las actualizaciones BGP.
IP Origen	Atributo de origen para el prefijo, cómo BGP programó la ruta.
MED	Atributo Discriminador de salida múltiple (MED) de la ruta. El MED es un atributo métrico para una ruta, que el AS que anuncia la ruta sugiere a un AS externo. Se prefiere un MED más bajo antes que uno más alto.
Recuento de flaps	Número de flaps de la ruta.
Pestaña RIB externa	
Prefijo	Entrada de enrutamiento de red en la base de información de enrutamiento.
siguiente salto	Dirección IP del siguiente salto hasta el prefijo.
Peer	Peer al que el VR anunciará esta ruta.
Preferencia local.	Atributo de preferencia local para acceder al prefijo, que se usa para seleccionar el punto de salida hacia el prefijo si hay múltiples puntos de salida. Es preferible una preferencia local más alta en lugar de más baja.
Ruta AS	Lista de sistemas autónomos en la ruta hacia la red de prefijo.
IP Origen	Atributo de origen para el prefijo, cómo BGP programó la ruta.
MED	Atributo Discriminador de salida múltiple (MED) del prefijo. El MED es un atributo métrico para una ruta, que el AS que anuncia la ruta sugiere a un AS externo. Se prefiere un MED más bajo antes que uno más alto.
Anunciar estado	Estado anunciado de la ruta.
Agregar estado	Indica si la ruta se ha agregado con otras rutas.

© 2020 Palo Alto Networks, Inc.

Pestaña Multicast

La siguiente tabla describe las estadísticas de tiempo de ejecución de multidifusión IP del enrutador virtual.

Estadísticas de tiempo de ejecución de multidifusión	Description (Descripción)
Pestaña FIB	
Grupo	La entrada de la ruta en la base de información de reenvío (Forwarding Information Base, FIB); dirección de grupo de multidifusión a la que el enrutador virtual reenviará los paquetes.
Source (Origen)	Dirección de origen de los paquetes de multidifusión para el grupo.
Interfaces entrantes	Interfaces donde llegan los paquetes de multidifusión del grupo.
Interfaces de salida	Interfaces desde las cuales el enrutador virtual reenvía los paquetes de multidifusión del grupo.
Pestaña Interfaz IGMP	
Interface (Interfaz)	Interfaz que tiene activado IGMP.
versión	Versión 1, 2 o 3 del Protocolo de gestión de grupos de Internet (Internet Group Management Protocol, IGMP) que se ejecuta en el enrutador virtual.
Solicitante	Dirección IP del solicitante IGMP en el segmento de multiacceso conectado a la interfaz.
Tiempo de activación del solicitante	Cantidad de segundos que el solicitante IGMP ha estado activo.
Tiempo de vencimiento del solicitante	Cantidad de segundos restantes para que expire el temporizador de presencia de otro solicitante.
Potencia	Potencia variable de la interfaz IGMP.
Límite de grupos	Cantidad máxima de grupos por interfaz que el IGMP puede procesar simultáneamente.
Límite de orígenes	Cantidad máxima de orígenes por interfaz que el IGMP puede procesar simultáneamente.
Salida inmediata	Sí o No indica si se ha configurado la Salida inmediata. Salida inmediata indica que el enrutador virtual eliminará una interfaz de la entrada de tabla de reenvíos sin enviar las consultas específicas de grupo IGMP de la interfaz.
Pestaña Pertenencia IGMP	

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de multidifusión	Description (Descripción)
Interface (Interfaz)	Nombre de la interfaz que pertenece al grupo.
Grupo	Dirección del grupo de multidifusión a la que pertenece la interfaz.
Source (Origen)	Dirección IP de los paquetes de multidifusión que envía el origen al grupo.
Tiempo de activación	Cantidad de segundos que ha estado activa esta pertenencia.
Tiempo de vencimiento	Cantidad de segundos restantes antes de que venza la pertenencia.
Modo de filtro	Incluir o excluir el origen. El enrutador virtual se ha configurado para incluir todo el tráfico o solo el que procede de este origen (incluir), o el tráfico de cualquier origen excepto este (excluir).
Excluir caducidad	Cantidad de segundos restantes hasta que vence el estado Excluir de la interfaz.
Temporizador de host V1	Tiempo restante hasta que el enrutador local asume que no quedan miembros de ningún IGMP versión 1 en la subred de IP adjuntada a la interfaz.
Temporizador de host V2	Tiempo restante hasta que el enrutador local asume que no quedan miembros de ningún IGMP versión 2 en la subred de IP adjuntada a la interfaz.
Pestaña Asignación de grupos PIM	
Grupo	Dirección IP del grupo asignado a un punto de encuentro.
RP	Dirección IP del punto de encuentro del grupo.
IP Origen	Indica la ubicación donde el enrutador virtual detectó el RP.
Modo PIM	ASM o SSM.
Inactivo	Indica si la asignación del grupo al RP está inactiva.
Pestaña Interfaz PIM	
Interface (Interfaz)	Nombre de la interfaz que participa en PIM.
Dirección	Dirección IP de la interfaz.
DR	Dirección IP del enrutador designado en el segmento de multiacceso conectado a la interfaz.
Intervalo de saludo	Intervalo de saludo configurado (en segundos).
Unir/eliminar intervalo	Intervalo configurado para los mensajes de unión y eliminación (en segundos).

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de multidifusión	Description (Descripción)
Imponer intervalo	Intervalo de imposición de PIM configurado (en segundos) para que el enrutador virtual envíe mensajes de imposición. PIM utiliza el mecanismo de imposición para iniciar la elección del reenviador de PIM para la red de multiacceso.
Prioridad de DR	Prioridad configurada para el enrutador designado en el segmento de multiacceso conectado a la interfaz.
Borde de BSR	Las opciones Si o No indican si el interfaz se encuentra en un enrutador virtual que es un enrutador de arranque (bootstrap router, BSR) ubicado en el borde de una LAN empresarial.
Pestaña Vecino PIM	
Interface (Interfaz)	Nombre de la interfaz en el enrutador virtual.
Dirección	Dirección IP del vecino PIM accesible desde la interfaz.
Dirección secundaria	Dirección IP secundaria del vecino PIM accesible desde la interfaz.
Tiempo de activación	Tiempo que el vecino ha estado activado.
Tiempo de vencimiento	Tiempo restante antes de que expire el vecino debido a que el enrutador virtual no recibe paquetes de saludo del vecino.
ID de generación	Valor de 32 bits generado de forma aleatoria que se regenera cada vez que se inicia o reinicia el reenvío de PIM en la interfaz (incluye el reinicio automático el enrutador).
Prioridad de DR	Prioridad de enrutador designado que el enrutador virtual ha recibido en el último mensaje de saludo PIM de este vecino.

Pestaña Información resumida de BFD.

La información resumida de BFD incluye los siguientes datos.

Estadísticas de tiempo de ejecución de la información resumida de BFD	Description (Descripción)
Interface (Interfaz)	Interfaz que está ejecutando BFD.
PROTOCOL	Ruta estática (familia de direcciones IP de ruta estática) o protocolo de enrutamiento dinámico que ejecuta BFD en la interfaz.
Dirección IP local	Dirección IP de la interfaz en la que configuró BFD.

© 2020 Palo Alto Networks, Inc.

Estadísticas de tiempo de ejecución de la información resumida de BFD	Description (Descripción)
Dirección IP vecina	Dirección IP del vecino de BFD.
Estatal o regional	Estados de BFD de los peers de BFD locales y remotos:**Admin down (Adminstrador deshabilitado)**, **down (deshabilitado)**, **init (iniciando)** o **up (habilitado)**.
Uptime	Período de tiempo que BFD estuvo activo (horas, minutos, segundos y milisegundos).
Discriminador (local)	Discriminador para peer local de BFD. Un discriminador es un valor único distinto de cero que los peers utilizan para distinguir varias sesiones BFD entre sí.
Discriminador (remoto)	Discriminador para peers remotos de BFD.
Errores	Cantidad de errores de BFD.
SESSION DETAILS	Haga clic en **Details (Detalles)** para ver la información BFD de una sesión como por ejemplo las direcciones IP de los vecinos locales y remotos, el último código de diagnóstico remoto recibido, el número de paquetes de control transmitidos y recibidos, el número de errores, la información sobre el último paquete que causó el cambio de estado y más.

© 2020 Palo Alto Networks, Inc.

Network > IPSec Tunnels

Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** para establecer y gestionar los túneles VPN IPSec entre los cortafuegos. Esta es la parte de fase 2 de la configuración VPN IKE/IPSec.

¿Qué está buscando?	Consulte:
Gestión de túneles VPN IPSec	Gestión de túnel VPN IPSec
Configuración de un túnel IPSec.	Pestaña General del túnel IPSec
	Pestaña Identificadores proxy de túnel IPSec
Visualización del estado de túnel IPSec	Estado del túnel IPSec en el cortafuegos
Reinicio o actualización de un túnel IPSec.	Reiniciar o actualizar el túnel IPSec
¿Busca más información?	Configuración de un túnel IPSec.

Gestión de túnel VPN IPSec

- Network > IPSec Tunnels

La siguiente tabla describe cómo gestionar sus túneles VPN IPSec.

Campos para la gestión de túneles VPN IPSec	
Añadir	**Add (Añadir)** un nuevo túnel IPSec VPN. Consulte en Pestaña General de IPSec Tunnel las instrucciones sobre la configuración del nuevo túnel.
delete	**Delete (Borrar)** un túnel que ya no necesite.
Habilitación	**Enable (Habilitar)** un túnel que se ha desactivado (los túneles están habilitados de forma predeterminada).
Deshabilitar	**Disable (Deshabilitar)** un túnel que no desea usar, pero que aún no está listo para borrar.
PDF/CSV	Exporte la configuración del túnel IPSec en formato **PDF/CSV**. Es posible aplicar filtros para personalizar el resultado de la tabla e incluir solo las columnas que desea. Únicamente las columnas visibles en el cuadro de diálogo Export (Exportación) se exportan. Consulte Datos de la tabla de configuración de exportación.

Pestaña General del túnel IPSec

- Network > IPSec Tunnels > General

© 2020 Palo Alto Networks, Inc.

Configure un túnel IPSec con estas opciones.

Configuración general de IPSec Tunnel	Description (Descripción)
Nombre	En **Name (Nombre)**, indique un nombre con el que identificar el túnel (hasta 63 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. El límite de 63 caracteres de este campo incluye el nombre del túnel además del ID de proxy, que está separado por dos puntos.
Interfaz túnel	Seleccione una interfaz de túnel existente o haga clic en **New Tunnel Interface (Nueva interfaz de túnel).**. Consulte en Network > Interfaces > Tunnel las instrucciones para crear una interfaz de túnel.
IPv4 o IPv6	Seleccione **IPv4** o **IPv6** para configurar el túnel para tener extremos con ese tipo de dirección IP.
Tipo	Seleccione si se utilizará una clave de seguridad generada automáticamente o introducida manualmente. Se recomienda seleccionar **Auto key (Clave automática)**.
Clave automática	Si selecciona **Auto key (Clave automática)**, especifique lo siguiente: • **IKE Gateway (Puerta de enlace de IKE)**: consulte Network > Network Profiles > IKE Gateways para obtener descripciones de la configuración de puertas de enlace IKE. • **IPSec Crypto Profile (Perfil criptográfico IPSec)**: Seleccione un perfil existente o mantenga el perfil predeterminado. Para definir un perfil nuevo , haga clic en **New (Nuevo)** y siga las instrucciones de Network > Network Profiles > IPSec Crypto. • Haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** para acceder a los campos restantes. • **Enable Replay Protection (Habilitar protección de reproducción)**: seleccione esta opción para proteger la reproducción ante ataques. • **Copy TOS Header (Copiar encabezado de TOS)**: copie el campo TOS (Tipo de servicio) desde el encabezado IP interno en el encabezado IP externo de los paquetes encapsulados con el fin de conservar la información original de TOS. Esta opción también copia el campo Explicit Congestion Notification (Notificación de congestión explícita, ECN). • **Add GRE Encapsulation (Añadir encapsulación GRE)**: seleccione esta opción para añadir un encabezado GRE encapsulado en el túnel IPSec. El cortafuegos genera un encabezado GRE después del encabezado IPSec para la interoperabilidad con otros endpoints de túnel del proveedor, con lo cual comparte un túnel GRE con el túnel IPSec. • **Tunnel Monitor (Monitor de túnel)**: Seleccione esta opción para alertar al administrador de dispositivos de los fallos del túnel y proporcionar una conmutación por error automática a otra interfaz. *Deberá asignar una dirección IP a la interfaz de túnel para su supervisión.*

© 2020 Palo Alto Networks, Inc.

Configuración general de IPSec Tunnel	Description (Descripción)
	• **Destination IP (IP de destino)**: especifique una dirección IP en el otro lado del túnel que el monitor de túnel utilizará para determinar si el túnel funciona correctamente. • **Profile (Perfil)**: seleccione un perfil existente que determine las acciones que se realizarán si falla el túnel. Si la acción especificada en el perfil del monitor es esperar recuperación, el cortafuegos esperará a que el túnel se haga funcional y NO buscará una ruta alternativa con la tabla de ruta. Si se usa la acción de conmutación por error, el cortafuegos comprobará la tabla de rutas para ver si hay una ruta alternativa que se podrá usar para alcanzar el destino. Para más información, consulte Network > Network Profiles > Monitor.
Clave manual	Si selecciona **Manual Key (Clave manual)**, especifique lo siguiente: • **Local SPI (SPI Local)**: especifique el índice de parámetros de seguridad (SPI) local para los paquetes transversales desde el cortafuegos local hasta el peer. SPI es un índice hexadecimal que se añade al encabezado para ayudar a los túneles IPSec a diferenciar entre flujos de tráfico IPSec. • **Interface (Interfaz)**: seleccione la interfaz que es el extremo del túnel. • **Local Address (Dirección local)**: seleccione la dirección IP de la interfaz local que es el extremo del túnel. • **Remote SPI (SPI remota)**: especifique el índice de parámetros de seguridad (SPI) remoto para los paquetes transversales desde el cortafuegos remoto hasta el peer. • **Protocol (Protocolo)**: seleccione el protocolo para el tráfico a través del túnel (**ESP** o **AH**). • **Authentication (Autenticación)**: seleccione el tipo de autenticación para el acceso al túnel (**SHA1**, **SHA256**, **SHA384**, **SHA512**, **MD5** o **Ninguno**). • **Key/Confirm Key (Clave/Confirmar clave)**: introduzca y confirme una clave de autenticación. • **Encryption (Cifrado)**: seleccione una opción de cifrado para el tráfico de túnel (**3des**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **des** o **null (nulo)** [sin cifrado]). • **Key/Confirm Key (Clave/Confirmar clave)**: introduzca y confirme una clave de cifrado.
Satélite de GlobalProtect	Si selecciona **GlobalProtect Satellite (Satélite de GlobalProtect)**, especifique lo siguiente: • **Name (Nombre)**: Introduzca un nombre para identificar el túnel (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. • **Tunnel Interface (Interfaz de túnel)**: seleccione una interfaz de túnel existente o haga clic en New Tunnel Interface (Nueva interfaz de túnel). • **Portal Address (Dirección del portal)**: introduzca la dirección IP del portal de GlobalProtect™. • **Interface (Interfaz)**: seleccione la interfaz de salida (egress) en la lista desplegable para llegar al portal de GlobalProtect. • **Local IP Address (Dirección IP local)**: introduzca la dirección IP de la interfaz de salida (egress) que se conecta con el portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Configuración general de IPSec Tunnel	Description (Descripción)
	• **Advanced Options (Opciones avanzadas)** • **Publish all static and connected routes to Gateway (Publicar todas las rutas estáticas y conectadas a puerta de enlace)**: seleccione esta opción para publicar todas las rutas hacia la puerta de enlace de GlobalProtect desde la que el satélite está conectado. • **Subnet**: Haga clic en **Add (Añadir)** para añadir subredes locales manualmente para la ubicación del satélite. Si otros satélites están utilizando la misma información de subred, debe aplicar la NAT a todo el tráfico hacia la IP de interfaz de túnel. Asimismo, el satélite no debe compartir rutas en este caso, así que todo el enrutamiento se realizará a través de la IP de túnel. • **External Certificate Authority (Autoridad de certificado externa)**: seleccione esta opción si va a utilizar una CA externa para gestionar certificados. Una vez que haya generado sus certificados, deberá importarlos al satélite y seleccionar el **Local Certificate (Certificado local)** y el **Certificate Profile (Perfil de certificado)**.

Pestaña Identificadores proxy de túnel IPSec

- Network > IPSec Tunnels > Proxy IDs

La pestaña **IPSec Tunnel Proxy IDs (Identificadores proxy de Túnel de IPSec)** se separa en dos pestañas: **IPv4** y **IPv6**. Esta ayuda es similar para ambos tipos; las diferencias entre IPv4 y IPv6 se describen en los campos **Local** y **Remote (Remoto)** en la siguiente tabla.

La pestaña **IPSec Tunnel Proxy IDs (Identificadores proxy de Túnel de IPSec)** también se usa para especificar los selectores de tráfico para IKEv2.

Configuración de Proxy IDs en IPv4 e IPv6	Description (Descripción)
ID proxy	Haga clic en **Add (Añadir)** e introduzca un nombre para identificar el proxy. Para un selector de tráfico IKEv2, esta campo se usa como el Nombre.
Local	Para IPv4: Introduzca una subred o dirección IP con el formato x.x.x.x/máscara (por ejemplo, 10.1.2.0/24). Para IPv6: Introduzca una dirección IP y una longitud de prefijo en el formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longitud-prefijo (o según la convención de IPv6, por ejemplo, 2001:DB8:0::/48). El direccionamiento IPv6 no requiere que se escriban todos los ceros; es posible omitir los ceros iniciales y reemplazar los consecutivos con dos puntos y coma yuxtapuestos (::). Para un selector de tráfico IKEv2, este campo se convertirá en Dirección IP de origen.
remota	Si lo requiere el peer: Para IPv4, introduzca una subred o dirección IP con el formato x.x.x.x/máscara (por ejemplo, 10.1.1.0/24).

© 2020 Palo Alto Networks, Inc.

Configuración de Proxy IDs en IPv4 e IPv6	Description (Descripción)
	Para IPv6, introduzca una dirección IP o longitud de prefijo en el formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longitud-prefijo (o según la convención de IPv6, por ejemplo, 2001:DB8:55::/48). Para un selector de tráfico IKEv2, este campo se convertirá en Dirección IP de destino.
PROTOCOL	Especifique los números de protocolo y puerto para los puertos locales y remotos: **Number**: especifique el número de protocolo (utilizado para la interoperabilidad con dispositivos de terceros). • **Any (Cualquiera)**: Permita el tráfico TCP y/o UDP. • **TCP**: Especifique los números de puertos TCP locales y remotos. • **UDP**: Especifique los números de puertos UDP locales y remotos. Cada ID de proxy configurado se tendrá en cuenta a la hora de calcular la capacidad de túnel VPN IPSec del cortafuegos. Este campo también se usa como selector de tráfico IKEv2.

Estado del túnel IPSec en el cortafuegos

- Network > IPSec Tunnels

Para ver el estado de los túneles de VPN IPSec definidos actualmente, abra la página **IPSec Tunnels (Túneles IPSec)**. En la página se indica la siguiente información de estado:

- Tunnel Status (Estado del túnel, primera columna de estado): el color verde indica un túnel de asociación de seguridad (SA) de fase 2 IPSec. El color rojo indica que la SA IPSec de fase 2 no está disponible o ha caducado.
- IKE Gateway Status (Estado de la puerta de enlace IKE): el color verde indica una SA de fase 1 IKE o SA IKE IKEv2 válida. El color rojo indica que la SA IKE de fase 1 no está disponible o ha vencido.
- Tunnel Interface Status (Estado de la interfaz del túnel): el color verde indica que la interfaz del túnel está activada (porque el monitor de túnel está deshabilitado o bien porque está activado y se puede conectar con la dirección IP de supervisión). El color rojo indica que la interfaz de túnel está desactivada porque el monitor de túnel está habilitado y no se puede conectar con la dirección IP de monitorización del túnel remoto.

Reiniciar o actualizar el túnel IPSec

- Network > IPSec Tunnels

Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** para ver el estado de los túneles. En la primera columna de estado hay un enlace a la información de túnel. Haga clic en el túnel que desea reiniciar o actualizar para abrir la página **Tunnel Info Información del túnel)** de ese túnel. Haga clic en una de las entradas de la lista y haga clic en:

- **Restart (Reiniciar)**: Reinicia el túnel seleccionado. Un reinicio interrumpirá el tráfico que atraviesa el túnel.
- **Refresh (Actualizar)**: Muestra el estado actual de la SA IPSec.

© 2020 Palo Alto Networks, Inc.

Network (Red) > GRE Tunnels (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). El túnel GRE conecta dos endpoints en un enlace lógico de punto a punto entre el cortafuegos y un enrutador (u otro cortafuegos). Los cortafuegos de Palo Alto Networks admiten la terminación de un túnel GRE.

¿Qué está buscando?	Consulte:
Componentes de un túnel GRE	Túneles GRE
Cómo proporcionar interoperabilidad con el endpoint de túnel de otro proveedor.	Seleccione **Add GRE Encapsulation (Añadir encapsulación de GRE)** cuando cree un túnel IPSec.
¿Busca más información?	Túneles GRE

Túneles GRE

- Network (Red) > GRE Tunnels (Túneles GRE)

Primero configure una interfaz de túnel (Network [Red] > Interfaces > Tunnel [Túnel]). Luego añada un túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) y proporcione la siguiente información, haciendo referencia a la interfaz de túnel que creó:

Campos del túnel de GRE	Description (Descripción)
Nombre	Nombre del túnel de GRE.
Interface (Interfaz)	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.
Dirección local	Seleccione la dirección IP local de la interfaz que debe usarse como la dirección de interfaz de túnel.
Dirección del peer	Introduzca la dirección IP en el extremo opuesto del túnel de GRE.
Interfaz túnel	Seleccione la interfaz de túnel que configuró. (Esta interfaz identifica el túnel cuando es el siguiente salto del enrutamiento).
TTL	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.

Campos del túnel de GRE	Description (Descripción)
Copy ToS Header (Copiar encabezado ToS)	Copie el campo de tipo de servicio (Type of Service, ToS) del encabezado IP interno en el encabezado IP externo de los paquetes encapsulados para conservar la información original de ToS.
Mantenimiento	Seleccione esta opción para habilitar la función de conexión persistente (Keep Alive) para el túnel de GRE (está deshabilitada de manera predeterminada). Si habilita la opción de conexión persistente, de manera predeterminada toma tres paquetes keepalive no devueltos (reintentos) en intervalos de 10 segundos para que el túnel GRE se desactive, y toma cinco intervalos del temporizador de suspensión con intervalos de 10 segundos para que el túnel de GRE se reactive.
Intervalo (seg)	Configure el intervalo entre los paquetes keepalive que el extremo local del túnel de GRE envía al peer del túnel, y el intervalo que cada temporizador de suspensión esperará después de los paquetes keepalive correctos antes de que el cortafuegos restablezca la comunicación con el peer del túnel (el intervalo es de 1 a 50, el valor predeterminado es 10).
Reintentar	Configure la cantidad de intervalos en que los paquetes keepalive no se devolverán antes de que el cortafuegos considere el peer del túnel como inactivo (el intervalo es de 1 a 255, el valor predeterminado es 3).
Temporizador de mantenimiento	Configure la cantidad de intervalos en que los paquetes keepalive son correctos antes de que el cortafuegos restablezca la comunicación con el peer (el intervalo es de 1 a 64, el valor predeterminado es 5).

© 2020 Palo Alto Networks, Inc.

Network > DHCP

El protocolo de configuración de host dinámico (DHCP) es un protocolo estandarizado que proporciona parámetros de configuración de capa de enlace y TCP/IP, y direcciones de red a los hosts configurados dinámicamente en una red TCP/IP. Una interfaz en un cortafuegos Palo Alto Networks puede actuar como un servidor, cliente o agente de retransmisión de DHCP. Al asignar esas funciones a distintas interfaces, el cortafuegos puede desempeñar múltiples funciones.

¿Qué está buscando?	Consulte:
¿Qué es el DHCP?	Descripción general de DHCP
¿Cómo asigna las direcciones un servidor DHCP?	Direccionamiento DHCP
Configure una interfaz en el cortafuegos para que funcione como un:	
	Servidor DHCP
	Retransmisión DHCP
	Network > DNS Proxy
¿Busca más información?	DHCP

Descripción general de DHCP

- Network > DHCP

DHCP usa un modelo cliente-servidor de comunicación. Este modelo consta de tres funciones que puede desempeñar el cortafuegos: Cliente DHCP, servidor DHCP y agente de relé DHCP.

- Un cortafuegos que funcione como cliente DHCP (host) puede solicitar una dirección IP y otros ajustes de configuración al servidor DHCP. Los usuarios de los cortafuegos 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 cortafuegos que actúa como un servidor DHCP puede atender a los clientes. Si se usa alguno de esos tres mecanismos de direcciones DHCP, el administrador de red ahorra tiempo y tiene el beneficio de reutilizar un número limitado de direcciones IP de clientes que ya no necesitan una conectividad de red. El servidor puede ofrecer direcciones IP y muchas opciones DHCP a muchos clientes.
- Un cortafuegos que actúa como un agente de retransmisión DHCP escucha mensajes de transmite mensajes de DHCP de unidifusión y difusión y los transmite 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). Los mensajes DHCP que un servidor envía a un cliente se envían al puerto 68.

Direccionamiento DHCP

El servidor DHCP asigna o envía una dirección IP a un cliente de tres formas:

© 2020 Palo Alto Networks, Inc.

- **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.
- **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 cortafuegos cliente. La asignación DHCP continúa en su lugar aunque el cliente se desconecte (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 cortafuegos cliente se usa para una función crucial y debe mantener la misma dirección IP aunque el cortafuegos se apague, desconecte, reinicie o sufra un corte de alimentación, etc.

  Tenga en cuenta los siguientes puntos cuando configure una **Reserved Address (Dirección reservada)**:

  - 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 asignarlas 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 **Dirección reservada (Dirección reservada)** a ningún cortafuegos. Puede reservar unas direcciones del grupo y asignarlas estáticamente a un fax e impresora, por ejemplo, sin usar DHCP.

Servidor DHCP

- Network > DHCP > DHCP Server

La siguiente sección describe cada componente del servidor DHCP. Antes de configurar un servidor DHCP, asegúrese de que ha configurado una interfaz Ethernet de capa 3 o VLAN de capa 3, y de que la interfaz se asigna a una zona y un enrutador virtual. También debería conocer un grupo válido de direcciones IP de su plan de red que pueda designarse para que su servidor DHCP lo asigne a los clientes.

Cuando añada un servidor DHCP, puede configurar los ajustes descritos en la tabla siguiente.

Configuración de servidor DHCP	Configurado en	Description (Descripción)
Interface (Interfaz)	**Servidor DHCP**	Nombre de la interfaz que funcionará como servidor DHCP.
Modo		Seleccione **enabled (habilitado)** o modo **auto (automático**. El modo **Auto (Automático** activa el servidor y lo desactiva si se detecta otro servidor DHCP en la red. El ajuste **disabled (deshabilitar)** desactiva el servidor.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor DHCP	Configurado en	Description (Descripción)
Hacer ping a la IP al asignar IP nuevas	**DHCP Server (Servidor DHCP)** > **Lease (Concesión)**	Si hace clic en **Ping IP when allocating new IP (Hacer ping a la IP al asignar IP nuevas)**, el servidor hará ping a la dirección IP antes de asignarla a su cliente. Si el ping recibe una respuesta, significará que ya hay un cortafuegos diferente con esa dirección, por lo que no está disponible. El servidor asigna la siguiente dirección desde el grupo. Si selecciona esta opción, la columna Rastrear IP de la pantalla tendrá una marca de selección.
Concesión		Especifique 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 **Minutes (Minutos)**.
Grupos de IP		Especifique el grupo de direcciones IP de estado desde el que el servidor DHCP seleccione una dirección y la asigna a un cliente DHCP. Puede introducir una única dirección, una dirección/<longitud de máscara>, como 192.168.1.0/24, o un intervalo de direcciones, como 192.168.1.10-192.168.1.20.
Dirección reservada		También puede especificar una dirección IP (formato x.x.x.x) desde los grupos de IP que no desee asignar dinámicamente mediante el servidor DHCP. Si también especifica una **MAC Address (Dirección MAC)** (formato xx:xx:xx:xx:xx:xx), la **Reserved Address (Dirección reservada)** se asigna al cortafuegos asociado con la dirección MAC cuando ese cortafuegos solicita una dirección IP a través de DHCP.
Origen de herencia	**DHCP Server (Servidor DHCP)** > **Options (Opciones)**	Seleccione **None (Ninguna)** (predeterminado) 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. Una de las ventajas de especificar un origen de herencia es que las opciones DHCP se transfieren rápidamente desde el servidor que está antes del cliente DHCP de origen. También mantiene

© 2020 Palo Alto Networks, Inc.

Configuración de servidor DHCP	Configurado en	Description (Descripción)
		actualizadas las opciones del cliente si se cambia una opción en el origen de herencia. Por ejemplo, si el cortafuegos de origen de herencia sustituye a su servidor NTP (que se ha identificado como el servidor **Primary NTP (NTP principal)**), el cliente heredará automáticamente la nueva dirección como su nuevo servidor **Primary NTP (NTP principal)**.
Comprobar estado de origen de herencia		Si ha seleccionado **Inheritance Source (Origen de herencia)**, al hacer clic en **Check inheritance source status (Comprobar estado de origen de herencia)** para abrir la ventana Estado de interfaz de IP dinámica que muestra las opciones que se han heredado desde el cliente DHCP.
Gateway	**DHCP Server (Servidor DHCP)** > **Options (Opciones) (cont.)**	Especifique 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.
Máscara de subred		Especifique la máscara de red que se aplica a las direcciones del campo **IP Pools (Grupos de IP)**.
Opciones		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)**. El servidor DHCP envía estos ajustes a sus clientes. • **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**, **Secondary WINS**: introduzca la dirección IP de los servidores Windows Internet Naming Service (WINS) preferidos y alternativos. • **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**, **Secondary NTP**: dirección IP de los servidores del protocolo de tiempo de redes (NTP) disponibles. • **POP3 Server**: introduzca la dirección IP del servidor Post Office Protocol de versión 3 (POP3).

© 2020 Palo Alto Networks, Inc.

Configuración de servidor DHCP	Configurado en	Description (Descripción)
		• **SMTP Server**: introduzca la dirección IP del servidor del protocolo simple de transferencia de correo (Simple Mail Transfer Protocol, SMTP). • **DNS Suffix**: sufijo para que el cliente lo use localmente cuando se introduce un nombre de host sin cualificar que no puede resolver el cliente.
Opciones de DHCP personalizadas		Haga clic en **Add (Añadir)** e introduzca el **Name (Nombre)** de la opción personalizada que desea que el servidor DHCP envíe a los clientes. Introduzca un **Option Code (Código de opción)** (el intervalo es 1-254). Si se introduce el **Option Code 43 (Código de opción 43)**, aparece el campo Identificador de clase de proveedor (VCI). Introduzca un criterio de coincidencia que se compare con el VCI entrante desde la opción 60 del cliente. El cortafuegos buscará en el VCI entrante desde la opción 60 del cliente, busca el VCI coincidente en su propia tabla de servidor DHCP y devuelve el valor correspondiente al cliente en la opción 43. El criterio de coincidencia de VCI es una cadena o valor hexagonal. Un valor hexagonal debe tener un prefijo "0x". Haga clic en **Inherited from DCHP server inheritance source (Heredado de fuente de herencia de DHCP)** para que el servidor herede el valor para ese código de opción desde el origen de herencia en lugar de introducir un **Option Value (Valor de opción)**. Como alternativa a esta opción, puede continuar con lo siguiente: **Option Type (Tipo de opción)**: Seleccione **IP Address (Dirección IP)**, **ASCII** o **Hexadecimal** para especificar el tipo de datos usado para el Valor de opción. En **Option Value (Valor de opción)**, haga clic en **Add (Añadir)** e introduzca el valor para la opción personalizada.

Retransmisión DHCP

- Network > DHCP > DHCP Relay

Antes de realizar la Configuración de una interfaz de cortafuegos como un agente de retransmisión DHCP, asegúrese de haber configurado una interfaz Ethernet de capa 3 o VLAN de capa 3, y que ha asignado la interfaz a una zona y un enrutador virtual. Si quiere que la interfaz pueda pasar mensajes DHCP entre los clientes y los servidores. Cada interfaz puede reenviar mensajes a un máximo de ocho servidores DHCP IPv4 externos y a ocho servidores DHCP IPv6 externos. Un mensaje de DHCPDISCOVER del cliente se

© 2020 Palo Alto Networks, Inc.

envía a todos los servidores configurados, y el cortafuegos retransmite el mensaje DHCPOFFER del primer servidor que responde al cliente que originó la petición.

Configuración de retransmisión DHCP	Description (Descripción)
Interface (Interfaz)	Nombre de la interfaz que será el agente de retransmisión DHCP.
IPv4 / IPv6	Seleccione el tipo de servidor DHCP y dirección IP que especificará.
Dirección IP de servidor DHCP	Introduzca la dirección IP del servidor DHCP desde donde y hacia donde retransmitirá los mensajes DHCP.
Interface (Interfaz)	Si ha seleccionado IPv6 como el protocolo de dirección IP para el servidor DHCP y especificado una dirección multicast, deberá también especificar una interfaz saliente.

Cliente DHCP

- Network > Interfaces > Ethernet > IPv4
- Network > Interfaces > VLAN > IPv4

Antes de configurar una interfaz de cortafuegos como un cliente DHCP, asegúrese de que ha configurado una interfaz Ethernet de capa 3 o VLAN de capa 3, y que ha asignado la interfaz a una zona y un enrutador virtual. Realice esta tarea si quiere usar DHCP para solicitar una dirección IPv4 para una interfaz en un cortafuegos.

Configuración de cliente DHCP	Description (Descripción)
Tipo	Seleccione **DHCP Client (Cliente DHCP)** y luego **Enable (Habilitar)** para configurar la interfaz como un cliente DHCP.
Crear automáticamente ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor	Esto provoca que el cortafuegos cree una ruta estática a una puerta de enlace predeterminada que será útil cuando los clientes intenten acceder a muchos destinos que no necesitan mantener rutas en una tabla de enrutamiento en el cortafuegos.
Métrica de ruta predeterminada	Una opción es introducir una **Default Route Metric (Métrica de ruta predeterminada)** (nivel de prioridad) para la ruta entre el cortafuegos y el servidor de actualización. 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 (el intervalo es 1-65535; sin valor predeterminado).
Mostrar información de tiempo de ejecución de cliente DHCP	Muestra todos los ajustes recibidos desde el servidor DHCP, incluidos el estado de concesión de DHCP, la asignación de dirección IP dinámica, la máscara de subred, la puerta de enlace, la configuración del servidor (DNS, NTP, dominio, WINS, NIS, POP3 y SMTP).

© 2020 Palo Alto Networks, Inc.

Network > DNS Proxy

Los servidores DNS realizan el servicio de resolver un nombre de dominio con una dirección IP y viceversa. Cuando configura el cortafuegos como un proxy DNS, esta actúa como un intermediario entre los clientes y servidores y como un servidor DNS resolviendo consultas desde su caché DNS o enviando consultas a otros servidores DNS. Use esta página para configurar los ajustes que determinan cómo el cortafuegos sirve como un proxy DNS.

¿Qué desea saber?	Consulte:
¿Cómo funciona el cortafuegos como proxy de las solicitudes DNS?	Resumen del proxy DNS
¿Cómo se configura un proxy DNS?	Configuración del proxy DNS
¿Cómo se configuran las asignaciones de FQDN estática a dirección IP?	
¿Cómo se puede administrar proxies DNS?	Acciones adicionales de proxy DNS
¿Busca más información?	DNS:

Resumen del proxy DNS

Puede configurar el servidor de seguridad para que actúe como servidor DNS. En primer lugar, cree un proxy DNS y seleccione las interfaces a las que se aplica el proxy. A continuación, especifique los servidores DNS primarios y secundarios predeterminados a los que el cortafuegos envía las consultas DNS cuando no encuentra el nombre de dominio en su caché de proxy de DNS (y cuando el nombre de dominio no coincide con una regla de proxy).

Para dirigir consultas DNS a diferentes servidores DNS basados en nombres de dominio, cree reglas de proxy DNS. La especificación de múltiples servidores DNS puede garantizar la localización de las consultas DNS y aumentar la eficiencia. Por ejemplo, puede reenviar todas las consultas DNS corporativas a un servidor DNS corporativo y reenviar todas las demás consultas a los servidores DNS ISP.

Utilice las siguientes pestañas para definir un proxy DNS (más allá de los servidores DNS primarios y secundarios predeterminados):

- **Static Entries (Entradas estáticas)**: permite configurar las asignaciones de direcciones FQDN a IP estáticas que el cortafuegos almacena en caché y las envía a los hosts en respuesta a las consultas DNS.
- **DNS Proxy Rules (Reglas de proxy de DNS)**: permite especificar nombres de dominio y servidores DNS primarios y secundarios correspondientes para resolver las consultas que coinciden con la regla. Si el nombre de dominio no se encuentra en la caché de proxy DNS, el cortafuegos busca una correspondencia en el proxy de DNS (en la interfaz en la que se recibe la consulta) y reenvía la consulta a un servidor DNS en función de los resultados. Si no hay resultados de coincidencia, el cortafuegos envía la consulta a los servidores primarios y secundarios DNS predeterminados. Puede habilitar el almacenamiento en caché de dominios que coincidan con la regla.
- **Avanzado**: debe habilitar el almacenamiento en caché (seleccione **Caché**) y **Respuestas de EDNS de caché** si el objeto proxy DNS se utiliza para resolver consultas DNS/FQDN que genera el cortafuegos. La pestaña Avanzado también le permite controlar las consultas TCP y los reintentos de consultas UDP. El cortafuegos envía consultas TCP o UDP DNS a través de la interfaz configurada. Las consultas UDP

© 2020 Palo Alto Networks, Inc.

cambian a TCP cuando una respuesta de una consulta DNS es demasiado larga para un único paquete UDP.

Configuración del proxy DNS

Haga clic en **Add (Añadir)** y configure el cortafuegos para actuar como un proxy DNS. Puede configurar un máximo de 256 proxies DNS en un cortafuegos.

Configuración del proxy DNS	Configurado en	Description (Descripción)
Habilitación	**Proxy Dns**	Seleccione esta opción para habilitar este proxy DNS.
Nombre		Especifique un nombre para identificar el objeto proxy DNS (hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación		Especifique el sistema virtual al que se aplique el objeto proxy DNS: • **Shared (Compartido)** El proxy se aplica a todos los sistemas virtuales. Si quiere seleccionar **Shared (Compartido)**, el campo **Server Profile (Perfil de servidor)** no está disponible. En su lugar, introduzca los objetos de direcciones o direcciones IP del servidor DNS **Primary (Primario)** y **Secondary (Secundario)**. • Seleccione un sistema virtual para utilizar este proxy DNS; debe configurar uno sistema virtual previamente. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)**, seleccione un sistema virtual y un **DNS Proxy (Proxy DNS)**.
Origen de herencia (Ubicación compartida únicamente)		Seleccione un origen del cual heredar las configuraciones del servidor DNS predeterminado. Se suele utilizar en implementaciones de sucursales, en las que a la interfaz WAN del cortafuegos se accede mediante DHCP o PPPoE.
Comprobar estado de origen de herencia (Ubicación compartida únicamente)		Seleccione para ver la configuración del servidor asignada actualmente a las interfaces del cliente DHCP y PPoE. Pueden incluir DNS, WINS, NTP, POP3, SMTP o sufijo DNS.
Primario/Secundario (Ubicación compartida únicamente)		Especifique las direcciones IP de los servidores DNS primarios y secundarios predeterminados a los que este cortafuegos (como proxy DNS) envía consultas DNS. Si el servidor DNS primario no se encuentra, el cortafuegos utilizará el servidor DNS secundario.
Perfil de servidor		Seleccione o cree un nuevo perfil de servidor DNS. Este campo no aparece si la ubicación de los sistemas virtuales se especifica como Compartido.

© 2020 Palo Alto Networks, Inc.

Configuración del proxy DNS	Configurado en	Description (Descripción)
(Solo ubicación del sistema virtual)		
Interface (Interfaz)		**Add (Añadir)** una interfaz para funcionar como un proxy DNS. Puede añadir varias interfaces. Para eliminar un proxy DNS de la interfaz, selecciónelo y haga clic en **Delete (Eliminar)**. No se requiere una interfaz si se usa el proxy DNS solo para la funcionalidad de la ruta de servicio. Use una ruta de servicio de destino con un proxy DNS sin interfaz, si desea que la ruta de servicio de destino establezca la dirección IP de origen. De lo contrario, el proxy DNS selecciona una dirección IP de interfaz como origen (cuando no se definen rutas de servicio DNS).
Nombre	**DNS Proxy (Proxy DNS) > DNS Proxy Rules (Reglas de proxy DNS)**	Se requiere un nombre para poder modificar y hacer referencia a una entrada mediante CLI.
Activar el almacenamiento en caché de dominios resueltos por esta asignación		Seleccione para activar el almacenamiento en caché de los dominios que se han resuelto mediante esta asignación.
Nombre de dominio		**Add (Añadir)** uno o más nombres de dominio a los que el cortafuegos compara los FQDN entrantes. Si el FQDN coincide con uno de los dominios de la regla, el servidor de seguridad reenvía la consulta al servidor DNS primario / secundario especificado para este proxy. Para eliminar un nombre de dominio de una regla, selecciónelo y haga clic en **Delete (Eliminar)**.
Perfil de servidor DNS (Ubicación compartida únicamente)		Seleccione o agregue un perfil de servidor DNS para definir la configuración de DNS para el sistema virtual, incluido el servidor DNS primario y secundario al que el cortafuegos envía consultas de nombres de dominio.
Primario/Secundario (Solo ubicación del sistema virtual)		Introduzca el nombre de host o la dirección IP de los servidores DNS primarios y secundarios a los que el cortafuegos envía consultas de nombres de dominio coincidentes.
Nombre	**DNS Proxy (Proxy DNS) > Static Entries (Entradas estáticas)**	Introduzca un nombre para la entrada estática.
FQDN		Introduzca el nombre de dominio completo (FQDN) que se asignará a las direcciones IP estáticas definidas en el campo Address (Dirección).
Dirección		Haga clic en **Add (Añadir)** una o más direcciones IP que se asignan a este dominio. El cortafuegos incluye todas estas direcciones en su respuesta DNS y el cliente elige la

© 2020 Palo Alto Networks, Inc.

Configuración del proxy DNS	Configurado en	Description (Descripción)
		dirección IP que va a utilizar. Para eliminar una dirección, selecciónela y haga clic en **Delete (Eliminar)**.
Consultas TCP	**DNS Proxy (Proxy DNS)** > **Advanced (Avanzado)**	Seleccione esta opción para activar las consultas DNS mediante TCP. Especifique el máximo del número de solicitudes DNS TCP pendientes simultáneas (**Max Pending Requests**) que admitirá el cortafuegos (intervalo 64-256, opción predeterminada: 64).
Reintentos de consultas de UDP	**DNS Proxy (Proxy DNS)** > **Advanced (Avanzado)**	Especifique los ajustes para los reintentos de consulta UDP: • **Interval (Intervalo)**: tiempo, en segundos, después del cual el proxy DNS envía otra solicitud si no ha recibido una respuesta (intervalo: 1-30, predeterminado: 2). • **Attempts (Intentos)**: número máximo de intentos (sin incluir el primer intento) después de los cuales el DNSP intentará con el siguiente servidor DNS (intervalo: 1-30, predeterminado: 5).
Caché	**DNS Proxy (Proxy DNS)** > **Advanced (Avanzado)**	Debe habilitar la **caché** (habilitada de forma predeterminada) si este objeto proxy DNS se utiliza para consultas que genera el cortafuegos (es decir, en **Dispositivo** > **Configuración** > **Servicios** > **DNS** o en **Dispositivo** > **Sistemas virtuales** y seleccione un sistema virtual y **General** > **Proxy DNS**). A continuación, especifique lo siguiente: • **Enable TTL (Habilitar TTL)**: limite el tiempo que el firewall almacena en caché las entradas DNS del objeto proxy. TTL está deshabilitada de manera predeterminada. Luego introduzca **Time to Live (sec) [Valor del tiempo de vida (seg.)]**: el número de segundos después de que todas las entradas almacenadas en caché para el objeto proxy se eliminan y las nuevas solicitudes de DNS deben resolverse y almacenarse en caché de nuevo. El intervalo es de 60-86.400. No hay TTL por defecto; las entradas permanecen hasta que el cortafuegos se queda sin memoria caché. • **Respuestas de EDNS de caché**: debe habilitar mecanismos de extensión de caché para respuestas DNS (EDNS) si este objeto de proxy DNS se usa para consultas que genera el cortafuegos. El cortafuegos debe poder almacenar en caché las respuestas DNS para que las consultas de los objetos de dirección FQDN se realicen correctamente.

Acciones adicionales de proxy DNS

Tras configurar el cortafuegos como un proxy DNS, puede realizar las siguientes acciones en la página **Network** > **DNS Proxy** (Red > Proxy DNS) para gestionar la configuración de proxy DNS:

© 2020 Palo Alto Networks, Inc.

- **Modify (Modificar)**: para modificar un proxy DNS, haga clic en el nombre de la configuración de proxy DNS.
- **Delete (Eliminar)**: seleccione una entrada de proxy DNS y haga clic en **Delete (Eliminar)** para eliminar la configuración de proxy DNS.
- **Disable (Deshabilitar)**: para deshabilitar un proxy DNS, haga clic en la entrada del proxy DNS y cancele la selección de **Enable (Habilitar)**. Para habilitar un proxy DNS que se haya deshabilitado, haga clic en el nombre de la entrada de proxy DNS y se seleccione **Enable (Habilitar)**.

© 2020 Palo Alto Networks, Inc.

Red > QoS

Los siguientes temas describen la calidad de servicio (QoS).

¿Qué está buscando?	Consulte:
Establecimiento de límites de ancho de banda para una interfaz y aplicación de QoS para el tráfico que sale de una interfaz.	Configuración de la interfaz de QoS
Supervisión del tráfico que sale de una interfaz habilitada con QoS.	Estadísticas de la interfaz de QoS
¿Busca más información?	Consulte Calidad de servicio para obtener los flujos de trabajo completos, los conceptos y los casos de uso de QoS.
	Seleccione Políticas > QoS para asignar una clase QoS al tráfico coincidente o seleccione Red > Perfiles de red > QoS para definir límites de ancho de banda y prioridad para hasta ocho clases de QoS.

Configuración de la interfaz de QoS

Habilite QoS en una interfaz para establecer los límites de ancho de banda de la interfaz o habilitar la interfaz para que aplique QoS al tráfico de salida. Habilitar QoS en una interfaz incluye asignar un perfil de QoS a la interfaz. QoS se admite en interfaces físicas y, según el modelo de cortafuegos, es compatible con subinterfaces e interfaces de Ethernet de agregación (AE). Consulte la herramienta de comparación de productos de Palo Alto Networks para ver la compatibilidad de la función de QoS para su modelo de cortafuegos.

Para comenzar, haga clic en **Add (Añadir)** o modifique una interfaz de QoS, y luego defina los campos descritos en la siguiente tabla.

Configuración de la interfaz de QoS	Configurado en	Description (Descripción)
Nombre de interfaz	**QoS Interface (Interfaz de QoS)** > **Physical Interface (Interfaz física)**	Seleccione la interfaz física en la que habilitar QoS.
Máximo de salida (Mbps)		Introduzca el valor máximo de rendimiento (en Mbps) para el tráfico que abandona el cortafuegos a través de esta interfaz. El valor predeterminado es 0, lo que especifica el límite del cortafuegos (60 000 Mbps en PAN-OS 7.1.16 y versiones posteriores; 16 000 en PAN-OS 7.1.15 y versiones posteriores). *Aunque no es un campo obligatorio, se recomienda definir siempre el valor de Egress Max (Máximo de salida) de una interfaz de QoS.*

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz de QoS	Configurado en	Description (Descripción)
Activar la función QoS en esta interfaz		Seleccione esta opción para habilitar QoS en la interfaz seleccionada.
Tráfico en claro Interfaz túnel	**QoS Interface (Interfaz de QoS)** > **Physical Interface (Interfaz física)** > **Default Profile (Perfil predeterminado)**	Seleccione los perfiles predeterminados de QoS para el tráfico en claro y de túnel. Debe especificar un perfil predeterminado para cada uno. Para el tráfico en claro, el perfil predeterminado se aplica a todo el tráfico en claro como un conjunto. Para el tráfico de túnel, el perfil predeterminado se aplica de forma individual a cada túnel que no cuenta con una asignación de perfil específico en la sección de configuración detallada. Para obtener instrucciones sobre la definición de perfiles QoS, consulte Network > Network Profiles > QoS.
Interfaz túnel		
Salida garantizada (Mbps)	**QoS Interface (Interfaz de QoS)** > **Clear Text Traffic/ Tunneled Traffic (Tráfico de texto en claro/Tráfico de túnel)**	Introduzca el ancho de banda garantizado para el tráfico de texto en claro o de túnel desde esta interfaz.
Máximo de salida (Mbps)		Introduzca el valor máximo de rendimiento (en Mbps) para el tráfico de texto en claro o de túnel que abandona el cortafuegos a través de esta interfaz. El valor predeterminado es 0, lo que especifica el límite del cortafuegos (60 000 Mbps en PAN-OS 7.1.16 y versiones posteriores; 16 000 en PAN-OS 7.1.15 y versiones posteriores). El valor **Egress Max (Máximo de salida)** para el tráfico de túnel o texto no cifrado debe ser menor o igual que el valor **Egress Max (Máximo de salida)** de la interfaz física.

Añadir		• Haga clic en **Add (Añadir)** en la pestaña **Clear Text Traffic (Tráfico no cifrado)** para definir la granularidad adicional para el tratamiento del tráfico en claro. Haga clic en las entradas individuales para configurar los siguientes ajustes:
		  • **Name (Nombre)**: introduzca un nombre para identificar estos ajustes.
		  • **QoS Profile (Perfil de QoS)**: seleccione el perfil de QoS para aplicar a la subred y la interfaz especificadas. Para obtener instrucciones sobre la definición de perfiles QoS, consulte Network > Network Profiles > QoS.
		  • **Source Interface (Interfaz de origen)**: seleccione la interfaz del cortafuegos.
		  • **Source Subnet (Subred de origen)**: seleccione una subred para restringir los ajustes al tráfico procedente de ese origen o mantenga el valor predeterminado **any (cualquiera)** para aplicar los ajustes a cualquier tráfico de la interfaz especificada.
		• Haga clic en **Add (Añadir)** en la pestaña **Tunneled Traffic (Tráfico de túnel)** para cancelar la asignación de perfil predeterminada para túneles específicos y configurar los siguientes ajustes:

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz de QoS	Configurado en	Description (Descripción)
		• **Tunnel Interface (Interfaz de túnel)**: seleccione la interfaz de túnel en el cortafuegos. • **QoS Profile (Perfil de QoS)**: seleccione el perfil de QoS para aplicar a la interfaz de túnel especificadas. Por ejemplo, asuma una configuración con dos sitios, uno de los cuales cuenta con una conexión de 45 Mbps y el otro con una conexión T1 con el cortafuegos. Puede aplicar una configuración de QoS restrictiva al sitio T1 de modo que la conexión no se sobrecarga a la vez que se proporciona una configuración más flexible para el sitio con la conexión de 45 Mbps. Para eliminar una entrada de tráfico en claro o de túnel, borre la entrada y haga clic en **Delete (Eliminar)**. Si se dejan en blanco las secciones de tráfico en claro o de túnel, los valores especificados en la sección Perfil predeterminado de la pestaña Interfaz física.

Estadísticas de la interfaz de QoS

- Network > QoS > Statistics

Para una interfaz de QoS, seleccione **Statistics (Estadísticas)** para ver información de ancho de banda, sesión y aplicación de las interfaces de QoS configuradas.

Estadísticas de QoS	Description (Descripción)
Ancho de banda	Muestra los gráficos de ancho de banda en tiempo real para el nodo y las clases seleccionados. Esta información se actualiza cada dos segundos. *Las limitaciones de salida garantizada y de salida máxima de QoS configuradas para las clases de QoS pueden mostrarse con un valor ligeramente distinto en la pantalla de estadísticas de QoS. Este es el comportamiento esperado y se debe a que el motor de hardware resume los límites de ancho de banda y recuentos. Esto no supone problema alguno para el funcionamiento, puesto que los gráficos de uso de ancho de banda muestran los valores y cantidades en tiempo real.*
applications	Enumera todas las aplicaciones activas para el nodo y/o clase de QoS seleccionados.
Usuarios de origen	Enumera todos los usuarios de origen activos para el nodo y/o clase de QoS seleccionados.
Usuarios de destino	Enumera todos los usuarios de destino activos para el nodo y/o clase de QoS seleccionados.

© 2020 Palo Alto Networks, Inc.

Estadísticas de QoS	Description (Descripción)
Reglas de seguridad	Enumera las reglas de seguridad coincidentes y que aplican el nodo y/o clase de QoS seleccionados.
Reglas de QoS	Enumera las reglas de QoS coincidentes y que aplican el nodo y/o clase de QoS seleccionados.

© 2020 Palo Alto Networks, Inc.

Network > LLDP

El protocolo de detección de nivel de enlace (LLDP) ofrece un método automático de detección de los dispositivos vecinos y sus funciones en la capa de enlace.

¿Qué está buscando?	Consulte:
¿Qué es el LLDP?	Descripción general de LLDP
Configuración de LLDP.	Componentes del LLDP
Configuración de un perfil de autenticación.	Network > Network Profiles > LLDP Profile
¿Busca más información?	LLDP

Descripción general de LLDP

El LLDP permite el cortafuegos para enviar y recibir las tramas Ethernet que contienen las unidades de datos LLDP (LLDPDUs) desde y hacia los vecinos. El dispositivo receptor almacena la información en un MIB, a la que se puede acceder mediante el protocolo simple de administración de redes (SNMP). LLDP permite a los dispositivos de red asignar su topología de red y aprender capacidades de los dispositivos conectados, lo que facilita la solución de problemas, especialmente para implementaciones de cables virtuales en las que el cortafuegos normalmente no se detecta en una topología de red.

Componentes del LLDP

Para habilitar el LLDP en el cortafuegos, haga clic en Edit y después en **Enable (Habilitar)** y configure los cuatro ajustes que se muestran en la siguiente tabla, si los ajustes predeterminado no se adapta en su entorno. El resto de entradas de la tabla describe las estadísticas de peer y estado.

Configuración de LLDP	Configurado en	Description (Descripción)
Intervalo de transmisión (segundos)	**General de LLDP**	Especifique el intervalo en segundos en el que se transmiten las LLDPDU (el intervalo es 1-3.600; el predeterminado es 30).
Retraso de transmisión (segundos)		Especifique el tiempo de intervalo (en segundos) entre las transmisiones LLDP enviados después de que se realice un cambio en un elemento de Tipo-Longitud-Valor (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 **Transmit Delay (Retraso de transmisión)** debe ser inferior al **Transmit Interval (Intervalo de transmisión)** (el intervalo es 1-600; el predeterminado es 2).
Múltiple tiempo de espera		Especifique un valor que se multiplica por el **Transmit Interval (Intervalo de transmisión)** para determinar el

© 2020 Palo Alto Networks, Inc.

Configuración de LLDP	Configurado en	Description (Descripción)
		tiempo total de espera TTL (el intervalo es 1-100; el predeterminado es 4). El tiempo de espera TTL es el tiempo que el cortafuegos conservará la información del peer como válido. El tiempo de espera TTL máximo es 65.535 segundos, independientemente del valor de multiplicador.
Intervalo de notificaciones		Especifique el intervalo en segundos en el que las notificaciones de Trap SNMP y syslog se transmiten cuando se producen los cambios MIB (el intervalo es 1-3.600; el predeterminado es 5).
filtro de catalejo	**LLDP** > **Status (Estado)**	También puede introducir un valor de datos en la fila de filtro y hacer clic en la flecha gris, que provoca que solo las filas que incluyen ese valor de datos se puedan ver. Haga clic en la X roja para borrar el filtro.
Interface (Interfaz)		Nombre de las interfaces que tienen asignados perfiles LLDP.
LLDP		Estado de LLDP: habilitado o deshabilitado.
Modo		Modo LLDP de la interfaz: Tx/Rx, Tx solo o Rx solo.
Perfil		Nombre del perfil asignado a la interfaz.
Total transmitidos		Número de LLDPDU transmitidos fuera de la interfaz.
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.
Total recibidos		Número de tramas LLDP recibidas de la interfaz.
TLV descartado		Recuento de las tramas LLDP descartadas en la recepción.
Errores		Número de elementos Tiempo-Longitud-Valor (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.
No reconocido		Número de TLV recibidos en la interfaz que no reconoce el agente local LLDP, por ejemplo, porque el tipo TLV está en el intervalo TLV reservado.
Caducado		Número de elementos eliminados desde Recibir MIB por una caducidad TTL adecuada.

© 2020 Palo Alto Networks, Inc.

Configuración de LLDP	Configurado en	Description (Descripción)
Borrado de estadísticas de LLDP		Seleccione para borrar todas las estadísticas de LLDP.
filtro de catalejo	**LLDP** > **Peers (Peers)**	También puede introducir un valor de datos en la fila de filtro y hacer clic en la flecha gris, que provoca que solo las filas que incluyen ese valor de datos se puedan ver. Haga clic en la X roja para borrar el filtro.
Interfaz local		Interfaz en el cortafuegos que detectó el dispositivo vecino.
ID de bastidor remoto		ID de bastidor del peer, se usa la dirección MAC.
ID de puerto	**LLDP** > **Peers (Peers) (cont.)**	IP de puerto del peer.
Nombre		Nombre del peer.
Más información		Haga clic **More Info (Más información)** para ver los detalles de peer remoto, que se basan en TLV obligatorios y opcionales.
Tipo de bastidor		El tipo de chasis en 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 NombreIf 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.

© 2020 Palo Alto Networks, Inc.

Red > Perfiles de red

Los siguientes temas describen los perfiles de red:

- Red > Perfiles de red > Criptográfico IPSec de GlobalProtect
- Network > Network Profiles > IKE Gateways
- Red > Perfiles de red > Criptográfico IPSec
- Red > Perfiles de red > Criptográfico IKE
- Red > Perfiles de red > Supervisar
- Network > Network Profiles > Interface Mgmt
- Network > Network Profiles > Zone Protection
- Red > Perfiles de red > QoS
- Network > Network Profiles > LLDP Profile
- Network > Network Profiles > BFD Profile
- Network (Red) > Network Profiles (Perfiles de red) > SD-WAN Interface Profile (Perfil de interfaz de SD-WAN)

Red > Perfiles de red > Criptográfico IPSec de GlobalProtect

Use la página **Perfiles criptográficos de IPSec de GlobalProtect** para especificar los algoritmos de autenticación y cifrado en los túneles de VPN entre un gateway y clientes de GlobalProtect. El orden en el que añade algoritmos es el orden en el que el cortafuegos los aplica, y puede afectar al rendimiento y la seguridad del túnel. Para cambiar el orden, seleccione un algoritmo y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**.

Para los túneles VPN entre las puertas de enlace de GlobalProtect y los satélites (cortafuegos), consulte Red> Perfiles de red> IPSec Crypto.

Configuración de perfiles criptográficos IPSec de GlobalProtect	
Nombre	Introduzca un nombre para identificar el perfil. El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede tener hasta **31** caracteres. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Cifrado	Haga clic en **Add (Añadir)** y seleccione los algoritmos de cifrado deseados. Para garantizar una seguridad máxima, cambie el orden (de arriba abajo) a:**aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.
Autenticación	Haga clic en **Add (Añadir)** y seleccione el algoritmo de autenticación. En estos momentos la única opción es **sha1**.

Network > Network Profiles > IKE Gateways

Utilice esta página para gestionar o definir una puerta de enlace, lo que puede incluir la información de configuración necesaria para realizar la negociación del protocolo de intercambio de claves por red (IKE) con puertas de enlace del peer. Esta es la parte de fase 1 de la configuración VPN IKE/IPSec.

Para gestionar, configurar, reiniciar o actualizar un gateway IKE, consulte lo siguiente:

- Gestión de la puerta de enlace de IKE
- Pestaña General de la puerta de enlace de IKE

© 2020 Palo Alto Networks, Inc.

- Pestaña Opciones avanzadas de la puerta de enlace de IKE
- Reiniciar o actualizar el gateway IKE

Gestión de la puerta de enlace de IKE

- Network > Network Profiles > IKE Gateways

La siguiente tabla describe cómo gestionar las puertas de enlace IKE.

Gestión de puertas de enlace IKE	Description (Descripción)
Añadir	Para crear una nueva gateway IKE, haga clic en **Add (Añadir)**. Consulte en Pestaña General en IKE Gateway y Pestaña Advanced Options en IKE Gateway las instrucciones para configurar la nueva puerta de enlace.
delete	Para eliminar un gateway, selecciónela y haga clic en **Delete (Eliminar)**.
Habilitación	Para habilitar un gateway que se ha desactivado, seleccione el gateway y haga clic en **Enable (Habilitar)**, que es el ajuste predeterminado para el gateway.
Deshabilitar	Para deshabilitar un gateway, selecciónela y haga clic en **Disable (Deshabilitar)**.
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de configuración de objeto como **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla para elementos como las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.

Pestaña General de la puerta de enlace de IKE

- Network > Network Profiles > IKE Gateways > General

La siguiente tabla describe los ajustes iniciales para realizar la Configuración de una puerta de enlace IKE. IKE es la fase 1 del proceso VPN IKE/IPSec. Después de realizar la configuración, consulte la Pestaña de opciones avanzadas de la puerta de enlace IKE.

Configuración general de IKE Gateway	Description (Descripción)
Nombre	Introduzca un **Name (Nombre)** para identificar la puerta de enlace (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
versión	Seleccione la versión IKE que admite el gateway y debe aceptar el uso de un gateway de peer: **IKEv1 only mode (Modo exclusivo IKEv1)**, **IKEv2 only mode (Modo exclusivo IKEv2)** o **IKEv2 preferred mode (Modo preferido IKEv2)**. IKEv2 preferred mode (Modo preferido IKEv2) provoca que la

© 2020 Palo Alto Networks, Inc.

Configuración general de IKE Gateway	Description (Descripción)
	puerta de enlace negocie para el IKEv2 y esto se utilizará si el peer admite IKEv2; de lo contrario, la puerta de enlace vuelve a IKEv2.
Tipo de dirección	Seleccione el tipo de dirección IP que utiliza la puerta de enlace: **IPv4** o **IPv6**.
Interface (Interfaz)	Especifique la interfaz de cortafuegos saliente hacia el túnel VPN.
Dirección IP local	Seleccione o introduzca la dirección IP para la interfaz local que es el extremo del túnel.
Dirección IP del peer Tipo	Seleccione una de las siguientes configuraciones e introduzca la información correspondiente para el peer: • **Dynamic (Dinámico)**: seleccione esta opción si la dirección IP del peer o el valor de FQDN es desconocido. Cuando el tipo de dirección IP del peer es Dynamic (Dinámico), el peer debe iniciar la negociación con la puerta de enlace IKE. • **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 introduce un FQDN o un objeto de dirección de FQDN que resuelva 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 ha negociado una asociación de seguridad (security association, SA) de IKE, la dirección preferida es la dirección IP con el valor más pequeño. • Si se utiliza una dirección en la puerta de enlace de IKE y se encuentra en el conjunto de direcciones ofrecidas, se utiliza esta dirección (sea o no la más pequeña). • Si una dirección se utiliza en la puerta de enlace de IKE, pero no se encuentra en el conjunto de direcciones ofrecidas, se selecciona una nueva dirección: la dirección más pequeña en el conjunto. *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).*
Autenticación	Seleccione el tipo de autenticación: **Pre-Shared Key (Clave precompartida)** o **Certificate (Certificado)** que se producirá con la puerta de enlace del peer. Dependiendo de la selección, consulte Campos de claves precompartidas o Campos del certificado.
Campos de claves precompartidas	

© 2020 Palo Alto Networks, Inc.

Configuración general de IKE Gateway	Description (Descripción)
Clave precompartida / Confirmar clave precompartida	Si selecciona **Pre-Shared Key (Clave precompartida)**, introduzca una única clave de seguridad para usarla en la autenticación simétrica en el túnel. El valor de **Pre-Shared Key (Clave precompartida)** es una cadena que crea el administrador utilizando 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.
Identificación local	Define el formato e identificación de el gateway local, que se usa con la clave precompartida para el establecimiento IKEv1 fase 1 SA e IKEv2 SA. Seleccione entre los siguientes tipos e introduzca el valor: **FQDN** (nombre de host), **IP address (Dirección IP)**, **KEYID** (cadena de ID de formato binario en HEX) o **User FQDN (FQDN de usuario)** (dirección de correo electrónico). Si no especifica un valor, la puerta de enlace utilizará la dirección IP local como el valor de **Local Identification (Identificación local)**.
Identificación del peer	Define el formato e identificación del gateway local, que se usa con la clave precompartida durante el establecimiento IKEv1 fase 1 SA e IKEv2 SA. Seleccione entre los siguientes tipos e introduzca el valor: **FQDN** (nombre de host), **IP address (Dirección IP)**, **KEYID** (cadena de ID de formato binario en HEX) o **User FQDN (FQDN de usuario)** (dirección de correo electrónico). Si no especifica un valor, la puerta de enlace utilizará la dirección IP del peer como el valor de **Peer Identification (Identificación de peer)**.
Campos de Certificate	

Certificado local	Si se selecciona **Certificate (Certificado)** como tipo de **Authentication (Autenticación)** en la lista desplegable, seleccione un certificado que ya esté en el cortafuegos.
	
	Además, puede **Import (Importar)** un certificado o **Generate** uno nuevo, como se indica a continuación:
	
	Import (Importar):
	
	• **Certificate Name (Nombre del certificado)**: Introduzca un nombre para el certificado que está importando.
	• **Shared (Compartido)**: haga clic si este certificado debe compartirse entre múltiples sistemas virtuales.
	• **Certificate File (Archivo del certificado)**: haga clic en el botón **Browse** para desplazarse hasta la ubicación en la que se encuentra el archivo del certificado. Haga clic en el archivo y seleccione **Open (abierto)**.
	• **File Format (Formato de archivo)**: seleccione una de las opciones que se indican a continuación.
	  • **Base64 Encoded Certificate (PEM)**: contiene el certificado, pero no la clave. Texto claro.
	  • **Encrypted Private Key and Certificate (PKCS12)**: contiene tanto el certificado como la clave.

© 2020 Palo Alto Networks, Inc.

Configuración general de IKE Gateway	Description (Descripción)

	• **Private key resides on Hardware Security Module (La clave privada reside en el módulo de seguridad de hardware)**: haga clic si el cortafuegos es un cliente de un servidor HSM en el que reside la clave.
	• **Import private key (Importar clave privada)**: haga clic si debe importarse una clave privada porque está en un archivo distinto del archivo de certificados.
	  • **Key File (Archivo de clave)**: examine y navegue hasta el archivo de la clave que desea importar. Esta entrada aparece si selecciona PEM como Formato de archivo.
	  • **Passphrase (Frase de contraseña)** y **Confirm Passphrase (Confirmar frase de contraseña)**: escriba para acceder a la clave.

Local Certificate (Certificado local) (cont)	**Generate (Generar)**: • **Certificate Name (Nombre del certificado)**: escriba un nombre para el certificado que está creando. • **Common Name (Nombre común)**: introduzca el nombre común, que es la dirección IP o FQDN que aparecerá en el certificado. • **Shared (Compartido)**: haga clic si este certificado debe compartirse entre múltiples sistemas virtuales. • **Signed By (Firmado por)**: seleccione una Autoridad externa (CSR) o escriba la dirección IP del cortafuegos. Esta entrada debe ser una CA. • **Certificate Authority (Entidad de certificación)**: haga clic si el cortafuegos es la CA raíz. • **OCSP Responder**: Introduzca el OCSP que supervisa si el certificado es válido o se ha revocado. • **Algorithm (Algoritmo)**: seleccione RSA o Curva elíptica DSA para generar la clave para el certificado. • **Number of Bits (Número de bits)**: seleccione 512, 1024, 2048 o 3072 como número de bits en la clave. • **Digest (Resumen)**: seleccione md5, sha1, sha256, sha384 o sha512 como método para invertir la cadena desde el hash. • **Expiration (days) [Vencimiento (días)]**: escriba el número de días durante los cuales es válido el certificado. • **Certificate Attributes (Atributos del certificado)**: **Type (Tipo)**: opcionalmente, puede seleccionar tipos de atributo adicionales desde la lista desplegable para que estén en el certificado. • **Value (Valor)**: escriba un valor para el atributo.
Intercambio de certificado HTTP	Haga clic en **HTTP Certificate Exchange (Intercambio de certificado HTTP)** e introduzca la **Certificate URL (URL de certificados)** para utilizar el método de hash y URL para notificar al peer dónde recuperar el certificado. La URL de certificado es la URL del servidor remoto en el que ha almacenado su certificado. Si el peer indica que también admite hash y URL, los certificados se intercambian a través del intercambio entre hash y URL SHA1. Cuando el peer recibe la carga del certificado IKE, ve la URL HTTP y recupera el certificado de ese servidor. El peer utiliza el hash especificado

© 2020 Palo Alto Networks, Inc.

Configuración general de IKE Gateway	Description (Descripción)
	en la carga del certificado para comprobar los certificados descargados desde el servidor HTTP.
Identificación local	Identifica cómo se identifica el peer local en el certificado. Seleccione entre los siguientes tipos e introduzca el valor: **Distinguished Name (Nombre distintivo)** (Asunto), **FQDN** (nombre de host), **IP address (Dirección IP)** y **User FQDN (FQDN de usuario)** (dirección de correo electrónico).
Identificación del peer	Identifica cómo se identifica el peer remoto en el certificado. Seleccione entre los siguientes tipos e introduzca el valor: **Distinguished Name (Nombre distintivo)** (Asunto), **FQDN** (nombre de host), **IP address (Dirección IP)** y **User FQDN (FQDN de usuario)** (dirección de correo electrónico).
Comprobación de ID de peer	Seleccione **Exact (Exacto)** o **Wildcard (Comodín)**. Esta configuración se aplica a la identificación del peer que se examina para validar el certificado. Por ejemplo, si la identificación del peer es un nombre igual a domain.com, selecciona **Exact (Exacto)** y el nombre del certificado en la carga de la ID de IKE es mail.domain2.com, la negociación IKE fallará. Pero si seleccionó **Wildcard (Comodín)**, solo los caracteres en la cadena Name (Nombre) que preceda al asterisco comodín (*) deben coincidir, y cualquier caracter posterior al comodín puede ser distinto.
Permitir identificación de peer y falta de coincidencia de identificación de carga de certificado	Seleccione si desea la flexibilidad de tener una SA IKE con éxito aunque la identificación de peers no coincida con el payload del certificado.
Perfil del certificado	Seleccione un perfil o cree un nuevo **Certificate Profile (Perfil de certificado)** que configure las opciones de certificado que se apliquen al certificado que la puerta de enlace local envía a la puerta de enlace del peer. Consulte Device > Certificate Management > Certificate Profile.
Habilitar validación estricta de uso de clave extendida de peer	Seleccione esta opción si desea controlar estrictamente la forma en que puede utilizarse la clave.

Pestaña Opciones avanzadas de la puerta de enlace de IKE

- Network > Network Profiles > IKE Gateways > Advanced Options

Configure la configuración avanzada de la puerta de enlace de IKE, como el modo pasivo, NAT Traversal y la configuración IKEv1 como la detección del fallo del peer.

Advanced Options en IKE Gateway	Description (Descripción)
Habilitar modo pasivo	Haga clic para que el cortafuegos únicamente responda a las conexiones IKE y nunca las inicie.

© 2020 Palo Alto Networks, Inc.

Advanced Options en IKE Gateway	Description (Descripción)
Habilitar NAT transversal	Haga clic en esta opción para utilizar la encapsulación UDP en los protocolos IKE y UDP, permitiéndoles pasar a través de dispositivos de NAT intermedios. Seleccione Habilitar NAT Transversal si la traducción de dirección de red (NAT) está configurada en un dispositivo entre los puntos de terminación VPN IPSec.
Pestaña IKEv1	
Modo de intercambio	Seleccione **auto (automático)**, **aggressive (agresivo)** o **main (principal)**. En el modo **auto (automático)** (predeterminado), puede aceptar solicitudes de negociación tanto del modo **main** como del modo **aggressive (agresivo)**; sin embargo, siempre que sea posible, inicia la negociación y permite intercambios en el modo **main (principal)**. Debe configurar el dispositivo peer con el mismo modo de intercambio para permitir que acepte las solicitudes de negociación desde el primer dispositivo.
Perfil criptográfico IKE	Seleccione un perfil existente, mantenga el predeterminado o cree uno nuevo. Los perfiles seleccionados para IKEv1 e IKEv2 pueden diferir. Para obtener información sobre perfiles criptográficos IKE, consulte Red> Perfiles de red> IKE Crypto.
Habilitar fragmentación	Haga clic para permitir el gateway local para recibir los paquetes IKE fragmentados. El tamaño del paquete fragmentado máximo es de 576 bytes.
Detección de fallo del peer	Haga clic para habilitar e introducir un intervalo (2-100 segundos) y un retraso antes de volver a intentarlo (2-100 segundos). La detección de fallo del peer identifica peers IKE inactivos o no disponibles y puede ayudar a restablecer recursos que se pierden cuando un peer no está disponible.
Pestaña IKEv2	
Perfil criptográfico IKE	Seleccione un perfil existente, mantenga el predeterminado o cree uno nuevo. Los perfiles seleccionados para IKEv1 e IKEv2 pueden diferir. Para obtener información sobre perfiles criptográficos IKE, consulte Red> Perfiles de red> IKE Crypto.
Validación estricta de cookies	Haga clic para habilitar **Strict Cookie Validation (Validación estricta de cookies)** en el gateway IKE. • Cuando activa **Strict Cookie Validation (Validación estricta de cookies)**, la validación de cookies IKEv2 siempre se establece; el iniciador debe enviar un IKE_SA_INIT con una cookie. • Cuando desactiva **Strict Cookie Validation (Validación estricta de cookies)** (predeterminado), el sistema comprobará el número de SAs medio abiertas con el valor global en **Cookie Activation Threshold**, que es una configuración de sesión de VPN. Si el número de SA medio abiertas supera el **Cookie Activation Threshold (Umbral de activación**

© 2020 Palo Alto Networks, Inc.

Advanced Options en IKE Gateway	Description (Descripción)
	de cookies),, el iniciador debe enviar un IKE_SA_INIT que contienen una cookie.
Comprobación de actividad	La **Liveness Check (Comprobación de actividad)** IKEv2 siempre está activada; todos los paquetes IKEv2 sirven para una comprobación de actividad. Haga clic en esta casilla para que el sistema envíe paquetes informativos vacíos cuando el peer haya estado inactivo para un número especificado de segundos. Intervalo: 2-100. Default: 5 Si es necesario, el lado que intenta enviar paquetes IKEv2 realiza la prueba de comprobación de actividad hasta 10 veces (todos los paquetes IKEv2 cuentan en el ajuste de retransmisión). Si no recibe respuesta, el remitente cierra y elimina el IKE_SA y CHILD_SA. El remitente comienza enviando otro IKE_SA_INIT.

Reiniciar o actualizar el gateway IKE

- Network > IPSec Tunnels

Seleccione **Network (Red)** > **IPSec Tunnels (Túneles IPSec)** para ver el estado de los túneles. En la segunda columna Status (Estado) hay un enlace a la información de IKE. Haga clic en el gateway que desea reiniciar o actualizar. Se abre la página Info IKE. Seleccione una de las entradas de la lista y haga clic:

- **Restart (Reiniciar)**: reinicia la puerta de enlace seleccionada. Si reinicia, se interrumpirá el tráfico que atraviesa el túnel. Los comportamientos de reinicio IKEv1 e IKEv2 son diferentes, como sigue:
  - **IKEv1**: puede reiniciar (borrar) un SA de fase 1 o fase 2 independientemente y solo si ese SA se ve afectado.
  - **IKEv2**: hace que todos los SA secundarios (túneles de IPSec) se borren cuando se reinicia el SA IKEv2.

    Si reinicia el SA IKEv2, todos los túneles IPSec subyacentes se borrarán también.

    Si reinicia el túnel IPSec (SA secundario) asociado con un SA IKEv2, el reinicio no afectará al SA IKEv2.
- **Refresh (Actualizar)**: muestra el estado actual del SA de IKE.

Red > Perfiles de red > Criptográfico IPSec

Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **IPSec Crypto (Criptográfico de IPSec)** para configurar los perfiles criptográficos IPSec que especifican protocolos y algoritmos para la autenticación y el cifrado en túneles de VPN basándose en la negociación de SA IPSec (fase 2).

En el caso de los túneles VPN entre las puertas de enlace y los clientes de GlobalProtect, consulte Network > Network Profiles > GlobalProtect IPSec Crypto.

Configuración de perfiles criptográficos de IPSec	Description (Descripción)
Nombre	Introduzca un nombre en **Name (Nombre)** para el perfil (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles criptográficos de IPSec	Description (Descripción)
Protocolo IPSec	Seleccione un protocolo para asegurar los datos que atraviesan el túnel VPN: • **ESP**: el protocolo de carga de seguridad encapsulada (ESP) cifra los datos, autentica el origen y verifica la integridad de los datos. • **AH**: el protocolo de encabezado de autenticación (AH) autentica el origen y verifica la integridad de los datos. *Utilice el protocolo ESP debido a que proporciona confidencialidad de la conexión (cifrado), además de autenticación.*
Encryption (protocolo ESP únicamente)	Haga clic en **Add (Añadir)** y seleccione los algoritmos de cifrado deseados. Para mayor seguridad, use **Move Up (Mover hacia arriba)** y **Move Down (Mover hacia abajo)** para cambiar el orden (de arriba a abajo) por el siguiente: **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (el cortafuegos VM-Series no admite esta opción), **aes-128-cbc**, **3des** y **des**. También puede seleccionar **null (nulo)** (sin cifrado). *Utilice un formulario de cifrado AES. (DES y 3DES son algoritmos débiles y vulnerables).*
Autenticación	Haga clic en **Add (Añadir)** y seleccione los algoritmos de autenticación deseados. Para mayor seguridad, use **Move Up (Mover hacia arriba)** y **Move Down (Mover hacia abajo)** para cambiar el orden (de arriba a abajo) por el siguiente: **sha512**, **sha384**, **sha256**, **sha1**, **md5**. Si el **IPSec Protocol (Protocolo IPSec)** es **ESP**, también podrá seleccionar **none (ninguno)** (sin autenticación). *Utilice sha256 o una autenticación más segura, ya que md5 y sha1 no son seguros. Use sha256 para las sesiones de corta duración y sha384 o más para el tráfico que requiere la autenticación más segura, tal como las transacciones financieras.*
Grupo Dh	Seleccione el grupo Diffie-Hellman (DH) de intercambio de claves de Internet (IKE): **group1 (grupo1)**, **group2 (grupo2)**, **group5 (grupo5)**, **group14 (grupo14)**, **group19 (grupo19)** o **group20 (grupo20)**. 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 hacia delante): el cortafuegos reutiliza la clave actual para las negociaciones de asociación de seguridad (SA) de IPSec.
Duración	Seleccione unidades e introduzca la cantidad de tiempo (el valor predeterminado es de una hora) que la clave negociada permanecerá efectiva.
Duración	Seleccione unidades opcionales e introduzca la cantidad de datos que la clave puede utilizar para el cifrado.

© 2020 Palo Alto Networks, Inc.

Red > Perfiles de red > Criptográfico IKE

Utilice la página **IKE Crypto Profiles (Perfiles criptográficos de IKE)** para especificar protocolos y algoritmos para la identificación, la autenticación y el cifrado (IKEv1 o IKEv2, Fase 1).

Para cambiar el orden en el que se enumera un algoritmo o grupo, seleccione el elemento y, a continuación, haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. El orden determina la primera opción cuando se negocian los ajustes con un peer remoto. En primer lugar se intenta el ajuste de la parte superior de la lista, continuando hacia abajo en la lista hasta que un intento tiene éxito.

Configuración de perfiles criptográficos de IKE	Description (Descripción)
Nombre	Introduzca un Nombre para el perfil.
Grupo Dh	Especifique la prioridad de grupos Diffie-Hellman (DH). Haga clic **Add (añadir)** y seleccione los grupos: **group1 (grupo1)**, **group2 (grupo2)**, **group5 (grupo5)**, **group14 (grupo14)**, **group19 (grupo19)** o **group20 (grupo20)**. Para mayor seguridad, seleccione un elemento y, a continuación, haga clic en el icono **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para mover los grupos con identificadores numéricos más altos a la parte superior de la lista. Por ejemplo, mueva el **group14 (grupo14)** encima del **group2 (grupo2)**.
Autenticación	Especifique la prioridad de los algoritmos de hash. Haga clic en **Add (Añadir)** y seleccione algoritmos. Para mayor seguridad, seleccione un elemento y, a continuación, haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar el orden (de arriba a abajo) por el siguiente: **sha512**, **sha384**, **sha256**, **sha1**, **md5**.
Cifrado	Seleccione las opciones de autenticación apropiadas de Carga de seguridad encapsuladora (Encapsulating Security Payload, ESP). Haga clic en **Add (Añadir)** y seleccione algoritmos. Para mayor seguridad, seleccione un elemento y, a continuación, haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para cambiar el orden (de arriba abajo) por el siguiente: **aes-256-cbc**, **aes-192-cbc**, **aes-128-cbc**, **3des**, **des**.
Duración de la clave	Seleccione la unidad de tiempo e introduzca la cantidad de tiempo que la clave IKE fase 1 negociada permanecerá efectiva (el valor predeterminado es 8 horas). • IKEv2: Antes de que venza la clave, se deberá volver a introducir la clave de registro de SA, cuando llegue el vencimiento, la SA deberá comenzar una nueva negociación de clave de fase 1. • IKEv1: No realizará activamente una clave de registro de fase 1 antes del vencimiento. Solo cuando venza la SA IPSec IKEv1 se activará la clave de registro del IKEv1 de fase 1.
Autenticación IKEv2 múltiple	Especifique un valor (el intervalo es 0-50, el valor predeterminado es 0) que se multiplique por la Duración de la clave para determinar el recuento de autenticaciones. El recuento de autenticaciones es el número de veces que la puerta de enlace puede regenerar la clave de codificación de SA IKE IKEv2 antes de que la puerta deba volver a empezar con la reautenticación IKEv2. El valor 0 desactiva la función de reautenticación.

© 2020 Palo Alto Networks, Inc.

Red > Perfiles de red > Supervisar

Un perfil de supervisión se utiliza para supervisar las reglas de reenvío basado en políticas (PBF) de túneles de IPSec y dispositivos de siguiente salto. En ambos casos, el perfil de supervisión se utiliza para especificar la medida que se adoptará cuando un recurso (túnel de IPSec o dispositivo de siguiente salto) no esté disponible. Los perfiles de supervisión son opcionales pero pueden ser de gran utilidad para mantener la conectividad entre sitios y para garantizar el cumplimiento de las reglas PBF. Los siguientes ajustes se utilizan para configurar un perfil de supervisión.

Campo	Description (Descripción)
Nombre	Introduzca un nombre para identificar el perfil de supervisión (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Acción	Especifique la acción que se realizará si el túnel no está disponible. Si el número de umbral de latidos se pierde, el cortafuegos realiza la acción especificada. • **wait-recover (esperar recuperación)**: Espera a que el túnel se recupere, no realiza ninguna acción adicional. Los paquetes continuarán enviándose de acuerdo con la regla PBF. • **fail-over (conmutación por error)**: El tráfico cambiará a una ruta de seguridad, si existe una disponible. El cortafuegos utiliza la búsqueda de tabla de enrutamiento para determinar el enrutamiento durante la sesión. En ambos casos, el cortafuegos intentará negociar nuevas claves de IPSec para acelerar la recuperación.
Intervalo	Especifique el tiempo entre latidos (intervalo 2-10; opción predefinida 3).
Umbral	Especifique el número de latidos que se perderán antes de que el cortafuegos realice la acción especificada (intervalo 2-10; opción predefinida 5).

Network > Network Profiles > Interface Mgmt

Un perfil de gestión de interfaz protege al cortafuegos del acceso no autorizado mediante la definición de los servicios y las direcciones IP que una interfaz de cortafuegos permite. 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) Para asignar un perfil de gestión de interfaz, consulte Network > Interfaces.

No adjunte un perfil de gestión de interfaz que permita Telnet, SSH, HTTP o HTTPS a una interfaz que permita acceso desde internet o desde otras zonas no fiables dentro de sus límites de seguridad empresariales. Esto incluye la interfaz donde ha configurado un portal o puerta de enlace de GlobalProtect; GlobalProtect no requiere un perfil de gestión de interfaz para permitir acceso al portal o la puerta de enlace. Consulte Prácticas recomendadas de seguridad del acceso administrativo *para obtener información detallada sobre cómo proteger el acceso a sus cortafuegos y Panorama.*

© 2020 Palo Alto Networks, Inc.

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.

Campo	Description (Descripción)
Nombre	Introduzca un nombre de perfil (de hasta **31** caracteres). Este nombre aparece en la lista de perfiles de gestión de interfaz cuando se configuran las interfaces. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Servicios de gestión administrativa	• **Telnet**: utilícelo para acceder a la CLI del cortafuegos. Telnet usa texto sin formato, lo cual no es tan seguro como SSH. *Habilite SSH en lugar de Telnet para la gestión del tráfico en la interfaz.* • **SSH**: utilícelo para el acceso seguro a la CLI del cortafuegos. • **HTTP**: utilícelo para acceder a la interfaz web del cortafuegos. HTTP usa texto sin formato, lo cual no es tan seguro como HTTPS. *Habilite HTTPS en lugar de HTTP para la gestión del tráfico en la interfaz.* • **HTTPS**: utilícelo para el acceso seguro a la interfaz web del cortafuegos.

Servicios de red	• **Ping**: utilícelo para probar la conectividad con los servicios externos. Por ejemplo, puede hacer ping a la interfaz para verificar que puede recibir el softwre PAN-OS y las actualizaciones de contenido del servidor de actualización de Palo Alto Networks.
	• **HTTP OCSP**: utilícelo para configurar el cortafuegos como un respondedor de Protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP). Para obtener más información, consulte Device > Certificate Management > OCSP Responder.
	• **SNMP**: utilícelo para procesar consultas de estadísticas de cortafuegos desde el gestor SNMP. Para obtener más información, consulte Habilitación de supervisión de SNMP.
	• **Response Pages (Páginas de respuesta)**: utilícela para habilitar páginas de respuesta para lo siguiente:
	  • **Captive Portal**: los puertos utilizados para atender las páginas de respuesta de Captive Portal permanecen abiertos en las interfaces de capa 3: puerto 6080 para NTLM, 6081 para Captive Portal sin perfil de servidor SSL/TLS y 6082 para Captive Portal con un perfil de servidor SSL/TLS. Para obtener más información, consulte Device > User Identification > Captive Portal Settings.
	  • **URL Admin Override (Cancelación de administrador de URL)**: para obtener más información, consulte Device > Setup > Content-ID.
	• **User-ID**: utilícelo para habilita la Redistribución de asignaciones de usuarios entre cortafuegos.
	• **User-ID Syslog Listener-SSL (SSL de escucha de Syslog de User-ID)**: utilícelo para habilitar el agente de ID de usuario integrado en PAN-OS para recopilar los mensajes de syslog en SSL. Para obtener más información, consulte Configuración de acceso a servidores supervisados.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **User-ID Syslog Listener-UDP (UDP de escucha de Syslog de User-ID)**: utilícelo para habilitar el agente de ID de usuario integrado en PAN-OS para recopilar los mensajes de syslog en UDP. Para obtener más información, consulte Configuración de acceso a servidores supervisados.
Direcciones IP permitidas	Introduzca la lista de direcciones IPv4 o IPv6 desde las que la interfaz permite el acceso.

Network > Network Profiles > Zone Protection

Un perfil de protección de zona aplicado a una zona ofrece protección frente a las habituales inundaciones, ataques de reconocimiento, otros ataques basados en paquetes y el uso de protocolos no IP. Está diseñado para proporcionar una protección amplia en la zona de entrada (la zona donde el tráfico entra en el cortafuegos) y no está diseñado para proteger un host de extremo específico o el tráfico dirigido a una zona de destino particular. Puede adjuntar un perfil de protección de zona a una zona.

Aplique un perfil de protección de zona a cada zona para extender protección adicional contra congestiones de IP, reconocimiento, ataques basados en paquetes y ataques de protocolo no IP. La protección de zona en el cortafuegos debe ser una segunda capa de protección después de un dispositivo DDoS dedicado en el perímetro de Internet.

Para mejorar las capacidades de protección de zona en el cortafuegos, configure una política de protección DoS (Policies > DoS Protection) de forma que coincida con una zona, una interfaz, una dirección IP o un usuario específico.

La protección de zona se aplica solo cuando no hay coincidencia de sesión del paquete porque la protección de zona se basa en conexiones por segundo (cps) nuevas, no en paquetes por segundo (pps). Si el paquete coincide con una sesión existente, sorteará el ajuste de protección de zona.

¿Qué está buscando?	Consulte:
¿Cómo creo un perfil de protección de zona?	Componentes de perfiles de protección de zonas Protección contra inundaciones Protección de reconocimiento Protección de ataque basada en paquetes Protección de protocolo

Componentes de perfiles de protección de zonas

Para crear un perfil de protección de zonas, haga clic en **Add (Añadir)** un perfil y nómbrelo.

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas	Configurado en	Description (Descripción)
Nombre	**Network (Red)** > **Network Profiles (Perfiles de redes)** > **Zone Protection (Protección de zonas)**	Introduzca un nombre de perfil (de hasta 31 caracteres). Este nombre aparece en la lista de perfiles de protección de zonas cuando se configuran las zonas. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice únicamente letras, números, espacios y guiones bajos.
Description (Descripción)		Introduzca una descripción opcional para el perfil de protección de zonas.

Continúe y cree un perfil de Protección de zona a través de la configuración de cualquier combinación de parámetros basados en los tipos de protección que su zona necesita:

- Protección contra inundaciones
- Protección de reconocimiento
- Protección de ataque basada en paquetes
- Protección de protocolo

Si tiene un entorno de sistema virtual múltiple y ha activado lo siguiente:

- *Zonas externas para permitir la comunicación entre sistemas virtuales*
- *Puertas de enlace compartidas para permitir que los sistemas virtuales compartan una interfaz común y una dirección IP para las comunicaciones externas.*

Los siguientes mecanismos de protección de zona y de DoS se deshabilitarán en la zona externa:

- *Cookies de sincronización*
- *Fragmentación de IP*
- *ICMPv6*

Para activar la fragmentación IP y la protección ICMPv6 para la puerta de enlace compartida, debe crear un perfil de Protección de zona separado para la puerta de enlace compartida.

Para activar la protección frente a inundaciones SYN en una puerta de enlace compartida puede aplicar un perfil de protección de inundación SYN con descarte aleatorio temprano o cookies SYN; en una zona externa solo está disponible el descarte aleatorio temprano para la protección frente a inundación SYN

Protección contra inundaciones

- Network > Network Profiles > Zone Protection > Flood Protection

Configure un perfil que proporcione protección contra inundaciones de paquetes SYN, ICMP, ICMPv6, SCTP INIT y UDP, además de protección contra inundaciones de otros tipos de paquetes IP. Las tasas se indican en conexiones por segundo; por ejemplo, un paquete SYN entrante que no coincida con una sesión existente se considera una conexión nueva.

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
SYN	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)**	Seleccione esta opción para activar la protección contra inundaciones SYN.

Acción		Seleccione la acción que se adoptará en respuesta a un ataque de inundación SYN.
		• **Random Early Drop (Descarte aleatorio temprano)**: permite descartar paquetes SYN para mitigar un ataque por inundación:
		  • Si el flujo supera el umbral de tasa de **Alert (Alerta)**, se genera una alarma.
		  • Cuando el flujo supera el umbral de tasa de **Activate (Activación)**, El cortafuegos descarta paquetes SYN individuales de forma aleatoria para restringir el flujo.
		  • Si el flujo supera el umbral de tasa **Maximum (Máxima)**, se descarta el 100 % de los paquetes SYN entrantes.
		• **Cookies SYN**: hace que el cortafuegos actúe como un proxy, intercepte el SYN, genere una cookie en nombre del servidor al que se dirigía el SYN, y envíe un SYN-ACK con la cookie a la fuente original. Sólo cuando la fuente devuelve una ACK (confirmación) con la cookie al cortafuegos, este considera la fuente válida y envía el SYN al servidor. Esta es la acción preferida.
		Las cookies SYN manejan el tráfico legítimo de manera equitativa, pero consumen mas recursos del cortafuegos que RED. Si las cookies SYN consumen muchos recursos, cambie a RED. Si no tiene un dispositivo de prevención de DDoS dedicado delante del cortafuegos (en el perímetro de Internet), siempre use RED.

Tasa de alarma (conexiones/seg)	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Introduzca el número de paquetes SYN (que no coincida con una sesión existente) que la zona recibe por segundo que activa una alarma. Las alarmas se pueden ver en el Dashboard y en el log de amenazas (Monitor > Packet Capture). El intervalo es 0-2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral un 15-20 % por encima de la tasa de CPS de zona promedio para contemplar

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
		las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas.
Activar (conexiones/seg)		Introduzca el número de paquetes SYN (que no coincida con una sesión existente) que la zona recibe por segundo y que activa la Acción especificada en este perfil de Protección de zona. El cortafuegos utiliza un algoritmo para progresivamente descartar más paquetes a medida que aumenta la tasa de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos deja de descartar paquetes SYN si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral apenas por encima de la tasa de CPS pico de la zona, para evitar la limitación del tráfico legítimo y ajustar el umbral según fuera necesario.
Máximo (conexiones/seg)		Introduzca el número máximo de paquetes SYN (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000; el valor predeterminado es 40 000. Si se cruza este umbral, se bloquean las conexiones nuevas hasta que la tasa de CPS disminuye por debajo del umbral. Se recomienda configurar el umbral al 80-90 % de la capacidad del cortafuegos, teniendo en cuenta otras características que consumen los recursos del cortafuegos.
ICMP	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Seleccione esta opción para habilitar la protección contra inundaciones ICMP.
Tasa de alarma (conexiones/seg)		Introduzca el número de solicitudes de eco ICMP (pings que no coincidan con una sesión existente) que la zona recibe por segundo y que activa una alarma de ataque. El intervalo es 0-2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral un 15-20 % por encima de la tasa de CPS de zona promedio para contemplar las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas.
Activar (conexiones/seg)		Introduzca el número de paquetes ICMP (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten paquetes ICMP posteriores. El cortafuegos utiliza un algoritmo para progresivamente

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
		descartar más paquetes a medida que aumenta la tasa de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos detiene el descarte de los paquetes ICMP si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral apenas por encima de la tasa de CPS pico de la zona, para evitar la limitación del tráfico legítimo y ajustar el umbral según fuera necesario.
Máximo (conexiones/seg)		Introduzca el número máximo de paquetes ICMP (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000; el valor predeterminado es 40 000. Se recomienda configurar el umbral al 80-90 % de la capacidad del cortafuegos, teniendo en cuenta otras características que consumen los recursos del cortafuegos.
SCTP INIT (INIT DE SCTP)	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Seleccione esta opción para habilitar la protección contra inundaciones de paquetes de Protocolo de transmisión de control de secuencias (Stream Control Transmission Protocol, SCTP) que contengan un fragmento de inicialización (INIT). Un fragmento de INIT no se puede agrupar con otros fragmentos, de modo que el paquete se denomina paquete de INIT de SCTP.
Tasa de alarma (conexiones/seg)		Introduzca el número de paquetes de INIT de SCTP (que no coincida con una sesión existente) que la zona recibe por segundo y que activa una alarma de ataque. El intervalo es de 0-2 000 000. El valor predeterminado por modelo de cortafuegos es: • **PA-5280**: 10 000 • **PA-5260**: 7000 • **PA-5250**: 5000 • **PA-5220**: 3000 • **VM-700**: 1000 • **VM-500**: 500 • **VM-300**: 250 • **VM-100**: 200 • **VM-50**: 100

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
Activar (conexiones/seg)		Introduzca el número de paquetes INIT de SCTP (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten paquetes de INIT de SCTP posteriores. El cortafuegos utiliza un algoritmo para progresivamente descartar más paquetes a medida que aumenta la tasa de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos detiene el descarte de los paquetes de INIT de SCTP si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000. El valor predeterminado por modelo de cortafuegos es el mismo que para la tasa de alarma.
Máximo (conexiones/seg)	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Introduzca el número máximo de paquetes de INIT de SCTP (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000. El valor predeterminado por modelo de cortafuegos es: • **PA-5280:** 20 000 • **PA-5260**: 14 000 • **PA-5250**—10.000 • **PA-5220**: 6000 • **VM-700**: 2000 • **VM-500**—1.000 • **VM-300**—500 • **VM-100**: 400 • **VM-50**—200
UDP	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Seleccione esta opción para habilitar la protección contra inundaciones UDP.
Tasa de alarma (conexiones/seg)		Introduzca el número de paquetes UDP (que no coincida con una sesión existente) que la zona recibe por segundo que activa una alarma de ataque. El intervalo es 0-2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral un 15-20 % por encima de la tasa de CPS de zona promedio para contemplar las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas.
Activar (conexiones/seg)		Introduzca el número de paquetes UDP (que no coincida con una sesión existente) que la zona recibe por segundo que activa el descarte aleatorio de paquetes UDP. El cortafuegos utiliza un algoritmo para progresivamente descartar más paquetes a medida que aumenta la tasa

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
		de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos detiene el descarte de los paquetes UDP si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral apenas por encima de la tasa de CPS pico de la zona, para evitar la limitación del tráfico legítimo y ajustar el umbral según fuera necesario.
Máximo (conexiones/seg)		Introduzca el número máximo de paquetes UDP (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000; el valor predeterminado es 40 000. Se recomienda configurar el umbral al 80-90 % de la capacidad del cortafuegos, teniendo en cuenta otras características que consumen los recursos del cortafuegos.
ICMPv6	**Network (Red) > Network Profiles (Perfiles de red) > Zone Protection (Zona de protección) > Flood Protection (Protección contra inundaciones)** (cont.)	Seleccione esta opción para habilitar la protección contra inundaciones ICMPv6.
Tasa de alarma (conexiones/seg)		Introduzca el número de solicitudes de eco ICMPv6 (pings que no coincidan con una sesión existente) que la zona recibe por segundo y que activa una alarma de ataque. El intervalo es 0-2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral un 15-20 % por encima de la tasa de CPS de zona promedio para contemplar las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas.
Activar (conexiones/seg)		Introduzca el número de paquetes ICMPv6 (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten paquetes ICMPv6 posteriores. El cortafuegos utiliza un algoritmo para progresivamente descartar más paquetes a medida que aumenta la tasa de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos detiene el descarte de los paquetes ICMPv6 si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral apenas por encima de la tasa de CPS pico de la zona, para evitar la limitación del tráfico legítimo y ajustar el umbral según fuera necesario.

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
Máximo (conexiones/seg)		Introduzca el número máximo de paquetes ICMPv6 (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000; el valor predeterminado es 40 000. Se recomienda configurar el umbral al 80-90 % de la capacidad del cortafuegos, teniendo en cuenta otras características que consumen los recursos del cortafuegos.
Otra IP	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** > **Flood Protection (Protección contra inundaciones)** (cont.)	Seleccione esta opción para habilitar la protección contra otras inundaciones IP (no TCP, no ICMP, no ICMPv6, no SCTP y no UDP).
Tasa de alarma (conexiones/seg)		Introduzca el número de otros paquetes IP (no TCP, no ICMP, no ICMPv6, no SCTP y no UDP) (que no coincida con una sesión existente) que recibe la zona por segundo y que activa una alarma de ataque. El intervalo es 0-2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral un 15-20 % por encima de la tasa de CPS de zona promedio para contemplar las fluctuaciones normales y ajustar el umbral si recibe demasiadas alarmas.
Activar (conexiones/seg)		Ingrese el número de otros paquetes IP (no-TCP, no-ICMP, no-ICMPv6 y no-UDP) (que no coincida con una sesión existente) que la zona recibe por segundo que activa el descarte aleatorio de otros paquetes IP. El cortafuegos utiliza un algoritmo para progresivamente descartar más paquetes a medida que aumenta la tasa de ataque, hasta que la tasa alcanza la tasa máxima. El cortafuegos deja de descartar los demás paquetes IP si la tasa de entrada cae por debajo del umbral Activate (Activación). El intervalo es de 1 a 2 000 000; el valor predeterminado es 10 000. Se recomienda configurar el umbral apenas por encima de la tasa de CPS pico de la zona, para evitar la limitación del tráfico legítimo y ajustar el umbral según fuera necesario.
Máximo (conexiones/seg)		Introduzca el número máximo de otros paquetes IP (no TCP, no ICMP, no ICMPv6 , no UDP) (que no coincida con una sesión existente) que la zona recibe por segundo antes de que se descarten los paquetes que excedan el máximo. El intervalo es de 1 a 2 000 000; el valor predeterminado es 40 000.

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección contra inundaciones	Configurado en	Description (Descripción)
		Se recomienda configurar el umbral al 80-90 % de la capacidad del cortafuegos, teniendo en cuenta otras características que consumen los recursos del cortafuegos.

Protección de reconocimiento

- Network > Network Profiles > Zone Protection > Reconnaissance Protection

Los siguientes ajustes definen la protección de reconocimiento:

Configuración de Perfil de protección de zonas: Protección de reconocimiento	Configurado en	Description (Descripción)
Examen de puerto TCP	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** > **Reconnaissance Protection (Protección de reconocimiento)**	**Enable (Habilitar)** configura el perfil para habilitar la protección contra los análisis del puerto TCP.
Examen de puerto de UDP		**Enable (Habilitar)** configura el perfil para habilitar la protección contra los análisis del puerto UDP.
Limpieza de host		**Enable (Habilitar)** configura el perfil para habilitar la protección contra la limpieza de host.
Acción		Acción que el sistema adoptará como respuesta al intento de reconocimiento correspondiente: • **Allow (Permitir)**: Permite la exploración de puerto o reconocimiento de limpieza de host. • **Alert (Alertar)**: Genera una alerta para cada exploración de puerto o limpieza de host que coincida con el umbral del intervalo de tiempo especificado (la acción predeterminada). • **Block (Bloquear)**: descarta todos los paquetes subsiguientes enviados desde el origen al destino durante el resto del intervalo de tiempo especificado. • **Block IP**: descarta todos los paquetes subsiguientes para la **Duration (Duración)** especificada, en segundos (el intervalo es 1-3.600). **Track By (Seguir por)** determina si bloquear el tráfico de origen o el de origen y destino. Por ejemplo, bloquea intentos por encima del número límite por intervalo que son de un único origen (más riguroso) o bloquea intentos que tienen un par de origen y destino (menores riguroso).

© 2020 Palo Alto Networks, Inc.

Configuración de Perfil de protección de zonas: Protección de reconocimiento	Configurado en	Description (Descripción)
		Bloquee todas las exploraciones de reconocimiento, excepto las exploraciones de prueba de vulnerabilidades internas.
Intervalo (seg)		El intervalo de tiempo, en segundos, para la detección del examen de puerto TCP o UDP (el intervalo es de 2 a 65 535; el valor predeterminado es 2). El intervalo de tiempo, en segundos, para la detección de limpieza de host (el intervalo es de 2 a 65 535; el valor predeterminado es 10).
Umbral (eventos)		El número de eventos de puertos o eventos de limpieza de host explorados dentro del intervalo de tiempo especificado que activa la acción (el intervalo es 2-65.535; el predeterminado es 100). *Utilice el límite de evento predeterminado para registrar algunos paquetes para el análisis, antes de bloquear los intentos de reconocimiento.*
Exclusión de dirección origen		Las direcciones IP que están permitidas en la protección de reconocimiento. La lista admite un máximo de 20 direcciones IP u objetos de dirección de máscara de red. • name: Introduzca un nombre descriptivo para la dirección que va a excluir. • Address Type: Seleccione IPv4 o IPv6 del menú desplegable. • Address: Seleccione una dirección u objeto de dirección del menú desplegable o introduzca uno manualmente. *Excluya solo las direcciones IP para los grupos internos fiables que realicen la prueba de vulnerabilidad de "sombrero blanco".*

Protección de ataque basada en paquetes

- Network > Network Profiles > Zone Protection > Packet Based Attack Protection

Puede configurar la protección de ataque basado en paquetes para descartar los siguientes tipos de paquetes:

- Descarte IP
- Descarte TCP
- Descarte de ICMP
- Colocación de IPv6
- Colocación de ICMPv6

© 2020 Palo Alto Networks, Inc.

Descarte IP

Para indicarle al cortafuegos qué hacer con determinados paquetes de IP que recibe en la zona, seleccione estas opciones:

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
Dirección IP replicada	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** > **Packet Based Attack Protection (Protección de ataque basada en paquetes)** > **IP Drop**	Verifique que la dirección IP de origen del paquete de entrada sea enrutable y que la interfaz de enrutamiento esté en la misma zona que la interfaz de entrada. Si alguna de las condiciones no se cumple, descarte el paquete. *Solo en las zonas internas, descarte los paquetes de dirección IP duplicada para garantizar que en la entrada, la dirección de origen coincida con la tabla de enrutamiento del cortafuegos.*
Comprobación de dirección IP estricta		Compruebe que ambas condiciones se cumplan: • La dirección IP de origen no es la dirección IP de transmisión de subred de la interfaz de entrada. • La dirección IP de origen se puede enrutar a través de la interfaz de entrada exacta. Si alguna de las condiciones no se cumple, descarte el paquete. En un cortafuegos en modo Criterios comunes (Common Criteria, CC), puede habilitar el registro para los paquetes descartados. En la interfaz web del cortafuegos, seleccione **Dispositivo** > **Configuración de log**. En la sección Manage Logs, seleccione **Selective Audit (Auditoría selectiva)** y habilite **Packet Drop Logging (Logs de descarte de paquetes)**.
Tráfico fragmentado		Descarte los paquetes IP fragmentados.
Descartar opciones IP		Seleccione la configuración de este grupo para habilitar el cortafuegos de forma que descarte los paquetes que contienen estas opciones de IP.
Enrutamiento de fuente estricto		Descarta paquetes con la opción de IP de enrutamiento de origen estricto activada. Strict Source Routing (Enrutamiento de fuente estricto) es una opción con la que una fuente de un datagrama proporciona información de enrutamiento a través de la cual una puerta de enlace o un host debe enviar el datagrama. *Descarte los paquetes con enrutamiento de origen estricto porque el enrutamiento de origen permite que los adversarios omitan las reglas de política de*

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
		seguridad que usen la dirección IP de destino como criterio de coincidencia.
Enrutamiento de origen no estricto		Descarta paquetes con la opción de IP de enrutamiento de origen no estricto activada. Loose Source Routing (Enrutamiento de origen no estricto) es una opción mediante la cual una fuente de un datagrama proporciona información de enrutamiento y una puerta de enlace o un host recibe autorización para elegir cualquier ruta de una serie de puertas de enlace intermedias para obtener el datagrama de la siguiente dirección de la ruta. *Descarte los paquetes con enrutamiento de origen flexible porque el enrutamiento de origen permite que los adversarios omitan las reglas de política de seguridad que usen la dirección IP de destino como criterio de coincidencia.*
Marca de tiempo		Descarta paquetes con la opción de marca de tiempo activada.
Ruta de log		Descarta paquetes con la opción de ruta de log activada. Cuando un datagrama presenta esta opción, cada enrutador que enruta el datagrama añade su propia dirección IP al encabezado, lo que proporciona la ruta al destinatario.
Security		Descarta paquetes con la opción de seguridad activada.
ID de secuencia		Descarta paquetes con la opción de ID de secuencia activada.
unknown		Descarta paquetes si no se conoce la clase ni el número. *Descarte los paquetes desconocidos.*
Formada incorrectamente		Descarta paquetes si tienen combinaciones incorrectas de clase, número y longitud basadas en RFC 791, 1108, 1393 y 2113. *Descarte los paquetes con formato incorrecto.*

© 2020 Palo Alto Networks, Inc.

Descarte TCP

Para indicarle al cortafuegos qué hacer con determinados paquetes de TCP que recibe en la zona, seleccione estas opciones:

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
Segmento TCP superpuesto no coincidente	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** > **Packet Based Attack Protection (Protección de ataque basada en paquetes)** > **TCP Drop (Descarte TCP)**	Los atacantes pueden construir conexiones con datos superpuestos pero diferentes en ellos, para conseguir una interpretación equivocada de la intención de la conexión. Los atacantes puede utilizar la replicación de IP y la predicción de números de secuencia para interceptar la conexión de un usuario e introducir sus propios datos. Utilice este parámetro para generar un informe sobre una falta de coincidencia de superposición y coloque el paquete cuando los datos de segmento no coincidan en estas situaciones: • El segmento está dentro de otro segmento. • El segmento está superpuesto a parte de otro segmento. • El segmento cubre otro segmento. Este mecanismo de protección utiliza números de secuencia para determinar el lugar donde residen los paquetes dentro del flujo de datos TCP. *Descarte los paquetes con segmentos TCP superpuestos coincidentes.*
Protocolo de enlace dividido		Evite que una sesión TCP se establezca si el procedimiento de establecimiento de sesión no usa la reconocida presentación de tres pasos. La presentación dividida de cuatro o cinco pasos o un procedimiento de establecimiento de sesión abierta simultánea son ejemplos de variaciones que no se permiten. El cortafuegos del última generación Palo Alto Networks gestiona correctamente sesiones y todos los procesos de capa 7 para la presentación de enlace dividido y un establecimiento de sesión abierta simultánea sin configurar **Split Handshake (Protocolo de enlace dividido)**. Cuando esto se configura para un perfil de protección de zona y el perfil se aplica a una zona, las sesiones TCP para interfaces de esa zona deben establecerse usando una presentación estándar de tres direcciones; no se permiten las variaciones. *Descarte los paquetes con protocolo de enlace dividido.*

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
TCP SYN con datos		Evita que se establezca una sesión TCP si el paquete TCP SYN contiene datos durante un protocolo de enlace de tres pasos. De forma predeterminada, esta opción está habilitada.
TCP SYNACK con datos		Evita que se establezca una sesión TCP si el paquete TCP SYN-ACK contiene durante un protocolo de enlace de tres pasos. De forma predeterminada, esta opción está habilitada.
Rechazar TCP sin SYN		Determine si el paquete se rechazará si el primer paquete de la configuración de sesión TCP no es un paquete SYN: • **global**: Utilice el ajuste del sistema asignado mediante CLI. • **yes (Sí)**: Rechaza TCP sin SYN. • **No**: Acepta TCP sin SYN. *El permitir el tráfico que no es de sincronización de TCP puede impedir que las políticas de bloqueo de archivos funcionen de la forma esperada en aquellos casos en los que no se establece la conexión del cliente o servidor después de que se produzca el bloqueo.* *Si configura la inspección de contenido de túnel en una zona y habilita Rematch Sessions (Volver a cotejar sesiones), solo para esa zona, deshabilite Reject Non-SYN TCP (Rechazar TCP no sincronizados) de modo que la habilitación o edición de una política de inspección de contenido de túnel no provoque que el cortafuegos descarte sesiones de túnel existentes.*
Ruta asimétrica		Determine si los paquetes que contienen números de secuencia fuera del umbral o ACK de fallo de sincronización se descartarán o se derivarán: • **global**: Utilice el ajuste del sistema asignado mediante CLI. • **drop (descartar)**: Descarte los paquetes que contienen una ruta asimétrica. • **bypass (derivar)**: Derive los paquetes que contienen una ruta asimétrica.
Quitar opciones TCP		Determine si quitar la opción TCP Timestamp o TCP Fast Open de los paquetes TCP.
Marca de tiempo TCP	**Network (Red)** > **Network**	Determine si el paquete tiene una marca de tiempo de TCP en el encabezado y, si es así, elimínela.

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
	Profiles (Perfiles de red) > **Zone Protection (Protección de zona)** > **Packet Based Attack Protection (Protección de ataque basada en paquetes)** > **TCP Drop (Descarte TCP)**	*Elimine la marca de tiempo de TCP en los paquetes que la tengan, para prevenir un ataque DoS de marca de tiempo.*
TCP de apertura rápida		Retire la opción TCP Fast Open (y la carga de datos, si la hubiere) del paquete TCP SYN o SYN-ACK durante un protocolo de enlace de tres pasos. Cuando está desactivada (deshabilitada), se permite la opción TCP Fast Open, que preserva la velocidad de una configuración de conexión incluyendo la entrega de datos. Esto funciona independientemente de TCP SYN con datos y TCP SYN-ACK con datos. De forma predeterminada, esta opción está deshabilitada.
Opciones TCP (MPTCP) multipath		MPTCP es una extensión de TCP que permite a un cliente mantener una conexión al utilizar simultáneamente varias rutas para conectarse al host de destino. De forma predeterminada, el soporte MPTCP está deshabilitado, basado en la configuración global MPTCP. Revise o ajuste la configuración de MPTCP para las zonas de seguridad asociadas con este perfil: • **no**: habilita el soporte MPTCP (no quitar la opción MPTCP). • **yes (sí)**: deshabilita el soporte MPTCP (retira la opción MPTCP). Con esta configuración, las conexiones MPTCP se convierten en conexiones TCP estándar, ya que MPTCP es compatible con TCP. • **(Default) global [(Predeterminado) global]**: soporta MPTCP basado en el ajuste global de MPTCP. De forma predeterminada, la configuración global MPTCP se establece en sí para que MPTCP se deshabilita (la opción MPTCP se quita del paquete). Puede revisar o ajustar la configuración MPTCP global mediante el siguiente comando CLI: `# set deviceconfig setting tcp strip-mptcp-option <yes| no>`

© 2020 Palo Alto Networks, Inc.

Descarte de ICMP

Para indicarle al cortafuegos que descarte determinados paquetes ICMP que recibe en la zona, active estas opciones:

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
ID de 0 de ping de ICMP	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** > **Packet Based Attack Protection (Protección de ataque basada en paquetes)** > **ICMP Drop (Descarte de ICMP)**	Descarte paquetes si el paquete de ping de ICMP tiene un identificador con el valor de 0.
Fragmento de ICMP		Descarte paquetes formados con fragmentos ICMP.
Paquete de ICMP de gran tamaño (>1024)		Descarte paquetes ICMP con un tamaño mayor de 1024 bytes.
Descartar ICMP incrustado con mensaje de error		Descarte los paquetes ICMP que se incrustan con un mensaje de error.
Suprimir error caducado ICMP TTL		Detiene el envío de mensajes caducados ICMP TTL.
Suprimir fragmento de ICMP necesario		Detiene el envío de mensajes necesarios para la fragmentación ICMP en respuesta a paquetes que exceden la interfaz MTU que tienen el bit no fragmentar (DF) activado. Este ajuste interfiere el proceso PMTUD que ejecutan los hosts tras el cortafuegos.

Colocación de IPv6

Para indicarle al cortafuegos que descarte determinados paquetes IPv6 que recibe en la zona, active estas opciones:

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
Encabezado de enrutamiento tipo 0	**Network (Red)** > **Network**	Descarte los paquetes IPv6 que contienen un encabezado de enrutamiento de Tipo 0. Consulte RFC 5095 para leer información de encabezado de enrutamiento de tipo 0.

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
IPv4 compatible address	**Profiles (Perfiles de red) > Zone Protection (Protección de zona) > Packet Based Attack Protection (Protección de ataque basada en paquetes) > IPv6 Drop**	Descarte los paquetes IPv6 que se definen como una dirección IPv6 compatible con IPv4 RFC 4291.
Anycast source address (Dirección de fuente de difusión por proximidad)		Descarte los paquetes IPv6 con una dirección de origen de difusión.
Needless fragment header (Encabezado de fragmento innecesario)		Descarte los paquetes IPv6 con la etiqueta del último fragmento (M=0) y un desplazamiento de cero.
MTU en paquete ICMP demasiado grande inferior a 1280 bytes		Descarte los paquetes IPv6 que contienen un mensaje Paquete de error de ICMPv6 demasiado grande MTU inferior a 1.280.
Extensión de salto a salto		Descarte los paquetes IPv6 que contienen el encabezado de extensión de salto por salto.
Extensión de routing		Descarte los paquetes IPv6 que contienen el encabezado de extensión de enrutamiento, que dirige los paquetes a uno o más nodos intermedios a su destino.
Destination extension (Extensión de destino)		Descarte los paquetes IPv6 que contienen la extensión de opciones de destino, que contiene opciones buscadas solo para el destino del paquete.
Invalid IPv6 options in extension header (Opciones de IPv6 no válidas en encabezado de extensión)		Descarte los paquetes IPv6 que contienen opciones IPv6 no válidas en el encabezado de extensión.

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
Campo reservado distinto de cero		Descarte paquetes IPv6 que tienen un encabezado con un campo reservado no definido a cero.

Colocación de ICMPv6

Para indicarle al cortafuegos qué hacer con determinados paquetes ICMPv6 que recibe en la zona, active estas opciones:

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
Destino ICMPv6 no alcanzable: requiere regla de seguridad explícita	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** > **Packet Based Attack Protection (Protección de ataque basada en paquetes)** > **ICMPv6 Drop (Descarte de ICMPv6)**	Requiere una búsqueda de política de seguridad explícita para mensajes de destinos ICMPv6 no alcanzables incluso cuando el mensaje está asociado a una sesión existente.
Paquete ICMPv6 demasiado grande: requiere coincidencia de regla de seguridad explícita		Requiere una búsqueda de política de seguridad explícita para mensajes de ICMPv6 de paquete demasiado grande, incluso cuando el mensaje está asociado a una sesión existente.
Tiempo superado de ICMPv6: requiere coincidencia explícita de regla de seguridad		Requiere una búsqueda de política de seguridad explícita para mensajes de ICMPv6 de tiempo superado incluso cuando el mensaje está asociado a una sesión existente.
Problema de parámetro de ICMPv6:		Requiere una búsqueda de política de seguridad explícita para mensajes de ICMPv6 de problema de parámetro incluso cuando el mensaje está asociado a una sesión existente.

© 2020 Palo Alto Networks, Inc.

Configuración de Zone Protection Profile: Packet Based Attack Protection	Configurado en	Description (Descripción)
requiere coincidencia explícita de regla de seguridad		
Redirección de ICMPv6: requiere coincidencia explícita de regla de seguridad		Requiere una búsqueda de política de seguridad explícita para mensajes de ICMPv6 de redirección de mensaje incluso cuando el mensaje está asociado a una sesión existente.

Protección de protocolo

- Network > Network Profiles > Zone Protection > Protocol Protection

El cortafuegos normalmente permite protocolos no IP entre las zonas de la capa 2 y entre las zonas de cable virtual. La protección de protocolo le permite controlar qué protocolos no IP se permiten (incluir) o se deniegan (excluir) entre las zonas de seguridad en una VLAN de capa 2 o un cable virtual o dentro de estas zonas. Ejemplos de protocolos no IP incluyen los sistemas AppleTalk, Banyan VINES, Novell, NetBEUI y SCADA (Supervisory Control And Data Acquisition), como GOOSE (Generic Object Oriented Substation Event).

Tras configurar la protección de protocolo en un perfil de protección de zona, aplique el perfil a una zona de seguridad de entrada en una VLAN de capa 2 o un cable virtual.

Habilite la protección de protocolo en las zonas accesibles desde Internet, para evitar que el tráfico de capa 2 de protocolos que no utiliza entre en la red.

Configuración del perfil de protección de zonas: Protección del protocolo	Configurado en	Description (Descripción)
Tipo de regla	**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Zona de protección)** >	Especifique el tipo de lista que está creando para la protección del protocolo: • **Include List (Lista de permitidos)**: solo se permiten los protocolos de la lista, además de las tramas etiquetadas IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) y VLAN (0x8100). Todos los demás protocolos se deniegan implícitamente (bloqueados). • **Exclude List (Lista de excluidos)**: solo se deniegan los protocolos en la lista; todos los demás protocolos se permiten

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de protección de zonas: Protección del protocolo	Configurado en	Description (Descripción)
	Protocol Protection (Protección del protocolo)	implícitamente. No puede excluir las tramas etiquetadas IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) o VLAN (0x8100). *Utilice la lista de inclusión para permitir únicamente los protocolos de capa 2 que utiliza y rechazar todos los demás protocolos. Esto reduce la superficie de ataque al denegar los protocolos que no utiliza en la red. La lista de exclusión es una lista negra que admite todos los protocolos que no incluye en la lista y si no configura la protección de protocolo, todos los protocolos de capa 2 estarán permitidos.*
Nombre de protocolo		Introduzca el nombre del protocolo que corresponde al código Ethertype que está añadiendo a la lista. El cortafuegos no verifica que el nombre del protocolo coincida con el código Ethertype, pero el código Ethertype determina el filtro del protocolo.
Habilitación		**Habilita** el código Ethertype en la lista. Si desea desactivar un protocolo para hacer pruebas sin eliminarlo, deshabilítelo.
Tipo de Ethernet (hex)		Introduzca un código Ethertype (protocolo) precedido por 0x para indicar hexadecimal (el intervalo es de 0x0000 a 0xFFFF). La lista puede tener un máximo de 64 Ethertypes. Algunas fuentes de códigos Ethertype son: • IEEE hexadecimal Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

Red > Perfiles de red > QoS

Haga clic en **Add (Añadir)** para añadir un perfil de QoS con el que definir los límites del ancho de banda y la prioridad de hasta ocho clases de servicio. Puede establecer límites de ancho de banda garantizados y máximos para clases individuales y para las clases colectivas. Las prioridades determinan cómo se trata el tráfico en presencia de conflictos.

Para habilitar completamente el cortafuegos y proporcionar QoS, también:

- Defina el tráfico para el que desea recibir tratamiento de QoS (seleccione Policies [Políticas] > QoS para agregar o modificar una política de QoS).
- Active QoS en una interfaz (seleccione Network > QoS).

Consulte Calidad de servicio para obtener los flujos de trabajo completos, los conceptos y los casos de uso de QoS.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de QoS	
Nombre de perfil	Introduzca un nombre para identificar el perfil (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Máximo de salida	Introduzca el valor máximo de rendimiento (en Mbps) para el tráfico que abandona el cortafuegos a través de esta interfaz. El valor predeterminado es 0, lo que especifica el límite del cortafuegos (60 000 Mbps en PAN-OS 7.1.16 y versiones posteriores; 16 000 en PAN-OS 7.1.15 y versiones posteriores). El valor de **Egress Max (Máximo de salida)** de un perfil de QoS debe ser menor o igual que el valor **Egress Max (Máximo de salida)** definido para la interfaz física habilitada con QoS. Consulte Network > QoS. *Aunque no es un campo obligatorio, se recomienda definir siempre el valor Egress Max (Máximo de salida) para un perfil de QoS.*
Salida garantizada	Introduzca el ancho de banda garantizado para este perfil (Mbps). Cuando se supera el ancho de banda garantizado de salida, el cortafuegos conmuta el tráfico en base a best-effort.

Clases	Haga clic en **Add (Añadir)** y especifique cómo se tratarán las clases de QoS individuales. Puede seleccionar una o más clases para configurar:
	
	• **Class (Clase)**: si no configura una clase, puede incluirla en una política de QoS. En este caso, el tráfico está sujeto a los límites generales de QoS. El tráfico que no coincide con una política de QoS se asignará a clase 4.
	• **Priority (Prioridad)**: haga clic y seleccione una prioridad para asignarla a una clase:
	  • **tiempo real**
	  • **high (alta)**
	  • **Intermedia**
	  • **low (baja)**
	
	Cuando se producen conflictos, se descarta el tráfico con la menor prioridad asignada. La prioridad en tiempo real utiliza su propia cola separada.
	
	• **Egress Max (Máximo de salida)**: haga clic e introduzca el valor máximo de rendimiento (en Mbps) para esta clase. El valor predeterminado es 0, lo que especifica el límite del cortafuegos (60 000 Mbps en PAN-OS 7.1.16 y versiones posteriores; 16 000 en PAN-OS 7.1.15 y versiones posteriores). El valor **Egress Max (Máximo de salida)** para una clase de QoS debe ser menor o igual que el valor **Egress Max (Máximo de salida)** definido para el perfil de QoS.
	
	Aunque no es un valor obligatorio, se recomienda definir siempre el valor de Egress Max (Máximo de salida) de un perfil de QoS.
	
	• **Egress Guaranteed (Salida garantizada)**: haga clic e introduzca el ancho de banda garantizado (Mbps) para esta clase. El ancho de banda garantizado asignado a una clase no está reservado para esa clase; el

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de QoS	
	ancho de banda que no se utiliza continúa permaneciendo disponible para todo el tráfico. Sin embargo, cuando se supera el ancho de banda garantizado de salida del tráfico, el cortafuegos permite el paso de ese tráfico en función de la mejor opción.

Network > Network Profiles > LLDP Profile

Un perfil de Protocolo de detección de nivel de enlace (LLDP) es la forma que le permite configurar el modo LLDP en el cortafuegos, habilitar las notificaciones de syslog y SNMP y configurar el Tipo-Longitud-Valores (TLV) opcional que desea se transmitan a los peer LLDP. Tras configurar el perfil LLDP, asigna el perfil a una o más interfaces.

Obtenga más información acerca de LLDP, incluyendo cómo configurar y supervisar LLDP.

Configuración de perfil de LLDP	Description (Descripción)
Nombre	Especifique un nombre para el perfil LLDP.
Modo	Seleccione el modo en el que funcionará LLDP: **transmit-receive (transmisión-recepción)**, **transmit-only (transmisión-solo)** o **receive-only (recepción-solo)**.
Notificación Syslog SNMP	Permite las notificaciones de syslog y trap SNMP, que ocurrirán en el **Notification Interva (Intervalo de notificaciones)** global. Si se habilita esta opción, el cortafuegos enviará tanto un evento de syslog como un trap SNMP según se haya configurado en **Device (Dispositivo)** > **Log Settings (Ajustes de log)** > **System (Sistema)** > **SNMP Trap Profile (Perfil de Trap SNMP)** y **Syslog Profile (Perfil syslog)**.
Descripción de puerto	Permite que el objeto ifAlias del cortafuegos se envíe en el TLV Descripción de puerto.
Nombre del sistema	Permite que el objeto sysName del cortafuegos se envíe en el TLV Nombre de sistema.
Descripción del sistema	Permite que el objeto sysDescr del cortafuegos se envíe en el TLV Descripción del sistema.
Capacidades del sistema	Habilita el modo de implementación (L3, L2 o cable virtual) de la interfaz que se enviará, a través de la siguiente asignación en el TLV Capacidades del sistema. • Si L3, el cortafuegos anuncia la funcionalidad de enrutador (bit 6) u el bit Otro (bit 1). • Si L2, el cortafuegos anuncia la funcionalidad de puente MAC (bit 3) u el bit Otro (bit 1). • Si el cable virtual, el cortafuegos anuncia la funcionalidad del Repetidor (bit 2) y el bit Otro (bit 1). SNMP MIB combina las funcionalidades configuradas en las interfaces en una única entrada.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de LLDP	Description (Descripción)
Dirección de gestión	Permite que **Management Address (Dirección de gestión)** se envíe en el TLV Dirección de gestión. Puede introducir hasta cuatro direcciones de gestión, que se envían en el orden especificado. Para cambiar el orden, haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**.
Nombre	Especifique un nombre para Dirección de gestión.
Interface (Interfaz)	Seleccione una interfaz cuya dirección IP será la Dirección de gestión. Si selecciona **None (Ninguna)**, puede introducir una dirección IP en el siguiente campo a la selección de IPv4 o IPv6.
Elección de IP	Seleccione **IPv4** o **IPv6** y, en el campo adyacente, seleccione o introduzca que la dirección IP se transmita como 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 a medida que se transmite la dirección de gestión.

Network > Network Profiles > BFD Profile

La detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) habilita la detección sumamente rápida de una falla de enlace, lo cual acelera la conmutación por error en una ruta diferente.

¿Qué está buscando?	Consulte:
¿Qué es BFD?	Descripción general de BFD
¿Qué campos están disponibles para crear un perfil BFD?	Componentes de un perfil BFD
Visualización de estado de BFD de un enrutador virtual.	Visualización de resumen y detalles de BFD
¿Busca más información?	Obtenga más información y configure BFD. Configuración de BFD para: Rutas estáticas BGP OSPF OSPFv3 RIP

Descripción general de BFD

BFD es un protocolo que reconoce una falla en la ruta bidireccional entre dos motores de reenvío, como interfaces, enlaces de datos o motores reales de reenvío. En la implementación de PAN-OS, uno de los

© 2020 Palo Alto Networks, Inc.

motores de reenvío es una interfaz en el cortafuegos y el otro es un peer BFD adyacente configurado. La detección de la falla de BFD entre dos motores es extremadamente rápida, lo que brinda una conmutación por error más rápida que la alcanzada por la supervisión de enlaces o las comprobación de enrutamiento dinámico frecuentes, como los paquetes de bienvenida o heartbeats.

Luego de que BFD detecta una falla, notifica al protocolo de enrutamiento para cambiarse a una ruta alternativa al peer. Si BFD está configurado para una ruta estática, el cortafuegos quita las rutas afectadas de las tablas RUB y FIB.

BFD se admite en los siguientes tipos de interfaces: Ethernet física, AE, VLAN, túnel (VPN de sitio a sitio y LSVPN) y subinterfaces de interfaces capa 3. Para cada ruta estática o protocolo de enrutamiento dinámico, puede habilitar o deshabilitar BFD, seleccionar el perfil BFD predeterminado o configurar un perfil BFD.

Componentes de un perfil BFD

- Network > Network Profiles > BFD Profile

Puede habilitar BFD para una ruta estática o protocolo de enrutamiento dinámico aplicando el perfil BFD predeterminado o un perfil BFD que crea. El perfil predeterminado usa la configuración BFD predeterminada y no puede modificarse. Haga clic en **Add (añadir)** para añadir un perfil BFD nuevo y especificar la siguiente información.

Configuración de perfil de BFD	Description (Descripción)
Nombre	Nombre del perfil de BFD (hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas y debe ser único en el cortafuegos. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Modo	Modo en el cual BFD opera: • **Active (Activo)**: BFD inicia el envío de los protocolos de control (predeterminado). Al menos uno de los peers de BFD debe estar activo; ambos pueden estar activos. • **Passive (Pasivo)**: BFD espera que el peer envíe los paquetes de control y responde según corresponda.
Intervalo Tx mínimo deseado (ms)	Intervalo mínimo (en milisegundos) en el cual desea que el protocolo BFD envíe paquetes de control BFD. El valor mínimo de PA-7000 Series es 50; el valor mínimo de PA-3200 Series es 100; el valor mínimo de VM-Series es 200 (el valor máximo es 2000; el valor predeterminado es 1000). *Si utiliza múltiples protocolos que usan diferentes perfiles BFD en la misma interfaz, configure los perfiles BFD con el mismo valor en Desired Minimum Tx Interval (Intervalo Tx mínimo deseado).*
Intervalo Tx mínimo requerido (ms)	Intervalo mínimo (en milisegundos) en el cual BFD puede recibir paquetes de control BFD. El valor mínimo de PA-7000 Series es 50; el valor mínimo de PA-3200 Series es 100; el valor mínimo de VM-Series es 200 (el valor máximo es 2000; el valor predeterminado es 1000).
Multiplicador de tiempo de detección	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

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de BFD	Description (Descripción)
	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 ha producido una falla (el intervalo es de 2 a 50; el valor predeterminado es 3).
Tiempo de espera (ms)	Demora (en milisegundos) luego de que un enlace se activa antes de que el cortafuegos transmita los paquetes de control de BFD. **Hold Time (Tiempo de espera)** se aplica al modo activo de BFD únicamente. Si el cortafuegos recibe paquetes de control BFD durante el **Hold Time (Tiempo de espera)**, los ignora (el intervalo es 0-120000; el predeterminado es 0). La configuración predeterminada de 0 significa que no se utiliza el **Hold Time (Tiempo de espera)** de transmisión; el cortafuegos envía y recibe paquetes de control BFD de inmediato después de que establece el enlace.
Habilitar Multihop	Permite a BFD en múltiples saltos. Se aplica únicamente a la implementación BGP.
TTL Rx mínimo	Valor de período de vida mínimo (número de saltos) que BFD aceptará (recibirá) cuando admite BFD en múltiples saltos. Se aplica a la implementación BGP únicamente (el intervalo es 1-254; no existen valores predeterminados).

Visualización de resumen y detalles de BFD

- Network > Virtual Routers

La siguiente tabla describe la información de resumen de BFD.

Visualización de información de BFD	
Visualice un resumen de BFD.	Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual en el que está interesado, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**. Seleccione la pestaña **BFD Summary Information**.
Visualice los detalles de BFD.	Seleccione **details (detalles)** en la fila de la interfaz en la que está interesado para ver los detalles de BFD.

Network (Red) > Network Profiles (Perfiles de red) > SD-WAN Interface Profile (Perfil de interfaz de SD-WAN)

Cree un perfil de interfaz de SD-WAN para agrupar enlaces físicos por etiqueta de enlace y controlar la velocidad de los enlaces y la frecuencia con la que el cortafuegos supervisa esos enlaces.

	Perfil de interfaz SD-WAN
Nombre	Introduzca el **nombre** del perfil de interfaz de SD-WAN con un máximo de 31 caracteres alfanuméricos. El nombre debe comenzar por un carácter alfanumérico

© 2020 Palo Alto Networks, Inc.

	Perfil de interfaz SD-WAN
	y puede contener letras, números, guiones bajos (_), guiones (-), puntos (.) y espacios.
Etiqueta de enlace	Seleccione la **etiqueta de enlace** que este perfil asignará a la interfaz o **añada** una nueva etiqueta. Una etiqueta de enlace agrupa enlaces físicos (diferentes ISP) para que el cortafuegos seleccione durante la selección de ruta y la conmutación por error.
Description (Descripción)	Especifique una descripción fácil de usar del perfil.
Tipo de enlace	Seleccione el tipo de enlace físico de la lista predefinida (**ADSL/DSL**, **Cable Modem** , **Ethernet**, **Fibra**, **LTE/3G/4G/5G**, **MPLS**, **Microondas/radio**, **Satélite**, **WiFi** u **Otros**). El cortafuegos puede admitir cualquier dispositivo CPE que termine y se transfiera como una conexión Ethernet al cortafuegos. Por ejemplo, los puntos de acceso Wi-Fi, los módems de evolución a largo plazo (LTE) y los equipos de las instalaciones del cliente (CPE) de microondas láser pueden terminar con una transferencia de Ethernet.
Compatibilidad de túnel de datos de VPN	(PAN-OS 9.1.2 y versiones 9.1 posteriores) Determina si el tráfico de la sucursal a la central y el tráfico de retorno fluyen a través de un túnel VPN para mayor seguridad (habilitado de forma predeterminada) o fluye fuera del túnel VPN para evitar la sobrecarga de cifrado. • Deje la opción **Compatibilidad del túnel de datos VPN** habilitada para los tipos de enlaces públicos que tienen conexiones directas a Internet o capacidad de conexión a Internet, como módem de cable, ADSL y otras conexiones a Internet. • Puede deshabilitar **Compatibilidad del túnel de datos VPN** para tipos de enlaces privados como MPLS, satélite o microondas que no tienen capacidad de conexión a Internet. Sin embargo, primero debe asegurarse de que el tráfico no pueda interceptarse, porque se enviará fuera del túnel VPN. • La sucursal puede tener tráfico de DIA que precise la conmutación por error en el enlace MPLS privado que se conecta a la central y que tenga que llegar a Internet desde la central. La configuración **Compatibilidad del túnel de datos VPN** determina si los datos privados fluyen a través del túnel VPN o si fluyen fuera del túnel, y el tráfico fallido usa la otra conexión (que el flujo de datos privados no usa). El cortafuegos usa zonas para segmentar el tráfico de conmutación por error de DIA del tráfico privado de MPLS.
Descarga máxima (Mbps)	Especifique la velocidad de descarga máxima del ISP en megabits por segundo (el intervalo es de 1 a 100 000; no hay ningún valor predeterminado). Solicítele a su ISP la velocidad del enlace o pruebe las velocidades máximas del enlace con una herramienta como speedtest.net y haga una media de los tiempos máximos durante un buen periodo.
Subida máxima (Mbps)	Especifique la velocidad de carga máxima del ISP en Mbps (el intervalo es de 1 a 100 000; no hay ningún valor predeterminado). Solicítele a su ISP la velocidad del enlace o pruebe las velocidades máximas del enlace con una herramienta como speedtest.net y haga una media de los tiempos máximos durante un buen periodo.

© 2020 Palo Alto Networks, Inc.

	Perfil de interfaz SD-WAN
Monitorización de rutas	Seleccione el modo Supervisión de rutas en el que el cortafuegos supervisa las interfaces donde aplica ese perfil de interfaz de SD-WAN. • **Agresivo**: (valor predeterminado para todos los tipos de enlace excepto LTE y satélite) el cortafuegos envía paquetes de sonda al extremo opuesto del enlace de SD-WAN a una frecuencia constante. *Utilice el modo Agresivo si necesita una detección rápida y una conmutación por error para condiciones de caída de tensión y apagón.* • **Relajado**: (valor predeterminado para los tipos de enlace LTE y satélite) el cortafuegos espera varios segundos (el **tiempo de inactividad de la sonda**) entre los conjuntos de envío de los paquetes de sonda, lo que hace que la supervisión de la ruta sea menos frecuente. Cuando se agota el tiempo de inactividad de la sonda, el cortafuegos envía sondas durante siete segundos a la **frecuencia de la sonda** configurada. *Utilice el modo Relajado cuando tenga enlaces de ancho de banda bajo, enlaces de pago por uso (como LTE) o cuando la detección rápida no sea tan importante como conservar el coste y el ancho de banda.*
Frecuencia de la sonda (por segundo)	Especifique la frecuencia de sonda, que es la cantidad de veces por segundo que el cortafuegos envía un paquete de sonda al extremo opuesto del enlace de SD-WAN (el intervalo es de 1 a 5; el valor predeterminado es 5).
Tiempo de inactividad de la sonda (segundos)	Si selecciona la supervisión de ruta **Relajada**, puede establecer el tiempo de inactividad de la sonda (en segundos) que el cortafuegos espera entre conjuntos de paquetes de sonda (el intervalo es de 1 a 60; el valor predeterminado es 60).
Tiempo de retención de conmutación por recuperación (segundos)	Introduzca el tiempo (en segundos) que el cortafuegos espera a que un enlace recuperado siga siendo apto antes de que el cortafuegos restablezca ese enlace como el enlace preferido después de que se haya realizado la conmutación por error (el intervalo es de 20 a 120; el valor predeterminado es 120). El tiempo de retención de conmutación por recuperación evita que un enlace recuperado se restablezca como enlace preferido demasiado rápido y que vuelva a fallar de inmediato.

Dispositivo

Utilice las siguientes secciones para obtener referencia de campo sobre la configuración de sistema básica y tareas de mantenimiento en el cortafuegos:

> Dispositivo > Configuración
> Device > High Availability
> Device (Dispositivo) > Log Forwarding Card (Tarjeta de reenvío de logs)
> Device > Config Audit
> Dispositivo > Perfiles de la contraseña
> Device > Administrators
> Device > Admin Roles
> Device > Access Domain
> Device > Authentication Profile
> Device > Authentication Sequence
> Identificación de usuarios
> Device > VM Information Sources
> Device (Dispositivo) > Troubleshooting (Solución de problemas)
> Device > Virtual Systems
> Device > Shared Gateways
> Dispositivo > Gestión de certificados
> Dispositivo > Páginas de respuesta
> Device > Log Settings
> Dispositivo > Perfiles de servidor > Netflow
> Device > Local User Database > Users
> Dispositivo > Base de datos de usuario local > Grupos de usuarios
> Dispositivo > Programación de la exportación de logs
> Device > Software
> Dispositivo > Cliente de GlobalProtect
> Device > Dynamic Updates
> Device > Licenses
> Device > Support
> Device > Master Key and Diagnostics

© 2020 Palo Alto Networks, Inc.

Dispositivo > Configuración

- Device (Dispositivo) > Setup (Configuración) > Management (Gestión)
- Device > Setup > Operations
- Device > Setup > HSM
- Device > Setup > Services
- Dispositivo > Configuración > Interfaces
- Dispositivo > Configuración > Telemetría
- Device > Setup > Content-ID
- Device > Setup > WildFire
- Device > Setup > Session

© 2020 Palo Alto Networks, Inc.

Device (Dispositivo) > Setup (Configuración) > Management (Gestión)

- **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**
- **Panorama** > **Setup (Configuración)** > **Management (Gestión)**

En un cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** para configurar los parámetros de gestión.

En Panorama™, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** para configurar los cortafuegos que desea gestionar con plantillas de Panorama. Seleccione **Panorama** > **Setup (Configuración)** > **Management (Gestión)** para configurar los ajustes de gestión de Panorama.

La siguiente configuración de gestión se aplica tanto al cortafuegos como a Panorama, excepto donde se indique lo contrario.

- Configuración general
- Configuración de autenticación
- Configuración de base de reglas de políticas
- Ajustes de Panorama: Device (Dispositivo) > Setup (Configuración) > Management (Gestión) (ajustes configurados en el cortafuegos para la conexión a Panorama)
- Ajustes de Panorama: Panorama > Setup > Management (Panorama > Configuración > Gestión) (ajustes establecidos en Panorama para su conexión a los cortafuegos)
- Configuración de log e informes
- Banners y mensajes
- Complejidad de contraseña mínima
- AutoFocus™
- Servicio de creación de logs

Elemento	Description (Descripción)
Configuración general	
Nombre de host	Introduzca un nombre de host (hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos. Si no introduce un valor, PAN-OS® utiliza el modelo de cortafuegos (por ejemplo, PA-5220_2) como predeterminado. De manera opcional, puede configurar el cortafuegos para usar un nombre de host que un servidor DHCP proporcione. Consulte Aceptar nombre de host proporcionado por servidor DHCP (solo cortafuegos) *Configure un nombre de host único para identificar fácilmente el dispositivo que está gestionando.*
Dominio	Especifique el nombre de dominio de la red para el cortafuegos (hasta 31 caracteres).

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	De manera opcional, puede configurar el cortafuegos y Panorama para usar un dominio que proporciona un servidor DHCP. Consulte Aceptar dominio proporcionado por servidor DHCP (solo cortafuegos)
Aceptar nombre de host proporcionado por servidor DHCP (solo cortafuegos)	(Se aplica solo cuando el tipo de IP de interfaz de gestión es cliente DHCP.) Seleccione esta opción para que la interfaz de gestión acepte el nombre de host que recibe del servidor DHCP. El nombre de host del servidor (si es válido) sobrescribe cualquier valor especificado en el campo Hostname.
Aceptar dominio proporcionado por servidor DHCP (solo cortafuegos)	(Se aplica solo cuando el tipo de IP de interfaz de gestión es cliente DHCP.) Seleccione esta opción para que la interfaz de gestión acepte el dominio (sufijo DNS) que recibe del servidor DHCP. El dominio del servidor sobrescribe cualquier valor especificado en el campo **Domain (Dominio)**.
Banner de inicio de sesión	Introduzca texto (hasta 3200 caracteres) para mostrar en la página de inicio de sesión de la interfaz web debajo de los campos **Name (Nombre)** y **Password (Contraseña)**.
Forzar administradores a confirmar el banner de inicio de sesión	Seleccione esta opción para mostrar y forzar a los administrador a seleccionar la opción **I Accept and Acknowledge the Statement Below (Acepto y reconozco la declaración que figura a continuación)** sobre el banner de inicio de sesión en la página de inicio; la cual obliga a los administradores a confirmar que comprenden y aceptan el contenido del mensaje antes de que puedan iniciar sesión en **Login (Inicio de sesión)**.
Perfil de servicio SSL/TLS	Asigne un perfil de servicio SSL / TLS existente o cree uno nuevo para especificar un certificado y los parámetros de protocolo SSL / TLS permitidos en la interfaz de gestión (consulte Device > Certificate Management > SSL/TLS Service Profile). El cortafuegos o Panorama utilizan este certificado para autenticar a los administradores que acceden a la interfaz web a través de la interfaz de gestión (MGT) o a través de cualquier otra interfaz que admita el tráfico de administración HTTP / HTTPS (consulte Network > Network Profiles > Interface Mgmt). Si selecciona **none (ninguno)** (predeterminado), el cortafuegos o Panorama usan el certificado autofirmado predefinido. *El certificado predefinido se proporciona para mayor comodidad. Para una mejor seguridad, asigne un perfil de servicio SSL / TLS. Para garantizar la confianza, el certificado debe estar firmado por un autoridad de certificación (CA) que esté en el almacén de certificados raíz de confianza de los sistemas cliente.*
Zona horaria	Seleccione la zona horaria del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
Configuración regional	Seleccione un idioma para los informes en PDF de la lista desplegable. Consulte Monitor > PDF Reports > Manage PDF Summary. Aunque haya establecido una preferencia de idioma específica para la interfaz web, los informes en PDF seguirán utilizando el idioma especificado en **Locale (Local)**.
Fecha	Establezca la fecha en el cortafuegos; introduzca la fecha actual (con el formato AAAA/MM/DD), o bien seleccione la fecha de la lista desplegable. *También puede definir un servidor NTP (Dispositivo > Configuración > Servicios).*
Time	Configure la hora en el cortafuegos; especifique la hora actual (en formato de 24 horas) o seleccione la hora en el menú desplegable. *También puede definir un servidor NTP (Device [Dispositivo] > Setup [Configuración] > Services [Servicios]).*
Número de serie (Solo dispositivo virtual de Panorama)	Introduzca el número de serie de Panorama. Busque el número de serie en el correo electrónico de ejecución de pedido que Palo Alto Networks® le envió.
Latitud	Introduzca la latitud (-90.0 a 90.0) del cortafuegos.
Longitud	Introduzca la latitud (--180.0 a 180.0) del cortafuegos.
Adquirir bloqueo de confirmación automáticamente	Seleccione esta opción para aplicar automáticamente un bloqueo de confirmación cuando cambie la configuración candidata. Para más información, consulte Bloquear configuraciones. *Habilite Automatically Acquire Commit Lock (Adquirir bloqueo de confirmación automáticamente) para que otros administradores no puedan realizar cambios en la configuración hasta que el primer administrador confirme sus cambios.*
Comprobación del vencimiento del certificado	Indique al cortafuegos que deberá crear mensajes de advertencia cuando se acerque la fecha de vencimiento de los certificados integrados. *Habilite Certificate Expiration Check (Comprobación del vencimiento del certificado)para generar un mensaje de*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	advertencia cuando se acerque la fecha de vencimiento de los certificados integrados.
Multiple Virtual System Capability	Habilita el uso de varios sistemas virtuales en cortafuegos que admiten esta función (consulte Device > Virtual Systems). *Para habilitar múltiples sistemas virtuales en un cortafuegos, las políticas de cortafuegos deben hacer referencia a no más de 640 grupos de usuarios distintos. Si es necesario, reduzca el número de grupos de usuario con referencia. Luego, después de habilitar y añadir múltiples sistemas virtuales, las políticas pueden hacer referencia a otros 640 grupos de usuario para cada sistema virtual adicional.*
Base de datos de filtrado de URL (Solo en Panorama)	Seleccione un proveedor de filtrado de URL en Panorama: **brightcloud** or **paloaltonetworks** (PAN-DB).
Usar hipervisor asignado a direcciones MAC (Solo en cortafuegos VM-Series)	Seleccione esta opción para que el cortafuegos VM-Series use las direcciones MAC asignadas por el hipervisor, en lugar de generar una dirección MAC usando el esquema personalizado de PAN-OS. Si habilita esta opción y usa una dirección IPv6 para la interfaz, el ID de la interfaz no puede usar el formato EUI-64, que procede de la dirección IPv6 de la dirección MAC de la interfaz. En una configuración activa/pasiva de alta disponibilidad (HA), se produce un error de compilación si se usa el formato EUI-64.
Seguridad de GTP	Seleccione esta opción para habilitar la capacidad de inspeccionar el plano de control y los mensajes de plano de datos de usuario en el tráfico del protocolo de túnel GPRS (GTP). Consulte Objects > Security Profiles > GTP Protection (Objetos > Perfiles de seguridad > Protección de GTP) para configurar un perfil de protección de GTP de modo que pueda aplicar la política al tráfico de GTP.
SCTP Security (Seguridad de SCTP)	Seleccione esta opción para habilitar la capacidad de inspeccionar, y filtrar los paquetes y fragmentos del protocolo de transmisión de control de secuencias (SCTP), y para aplicar la protección contra inundaciones de inicialización (INIT) del SCTP. Consulte Objects > Security Profiles > GTP Protection (Objetos > Perfiles de seguridad > Protección de GTP). Para obtener información sobre la protección contra inundaciones de inicialización (INIT) del SCTP, consulte Configuración de protección contra inundaciones de inicialización (INIT) del SCTP.
Certificado de Dispositivo (solo PAN-OS 9.1.3 y versiones posteriores)	
Obtener certificado	Haga clic para introducir la contraseña de un solo uso (OTP) generada desde el portal de atención al cliente de Palo Alto Networks. El certificado del dispositivo es necesario para

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	autenticar correctamente Panorama con el CSP y aprovechar Zero Touch Provisioning (ZTP). Después de instalar correctamente el certificado del dispositivo, aparece lo siguiente: • **Estado actual del certificado del dispositivo**: el estado actual del certificado del dispositivo (`Válido`, `No válido` o `Caducado`) • **No válido antes de**: marca de tiempo que indica cuándo comienza la validez del certificado del dispositivo. • **No válido después de**: marca de tiempo que indica cuándo caduca la validez del certificado del dispositivo y el certificado del dispositivo pasa a ser `No válido` o `Caducado`. • **Último mensaje recuperado**: mensaje que muestra si el certificado del dispositivo se ha instalado correctamente o si la instalación del certificado del dispositivo ha fallado. • **Último estado recuperado**: el estado en el que se obtuvo el certificado del dispositivo (`Correcto)` o `Erróneo`). • **Última marca de tiempo recuperada**: marca de tiempo del último intento de instalación del certificado de dispositivo.
Configuración de autenticación	
Perfil de autenticación	Seleccione el perfil de autenticación (o secuencia) que el cortafuegos utiliza para autenticar cuentas administrativas que define en un servidor externo en lugar de localmente en el cortafuegos (consulte Device > Authentication Profile). Cuando los administradores externos inician sesión, el cortafuegos les solicita la información de autenticación (como por ejemplo la función administrativa) desde el servidor externo. La habilitación de la autenticación para administradores externos requiere pasos adicionales basados en el tipo de servidor especificado por el perfil de autenticación, que debe ser uno de los siguientes: • RADIUS • TACACS+ • SAML *Los administradores pueden utilizar SAML para autenticarse en la interfaz web, pero no en la CLI.* Seleccione **None (Ninguna)** para deshabilitar la autenticación para administradores externos. Para las cuentas administrativas que se definen localmente (en el cortafuegos), el cortafuegos autentica mediante el perfil de autenticación asignado a esas cuentas (consulte Device > Administrators).
Perfil del certificado	Seleccione un perfil de certificado para verificar los certificados de cliente de los administradores que están configurados para el acceso basado en certificados a la interfaz web del cortafuegos. Para obtener instrucciones sobre cómo configurar perfiles

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	de certificado, consulte Device > Certificate Management > Certificate Profile. *Configure un perfil de certificado para garantizar que el equipo host del administrador tenga los certificados adecuados para autenticarse con el certificado de CA raíz definido en el perfil del certificado.*
Tiempo de espera de inactividad	Introduzca el tiempo máximo (en minutos) sin actividad en la interfaz web o CLI antes de que un administrador se cierre automáticamente (el intervalo es 0-1.440 y el predeterminado es 60). Un valor de 0 significa que la inactividad no activa un cierre de sesión automático. *La actualización manual y automática de páginas de interfaz web (como el Dashboard [Panel] y el cuadro de diálogo System Alarms [Alarmas del sistema]) restablecen el contador de Idle Timeout (Tiempo de inactividad). Para habilitar el cortafuegos para que imponga el tiempo de espera cuando está en una página que admita la actualización automática, establezca el intervalo de actualización como Manual o a un valor mayor que el Idle Timeout (Tiempo de inactividad). También puede desactivar Auto Refresh (Actualizar automáticamente) en la pestaña ACC.* *Configure el Idle Timeout (Tiempo de espera de inactividad) en 10 minutos para evitar que los usuarios accedan al cortafuegos si un administrador deja una sesión del cortafuegos abierta.*
Vigencia de clave de API	Introduzca el tiempo (en minutos) durante el cual la clave de API será válida (el intervalo es de 0 a 525 600; el valor predeterminado es 0). Un valor de 0 significa que la clave de API está siempre activa. Seleccione **Expire All API Keys (Caducar todas las claves de API)** para invalidar todas las claves de API generadas. Utilice esta opción con precaución, ya que todas las claves existentes dejarán de ser válidas y todas las operaciones en las que esté utilizando dichas claves de API dejarán de funcionar. *Realice esta operación durante un periodo de mantenimiento, de manera que pueda reemplazar las claves sin alterar las implementaciones actuales en las que se haga referencia a las claves de API.*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
Última fecha de caducidad de claves API	Muestra la marca de tiempo del último vencimiento de la clave de API. Este campo no muestra ningún valor si nunca restableció las claves.
Intentos fallidos	Introduzca el número de intentos de inicio de sesión fallidos (el intervalo es de 0 a 10) que el cortafuegos permite para la interfaz web y la CLI antes de bloquear la cuenta del administrador. Un valor 0 significa que el número de intentos es ilimitado. El valor predeterminado es 0 en los cortafuegos con modo de operación normal y 10 en los cortafuegos con modo FIPS-CC. Limitar los intentos de inicio de sesión puede ayudar a proteger el cortafuegos contra los ataques de fuerza bruta. *Si define Failed Attempts (Intentos fallidos) con un valor diferente de 0 pero deja Lockout Time (Tiempo de bloqueo) en 0, se ignora Failed Attempts (Intentos fallidos) y nunca se bloquea al usuario.* *Configure la cantidad de Failed Attempts (Intentos fallidos) en 5 o menos para permitir una cantidad razonable de reintentos en caso de errores de escritura, a la vez que se impide que sistemas malintencionados intenten métodos de fuerza bruta para iniciar sesión en el cortafuegos.*
Tiempo de bloqueo	Introduzca el número de minutos (el intervalo es 0-60) que el cortafuegos bloquea el acceso de un administrador a la interfaz web y a la CLI después de alcanzar el límite de **Failed Attempts (Intentos fallidos)**. Un valor de 0 (predeterminado) significa que el bloqueo se aplica hasta que otro administrador desbloquee manualmente la cuenta. *Si configura Failed Attempts (Intentos fallidos) en un valor distinto de 0, pero deja Lockout Time (Tiempo de bloqueo) en 0, el usuario será bloqueado después de la cantidad establecida de intentos fallidos de inicio de sesión, hasta que otro administrador desbloquee manualmente la cuenta.* *Configure el Lockout Time (Tiempo de bloqueo) en al menos 30 minutos para impedir los intentos continuados de inicio de sesión de un usuario malintencionado.*
Configuración de base de reglas de políticas	
Requiere etiqueta en las políticas	Requiere al menos una etiqueta al crear una nueva regla de política. Si una regla de política ya existe cuando usted habilita

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	esta opción, debe añadir al menos una etiqueta la próxima vez que edite la regla.
Requiere descripción de políticas	Exige que añada una **Description (Descripción)** al crear una nueva regla de política. Si una regla de política ya existe cuando usted habilita esta opción, debe añadir al menos una **descripción** la próxima vez que edite la regla.
Fail Commit if Policies Have No Tags or Descriptions (Fallo de compilación si las políticas no tienen etiquetas o descripción)	Fuerza el fallo de la compilación si no añade etiquetas o una descripción a la regla de política. Si una regla de política ya existe cuando usted habilita esta opción, la compilación fallará si no se añaden etiquetas o una descripción la próxima vez que edite la regla. Para forzar el fallo de la compilación, debe **Require tag on policies (Exigir etiqueta en las políticas)** o **Require description on policies (Exigir descripción en las políticas)**.
Require Audit Comment on Policies (Exigir el comentario de auditoría en las políticas)	Exige un **Audit Comment (Comentario de auditoría)** al crear una nueva regla de política. Si una regla de política ya existe cuando usted habilita esta opción, debe añadir un **comentario de auditoría** la próxima vez que edite la regla.
Auditar comentario de expresión regular	Especifique los requisitos para los parámetros del formato de comentario en los comentarios de auditoría.
Policy Rule Hit Count (Conteo de resultados de reglas de la política)	Registra la frecuencia de las coincidencias del tráfico con las reglas de la política que configuró en el cortafuegos. Cuando se habilita, es posible ver el conteo total de resultados de las coincidencias del tráfico total con cada regla, junto con la fecha y la hora en que la regla se creó y modificó, y la fecha y hora del primer y el último resultado.
Uso de la aplicación de política	

Ajustes de Panorama: Device (Dispositivo) > Setup (Configuración) > Management (Gestión)

Configure el siguiente ajuste en el cortafuegos o en una plantilla de Panorama. Estos ajustes establecen una conexión entre el cortafuegos y Panorama.

También debe configurar los ajustes de conexión y uso compartido del objeto en Panorama (Panorama Settings: (Configuración de Panorama) Panorama > Setup (Configuración)> Management (Gestión)).

El cortafuegos usa una conexión SSL con un cifrado AES256 para registrarse con Panorama. De manera predeterminada, Panorama y el cortafuegos se autentican entre sí utilizando certificados de 2048 bits y usan la conexión SSL para la gestión de configuración y la recopilación de logs. Para asegurar aún más las conexiones SSL entre Panorama, cortafuegos y recopiladores de logs, consulte Comunicación de cliente segura *Para configurar certificados personalizados entre el cortafuegos y Panorama o un recopilador de logs.*

Servidores de Panorama	Introduzca la dirección IP o FQDN del servidor de Panorama Si Panorama tiene una configuración de alta disponibilidad (HA),

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	introduzca la dirección IP o FQDN del servidor secundario de Panorama en el segundo campo **Panorama Servers (Servidores de Panorama)**.
Receive Timeout for Connection to Panorama (Tiempo de espera de recepción para conexión a Panorama)	Introduzca el tiempo de espera (en segundos) para recibir mensajes de TCP de Panorama (el intervalo es de 1 a 240 segundos; el valor predeterminado es 240).
Send Timeout for Connection to Panorama (Tiempo de espera de envío para conexión a Panorama)	Introduzca el tiempo de espera (en segundos) para enviar mensajes de TCP a Panorama (el intervalo es de 1 a 240; el valor predeterminado es 240).
Retry Count for SSL Send to Panorama (Reintentar recuento de envíos SSL a Panorama)	Introduzca el número de reintentos permitidos al enviar mensajes de capa de sockets seguros (SSL) a Panorama (intervalo: 1-64; predeterminado: 25).
Habilitación de la recuperación de confirmación automatizada	Habilite esta opción para permitir que el cortafuegos verifique automáticamente su conexión con el servidor de gestión Panorama cuando se confirme una configuración y se envíe al cortafuegos, y a intervalos configurados después de que se envíe una configuración correctamente. Cuando esta opción esté habilitada, y el cortafuegos no pueda verificar su conexión con el servidor de gestión Panorama, el cortafuegos y la gestión de Panorama revertirán automáticamente su configuración a la configuración en ejecución anterior para restaurar la conectividad.
Número de intentos de comprobar la conectividad de Panorama	Cuando **Recuperación de confirmación automática habilitada** esté habilitada, configure la cantidad de veces que el cortafuegos prueba su conexión con el servidor de gestión Panorama.
Intervalo entre reintentos (s)	Cuando **Habilitar recuperación de confirmación automática** esté habilitada, configure el tiempo en segundos entre el número de intentos que el cortafuegos prueba su conexión con el servidor de gestión Panorama.
Comunicación de cliente segura	Habilite **Secure Client Communication (Comunicación de cliente segura)** para garantizar que el cortafuegos utilice certificados personalizados configurados (en lugar del certificado predeterminado) para autenticar las conexiones SSL con los recopiladores de logs o Panorama. • **None (Ninguno)**: (predeterminado) no se ha configurado ningún certificado de dispositivo y se utiliza el certificado predefinido predeterminado. • **Local**: el cortafuegos utiliza un certificado de dispositivo local y la clave privada correspondiente generada en el cortafuegos o importada de un servidor PKI empresarial existente. • **Certificate (Certificado)**: seleccione el certificado de dispositivo local que generó o importó. Este certificado puede ser exclusivo del cortafuegos (basado en un hash del

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	número de serie del cortafuegos) o puede ser un certificado de dispositivo común utilizado por todos los cortafuegos que se conectan a Panorama. • **Perfil de certificado**: Seleccione el perfil de certificado del menú desplegable. Certificate Profile (Perfil de certificado) define el certificado de CA para que verifique los certificados de cliente y cómo verificar el estado de revocación del certificado. • **SCEP**: el cortafuegos utiliza un certificado de dispositivo y una clave privada generada por un servidor SCEP (Simple Certificate Enrollment Protocol). • **SCEP Profile (Perfil de SCEP)**: seleccione un SCEP Profile (Perfil de SCEP) del menú desplegable. El perfil de SCEP brinda a Panorama la información necesaria para autenticar los dispositivos del cliente en un servidor SCEP en la PKI de su empresa. • **Certificate Profile (Perfil de certificado)**: seleccione el Certificate Profile (Perfil de certificado) del menú desplegable. Certificate Profile (Perfil de certificado) define el certificado de CA para que verifique los certificados de cliente y cómo verificar el estado de revocación del certificado.
	• **Customize Communication (Personalizar comunicación)**: el cortafuegos utiliza el certificado personalizado configurado para autenticar los dispositivos seleccionados. • **Panorama Communication (Comunicación con Panorama)**: el cortafuegos utiliza el certificado de cliente configurado para la comunicación con Panorama. • **Panorama Communication (Comunicación con Panorama)**: el cortafuegos utiliza el certificado de cliente configurado para la comunicación con Panorama. • **Comunicación con WildFire**: el cortafuegos utiliza el certificado de cliente configurado para la comunicación con un dispositivo WildFire®. • **Log Collector Communication (Comunicación con recopiladores de logs)**: el cortafuegos utiliza el certificado de cliente configurado para la comunicación con un recopilador de logs. • **Comprobar identidad de servidor** (Únicamente para comunicación entre Panorama y recopiladores de logs): el cortafuegos confirma la identidad del servidor haciendo coincidir el nombre común (Common Name, CN) con la dirección IP o FQDN del servidor.
Deshabilitar/Habilitar objetos y política de Panorama	Esta opción solo aparece cuando edita **Panorama Settings (Ajustes de Panorama)** en un cortafuegos (no en una plantilla en Panorama). Si hace clic en **Disable Panorama Policy and Objects (Deshabilitar política y objetos de Panorama)**, se deshabilita la propagación de

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	las políticas de grupo de dispositivos y objetos al cortafuegos. De forma predeterminada, esta acción también elimina estas políticas y objetos del cortafuegos. Para conservar una copia local de las políticas y objetos del grupo de dispositivos del cortafuegos, en el cuadro de diálogo que se abre al hacer clic en esta opción, seleccione**Import Panorama Policy and Objects before disabling (Importar política y objetos de Panorama antes de deshabilitar)**. Después de confirmar, las políticas y objetos pasan a formar parte de la configuración del cortafuegos y Panorama deja de gestionarlos. En condiciones normales de funcionamiento, desactivar la gestión de Panorama es innecesario y podría complicar el mantenimiento y la configuración de los cortafuegos. Esta opción suele aplicarse a situaciones en las que los cortafuegos requieren valores de objetos y reglas diferentes a los definidos en el grupo de dispositivos. Un ejemplo de esto consiste en retirar un cortafuegos del entorno de trabajo e introducirlo en un entorno de laboratorio para realizar pruebas. Para invertir la política de cortafuegos y la gestión de objetos en Panorama, haga clic en **Enable Panorama Policy and Objects (Habilitar objetos y política de Panorama)**.
Deshabilitar/habilitar plantilla de dispositivo y red	Esta opción solo aparece cuando edita **Panorama Settings (Ajustes de Panorama)** en un cortafuegos (no en una plantilla en Panorama). Si hace clic en **Disable Device and Network Template (Deshabilitar plantilla de dispositivo y red).**, se deshabilita la propagación de información de plantillas (configuraciones de dispositivo y red) al cortafuegos. De forma predeterminada, esta acción también elimina la información de plantilla del cortafuegos. Para conservar una copia de la información de la plantilla en el cortafuegos, en el cuadro de diálogo que se abre al hacer clic en esta opción, seleccione **Import Device and Network Templates before disabling (Importar plantillas de dispositivos y red antes de deshabilitarlas)**. Después de realizar una compilación, la información de la plantilla pasa a formar parte de la configuración del cortafuegos y Panorama deja de gestionarla. *En condiciones normales de funcionamiento, desactivar la gestión de Panorama es innecesario y podría complicar el mantenimiento y la configuración de los cortafuegos. Esta opción suele aplicarse a situaciones en las que los cortafuegos requieren valores configuración de dispositivos y red diferentes a los definidos en el grupo de dispositivos. Un ejemplo de esto consiste en retirar un cortafuegos del entorno de trabajo e introducirlo en un entorno de laboratorio para realizar pruebas.*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	Si quiere configurar el cortafuegos para que vuelva a aceptar plantillas, haga clic en **Enable Device and Network Templates (Habilitar plantillas de dispositivo y red)**.

Ajustes de Panorama: Panorama > Setup > Management

Si usa Panorama para gestionar los cortafuegos, configure los siguientes ajustes en Panorama. Estos ajustes determinan los tiempos de espera y los intentos de mensaje de SSL para las conexiones desde Panorama a los cortafuegos gestionados, así como los parámetros de uso compartido de los objetos.

También debe configurar los ajustes de conexión de Panorama en el cortafuegos o en una plantilla en Panorama: consulte Panorama Settings (Configuración de Panorama): Device [Dispositivo] > Setup [Configuración] > Management [Gestión].

El cortafuegos usa una conexión SSL con un cifrado AES256 para registrarse con Panorama. De manera predeterminada, Panorama y el cortafuegos se autentican entre sí utilizando certificados de 2048 bits y usan la conexión SSL para la gestión de configuración y la recopilación de logs. Para proteger aún más estas conexiones SSL, consulte Customize Secure Server Communication (Personalizar comunicación del servidor segura) *para configurar certificados personalizados entre Panorama y sus clientes.*

Tiempo de espera de recepción para conexión a dispositivo	Introduzca el tiempo de espera (en segundos) para recibir mensajes de TCP de todos los cortafuegos gestionados (el intervalo es de 1 a 240; el valor predeterminado es 240).
Enviar tiempo de espera de conexión a dispositivo	Introduzca el tiempo de espera (en segundos) para enviar mensajes de TCP de todos los cortafuegos gestionados (el intervalo es de 1 a 240; el valor predeterminado es 240).
Reintentar recuento de envío SSL a dispositivo	Introduzca el número de reintentos permitidos al enviar mensajes de capa de sockets seguros (SSL) a cortafuegos gestionados (intervalo: 1-64; predeterminado: 25).
Compartir dirección sin utilizar y objetos de servicio con dispositivos	Seleccione esta opción (habilitada de manera predeterminada) para compartir todos los objetos compartidos de Panorama y los objetos específicos de grupos de dispositivos con cortafuegos gestionados. Si deshabilita esta opción, la aplicación busca en las políticas de Panorama referencias a direcciones, grupos de direcciones, servicios y objetos de grupos de servicios, y no comparte ningún objeto sin referencia. Esta opción reduce el recuento total de objetos asegurándose de que PAN-OS solo envíe los objetos necesarios a los cortafuegos gestionados. Si tiene una regla de políticas que se dirige a dispositivos específicos en un grupo de dispositivos, los objetos usados en esa política se consideran utilizados en ese grupo de dispositivos.
Los objetos definidos en antecesores tendrán más prioridad	Seleccione esta opción (deshabilitada de forma predeterminada) para especificar que los valores de los objetos en los grupos antecesores tienen prioridad sobre los de los grupos de descendientes, cuando los grupos de dispositivos en diferentes

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	niveles de la jerarquía tienen objetos del mismo tipo y nombre pero con valores diferentes. Esto significa que si realiza una compilación de grupo de dispositivos, el valor antecesor sustituirá a cualquier valor de cancelación. De la misma manera, esta opción hace que el valor de un objeto compartido reemplace los valores de objetos del mismo tipo y nombre en grupos de dispositivos. Si selecciona esta opción vera el enlace Buscar objetos cancelados.
Find Overridden Objects	Seleccione esta opción (botón en el cuadro de diálogo Settings [Configuración] de Panorama) para enumerar los objetos *difuminados*. Un objeto difuminado es un objeto en la ubicación Compartida que tiene el mismo nombre pero un valor diferente en un grupo de dispositivos. El enlace solo se muestra si especifica Los objetos definidos en antecesores tendrán más prioridad.
Habilitar informes y filtrado en grupos	Seleccione esta opción (deshabilitada de forma predeterminada) para que Panorama pueda almacenar localmente los nombres de usuario, los nombres de grupos de usuarios y la información de asignación de nombre de usuario a grupo que recibe de los cortafuegos. Esta opción es global para todos los grupos de dispositivos de Panorama. Sin embargo, también debe habilitar el almacenamiento local al nivel de cada grupo de dispositivos especificando un Master Device (Dispositivo maestro) y seleccionando la opción Store users and groups from Master Device (Almacenar usuarios y grupos del dispositivo maestro).
Configuración de comunicación segura: Panorama > Setup > Management	
Customize Secure Server Communication (Personalizar comunicación del servidor segura)	• **Custom Certificate Only (Certificado personalizado únicamente)**: cuando esta opción está habilitada, Panorama solo acepta certificados personalizados para la autenticación con cortafuegos gestionados y recopiladores de logs. • **SSL/TLS Service Profile (Perfil del servicio SSL / TLS)**: seleccione un perfil de servicio SSL / TLS del menú desplegable. Este perfil define el certificado y las versiones SSL / TLS admitidas que el cortafuegos puede utilizar para comunicarse con Panorama. • **Certificate Profile (Perfil de certificado)**: seleccione el perfil de certificado del menú desplegable. Este perfil de certificado define la conducta de la comprobación y revocación de certificados y la CA raíz utilizada para autenticar la cadena de certificados presentada por el cliente. • **Authorization List (Lista de autorización)**: haga clic en **Add (Añadir)** para añadir y configurar un nuevo perfil de autorización con los siguientes campos para configurar los criterios de autorización para los dispositivos de cliente que se pueden conectar a Panorama. La lista de autorización admite un máximo de 16 perfiles.

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	• **Identifier (Identificador)**: seleccione **Subject (Asunto)** o **Subject Alt. (Asunto Alt.) Name (Nombre)** como el identificador de autorización. • **Type (Tipo)**: si seleccionó **Subject Alt. (Asunto Alt.) Name (Nombre)**como el identificador, luego seleccione **IP**, **hostname (nombre de host)** o **e-mail (correo electrónico)** como el tipo del identificador. Si ha seleccionado **Subject (Asunto)**, entonces debe utilizar **common name (nombre común)** como el tipo de identificador. • **Value (Valor)**: introduzca el valor del identificador. • **Authorize Clients Based on Serial Number (Autorizar clientes según el número de serie)**: Panorama autoriza dispositivos cliente basado en un hash del número de serie del dispositivo. • **Check Authorization List (Comprobar lista de autorización)**: Panorama comprueba la identidad de los dispositivos cliente con la lista de autorización. Un dispositivo debe coincidir solo con un criterio de la lista para recibir autorización. Si no se encuentra ninguna coincidencia, el dispositivo no está autorizado. • **Disconnect Wait Time (min) (Tiempo de espera de desconexión [min])**: el periodo de tiempo (en minutos) que Panorama espera antes de terminar la conexión actual con sus dispositivos gestionados. Panorama vuelve a establecer las conexiones con sus dispositivos gestionados utilizando los ajustes de comunicaciones del servidor seguro configurada. El tiempo de espera comienza luego de que confirma la configuración de comunicación segura con el servidor.

Comunicación segura con el cliente	Si utiliza **Secure Client Communication (Comunicación de cliente segura)**, esto garantizará que el cliente que utiliza Panorama configure certificados personalizados configurados (en lugar de certificados predefinidos predeterminados) para autenticar las conexiones SSL con otro dispositivo Panorama en un par de HA o un dispositivo WildFire.
	• **Predefined (Predefinido)** (predeterminado): no se configuran certificados de dispositivo y Panorama utiliza el certificado predefinido predeterminado.
	• **Local**: Panorama utiliza un certificado de dispositivo local y la clave privada correspondiente generada en el cortafuegos o importada de un servidor PKI empresarial existente.
	  • **Certificado**: Seleccione el certificado del dispositivo local.
	  • **Perfil de certificado**: Seleccione el perfil de certificado del menú desplegable.
	• **SCEP**: Panorama utiliza un certificado de dispositivo y una clave privada generada por un servidor de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP).
	  • **Perfil de SCEP**: Seleccione un perfil de SCEP del menú desplegable.

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)

	• **Perfil de certificado**: Seleccione el perfil de certificado del menú desplegable.
	• **Customize Communication (Personalizar comunicación)**
	  • **HA Communication (Comunicación de HA)**: Panorama utiliza el certificado de cliente configurado para la comunicación de HA con su par de HA.
	  • **WildFire Communication (Comunicación con WildFire)**: Panorama utiliza el certificado de cliente configurado para la comunicación con un dispositivo WildFire.

Configuración de log e informes

Use esta sección para modificar:

- Periodos de vencimiento y cuotas de almacenamiento para informes y los siguientes tipos de logs. Los ajustes se sincronizan a través de alta disponibilidad.
  - Logs de todos los tipos que el cortafuegos genera y almacena localmente (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]**). Los ajustes se aplican a todos los sistemas virtuales del cortafuegos.
  - Logs que un dispositivo M-Series o un dispositivo virtual Panorama en modo Panorama genera y almacena localmente: Logs de sistema, de configuración, de estadísticas de la aplicación y de User-ID™ (**Panorama** > **Setup [Configuración]** > **Management [Gestión]**).
  - Logs de todos los tipos que el dispositivo virtual Panorama en modo heredado genera localmente o recopila de los cortafuegos (**Panorama** > **Setup (Configuración)** > **Management (Gestión)**).

    Para los logs que los cortafuegos envían a los recopiladores de logs de Panorama, se establecen las cuotas de almacenamiento y los períodos de vencimiento en cada grupo de recopiladores (consulte Panorama > Collector Groups).
- Atributos para calcular y exportar informes de actividad de usuarios.
- Informes predefinidos creados en el cortafuegos o Panorama.

Pestaña Almacenamiento de logs	Para cada tipo de log, especifique:
(Servidor de gestión Panorama y todos los modelos de cortafuegos excepto los cortafuegos de la serie PA-5200 y PA-7000) *Panorama muestra esta pestaña si edita la configuración de logs e informes (Panorama > Setup [Configuración] > Management [Gestión]). Si utiliza una plantilla Panorama para configurar los parámetros de los*	• **Quota (Cuota)**: la **Quota (Cuota)**, en porcentaje, asignada en el disco duro para el almacenamiento de logs. Al cambiar un valor de **Quota (Cuota)**, la asignación de disco asociada cambia automáticamente. Si el total de todos los valores supera el 100%, aparecerá un mensaje de color rojo y un mensaje de error cuando intente guardar la configuración. Si esto sucede, ajuste los porcentajes de modo que el total quede por debajo del límite del 100%. *Los cortafuegos serie VM, de manera predeterminada, tienen una cuota de 0%, que se asigna al almacenamiento de logs de SCTP, al resumen de SCTP, al resumen por hora de SCTP, al resumen diario de SCTP y al resumen semanal de SCTP, de modo que debe asignar un porcentaje a estos cortafuegos para registrar la información del SCTP.*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
cortafuegos (Device [Dispositivo] > Setup [Configuración] > Management [Gestión]), consulte Pestañas Almacenamiento en un único disco y Almacenamiento en múltiples discos*.*	• **Max Days (Días Máx.)**: el periodo de tiempo (en días) para el vencimiento de los logs (el intervalo es de 1 a 2000). El cortafuegos o el dispositivo de Panorama elimina automáticamente los logs que superen el periodo especificado. De manera predeterminada, no se fija ningún periodo de vencimiento, lo que significa que los logs no vencen nunca. El cortafuegos o el dispositivo de Panorama evalúa los logs durante la creación y elimina los logs que superen el periodo de vencimiento o el tamaño de cuota. *Los logs de resumen semanales pueden superar el umbral y continuar hasta la siguiente eliminación si alcanzan el umbral de vencimiento entre dos fechas cuando el cortafuegos elimina los logs. Cuando una cuota de logs alcanza el tamaño máximo, las nuevas entradas de logs comienzan a sobrescribir las entradas de logs antiguas. Si reduce el tamaño de una cuota de log, el cortafuegos o Panorama elimina los logs más antiguos cuando compila los cambios. En una configuración activa/pasiva de HA, el peer pasivo no recibe logs y, por lo tanto, no los elimina a menos que se produzca una conmutación por error y se vuelva activo.*

	• **Core files (Archivos core)**: si su cortafuegos experimenta un fallo del proceso del sistema, generará un archivo core que contiene detalles sobre el proceso y por qué falló. Si un archivo core es demasiado grande para la ubicación de almacenamiento predeterminada del archivo core (partición `/var/cores`), puede habilitar la opción de archivo **`large-core`** para asignar una ubicación de almacenamiento alternativa y de mayor volumen (`/opt/panlogs/cores`). Un ingeniero de soporte de Palo Alto Networks puede aumentar el almacenamiento asignado si es necesario.
	
	Para habilitar o deshabilitar la opción de archivo **`large-core`** , introduzca el siguiente comando CLI desde el modo de configuración y luego **`commit`** la configuración:
	
	`# set deviceconfig setting management large-core [yes|no]`
	
	El archivo core se elimina cuando deshabilita esta opción.
	
	Debe utilizar SCP desde el modo operativo para exportar el archivo core:
	
	`> scp export core-file large-corefile`

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	Únicamente un ingeniero de soporte de Palo Alto Networks puede interpretar el contenido de los archivos core. • **Restore Defaults (Restablecer valores predeterminados)**: seleccione esta opción para volver a los valores predeterminados.
Pestañas **Session Log Storage (Almacenamiento de log de sesión)** y **Management Log Storage (Almacenamiento de log de gestión)** (únicamente cortafuegos serie PA-5200 y PA-7000)	Los cortafuegos Serie PA-5200 y y serie PA-7000 almacenan logs de gestión y logs de sesión en discos separados. Seleccione la pestaña para cada conjunto de logs y configure los ajustes descritos en Pestaña Almacenamiento de logs: • **Almacenamiento de log de sesión**: seleccione **Cuota de log de sesión** y establezca las cuotas y los períodos de vencimiento para Tráfico, Amenaza, URL Filtrado de URL, Coincidencia HIP, User-ID, GTP/Túnel, SCTP, Autenticación y logs de GlobalProtect, además de PCAP de amenaza extendida. • **Management Log Storage (Almacenamiento de log de gestión)**: establece las cuotas y los períodos de vencimiento de los logs de Sistema, Configuración y Estadísticas de la aplicación, así como de Informes HIP, Capturas de filtrado de datos, App PCAP y Debug Filter PCAP.
Pestañas **Single Disk Storage (Almacenamiento en un único disco)** y **Multi Disk Storage (Almacenamiento en múltiples discos)** (Solo plantilla Panorama)	Si utiliza una plantilla de Panorama para configurar las cuotas de logs y los períodos de vencimiento, configure los valores en una o ambas pestañas basadas en los cortafuegos asignados a la plantilla: • Cortafuegos **serie PA-5200 y** PA-7000: seleccione **Multi Disk Storage (Almacenamiento en múltiples discos)** y configure los ajustes en las Pestañas Session Log Storage (Almacenamiento de logs de sesión) y Management Log Storage (Almacenamiento de logs de almacenamiento). *Los cortafuegos serie PA-5200, de manera predeterminada, tienen una cuota de 0%, que se asigna al almacenamiento de logs de SCTP, al resumen de SCTP, al resumen por hora de SCTP, al resumen diario de SCTP y al resumen semanal de SCTP, de modo que debe asignar un porcentaje a estos cortafuegos para registrar la información del SCTP.* • **Todos los demás modelos de cortafuegos**: seleccione **Single Disk Storage (Almacenamiento en un único disco)**, seleccione **Session Log Quota (Cuota de log de sesión)** y configure los ajustes en la Pestaña Log Storage (Almacenamiento de logs).
Pestaña Log Export and Reporting	Configure los siguientes valores de exportación e informes de logs según sea necesario: • **Number of Versions for Config Audit**: introduzca el número de versiones de configuración que se deben guardar antes de

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	descartar las más antiguas (valor predeterminado: 100). Puede utilizar estas versiones guardadas para auditar y comparar cambios en la configuración. • **Number of Versions for Config Backups (Número de versiones para Configurar copias de seguridad)**: (solo Panorama) introduzca el número de copias de seguridad de configuraciones que se deben guardar antes de descartar las más antiguas (valor predeterminado: 100). • **Max Rows in CSV Export (Máx. de filas en exportación CSV)**: introduzca el número máximo de filas que aparecerán en los informes CSV generados cuando selecciona **Export to CSV (Exportar a CSV)** desde la vista de logs de tráfico (el intervalo es 1-1.048.576, el valor predeterminado es 65.535). • **Max Rows in User Activity Report (Máx. de filas en informe de actividad de usuario)**: introduzca el número máximo de filas que se admite para los informes de actividad de usuario detallada (intervalo: 1-1.048.576; valor predeterminado: 5.000).
Pestaña Exportación de Logs e Informes (continuación)	• **Average Browse Time (sec) [Tiempo medio de exploración (seg)]**: configure esta variable para ajustar cómo se calcula el tiempo de exploración en segundos para el informe de actividad del usuario Monitor > PDF Reports > User Activity Report (intervalo: 0-300 s; predeterminado: 60). El cálculo ignorará los sitios categorizados como anuncios web y redes de entrega de contenido. El cálculo del tiempo de exploración se basa en las páginas contenedoras registradas en los logs de filtrado de URL. Las páginas contenedoras se utilizan como base para este cálculo debido a que muchos sitios cargan contenido de sitios externos que no debería considerarse. Para obtener más información sobre la página del contenedor, consulte Páginas de Contenedores. La configuración de tiempo medio de navegación es el tiempo medio que el administrador cree que debería dedicar un usuario a navegar por una página web. Cualquier solicitud realizada después de que haya transcurrido el tiempo medio de exploración se considerará una nueva actividad de exploración. El cálculo ignorará las páginas web nuevas que se carguen entre el momento de la primera solicitud (hora de inicio) y el tiempo medio de exploración. Este comportamiento se ha diseñado para excluir los sitios externos que se carguen dentro de la página web de interés Ejemplo: si el tiempo medio de exploración 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. • **Umbral de carga de página [seg]**: le permite ajustar el tiempo previsto (en segundos) que tardan los elementos de una página en cargarse (el intervalo es de 0 a 60; el valor predeterminado es 20). Cualquier solicitud que se produzca

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	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. El umbral de carga de página también se utiliza en los cálculos para el informe de actividad de usuario Monitor > PDF Reports > User Activity Report. • **Syslog HOSTNAME Format (Formato de HOSTNAME de syslog**: seleccione si desea utilizar el FQDN, el nombre de host o la dirección IP (IPv4 o IPv6) en el encabezado del mensaje syslog. Este encabezado identifica el cortafuegos o el servidor de gestión Panorama en el que se originó el mensaje. • **Report Runtime (Tiempo de ejecución del informe)**: seleccione la hora del día (el valor predeterminado es 2 a. m.) cuando el cortafuegos o Panorama comienza a generar informes diarios programados. • **Report Expiration Period (Periodo de vencimiento de informes)**: defina el periodo de vencimiento en días para los informes (intervalo: 1-2000). De manera predeterminada, no se fija ningún periodo de vencimiento, lo que significa que los informes no vencen nunca. El cortafuegos o el dispositivo de Panorama elimina los informes vencidos por la noche a las 2 a. m. según el horario de su sistema.
	• **Stop Traffic when LogDb full (Detener tráfico cuando LogDb esté lleno)**: (solo cortafuegos; opción deshabilitada de manera predeterminada): seleccione esta opción si desea que se detenga el tráfico a través del cortafuegos cuando la base de datos de logs esté llena. • **Enable Threat Vault Access (Habilitar el acceso a Threat Vault)**: (opción habilitada de forma predeterminada): permite que el cortafuegos acceda a Threat Vault para recopilar la información más reciente sobre las amenazas detectadas. Esta información está disponible para los logs de amenazas y para las principales actividades de amenazas registradas en el ACC. • **Enable Log on High DP Load (Habilitar log con carga alta)**: (solo cortafuegos; opción deshabilitada de manera predeterminada): seleccione esta opción si desea que se genere una entrada de log del sistema cuando la carga de procesamiento del paquete en el cortafuegos esté al 100% de la utilización de la CPU. *Enable Log on High DP Load (Habilitar log con carga alta) permite a los administradores investigar e identificar la causa de la alta utilización de la CPU.* *Una carga alta de CPU puede degradar el funcionamiento porque la CPU no tiene suficientes ciclos para procesar todos los paquetes. El log del sistema le avisa sobre este problema (se genera una entrada de log*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	cada minuto) y le permite investigar la posible causa. • **Enable High Speed Log Forwarding (Habilitación reenvío de logs a alta velocidad)** (Solo cortafuegos serie PA-5200 y PA-7000; opción deshabilitada de forma predeterminada): la práctica recomendada es seleccionar esta opción si desea reenviar logs a Panorama a una velocidad máxima de 120 000 logs / segundo. Cuando la opción está deshabilitada, el cortafuegos envía los logs a Panorama a una velocidad máxima de solo 80 000 logs / segundo. Si habilita esta opción, el cortafuegos no almacena los logs localmente ni los muestra en las pestañas **Dashboard (Panel)**, **ACC** o **Monitor (Supervisor)**. Además, debe configurar el reenvío de logs a Panorama para usar esta opción. • **Log Collector Status (Estado del recopilador de logs)** indica si el cortafuegos estableció correctamente una conexión con la arquitectura de recopilación de logs distribuida y si está enviando logs hacia dicha arquitectura. Si el cortafuegos también está configurado para enviar logs al servicio de creación de logs, verifique el **Logging Service Status (Estado del servicio de creación de logs)**, en la sección Servicio de creación de logs.
(Solo en Panorama)	• **Buffered Log Forwarding from Device (Reenvío de log en búfer desde dispositivo)** (opción habilitada de forma predeterminada): permite al cortafuegos almacenar en búfer las entradas de log en su disco duro (almacenamiento local) cuando pierde la conexión con Panorama. Cuando se restaura la conexión con Panorama, el cortafuegos reenvía las entradas de log a Panorama; el espacio en disco disponible para el almacenamiento en búfer depende de la cuota de almacenamiento de logs para el modelo de cortafuegos y el volumen de los logs que quedan por ejecutar. Si se consume el espacio, las entradas más antiguas se eliminarán para permitir el registro de nuevos eventos. *Habilite Buffered Log Forwarding from Device (Reenvío de log en búfer desde dispositivo) para ayudar a prevenir la pérdida de logs si la conexión a Panorama se desactiva.* • **Get Only New Logs on Convert to Primary (Obtener únicamente nuevos logs al convertir a principal)** (opción deshabilitada de forma predeterminada): esta opción solo se aplica a un dispositivo virtual Panorama en modo heredado que graba logs en un sistema de archivos de red (Network File System, NFS). Con los logs de NFS solo se monta la instancia principal de Panorama en el NFS. Por lo tanto, los cortafuegos solo envía logs a la instancia activa principal de Panorama. Esta opción le permite configurar los cortafuegos para que solo envíen los logs recién generados a Panorama cuando se produce una conmutación por error de HA y la

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	instancia secundaria de Panorama continúa creando logs para el NFS (después de promocionarse como principal). Este comportamiento suele habilitarse para impedir que los cortafuegos envíen grandes volúmenes de logs almacenados en búfer cuando se restablezca la conexión con Panorama después de un período de tiempo significativo. • **Only Active Primary Logs to Local Disk (Solo logs principales activos al disco local)** (opción deshabilitada de forma predeterminada): esta opción solo se aplica a un dispositivo virtual de Panorama en modo heredado. Esta opción le permite configurar únicamente el Panorama activo-para guardar logs en el disco local.
	Pre-Defined Reports (Informes predefinidos): (opción deshabilitada de forma predeterminada): los informes predefinidos de aplicación, tráfico, amenazas, filtrado de URL y Protocolo de transmisión de control de secuencias (Stream Control Transmission Protocol, SCTP) se encuentran disponibles en el cortafuegos y en Panorama. Los informes predefinidos para el SCTP se encuentran disponibles en el cortafuegos y en Panorama luego de que se habilita la seguridad de SCTP en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **General Settings (Configuración general)**. Debido a que los cortafuegos consumen recursos de memoria para generar resultados cada hora (y reenviarlos a Panorama donde se agregan y se compilan para su visualización), puede deshabilitar los informes que no sean relevantes para reducir el uso de la memoria. Para deshabilitar un informe, deshabilite esta opción del informe. Haga clic en**Select All (Seleccionar todo)** o **Deselect All (Anular selección)** para habilitar o deshabilitar completamente la generación de los informes predefinidos. *Antes de deshabilitar un informe, compruebe de que no hay un informe de grupo o un informe de PDF que lo esté usando. Si deshabilita un informe predefinido asignado a un conjunto de informes, el conjunto completo de informes no tendrán datos.*
Banners y mensajes Para ver todos los mensajes en un diálogo de Mensaje del día, consulte Mensaje del día. *Después de configurar el mensaje del día y hacer clic en OK (Aceptar), los administradores que inician sesión después y los administradores activos que actualizan sus navegadores verán el mensaje nuevo y actualizado de inmediato; no es necesaria una confirmación. Esto le permite advertirles a otros administradores de una confirmación inminente antes de llevarla a cabo.*	

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
Mensaje del día (casilla de verificación)	Seleccione esta opción para habilitar el cuadro de diálogo del mensaje del día y mostrarlo cuando el administrador inicia sesión en la interfaz web.
Mensaje del día (text-entry field)	Ingrese el texto (hasta 3200 caracteres) para el cuadro de diálogo del mensaje del día.
Permitir no mostrar de nuevo	Seleccione esta opción (deshabilitada de forma predeterminada) para incluir la opción **Do not show again (No volver a mostrar)** en el cuadro de diálogo del mensaje del día. Esto le brinda a los administradores la opción de evitar ver el mismo mensaje en inicios de sesión subsiguientes. *Si modifica el texto del campo Message of the Day (Mensaje del día):, el mensaje se muestra hasta a los administradores que seleccionaron Do not show again (No volver a mostrar). Los administradores deben volver a seleccionar esta opción para evitar ver el mensaje modificado en las siguientes sesiones a menos que el mensaje se vuelta a modificar.*
Title	Ingrese texto para el encabezado del mensaje del día (el texto predeterminado es `Message of the Day`).
Color de fondo	Seleccione un color de fondo para el cuadro de diálogo del mensaje del día. El valor predeterminado (**None (Ninguno)**) es un fondo de color gris claro.
Icono	Seleccione un icono predefinido para que aparezca por encima del texto en el cuadro de diálogo Day dialog (Mensaje del día): • **None (Ninguno)** (predeterminado) • **Error** • **Help (Ayuda)** • **Information (Información)** • **Warning (Advertencia)**
Banner del encabezado	Ingrese el texto que muestra el banner del encabezado (hasta 3200 caracteres).
Color de encabezado	Seleccione un color para el fondo del encabezado. El valor predeterminado (**None (Ninguno)**) es un fondo transparente.
Color de texto de encabezado	Seleccione un color para el texto del encabezado. El valor predeterminado (**None (Ninguno)**) es negro.
Mismo banner para encabezado y pie de página	Seleccione esta opción (habilitado de manera predeterminada) si desea que el banner del pie de página tenga el mismo texto y

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	colores que el banner del encabezado. Cuando está habilitada esta opción, los colores y los campos de texto del banner del pie de página están atenuados.
Banner del pie de página	Ingrese el texto que muestra el banner del pie de página (hasta 3200 caracteres).
Color de pie de página	Seleccione un color para el fondo del pie de página. El valor predeterminado (**None (Ninguno)**) es un fondo transparente.
Color de texto de pie de página	Seleccione un color para el texto del pie de página. El valor predeterminado (**None (Ninguno)**) es negro.
Complejidad de contraseña mínima	
Habilitado	Habilite los requisitos de contraseña mínimos para cuentas locales. Con esta función, puede garantizar que las cuentas de administrador locales del cortafuegos cumplan un conjunto definido de requisitos de contraseña. También puede crear un perfil de contraseña con un subconjunto de estas opciones que cancelará estos ajustes y que puede aplicarse a cuentas específicas. Para obtener más información, consulte Device > Password Profiles y consulte Requisitos de nombre de usuario y contraseña para obtener información sobre los caracteres válidos que pueden utilizarse en las cuentas. *La longitud máxima de la contraseña es de 31 caracteres. Evite los requisitos de configuración que PAN-OS no acepta. Por ejemplo, no establezca un requisito de 10 mayúsculas, 10 minúsculas, 10 números y 10 caracteres especiales, ya que esto excedería la longitud máxima de 31 caracteres.* Si la alta disponibilidad (HA) ya se encuentra configurada, utilice siempre el peer principal cuando configure opciones de complejidad de contraseña y confirme lo antes posible después de realizar cambios. La configuración mínima de complejidad de contraseñas no se aplica a las cuentas de base de datos locales para las que indicó **Password Hash (Contraseña con hash)** (consulte Device > Local User Database > Users). *Exija contraseñas seguras para ayudar a evitar que prosperen los ataques de fuerza bruta de acceso a la red. Exija una longitud mínima y el uso de al menos una letra mayúscula, una letra minúscula, un número y un carácter especial. Además, impida la repetición excesiva de caracteres y nombres de usuario y contraseñas, establezca límites sobre la frecuencia con la que se pueden reutilizar las contraseñas, y fije*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	periodos regulares de cambio de contraseña, para que las contraseñas no se utilicen durante demasiado tiempo. Mientras más estrictos sean los requisitos para la contraseña, más difícil será para los atacantes hackearla. Asegúrese de seguir las prácticas recomendadas sobre seguridad de la contraseña *para garantizar que la contraseña sea segura.*
Longitud mínima	Requiere una longitud mínima de contraseña (el intervalo es de 1 a 15 caracteres).
Letras en mayúscula mínimas	Requiere un número mínimo de letras en mayúscula (el intervalo es de 0 a 15 caracteres).
Letras en minúscula mínimas	Requiere un número mínimo de letras en minúscula (el intervalo es de 0 a 15 caracteres).
Letras numéricas mínimas	Requiere un número mínimo de letras numéricas (el intervalo es de 0 a 15 caracteres).
Caracteres especiales mínimos	Requiere un número mínimo de caracteres especiales (no alfanuméricos) (el intervalo es de 0 a 15 caracteres).
Bloquear caracteres repetidos	Especifique el número de caracteres duplicados secuenciales permitidos en una contraseña (el intervalo es 2-15). Si establece el valor en 2, la contraseña puede contener el mismo carácter dos veces seguidas, pero si el mismo carácter se usa tres o cuatro veces seguidas, la contraseña no se permitirá. Por ejemplo, si el valor se fija en 2, el sistema aceptará la contraseña test11 u 11test11, pero no test111, porque el número 1 aparece tres veces seguidas.
Bloquear inclusión de nombre de usuario (incluida su inversión)	Seleccione esta opción para impedir que el nombre de usuario de la cuenta (o la versión invertida del nombre) se utilice en la contraseña.
La nueva contraseña difiere por caracteres	Cuando los administradores cambien sus contraseñas, los caracteres deben diferir según el valor especificado.
Es necesario cambiar la contraseña al iniciar sesión por primera vez.	Seleccione esta opción para pedir a los administradores que cambien sus contraseñas la primera vez que inicien sesión en el cortafuegos.
Límite para impedir la reutilización de contraseñas	Exija que no se reutilice una contraseña anterior basándose en el recuento especificado. Por ejemplo, si el valor se establece en 4, no podrá reutilizar ninguna de sus últimas 4 contraseñas (el intervalo es 0 a 50).

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
Bloquear período de cambio de contraseña (días)	El usuario no podrá cambiar sus contraseñas hasta que no se haya alcanzado el número de días especificado (el intervalo es de 0 a 365 días).
Required Password Change Period (Período necesario para el cambio de contraseña) (días)	Requiere que los administradores cambien su contraseña con regularidad (en días) (el intervalo es de 0 a 365 días). Por ejemplo, si el valor se establece en 90, se pedirá a los administradores que cambien su contraseña cada 90 días. También puede establecer una advertencia de vencimiento de 0-30 días y especificar un período de gracia.
Expiration Warning Period (Período de advertencia de vencimiento) (días)	Si se establece un **Required Password Change Period (Período necesario para el cambio de contraseña)**, puede utilizar el **Expiration Warning Period (Período de advertencia de vencimiento)** para pedir a los usuarios en cada log que cambien sus contraseñas cuando resten menos de un número días especificado antes de la fecha de cambio requerida (el intervalo es de 0 a 30).
Post Expiration Admin Login Count (Recuento de inicio de sesión de administrador posterior al vencimiento) (conteo)	Permite que el administrador inicie sesión un número de días especificado después de la fecha de cambio requerida (el intervalo es de 0 a 3). Por ejemplo, si establece este valor en 3 y su cuenta ha vencido, podrán iniciar sesión 3 veces más sin cambiar su contraseña antes de que su cuenta se bloquee.
Período de gracia posterior al vencimiento (días)	Permite que el administrador inicie sesión el número de días especificado después de que su cuenta haya vencido (intervalo es de 0 a 30).
AutoFocus™	
Habilitado	Habilite el cortafuegos para que se conecta a un portal de AutoFocus para recuperar los datos de inteligencia de amenazas y habilitar las búsquedas integradas entre el cortafuegos y AutoFocus. Cuando está conectado a AutoFocus, el cortafuegos muestra los datos de AutoFocus asociados a entradas de logs de tráfico, amenazas, filtrado de URL, envíos de WildFire y filtrado de datos (**Monitor [Supervisar]** > **Logs**). Puede hacer clic en un artefacto en estos tipos de entradas de logs (como una dirección IP o una URL) para mostrar un resumen de las estadísticas y resultados de AutoFocus para ese artefacto. Puede abrir una búsqueda de AutoFocus ampliada para el artefacto directamente desde el cortafuegos. *Compruebe que su licencia de AutoFocus esté activa en el cortafuegos (Device [Dispositivo] > Licenses [Licencias]). Si no se muestra la licencia de AutoFocus, use una de las siguientes*

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	opciones de License Management (Gestión de licencias) para activar la licencia.
URL de AutoFocus	Ingrese la URL de AutoFocus: **`https://autofocus.paloaltonetworks.com:10443`**
Tiempo de espera de la consulta (segundos)	Establezca la duración de tiempo (en segundos) para que el cortafuegos intente consultar a AutoFocus sobre los datos de inteligencia de amenazas. Si el portal de AutoFocus no responde antes del final del período especificado, el cortafuegos cerrará la conexión.

Servicio de creación de logs

Utilice esta sección para configurar los cortafuegos VM-Series y basados en hardware para reenviar logs a Cortex Data Lake. A continuación se muestra el flujo de trabajo completo para configurar las opciones que se describen a continuación:

- Iniciar el envío de logs en Cortex Data Lake (sin Panorama)
- Iniciar el envío de logs en Cortex Data Lake (para cortafuegos gestionados por Panorama)

El servicio de envío de logs ahora se llama Cortex Data Lake; sin embargo, algunas funciones y botones del cortafuegos aún muestran el nombre Servicio de envío de logs.

Enable Logging Service (Habilitar servicio de creación de logs)	Elija esta opción para habilitar el cortafuegos (o, si está usando Panorama, cortafuegos que pertenecen a la **plantilla** seleccionada) para reenviar registros a Cortex Data Lake (Cortex Data Lake anteriormente se llamaba Servicio de envío de logs) . Después de configurar el reenvío de registros (Objetos > Reenvío de logs), el cortafuegos reenvía los registros directamente a Cortex Data Lake; esto es cierto incluso para los cortafuegos gestionados por Panorama.
Habilitar el registro duplicado (solo para cortafuegos gestionado por Panorama)	**Habilite el registro duplicado** para continuar enviando logs a Panorama y recopiladores de logs distribuidos, además de enviar registros a Cortex Data Lake. Esta es una opción útil si está evaluando Cortex Data Lake; cuando se habilita, los cortafuegos que pertenecen a la plantilla seleccionada guardarán una copia de los registros en Cortex Data Lake y en su arquitectura Panorama o de la recopilación de logs distribuida.
Enable Enhanced Application Logging (Habilitar creación mejorada de logs de aplicación)	Seleccione la opción **Enable Enhanced Application Logging (Habilitar creación mejorada de logs de aplicación)** si desea que el cortafuegos recopile datos que aumenten la visibilidad de la red para las aplicaciones de Palo Alto Networks. Por ejemplo, la visibilidad mejorada de la red permite que las aplicaciones de Palo Alto Networks Cortex XDR categoricen y establezcan mejor referencias para una actividad de red normal, de modo que el cortafuegos pueda detectar comportamientos inusuales que podrían indicar un ataque.

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	La creación mejorada de logs de aplicaciones requiere una licencia de servicio de envío de logs (Cortex Data Lake). No podrá ver estos logs; se diseñan para que solo las aplicaciones de Palo Alto Networks los utilicen.
Región	Seleccione la región geográfica de la instancia de Cortex Data Lake (servicio de registro) a la que el cortafuegos reenviará los registros. Inicie sesión en la central de Cortex para confirmar la región en la que se implementa una instancia de Cortex Data Lake (en la central, seleccione el engranaje de configuración en la barra de menú superior y haga clic en **Gestionar aplicaciones**).
recuento de conexión para servicio de logging para la serie PA-7000 ay PA-5200	(Cortafuegos PA-7000 Series y PA-5200 Series) Especifique la cantidad de conexiones para enviar logs desde los cortafuegos hacia Cortex Data Lake (el intervalo es de 1 a 20; el valor predeterminado es 5). Puede usar el comando de la CLI **`request logging-service-forwarding status`** en el cortafuegos para verificar la cantidad de conexiones activas entre el cortafuegos y Cortex Data Lake.
Incorporado sin Panorama (para cortafuegos no gestionados por Panorama)	Puede habilitar cortafuegos no gestionados por Panorama para iniciar sesión en Cortex Data Lake. Para hacer esto, primero deberá generar una clave en la aplicación de Cortex Data Lake. Esta clave permite que el cortafuegos se autentique y se conecte de forma segura a Cortex Data Lake. Una vez que haya generado la clave, introdúzcala aquí. A continuación, continúe para habilitar el cortafuegos para comenzar a reenviar registros a Cortex Data Lake.
Estado de servicio de logging	Visualice el estado de la conexión a Cortex Data Lake. Seleccione **Show Status (Mostrar estado)** para ver los detalles de las siguientes comprobaciones: • **Licencia**: `Correcto` o `Error` para indicar si el cortafuegos tiene una licencia válida para reenviar logs a Cortex Data Lake. • **Certificado**: `Correcto` o `Error` para indicar si el cortafuegos recuperó correctamente el certificado necesario para la autenticación en Cortex Data Lake. • **Información del cliente**: `Correcto` o `Error` para indicar si el cortafuegos tiene el número de identificación del cliente requerido para usar Cortex Data Lake. Cuando el estado es `OK (Correcto)`, puede ver también el número de identificación del cliente. • **Conectividad del dispositivo**: indica si el cortafuegos se conectó correctamente a Cortex Data Lake.

© 2020 Palo Alto Networks, Inc.

Device > Setup > Operations

Puede llevar a cabo las siguientes tareas para gestionar las configuraciones candidatas y en ejecución del cortafuegos y Panorama™. Si está utilizando un dispositivo virtual Panorama, también puede utilizar los ajustes en esta página para configurar Particiones de almacenamiento de logs para un dispositivo virtual de Panorama en modo Legacy.

Debe realizar la Confirmación de los cambios que realizó en la configuración candidata para activar esos cambios, cuando se convertirán en parte de la configuración en ejecución. Como práctica recomendada, periódicamente seleccione Guardar configuraciones candidatas.

Puede utilizar Secure Copy (SCP) commands from the CLI (Comandos Secure Copy [SCP] de la CLI) para exportar los archivos, logs, informes y otros archivos de la configuración a un servidor SCP, e importarlos a otro cortafuegos, dispositivo virtual o dispositivo Panorama serie M. Sin embargo, debido a que la base de datos de logs es demasiado grande para una exportación o importación, los siguientes modelos no admiten exportar o importar la base de datos de logs completa: Los cortafuegos serie PA-7000 (todas las versiones de PAN-OS®), los dispositivos virtuales de Panorama que ejecutan Panorama 6.0 o versiones posteriores y los dispositivos Panorama serie M (todas las versiones de Panorama).

Función	Description (Descripción)
gestión de la configuración	
Volver a la última configuración guardada	Restaura la instantánea predeterminada (.snapshot.xml) de la configuración candidata (la instantánea que crea o sobrescribe cuando selecciona **Config (Configuración)** > **Save Changes (Guardar cambios)** en la parte superior derecha de la interfaz web). (Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para revertir. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Volver a la configuración en ejecución	Restablece la configuración en ejecución actual. Esta operación deshace todos los cambios que realizaron todos los administradores a la configuración candidata desde la última confirmación. Para revertir solo los cambios de administradores específicos, consulte Revertir cambios. (Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para revertir. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Guardar instantánea de configuración con nombre	Crea una instantánea de la configuración candidata que no sobrescribe la instantánea predeterminada (.snapshot.xml). Introduzca un **Name (Nombre)** para la instantánea o seleccione una existente para sobrescribirla.

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
	(Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para guardar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Guardar configuración candidata	Crea o sobrescriba la instantánea predeterminada de la configuración candidata (.snapshot.xml) con la configuración candidata actual. Esta es la misma acción que cuando hace clic en **Config** > **Save Changes (Guardar cambios)** en la parte superior derecha de la interfaz web. Para guardar sólo los cambios de administradores específicos, consulte Guardar configuraciones candidatas. (Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para guardar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Cargar instantánea de configuración con nombre (cortafuegos) O Cargar instantánea de configuración Panorama con nombre	Sobrescribe la configuración candidata actual con una de las siguientes: • Instantánea de la configuración candidata con nombre personalizado (en lugar de la instantánea predeterminada). • Configuración en ejecución con nombre personalizado que importó. • Configuración en ejecución actual. La configuración debe residir en el cortafuegos o Panorama en el que lo está cargando. Seleccione el **Name (Nombre)** de la configuración e introduzca la **Decryption Key (Clave de descifrado)**, que es la clave maestra del cortafuegos o Panorama (consulte Device > Master Key and Diagnostics). La clave maestra es necesaria para descifrar todas las contraseñas y claves privadas dentro de la configuración. Si está cargando una configuración importada, debe introducir la clave maestra del cortafuegos o Panorama desde el que importó. Una vez finalizada la operación de carga, la clave maestra del cortafuegos o Panorama en el que se cargó la configuración vuelve a cifrar las contraseñas y las claves privadas. Para generar nuevos identificadores únicos universales (Universal Unique Identifier, UUID) para todas las reglas de la configuración (por ejemplo, si está cargando una configuración de otro cortafuegos, pero desea mantener reglas únicas al cargar esa configuración), el superusuario debe **Regenerate Rule UUIDs for selected named configuration (Regenerar UUID de regla para la configuración con nombre seleccionada)** para generar nuevos UUID para todas las reglas. (Solo Panorama) Especifique el objeto, la política, el grupo de dispositivos o las configuraciones de plantilla para cargar parcialmente las configuraciones desde la configuración con nombre al seleccionar lo siguiente: • **Load Shared Objects (Cargar objetos compartidos)**: cargue únicamente los objetos compartidos, junto con todas las configuraciones de grupo de dispositivos y plantilla.

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
	• **Load Shared Policies (Cargar políticas compartidas)**: cargue únicamente las políticas compartidas, junto con todas las configuraciones de grupo de dispositivos y plantilla. • Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)**: especifique grupos de dispositivos, plantillas o configuraciones de pilas de plantillas para cargar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado. • **Retain Rule UUIDs (Conservar UUID de la regla)**: mantenga los UUID de la configuración que se está ejecutando.
Cargar versión de configuración (cortafuegos) O Cargar versión de configuración de Panorama	Restaura la configuración candidata actual con una versión anterior de la configuración en ejecución que se almacena en el cortafuegos o en Panorama. Seleccione el **Name (Nombre)** de la configuración e introduzca la **Decryption Key (Clave de descifrado)**, que es la clave maestra del cortafuegos o Panorama (consulte Device > Master Key and Diagnostics). La clave maestra es necesaria para descifrar todas las contraseñas y claves privadas dentro de la configuración. Una vez finalizada la operación de carga, la clave maestra vuelve a cifrar las contraseñas y las claves privadas. (Solo Panorama) Especifique el objeto, la política, el grupo de dispositivos o las configuraciones de plantilla para cargar parcialmente las configuraciones desde la configuración con nombre al seleccionar lo siguiente: • **Load Shared Objects (Cargar objetos compartidos)**: cargue únicamente los objetos compartidos, junto con todas las configuraciones de grupo de dispositivos y plantilla. • **Load Shared Policies (Cargar políticas compartidas)**: cargue únicamente las políticas compartidas, junto con todas las configuraciones de grupo de dispositivos y plantilla. • Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)**: especifique grupos de dispositivos, plantillas o configuraciones de pilas de plantillas para cargar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Exportar instantánea de configuración con nombre	Exporta la configuración en ejecución actual, una instantánea de la configuración candidata o una configuración previamente importada (candidata o en ejecución). El cortafuegos exporta la configuración como un archivo XML con el nombre especificado. Puede guardar la instantánea en cualquier ubicación de red. (Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para exportar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
Exportar versión de configuración	Exporta una **Version (Versión)** de la configuración en ejecución como un archivo XML. (Solo Panorama) Seleccione **Select Device Groups & Templates (Seleccionar grupos de dispositivos y plantillas)** para seleccionar grupos de dispositivos, plantillas o configuraciones de pilas de plantillas específicas para exportar. Los administradores de grupos de dispositivos y plantillas solo pueden seleccionar los grupos de dispositivos, plantillas o pilas de plantillas designadas en su dominio de acceso asignado.
Exportar lote de configuración de dispositivos y Panorama (Solo en Panorama)	Genera y exporta la versión más reciente de la copia de seguridad de configuración en curso de Panorama y de los cortafuegos gestionados. Para automatizar el proceso de crear y exportar el lote de configuración diariamente a un servidor SCP o FTP, consulte Panorama > Device Deployment.
Export or push device config bundle (Exportar o insertar lote de configuración de dispositivo) (Solo en Panorama)	Le indica que seleccione un cortafuegos y realice una de las siguientes acciones en la configuración del cortafuegos almacenada en Panorama: • **Push & Commit** envía y confirma la configuración en el cortafuegos. La acción limpia el cortafuegos (elimina cualquier configuración local del mismo) y envía la configuración del cortafuegos almacenada en Panorama. Después de importar una configuración de cortafuegos, use esta opción para limpiarlo, de modo que pueda gestionarlo usando Panorama. • **Export (Exportar)**: exporte la configuración al cortafuegos sin cargarlo. Para cargar la configuración, debe acceder a la CLI del cortafuegos y ejecutar el comando del modo de configuración **load device-state (cargar estado de dispositivo)**. Este comando limpia el cortafuegos del mismo modo que la opción **Push & Commit (Enviar y compilar)**. *Estas opciones están disponibles solo para los cortafuegos que ejecutan PAN-OS 6.0.4 y versiones posteriores.*
Exportar estado de dispositivo (Solo cortafuegos)	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™, el lote también incluye información del certificado, una lista de satélites que el portal gestiona 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. *Debe realizar manualmente la exportación del estado del cortafuegos o crear una secuencia de comandos programada de la API XML para exportar el archivo a un servidor remoto. Esto debe hacerse con regularidad, ya que puede que los certificados de satélite cambien a menudo.* Para crear el archivo de estado del cortafuegos a partir de la CLI, a partir del modo de configuración, ejecute el comando **`save device state`**. El archivo se denominará `device_state_cfg.tgz` y se guardará en `/opt/pancfg/mgmt/device-state`. El comando operativo para exportar

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
	el archivo de estado del cortafuegos es **`scp export device-state`** (también puedes usar **`tftp export device-state`**). Para obtener información sobre cómo utilizar la API XML o REST, consulte la Guía de la API de Panorama y PAN-OS.
Importar instantánea de configuración con nombre	Importa una configuración candidata o en ejecución desde cualquier ubicación de red. Haga clic en **Browse (Buscar)** y seleccione el archivo de configuración que debe importarse.
Importar estado de dispositivo (Solo cortafuegos)	Importa el lote de información de estado que se exportó desde el cortafuegos mediante la opción **Export device state (Exportar estado de dispositivo)** 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, el lote 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.
Importar configuración del dispositivo en Panorama (Solo en Panorama)	Importa una configuración de cortafuegos en Panorama. Panorama crea automáticamente una plantilla que contenga las configuraciones de red y dispositivo. Para cada sistema virtual (vsys) en el cortafuegos, Panorama crea automáticamente un grupo de dispositivos que contenga las configuraciones de política y objetos. Los grupos de dispositivos estarán un nivel por debajo de la ubicación compartida en la jerarquía, aunque puede reasignarlos a un grupo de dispositivos principal diferente cuando finalice la importación (consulte Panorama > VMware NSX). *Las versiones de contenido en Panorama (por ejemplo, base de datos de aplicaciones y amenazas) deben ser iguales o superiores a las versiones del cortafuegos desde el que importa una configuración.* Configure las siguientes opciones de importación: • **Device (Dispositivo)**: Seleccione el cortafuegos desde el que Panorama importará las configuraciones. El menú desplegable solo incluye los cortafuegos conectados a Panorama y no asignados a ningún grupo de dispositivos o plantilla. Puede seleccionar solamente un cortafuegos completo, no un vsys individual. • **Template Name (Nombre de plantilla)**: Introduzca un nombre para la plantilla que contendrá el dispositivo importado y los ajustes de red. Para un cortafuegos con vsys múltiple, el campo estará vacío. Para otros cortafuegos, el valor predeterminado es el nombre del cortafuegos. No puede usar el nombre de una plantilla existente. • **Device Group Name Prefix (Prefijo de nombre de grupo de dispositivos)** (únicamente cortafuegos vsys múltiple): de manera opcional, añada una cadena de caracteres como prefijo para cada nombre de grupo de dispositivos. • **Device Group Name (Nombre de grupo de dispositivo)**: Para un cortafuegos vsys múltiple, cada grupo de dispositivo tiene un nombre vsys de manera predeterminada. Para otros cortafuegos, el valor

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)

	predeterminado es el nombre del cortafuegos. Puede editar los nombres predeterminados, pero no puede usar el nombre de un grupo de dispositivo existente.
	• **Import devices' shared objects into Panorama's shared context (Importar objetos compartidos de los dispositivos en el contexto compartido de Panorama)** (habilitada de manera predeterminada): Panorama importa objetos de Shared (Compartido) en el cortafuegos a Shared (Compartido) en Panorama.
	
	Panorama considera que todos los objetos se comparten en un cortafuegos sin varios sistemas virtuales. Si deshabilita esta opción, Panorama copia los objetos del cortafuegos compartidos en grupos de dispositivos en lugar de en Compartidos. Este ajuste tiene las siguientes excepciones:
	
	  • Si un objeto de cortafuegos compartido se llama igual y tiene el mismo valor que un objeto de Panorama existente, la importación excluye el objeto del cortafuegos.
	  • Si el nombre o el valor del objeto compartido del cortafuegos no coinciden con el objeto compartido de Panorama, este importa el objeto del cortafuegos en cada grupo de dispositivos.
	  • Si una configuración importada en una plantilla hace referencia a un objeto de cortafuegos compartido, Panorama importa ese objeto en Compartidos independientemente de que seleccione esta opción.
	  • Si un objeto compartido hace referencia a una configuración importada en una plantilla, Panorama importa el objeto en un grupo de dispositivos independientemente de que seleccione esta opción.
	• **Rule Import Location (Ubicación de importación de reglas)**: Seleccione si Panorama importará las políticas como reglas previas o posteriores. Independientemente de su selección, Panorama importa reglas de seguridad predeterminadas (predeterminada intrazona y predeterminada entre zonas) en la base de reglas posterior.
	
	Si Panorama tiene una regla que se llama igual que una regla de cortafuegos que está importando, Panorama muestra ambas reglas. Sin embargo, los nombres de reglas deben ser exclusivos: elimine una de las reglas antes de confirmar en Panorama; de lo contrario, la confirmación fallará.

Operaciones de dispositivo	
Reiniciar	Para reiniciar el cortafuegos o Panorama, haga clic en **Reboot Device (Reiniciar dispositivo)**. El cortafuegos o Panorama cierra su sesión, vuelve a cargar el software (PAN-OS o Panorama) y la configuración activa, cierra y registra las sesiones existentes, y crea un log del sistema que muestra el nombre del administrador que inició el apagado. Todos los cambios de configuración que no se guardan o confirman se pierden (consulte Device > Setup > Operations).

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
	Si la interfaz web no está disponible, utilice el siguiente comando de la CLI: **`request restart system`**
Apagar	Para realizar el apagado correcto del cortafuegos o Panorama, haga clic en **Shutdown Device (Apagar dispositivo)** o **Shutdown Panorama (Apagar Panorama)** y, a continuación, haga clic en **Yes (Sí)** en el mensaje de confirmación. Todos los cambios de configuración que no se hayan guardado o confirmado se perderán. Todos los administradores cerrarán sesión y se producirán los siguientes procesos: • Se cerrarán todas las sesiones de inicio de sesión. • Se deshabilitarán las interfaces. • Se detendrán todos los procesos del sistema. • Se cerrarán y registrarán las sesiones existentes. • Se crearán logs del sistema que mostrarán el nombre del administrador que inició el apagado. Si no se puede crear esta entrada de log, aparecerá una advertencia y el sistema no se apagará. • Ahora podrá desmontar de manera limpia las unidades de disco y el cortafuegos o Panorama dejará de recibir alimentación. Debe desenchufar la fuente de alimentación y volver a enchufarla antes de poder activar el cortafuegos o Panorama. *Si la interfaz web no está disponible, utilice el siguiente comando de la CLI:* **`request shutdown system`**
Reiniciar plano de datos	Seleccione **Restart Dataplane (Reiniciar plano de datos)** para reiniciar las funciones de datos del cortafuegos sin reiniciarlo. Esta opción no está disponible en Panorama o en los cortafuegos de la serie PA-220, PA-800 o VM. *Si la interfaz web no está disponible, utilice el siguiente comando de la CLI:* ***`request restart dataplane`*** En los cortafuegos serie PA-7000, cada NPC tiene un plano de datos de modo que pueda reiniciar el PNC y realizar esta operación ejecutando el comando **`request chassis restart slot`**.
Varios	
Logotipos personalizados	Utilice **Custom Logos (Logotipos personalizados)** para personalizar cualquiera de los siguientes elementos: • Imagen de fondo de la **pantalla de inicio de sesión** • Imagen de encabezado de la **interfaz de usuario principal** (interfaz web)

© 2020 Palo Alto Networks, Inc.

Función	Description (Descripción)
	• Imagen de la **página de título del informe en PDF** Consulte Monitor > PDF Reports > Manage PDF Summary. • Imagen de **pie de página del informe en PDF** Cargue (<image>) un archivo de imagen para obtener una vista previa o eliminar ( ) una imagen cargada previamente. Para volver al logotipo predeterminado, elimine su entrada y haga clic en **Commit (Confirmar)**. En **Login Screen (Pantalla de inicio de sesión)** y **Main UI (Interfaz de usuario principal)**, puede mostrar ( ) la imagen como aparecerá; si es necesario, el cortafuegos recorta la imagen para que se ajuste. En el caso de informes en PDF, el tamaño de las imágenes se ajustará automáticamente sin recortarlas. En todos los casos, la vista previa muestra las dimensiones de imagen recomendadas. El tamaño máximo de imagen 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 debido a que interfieren con la generación del informe en PDF. Es posible que tenga que ponerse en contacto con el creador de la imagen para eliminar los canales alfa o asegurarse de que el software de gráficos que está utilizando no guarde los archivos con la función de canal alfa. Para obtener información sobre la generación de informes PDF, consulte Monitor > PDF Reports > Manage PDF Summary.
Configuración de SNMP	Habilitación de supervisión de SNMP.
Configuración de partición de almacenamiento (Panorama únicamente)	Particiones de almacenamiento de logs para un dispositivo virtual de Panorama en modo Legacy.

Habilitación de supervisión de SNMP

- Device > Setup > Operations

SNMP (Protocolo simple de administración de redes) es un protocolo estándar para la supervisión de los dispositivos de su red. Seleccione **Operations (Operaciones)** para configurar el cortafuegos y usar la versión de SNMP compatible con su gestor de SNMP (SNMPv2c o SNMPv3). Para obtener una lista de los MIB que debe cargar en el gestor de SNMP para que pueda interpretar las estadísticas que recopila del cortafuegos, consulte MIB admitidas. Para configurar el perfil del servidor que permite que el cortafuegos se comunique con los destinos de trap SNMP de su red, consulte Device (Dispositivo) > Server Profiles (Perfiles de servidor) > SNMP Trap (Trap SNMP). Los MIB SNMP definen todos los traps SNMP que genera el cortafuegos. Un trap SNMP identifica un evento con un ID de objeto único (OID) y los campos individuales se definen como una lista de enlaces de variables (varbind). Haga clic en **NMP Setup (Configuración NMP)** y especifique los siguientes ajustes para permitir las solicitudes GET SNMP desde su gestor de SNMP:

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Ubicación física	Especifique la ubicación física del cortafuegos. Cuando se genera un log o trap, esta información le permite identificar (en un gestor de SNMP) el cortafuegos que ha generado la notificación.
Contacto	Introduzca el nombre o la dirección de correo electrónico de la persona responsable del mantenimiento del cortafuegos Este ajuste se indica en la MIB de información del sistema estándar.
Utilizar definiciones de traps específicas	Esta opción está seleccionada de manera predeterminada, lo que significa que el cortafuegos usa un OID exclusivo para cada trap SNMP en función del tipo de evento. Si quita esta opción, todos los traps tendrán el mismo OID.
versión	Seleccione la versión de SNMP: **V2c** (predeterminado) o **V3**. Su selección controla los campos restantes que muestra el cuadro de diálogo.
Para SNMP V2c	
Cadena de comunidad SNMP	Introduzca la cadena de comunidad, que identifica a una *comunidad* SNMP de gestores SNMP y dispositivos supervisados, además de servir como contraseña para autenticar a los miembros de la comunidad entre sí cuando intercambian mensajes get (solicitud de estadísticas) y trap SNMP. Esta cadena puede tener hasta 127 caracteres, admite todos los caracteres y distingue entre mayúsculas y minúsculas. *No utilice la cadena de comunidad predeterminada public (pública). Dado que los mensajes SNMP contienen cadenas de comunidad en texto sin cifrar, tenga en cuenta los requisitos de seguridad de su red cuando defina la pertenencia a la comunidad (acceso de administradores).*
Para SNMP V3	
Nombre / Vista	Puede asignar un grupo de una o más vistas al usuario de un gestor de SNMP para controlar qué objetos MIB (estadísticas) del cortafuegos puede obtener el usuario. Cada vista es un 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. Por ejemplo, si el **OID** es 1.3.6.1, la **Option (Opción)** coincidente está fijada en **include (incluir)** y **Mask (Máscara)** es 0xf0, los objetos que solicite el usuario deberán tener OID que coincidan con los primeros cuatro nodos (f = 1111) de 1.3.6.1. Los objetos no necesitan coincidir con los nodos restantes. En este ejemplo, 1.3.6.1.2 coincide con la máscara y 1.4.6.1.2 no. Para cada grupo de vistas, haga clic en **Add (Añadir)**, introduzca un nombre en **Name (nombre)** para el grupo y configure lo siguiente en cada vista que seleccione **Add (Añadir)** al grupo: • **View (Ver)**: especifique un nombre para una vista. El nombre puede tener hasta 31 caracteres que pueden ser alfanuméricos, puntos, guiones bajos o guiones. • **OID**: Especifique el OID del MIB.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• **Option (Opción)**: seleccione la lógica de coincidencia que se aplica al MIB. • **Mask (Máscara)**: especifique la máscara en formato hexadecimal. *Para proporcionar acceso a toda la información de gestión, use el OID de máximo nivel 1.3.6.1, defina la Mask (Máscara) en 0xf0 y configure la Option (Opción) de coincidencia en include (incluir).*
Usuarios	Las cuentas de usuario SNMP proporcionan autenticación, privacidad y control de acceso cuando los cortafuegos reenvían traps y los gestores SNMP obtienen estadísticas de cortafuegos. Para cada usuario, haga clic en **Add (Añadir)** y configure los siguientes ajustes: • **Users (Usuarios)**: especifique un nombre de usuario para identificar una cuenta de usuario de SNMP. El nombre de usuario que configure en el cortafuegos debe tener el mismo nombre de usuario configurado en el gestor SNMP. El nombre de usuario puede tener hasta 31 caracteres. • **View (Ver)**: asigne un grupo de vistas al usuario. • **Auth Password (Contraseña de autenticación)**: especifique la contraseña de autenticación del usuario. El cortafuegos usa la contraseña para autenticar el gestor SNMP cuando se reenvían traps y se responde a solicitudes de estadísticas. El cortafuegos usa el algoritmo de hash seguro (SHA-1 160) para cifrar la contraseña. La contraseña debe tener entre 8 y 256 caracteres y todos están permitidos. • **Priv Password (Contraseña priv)**: especifique la contraseña de privacidad del usuario. El cortafuegos usa la contraseña y el estándar de cifrado avanzado (AES-128) para cifrar traps SNMP y respuestas a solicitudes de estadísticas. La contraseña debe tener entre 8 y 256 caracteres y todos están permitidos.

© 2020 Palo Alto Networks, Inc.

Device > Setup > HSM

Seleccione **Device** > **Setup** > **HSM** (Dispositivo > Configuración > HSM) para configurar un módulo de seguridad de hardware (Hardware Security Module, HSM) y para ver el estado del HSM.

¿Qué está buscando?	Consulte:
¿Cuál es el propósito de un módulo de seguridad de hardware (HSM) y dónde puedo encontrar procedimientos detallados de configuración?	Claves seguras con un módulo de seguridad de hardware
Configurar:	Ajustes del proveedor del módulo de seguridad de hardware
	Autenticación HSM
Realice las operaciones de seguridad de hardware	Operaciones de seguridad de hardware
¿Cómo veo el estado de HSM?	Configuración y estado del proveedor del módulo de seguridad de hardware
	Estado de módulo de seguridad de hardware

Ajustes del proveedor del módulo de seguridad de hardware

Para configurar un módulo de seguridad de hardware (Hardware Security Module, HSM) en el cortafuegos, edite la configuración del Proveedor de módulo de seguridad de hardware:

Ajustes del proveedor del módulo de seguridad de hardware	Description (Descripción)
Proveedor configurado	Seleccione el proveedor del HSM: • **None (Ninguno)** (predeterminado): el cortafuegos no se conecta a ningún HSM. • **SafeNet Network HSM** • **nCipher nShield Connect** *La versión de servidor de HSM debe ser compatible con la* versión de cliente de HSM *en el cortafuegos.*
Nombre de módulo	Añada un nombre de módulo para el HSM. Puede ser cualquier cadena ASCII con una longitud de hasta 31 caracteres. Añada hasta 16 nombres de módulo si realiza configuraciones independientes o de HSM SafeNet de alta disponibilidad.

© 2020 Palo Alto Networks, Inc.

Ajustes del proveedor del módulo de seguridad de hardware	Description (Descripción)
Server Address (Dirección del servidor)	Especifique una dirección IPv4 para cualquier módulo HSM que configure.
High Availability (Solo SafeNet Network)	(Opcional) Seleccione esta opción si está definiendo módulos HSM SafeNet en una configuración de alta disponibilidad. Debe configurar el nombre del módulo y la dirección del servidor para cada módulo HSM.
Reintento de recuperación automática (Solo SafeNet Network)	Especifique el número de intentos que debe realizar el cortafuegos para recuperar la conexión con HSM antes de pasar a otro HSM en una configuración de HA del HSM (el intervalo es 0 a 500; el valor predeterminado es 0).
Nombre de grupo de alta disponibilidad (Solo SafeNet Network)	Especifique un nombre de grupo que se debe utilizar para el grupo de HA del HSM. Este nombre lo utiliza el cortafuegos de forma interna. Puede ser cualquier cadena ASCII con una longitud de hasta 31 caracteres.
Remove Filesystem Address (Eliminar dirección del sistema de archivos remoto) Solo nCipher nShield Connect	Configure la dirección IPv4 del sistema de archivos remoto utilizado en la configuración del HSM de nCipher nShield Connect.

Autenticación HSM

Seleccione **Setup Hardware Security Module (Configurar módulo de seguridad de hardware)** y realice estos ajutes para autenticar el cortafuegos en el HSM.

Autenticación de módulo de HSM	
Nombre de servidor	Seleccione un nombre de servidor HSM en el menú desplegable.
Contraseña de administrador	Introduzca la contraseña del administrador de HSM para autenticar el cortafuegos en el HSM.

Operaciones de seguridad de hardware

Para realizar una operación en el Modulo de seguridad de hardware (Hardware Security Module, HSM) o el cortafuegos conectado al HSM, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **HSM** y seleccione una de las siguientes opciones de seguridad de hardware:

Operaciones de seguridad de hardware	
Configurar módulo de seguridad de hardware	Configura el cortafuegos para autenticarlo con un HSM.

© 2020 Palo Alto Networks, Inc.

Operaciones de seguridad de hardware	
Mostrar información detallada	Muestra información sobre servidores de HSM, estado de alta disponibilidad de HSM y hardware de HSM.
Sincronizar con sistemas de archivos remotos (solo HSM de nCipher nShield Connect)	Sincroniza los datos clave desde el sistema de archivos remotos HSM de nShield Connect al cortafuegos.
Restaurar configuración	Elimina todas las conexiones de HSM del cortafuegos. Debe repetir todos los procedimientos de autenticación tras reiniciar la configuración de HSM.
Seleccionar la versión de cliente de HSM (solo HSM de SafeNet Network)	Le permite seleccionar la versión de software que se ejecuta en el cliente de HSM (el cortafuegos). La versión de cliente de HSM debe ser compatible con la versión de servidor de HSM. Consulte la documentación del proveedor de HSM para conocer la matriz de compatibilidad de versiones entre servidores y clientes.

Configuración y estado del proveedor del módulo de seguridad de hardware

La sección Proveedor de módulo de seguridad de hardware muestra los valores de configuración y el estado de conectividad del HSM.

Estado del proveedor del módulo de seguridad de hardware	
Proveedor configurado	Seleccione el proveedor del HSM configurado en el cortafuegos: • **ninguno** • **SafeNet Network HSM** • **nCipher nShield Connect**
High Availability	(Solo SafeNet Network) Si se selecciona, se configura la alta disponibilidad del HSM.
Nombre de grupo de alta disponibilidad	(Solo SafeNet Network) Nombre de grupo configurado en el cortafuegos para la alta disponibilidad del HSM.
Dirección de origen de cortafuegos	Dirección del puerto utilizado para el servicio HSM. De forma predeterminada, se trata de la dirección del puerto de gestión. Sin embargo, se puede especificar como un puerto diferente a través de la opción Services Route Configuration (Configuración de ruta de servicios) en **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)**.
Clave maestra asegurada por HSM	Si se activa, la clave maestra se asegura en el HSM.
estado	Se muestra en verde si el cortafuegos está conectado y autenticado en el HSM, y en rojo si el cortafuegos no está autenticado o si la conectividad de red del HSM está inactiva.

© 2020 Palo Alto Networks, Inc.

Estado del proveedor del módulo de seguridad de hardware	
	También puede consultar Estado de módulo de seguridad de hardware para obtener más detalles sobre la conexión del HSM.

Estado de módulo de seguridad de hardware

El estado del módulo de seguridad de hardware incluye la siguiente información sobre los HSM que se han autenticado correctamente. La pantalla mostrará opciones diferentes dependiendo el proveedor HSM configurado (SafeNet o nCipher).

Estado de módulo de seguridad de hardware	
SafeNet Network HSM	• **Serial Number (Número de serie)**: se muestra el número de serie de la partición del HSM si esta se ha autenticado correctamente. • **Partition (Partición)**: nombre de la partición del HSM que se asignó al cortafuegos. • **Module State (Estado de módulo)**: estado de funcionamiento actual del HSM. Siempre tiene el valor **Authenticated (Autenticado)** si el HSM se muestra en esta tabla.
nCipher nShield Connect	• **Name (Nombre)**: nombre del servidor del HSM. • **IP address (Dirección IP)**: dirección IP que se asignó al HSM en el cortafuegos. • **Module State (Estado de módulo)**: estado de funcionamiento actual del HSM. Este ajuste muestra **Authenticated (Autenticado)** si el cortafuegos se autenticó correctamente en el HSM y muestra **Not Authenticated (No autenticado)** si la autenticación falló.

© 2020 Palo Alto Networks, Inc.

Device > Setup > Services

Los temas siguientes describen la configuración de servicios de sistemas globales y virtuales en el cortafuegos:

- Configurar servicios para sistemas globales y virtuales
- Configuración de servicios globales
- Soporte IPv4 e IPv6 para la configuración de la ruta de servicio
- Ruta de servicio de destino

Configurar servicios para sistemas globales y virtuales

En un cortafuegos donde hay múltiples sistemas virtuales habilitados, seleccione **Services (Servicios)** para mostrar las pestañas **Global** y **Virtual Systems (Sistemas virtuales)** donde define los servicios que el cortafuegos o sus sistemas virtuales, respectivamente, usan para operar eficientemente. (Si el cortafuegos es un único sistema virtual o si hay varios sistemas virtuales deshabilitados, la pestaña **Virtual Systems (Sistemas virtuales)** no se muestra.

Seleccione **Global** para definir servicios para todo el cortafuegos. Estos ajustes también se usan como los valores predeterminados para sistemas virtuales que no tienen un ajuste personalizado para un servicio.

- Edite **Services (Servicios)**para definir las direcciones IP de destino de los servidores DNS, el servidor de actualización y el servidor proxy. Utilice la pestaña **NTP** específica para configurar los ajustes del protocolo de tiempo de red (Network Time Protocol, NTP). Consulte la tabla 12 para la descripción de campos de las opciones de Servicios disponibles.
- En la sección **Service Features (Características de servicios)**, haga clic en **Service Route Configuration (Ajustes de Service Route Configuration)** para especificar cómo se comunicará el cortafuegos con otros dispositivos o servidores para servicios como DNS, correo electrónico, LDAP, RADIUS, syslog y mucho más. Hay dos formas de configurar rutas de servicio globales:
  - La opción **Use Management Interface for all (Utilizar interfaz de gestión para todos)** forzará todas las comunicaciones de servicios de cortafuegos con servidores externos a través de la interfaz de gestión (management interface, MGT). Si selecciona esta opción, deberá configurar la interfaz de gestión para permitir las comunicaciones entre el cortafuegos y los servidores/dispositivos que proporcionan servicios. Para configurar la interfaz MGT, seleccione Device > Setup > Management y edite los ajustes.
  - La opción **Customize (Personalizar)** le ofrece un control granular sobre la comunicación del servicio mediante la configuración de una interfaz de origen y una dirección IP específicas que el servicio usará como interfaz de destino y dirección IP de destino en su respuesta. (Por ejemplo, puede configurar una IP/interfaz de origen específica para toda la comunicación por correo electrónico entre el cortafuegos y un servidor de correo electrónico y utilizar una interfaz/IP de origen diferente para Palo Alto Networks Services.) Seleccione los servicios que quiere personalizar para que tengan la misma configuración y haga clic en **Set Selected Service Routes (Establecer rutas de servicio seleccionadas)**. Estos servicios se enumeran en la tabla 13, que indica si se puede configurar un servicio para el cortafuegos **Global** o los **Virtual Systems (Sistemas virtuales)** y si el servicio es compatible con direcciones de origen IPv4 o IPv6.

La pestaña **Destination (Destino)** es otra función de ruta de servicio global que puede personalizar. Esta pestaña se muestra en la ventana Configuración de ruta de servicios y se describe en Ruta de servicio de destino.

Use la pestaña **Virtual Systems (Sistema virtuales)** para especificar rutas de servicios para un único sistema virtual. Seleccione una ubicación (sistema virtual) y haga clic en **Service Route Configuration (Configuración de ruta de servicios)**. Seleccione **Inherit Global Service Route Configuration (Heredar configuración de ruta de servicios globales)** o **Customize (Personalizar)** rutas de servicio para un sistema virtual. Si elige

© 2020 Palo Alto Networks, Inc.

personalizar configuraciones, seleccione **IPv4** o **IPv6**. Seleccione los servicios que quiere personalizar para que tengan la misma configuración y haga clic en **Set Selected Service Routes (Establecer rutas de servicio seleccionadas)**. Consulte en la tabla 13 los servicios que se pueden personalizar.

Para controlar y redirigir solicitudes de DNS entre sistemas virtuales específicos, puede usar un Proxy DNS y un perfil de servidor DNS.

Configuración de servicios globales

- Device > Setup > Services

Para controlar y redirigir solicitudes de DNS entre sistemas virtuales específicos, puede usar un Proxy DNS y un perfil de servidor DNS.

Configuración de servicios globales	Description (Descripción)
Services	
Actualizar servidor	Representa la dirección IP o el nombre de host del servidor utilizado para descargar actualizaciones de Palo Alto Networks. El valor actual es **updates.paloaltonetworks.com**. No cambie esta configuración a menos que se lo indique la asistencia técnica.
Verificar identidad del servidor de actualización	Si habilita esta opción, el cortafuegos o Panorama comprobarán que el servidor desde el que se descarga el software o el paquete de contenidos cuenta con un certificado SSL firmado por una autoridad fiable. Esta opción añade un nivel de seguridad adicional para la comunicación entre el cortafuegos o los servidores de Panorama y el servidor de actualización. *Verifique la identidad del servidor de actualización para validar que el servidor tenga un certificado SSL firmado por una autoridad de confianza.*
Configuración DNS	Seleccione el tipo de servicio DNS (**Servers [Servidores]** o **DNS Proxy Object [Objeto proxy DNS]**) para todas las consultas DNS que inicia el cortafuegos para respaldar objetos con dirección de FQDN, la creación de logs y la gestión del cortafuegos. Las opciones incluyen las siguientes: • Servidores DNS principal y secundario para proporcionar resolución de nombres de dominio. • Un proxy DNS configurado en el cortafuegos es otra opción para configurar los servidores DNS. Si habilita un proxy de DNS, debe habilitar **Caché** y **Respuestas de caché de EDNS** (**Red** > **Proxy de DNS** > **Avanzado**).
Servidor DNS principal	Introduzca la dirección IP del servidor DNS principal para las consultas DNS del cortafuegos. Por ejemplo, para buscar el servidor de actualización, para resolver entradas DNS en logs o resolver objetos con direcciones basadas en FQDN.
Servidor DNS secundario	(Opcional) Introduzca la dirección IP de un servidor DNS secundario que deberá utilizarse si el servidor principal no está disponible.

© 2020 Palo Alto Networks, Inc.

Configuración de servicios globales	Description (Descripción)
Tiempo mínimo de actualización de FQDN (seg.)	Establezca un límite para la rapidez con la que el cortafuegos actualizará los FQDN que recibe de un DNS. El cortafuegos actualiza un FQDN en función del TTL del FQDN, siempre que el TTL sea mayor o igual que este **tiempo mínimo de actualización de FQDN** (en segundos). Si el TTL es menor que el tiempo mínimo de actualización de FQDN, el cortafuegos actualizará el FQDN en función de este tiempo mínimo de actualización de FQDN (es decir, el cortafuegos no reflejará los TTL más rápido que este ajuste). El temporizador se inicia cuando el cortafuegos recibe una respuesta DNS del servidor DNS o el objeto proxy DNS que resuelve el FQDN (el intervalo es de 0 a 14 400, el valor predeterminado es 30). Un ajuste de 0 significa que el cortafuegos actualizará el FQDN en función del valor TTL en el DNS y no aplicará un tiempo mínimo de actualización de FQDN. *Si el TTL para el FQDN en el DNS es corto, pero las resoluciones de FQDN no cambian con tanta frecuencia como el intervalo de tiempo del TTL, por lo que no requiere una actualización más rápida, debe configurar un tiempo mínimo de actualización de FQDN para evitar intentos innecesarios de actualización de FQDN.*
Tiempo de espera de entrada obsoleta de FQDN (min.)	Especifique el periodo de tiempo (en minutos) en que el cortafuegos continuará usando resoluciones de FQDN obsoletas en caso de un fallo de la red o un servidor DNS inaccesible, durante el cual el FQDN no se actualizará (el intervalo es de 0 a 10 080, el valor predeterminado es 1440). Un valor de 0 significa que el cortafuegos no continúa usando una entrada obsoleta. Si el servidor DNS aún es inaccesible al final del tiempo de espera de estado, la entrada de FQDN no se resolverá (se eliminan las resoluciones obsoletas). *Asegúrese de que el valor de FQDN Stale Entry Timeout (Tiempo de espera de entrada obsoleta de FQDN) sea lo suficientemente bajo como para no permitir el reenvío de tráfico incorrecto (lo cual supone un riesgo para la seguridad), pero lo suficientemente extenso para permitir la continuidad del tráfico sin causar una interrupción no planificada de la red.*
Sección Servidor proxy	
Servidor	Si el cortafuegos necesita utilizar un servidor proxy para acceder a los servicios de actualización de Palo Alto Networks, introduzca la dirección IP o el nombre de host del servidor proxy.
Puerto	Introduzca el puerto para el servidor proxy.
Usuario	Introduzca el nombre de usuario para cuando el administrador ingrese al servidor proxy.
Contraseña/ Confirmar contraseña	Introduzca y confirme la contraseña para que el administrador acceda al servidor proxy.
NTP	

© 2020 Palo Alto Networks, Inc.

Configuración de servicios globales	Description (Descripción)
Dirección de servidor NTP	Introduzca la dirección IP o el nombre de host del servidor NTP que utilizará para sincronizar el reloj del cortafuegos. De forma opcional, puede introducir la dirección IP o nombre de host de un segundo servidor NTP para sincronizar el reloj del cortafuegos si el servidor principal no está disponible. *Cuando un servidor NTP mantiene todos los relojes del cortafuegos de la red sincronizados, las tareas programadas se ejecutan según lo previsto y las marcas de tiempo pueden ayudar a identificar las causas raíces de los problemas que involucran a varios dispositivos. Configure un servidor NTP primario y secundario en caso de que el servidor NTP primario se vuelva inaccesible.*

Tipo de autenticación	Puede activar el cortafuegos para autenticar las actualizaciones de hora desde un servidor NTP. Para cada servidor NTP, seleccione el tipo de autenticación que debe utilizar el cortafuegos:
	• **None (Ninguna)** (predeterminado): seleccione esta opción para desactivar la autenticación de NTP.
	• **Symmetric Key (Clave simétrica)**: seleccione esta opción para que el cortafuegos utilice intercambio de clave simétrica (secretos compartidos) para autenticar las actualizaciones de hora del servidor NTP. Si selecciona la clave simétrica, especifique los siguientes valores:
	  • **Key ID (ID de clave)**: introduzca el ID de clave (1--65534).
	  • **Algorithm (Algoritmo)**: seleccione el algoritmo MD5 o SHA1 para la autenticación de NTP.
	  • **Authentication Key/Confirm Authentication Key (Clave de autenticación/ Confirme clave de autenticación)**: introduzca y confirme la clave de autenticación del algoritmo de autenticación.
	• **Autokey (Clave automática)**: seleccione esta opción para que el cortafuegos utilice la clave automática (criptografía de clave pública) para autenticar las actualizaciones de hora del servidor NTP.
	
	Habilite la autenticación de servidor NTP, de manera que el servidor NTP apruebe al cliente y proporcione actualizaciones sincronizadas.

Soporte IPv4 e IPv6 para la configuración de la ruta de servicio

La siguiente tabla muestra la compatibilidad con IPv4 e IPv6 de las configuraciones de rutas de servicio en sistemas globales y virtuales.

Configuración de Service Route Configuration	Global		Sistema virtual	
	IPv4	IPv6	IPv4	IPv6
AutoFocus: servidor de AutoFocus™.	✓	—	—	—

© 2020 Palo Alto Networks, Inc.

Configuración de Service Route Configuration	Global		Sistema virtual	
	IPv4	IPv6	IPv4	IPv6
CRL Status (**Estado de CRL):** servidor de lista de revocación de certificado (CRL).	✓	✓	—	—
DDNS: servicio DNS dinámico.	✓	✓	✓	✓
Panorama pushed updates (Actualizaciones enviadas de Panorama): actualizaciones de contenido y software implementadas desde Panorama™.	✓	✓	—	—
DNS: servidor de sistema de nombres de dominio. * Para sistemas virtuales, el DNS se realiza en el perfil de servidor de DNS.	✓	✓	✓ *	✓ *
External Dynamic Lists (Listas dinámicas externas): actualizaciones de listas dinámicas externas.	✓	✓	—	—
Email (Correo electrónico): servidor de correo electrónico.	✓	✓	✓	✓
HSM: servidor de módulo de seguridad de hardware.	✓	—	—	✓
HTTP: reenvío de HTTP.	✓	✓	✓	✓
Kerberos: servidor de autenticación Kerberos.	✓	—	✓	✓
LDAP: servidor de protocolo ligero de acceso a directorios.	✓	✓	✓	✓
MDM: servidor de gestión de dispositivos móviles.	✓	✓	—	—
Multi-Factor Authentication (Autenticación de múltiples factores): servidor de autenticación de múltiples factores (Multi-factor authentication, MFA).	✓	✓	✓	✓
NetFlow: recopilador NetFlow de estadísticas de tráfico de red.	✓	✓	✓	✓
NTP: servidor de protocolo de tiempo de red.	✓	✓	—	—
Palo Alto Networks Services (Servicios de Palo Alto Networks): actualizaciones de Palo Alto	✓	—	—	—

© 2020 Palo Alto Networks, Inc.

Configuración de Service Route Configuration	Global		Sistema virtual	
	IPv4	IPv6	IPv4	IPv6
Networks® y el servidor público de WildFire®. Esta es también la ruta de servicio para enviar los datos de telemetría a Palo Alto Networks.				
Panorama: servidor de gestión de Panorama.	✓	✓	—	—
Panorama Log Forwarding (Reenvío de logs de Panorama) (solo cortafuegos serie PA-5200): reenvío de logs desde el cortafuegos a los recopiladores de logs.	✓	✓	—	—
Proxy: servidor que actúa como proxy para el cortafuegos.	✓	✓	—	—
RADIUS: servidor de servicio de autenticación remota telefónica de usuario.	✓	✓	✓	✓
SCEP: protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP) para solicitar y distribuir certificados de clientes.	✓	✓	✓	—
SNMP Trap (Trap SNMP): servidor trap de protocolo simple de administración de redes.	✓	—	✓	—
Syslog: servidor para registro de mensajes de sistema.	✓	✓	✓	✓
TACACS+: servidor del sistema mejorado de control de acceso mediante control del acceso desde terminales (Terminal Access Controller Access-Control System Plus) para servicios de autenticación, autorización y contabilidad (Authentication, Authorization, and Accounting, AAA).	✓	✓	✓	✓
UID Agent (Agente UID): servidor de agente de User-ID.	✓	✓	—	✓
URL Updates (Actualizaciones de URL): servidor de actualizaciones de Localizador de recursos uniforme (Uniform Resource Locator, URL).	✓	✓	—	—
VM Monitor (Supervisor de VM): supervisa la información de la máquina virtual cuando habilita esta opción Device (Dispositivo) > VM Information Sources (Orígenes de información de VM).	✓	✓	✓	✓

© 2020 Palo Alto Networks, Inc.

Configuración de Service Route Configuration	Global		Sistema virtual	
	IPv4	IPv6	IPv4	IPv6
Los cortafuegos serie VM en implementaciones de nube pública que supervisan máquinas virtuales deben utilizar la interfaz MGT. No puede utilizar una interfaz de plano de datos como una ruta de servicio.				
Wildfire Private (Servidor privado de WildFire): servidor privado de WildFire de Palo Alto Networks.	✓	—	—	—

Cuando personalice una ruta de servicio **Global**, seleccione **Service Route Configuration (Configuración de ruta de servicios)** y, en la pestaña **IPv4** o **IPv6**, seleccione un servicio de la lista de servicios disponibles; también puede seleccionar múltiples servicios y seleccionar la opción **Set Selected Service Routes (Establecer rutas de servicio seleccionadas)** para configurar múltiples rutas de servicio al mismo tiempo. Para limitar las selecciones en la lista desplegable **Source Address (Dirección de origen)**, seleccione una **Source Interface (Interfaz de origen)** y una **Source Address (Dirección de origen)** (para esa interfaz). Una interfaz de origen definida en **Any (Cualquiera)** permite seleccionar una dirección de origen desde cualquiera de las interfaces disponibles. La dirección de origen muestra la dirección IPv4 o IPv6 asignada a la interfaz seleccionada; la dirección IP seleccionada será el origen del tráfico de servicio. Puede seleccionar **Use default (Utilizar predeterminado)** si desea que el cortafuegos utilice la interfaz de gestión para la ruta de servicio; sin embargo, si la dirección IP de destino del paquete coincide con la dirección IP de destino configurada, la dirección IP de origen se establecerá como Source Address (Dirección de origen) configurada para la dirección de Destination (Destino). No tiene que definir la dirección de destino porque el destino se configura cuando configura cada servicio. Por ejemplo, cuando define sus servidores DNS (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]**), establecerá el destino de las consultas DNS. Puede especificar direcciones IPv4 y IPv6 para un servicio.

Una manera alternativa de personalizar una ruta de servicio **Global** es seleccionar **Service Route Configuration (Configuración de ruta de servicios)** y seleccionar **Destination (Destino)**. Especifique una dirección IP de **Destination (Destino)** con la que se compara un paquete entrante. Si la dirección de destino del paquete coincide con la dirección IP de destino configurada, la dirección IP de origen se define con la dirección de origen configurada para el destino. Para limitar las selecciones en la lista desplegable **Source Address (Dirección de origen)**, seleccione una **Source Interface (Interfaz de origen)** y una **Source Address (Dirección de origen)** (para esa interfaz). Una interfaz de origen definida en **Any (Cualquiera)** permite seleccionar una dirección de origen desde cualquiera de las interfaces disponibles. La interfaz de origen de **MGT (Gestión)** causa que el cortafuegos utilice la interfaz de gestión en la ruta de servicio.

Cuando configura rutas de servicio para un **Virtual System (Sistema virtual)**, seleccionar la opción **Inherit Global Service Route Configuration (Heredar configuración de ruta de servicios globales)** significa que todos los servicios del sistema virtual heredarán la configuración global de ruta de servicios. En cambio, puede seleccionar **Customize (Personalizar)**, seleccione **IPv4** o **IPv6**, y seleccione un servicio; también puede seleccionar múltiples servicios y **Set Selected Service Routes (Establecer rutas de servicio seleccionadas)**. La **Source Interface (Interfaz de origen)** tiene las siguientes tres opciones:

- **Inherit Global Setting (Heredar configuración global)**: los servicios seleccionados heredan la configuración global de estos servicios.
- **Any (Cualquiera)**: Permite seleccionar una dirección de origen desde cualquiera de las interfaces disponibles (interfaces en el sistema virtual específico).

© 2020 Palo Alto Networks, Inc.

- **An interface from the drop-down (Una interfaz de la lista desplegable):** limita la lista desplegable de **Source Address (Dirección de origen)** a las direcciones IP de esta interfaz.

Para **Source Address (Dirección de origen)**, seleccione una dirección del menú desplegable. Para los servicios seleccionados, las respuestas del servidor se envían a esta dirección de origen.

Ruta de servicio de destino

- Device > Setup > Services > Global

En la pestaña **Global**, si hace clic en **Service Route Configuration (Configuración de ruta de servicios)** y luego en **Customize (Personalizar)**, aparece la pestaña **Destination (Destino)**. Las rutas de servicio de destino están disponibles solo en la pestaña **Global** (no la pestaña **Virtual Systems [Sistemas virtuales]**), de modo que la ruta de servicio de un sistema virtual individual no puede cancelar entradas de tabla de rutas que no están asociadas a un sistema virtual.

Se puede usar una ruta de servicio de destino para añadir una redirección personalizada de un servicio compatible con la lista de servicios **Customize (Personalizar)**. Una ruta de servicio de destino es un modo de configurar la ruta para cancelar la tabla de rutas de base de información de reenvío (FIB). Cualquier configuración en las rutas de servicio de destino cancelan las entradas de tabla de rutas. Pueden estar relacionadas o no relacionadas con cualquier servicio.

La pestaña **Destination (Destino)** sirve para los siguientes casos de uso:

- Cuando un servicio no tiene una ruta de servicio de aplicaciones.
- Dentro de un único sistema virtual, cuando quiere usar varios enrutadores virtuales o una combinación de enrutador virtual y puerto de gestión.

Configuración de ruta de servicio de destino	Description (Descripción)
IP Destino	Introduzca la dirección IP de **Destination (Destino)**. Un paquete entrante con una dirección de destino que coincide con esta dirección utilizará la dirección de origen que especificó para esta ruta de servicio como su origen.
Interfaz de origen	Para limitar la lista desplegable de Source Address (Dirección de origen), seleccione una **Source Interface (Interfaz de origen)**. Si selecciona **Any (Cualquiera)**, todas las direcciones IP en todas las interfaces estarán disponibles en la lista desplegable Source Address (Dirección de origen). Si selecciona **MGT (Gestión)**, el cortafuegos utilizará la interfaz MGT (Gestión) en la ruta de servicio.
Dirección de origen	Seleccione la **Source Address (Dirección de origen)** para la ruta de servicio; esta dirección se utilizará para los paquetes que regresen del destino. No necesita introducir la subred de la dirección de destino.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Configuración > Interfaces

Utilice esta página para configurar los ajustes de conexión, los servicios permitidos y el acceso administrativo para la interfaz de administración (MGT) en todos los modelos de cortafuegos y para las interfaces auxiliares (AUX-1 y AUX-2) en los cortafuegos de la serie PA-5200.

Palo Alto Networks recomienda que especifique siempre la dirección IP y la máscara de red (para IPv4) o la longitud de prefijo (para IPv6) y la puerta de enlace predeterminada para cada interfaz. Si omite alguna de estas configuraciones para la interfaz MGT (como la puerta de enlace predeterminada), puede acceder al cortafuegos sólo a través del puerto de la consola para los cambios de configuración futuros.

Para configurar la interfaz MGT en el dispositivo M-500 o en el dispositivo virtual Panorama, consulte Panorama > Setup (Configuración) > Interfaces*.*

*Puede utilizar una interfaz de bucle invertido como alternativa a la interfaz MGT para la gestión de cortafuegos (*Network > Interfaces > Loopback*).*

Elemento	Description (Descripción)

Tipo
(Solo interfaz MGT)
	Seleccione una opción:
	• **Static**: requiere que ingrese la **IP Address (Dirección IP)** (IPv4), la máscara de red en **Netmask (Máscara de red)** (IPv4) y la puerta de enlace predeterminada en **Default Gateway (Puerta de enlace predeterminada)** de manera manual.
	• **DHCP Client (Cliente DHCP)**: configura la interfaz MGT como un cliente DHCP de modo que el cortafuegos pueda enviar mensajes de solicitud o descubrimiento DHCP para encontrar un servidor DHCP. El servidor responde brindando una dirección IP (OP v4), la máscara de red (IPv4) y la puerta de enlace predeterminada para la interfaz MGT. DHCP en la interfaz MGT está desactivo de manera predeterminada para el cortafuegos VM-Series (excepto por el cortafuegos VM-Series en AWS y Azure). Si selecciona **DHCP Client (Cliente DHCP)**, de forma opcional seleccione una o ambas de las siguientes opciones de cliente:
	  • **Send Hostname (Enviar nombre de host)**: provoca que la interfaz de MGT envíe su nombre de host al servidor DHCP como parte de la opción 12 de DHCP.
	  • **Send Client ID (Enviar ID de cliente)**: provoca que la interfaz MGT envíe su identificador de cliente como parte de la opción 61 de DHCP.
	Si selecciona **DHCP Client (Cliente DHCP)**, opcionalmente haga clic en **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)** para ver el estado de interfaz de la IP dinámica:
	• Interface: indica la interfaz MGT.
	• IP Address: dirección IP de la interfaz MGT.
	• Netmask: máscara de subred para la dirección IP, que indica cuáles bits son red o subred y cuáles son host.
	• Gateway: puerta de enlace predeterminada para el tráfico que deja la interfaz MGT.
	• Primary/Secondary NTP: dirección IP de hasta dos servidor NTP que facilitan la interfaz MGT. Si el servidor DHCP brinda direcciones de servidor NTP, el cortafuegos solo las considera si no configuró

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	manualmente las direcciones de servidor NTP. Si configuró manualmente las direcciones del servidor NTP, el cortafuegos no las sobrescribe con aquellas del servidor DHCP. • Lease Time: número de días, horas, minutos y segundos que la dirección IP de DHCP está asignada. • Expiry Time: año/mes/día, horas/minutos/segundos, y la zona horaria que indican cuándo vencerá la concesión de DHCP. • DHCP Server: dirección IP del servidor DHCP que responde a la interfaz MGT del cliente DHCP. • Domain: nombre del dominio al cual pertenece la interfaz MGT. • DNS Server: dirección IP de hasta dos servidores DNS que facilitan la interfaz MGT. Si el servidor DHCP brinda direcciones del servidor DNS, el cortafuegos solo las considera si no configuró manualmente las direcciones del servidor DNS. Si configuró manualmente las direcciones del servidor DNS, el cortafuegos no las sobrescribe con aquellas del servidor DHCP. De manera opcional, puede **Renew (Renovar)** la concesión de DHCP en Renew (Renovar) para la direcciones IP asignadas a la interfaz MGT. De lo contrario, cierre la ventana haciendo clic en **Close (Cerrar)**.
Aux 1 / Aux 2 (Solo cortafuegos PA-5200 Series)	Seleccione cualquiera de las siguientes opciones para habilitar una interfaz auxiliar. Estas interfaces proporcionan un rendimiento de 10 Gbps (SFP+) para: • Firewall management traffic (Tráfico de gestión de cortafuegos): debe habilitar los Servicios de red (protocolos) que los administradores utilizarán al acceder a la interfaz web y la CLI para gestionar el cortafuegos. *Habilite HTTPS en lugar de HTTP para la interfaz web y habilite SSH en lugar de Telnet para la CLI.* • High availability (HA) synchronization between firewall peers (Sincronización de alta disponibilidad (HA) entre peers de cortafuegos): después de configurar la interfaz, debe seleccionarla como el Enlace de controlde HA (**Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **General**). • Log forwarding to Panorama (Reenvío de logs a Panorama): debe configurar una ruta de servicio con el servicio **Panorama Log Forwarding (Reenvío de logs de Panorama)** habilitado (Device > Setup > Services).
Dirección IP (IPv4)	Si su red utiliza IPv4, asigne una dirección IPv4 a la interfaz. De forma alternativa, puede asignar la dirección IP de una interfaz de bucle invertido para la gestión de cortafuegos (consulte Network > Interfaces > Loopback). De manera predeterminada, la dirección IP que introduzca es la dirección de origen para el reenvío de logs.
Máscara de red (IPv4)	Si ha asignado una dirección IPv4 a la interfaz, debe introducir también una máscara de red (por ejemplo, 255.255.255.0).
Gateway predeterminada	Si ha asignado una dirección IPv4 a la interfaz, también debe asignar una dirección IPv4 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz).

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
Dirección IPv6/longitud de prefijo	Si su red utiliza IPv6, asigne una dirección IPv6 a la interfaz. Para indicar la máscara de red, introduzca una longitud de prefijo para IPv6 (por ejemplo 2001:400:f00::1/64).
Puerta de enlace IPv6 predeterminada	Si ha asignado una dirección IPv6 a la interfaz, también debe asignar una dirección IPv6 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz).
Velocidad	Configure una tasa de datos y una opción de dúplex para la interfaz. Las opciones incluyen 10 Mbps, 100 Mbps y 1 Gbps con dúplex completo o medio. Utilice el ajuste de negociación automática predeterminado para que el cortafuegos determine la velocidad de interfaz. *Este ajuste debe coincidir con la configuración de los puertos del equipo de red vecino. Para garantizar que los ajustes coinciden, seleccione auto-negotiate si el equipo vecino admite esa opción.*
MTU	Introduzca la unidad máxima de transmisión (MTU, por sus siglas en inglés) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 1500 y el valor predeterminado, 1500).
Servicios de gestión administrativa	• **HTTP**: utilice este servicio para acceder a la interfaz web del cortafuegos. *HTTP usa texto sin formato, lo cual no es tan seguro como HTTPS. Por lo tanto, Palo Alto Networks recomienda habilitar HTTPS en lugar de HTTP para la gestión del tráfico en la interfaz.* • **Telnet**: utilice este servicio para acceder a la CLI del cortafuegos. *Telnet usa texto sin formato, lo cual no es tan seguro como SSH. Por lo tanto, Palo Alto Networks recomienda habilitar SSH en lugar de Telnet para la gestión del tráfico en la interfaz.* • **HTTPS**: utilice este servicio para el acceso seguro a la interfaz web del cortafuegos. • **SSH**: utilice este servicio para el acceso seguro a la CLI del cortafuegos.
Servicios de red	Seleccione los servicios que desea activar en la interfaz: • **HTTP OCSP**: utilice este servicio para configurar el cortafuegos como un respondedor de Protocolo de estado de certificado en línea (OCSP). Para obtener más información, consulte Device > Certificate Management > OCSP Responder. • **Ping**: utilice este servicio para probar la conectividad con los servicios externos. Por ejemplo, puede hacer ping a la interfaz para verificar que puede recibir el softwre PAN-OS y las actualizaciones de contenido del servidor de actualización de Palo Alto Networks. En una implementación de alta disponibilidad (HA), los peers de HA usan el ping para intercambiar información de copias de seguridad de heartbeat.

© 2020 Palo Alto Networks, Inc.

Elemento	Description (Descripción)
	• **SNMP**: utilice este servicio para procesar consultas de estadísticas de cortafuegos desde el gestor SNMP. Para obtener más información, consulte Habilitación de supervisión de SNMP. • **User-ID**: utilice este servicio para habilitar Redistribution (Redistribución) de asignaciones de usuarios entre cortafuegos. • **User-ID Syslog Listener-SSL (SSL de escucha de Syslog de User-ID)**: utilice este servicio para habilitar el agente User-ID™ integrado en PAN-OS para recopilar los mensajes de syslog en SSL. Para obtener más información, consulte Configuración de acceso a servidores supervisados. • **User-ID Syslog Listener-UDP (UDP de escucha de Syslog de User-ID)**: utilice este servicio para habilitar el agente User-ID integrado en PAN-OS para recopilar los mensajes de syslog en UDP. Para obtener más información, consulte Configuración de acceso a servidores supervisados.
Direcciones IP permitidas	Introduzca las direcciones IP desde las que los administradores pueden acceder al cortafuegos a través de la interfaz. Una lista vacía (predeterminada) especifica que el acceso está disponible desde cualquier dirección IP. *No deje la lista en blanco; especifique solo las direcciones IP de los administradores de cortafuegos para evitar el acceso no autorizado.*

© 2020 Palo Alto Networks, Inc.

Dispositivo > Configuración > Telemetría

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 datos que incluyen información sobre aplicaciones, amenazas, estado del dispositivo y DNS pasivo a Palo Alto Networks. Todos los usuarios de Palo Alto Networks se benefician de los datos que cada participante de telemetría comparte, convirtiendo la telemetría en un enfoque impulsado por la comunidad para la prevención de amenazas. Obtenga más información acerca de Telemetría y sus beneficios.

La telemetría es una función de opt-in y, para la mayoría de los datos de telemetría, se puede obtener una vista previa de la información que el cortafuegos recoge. Palo Alto Networks no comparte sus datos de telemetría con otros clientes u organizaciones externas.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Telemetry (Telemetría)** para seleccionar datos de telemetría para compartir con Palo Alto Networks. Los datos de prevención de amenazas y los informes de capturas de paquetes de prevención de amenazas proporcionan a Palo Alto Networks mayor visibilidad en su tráfico de red que otros informes de telemetría.

Configuración de telemetría	Description (Descripción)
Muestra de informa	Haga clic en una muestra de informe ( ) para ver un informe con formato XML en una pestaña independiente. Los datos del ejemplo de informe se basan en la actividad del cortafuegos en las cuatro horas desde que visualizó la muestra del informe por primera vez. El cortafuegos proporciona un informe de muestra solo para informes de Aplicación, Prevención de amenazas, URL e Identificación de tipo de archivo. Un informe puede consistir en varios informes: • **Tipo**: describe el nombre del informe. • **Agregado**: lista los campos de logs que el cortafuegos recoge para el informe (consulte Descripciones de los campos de Syslog para determinar el nombre de los campos tal como aparecen en los logs del cortafuegos). • **Valores**: indica las unidades de medida utilizadas en el informe (por ejemplo, el valor **count (recuento)** para el informe Países atacantes se refiere al número de veces que el cortafuegos detectó un evento de amenaza asociado con un país en particular). Un ejemplo de informe no muestra ninguna entrada si el cortafuegos no encontró ningún tráfico coincidente para el informe. Solo puede generar una nueva muestra del informe cuando reinicie el cortafuegos.
Informes de aplicación (Deshabilitada de forma predeterminada.)	Comparta el número y el tamaño de las aplicaciones conocidas agrupadas por el puerto de destino, las aplicaciones desconocidas agrupadas por el puerto de destino y las aplicaciones desconocidas agrupadas por la dirección IP de destino. El cortafuegos genera estos informes a partir de los logs de tráfico. Cuando está habilitado, el cortafuegos reenvía informes de aplicaciones cada 4 horas.
Informes de prevención de amenazas	Comparta el número de amenazas para cada país de origen y puerto de destino, información del atacante y los objetos de correlación que los eventos

© 2020 Palo Alto Networks, Inc.

Configuración de telemetría	Description (Descripción)
(Deshabilitada de forma predeterminada.)	de amenaza desencadenaron cuando el cortafuegos estaba recopilando datos para estos informes. Cuando está habilitado, el cortafuegos envía los informes de prevención de amenazas cada 4 horas.
Informes de URL (Deshabilitada de forma predeterminada.)	Compartir informes generados a partir de logs de filtrado de URL con las siguientes categorías de URL de PAN-DB: malware, phishing, DNS dinámico, evasión de proxy, contenido sospechoso, estacionado y desconocido (URL que PAN-DB aún no ha categorizado). El servidor de seguridad también envía estadísticas de PAN-DB en el momento en que se recopilaron los datos de los informes de URL. Estas estadísticas incluyen la versión de la base de datos de filtrado de URL en el cortafuegos y la nube de PAN-DB, el número de URL en esas bases de datos y el número de URL que clasificó el cortafuegos. Estas estadísticas se basan en el tiempo que el cortafuegos reenvió los informes de URL. Cuando se habilita, el cortafuegos reenvía informes de URL cada 4 horas.
Informes de identificación de tipo de archivo (Deshabilitada de forma predeterminada.)	Compartir informes sobre los archivos que el cortafuegos permite o bloquea basados en configuraciones de Filtrado de datos y Bloqueo de archivos. Cuando está habilitado, el cortafuegos reenvía los informes de identificación de tipo de archivo cada 4 horas.
Datos de prevención de amenazas (Deshabilitada de forma predeterminada.)	Compartir logs de eventos de amenazas que activaron firmas que Palo Alto Networks está evaluando. La información recopilada puede incluir direcciones IP de origen o de víctima. Habilitar esta opción también permite que firmas no publicadas, que Palo Alto Networks está probando, se ejecuten en segundo plano. Estas firmas no afectan a las reglas de políticas de seguridad ni a los logs de cortafuegos, y no tienen ningún impacto en el rendimiento de su cortafuegos. Cuando está habilitado, el cortafuegos envía los datos de prevención de amenazas cada 5 minutos. Haga clic en **Download Threat Prevention Data (Descargar los datos de prevención de amenazas)** ( ) para descargar un archivo tarball (.tar.gz) con las últimas 100 carpetas de **Threat Prevention Data (Datos de prevención de amenazas)** y **Threat Prevention Packet Captures (Captura de paquetes de prevención de amenazas)** que el cortafuegos remitió a Palo Alto Networks. Si nunca habilitó estas configuraciones o si las habilitó, pero no hay eventos de amenaza que coincidan con las condiciones para estas configuraciones de telemetría, el cortafuegos no genera un archivo y en su lugar devuelve un mensaje de error.
Capturas de paquetes de prevención de amenazas (Deshabilitada de forma predeterminada.)	Comparta las capturas de paquetes (si activó su cortafuegos para tomar capturas de paquetes de amenazas) de los eventos de amenaza que desencadenan las firmas que Palo Alto Networks está evaluando. La información recopilada puede incluir direcciones IP de origen o de víctima. Cuando está habilitado, el cortafuegos envía Capturas de paquetes de prevención de amenazas cada 5 minutos.

© 2020 Palo Alto Networks, Inc.

Configuración de telemetría	Description (Descripción)
	Para habilitar las capturas de paquetes de prevención de amenazas, también debe habilitar los datos de prevención de amenazas.
Estadísticas de uso de producto (Deshabilitada de forma predeterminada.)	Comparte retrocesos de procesos de cortafuegos que han fallado, así como información sobre el estado del cortafuegos. Los retrocesos de procesos describen el historial de ejecución de los procesos fallidos. Las estadísticas de uso del producto también incluyen detalles sobre el modelo de cortafuegos y las versiones de liberación de contenido y de PAN-OS instaladas en el cortafuegos. Para ver la información que el cortafuegos envía como Estadísticas de uso del producto, escriba el siguiente comando CLI operativo: `show system info` Cuando está habilitado, el cortafuegos envía Estadísticas de uso del producto cada 5 minutos.
Monitorización de DNS pasivo (Deshabilitada de forma predeterminada.)	Permite que el cortafuegos actúe como un sensor DNS pasivo y envíe información de DNS a Palo Alto Networks para su análisis. Los datos que comparte a través de la Supervisión de DNS pasivo consiste únicamente en asignaciones de direcciones de dominio a IP. El equipo de investigación de amenazas de Palo Alto Networks utiliza esta información para mejorar la categoría de URL de PAN-DB y la precisión de firmas C2 basadas en DNS, y la detección de malware de WildFire. La supervisión de DNS pasivo es una configuración global que se aplica a todo el tráfico de cortafuegos. Cuando está habilitado, el cortafuegos reenvía los datos de supervisión de DNS pasivo en lotes de 1 MB.
Seleccionar todo	Habilita todos los ajustes de telemetría.
Anular selección	Deshabilita todos los ajustes de telemetría.

© 2020 Palo Alto Networks, Inc.

Device > Setup > Content-ID

Utilice la pestaña **Content-ID (ID de contenido)** para definir la configuración del filtrado de URL, la protección de datos y las páginas contenedoras.

Configuración de ID de contenido	Description (Descripción)
Filtrado de URLs	
Tiempo de espera de caché de URL dinámica	Haga clic en **Editar** e introduzca el tiempo de espera (en horas). Este valor se utiliza en el filtrado de URL dinámica para determinar la cantidad de tiempo que una entrada permanece en la caché después de ser devuelta por el servicio de filtrado de URL. Esta opción únicamente es aplicable al filtrado de URL que utilice la base de datos de BrightCloud. Para obtener más información sobre el filtrado de URL, seleccione Objetos > Perfiles de seguridad > Filtrado de URL.
Tiempo de espera de caché de URL dinámica	Especifique el intervalo que transcurre desde una acción de **Continuar** por parte del usuario hasta el momento en que el usuario debe volver a pulsar el botón de continuación para las URL de la misma categoría (intervalo de 1 a 86 400 minutos; el valor predeterminado es 15).
Tiempo de espera de cancelación de administrador de URL	Especifique el intervalo que transcurre desde que el usuario introduce la contraseña de **Cancelación de Administrador** hasta que el usuario debe volver a introducir la contraseña para las URL de la misma categoría (el intervalo es de 1 a 86 400 minutos; el valor predeterminado es 15).
Retener solicitud de cliente para búsqueda de categoría	Habilite esta opción para especificar que cuando el cortafuegos no pueda encontrar información de categoría para una URL en su caché local, mantenga la solicitud web mientras consulta PAN-DB. *Esta opción está deshabilitada de manera predeterminada. Habilítelo como parte de unas* prácticas recomendadas para el perfil de filtrado de URL.
Tiempo de espera de búsqueda de categoría (segundos)	Especifique la cantidad de tiempo, en segundos, que el cortafuegos intentará buscar la categoría para una URL antes de determinar que la categoría es `no resuelta` (el intervalo es de 1 a 60 segundos; el valor predeterminado es 2).
Tiempo de espera de bloqueo de administrador de URL	Especifique el periodo que un usuario está bloqueado y no puede utilizar la contraseña de cancelación de administrador de URL después de tres intentos incorrectos (el intervalo es de 1 a 86 400 minutos; el valor predeterminado es 30).
Servidor PAN-DB (Necesario para la conexión a un servidor PAN-DB privado)	Especifique la dirección IPv4, dirección IPv6 o FQDN para los servidores PAN-DB privados en su red. Puede añadir hasta 20 entradas. El cortafuegos conecta con la nube PAN-DB pública de manera predeterminada. La solución PAN-DB privada es para empresas que no permiten que los cortafuegos accedan directamente a los servidores de

© 2020 Palo Alto Networks, Inc.

Configuración de ID de contenido	Description (Descripción)
	PAN-DB en la nube pública. Los cortafuegos acceden a los servidores incluidos en esta lista de servidores de PAN-DB para bases de datos de URL, actualizaciones de URL y búsquedas de URL para categorizar páginas web.
Cancelación de administrador de URL	
Configuración de la cancelación de administrador de URL	Para cada sistema virtual que quiera configurar para la cancelación de administradores de URL, **añada** y especifique la configuración que se aplica cuando un perfil de filtrado de URL bloquea una página y se especifica la acción **Cancelar**. Para obtener más información, consulte Objetos > Perfiles de seguridad > Filtrado de URL. • **Ubicación**: (solo para cortafuegos de sistemas virtuales múltiples) seleccione el sistema virtual en el menú desplegable. • **Password/Confirm Password (Contraseña/Confirmar contraseña)**: Introduzca la contraseña que el usuario debe introducir para cancelar la página de bloque. • **SSL/TLS Service Profile (Perfil del servicio SSL / TLS)**: Para especificar un certificado y las versiones de protocolo TLS para protección de comunicaciones al redireccionar a través del servidor especificado, seleccione un perfil de servicio SSL/TLS. Para obtener más detalles, consulte Device > Certificate Management > SSL/TLS Service Profile. • **Mode (Modo)**: Determina si la página de bloqueo se entrega de manera transparente (parece originarse en el sitio web bloqueado) o redirige al usuario al servidor especificado. Si selecciona **Redirigir**, introduzca después la dirección IP para el redireccionamiento. También puede **Eliminar** una entrada.
Configuración de ID de contenido	
Allow Forwarding of Decrypted Content (Permitir reenvío de contenido descifrado)	Habilite esta opción para configurar el cortafuegos para que reenvíe el contenido descifrado a un servicio exterior cuando tenga el «mirror» de puerto o el envío de archivos de WildFire® para análisis. *Habilite esta opción y envíe todos los archivos desconocidos en tráfico descifrado a WildFire para su análisis.* Para un cortafuegos con capacidad para varios sistemas virtuales (multi-sys), esta opción se habilita para cada sistema virtual. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas Virtuales)** y seleccione el sistema virtual en el que desea habilitar el reenvío de contenido descifrado. Esta opción está disponible en el cuadro de diálogo Sistema Virtual.
Longitud de captura de paquetes extendida	Establezca el número de paquetes que se deben capturar cuando la opción de captura extendida se habilita en perfiles de antispyware y protección frente a vulnerabilidades (intervalo: 1-50; predeterminado: 5).
Reenviar segmentos que superan la cola de	Habilite esta opción para reenviar segmentos y clasificar la aplicación como `unknown-tcp` cuando la cola de App-ID supere el límite de 64 segmentos.

© 2020 Palo Alto Networks, Inc.

Configuración de ID de contenido	Description (Descripción)
inspección de App-ID™ de TCP	Utilice el siguiente contador global para ver el número de segmentos que supera esta cola, independientemente de si habilitó o deshabilitó esta opción: `appid_exceed_queue_limit` Deshabilite esta opción para evitar que el cortafuegos reenvíe segmentos de TCP y omita la inspección de App-ID cuando la cola de inspección de App-ID está llena. *Esta opción está deshabilitada de manera predeterminada y se aconseja dejarla deshabilitada para mayor seguridad.* *Cuando se deshabilita esta opción, es posible que note una mayor latencia en las secuencias donde más de 64 segmentos estaban en cola a la espera del procesamiento de App-ID.*

Reenviar Segmentos que superan la cola de inspección de contenido de TCP)	Habilite esta opción para reenviar datagramas de TCP y omitir la inspección de contenido cuando la cola de inspección de contenido TCP está llena. El cortafuegos puede poner en cola hasta 64 segmentos mientras espera al motor de contenido. Cuando el cortafuegos reenvía un segmento y omite la inspección de contenido debido a la cola de inspección de contenido completa, aumenta el siguiente contador global:
	
	`ctd_exceed_queue_limit`
	
	Deshabilite esta opción para evitar que el cortafuegos reenvíe segmentos de TCP y omita la inspección de contenido cuando la cola de inspección de contenido está llena. Cuando deshabilite esta opción, el cortafuegos omitirá los segmentos que superen el límite de la cola y aumentará el siguiente contador global:
	
	`ctd_exceed_queue_limit_drop`
	
	Este par de contadores globales se aplica a los paquetes de TCP y UDP. Si después de ver los contadores globales decide cambiar la configuración, puede modificarla desde la CLI utilizando el siguiente comando CLI:
	
	`set deviceconfig setting ctd tcp-bypass-exceed-queue`
	
	Esta opción se habilita de forma predeterminada. Sin embargo, Palo Alto Networks recomienda que deshabilite esta opción para mayor seguridad. Sin embargo, debido a las retransmisiones de TCP para el tráfico descartado, la inhabilitación de esta opción puede provocar una degradación del rendimiento y algunas aplicaciones

© 2020 Palo Alto Networks, Inc.

Configuración de ID de contenido	Description (Descripción)
	pueden perder funcionalidad, especialmente en entornos de tráfico de alto volumen.

Reenviar datagramas que superan la cola de inspección de contenido UDP	Habilite esta opción para reenviar datagramas de UDP y omitir la inspección de contenido cuando la cola de inspección de contenido UDP está llena. El cortafuegos puede poner en cola hasta 64 datagramas mientras espera una respuesta del motor de contenido. Cuando el cortafuegos reenvía un datagrama y omite la inspección de contenido debido a un exceso en la cola de inspección de contenido UDSP, aumenta el siguiente contador global:
	`ctd_exceed_queue_limit`
	Deshabilite esta opción para evitar que el cortafuegos reenvíe datagramas y omita la inspección de contenido cuando la cola de inspección de contenido UDP está llena. Con esta opción deshabilitada, el cortafuegos descarta los datagramas que superan el límite de la cola y aumenta el siguiente contador global:
	`ctd_exceed_queue_limit_drop`
	Este par de contadores globales se aplica a los paquetes de TCP y UDP. Si después de ver los contadores globales decide cambiar la configuración, puede modificarla desde la CLI utilizando el siguiente comando:
	`set deviceconfig setting ctd udp-bypass-exceed-queue`
	Esta opción se habilita de forma predeterminada. Sin embargo, Palo Alto Networks recomienda que deshabilite esta opción para mayor seguridad. Sin embargo, debido a los paquetes descartados, la inhabilitación de esta opción puede provocar una degradación del rendimiento y algunas aplicaciones pueden perder funcionalidad, especialmente en situaciones de tráfico de alto volumen.

Allow HTTP partial response (Permitir respuesta parcial de HTTP)	Habilite esta opción de respuesta parcial HTTP para que un cliente pueda recuperar solo parte de un archivo. Cuando un cortafuegos de próxima generación en una transferencia identifica y omite un archivo malicioso, finaliza la sesión TCP con un paquete RST. Si el navegador web implementa la opción de rango HTTP, puede iniciar una nueva sesión para recuperar solo la parte restante del archivo. Esto evita que el cortafuegos active la misma firma de nuevo debido a la falta de contexto en la sesión inicial, mientras permite que el navegador web vuelva a armar el archivo y proporcione el contenido malicioso; para evitar esto, asegúrese de deshabilitar esta opción. *La opción Permitir respuesta parcial HTTP se habilita de forma predeterminada. Sin embargo, Palo Alto Networks recomienda que deshabilite esta opción para*

© 2020 Palo Alto Networks, Inc.

Configuración de ID de contenido	Description (Descripción)
	mayor seguridad. Deshabilitar esta opción no afectará el rendimiento del dispositivo, sin embargo, es posible que afecte la recuperación tras la interrupción de la transferencia del archivo HTTP. Además, la inhabilitación de esta opción puede afectar a los servicios de transmisión de medios, como por ejemplo Netflix, las actualizaciones de Microsoft y las actualizaciones de contenido de Palo Alto Networks.
Búsqueda de firma en tiempo real	
Tiempo de espera de consulta de firma DNS (ms)	Especifique la duración, en milisegundos, para que el cortafuegos consulte al servicio de seguridad de DNS. Si la nube no responde antes del final del periodo especificado, el cortafuegos libera la respuesta DNS asociada al cliente que originó la solicitud (el intervalo es de 0 a 60 000; el valor predeterminado es 80).
X-Forwarded-For Headers	
Usar X-Forwarded-For Header en ID de usuario	Habilite esta opción para especificar que User-ID lea las direcciones IP del encabezado de X-Forwarded-For (XFF) en las solicitudes del cliente de servicios web cuando se implementa el cortafuegos entre Internet y un servidor proxy que, de lo contrario, ocultaría las direcciones IP de clientes. User-ID compara los nombres de usuario que lee con los nombres de usuario que menciona su regla, de modo que esas políticas puedan controlar y registrar el acceso a los usuarios y grupos asociados. Si el encabezado tiene varias direcciones IP, User-ID usa la primera entrada desde la izquierda. En algunos casos, el valor del encabezado es una cadena de caracteres en lugar de una dirección IP. Si la cadena coincide con un nombre de usuario que User-ID ha asignado a una dirección IP, el cortafuegos utiliza ese nombre de usuario para referencias de asignación de grupos en políticas. Si no existe ninguna asignación de direcciones IP para la cadena, el cortafuegos invoca las reglas de políticas en las que está establecido el usuario de origen como**any (cualquiera)** o **unknown (desconocida)**. Los logs de filtrado de URL muestran los nombres de usuario coincidentes en el campo Source User (Usuario de origen). Si User-ID no puede encontrar una coincidencia o no tiene permiso en la zona asociada con la dirección IP, el campo Source User (Usuario de origen) muestra la dirección IP XFF con el prefijo **`x-fwd-for`**. *Habilite la opción utilizando el encabezado XFF en User-ID, para que la dirección IP del cliente original aparezca en los logs cuando necesite investigar un problema.*
Strip-X-Forwarded-For Header	Habilite esta opción para eliminar el encabezado X-Forwarded-For (XFF), que contiene las direcciones IP de un cliente que solicita un servicio web cuando se implementa el cortafuegos entre Internet y un servidor proxy. El cortafuegos pone a cero el valor del encabezado antes de reenviar la

© 2020 Palo Alto Networks, Inc.

Configuración de ID de contenido	Description (Descripción)
	solicitud y los paquetes reenviados no contienen información de IP de origen interna. *Al habilitar esta opción no se deshabilita el uso de los encabezados XFF para la atribución de usuarios en políticas; el cortafuegos solamente pone a cero el valor de XFF tras usarlo para atribución de usuarios.* *Cuando habilita el uso de encabezados XFF en User-ID, también habilita la eliminación del encabezado XFF antes del reenvío del paquete para proteger la privacidad del usuario sin perder la capacidad de realizar el seguimiento de los usuarios. La habilitación de ambas opciones le permite registrar y realizar el seguimiento de las direcciones IP de usuario originales, al mismo tiempo que protege la privacidad del usuario al no reenviar la dirección IP original.*
Características de ID de contenido	
Gestionar protección de datos	Aumente la protección para acceder a logs que puedan incluir información confidencial, como números de tarjetas de crédito o de la Seguridad Social. Haga clic en **Administrar protección de datos** para realizar las siguientes tareas: • **Establecer contraseña**: si aún no hay una configurada, especifique y confirme una nueva contraseña. • **Cambiar contraseña**: introduzca la contraseña anterior y, a continuación, especifique y confirme la nueva contraseña. • **Eliminar contraseña**: permite eliminar la contraseña y los datos protegidos.
Páginas contenedoras	Utilice estos ajustes para especificar los tipos de URL que el cortafuegos seguirá o registrará basándose en el tipo de contenido, como application/pdf, application/soap+xml, application/xhtml+, text/html, text/plain y text/xml. Las páginas contenedoras se establecen según el sistema virtual, el cual puede seleccionar en el menú desplegable **Location (Ubicación)**. Si un sistema virtual no tiene una página contenedora explícita definida, el cortafuegos utilizará los tipos de contenido predeterminados. **Añada** y especifique un tipo de contenido o seleccione un tipo de contenido existente. La adición de nuevos tipos de contenido para un sistema virtual cancela la lista predeterminada de tipos de contenido. Si no hay tipos de contenido asociados a un sistema virtual, se utilizará la lista predeterminada de tipos de contenido.

© 2020 Palo Alto Networks, Inc.

Device > Setup > WildFire

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **WildFire** para configurar los ajustes de WildFire en el cortafuegos y Panorama. Puede habilitar tanto la nube de WildFire como un dispositivo WildFire para que se usen para realizar análisis de archivos. También puede establecer los límites de tamaño de archivo y la información de sesión sobre la que se informará. Tras rellenar la configuración de WildFire, puede especificar qué archivos se reenvían a la nube de WildFire o al dispositivo de WildFire creando un perfil de **WildFire Analysis (Análisis de WildFire)** (**Objects [Objetos]** > **Security Profiles [Perfiles de seguridad]** > **WildFire Analysis [Análisis de WildFire]**).

Para reenviar contenido descifrado a WildFire, consulte Reenvío de tráfico SSL descifrado para el análisis de WildFire.

Configuración de WildFire	Description (Descripción)
Configuración general	
Nube pública de WildFire	Introduzca **`wildfire.paloaltonetworks.com`** para enviar archivos a la WildFire Public Cloud (Nube pública de WildFire) alojada en EE. UU. O bien, puede enviar archivos a una nube regional de WildFire para su análisis. Las nubes regionales están diseñadas para cumplir con las expectativas de privacidad de datos que pueda tener en función de su ubicación. *Reenvíe muestras a una nube regional de WildFire para garantizar el cumplimiento de la privacidad de los datos y los estándares de cumplimiento específicos de su región. Las nubes regionales son las siguientes:* • *Europa:* **`eu.wildfire.paloaltonetworks.com`** • *Japón:* **`jp.wildfire.paloaltonetworks.com`** • *Singapur:* **`sg.wildfire.paloaltonetworks.com`**
Nube privada de WildFire	Especifique la dirección IP o FQDN del dispositivo WildFire El cortafuegos envía archivos para su análisis al dispositivo WildFire especificado. Panorama recoge los ID de amenazas del dispositivo WildFire para habilitar la adición de excepciones de amenaza en perfiles de Anti-Spyware (solo para firmas DNS) y Antivirus que se configuran en grupos de dispositivos. Panorama también recopila información del dispositivo WildFire para rellenar los campos que faltan en los logs de envíos de WildFire recibidos de cortafuegos que ejecutan versiones de software anteriores a PAN-OS 7.0.
Límites de tamaño de archivo	Especifique el tamaño de archivo máximo que se reenviará al servidor WildFire. En cuanto a las recomendaciones sobre los límites del tamaño del archivo, si el límite es demasiado alto e impide que el cortafuegos reenvíe varios archivos grandes de día cero al mismo tiempo, reduzca y ajuste el límite máximo en función de la cantidad de espacio disponible en el búfer del cortafuegos. Si hay más espacio disponible en el búfer, puede aumentar el límite de tamaño de archivo por encima de la recomendación. Las

© 2020 Palo Alto Networks, Inc.

Configuración de WildFire	Description (Descripción)
	recomendaciones son un buen punto de partida para fijar límites efectivos que no sobrecarguen los recursos del cortafuegos. Los rangos disponibles son: • **pe** (Portable Executable [Portable ejecutable]): el intervalo es de 1 a 50 MB, el valor predeterminado es 16 MB. *Establezca el tamaño de los archivos PE en 16 MB.* • **apk** (aplicaciones para Android): el intervalo es 1-50 MB, 10 MB de forma predeterminada. *Establezca el tamaño de los archivos APK en 10 MB.* • **pdf** (Portable Document Format [Formato de documento portátil]): el intervalo es de 100 KB a 51 200 KB, el valor predeterminado es 3072 KB. *Establezca el tamaño de los archivos PDF en 3072 KB.* • **ms-office** (Microsoft Office): el intervalo es de 200 KB a 51 200 KB, el valor predeterminado es 16 384 KB. *Establezca el tamaño de los archivos ms-office en 16 384 KB.* • **jar** (archivo de clase de Java empaquetado): el intervalo es de 1 a 20 MB, el valor predeterminado es 5 MB. *Establezca el tamaño de los archivos jar en 5 MB.* • **flash** (Adobe Flash): el intervalo es de 1 a 10 MB, el valor predeterminado es 5 MB. *Establezca el tamaño de los archivos flash en 5 MB.* • **Mac OS X** (Archivos DMG / MAC-APP / MACH-O PKG): el intervalo es de 1 a 50 MB, el valor predeterminado es 10 MB. *Establezca el tamaño de los archivos MacOSX en 1 MB.* • **archive (archivo comprimido)** (RAR y archivos 7z): el intervalo es de 1 a 50 MB, el valor predeterminado es 50 MB. *Establezca el tamaño de los archivos comprimidos en 50 MB.* • **linux** (archivos ELF): el intervalo es de 1 a 50 MB, el valor predeterminado es 50 MB.

© 2020 Palo Alto Networks, Inc.

Configuración de WildFire	Description (Descripción)
	Establezca el tamaño de los archivos linux en 50 MB. • **script** (archivos JScript, VBScript, PowerShell y Shell Script): el intervalo es de 10 a 4096 KB, el valor predeterminado es 20 KB. *Establezca el tamaño de los archivos script en 20 KB.* *Los anteriores valores podrían ser diferentes según la versión actual de PAN-OS o la versión de contenido. Para ver los intervalos válidos, haga clic en el campo Size Limit (Límite de tamaño), aparecerá un mensaje emergente que mostrará el intervalo disponible y el valor predeterminado.*
Informar de archivos benignos	Cuando esta opción está habilitada (deshabilitada de forma predeterminada), los archivos analizados por WildFire indicados como benignos aparecerán en el log **Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)**. Incluso si esta opción está activada en el cortafuegos, los enlaces de correo electrónico que WildFire considera benignos no se registrarán debido a la cantidad potencial de enlaces procesados.
Archivos Grayware del informe	Cuando esta opción está habilitada (deshabilitada de forma predeterminada), los archivos analizados por WildFire indicados como grayware aparecerán en el log **Monitor (Supervisar)** > **WildFire Submissions (Envíos de WildFire)**. *Incluso si esta opción está activada en el cortafuegos, los enlaces de correo electrónico que WildFire considera grayware no se registrarán debido a la cantidad potencial de enlaces procesados.* *Habilite los archivos grayware de creación de informe para registrar información de la sesión, la actividad de la red, la actividad del host y otra información que contribuya con los análisis.*
Ajustes de información de sesión	
Configuración	Especifique la información que se reenviará al servidor WildFire. De manera predeterminada, todas las opciones están seleccionadas y la recomendación es reenviar toda la información de la sesión para proporcionar estadísticas y otros indicadores que le permitan tomar medidas para evitar los eventos de amenaza: • **Source IP (IP de origen)**: Dirección IP de origen que envió el archivo sospechoso. • **Source Port (Puerto de de origen)**: Puerto de origen que envió el archivo sospechoso.

© 2020 Palo Alto Networks, Inc.

Configuración de WildFire	Description (Descripción)
	• **Destination IP (IP de destino)**: Dirección IP de destino del archivo sospechoso. • **Destination Port (Puerto de destino)**: Puerto de destino del archivo sospechoso. • **Vsys**: Sistema virtual del cortafuegos que identificó al posible software malintencionado. • **Application (Aplicación)**: Aplicación de usuario que se utilizó para transmitir el archivo. • **User (Usuario)**: Usuario de destino. • **URL**: URL asociada al archivo sospechoso. • **Filename**: Nombre del archivo que se envió. • **Email sender (Remitente)**: Proporciona el nombre del remitente en los logs de WildFire e informes de WildFire detallados cuando se detecta un enlace de correo electrónico malicioso en el tráfico del SMTP y POP3. • **Email recipient (Destinatario)**: Proporciona el nombre del destinatario en los logs de WildFire e informes de WildFire detallados cuando se detecta un enlace de correo electrónico malicioso en el tráfico del SMTP y POP3. • **Email subject (Asunto de email)**: Proporciona el asunto del correo electrónico en los logs e informes detallados de WildFire cuando se detecta un enlace de correo electrónico malicioso en el tráfico del SMTP y POP3.

© 2020 Palo Alto Networks, Inc.

Device > Setup > Session

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** para configurar los tiempos de vencimiento de las sesiones, la configuración de certificados de descifrado y los ajustes globales relacionados con las sesiones, como aplicar cortafuegos al tráfico IPv6 y volver a hacer coincidir la política de seguridad con las sesiones existentes cuando cambia la política. La pestaña presenta las siguientes secciones:

- Configuración de sesión
- Tiempos de espera de sesión
- Ajustes de TCP
- Ajustes de descifrado: Comprobación de revocación de certificado
- Ajustes de descifrado: Reenvío de los ajustes de certificados del servidor proxy
- Configuración de sesión de VPN

Configuración de sesión

La siguiente tabla describe los ajustes de sesión.

Configuración de sesión	Description (Descripción)
Reanalizar sesiones establecidas	Haga clic en **Edit** y seleccione **Rematch Sessions (Reanalizar sesiones establecidas** para que el cortafuegos aplique las políticas de seguridad recién configuradas a las sesiones que ya están en curso. Esta capacidad está habilitada de manera predeterminada. Si este ajuste está deshabilitado, cualquier cambio de política se aplica solo a las sesiones iniciadas después de que se haya compilado un cambio de política. Por ejemplo, si se ha iniciado una sesión de Telnet mientras había configurada una política que permitía Telnet y, en consecuencia, ha compilado un cambio de política para denegar Telnet, el cortafuegos aplica la política revisada a la sesión actual y la bloquea. *Habilite Rematch Sessions (Volver a cotejar sesiones) para aplicar su política de seguridad más reciente a las sesiones que actualmente están activas.*
Tamaño de depósito de testigo de ICMPv6	Introduzca el tamaño de depósito para la limitación de tasa de mensajes de error de ICMPv6. El tamaño de depósito de testigo es un parámetro del algoritmo de depósito de testigo que controla la intensidad de las ráfagas de transmisión de los paquetes de error de ICMPv6 (rango: 10-65.535 paquetes; valor predeterminado: 100).
Tasa de paquetes de error de ICMPv6	Introduzca el número medio de paquetes de error de ICMPv6 por segundo que se permiten globalmente a través del cortafuegos (el intervalo es 10-65.535 paquetes/segundo, de forma predeterminada es 100 paquetes/segundo). Este valor se aplica a todas las interfaces. Si el cortafuegos alcanza la tasa de paquetes de error de ICMPv6, el depósito de testigo de ICMPv6 se utiliza para activar la limitación de mensajes de error de ICMPv6.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión	Description (Descripción)
Habilitar cortafuegos IPv6	Para habilitar capacidades de cortafuegos para IPv6, haga clic en **Edit (Editar)** y seleccione **IPv6 Firewalling**. Todas las configuraciones basadas en IPv6 se ignorarán si IPv6 no se habilita. Incluso si IPv6 está activado para una interfaz, la opción **IPv6 Firewalling** también debe estar activado para que IPv6 funcione.
Habilitar trama gigante MTU global	Seleccione esta opción para habilitar la compatibilidad con tramas gigantes en interfaces de Ethernet. Las tramas gigantes tienen una unidad de transmisión máxima (maximum transmission unit, MTU) de 9.192 bytes y están disponibles en determinados modelos. • Si no activa **Enable Jumbo Frame (Habilitar trama gigante)**, **Global MTU (MTU global)** vuelve al valor predeterminado de 1500 bytes (el intervalo es de 576-1.500 bytes). • Si activa **Enable Jumbo Frame**, **Global MTU** vuelve al valor predeterminado de 9.192 bytes (el intervalo es de 9.192-9.216 bytes). *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. Para configurar la MTU para la interfaz (**Red** > **Interfaces** > **Ethernet**), consulte Interfaz de la capa 3 de la serie PA-7000.
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. El intervalo es de 1.280-9.216.
Ratio de sobresuscripción NAT	Seleccione la velocidad 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. La reducción de la velocidad de sobresuscripción disminuirá el número de traducciones de dispositivo origen, pero proporcionará más capacidades de regla de NAT. • **Platform Default (Valor predeterminado de plataforma)**: la configuración explícita de la velocidad de sobresuscripción está desactivada; se aplica la velocidad de sobresuscripción predeterminada para el modelo. Consulte las tasas por defecto de los modelos de cortafuegos en Https://www.paloaltonetworks.com/products/product-selection.html.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión	Description (Descripción)
	• **1x**: 1 vez. Esto significa que no existe ninguna sobresuscripción; cada par de dirección IP y puerto traducido se puede utilizar solo una vez en cada ocasión. • **2x**: 2 veces • **4x**: 4 veces • **8x**: 8 veces
Tasa de paquetes (por segundo) inalcanzable de ICMP	Define el número máximo de respuestas de ICMP inalcanzable que puede enviar el cortafuegos por segundo. Este límite es compartido por los paquetes IPv4 e IPv6. El valor predeterminado es 200 mensajes por segundo (el intervalo es 1-65.535).
Vencimiento acelerado	Activa el vencimiento acelerado de las sesiones inactivas. Seleccione esta opción para habilitar el vencimiento acelerado y especificar el umbral (%) y el factor de escala. Cuando la tabla de sesión alcanza el **Accelerated Aging Threshold (Umbral de vencimiento acelerado)** (% lleno), PAN-OS aplica el **Accelerated Aging Scaling Factor (Factor de escala de vencimiento acelerado)** a los cálculos de vencimiento de todas las sesiones. El factor de escala predeterminado es 2, lo que significa que el vencimiento acelerado se produce a una velocidad dos veces más rápida 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. *Habilite un límite de vencimiento acelerado y configure un factor de escala aceptable para liberar espacio en la tabla de sesiones cuando comience a llenarse.*
Protección de búfer de paquetes	Se recomienda habilitar la protección del búfer de paquetes globalmente y en cada zona para proteger el búfer del cortafuegos de los ataques DoS y orígenes y sesiones agresivos. Esta opción protege los búferes de recepción en el cortafuegos contra ataques o tráfico abusivo que hace que los recursos del sistema se respalden y provoquen la caída del tráfico legítimo. La protección del búfer de paquetes identifica las sesiones infractoras, utiliza el descarte aleatorio anticipado (RED) como primera línea de defensa y descarta la sesión o bloquea la dirección IP infractora si continúa el abuso. Si el cortafuegos detecta muchas sesiones pequeñas o creación rápida de sesiones (o ambas) de una dirección IP particular, bloquea esa dirección IP. Tome las mediciones de referencia de uso del búfer de paquetes del cortafuegos para comprender la capacidad del cortafuegos y garantizar que el cortafuegos tenga el tamaño adecuado, de modo que solo un ataque provoque un gran pico en el uso del búfer.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión	Description (Descripción)
	• **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 cortafuegos genera eventos de log cuando la protección de búfer de paquetes se habilita globalmente (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. Comience con el valor límite predeterminado y ajústelo si fuera necesario. • **Activar (%)**: cuando se alcanza este umbral, el cortafuegos comienza a reducir las sesiones más abusivas (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). Comience con el valor límite predeterminado y ajústelo si fuera necesario. • **Tiempo de espera del bloqueo (s)**: el tiempo, en segundos, que se permite a la sesión continuar antes de que se descarte o se bloquee la dirección IP de origen (el intervalo es de 0 a 65 535; el valor predeterminado es 60). Este temporizador supervisa las sesiones RED-mitigadas para ver si todavía están forzando el uso del búfer por encima del umbral configurado. Si el comportamiento abusivo continúa pasado el tiempo de espera del bloqueo, la sesión se descarta. Si el valor es 0, el cortafuegos no descarta sesiones basadas en la protección de búfer de paquetes. Comience con el valor predeterminado, supervise la utilización del búfer de paquete y ajuste el valor del tiempo si fuera necesario. • **Duración del bloqueo (seg)**: la cantidad de tiempo, en segundos, que una sesión descartada permanece desechada o una dirección IP bloqueada permanece bloqueada (el intervalo es de 1 a 15 999 999; el valor predeterminado es 3600). Utilice el valor predeterminado, a menos que el bloqueo de una dirección IP durante una hora sea una penalización demasiado severa para las condiciones de su empresa, en cuyo caso puede reducir la duración. Supervise el uso del búfer de paquetes y ajuste la duración según sea necesario. *La traducción de direcciones de red puede aumentar la utilización del búfer de paquetes. Si esto afecta la utilización del búfer, reduzca el tiempo de espera de bloqueo (Block Hold Time) para bloquear sesiones individuales más rápido y reduzca la duración del bloqueo, de modo que no se penalicen de manera indebida otras sesiones de la dirección IP subyacente.*
Configuración de buffering de ruta multicast	Seleccione esta opción (deshabilitada de manera predeterminada) para habilitar la configuración de buffering de ruta multicast, lo que permite que el cortafuegos reserve el primer paquete en una sesión multicast cuando la ruta multicast o la entrada de la base de información de reenvío (forwarding information base, FIB) todavía no existe para el grupo multicast 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.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión	Description (Descripción)
Tamaño de búfer de establecimiento de ruta multicast	Si habilita la configuración de bufering de ruta multicast, puede ajustar el tamaño del búfer, lo que especifica el tamaño del búfer por flujo (el intervalo es 1-2.000; el valor predeterminado es 1.000.) El cortafuegos puede almacenar en búfer un máximo de 5000 paquetes.

Tiempos de espera de sesión

El tiempo de espera de una sesión define la duración por 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. El período de tiempo de espera de la sesión descartada define el tiempo máximo durante el cual una sesión permanece abierta después de que PAN-OS deniega la sesión en función de las reglas de la política de seguridad.

En el cortafuegos, puede definir un número de tiempos de espera para sesiones TCP, UDP, ICMP y SCTP por separado. El tiempo de espera **Default (Predeterminado)** se aplica a cualquier otro tipo de sesión. Todos estos tiempos de espera son globales, lo que significa que se aplican a todas la sesiones de ese tipo en el cortafuegos.

Además de los ajustes globales, tiene la posibilidad de definir tiempos de espera para cada aplicación en la pestaña **Objects (Objetos)** > **Applications (Aplicaciones)**. Los tiempos de espera disponibles para esa aplicación aparecen en la ventana Opciones. 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 sesiones TCP, UDP o SCTP.

Utilice las opciones de esta sección para configurar los ajustes de tiempo de espera de sesión globales: específicamente para las sesiones TCP, UDP, ICMP y SCTP, y para el resto de los tipos de sesiones.

Los valores predeterminados son valores óptimos y la recomendación es utilizar dichos valores. 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.

Ajustes de tiempos de espera de sesión	Description (Descripción)
predeterminado	El tiempo máximo, en segundos, que una sesión que no es TCP/UDP, SCTP 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 (en segundos) que una sesión no TCP/UDP/SCTP permanece abierta cuando PAN-OS deniega 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).
Descartar TCP	Tiempo máximo (en segundos) que una sesión TCP permanece abierta cuando PAN-OS deniega 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 90).
Descartar UDP	Tiempo máximo (en segundos) que una sesión UDP permanece abierta cuando PAN-OS deniega una sesión debido a las políticas de seguridad

© 2020 Palo Alto Networks, Inc.

Ajustes de tiempos de espera de sesión	Description (Descripción)
	configuradas en el cortafuegos (el intervalo es de 1 a 15 999 999; el valor predeterminado es 60).
ICMP	El tiempo máximo que una sesión ICMP se puede abrir sin una respuesta de ICMP (el intervalo es 1-15.999.999; el valor predeterminado es 6).
Analizar	Tiempo máximo, en segundos, que una sesión puede estar inactiva antes de que el cortafuegos borre la sesión y recupere los recursos de búfer que la sesión estaba usando. El tiempo inactivo es el tiempo que ha pasado desde que la sesión se actualizó por última vez mediante un paquete o un evento. El intervalo es de 5 a 30; el valor predeterminado es 10.
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); (el intervalo es 1-15.999.999; el valor predeterminado es 3600).
Protocolo de enlace TCP	Tiempo máximo, en segundos entre la recepción de SYN-ACK y la siguiente ACK para establecer completamente la sesión (el intervalo es 1-60; el valor predeterminado es 10).
Inicialización de TCP	Tiempo máximo, en segundos, entre la recepción de SYN y SYN-ACK antes de iniciar el temporizador de protocolo TCP (el intervalo es 1-60; el valor predeterminado es 5).
TCP semicerrado	Tiempo máximo, en segundos, entre la recepción de FIN y la recepción del segundo FIN o un RST (el intervalo es 1-604.800; el valor predeterminado es 120).
Tiempo de espera TCP	Tiempo máximo, en segundos, luego de recibir el segundo FIN o un RST (el intervalo es 1-600; el valor predeterminado es 15).
RST sin verificar	Tiempo máximo después, en segundos, 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); (el intervalo es 1-600; el valor predeterminado es 15).
UDP	El tiempo máximo, en segundos, que una sesión UDP permanece abierta sin una respuesta de UDP (el intervalo es 1-1.599.999; el valor predeterminado es 30).
portal cautivo	El tiempo de espera de la sesión de autenticación en segundos para el formulario web del portal cautivo (valor predeterminado es 30; intervalo es 1-1.599.999). Para acceder al contenido solicitado, el usuario debe introducir las credenciales de autenticación en este formato y autenticarse correctamente. El tiempo de espera de la sesión de autenticación en segundos para el formulario web del portal cautivo (valor predeterminado es 30; intervalo es 1-1.599.999). Para acceder al contenido solicitado, el usuario debe

© 2020 Palo Alto Networks, Inc.

Ajustes de tiempos de espera de sesión	Description (Descripción)
	introducir las credenciales de autenticación en este formato y autenticarse correctamente.
SCTP INIT (INIT de SCTP)	El tiempo máximo, en segundos, desde la recepción de un fragmento de INIT de SCTP en el que un cortafuegos debe recibir un fragmento de INIT de ACK antes de que el cortafuegos detenga la inicialización de la asociación de SCTP (el intervalo es de 1 a 60; el valor predeterminado es 5).
SCTP COOKIE (Cookie de SCTP)	El tiempo máximo, en segundos, desde la recepción de un fragmento de INIT ACK de SCTP con el parámetro COOKIE de estado en el que un cortafuegos debe recibir el fragmento ECO de COOKIE con la cookie antes de que el cortafuegos detenga la inicialización de la asociación de SCTP (el intervalo es de 1 a 600; el valor predeterminado es 60).
Discard SCTP (Descartar SCTP)	Tiempo máximo (en segundos) que una asociación de SCTP permanece abierta después de que PAN-OS deniega la sesión en función de las reglas de la política de seguridad configuradas en el cortafuegos (el intervalo es de 1 a 604 800; el valor predeterminado es 30).
SCTP	Tiempo máximo (en segundos) que puede transcurrir sin tráfico de SCTP para una asociación antes de que todas las sesiones de la asociación se agoten (el intervalo es de 1 a 604 800; el valor predeterminado es 3600).
SCTP Shutdown (Apagado de SCTP)	El tiempo máximo, en segundos, que el cortafuegos espera después de que un fragmento SHUTDOWN de SCTP reciba un fragmento SHUTDOWN ACK antes de que el cortafuegos ignore el fragmento SHUTDOWN (el intervalo es de 1 a 600; el valor predeterminado es 30).

Ajustes de TCP

La siguiente tabla describe los ajustes TCP

Ajustes de TCP	Description (Descripción)
Reenviar segmentos que superan la cola fuera de servicio de TCP	Seleccione esta opción si desea que el cortafuegos reenvíe segmentos que superen el límite de 64 por sesión de la cola fuera de servicio de TCP. Si deshabilita esta opción, el cortafuegos omite segmentos que superan el límite de la cola fuera de servicio. Para ver un recuento del número de segmentos que el cortafuegos descartó como resultado de habilitar esta opción, ejecute el siguiente comando CLI. `show counter global tcp_exceed_flow_seg_limit` *Esta opción está desactivada de forma predeterminada y debe permanecer así para la implementación más segura. Deshabilitar esta opción puede resultar en una mayor latencia para la secuencia específica que recibió en 64 segmentos fuera de servicio. No debería haber pérdida*

© 2020 Palo Alto Networks, Inc.

Ajustes de TCP	Description (Descripción)
	de conectividad porque la pila TCP debería gestionar la retransmisión de segmentos perdidos.
Omitir segmentos con la opción de marca de tiempo nula	La marca de tiempo de TCP registra cuándo se envió el segmento y permite que el cortafuegos verifique si la marca de tiempo es válida para esa sesión, lo que evita el ajuste del número de secuencia de TCP. La marca de tiempo de TCP también se utiliza para calcular el tiempo de ida y vuelta. Con esta opción habilitada, el cortafuegos descarta paquetes con marcas de tiempo nulas. Para ver un recuento del número de segmentos que el cortafuegos descartó como resultado de habilitar esta opción, ejecute el siguiente comando CLI. `show counter global tcp_invalid_ts_option` *Esta opción está habilitada de forma predeterminada y debe permanecer así para la implementación más seguro. Habilitar esta opción no debe degradar el rendimiento. Sin embargo, si una red ordenada de manera incorrecta genera segmentos con un valor de opción de marca de tiempo de TCP nula, habilitar esta opción puede provocar problemas de conexión.*
Indicador de datos urgentes	Use esta opción para configurar si el cortafuegos permite el puntero de urgencia (indicador bit URG) en el encabezado TCP. El puntero de urgencia en el encabezado TCP se utiliza para promover un paquete para su procesamiento inmediato; el cortafuegos lo quita de la cola de procesamiento y lo envía a través de la pila TCP/IP en el host. Este proceso se denomina procesamiento fuera de banda. Debido a que la implementación del puntero de urgencia varía según el host, configurar esta opción a **Clear (Borrar)** (el ajuste predeterminado y recomendado) elimina cualquier ambigüedad, mediante la desautorización del procesamiento fuera de banda para que el byte fuera de banda en la carga se convierta en parte de la carga y el paquete no se procese con urgencia. Además, el ajuste **Clear (Borra)** garantiza que el cortafuegos observa la secuencia exacta en la pila de protocolos que el host para el que está destinado el paquete. Para ver un recuento del número de segmentos en los cuales el cortafuegos borró el indicador URG cuando se estableció esta opción en **Clear (Borrar)**, ejecute el siguiente comando CLI: `show counter global tcp_clear_urg` *De forma predeterminada, este indicador se establece en Clear (Borrar) y debe permanecer así para la implementación más segura. Esto no debe afectar el rendimiento; en el caso poco frecuente que las aplicaciones, como telnet, utilicen la función de datos urgentes, es posible que TCP se vea afectado. Si establece este indicador en Do Not Modify (No modificar), el cortafuegos permite paquetes con el*

© 2020 Palo Alto Networks, Inc.

Ajustes de TCP	Description (Descripción)
	indicador bit URG en el encabezado de TCP y permite el procesamiento fuera de banda (no recomendado).
Omitir segmentos sin indicador	Los segmentos TCP ilegales sin ningún conjunto de indicadores pueden utilizarse para evadir inspecciones de contenido. Con esta opción habilitada (de manera predeterminada) el cortafuegos descarta paquetes que no tienen indicadores establecidos en el encabezado de TCP. Para ver un recuento del número de segmentos que el cortafuegos descartó como resultado de habilitar esta opción, ejecute el siguiente comando CLI. `show counter global tcp_flag_zero` *Esta opción está habilitada de forma predeterminada y debe permanecer así para la implementación más seguro. Habilitar esta opción no debe degradar el rendimiento. Sin embargo, si una red ordenada de manera incorrecta genera segmentos sin indicadores TCP, habilitar esta opción puede provocar problemas de conexión.*

Ajustes de descifrado: Comprobación de revocación de certificado

Seleccione **Session (Sesión)**, y en Decryption Settings, seleccione **Certificate Revocation Checking (Comprobación de revocación de certificado)** para configurar los parámetros descritos en la siguiente tabla.

Características de sesión: Comprobación de revocación de certificado	Description (Descripción)
Habilitar: CRL	Seleccione esta opción para utilizar el método de la lista de revocación de certificados (CRL) y verificar el estado de revocación de los certificados. Si también activa el protocolo de estado de certificado en línea (OCSP), el cortafuegos primero prueba con él; si el servidor OCSP no está disponible, entonces el cortafuegos intenta utilizar el método CRL. Para obtener más información sobre certificados de descifrado, consulte Políticas de claves y certificados para el descifrado.
Tiempo de espera de recepción: CRL	Si ha activado el método CLR para verificar el estado de revocación de certificados, especifique el intervalo en segundos (1-60, el valor predeterminado es 5) después del cual el cortafuegos deja de esperar una respuesta procedente del servicio de CRL.
Habilitar: Ocsp	Seleccione esta opción para utilizar OCSP y verificar el estado de revocación de los certificados.
Tiempo de espera de recepción: Ocsp	Si ha activado el método OCSP para verificar el estado de revocación de certificados, especifique el intervalo en segundos (1-60, el valor

© 2020 Palo Alto Networks, Inc.

Características de sesión: Comprobación de revocación de certificado	Description (Descripción)
	predeterminado es5) después del cual el cortafuegos deja de esperar una respuesta procedente del servicio de OCSP.
Bloquear sesión con estado de certificado desconocido	Seleccione esta opción para bloquear sesiones SSL/TLS cuando el servicio OCSP o CRL devuelva un estado de revocación de certificados desconocido. De lo contrario, el cortafuegos continuará con la sesión.
Bloquear sesión tras el tiempo de espera de comprobación del estado del certificado	Seleccione esta opción para bloquear sesiones SSL/TLS después de que el cortafuegos registre un tiempo de espera de la solicitud de OCSP o CRL. De lo contrario, el cortafuegos continuará con la sesión.
Tiempo de espera del estado del certificado	Especifique el intervalo en segundos (1-60 segundos, el valor predeterminado es 5) tras el cual el cortafuegos deja de esperar una respuesta de cualquier servicio de estado de certificados y aplica cualquier lógica de bloqueo de sesión que opcionalmente 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.

Ajustes de descifrado: Reenvío de los ajustes de certificados del servidor proxy

En la sección Decryption Settings (Configuración de descifrado) (pestaña **Session [Sesión]**), seleccione **SSL Forward Proxy Settings (Configuración de proxy de reenvío de SSL)** para configurar **RSA Key Size (Tamaño de clave RSA)** o **ECDSA Key Size (Tamaño de clave ECDSA)**, y el algoritmo de hash de los certificados que presenta el cortafuegos a los clientes cuando establecen sesiones para el descifrado de proxy de reenvío SSL/TLS. La siguiente tabla describe los parámetros.

Características de sesión: Reenvío de los ajustes de certificados del servidor proxy	
Tamaño de clave RSA	Seleccione una de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

Características de sesión: Reenvío de los ajustes de certificados del servidor proxy	

	• **Defined by destination host (Definido por host de destino)** (predeterminado): seleccione esta opción si desea que el cortafuegos genere certificados en función de la clave que utiliza el servidor de destino:
	  • Si el servidor de destino utiliza una clave RSA de 1024 bits, el cortafuegos genera un certificado con ese tamaño de clave y un algoritmo de hash SHA1.
	  • Si el servidor de destino utiliza un tamaño de clave superior a 1024 bits (por ejemplo, 2048 bits o 4096 bits), el cortafuegos genera un certificado que utilizará una clave RSA de 2048 bits y un algoritmo SHA-256.
	• **1024-bit RSA (RSA de 1024 bits)**: seleccione esta opción si desea que el cortafuegos genere certificados que utilicen una clave RSA de 1024 bits y un algoritmo de hash SHA1 independientemente del tamaño de la clave que utiliza el 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 (RSA de 2.048 bits)**: seleccione esta opción si desea que el cortafuegos genere certificados que utilicen una clave RSA de 2.048 bits y un algoritmo de hash SHA-256 independientemente del tamaño de la clave que utiliza el 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.

Tamaño de clave ECDSA	Seleccione una de las siguientes opciones:
	• **Defined by destination host (Definido por host de destino)** (predeterminado): seleccione esta opción si desea que el cortafuegos genere certificados en función de la clave que utiliza el servidor de destino:
	  • Si el servidor de destino utiliza una clave ECDSA de 256 bits o 384 bits, el cortafuegos genera un certificado con ese tamaño de clave.
	  • Si el servidor de destino utiliza un tamaño de clave superior a 384 bits, el cortafuegos genera un certificado que utilizará una clave de 521 bits.
	• **256-bit ECDSA (ECDSA de 256 bits)**: seleccione esta opción si desea que el cortafuegos genere certificados que utilicen una clave ECDSA de 256 bits, independientemente del tamaño de la clave que utiliza el servidor de destino.
	• **384-bit ECDSA (ECDSA de 384 bits)**: seleccione esta opción si desea que el cortafuegos genere certificados que utilicen una clave ECDSA de 384 bits, independientemente del tamaño de la clave que utiliza el servidor de destino.

Configuración de sesión de VPN

Seleccione **Session**, y en Configuración de sesión de VPN, configure los ajustes globales relacionados con el cortafuegos que establece una sesión de VPN. La siguiente tabla describe la configuración.

© 2020 Palo Alto Networks, Inc.

Configuración de sesión de VPN	Description (Descripción)
Umbral de activación de cookies	Especifique un número máximo de asociaciones de seguridad (SA) IKE a medio abrir IKEv2 permitidas por el cortafuegos, por encima del cual se activa la validación de cookies. Si el número de SA IKE a medio abrir supera el umbral de activación de cookies, el respondedor solicita una cookie y el iniciador debe responder con una IKE_SA_INIT que contenga una cookie. Si la cookie se valida correctamente, se puede iniciar otra sesión de SA. Un valor de 0 significa que la validación de cookies está siempre activa. El Umbral de activación de cookies es una configuración de cortafuegos global y debería ser inferior a la configuración de SA medio abiertas máx., que también es global (intervalo es 0-65.535; predeterminado es 500).
SA medio abiertas máx.	Especifique el número máximo de SA IKE a medio abrir IKEv2 que los iniciadores pueden enviar al cortafuegos sin obtener una respuesta. Cuando se alcance el máximo, el cortafuegos no responderá a nuevos paquetes IKE_SA_INIT (intervalo es 1-65.535; predeterminado es 65.535).
Certificados en caché máx.	Especifique el número máximo de certificados de autoridades de certificados (CA) de peer recuperados por HTTP que el cortafuegos puede almacenar en caché. Este valor solo lo usan las funciones IKEv2 Hash y URL (intervalo es 1-4.000; predeterminado es 500).

© 2020 Palo Alto Networks, Inc.

Device > High Availability

- Device > High Availability

En la redundancia, implemente sus cortafuegos de próxima generación de Palo Alto Networks en una configuración de alta disponibilidad. Existen dos implementaciones de HA:

- activa/pasiva: en esta implementación, el peer activo sincroniza continuamente la información de configuración y sesión con el peer pasivo en dos interfaces dedicadas. En el caso de una interrupción de hardware o software en el cortafuegos activo, el cortafuegos pasivo se activa automáticamente sin la pérdida del servicio. Las implementaciones de HA activas/pasivas se admiten en todos los modos de interfaz: virtual-wire, capa 2 o capa 3.
- activa/activa: en esta implementación, ambos peers de HA se activan y procesan el tráfico. Estas implementaciones son las más adecuadas para los casos que involucran el enrutamiento asimétrico o en casos en donde desea permitir protocolos de enrutamiento dinámico (OSPF, BGP) para mantener el estado activo en ambos peers. La HA activa/activa se admite solo en los modos de interfaz virtual-wire y capa 3. Además de los enlaces de HA1 y HA2, las implementaciones activa/activa requieren un enlace HA3 dedicado. El enlace HA3 se utiliza como enlace de reenvío de paquetes para la configuración de sesión y la gestión de tráfico asimétrico.

En un par de HA, ambos peers deben tener el mismo modelo, deben ejecutar la misma versión de PAN-OS y la versión de contenido, y deben tener el mismo conjunto de licencias.

Asimismo, para los cortafuegos VM-Series, ambos peers deben estar en el mismo hipervisor y deben tener el mismo número de núcleos de CPU asignados a cada peer.

- Consideraciones importantes para la configuración de alta disponibilidad (HA)
- Configurar los ajustes de HA

Consideraciones importantes para la configuración de alta disponibilidad (HA)

- La subred utilizada para la IP local y del peer no debe utilizarse en ningún otro lugar del enrutador virtual.
- Las versiones del sistema operativo y del contenido deben ser las mismas en cada cortafuegos. Una falta de coincidencia puede evitar que los cortafuegos de peer se sincronicen.
- Los LED son de color verde en los puertos de HA para el cortafuegos activo y de color ámbar en el cortafuegos pasivo.
- Puede comparar la configuración de los cortafuegos local y peer mediante la herramienta **Config Audit (Auditoría de config.)** de la pestaña **Device (Dispositivo)**, seleccionando la configuración local deseada en el cuadro de selección de la izquierda y la configuración del peer en el cuadro de selección de la derecha.
- Sincronice los cortafuegos desde la interfaz web haciendo clic en **Push Configuration (Configuración de envío)** en el widget de HA en la pestaña **Dashboard (Panel)**. La configuración del cortafuegos desde el que la inserta sobrescribirá aquella del cortafuegos del peer. Para sincronizar los cortafuegos desde la CLI del cortafuegos activo, ejecute el comando "request high-availability sync-to-remote running-config".

En una configuración activa/pasiva de alta disponibilidad (HA) con cortafuegos que utilizan puertos de SFP+ de 10 gigabits, cuando se produce una conmutación por error y el cortafuegos activo cambia a un estado pasivo, el puerto Ethernet de 10 gigabits se desactiva y se vuelve a activar para actualizar el puerto, pero no permite la transmisión hasta que el cortafuegos vuelve a activarse. Si cuenta con un software de supervisión en el dispositivo vecino, este verá el puerto como flap debido a su desactivación y posterior activación. Este comportamiento es distinto al de otros puertos, como el puerto Ethernet

© 2020 Palo Alto Networks, Inc.

de 1 gigabit. Aunque se deshabilite, este puerto sigue permitiendo la transmisión, por lo que el dispositivo vecino no detecta ningún flap.

Configurar los ajustes de HA

Para configurar los ajustes de HA, seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** y luego, en cada grupo de opciones, especifique la información correspondiente descrita en la siguiente tabla.

Configuración de HA	Description (Descripción)
Pestaña General	
Configuración	Especifique los siguientes ajustes: • **Enable HA (Habilitar HA)**: Active las prestaciones de HA. • **Group ID (ID de grupo)**: Introduzca un número para identificar el par de HA (de 1 a 63). Este campo es obligatorio (y debe ser único) si varios pares de HA residen en el mismo dominio de difusión. • **Description (Descripción)**: Introduzca una descripción del par de HA (Opcional). • **Mode (Modo)**: configure el tipo de implementación de HA: **Active Passive (Activo-Pasivo)** o **Active Active (Activo-Activo)**. • **Device ID (ID de dispositivo)**: en una configuración activa/activa, establezca el ID del dispositivo para determinar qué peer será el activo principal (configure **Device ID (ID de dispositivo)** en **0**) y cuál será el activo secundario (configure **Device ID (ID de dispositivo)** en **1**). • **Enable Config Sync (Habilitar sincronización de configuración)**: seleccione esta opción para habilitar la sincronización de la configuración entre los peers. *Siempre permita la sincronización de configuración, de manera que ambos dispositivos tengan la misma configuración y procesen el tráfico de la misma manera en todo momento.* • **Peer HA1 IP Address (Dirección IP de HA del peer)**: ingrese la dirección IP de la interfaz HA1 del cortafuegos del peer. • **Backup Peer HA1 IP Address (Crear copia de seguridad de la dirección IP de HA1 del peer)**: Introduzca la dirección IP del enlace de control de copia de seguridad del peer. *Configure una copia de seguridad de la dirección IP de HA1 del peer, para que, en caso de fallo del enlace principal, el enlace de seguridad mantenga los dispositivos sincronizados y actualizados.*
Configuración Activa/ Pasiva	• **Passive Link State (Estado de los enlaces en el pasivo)** : seleccione una de las siguientes opciones para especificar si los enlaces de datos en el cortafuegos pasivo deben permanecer activos. Esta opción no está disponible en el cortafuegos VM-Series en AWS. • **auto (automático)**: los enlaces que tienen conectividad física permanecen físicamente activos pero en un estado deshabilitado; no participan en el aprendizaje ARP ni en el reenvío de paquetes. Esto ayudará en los momentos de convergencia durante la conmutación por

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	error ya que se ahorra tiempo para activar los enlaces. Para evitar bucles de red, no seleccione esta opción si el cortafuegos tienen alguna interfaz de capa 2 configurada. • **Shutdown (Apagar)**: Obliga a aplicar el estado desactivado al enlace de interfaz. Esta es la opción predeterminada, que garantiza que no se creen bucles en la red. *Si el cortafuegos no tiene interfaces de capa 2 configuradas, configure el Passive Link State (Estado de los enlaces en el pasivo) en auto (automático).* • **Monitor Fail Hold Down Time (min) [Supervisar fallo de tiempo de espera descendente (min)]**: Este valor entre 1 y 60 minutos determina el intervalo en el que un cortafuegos estará en un estado no funcional antes de volverse pasivo. Este temporizador se utiliza cuando faltan latidos o mensajes de saludo debido a un fallo de supervisión de ruta o de enlace.
Configuración de elección	Especifique o habilite los siguientes ajustes: • **Device Priority (Prioridad de dispositivo)**: Introduzca un valor de prioridad para identificar el cortafuegos activo. El cortafuegos con el valor más bajo (alta prioridad) se convierte en el cortafuegos activo (el intervalo es 0-255) cuando la función Preferente está activada en ambos cortafuegos del par. • **Heartbeat Backup (Backup de heartbeat)**: Utiliza los puertos de gestión en los cortafuegos de HA para proporcionar una ruta de copia de seguridad para mensajes de latidos y saludos. La dirección IP del puerto de gestión se compartirá con el peer de HA a través del enlace de control HA1. No se requiere ninguna configuración adicional. *Habilite Heartbeat Backup (Copia de seguridad de heartbeat) si utiliza un puerto interno para los enlaces de copia de seguridad de HA1 y HA1. No habilite Heartbeat Backup (Copia de seguridad de heartbeat) si utiliza el puerto de gestión para los enlaces de copia de seguridad de HA1 y HA1.* • **Preemptive (Preferente)**: Habilita el cortafuegos de mayor prioridad para reanudar el funcionamiento activo (activo/pasivo) o activo principal (activo/activo) tras recuperarse de un fallo. La opción Preferencia debe estar habilitada en ambos cortafuegos para que los de mayor prioridad reanuden el funcionamiento activo o activo principal tras recuperarse de un fallo. Si este ajuste está desactivado, el cortafuegos de menor prioridad permanecerá activo o activo principal incluso después de que el cortafuegos de mayor prioridad se recupere de un fallo. *La habilitación o no de la opción Preemptive (Preferente) depende de los requisitos de la empresa. Si necesita que el dispositivo principal sea el dispositivo activo, habilite Preemptive (Preferente), para que, después de recuperarse de un fallo, el dispositivo principal se adelante al dispositivo secundario. Si necesita la menor cantidad posible de eventos de conmutación por error, deshabilite la opción Preemptive (Preferente) para que, después de una conmutación por error, el par HA no vuelva a ejecutar*

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)

	la conmutación por error, para convertir el cortafuegos de prioridad más alta en el cortafuegos principal.
	• **HA Timer Settings (Configuración del temporizador HA)**: Seleccione uno de los perfiles preestablecidos:
	  • **Recommended (Recomendada)**: Utilícelo para la configuración de temporizador de conmutación por error típica. A menos que tenga la certeza de que necesita una configuración diferente, se recomienda usar la configuración **Recommended (Recomendada)**.
	  • **Aggressive (Agresiva)**: Para configuración de temporizador de conmutación por error más rápida.
	  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.
	  • **Advanced (Avanzado)**: Le permite personalizar los valores para adaptarse a sus requisitos de red para cada uno de los siguientes temporizadores:
	  • **Promotion Hold Time (Tiempo de espera de promoción)**: introduzca el tiempo que el peer pasivo (en el modo activo/pasivo) o el peer secundario activo (en el modo activo/activo) esperará antes de tomar el control como peer 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.
	  • **Hello Interval (Intervalo de saludo)**: Introduzca el número de milisegundos entre los paquetes de saludo enviados para verificar que el programa de HA del otro cortafuegos sea operativo (el intervalo es 8000-60 000; el valor predeterminado es 8000).
	  • **Heartbeat Interval (Intervalo de heartbeat)**: especifique con qué frecuencia los peers de HA intercambian mensajes de latidos con la forma de un ping ICMP (el intervalo es 1000-60 000 ms; no hay valor predeterminado).
	  • **Maximum No. of Flaps (N.º máximo de fluctuaciones)**: Se cuenta un fluctuación cuando el cortafuegos deja el estado activo antes de que transcurran 15 minutos desde la última vez que dejó el estado activo. Puede especificar el número máximo de fluctuaciones permitidas antes de que se determine suspender el cortafuegos y que el cortafuegos pasivo tome el control (el intervalo es 0-16; el valor predeterminado es 3). El valor 0 significa que no hay máximo (se necesita un número infinito de flaps antes de que el cortafuegos pasivo tome el control).
	  • **Preemption Hold Time (Tiempo de espera para ser preferente)**: Introduzca el tiempo en minutos que un peer secundario pasivo o activo espera antes de tomar el control como peer activo o principal activo (el intervalo es 1-60; el predeterminado es 1).

	• **Monitor Fail Hold Up Time (ms) [Tiempo de espera ascendente tras fallo de supervisor (ms)]**: Especifique el 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

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	de HA debido a las fluctuaciones ocasionales de los dispositivos vecinos (el intervalo es 0-60.000 ms; el predeterminado es 0 ms). • **Additional Master Hold Up Time (min) [Tiempo de espera ascendente principal adicional (min.)]**: Este intervalo de tiempo se aplica al mismo evento que Supervisar fallo de tiempo de espera ascendente (el intervalo es 0-60.000 ms; el valor predeterminado es 500 ms). El intervalo de tiempo adicional únicamente se aplica al peer activo en el modo activo/pasivo y al peer principal activo en el modo activo/activo. Se recomienda este temporizador para evitar una conmutación por error cuando ambos peers experimentan el mismo fallo de supervisor de enlace/ruta simultáneamente.
Enlace de control (HA1)/Enlace de control (copia de seguridad de HA1)	Los cortafuegos en un clúster en HA usan enlaces de HA para sincronizar datos y mantener la información de estado. Algunos modelos de cortafuego tienen un enlace de control dedicado y un enlace de control de copia de seguridad dedicado; por ejemplo, los cortafuegos de la serie PA-5200 tienen HA1-A y HA1-B. En ese caso, usted debe habilitar la opción de copia de seguridad de heartbeat en la página Configuración de elección. Si está utilizando un puerto HA1 dedicado para el enlace de HA de enlace de control y un puerto de datos para el enlace de control (copia de seguridad de HA), se recomienda habilitar la opción Copia de seguridad de heartbeat. En el caso de cortafuegos que no tienen un puerto de HA específico, como el cortafuegos PA-220, debe configurar el puerto de gestión para la conexión de HA del enlace de control y una interfaz de puerto de datos configurada con el tipo HA para la conexión de copia de seguridad de HA1 del enlace de control. Como en este caso se está utilizando el puerto de gestión, no es necesario habilitar la opción Copia de seguridad de heartbeat, porque las copias de seguridad de heartbeat ya se realizarán a través de la conexión de interfaz de gestión. En el cortafuegos VM-Series en AWS, el puerto de gestión se usa como el enlace HA1. *Al utilizar un puerto de datos para el enlace de control de HA, debe tener en cuenta que, dado que los mensajes de control tienen que comunicarse desde el plano de datos hasta el plano de gestión, si se produce un fallo en el plano de datos, los peers no pueden comunicar la información del enlace de control de HA y se producirá una conmutación por error. Lo mejor es utilizar los puertos de HA específicos o, en cortafuegos que no tengan ningún puerto de HA específico, el puerto de gestión.* Especifique los siguientes ajustes para los enlaces de control de HA principal y de copia de seguridad: • **Port (Puerto)**: Seleccione el puerto de HA para las interfaces de HA1 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **IPv4/IPv6 Address (Dirección IPv4/IPv6)**: Introduzca la dirección IPv4 o IPv6 de la interfaz de HA1 para las interfaces de HA1 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional.

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	Los cortafuegos de la serie PA-3200 no admiten direcciones IPv6 para las interfaces HA1 de copia de seguridad. Utilice direcciones IPv4. • **Netmask (Máscara de red)**: Introduzca la máscara de red de la dirección IP (como por ejemplo 255.255.255.0) para las interfaces de HA1 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **Gateway (Puerta de enlace)**: Introduzca la dirección IP de la puerta de enlace predeterminada para las interfaces de HA1 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **Link Speed (Velocidad del enlace)**: (solo modelos con puertos de HA dedicados) seleccione la velocidad del enlace de control entre los cortafuegos para el puerto de HA1 específico. • **Link Duplex (Dúplex de enlace)**: (solo modelos con puertos de HA dedicados) seleccione una opción de dúplex para el enlace de control entre los cortafuegos para el puerto de HA1 específico. • **Encryption Enabled (Cifrado habilitado)**: Habilite el cifrado después de exportar la clave de HA desde el peer de HA e importarla a este cortafuegos. La clave de HA de este cortafuegos también debe exportarse desde este cortafuegos e importarse al peer de HA. Configure este ajuste para la interfaz de HA1 principal. Claves de importación / exportación en la página Certificados (consulte Device > Certificate Management > Certificate Profile). *Habilite el cifrado cuando los cortafuegos no estén directamente conectados (las conexiones HA1 atraviesan dispositivos de red que pueden inspeccionar, procesar o capturar tráfico).* • **Monitor Hold Time (ms) [Tiempo de espera de supervisor (ms)]**: Introduzca el tiempo (milisegundos) que el cortafuegos esperará antes de declarar un fallo de peer debido a un fallo del enlace de control (el intervalo es 1.000-60.000; el valor predeterminado es 3.000). Esta opción supervisa el estado del enlace físico de los puertos de HA1.
Enlace de datos (HA2) *Cuando se configura un enlace de copia de seguridad de HA2, se producirá una conmutación por*	Especifique los siguientes ajustes para el enlace de datos principal y de copia de seguridad: • **Port (Puerto)**: Seleccione el puerto de HA. Configure este ajuste para las interfaces de HA2 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **IP Address (Dirección IP)**: Especifique la dirección IPv4 o IPv6 de la interfaz de HA para las interfaces de HA2 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **Netmask (Máscara de red)**: Especifique la máscara de red de la interfaz de HA para las interfaces de HA2 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. • **Gateway (Puerta de enlace)**: Especifique la puerta de enlace predeterminada de la interfaz de HA para las interfaces de HA2 principal y de copia de seguridad. El ajuste de copia de seguridad es opcional. Si las direcciones IP de HA2 de los cortafuegos están en la misma subred, el campo Puerta de enlace debería quedarse en blanco.

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)

error en el enlace de copia de seguridad si hay un fallo en el enlace físico. Con la opción Conexión persistente de HA2 habilitada, la conmutación por error también se producirá si fallan los mensajes de conexión persistente de HA basados en el umbral definido.	• **Enable Session Synchronization (Habilitar sincronización de sesión)**: Habilite la sincronización de la información de la sesión con el cortafuegos pasivo y seleccione una opción de transporte.
	
	Habilite la sincronización de sesión, de manera que el dispositivo secundario tenga la sesión en su plano de datos, lo que permite que el cortafuegos haga coincidir los paquetes con la sesión sincronizada y reenvíe los paquetes rápidamente. Si no habilita la sincronización de sesión, el cortafuegos debe crear la sesión nuevamente, lo cual introduce latencia y podría desactivar las conexiones.
	• **Transport (Transporte)**: Seleccione una de las siguientes opciones de transporte:
	  • **Ethernet**: Utilice esta opción cuando los cortafuegos estén conectados opuesto con opuesto o a través de un conmutador (Ethertype 0x7261).
	  • **IP**: Utilice esta opción cuando se requiera el transporte de capa 3 (número de protocolo IP: 99).
	  • **UDP**: Utilice esta opción para aprovechar el hecho de que la suma de comprobación se calcula sobre todo el paquete y no solamente el encabezado, como en la opción IP (puerto UDP 29281). El beneficio de usar el modo UDP es la presencia de la suma de comprobación UDP para verificar la integridad de un mensaje de sincronización de sesión.
	• **Link Speed (Velocidad del enlace)**: (solo modelos con puertos de HA dedicados) seleccione la velocidad del enlace de control entre los peers para el puerto de HA1 específico.
	• **Link Duplex (Dúplex de enlace)**: (solo modelos con puertos de HA dedicados) seleccione una opción de dúplex para el enlace de control entre peers para el puerto de HA2 específico.
	  • **HA2 keep-alive (Conexión persistente de HA2)**: se recomienda seleccionar esta opción para supervisar el estado del enlace de datos de HA2 entre los peers de HA. Esta opción está deshabilitada de manera predeterminada y puede habilitarla en uno o ambos peers. Si está habilitada, los peers usarán los mensajes de persistencia para supervisar la conexión de HA para detectar una falla sobre la base del **Threshold (Umbral)** que configuró (el valor predeterminado es 10 000 ms). Si habilita la persistencia de HA2, se tomará la medida de recuperación de persistencia de HA2. Seleccione una **Action (Acción)**:
	  • **Log Only (Solo log)**: registra la falla de la interfaz de HA2 en el log del sistema como un evento crítico. Seleccione esta opción para las implementaciones activa/pasiva dado que el peer activo es el único cortafuegos que reenvía tráfico. El peer pasivo se encuentra en un estado de copia de seguridad y no reenvía tráfico; por lo tanto, no se requiere una ruta de datos dividida. Si no configuró ningún vínculo de copia de seguridad de HA2, la sincronización del estado se desactivará. Si la ruta de HA2 se recupera, se generará un log informativo.
	  • **Split Datapath (Dividir ruta de datos)**: seleccione esta opción en las implementaciones activa/activa de HA para indicar a cada peer que tome posesión de su estado local y las tablas de sesión cuando detecte una falla de la interfaz de HA2. Sin la conectividad de HA2, no se puede dar una sincronización de estado y sesión; esta acción permite separar la gestión de las tablas de sesión para garantiza el reenvío de tráfico

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	correcto por parte de cada peer de HA. Para evitar esta condición, configure un enlace de copia de respaldo de HA2. • **Threshold (ms) [Umbral (ms)]**: Tiempo durante el cual los mensajes de conexión persistente han fallado antes de que se haya activado una de las acciones anteriores (el intervalo es 5.000-60.000 ms; el valor predeterminado es 10.000 ms).
Pestaña Supervisión de enlaces y rutas (no disponible para el cortafuegos VM-Series en AWS**)**	
Monitorización de rutas	Especifique lo siguiente: • **Enabled (Habilitado)**: Habilite la supervisión de rutas. La supervisión de rutas permite que el cortafuegos supervise direcciones IP de destino especificadas enviando mensajes de ping ICMP para asegurarse de que responden. Utilice la supervisión de rutas para configuraciones de Virtual Wire, capa 2 o capa 3 cuando se necesite la supervisión de otros dispositivos de red en caso de conmutación por error y la supervisión de enlaces no sea suficiente por sí sola. • **Failure Condition (Condición de fallo)**: Seleccione si se produce una conmutación por error cuando alguno o todos los grupos de rutas supervisados presentan fallos al responder. *Habilite y configure una supervisión de rutas o una supervisión de enlaces para ayudar a activar una conmutación por error si una ruta o enlace se desactivan. Configure al menos un Path Group (Grupo de rutas) para la supervisión de rutas y configure al menos un Link Group (Grupo de enlaces) para la supervisión de enlaces.*
Grupo de rutas	Defina uno o más grupos de rutas para supervisar direcciones de destino específicas. Para agregar un grupo de rutas, haga clic en **Add (Añadir)** para el tipo de interfaz (**Virtual Wire**, **VLAN** o **Virtual Router (Enrutador virtual)**) y especifique lo siguiente: • **Name (Nombre)**: seleccione un cable virtual, VLAN o enrutador virtual del menú desplegable (la selección desplegable se completa dependiendo de si añade un cable virtual, VLAN o ruta de enrutador virtual). • **Enabled (Habilitado)**: Habilite el grupo de rutas. • **Failure Condition (Condición de fallo)**: Seleccione si se produce un fallo cuando alguna o todas las direcciones de destino especificadas presentan fallos al responder. • **Source IP (IP de origen)**: en el caso de interfaces de Virtual Wire y de VLAN, introduzca la dirección IP de origen utilizada en los paquetes sonda enviados al enrutador de siguiente salto (dirección IP de destino). El enrutador local debe ser capaz de enrutar la dirección al cortafuegos. La dirección IP de origen para grupos de rutas asociados a enrutadores virtuales se configurará automáticamente como la dirección IP de interfaz que se indica en la tabla de rutas como la interfaz de salida (egress) para la dirección IP de destino especificada. • **Destination IPs (IP de destino)**: Introduzca una o más direcciones de destino (separadas por comas) que se supervisarán.

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	• **Ping Interval (Intervalo de ping)**: especifique el intervalo entre los pings que se envían a la dirección de destino (el intervalo es 200-60.000 ms; el valor predeterminado es 200 ms). • **Ping Count (Recuento de pings)**: Especifique la cantidad de pings fallidos antes de declarar un fallo (el intervalo es 3-10; el valor predeterminado es 10).
Supervisión de enlaces	Especifique lo siguiente: • **Enabled (Habilitado)**: Habilite la supervisión de enlaces. La supervisión de enlaces permite activar una conmutación por error cuando falla un enlace físico o un grupo de enlaces físicos. • **Failure Condition (Condición de fallo)**: Seleccione si se produce una conmutación por error cuando alguno o todos los grupos de enlaces supervisados presentan fallos. *Habilite y configure una supervisión de rutas o una supervisión de enlaces para ayudar a activar una conmutación por error si una ruta o enlace se desactivan. Configure al menos un Path Group (Grupo de rutas) para la supervisión de rutas y configure al menos un Link Group (Grupo de enlaces) para la supervisión de enlaces.*
Link Groups	Defina uno o más grupos de enlaces para supervisar enlaces Ethernet específicos. Para añadir un grupo de enlaces, especifique los siguientes ajustes y haga clic en **Add (Añadir)**: • **Name (Nombre)**: Introduzca un nombre de grupo de enlaces. • **Enabled (Habilitado)**: Habilite el grupo de enlaces. • **Failure Condition (Condición de fallo)**: Seleccione si se produce un fallo cuando alguno o todos los enlaces seleccionados presentan fallos. • **Interfaces**: Seleccione una o más interfaces Ethernet que se supervisarán.
Pestaña Configuración Activa/Activa	
Reenvío de paquetes	Haga clic en **Enable (Habilitar)** para habilitar los peers con el fin de reenviar paquetes en el enlace de HA3 para la configuración de sesión y para la inspección de capa 7 (App-ID, Content-ID e inspección de amenazas) de sesiones enrutadas asimétricamente.
Interfaz HA3	Seleccione la interfaz de datos que planea usar para reenviar paquetes entre los peers de HA activo/activo. La interfaz que usa debe ser una interfaz de capa 2 dedicada establecida en el tipo de interfaz **HA**. *Si el enlace de HA3 falla, el peer secundario activo realizará la transición al estado no funcional. Para evitar esta condición, configure la interfaz del Grupo de agregación de enlaces (Link Aggregation Group, LAG) con dos o más interfaces físicas como el enlace de HA3. El cortafuegos no admite un enlace de copia de seguridad de HA3. Una interfaz agregada con múltiples interfaces brindará capacidad adicional y*

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	redundancia de enlaces para admitir el reenvío de paquetes entre los peers de HA. Cuando utilice la interfaz de HA3, debe activar las tramas gigantes (Jumbo Frames) en el cortafuegos y en todos los dispositivos de red intermediarios. Para habilitar las tramas gigantes, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y la opción para **Enable Jumbo Frame (Habilitar trama gigante)** en la sección Session Settings (Configuración de sesión).
Sincronización de VR	Fuerce la sincronización de todos los enrutadores virtuales configurados en los peers de HA. Use esta opción cuando el enrutador virtual no está 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.
Sincronización de QoS	Sincronice 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.
Tiempo de espera de tentativa (seg.)	Cuando falla un cortafuegos en una configuración activo/activo de HA, este entrará en estado de tentativa. La transición de estado tentativo a estado activo secundario activa el tiempo de espera de tentativa, durante el cual el cortafuegos intenta crear adyacencias de enrutamiento y completa su tabla de ruta antes de procesar cualquier paquete. Sin este temporizador, el cortafuegos de recuperación entraría en estado activo-secundario inmediatamente y bloquearía los paquetes, ya que carecería de las rutas necesarias (predeterminada es 60 segundos).
Selección de propietario de sesión	El propietario de la sesión es el responsable de toda la inspección de capa 7 (App-ID and Content-ID) para la sesión y de generar todos los logs de tráfico para la sesión. Seleccione una de las siguientes opciones para especificar cómo determinar el propietario de sesión de un paquete: • **First packet (Primer paquete)**: Seleccione esta opción para designar el cortafuegos que recibe el primer paquete en una sesión como el propietario de sesión. Esta es la configuración recomendada para minimizar el tráfico en HA3 y distribuir la carga del plano de datos en todos los peers. • **Primary Device (Dispositivo principal)**: Seleccione esta opción si desea que el cortafuegos activo principal sea el propietario de todas las sesiones. En este caso, si el cortafuegos activo secundario recibe el primer paquete, reenviará todos los paquetes que requieren la inspección de capa 7 al cortafuegos activo principal en el enlace de HA3.
Configuración de sesión	El cortafuegos responsable de la configuración de la sesión lleva a cabo el procesamiento de capa 2 a capa 4 (incluida la traducción de la dirección) y crea la entrada de tabla de la sesión. Debido a que la configuración de la sesión consume los recursos del plano de gestión, puede selecciona una de las siguientes opciones para ayudar a distribuir la carga:

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	• **Primary Device (Dispositivo principal)**: El cortafuegos activo principal configura todas las sesiones. • **IP Module (Módulo IP)**: distribuye la configuración de la sesión sobre la base de la paridad de la dirección IP de origen. • **IP Hash (Hash de IP)**: determina la configuración de sesión sobre la base de un hash de la dirección IP de origen o dirección IP de origen y destino y valor de inicialización de hash si se desea una mayor aleatorización. • **First Packet (Primer paquete)**: el cortafuegos que recibe el primer paquete realiza la configuración de sesión, incluso en los casos en donde el peer es el propietario de la sesión. Esta opción minimiza el tráfico en el enlace de HA3 y garantiza que el intenso trabajo de configurar la sesión en el plano de gestión siempre suceda en el cortafuegos que recibe el primer paquete.

Dirección virtual	Haga clic en **Add (Añadir)**, seleccione las pestañas **IPv4** o **IPv6** y luego **Add (Añadir)** de nuevo para ingresar las opciones para especificar el tipo de dirección virtual de HA a utilizar: Uso compartido de carga de ARP o IP flotante También puede combinar los tipos de direcciones virtuales en el par. Por ejemplo, puede usar el uso compartido de la carga de ARP en la interfaz LAN y una IP flotante en la interfaz web.
	• **Floating (Flotante)**: Introduzca una dirección IP que se desplazará entre los peers de HA en el caso de un fallo de enlace o sistema. Configure dos direcciones IP flotantes en la interfaz, de modo que cada cortafuegos posea una y, a continuación, establezca la prioridad. Si falla alguno de los cortafuegos, la dirección IP flotante pasa al peer de HA.
	  • **Device 0 Priority (Prioridad de dispositivo 0)**: establezca la prioridad para que el cortafuegos con ID de dispositivo 1 determine qué cortafuegos poseerá la dirección IP flotante. El cortafuegos con el valor más bajo tendrá la prioridad.
	  • **Device 1 Priority (Prioridad de dispositivo 1)**: establezca la prioridad para que el cortafuegos con ID de dispositivo 1 determine qué cortafuegos poseerá la dirección IP flotante. El cortafuegos con el valor más bajo tendrá la prioridad.
	  • **Failover address if link state is down (Dirección de conmutación por error si el estado de enlace no está operativo)**: utilice la dirección de conmutación por error cuando el estado del enlace esté desactivado en la interfaz.
	  • **Floating IP bound to the Active-Primary HA device (IP flotante vinculada al dispositivo HA activo-principal)**: seleccione esta opción para unir la dirección IP flotante con el peer activo principal. En caso de que un peer falle, el tráfico se envía continuamente al peer activo principal incluso después de que el cortafuegos con fallas se recupere y se convierta en el peer activo secundario.
	• **ARP Load Sharing (Uso compartido de carga de ARP)**: introduzca una dirección IP que compartirá el par de HA y proporcionará servicios de puerta de enlace para hosts. Esta opción solo es obligatoria si el cortafuegos está en el mismo dominio de difusión que los hosts. Seleccione **Device Selection Algorithm (Algoritmo de selección de dispositivo)**:
	  • **IP Modulo (Módulo de IP)**: seleccione el cortafuegos que responderá a las solicitudes de ARP basándose en la paridad de la dirección IP de los solicitantes de ARP.

© 2020 Palo Alto Networks, Inc.

Configuración de HA	Description (Descripción)
	• **IP Hash (Hash de IP)**: seleccione el cortafuegos que responderá a las solicitudes de ARP basándose en un hash de la dirección IP de los solicitantes de ARP.
Comandos de operación	
Suspender dispositivo local (o hacer funcionar el dispositivo local)	El siguiente comando CLI en modo de operación coloca al peer de HA local en un estado suspendido y deshabilita temporalmente la funcionalidad de HA en el cortafuegos. Si suspende el cortafuegos activo actual, el otro peer tomará el control. `request high-availability state suspend` Para volver a poner un cortafuegos suspendido en un estado funcional, utilice el siguiente comando de la CLI del modo operativo. **`request high-availability state functional`** Para probar la conmutación por error, puede desconectar el cable del cortafuegos activo (o activo-principal) o puede hacer clic en este enlace para suspender el cortafuegos activo.

© 2020 Palo Alto Networks, Inc.

Device (Dispositivo) > Log Forwarding Card (Tarjeta de reenvío de logs)

- Device (Dispositivo) > Log Forwarding Card (Tarjeta de reenvío de logs)

La tarjeta de reenvío de logs (Log Forwarding Card LFC) es una tarjeta de log de alto rendimiento que reenvía todos los logs del plano de datos (tráfico y amenazas, por ejemplo) desde el cortafuegos hacia uno o varios sistemas de creación de logs externos, tal como Panorama o un servidor syslog. Debido a que los logs del plano de datos ya no están disponibles en el cortafuegos local, la pestaña ACC se elimina de la interfaz web de gestión y Monitor Supervisar) > Logs contiene solo logs de gestión (Configuración, Sistema y Alarmas).

Debe configurar los puertos para la LFC. El puerto 1 opera a 10 Gbps y el puerto 9 opera a 40 Gbps. Configure los puertos en **Device (Dispositivo) > Log Forwarding Card (Tarjeta de reenvío de logs)**. El cortafuegos utiliza estos puertos para reenviar todos los logs del plano de datos a un sistema externo, tal como Panorama o un servidor syslog.

Consulte la Guía de referencia del hardware de la serie PA-7000 para obtener información sobre los requisitos y componentes de la LFC.

Para la interfaz de una LFC, configure los ajustes descritos en la siguiente tabla.

Configuración de la interfaz de LFC	Description (Descripción)
Nombre	Introduzca un nombre para la interfaz. Para una LFC, debe seleccionar **lfc1/1** o **lfc1/9**.
Comentarios	Introduzca una descripción opcional para la interfaz.
IPv4	Si su red use IPv4, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv4 del puerto. • **Netmask Máscara de red)**: la máscara de red para la dirección IPv4 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv4 del puerto de enlace predeterminado al puerto.
IPv6	Si su red use IPv6, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv6 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv6 del puerto de enlace predeterminado al puerto.
Velocidad de enlace	Seleccione la velocidad de interfaz en Mbps (**10000** o **40000**) o seleccione **auto (automático)** (valor predeterminado) para que el cortafuegos determine automáticamente la velocidad según la conexión. La velocidad disponible para la interfaz depende del puerto utilizado (lfc1/1 o lfc1/9). Para interfaces que tienen una velocidad que no puede configurarse, **auto (automático)** es la única opción.
estado del enlace	Seleccione si el estado de la interfaz es activada (**up (activada)**), desactivada (**down (desactivada)**) o determinado automáticamente según la conexión (**auto (automático)**). El valor predeterminado es **auto**.

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz de LFC	Description (Descripción)
Prioridad de puerto LACP	El cortafuegos solo utiliza este campo si ha activado el Protocolo de control de agregación de grupo (LACP) para el grupo de agregación. Si el número de interfaces que asigna al grupo supera el número de interfaces activas (el campo Max Ports [Puertos máx.]), el cortafuegos utiliza las prioridades del puerto LACP de las interfaces para determinar cuáles están en modo de espera. Cuanto más bajo es el número, más alta es la prioridad (intervalo 1-65.535; predeterminado 32.768).

Las subinterfaces están disponibles si tiene la opción multi-vsys (múltiples sistemas virtuales) habilitada. Para configurar una subinterfaz de LFC, añada una subinterfaz y utilice la configuración que se describe en la siguiente tabla.

Configuración de la subinterfaz de LFC	Description (Descripción)
Nombre de interfaz	El campo **Interface Name (Nombre de interfaz)** (solo lectura) muestra el nombre de la interfaz de tarjeta log que ha seleccionado. En el campo adyacente, introduzca un sufijo numérico (1-9.999) para identificar la subinterfaz.
Comentarios	Introduzca una descripción opcional para la interfaz.
Tag (Etiqueta)	Introduzca la **Tag (Etiqueta)** VLAN (0-4.094) para la subinterfaz. *Por comodidad, lo recomendable es que el número de la etiqueta sea igual que el de la subinterfaz.*
Sistema virtual	Seleccione el sistema virtual (vsys) al que se asigna la subinterfaz de la tarjeta de reenvío de logs (LFC). Alternativamente, puede hacer clic en **Virtual Systems (Sistemas virtuales)** para añadir un nuevo vsys. Una vez que una subinterfaz de LPC se asigna a un sistema virtual, esa interfaz se usa como interfaz de origen para todos los servicios que reenvían logs (syslog, correo electrónico, SNMP) desde la tarjeta de logs.
IPv4	Si su red use IPv4, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv4 del puerto. • **Netmask Máscara de red)**: la máscara de red para la dirección IPv4 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv4 del puerto de enlace predeterminado al puerto.
IPv6	Si su red use IPv6, defina lo siguiente: • **IP address (Dirección IP)**: dirección IPv6 del puerto. • **Default Gateway (Puerta de enlace predeterminada)**: la dirección IPv6 del puerto de enlace predeterminado al puerto.

© 2020 Palo Alto Networks, Inc.

Device > Config Audit

Seleccione **Device (Dispositivo)** > **Config Audit (Configuración de auditoría)** para ver las diferencias entre los archivos de configuración. La página muestra las configuraciones lado a lado en paneles separados y resalta las diferencias línea por línea con colores para indicar lo añadido (verde), modificado (amarillo) o eliminado (rojo).

Added	Modified	Deleted

Configuración de parámetros de auditoría	Description (Descripción)
Menús desplegables de nombre de configuración (sin etiquetas)	Seleccione dos configuraciones a comparar en los menús desplegables de nombre de configuración (sin etiqueta) (los valores predeterminados son **Running config (Ejecutando configuración)** y **Candidate config [Configuración candidata]**). *Puede filtrar un menú desplegable ingresando una secuencia de texto derivada del valor de Description de la operación de confirmación asociada con la configuración deseada (consulte Confirmar cambios).*
Menú desplegable de contexto	Use el menú desplegable **Context (Contexto)** para especificar el número de líneas a mostrar antes y después de las diferencias resaltadas en cada archivo. Especificar más líneas puede ayudarlo a correlacionar los resultados de auditoría de las configuraciones en la interfaz web. Si configura **Context (Contexto)** en **All (Todos)**, los resultados incluirán los archivos completos de configuración.
Ir	Haga clic en **Go (Iniciar)** para iniciar la auditoría.
Anterior (<<) y Siguiente (>>)	Estas flechas de navegación se habilitan cuando se seleccionan versiones de configuración consecutivas en los menús desplegables del nombre de configuración. Haga clic en << para comprar el par anterior de configuraciones en el menú desplegable o haga clic en >> para comparar el siguiente par de configuraciones.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Perfiles de la contraseña

- Dispositivo > Perfiles de la contraseña
- Panorama > Password Profiles

Seleccione **Device (Dispositivo)** > **Password Profiles (Perfiles de contraseña)** o **Panorama** > **Password Profiles (Perfiles de contraseña)** para configurar los requisitos de contraseña básicos de las cuentas locales individuales. Los perfiles de contraseña anulan cualquier ajuste de Complejidad mínima de la contraseña que haya definido para todas las cuentas locales (**Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]**).

Para aplicar un perfil de contraseña a una cuenta, seleccione **Device (Dispositivo)** > **Administrators (Administradores)** (cortafuegos) o **Panorama** > **Administrators (Administradores)** (Panorama), seleccione una cuenta y, a continuación, seleccione **Password Profile (Perfil desplegable)**.

No puede asignar perfiles de contraseña a cuentas administrativas que usan autenticación de base de datos local (consulte Device > Local User Database > Users).

Para crear un perfil de contraseña, haga clic en **Add (Añadir)** y especifique la información en la siguiente tabla.

Configuración de perfil de contraseña	Description (Descripción)
Nombre	Introduzca un nombre para identificar el perfil de contraseña (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Required Password Change Period (Período necesario para el cambio de contraseña) (días)	Exija que los administradores cambien su contraseña con la regularidad especificada por un número de días establecido (el intervalo 0-365 días). Por ejemplo, si el valor se establece como 90, se pedirá a los administradores que cambien su contraseña cada 90 días. También puede establecer una advertencia de vencimiento de 0-30 días y especificar un período de gracia.
Expiration Warning Period (Período de advertencia de vencimiento) (días)	Si se establece un período necesario para el cambio de contraseña, este ajuste puede utilizarse para pedir al usuario que cambie su contraseña cada vez que inicie sesión a medida que se acerque la fecha obligatoria de cambio de contraseña (el intervalo es 0-30).
Recuento de inicio de sesión de gestor posterior al vencimiento	Permita que el administrador inicie sesión el número de veces especificado después de que su cuenta haya vencido. Por ejemplo, si el valor se ha establecido como 3 y su cuenta ha vencido, podrá iniciar sesión 3 veces más antes de que se bloquee la cuenta (el intervalo es 0-3).
Período de gracia posterior al vencimiento (días)	Permita que el administrador inicie sesión el número de días especificado después de que su cuenta haya vencido (intervalo es 0-30).

Requisitos de nombre de usuario y contraseña

La tabla siguiente enumera los caracteres válidos que se pueden utilizar en nombres de usuario y contraseñas para cuentas de PAN-OS y Panorama.

© 2020 Palo Alto Networks, Inc.

Tipo de cuenta	Restricciones de nombre de usuario y contraseña
Conjunto de caracteres de contraseña	No hay ninguna restricción en los conjuntos de caracteres de los campos de contraseña.
Administrador remoto, VPN SSL o portal cautivo	Los siguientes caracteres no están permitidos para el nombre de usuario: • Acento grave (`) • Corchetes angulares (< y >) • Y comercial (&) • Asterisco (*) • Arroba (@) • Signos de interrogación (¿ y ?) • Barra vertical (|) • Comilla simple (') • Punto y coma (;) • Comilla doble (") • Signo del dólar ($) • Paréntesis ('(' and ')') • Dos puntos (:)
Cuentas de administrador locales	Los siguientes son los caracteres permitidos para los nombres de usuario locales: • Minúsculas (a-z) • Mayúsculas (A-Z) • Números (0-9) • Guión bajo (_) • Punto (.) • Guión (-) *Los nombres de inicio de sesión no pueden empezar por guión (-).*

© 2020 Palo Alto Networks, Inc.

Device > Administrators

Las cuentas de administrador controlan el acceso a cortafuegos y Panorama. Un administrador de cortafuegos puede tener acceso completo o de solo lectura a un único cortafuegos o a un sistema virtual en un único cortafuegos. Los cortafuegos tienen una cuenta de **admin (administrador)** predefinida con acceso completo.

Para definir los administradores de Panorama, consulte Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen).

Se admiten las siguientes opciones de autenticación:

- Autenticación con contraseña: el administrador introduce un nombre de usuario y una contraseña para iniciar sesión. No se necesitan certificados. Puede utilizar este método junto con los perfiles de autenticación o para la autenticación de base de datos local.
- Autenticación con certificado de cliente (web): Esta autenticación no necesita nombre de usuario o contraseña; el certificado será suficiente para autenticar el acceso al cortafuegos.
- Autenticación con clave pública (SSH): El administrador genera un par de claves pública y privada en la máquina que requiere acceso al cortafuegos y, a continuación, carga la clave pública en el cortafuegos para permitir un acceso seguro sin exigir que el administrador introduzca un nombre de usuario y una contraseña.

Para añadir un administrador, haga clic en **Add (Añadir)** y especifique la siguiente información.

Configuración de cuentas de administrador	Description (Descripción)
Nombre	Introduzca un nombre de inicio de sesión para el administrador (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice únicamente letras, números, guiones, puntos y guiones bajos. Los nombres de inicio de sesión no pueden empezar por guión (-).
Perfil de autenticación	Seleccione un perfil de autenticación para la autenticación del administrador. Este ajuste se puede utilizar para RADIUS, TACACS+, LDAP, Kerberos, SAML o la autenticación de base de datos local. Para obtener más información, consulte Device > Authentication Profile.
Utilizar solo la autenticación con certificado de cliente (web)	Seleccione esta opción para utilizar la autenticación con certificado de cliente para el acceso web. Si selecciona esta opción, no es necesario ni el nombre de usuario ni la contraseña; el certificado es suficiente para autenticar el acceso al cortafuegos.
Nueva contraseña Confirmar nueva contraseña	Introduzca y confirme una contraseña que haga distinción entre mayúsculas y minúsculas para el administrador (de hasta 31 caracteres). También puede seleccionar **Setup (Configuración)** > **Management (Gestión)** para aplicar una longitud mínima de la contraseña.

© 2020 Palo Alto Networks, Inc.

Configuración de cuentas de administrador	Description (Descripción)
	Para garantizar la seguridad de la interfaz de gestión del cortafuegos, se recomienda cambiar periódicamente las contraseñas administrativas utilizando una mezcla de minúsculas, mayúsculas y números. También puede configurar los parámetros de complejidad mínima de contraseña de todos los administradores en el cortafuegos.
Utilizar autenticación de clave pública (SSH)	Seleccione esta opción para utilizar la autenticación con clave pública SSH. Haga clic en **Import Key (Importar clave)** y explore para seleccionar el archivo de clave pública. La clave cargada se muestra en el área de texto de solo lectura. Los formatos de archivo de clave admitidos son IETF SECSH y OpenSSH. Los algoritmos de clave admitidos son DSA (1.024 bits) y RSA (de 768 a 4.096 bits). *Si falla la autenticación de clave pública, el cortafuegos solicita al administrador el nombre de usuario y la contraseña.*
Tipo de administrador	Asigne una función a este administrador. La función determina lo que el administrador puede ver y modificar. Si selecciona **Role Based (Basado en función)**, seleccione un perfil de función personalizado en el menú desplegable. Para obtener más información, consulte Device > Admin Roles. Si selecciona **Dynamic (Dinámica)**, puede seleccionar una de las siguientes funciones predefinidas: • **superuser (superusuario)**: tiene acceso completo al cortafuegos y puede definir nuevas cuentas de administrador y sistemas virtuales. Debe tener los privilegios de superusuario para crear un usuario de administrador con los privilegios de superusuario. • **Superuser (Superusuario)**(solo lectura): tiene acceso de solo lectura al cortafuegos. • **deviceadmin**: tiene acceso completo a todas las configuraciones del cortafuegos excepto para definir nuevas cuentas o sistemas virtuales. • **Device administrator (Administrador de dispositivo)** (solo lectura): tiene acceso de solo lectura a todas las configuraciones excepto a los perfiles de contraseña (sin acceso) y a las cuentas del administrador (solo la cuenta de acceso está visible). • **Virtual Administrador de sistemas virtuales**: tiene acceso a determinados sistemas virtuales del cortafuegos para crear y gestionar aspectos concretos de dichos sistemas (si está habilitada la opción de Capacidad de varios sistemas virtuales). Los administradores de sistemas virtuales no tienen

© 2020 Palo Alto Networks, Inc.

Configuración de cuentas de administrador	Description (Descripción)
	acceso a las interfaces de red, los enrutadores virtuales, los túneles de IPSec, las VLAN, los cables virtuales, los túneles de GRE, los perfiles de red, el proxy DNS, DHCP, QoS ni LLDP. • **Administrador de sistemas virtuales** (solo lectura): tiene acceso de solo lectura a determinados sistemas virtuales del cortafuegos para ver aspectos concretos de dichos sistemas (si está habilitada la opción de Capacidad de varios sistemas virtuales). Los administradores de sistemas virtuales con acceso de solo lectura no tienen acceso a las interfaces de red, los enrutadores virtuales, los túneles de IPSec, las VLAN, los cables virtuales, los túneles de GRE, el proxy DNS, DHCP, QoS, LLDP o perfiles de red.
Sistema virtual (Administrador de sistema virtual únicamente)	Haga clic en **Add (Añadir)** para seleccionar los sistemas virtuales que el administrador puede gestionar.
perfil de contraseña	Seleccione el perfil de contraseña, si es aplicable. Para crear un nuevo perfil de contraseña, consulte Device > Password Profiles. *Cree un perfil de contraseña para los administradores para garantizar que las contraseñas de los administradores caduquen después de un periodo configurado. El cambio periódico de las contraseñas de los administradores ayuda a prevenir que los atacantes utilicen las credenciales guardadas o robadas.*

© 2020 Palo Alto Networks, Inc.

Device > Admin Roles

Seleccione **Device (Dispositivo)** > **Admin Roles (Funciones de administrador)** para definir los perfiles de funciones del administrador, las cuales son funciones personalizadas que determinan los privilegios de acceso y las responsabilidades de los usuarios administrativos. Asigne perfiles de función de administrador o funciones dinámicas cuando cree cuentas administrativas (Device [Dispositivo] > Administrators [Administradores]).

Para definir perfiles de funciones de administrador para los administradores de Panorama, consulte Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)*.*

El cortafuegos tiene tres funciones predefinidas que puede usar con fines comunes. Primero utiliza la función Superusuario para la configuración inicial del cortafuegos y para crear las cuentas de administrador para el administrador de seguridad, el administrador de auditoría y el administrador criptográfico. Luego cree estas cuentas y aplique las funciones de administrador con los criterios comunes correctos, después inicie sesión utilizando estas cuentas. La cuenta superusuario predeterminada en el modo FIPS-CC, Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) y Criterios comunes (Common Criteria, CC), es **admin** y la contraseña predeterminada es **paloalto**. En el modo de funcionamiento estándar, la contraseña predeterminada de **admin** es **admin**. Las funciones de administrador predefinidas se han creado donde las capacidades no se solapan, excepto en que todas tienen un acceso de solo lectura a la traza de auditoría (excepto el administrador de auditoría con acceso de lectura/eliminación completo). Estas funciones de administrador no se pueden modificar y se definen de la manera siguiente:

- Administrador de auditoría: El administrador de auditoría es responsable de la revisión regular de los datos de auditoría del cortafuegos.
- Administrador criptográfico: El administrador criptográfico es responsable de la configuración y el mantenimiento de los elementos criptográficos relacionados con el establecimiento de conexiones seguras con el cortafuegos.
- Administrador de seguridad: El administrador de seguridad es responsable del resto de tareas administrativas (por ejemplo, la creación de la política de seguridad) no asumidas por las otras dos funciones administrativas.

Para añadir un perfil de funciones de administrador, haga clic en **Add (Añadir)** y especifique la configuración que se describe en la siguiente tabla.

Cree funciones personalizadas para limitar el acceso del administrador únicamente a lo que necesita cada tipo de administrador. Para cada tipo de administrador, habilite, deshabilite o configure el acceso de solo lectura para el acceso IU web, API XML/REST y Línea de comandos.

Configuración de funciones de administrador	
Nombre	Introduzca un nombre para identificar esta función de administrador (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	(Opcional) Introduzca una descripción de la función (hasta 255 caracteres).
Función	Seleccione el ámbito de responsabilidad administrativa: • **Device (Dispositivo)**: la función se aplica al cortafuegos completo, independientemente de si tiene más de un sistema virtual (vsys).

© 2020 Palo Alto Networks, Inc.

Configuración de funciones de administrador	
	• **Sistema virtual**: la función se aplica a determinados sistemas virtuales del cortafuegos a aspectos concretos de dichos sistemas (si está habilitada la opción de Capacidad de varios sistemas virtuales). Un perfil de función de administración basado en **Virtual System** (Sistema virtual) no tiene acceso en la pestaña **Web UI (Interfaz de usuario web)** a las interfaces de red, las VLAN, los cables virtuales, los túneles de IPSec, los túneles de GRE, DHCP, el proxy DNS, QoS, LLDP o los perfiles de red. Seleccione los sistemas virtuales cuando cree cuentas administrativas (Device [Dispositivo] > Administrators [Administradores]).
WebUI (Interfaz de usuario web)	Haga clic en los iconos de funciones de interfaz web específicas para establecer los privilegios de acceso permitidos: • **Enable (Habilitar)**: acceso de lectura/escritura a la función seleccionada. • **Read Only (Solo lectura)**: acceso de solo lectura a la función seleccionada. • **Disable (Deshabilitar)**: sin acceso a la función seleccionada.
API REST/XML	Haga clic en los iconos de funciones XML/REST API específicas para establecer los privilegios de acceso permitidos (**Habilitar** o **Deshabilitar**).

Línea de comandos	Seleccione el tipo de función para el acceso a la CLI: El ajuste predeterminado **None (Ninguno)**, lo significa que el acceso a la CLI no está permitido. Las demás opciones varían según el alcance de la función determinado en Role:
	• **Dispositivo**
	  • **superuser (superusuario)**: tiene acceso completo al cortafuegos y puede definir nuevas cuentas de administrador y sistemas virtuales. Debe tener los privilegios de superusuario para crear un usuario de administrador con los privilegios de superusuario.
	  • **superreader (superlector)**: tiene acceso de solo lectura al cortafuegos.
	  • **deviceadmin**: tiene acceso completo a todas las configuraciones del cortafuegos excepto para definir nuevas cuentas o sistemas virtuales.
	  • **devicereader**: tiene acceso de solo lectura a todas las configuraciones excepto a los perfiles de contraseña (sin acceso) y a las cuentas del administrador (solo la cuenta de acceso está visible).
	• **Sistema virtual**
	  • **vsysadmin (administrador de sistemas virtuales)**: tiene acceso a determinados sistemas virtuales del cortafuegos para crear y gestionar aspectos concretos de dichos sistemas. La configuración **vsysadmin** no controla las funciones de nivel de cortafuegos o de red (como el enrutamiento estático y dinámico, las direcciones IP de interfaces, los túneles de IPSec, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de GRE, DHCP, el DNS de proxy, QoS, LLDP o los perfiles de red).
	  • **vsysreader** : tiene acceso de solo lectura a determinados sistemas virtuales del cortafuegos y a aspectos concretos de dichos sistemas. La configuración **vsysreader** no dispone de acceso a las funciones de nivel de cortafuegos o de red (como el enrutamiento estático y

© 2020 Palo Alto Networks, Inc.

Configuración de funciones de administrador	
	dinámico, las direcciones IP de interfaces, los túneles de IPSec, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de GRE, DHCP, el DNS de proxy, QoS, LLDP o los perfiles de red).

© 2020 Palo Alto Networks, Inc.

Device > Access Domain

- Device > Access Domain

Configure los dominios de acceso para restringir el acceso del administrador a sistemas virtuales específicos en el cortafuegos. El cortafuegos admite dominios de acceso solo si utiliza un servidor RADIUS, TACACS+ o servidor de identidad SAML (IdP) para gestionar la autenticación y la autorización del administrador. Para habilitar los dominios de acceso, debe definir:

- Un perfil de servidor para el servidor de autenticación externo: consulte Device > Server Profiles > RADIUS, Device > Server Profiles > TACACS+, Y Device > Server Profiles > SAML Identity Provider.
- Atributos específicos del proveedor (VSA) RADIUS, TACACS VSAs o Atributos SAML.

Cuando un administrador intenta iniciar sesión en el cortafuegos, este consulta al servidor externo acerca del dominio de acceso del administrador. El servidor externo devuelve el dominio asociado y el cortafuegos restringe al administrador a los sistemas virtuales que especificó en el dominio de acceso. Si el cortafuegos no utiliza un servidor externo para autenticar y autorizar administradores, los ajustes de **Device (Dispositivo)** > **Access Domain (Dominio de acceso)** se ignoran.

En Panorama, puede administrar los dominios de acceso localmente o mediante los atributos RADIUS VSA, TACACS+ VSA o SAML (consulte Panorama > Access Domains*).*

Configuración de dominio de acceso	Description (Descripción)
Nombre	Introduzca un nombre para el dominio de acceso (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice únicamente letras, números, guiones, guiones bajos y puntos.
Virtual Systems	Seleccione sistemas virtuales en la columna Disponibles y haga clic en **Add (Añadir)** para seleccionarlos. Los dominios de acceso únicamente son compatibles en cortafuegos que admiten sistemas virtuales.

© 2020 Palo Alto Networks, Inc.

Device > Authentication Profile

Utilice esta página para configurar la configuración para autenticar administradores y usuarios finales. El cortafuegos y Panorama son compatibles con servicios de autenticación locales, RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0 y autenticación de múltiples factores (MFA).

Cree al menos un perfil de autenticación para proporcionar autenticación externa, lo cual mantiene todas las solicitudes de autenticación en el mismo lugar para facilitar la gestión y utiliza un proceso de autenticación estándar que incluye servicios tales como seguimiento. Se recomienda crear y establecer la prioridad (Device [Dispositivo] > Authentication Sequence [Secuencia de autenticación]) de varios perfiles de autenticación usando diferentes métodos en caso de fallo de autenticación, y crear al menos una cuenta de inicio de sesión local a la cual volver si todos los métodos externos fallan.

También puede utilizar esta página para registrar un cortafuegos o servicio de Panorama (como el acceso administrativo a la interfaz web) con un proveedor de identidad SAML (IdP). El registro del servicio permite al cortafuegos o Panorama utilizar IdP para autenticar a los usuarios que solicitan el servicio. El servicio se registra introduciendo sus metadatos SAML en el IdP. El cortafuegos y Panorama hacen que el registro sea fácil al generar automáticamente un archivo de metadatos SAML basado en el perfil de autenticación que asignó al servicio; puede exportar este archivo de metadatos al IdP.

- Perfil de autenticación
- Exportación de metadatos SAML desde un perfil de autenticación

Perfil de autenticación

- Device > Authentication Profile

Seleccione **Device (Dispositivo)** > **Authentication Profile (Perfil de autenticación)** o **Panorama** > **Authentication Profile (Perfil de autenticación)** para gestionar perfiles de autenticación. Para crear un perfil nuevo, haga clic en **Add (Añadir)** y complete los siguientes campos.

Después de configurar un perfil de autenticación, use el comando CLI ***`test authentication`*** *para determinar si el cortafuegos o servidor de gestión Panorama puede comunicarse con el servicio de autenticación de back-end y si la solicitud de autenticación se realizó correctamente. Puede realizar pruebas de autenticación con la configuración candidata para determinar cuál es la configuración correcta antes de confirmarla.*

Configuración del perfil de autenticación	Description (Descripción)
Nombre	Introduzca un nombre para identificar el perfil. El nombre distingue entre mayúsculas y minúsculas, puede tener hasta 31 caracteres, incluidas letras, números, espacios, guiones, guiones bajos y puntos. El nombre debe ser exclusivo en la **Location (Ubicación actual)** (cortafuegos o sistema virtual) en relación con otros perfiles de autenticación y secuencias de autenticación. *En un cortafuegos en modo de sistemas virtuales múltiples, si la Location (ubicación) del perfil de autenticación es un sistema virtual, no introduzca el mismo nombre como secuencia de autenticación en la ubicación Compartido. Del mismo modo, si el perfil Location (ubicación) está compartido, no introduzca el mismo nombre como secuencia en un sistema virtual. Aunque*

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	se puede confirmar un perfil de autenticación y una secuencia con los mismos nombres en estos casos, se pueden producir errores de referencia.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Pestaña Autenticación El cortafuegos invoca el servicio de autenticación que configura en esta pestaña antes de invocar cualquier servicio de autenticación multifactor (MFA) que agregue en la Pestaña Factores. *Si el cortafuegos se integra con un proveedor de MFA a través de RADIUS en lugar de la API de proveedor, debe configurar un perfil de servidor RADIUS para ese proveedor, no un perfil de servidor MFA.*	
Tipo	Seleccione el tipo de servicio que proporcione el primer (y Opcionalmente el único) desafío de autenticación que los usuarios ven. En función de su selección, el cuadro de diálogo muestra otras configuraciones que define para el servicio. Las opciones son las siguientes: • **None (Ninguna)**: No utilice ninguna autenticación del cortafuegos. • **Local Database (Base de datos local)**: Utilice la base de datos de autenticación del cortafuegos. Esta opción no está disponible en Panorama. • **RADIUS**: Utilice un servidor de Servicio de autenticación remota telefónica de usuario (RADIUS). • **TACACS+**: Utilice un servidor de Sistema de control de acceso del controlador de acceso a terminales (TACACS+). • **LDAP**: Utilice un servidor de Protocolo ligero de acceso a directorios(LDAP). • **Kerberos**: Utilice un servidor Kerberos. • **SAML**: Utilice un proveedor de identidad del lenguaje de marcado de seguridad Assertion 2.0 (SAML 2.0) (IdP). *Los administradores pueden utilizar SAML para autenticarse en el cortafuegos o en la interfaz web Panorama, pero no en la CLI.*
Perfil de servidor (RADIUS, TACACS, LDAP o Kerberos solamente)	Seleccione el perfil del servidor de autenticación en la lista desplegable. Consulte Dispositivo > Perfiles de servidor > RADIUS, Dispositivo > Perfiles de servidor > TACACS+, Dispositivo > Perfiles de servidor > LDAP o Dispositivo > Perfiles de servidor > Kerberos.
IdP Server Profile (Sólo SAML)	Seleccione el perfil del servidor SAML Identity Provider en el menú desplegable. Consulte Device (Dispositivo) > Server Profiles (Perfiles de servidor) > SAML Identity Provider (Proveedor de identidad SAML).

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
Retrieve user group from RADIUS (Recuperar grupo de usuarios de RADIUS) (Sólo RADIUS)	Seleccione esta opción para recopilar información de grupos de usuarios de Atributos específicos del proveedor (VSA) definidos en el servidor RADIUS. El cortafuegos utiliza la información para hacer coincidir los usuarios de autenticación con entradas de la Lista de permitidas, no para hacer cumplir las políticas o generar informes.
Recuperar grupo de usuarios de TACACS + (Sólo TACACS)	Seleccione esta opción para recopilar información del grupo de usuarios de Atributos específicos del proveedor (VSA) definidos en el servidor TACACS +. El cortafuegos utiliza la información para hacer coincidir los usuarios de autenticación con entradas de la Lista de permitidas, no para hacer cumplir las políticas o generar informes.
Atributo de inicio de sesión (Sólo LDAP)	Introduzca un atributo de directorio LDAP que identifique exclusivamente al usuario y que actúe como ID de inicio de sesión para ese usuario.
Aviso de caducidad de contraseña (Sólo LDAP)	Si el perfile de autenticación es para usuarios de GlobalProtect, defina con cuántos días de antelación antes del vencimiento de la contraseña empezarán a mostrarse mensajes de notificación a los usuarios para alertarles de que sus contraseñas vencen en x número de días. De forma predeterminada, los mensajes de notificación se mostrarán 7 días antes de la caducidad de la contraseña (el intervalo es 1255). Los usuarios no podrán acceder a la VPN si las contraseñas caducan. *Plantéese configurar los agentes de GlobalProtect para que utilicen el método de conexión anterior al inicio de sesión. Esto permitirá a los usuarios conectarse al dominio para cambiar sus contraseñas incluso aunque la contraseña haya caducado.* Si los usuarios dejan caducar sus contraseñas, el administrador puede asignar una contraseña de LDAP temporal que permita a los usuarios iniciar sesión en la VPN. En este flujo de trabajo, se recomienda establecer el campo **Authentication Modifier (Modificador de autenticación)** en la configuración del portal a **Cookie authentication for config refresh (Autenticación de cookies para la actualización de configuración)** (de lo contrario, la contraseña temporal se utilizará para autenticarse en el portal, pero el inicio de sesión de la puerta de enlace fallará, lo que evitará el acceso a la VPN).
Certificado para solicitudes de firma (Sólo SAML)	Seleccione el certificado que el cortafuegos utilizará para firmar los mensajes SAML que envía al proveedor de identidad (IdP). Este campo es obligatorio si habilita la opción **Firmar mensaje de SAML al IdP** en el **Perfil del servidor IdP** (consulte Dispositivo > Perfiles de servidor > Proveedor de identidad SAML). De lo contrario, seleccionar un certificado para firmar mensajes SAML es opcional. Al generar o importar un certificado y su clave privada asociada, los atributos de uso de clave especificados en el certificado controlan cómo puede utilizar la clave: • Si el certificado enumera explícitamente atributos de uso de clave, uno de los atributos debe ser Firma digital, que no está disponible en los certificados

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	que genera en el cortafuegos En este caso, debe Importar el certificado y la clave de su entidad emisora de certificados de empresa (CA) o de una entidad emisora de certificados de terceros. • Si el certificado no especifica los atributos de uso de clave, puede utilizar la clave para cualquier propósito, incluida la firma de mensajes. En este caso, puede utilizar cualquier método para Obtener el certificado y la clave para firmar mensajes SAML. *Palo Alto Networks recomienda utilizar un certificado de firma para garantizar la integridad de los mensajes SAML enviados al IdP.*
Habilitar cierre de sesión único (Sólo SAML)	Seleccione esta opción para permitir a los usuarios cerrar sesión de cada servicio autenticado cerrando sesión de cualquier servicio único. El inicio de sesión único (SLO) sólo se aplica a los servicios a los que se accede mediante autenticación SAML. Los servicios pueden ser externos a su organización o internos (como la interfaz web del cortafuegos). Esta opción sólo se aplica si ha introducido un **Identity Provider SLO URL (Proveedor de Identidad URL de SLO)** en el Perfil del servidor IdP. No puede habilitar SLO para los usuarios del portal cautivo. *Después de cerrar la sesión, el cortafuegos elimina automáticamente sus asignaciones de dirección IP a nombre de usuario.*
Perfil del certificado (Sólo SAML)	Seleccione el perfil de certificado que el cortafuegos utilizará para validar: • el **Identity Provider Certificate (Certificado de Proveedor de Identidad)** especificado en el Perfil del servidor IdP. El IdP utiliza este certificado para autenticarse en el cortafuegos. El cortafuegos valida el certificado cuando se hace clic en **Commit (Confirmar)** para confirmar la configuración del perfil de autenticación. • Mensajes SAML que el IdP envía al cortafuegos para la autenticación de inicio de sesión único (SSO) y de cierre de sesión único (SLO). El IdP utiliza la **Identity Provider Certificate (Certificado de Proveedor de Identidad)** especificado en el Perfil del servidor IdP para firmar los mensajes. Consulte Device > Certificate Management > Certificate Profile.
Dominio de usuario y Modificador de nombre de usuario (Todos los tipos de autenticación excepto SAML)	El cortafuegos utiliza el **User Domain (Dominio de usuario)** para hacer coincidir los usuarios de autenticación con las entradas de la Lista de permitidas y para la asignación de grupos a ID de usuarios. Puede especificar un **Username Modifier (Modificador de nombre de usuario)** para modificar la cadena de dominio/nombre de usuario que introduce un usuario durante el inicio de sesión. El servidor de seguridad utiliza la cadena modificada para la autenticación. Seleccione entre las siguientes opciones: • Parar enviar solamente la información de usuario sin modificar, dejar en blanco el **User Domain (Dominio de usuario)** (predeterminado) y definir el **Username Modifier (Modificador de nombre de usuario)** con la variable **%USERINPUT%** (predeterminado).

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	• Para que un dominio preceda a la entrada del usuario, introduzca **User Domain (Dominio de usuario)** y defina **Username Modifier (Modificador de nombre de usuario)** como **%USERDOMAIN%\%USERINPUT%**. • Para anexar un dominio a la entrada del usuario, introduzca un **User Domain (Dominio de usuario)** y defina **Username Modifier (Modificador de nombre de usuario)** como **%USERINPUT%@%USERDOMAIN%**. *Si el Username Modifier (Modificador de nombre de usuario) incluye la variable %USERDOMAIN%, el valor User Domain (Dominio de usuario) sustituye a cualquier cadena de dominio que introduzcan los usuarios. Si especifica la variable %USERDOMAIN% y deja en blanco User Domain (Dominio de usuario), el cortafuegos elimina todas las cadenas de dominio introducidas por usuarios. El cortafuegos resuelve nombres de dominio con el nombre NetBIOS adecuado para la asignación de grupos de User-ID. Esto se aplica tanto para dominios principales como secundarios. Los modificadores User Domain (Dominio de usuario) tiene prioridad con respecto a nombres NetBIOS derivados automáticamente.* • Para permitir que el cortafuegos utilice el tipo de perfil de servidor para determinar el cómo y el cuándo en la secuencia de autenticación para modificar el formato de la entrada del usuario, especifique manualmente `Ninguno` como **Modificador de nombre de usuario**. Para obtener más información sobre esta opción, consulte Configuración de una secuencia y perfil de autenticación en la Guía del administrador de PAN-OS.
Dominio de Kerberos (Todos los tipos de autenticación excepto SAML)	Si su red es compatible con el registro único (SSO) de Kerberos, introduzca el **Kerberos Realm (Dominio de Kerberos)** (hasta 127 caracteres). Corresponde al nombre de host del nombre de inicio de sesión del usuario. Por ejemplo, en el nombre de cuenta de usuario usuario@EJEMPLO.LOCAL, el dominio es EJEMPLO.LOCAL.
Keytab de Kerberos (Todos los tipos de autenticación excepto SAML)	Si su red es compatible con el registro único (SSO) de Kerberos, haga clic en **Import (Importar)** y luego en **Browse (Navegar)** para buscar el archivo keytab; a continuación, haga clic en **OK (Aceptar)**. Un keytab contiene la información de cuenta de Kerberos (nombre principal y contraseña con hash) para el cortafuegos, necesaria para la autenticación SSO. Cada perfil de autenticación puede tener un keytab. Durante la autenticación, el cortafuegos intenta primero usar el keytab para establecer SSO. Si lo logra y el usuario que intenta acceder está en la Allow List, la autenticación es inmediata. De lo contrario, el proceso de autenticación se revierte a autenticación manual (nombre de usuario/contraseña) del **Type (tipo)** especificado, que no tiene por qué ser Kerberos. *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. No obstante, si el algoritmo en el keytab no coincide con el algoritmo del vale de servicio que el servicio de concesión de vales emite para habilitar a los clientes para SSO, fallará*

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	el proceso SSO. Su administrador de Kerberos determina qué algoritmos usan los tickets de servicio.
Atributo de nombre de usuario (Sólo SAML)	Introduzca el atributo SAML que identifica el nombre de usuario de un usuario de autenticación en los mensajes del IdP (por defecto es **username (nombre de usuario)**). Si el **IdP Server Profile (Perfil del servidor IdP)** contiene metadatos que especifican un atributo de nombre de usuario, el cortafuegos rellenará automáticamente este campo con ese atributo. El cortafuegos comparará los nombres de usuario recuperados de los mensajes SAML con los usuarios y grupos de usuarios en la **Allow List (Lista de permitidas)** del perfil de autenticación. Debido a que no se puede configurar el cortafuegos para modificar la cadena de dominio / nombre de usuario que un usuario introduce durante los inicios de sesión de SAML, el nombre de usuario de inicio de sesión debe coincidir exactamente con la entrada de la **Allow List (Lista de permitidas)**. Este es el único atributo SAML que es obligatorio. *Los mensajes SAML pueden mostrar el nombre de usuario en el campo de asunto. El cortafuegos comprueba automáticamente el campo de asunto si el atributo de nombre de usuario no muestra el nombre de usuario.*
Atributo de grupo de usuarios (Sólo SAML)	Introduzca el atributo SAML que identifique el grupo de usuarios de un usuario de autenticación en los mensajes del IdP (por **grupo de usuario**). Si el **IdP Server Profile (Perfil del servidor IdP)** contiene metadatos que especifica un atributo de grupo de usuarios, el campo utiliza automáticamente ese atributo. El cortafuegos utiliza la información de grupo para hacer coincidir los usuarios de autenticación con **Allow List (Lista de permitidas)** Entradas, no para políticas o informes.
Atributo de función de administrador (Sólo SAML)	Introduzca el atributo SAML que identifica la función de administrador de un usuario de autenticación en los mensajes del IdP (por defecto es **Papel de administrador**). Este atributo sólo se aplica a los administradores de cortafuegos, no a los usuarios finales. Si el **IdP Server Profile (Perfil del servidor IdP)** Contiene metadatos que especifican un atributo admin-role, el cortafuegos rellena automáticamente este campo con ese atributo. El cortafuegos coincide con sus funciones predefinidas (dinámicas) o perfiles de funciones de administración con las funciones recuperadas de los mensajes SAML para reforzar el control de acceso basado en roles. Si un mensaje SAML tiene varios valores de rol de administración para un administrador con un solo rol, la coincidencia sólo se aplica al primer valor (de la izquierda) en el atributo de rol de administración. Para un administrador con más de un rol, la coincidencia puede aplicarse a varios valores en el atributo.
Atributo de dominio de acceso (Sólo SAML)	Introduzca el atributo SAML que identifica el dominio de acceso de un usuario de autenticación en los mensajes del IdP (por **Dominio de acceso**). Este atributo sólo se aplica a los administradores de cortafuegos, no a los usuarios finales. Si el **IdP Server Profile (Perfil del servidor IdP)** Contiene metadatos que especifiquen un atributo de dominio de acceso, el cortafuegos rellenará automáticamente este campo con ese atributo. El cortafuegos comparará sus dominios de acceso configurados localmente con los recuperados de los mensajes SAML para aplicar el control de acceso. Si un mensaje SAML tiene

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	varios valores de dominio de acceso para un administrador con solo un dominio de acceso, la coincidencia sólo se aplicará al primer valor (de la izquierda) en el atributo de dominio de acceso. Para un administrador con más de un dominio de acceso, la coincidencia puede aplicarse a varios valores del atributo.
Pestaña Factores	
Habilitar factores de autenticación adicionales	Seleccione esta opción si desea que el cortafuegos invoque factores de autenticación adicionales (desafíos) después de que los usuarios respondan satisfactoriamente al primer factor (especificado en el campo **Type (Tipo)** de la pestaña **Authentication (Autenticación)**). *Solo se admiten factores adicionales de autenticación en la autenticación de usuario final a través de la política de autenticación. No se admiten factores adicionales en la autenticación de usuario remoto para portales y puertas de enlace de GlobalProtect, o en la autenticación de administrador para PAN-OS o la interfaz web de Panorama. Aunque puede configurar factores adicionales, no se aplicarán en estos casos de uso. Sin embargo, se pueden integrar con proveedores de MFA utilizando RADIUS o SAML en todos los casos de uso de autenticación.* Después de configurar un perfil de autenticación que utilice autenticación de múltiples factores (multi-factor authentication, MFA), debe asignarlo a un objeto de aplicación de autenticación (Objects [Objetos] > Authentication [Autenticación]) y asignar el objeto a las reglas de la política de autenticación (Policies [Políticas] > Authentication [Autenticación]) que controlan el acceso a los recursos de su red.
Factores	Añada un perfil de servidor MFA (Device [Dispositivo] > Server Profiles [Perfiles de servidor] > Multi Factor Authentication [autenticación de múltiples factores]) para cada factor de autenticación que invoque el cortafuegos después de que los usuarios respondan correctamente al primer factor (especificado en el campo **Type [Tipo]** en la pestaña **Authentication [Autenticación]**). El cortafuegos invoca cada factor en el orden de arriba abajo para enumerar los servicios MFA que proporcionan los factores. Para cambiar el orden, seleccione un perfil de servidor y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. Puede especificar hasta tres factores adicionales. Cada servicio MFA proporciona un factor. Algunos servicios MFA permiten a los usuarios elegir un factor de una lista de varios. El cortafuegos se integra con estos servicios MFA a través de APIs de proveedores. Periódicamente, se añaden MFA vendor API integrations (integraciones de API de proveedor de MFA) adicionales con las actualizaciones de contenido de aplicaciones o aplicaciones y amenazas.
Pestaña Avanzada	
Lista de permitidos	Haga clic en **Add (Añadir)** y seleccione **all (todos)**, o seleccione los usuarios y grupos específicos que tienen permiso para autenticarse con este perfil. Cuando un usuario se autentica, el cortafuegos coincide con el nombre de usuario o

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de autenticación	Description (Descripción)
	grupo asociado con las entradas de esta lista. Si no añade entradas, ningún usuario se puede autenticar. *Para limitar la autenticación solo a aquellos usuarios que tengan una necesidad de acceso laboral legítima y reducir la superficie de ataque, especifique usuarios o grupos de usuarios, y no utilice all (todos).* *Si ha introducido un valor de User Domain (Dominio de usuario), no necesita especificar dominios en la Allow List (Lista de permitidas). Por ejemplo, si el User Domain (Dominio de usuario) es **businessinc** y quiere añadir el usuario **admin1** a la Allow Llist (Lista de permitidas), introducir `admin1` tiene el mismo efecto que introducir `businessinc\admin1`. Puede especificar grupos que ya existen en su servicio de directorios o especificar grupos personalizados basados en filtros LDAP.*
Intentos fallidos (Todos los tipos de autenticación excepto SAML)	Introduzca el número de intentos de inicio de sesión erróneos consecutivos (0 a 10) que permite el cortafuegos antes de bloquear la cuenta de usuario. Un valor 0 significa que el número de intentos es ilimitado. El valor predeterminado es 0 en los cortafuegos con modo de operación normal y 10 en los cortafuegos con modo FIPS-CC. *Configure la cantidad de Failed Attempts (Intentos fallidos) en 5 o menos para permitir una cantidad razonable de reintentos en caso de errores de escritura, a la vez que se impide que sistemas malintencionados intenten métodos de fuerza bruta para iniciar sesión en el cortafuegos.* *Si define Failed Attempts (Intentos fallidos) con un valor diferente de 0 pero deja Lockout Time (Tiempo de bloqueo) en 0, se ignora Failed Attempts (Intentos fallidos) y nunca se bloquea al usuario.*
Tiempo de bloqueo (Todos los tipos de autenticación excepto SAML)	Introduzca el número de minutos (el intervalo está entre 0 y 60, el predeterminado es 0) que el cortafuegos bloqueará una cuenta de usuario desde que el usuario alcanza el número de **Failed Attempts (intentos fallidos)**. Un valor 0 significa que el bloqueo se aplica hasta que el administrador desbloquee manualmente la cuenta de usuario. *Configure el Lockout Time (Tiempo de bloqueo) en al menos 30 minutos para impedir los intentos continuados de inicio de sesión de un usuario malintencionado.* *Si define Lockout Time (Tiempo de bloqueo) con un valor diferente de 0 pero deja Failed Attempts (Intentos fallidos) en 0, se ignora el Lockout Time (Tiempo de bloqueo) y nunca se bloquea al usuario.*

© 2020 Palo Alto Networks, Inc.

Exportación de metadatos SAML desde un perfil de autenticación

- Device > Authentication Profile

El cortafuegos y Panorama pueden utilizar un Proveedor de identidad SAML (identity provider, IdP) para autenticar usuarios que solicitan servicios. Para los administradores, el servicio puede tener acceso a la interfaz web. Para los usuarios finales, el servicio puede ser portal cautivo o GlobalProtect, que permiten el acceso a sus recursos de red. Para habilitar la autenticación SAML para un servicio, debe registrar ese servicio introduciendo información específica sobre el mismo en el IdP en forma de metadatos SAML. El cortafuegos y Panorama simplifican el registro generando automáticamente un archivo de metadatos SAML basado en el perfil de autenticación que asignó al servicio y puede exportar este archivo de metadatos al IdP. Exportar los metadatos es una alternativa más sencilla que escribir los valores de cada campo de metadatos en el IdP.

Algunos de los metadatos del archivo exportado se derivan del perfil del servidor IdP de SAML asignado al perfil de autenticación (Device > Server Profiles > SAML Identity Provider). Sin embargo, el archivo exportado siempre especifica POST como el método de enlace HTTP, independientemente del método especificado en el perfil del servidor IdL de SAML. El IdP utilizará el método POST para enviar mensajes SAML al cortafuegos o Panorama.

Para exportar metadatos SAML desde un perfil de autenticación, haga clic en SAML **Metadata (Metadatos)** en la columna Authentication (Autenticación) y complete los siguientes campos. Para importar el archivo de metadatos en un IdP, consulte la documentación de IdP.

Configuración de exportación de metadatos de SAML	Description (Descripción)
Comandos	Seleccione el servicio para el que desea exportar metadatos de SAML: • **management (gestión)** (Predeterminado): proporciona acceso de administrador a la interfaz web. • **captive-portal (portal cautivo)**-Proporciona el acceso del usuario final a los recursos de la red a través de Captive Portal. • **global-protect**-Proporciona acceso de usuario final a recursos de red a través de GlobalProtect. Su selección determina cuáles otros campos muestra el diálogo.
[Management | Captive Portal | GlobalProtect] Auth Profile	Introduzca el nombre del perfil de autenticación del que está exportando metadatos. El valor predeterminado es el perfil desde el que abrió el diálogo haciendo clic en el enlace **Metadata (Metadatos)**.
Management Choice (Solo Management)	Seleccione una opción para especificar una interfaz habilitada para el tráfico de gestión (como la interfaz MGT): • **Interface (Interfaz)**: seleccione la interfaz de la lista de interfaces en el cortafuegos. • **IP Hostname (Nombre de host IP)**: introduzca la dirección IP o el nombre de host de la interfaz. Si introduce un nombre de host, el servidor DNS debe tener un registro de dirección (A) que se correlaciona con la dirección IP.

© 2020 Palo Alto Networks, Inc.

Configuración de exportación de metadatos de SAML	Description (Descripción)
[Captive Portal | GlobalProtect] Virtual System (Solo Captive Portal o GlobalProtect)	Seleccione el sistema virtual para el que se definen la configuración del Portal de Captive o el portal de GlobalProtect.
Nombre de host IP (Solo Captive Portal o GlobalProtect)	Introduzca la dirección IP o el nombre de host del servicio. • **Captive portal (Portal cautivo)**: introduzca la dirección IP o nombre de host de **Redirect Host (Host de redireccionamiento)** (**Device [Dispositivo]** > **User Identification [Identificación del usuario]** > **Captive Portal Settings [Configuración del portal cautivo]**). • **GlobalProtect**: introduzca el **Hostname (Nombre de host)** o **IP Address (Dirección IP)** del servidor. Si introduce un nombre de host, el servidor DNS debe tener un registro de dirección (A) que se correlaciona con la dirección IP.

© 2020 Palo Alto Networks, Inc.

Device > Authentication Sequence

- Device > Authentication Sequence
- Panorama > Authentication Sequence

En algunos entornos, las cuentas de usuario residen en varios directorios (p. ej.: LDAP y RADIUS). Una secuencia de autenticación es un conjunto de perfiles de autenticación que el cortafuegos intenta usar para la autenticación de usuarios cuando estos inician sesión. El cortafuegos prueba los perfiles de manera secuencial descendente (aplicando la autenticación, registro único de Kerberos, lista de permitidas y valores de bloqueo de cuenta) hasta que un perfil autentica correctamente al usuario. El cortafuegos solo deniega el acceso si la autenticación falla con todos los perfiles de la secuencia. Para ver información sobre perfiles de autenticación, consulte Device > Authentication Profile.

Configure una secuencia de autenticación con varios perfiles de autenticación que utilicen diferentes métodos de autenticación. Configure al menos dos métodos de autenticación externos y uno local (interno) para que los problemas de conectividad no impidan la autenticación. Convierta el perfil de autenticación local en el último perfil de la secuencia, para que solo sea utilizado si todos los métodos de autenticación externa fallan. (La autenticación externa ofrece servicios de autenticación centralizados, confiables y dedicados, incluidas las funciones de inicio de sesión y solución de problemas).

Configuración de secuencias de autenticación	Description (Descripción)
Nombre	Introduzca un nombre para identificar la secuencia. El nombre distingue entre mayúsculas y minúsculas, puede tener hasta 31 caracteres, incluidas letras, números, espacios, guiones, guiones bajos y puntos. El nombre debe ser exclusivo en la **Location (Ubicación)** actual (cortafuegos o sistema virtual) en relación con otras secuencias de autenticación y perfiles de autenticación. *En un cortafuegos con sistemas virtuales múltiples, si la Location (Ubicación) de la secuencia de autenticación es un sistema virtual (vsys), no introduzca el mismo nombre como un perfil de autenticación en la ubicación Compartido. Del mismo modo, si la secuencia Location (Ubicación) es Shared (Compartida), no introduzca el mismo nombre como un perfil en un vsys. Se pueden producir errores de referencia mientras compila una secuencia de autenticación y un perfil con los mismos nombres en estos casos.*
Ubicación	Seleccione el ámbito en el que está disponible la secuencia. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardada la secuencia, no puede cambiar su **Location (Ubicación)**.
Usar el dominio para determinar el perfil de autenticación	Seleccione esta opción (seleccionada de manera predeterminada) si quiere que el cortafuegos busque coincidencias con el nombre de dominio que introduce un usuario durante el inicio de sesión con **User Domain (Dominio de usuario)** o **Kerberos Realm (Dominio de Kerberos)** de un perfil de

© 2020 Palo Alto Networks, Inc.

Configuración de secuencias de autenticación	Description (Descripción)
	autenticación asociado a la secuencia y luego usar el perfil para autenticar el usuario. La entrada del usuario que usa el cortafuegos para la coincidencia puede ser el texto que precede al nombre de usuario (separado por una barra invertida) o el texto que sigue al nombre de usuario (separado por el símbolo @). Si el cortafuegos no encuentra una coincidencia, prueba los perfiles de autenticación en la secuencia en orden descendente.
Perfiles de autenticación	Haga clic en **Add (Añadir)** y en el menú desplegable seleccione los perfiles de autenticación que quiera añadir a la secuencia. Para cambiar el orden de la lista, seleccione un perfil y haga clic en **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. Para eliminar un perfil, selecciónelo y haga clic en **Delete (Eliminar)**. *No puede agregar un perfil de autenticación que especifique un perfil de servidor de autenticación de múltiples factores (MFA) o un perfil de servidor de proveedor de identidad de SAML (Security Assertion Markup Language).*

© 2020 Palo Alto Networks, Inc.

Device > VM Information Sources

Utilice esta pestaña para registrar cambios activamente en las máquinas virtuales (Virtual Machine, VM) implementadas en cualquiera de estos orígenes: servidor VMware ESXi, servidor VMware vCenter, Amazon Web Services Virtual Private Cloud (AWS-VPC) o Google Compute Engine (GCE).

Cuando supervisa los hosts ESXi que son parte de la solución VM-Series edición NSX, use 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.

Puede registrar hasta un número máximo de 32 etiquetas para una dirección IP.

Hay dos formas de supervisar los orígenes de información de VM.

- El cortafuegos puede supervisar su servidor VMware ESXi, VMware vCenter, las instancias de GCE o las AWS-VPC, además de recuperar cambios conforme realiza el abastecimiento o modifica los invitados en estos orígenes supervisados. En cada cortafuegos o sistema virtual de un cortafuegos configurado con múltiples sistemas virtuales, puede configurar hasta 10 orígenes.

  Las siguientes condiciones aplican cuando sus cortafuegos se configuran en una configuración de alta disponibilidad (high availability, HA).

  - **Configuración de HA activa/pasiva:** solo el cortafuegos activo supervisa los orígenes de la información de la VM.
  - **Configuración de HA activa/pasiva:** solo el cortafuegos con el valor de prioridad `primary` (principal) supervisa los orígenes de información de VM.

  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 la serie VM.
- Para la asignación de dirección IP a nombre de usuario, puede configurar los orígenes de la información de VM en el agente de User-ID de Windows o en el cortafuegos para supervisar los servidores VMware ESXi y vCenter, y recuperar los cambios conforme realiza el abastecimiento o modifica los invitados configurados en el servidor. El agente de User-ID de Windows admite hasta 100 orígenes. El agente de User ID no admite AWS y Google Compute Engine.

  Las VM de servidores ESXi o vCenter supervisados deben tener las herramientas de VMware instaladas y en ejecución. Las herramientas de VMware brindan la capacidad a direcciones IP y otros valores asignados a cada VM.

Para recopilar los valores asignados a las VM supervisadas, el cortafuegos supervisa los atributos en las siguientes tablas.

Atributos supervisados en un origen de VMware
• UUID • Nombre • Sistema operativo invitado • Anotación

© 2020 Palo Alto Networks, Inc.

Atributos supervisados en un origen de VMware
• VM State (Estado de VM): el estado de alimentación puede ser `poweredOff` (apagado), `poweredOn` (encendido), `standBy` (en espera) o `unknown` (desconocido). • versión • Network (Red): nombre del conmutador virtual, nombre del grupo de puertos e ID de VLAN • Container Name (Nombre del contenedor): nombre de vCenter, nombre del objeto del centro de datos, nombre del grupo de recursos, nombre del clúster, host y dirección IP del host.

Atributos supervisados en el AWS-VPC
• Arquitectura • Sistema operativo invitado • ID de imagen • ID de instancia • Estado de instancia • Tipo de instancia • Nombre de clave • Placement (Colocación): Tenancy (Arrendamiento), Group Name (Nombre de grupo) y Availability Zone (Zona de disponibilidad) • Nombre DNS privado • Nombre DNS público • ID de subred • Etiqueta (clave, valor) (se admiten hasta 18 etiquetas por instancia) • ID de VPC

Atributos supervisados por 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) • Zona

Add (Añadir): haga clic en **Add (Añadir)** para añadir un nuevo origen para la supervisión de VM y complete los detalles basados en el origen que se está supervisando:

- Para VMware ESXi o vCenter Server, consulte Ajustes para habilitar los orígenes de información de la VM para los servidores ESXi de VMware o vCenter.
- Para AWS-VPC, consulte Ajustes para habilitar los orígenes de información de la VM para AWS VPC.
- Para Google Compute Engine (GCE), consulte Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine.

Refresh Connected (Actualizar conectados): actualiza el estado de conexión en la pantalla; no actualiza la conexión entre el cortafuegos y los orígenes supervisados.

Delete (Eliminar): elimina los orígenes de la información de VM configurada que selecciona.

© 2020 Palo Alto Networks, Inc.

PDF/CSV: exporta la tabla de configuración de origen de la información de VM como un archivo PDF o un archivo con valores separados por comas (comma-separated values, CSV). Consulte Exportación de la tabla de configuración.

Ajustes para habilitar los orígenes de información de la VM para los servidores ESXi de VMware o vCenter

En la siguiente tabla se describen los parámetros que puede configurar para habilitar las fuentes de información de VM para los servidores VMware ESXi y vCenter.

Para recuperar las etiquetas de las máquinas virtuales, el cortafuegos requiere una cuenta con acceso de solo lectura en los servidores VMware ESXi y vCenter.

Ajustes para habilitar las fuentes de información de la VM para los servidores ESXi de VMware o vCenter	
Nombre	Introduzca un nombre para identificar el origen supervisado (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Tipo	Seleccione si el host/origen que se está supervisando es un **ESXi server (Servidor ESXi)** o **vCenter**.
Description (Descripción)	(Opcional) Añada una etiqueta para identificar la ubicación o función del origen.
Puerto	Especifique el puerto en el que está escuchando el host/origen. (puerto predeterminado 443).
Habilitado	De forma predeterminada, la comunicación entre el cortafuegos y el origen configurado está activada. El estado de conexión entre el origen supervisado y el cortafuegos aparece en la interfaz de la siguiente forma: • Connected (Conectado) • Disconnected (Desconectado) • Pending (Pendiente); el estado de la conexión también aparece en amarillo cuando se deshabilita el origen supervisado. Quite la opción **Enable (Habilitar)** para deshabilitar la comunicación entre el host y el cortafuegos.
Tiempo de espera	Introduzca el intervalo en horas después del cual se cierra la conexión al origen supervisado, si el host no responde (el intervalo es 2-10; el predeterminado es 2). (Opcional) Para cambiar el valor predeterminado, seleccione **Enable timeout when the source is disconnected (Habilitar el tiempo de espera cuando el origen esté desconectado)** y especifique el valor. Cuando se alcanza el límite especificado, si no se puede acceder al host o este no responde, el cortafuegos cerrará la conexión al origen.

© 2020 Palo Alto Networks, Inc.

Ajustes para habilitar las fuentes de información de la VM para los servidores ESXi de VMware o vCenter	
Source (Origen)	Introduzca el FQDN o la dirección IP del host/origen que se está supervisando.
Nombre de usuario	Especifique el nombre de usuario necesario para autenticar para el origen.
Contraseña	Introduzca la contraseña y confirme la entrada.
Intervalo de actualización	Especifique el intervalo en segundos en el que el cortafuegos recupera información del origen (el intervalo es 5-600; el predeterminado es 5).

Ajustes para habilitar los orígenes de información de la VM para AWS VPC

La tabla siguiente describe la configuración que debe realizar para habilitar fuentes de información de VM para un VPC AWS.

Ajustes para habilitar los orígenes de información de la VM para AWS VPC	
Nombre	Introduzca un nombre para identificar el origen supervisado (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Tipo	Seleccione **AWS VPC**.
Description (Descripción)	(Opcional) Añada una etiqueta para identificar la ubicación o función del origen.
Habilitado	De forma predeterminada, la comunicación entre el cortafuegos y el origen configurado está activada. El estado de conexión entre el origen supervisado y el cortafuegos aparece en la interfaz de la siguiente forma: • Connected (Conectado) • Disconnected (Desconectado) • Pending (Pendiente); el estado de la conexión también aparece en amarillo cuando se deshabilita el origen supervisado. Quite la opción **Enable (Habilitar)** para deshabilitar la comunicación entre el host y el cortafuegos.
Source (Origen)	Añada la URI en la que reside la Virtual Private Cloud. Por ejemplo, ec2.us-west-1.amazonaws.com. La sintaxis es: ec2.<*your_AWS_region*>.amazonaws.com; para AWS China, es: ec2.<AWS_region>.amazonaws.com.cn.
ID de clave de acceso	Introduzca la cadena de texto alfanumérico que identifica de forma exclusiva al usuario propietario o con autorización de acceso a la cuenta de AWS.

© 2020 Palo Alto Networks, Inc.

Ajustes para habilitar los orígenes de información de la VM para AWS VPC	
	Esta información es una parte de las credenciales de seguridad de AWS. El cortafuegos necesitas las credenciales (ID de clave de acceso y clave de acceso secreto) para firmar digitalmente las llamadas de API realizadas a los servicios de AWS.
Clave de acceso secreto	Introduzca la contraseña y confirme la entrada.
Intervalo de actualización	Especifique el intervalo en segundos en el que el cortafuegos recupera información del origen (el intervalo es 60-1.200; el predeterminado es 60).
Tiempo de espera	Intervalo en horas después del cual se cierra la conexión al origen supervisado, si el host no responde (el predeterminado es 2). (Opcional) Seleccione **Enable timeout when the source is disconnected (Habilitar el tiempo de espera cuando el origen esté desconectado)**. Cuando se alcanza el límite especificado, si no se puede acceder al origen o este no responde, el cortafuegos cerrará la conexión al origen.
ID de VPC	Introduzca el ID del AWS-VPC para supervisar, por ejemplo, vpc-1a2b3c4d. Solo se supervisan las instancias de EC2 implementadas en este VPC. Si su cuenta se configura para usar un VPC predeterminado, el ID del VPC predeterminado aparecerá en los atributos de cuenta de AWS.

Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine

Device (Dispositivo) > **VM Information Sources (Fuentes de información de VM)** > **Add (Añadir)**

La siguiente tabla describe los ajustes que debe establecer en la configuración para habilitar las fuentes de información de VM para las instancias de Google Compute Engine en Google Cloud Platform. Habilite la supervisión de las instancias de Google Compute Engine (GCE) para permitir que el cortafuegos (físico o virtual de manera local, o que se ejecuta en Google Cloud) recupere etiquetas y otros metadatos sobre las instancias que se ejecutan en una zona concreta de Google Cloud del proyecto especificado. Para obtener información sobre la serie VM en Google Cloud Platform, consulte la Guía de implementación de la serie VM.

Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine	
Nombre	Introduzca un nombre para identificar el origen supervisado (de hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos.
Tipo	Seleccione **Google Compute Engine**.
Description (Descripción)	(Opcional) Añada una etiqueta para identificar la ubicación o función del origen.

© 2020 Palo Alto Networks, Inc.

Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine	
Habilitado	La comunicación entre el cortafuegos y el origen configurado está habilitada de manera predeterminada. El estado de conexión entre el origen supervisado y el cortafuegos aparece en la interfaz de la siguiente forma: • —Conectado • —Desconectado • —Pendiente o el origen de supervisión está deshabilitado. Quite la opción **Enabled (Habilitado)** para deshabilitar la comunicación entre el origen configurado y el cortafuegos. Cuando deshabilita la comunicación, todas las direcciones IP y etiquetas registradas se eliminan del grupo de direcciones dinámicas asociado. Esto significa que las reglas de la política no se aplicarán a las instancias de GCE desde este proyecto de Google Cloud.
Service Authentication Type (Tipo de autenticación de servicio)	Seleccione entre VM-Series running on GCE (Serie VM en ejecución en GCE) o Service Account (Cuenta de servicio). • **VM-Series running on GCE (Serie VM en ejecución en GCE)**: seleccione esta opción si el cortafuegos basado en hardware o de serie VM en el que habilita la supervisión de VM no se ha implementado en Google Cloud Platform. • **Service Account (Cuenta de servicio)**: seleccione esta opción si supervisa instancias de Google Cloud Engine en un cortafuegos que no se ha implementado en Google Cloud Platform. Esta opción le permite utilizar una cuenta especial de Google que pertenece a la máquina virtual o aplicación, en lugar de utilizar una cuenta individual de usuario final. Esta cuenta de servicio debe tener las políticas de IAM (privilegio **Compute Engine** > **Compute Viewer (Observador de cómputos)**) que autorizan el acceso a la API de Google y que le permiten consultar los equipos virtuales del proyecto de Google Cloud acerca de sus metadatos.
Service Account Credential (Credencial de cuenta de servicio)	(Solo para cuentas de servicio) Cargue un archivo JSON con las credenciales de la cuenta de servicio. Este archivo le permite al cortafuegos autenticarse en la instancia y autoriza acceso a los metadatos. Puede crear una cuenta en la consola de Google Cloud (**IAM & admin [IAM y administrador]** > **Service Accounts [Cuentas de servicio]**). Consulte la documentación de Google para obtener información sobre cómo crear una cuenta, añadirle una clave y descargar el archivo JSON que debe cargar para el cortafuegos.
Project ID (ID de proyecto)	Introduzca una cadena de texto alfanumérica que identifique de manera única al proyecto de Google Cloud que desea supervisar.
Zone Name (Nombre de zona)	Introduzca la información de la zona como una cadena de hasta 63 caracteres. Por ejemplo: `us-west1-a`.

© 2020 Palo Alto Networks, Inc.

Configuración para habilitar los orígenes de la información de la VM para Google Compute Engine	
Intervalo de actualización	Especifique el intervalo (en segundos) en el que el cortafuegos recupera información del origen (el intervalo es 60 a 1200; el valor predeterminado es 60).
Tiempo de espera	Intervalo (en horas) después del cual se cierra la conexión al origen supervisado, si el host no responde (el valor predeterminado es 2). (Opcional) Seleccione **Enable timeout when the source is disconnected (Habilitar el tiempo de espera cuando el origen esté desconectado)**. Cuando se alcanza el límite especificado, si no se puede acceder al origen o este no responde, el cortafuegos cerrará la conexión al origen. Cuando el origen está desconectado, todas las direcciones IP y etiquetas que se registraron desde este proyecto se eliminan del grupo de direcciones dinámicas.

© 2020 Palo Alto Networks, Inc.

Device (Dispositivo) > Troubleshooting (Solución de problemas)

- **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)**
- **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Troubleshooting (Solución de problemas)**

Antes de confirmar el grupo de dispositivos o los cambios de la configuración de la plantilla, compruebe la funcionalidad desde la interfaz web, para verificar que los cambios no hayan introducido problemas de conectividad en la configuración que se está ejecutando, y que sus políticas permitan o rechacen el tráfico correctamente.

- **Pruebas de coincidencia de política**
  - Coincidencia de política de seguridad
  - Coincidencia de política de QoS
  - Coincidencia de política de autenticación
  - Coincidencia de política de descifrado/SSL
  - Coincidencia de política de NAT
  - Coincidencia de política de reenvío basado en políticas
  - Coincidencia de política de DoS
- **Pruebas de conectividad**
  - Enrutamiento
  - Probar Wildfire
  - Cámara de amenazas
  - Ping
  - Realizar seguimiento de ruta
  - Conectividad de recopilador de logs
  - Lista dinámica externa
  - Actualizar servidor
  - Comprobar el estado del servicio de logging en nube
  - Comprobar el estado del servicio GP en nube

Coincidencia de política de seguridad

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
Para	Seleccione la zona de destino del tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Puerto de destino	Introduzca el puerto de destino específico para el cual está previsto el tráfico.
Source User (Usuario de origen)	Introduzca el usuario desde el cual se originó el tráfico.
PROTOCOL	Introduzca el protocolo IP utilizado para el enrutamiento. Puede ser de 0 a 255.
Show all potential match rules until first allow rule (Mostrar las posibles coincidencias de reglas hasta la primera regla permitir)	Habilite esta opción para que se muestren todas las posibles coincidencias de la regla hasta el primer resultado de coincidencia de regla. Deshabilite (desmarque) la opción para devolver únicamente la primera regla coincidente en los resultados de la prueba.
Application (Aplicación)	Seleccione el tráfico de la aplicación que desea poner a prueba.
Category	Seleccione la categoría de tráfico que desea poner a prueba.
(Solo cortafuegos) Check HIP mask (Comprobar máscara HIP)	Seleccione esta opción para comprobar el estado de seguridad del dispositivo terminal que está accediendo a su red.
RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada. (Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado: • Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico. • Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico. • Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`. • Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones: • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo. • `Shared policy disabled on device (Política compartida deshabilitada en el dispositivo)`: los ajustes de Panorama en el dispositivo no permiten que la política se envíe desde Panorama.

Coincidencia de política de QoS

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
Para	Seleccione la zona de destino del tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Puerto de destino	Introduzca el puerto de destino específico para el cual está previsto el tráfico.
Source User (Usuario de origen)	Seleccione el usuario desde el cual se originó el tráfico.
PROTOCOL	Introduzca el protocolo IP utilizado para el enrutamiento. Puede ser de 0 a 255.
Application (Aplicación)	Seleccione el tráfico de la aplicación que desea poner a prueba.
Category	Seleccione la categoría de tráfico que desea poner a prueba.
Codepoint Type (Tipo de codepoint)	Seleccione el tipo de codificación codepoint que desea comprobar.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Codepoint Value (Valor de codepoint)	Especifique el valor de la codificación de codepoint: • **DSCP**: de 0 a 63 • **ToS**: de 0 a 7

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.
	  • `Shared policy disabled on device (Política compartida deshabilitada en el dispositivo)`: los ajustes de Panorama en el dispositivo no permiten que la política se envíe desde Panorama.

Coincidencia de política de autenticación

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Para	Seleccione la zona de destino del tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Category	Seleccione la categoría de tráfico que desea poner a prueba.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.
	  • `Shared policy disabled on device (Política compartida deshabilitada en el dispositivo)`: los ajustes de Panorama en el dispositivo no permiten que la política se envíe desde Panorama.

Coincidencia de política de descifrado/SSL

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
Para	Seleccione la zona de destino del tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Application (Aplicación)	Seleccione el tráfico de la aplicación que desea poner a prueba.
Category	Seleccione la categoría de tráfico que desea poner a prueba.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Coincidencia de política de NAT

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
Para	Seleccione la zona de destino del tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Puerto de origen	Introduzca el puerto específico donde se originó el tráfico.
Puerto de destino	Introduzca el puerto de destino específico para el cual está previsto el tráfico.
PROTOCOL	Introduzca el protocolo IP utilizado para el enrutamiento. Puede ser de 0 a 255.
To Interface (Interfaz de destino)	Introduzca la interfaz de destino del dispositivo para el cual está destinado el tráfico.
ID de dispositivo HA	Introduzca el ID del dispositivo HA: • **0**: peer HA principal • **1**: peer HA secundario

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.
	  • `Shared policy disabled on device (Política compartida deshabilitada en el dispositivo)`:

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	los ajustes de Panorama en el dispositivo no permiten que la política se envíe desde Panorama.

Coincidencia de política de reenvío basado en políticas

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
From Interface (Interfaz de origen)	Introduzca la interfaz del dispositivo desde el cual se originó el tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Puerto de destino	Introduzca el puerto de destino específico para el cual está previsto el tráfico.
Source User (Usuario de origen)	Introduzca el usuario desde el cual se originó el tráfico.
PROTOCOL	Introduzca el protocolo IP utilizado para el enrutamiento. Puede ser de 0 a 255.
Application (Aplicación)	Seleccione el tráfico de la aplicación que desea poner a prueba.
ID de dispositivo HA	ID del dispositivo HA: • **0**: peer HA principal • **1**: peer HA secundario
RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)

	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.
	  • `Shared policy disabled on device (Política compartida deshabilitada en el dispositivo)`: los ajustes de Panorama en el dispositivo no permiten que la política se envíe desde Panorama.

Coincidencia de política de DoS

Campo	Description (Descripción)
Configuración de prueba	
Seleccionar prueba	Seleccione la prueba de coincidencia de política que desea ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
De	Introduzca la zona donde se originó el tráfico.
Para	Seleccione la zona de destino del tráfico.
From Interface (Interfaz de origen)	Introduzca la interfaz del dispositivo desde el cual se originó el tráfico.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
To Interface (Interfaz de destino)	Introduzca la interfaz de destino del dispositivo para el cual está destinado el tráfico.
Source (Origen)	Introduzca la dirección IP donde se originó el tráfico.
IP Destino	Introduzca la dirección IP de destino del tráfico.
Puerto de destino	Introduzca el puerto de destino específico para el cual está previsto el tráfico.
Source User (Usuario de origen)	Introduzca el usuario desde el cual se originó el tráfico.
PROTOCOL	Introduzca el protocolo IP utilizado para el enrutamiento. Puede ser de 0 a 255.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Enrutamiento

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
Búsqueda FiB, búsqueda Mfib	Seleccione una de las siguientes opciones para la búsqueda: • **FiB**: realice búsqueda de rutas dentro de la tabla de rutas activa. • **MfiB**: realice búsqueda de rutas de multidifusión dentro de la tabla de rutas activa.
IP de destino	Introduzca la dirección IP a la que se dirige el tráfico.
Enrutador virtual	Enrutador virtual específico dentro del cual se realiza la prueba de enrutamiento. Seleccione el enrutador virtual en la lista desplegable.
ECMP	
IP de origen	Introduzca la dirección IP específica desde la cual se originó el tráfico.
Puerto de origen	Introduzca el puerto específico desde el cual se originó el tráfico.
IP de destino	Introduzca la dirección IP específica a la que está destinado el tráfico.
Puerto de destino	Introduzca el puerto de destino específico al que está destinado el tráfico.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

© 2020 Palo Alto Networks, Inc.

Probar Wildfire

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
Canal	Seleccione el canal de WildFire: **`Público`** o **`Privado`**.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Cámara de amenazas

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Ping

La prueba de solución de problemas de ping solo es compatible con los cortafuegos que ejecutan PAN-OS 9.0 o versiones posteriores.

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
Bypass routing table, use specified interface (Omitir tabla	Habilite esta opción para omitir la tabla de enrutamiento y usar una interfaz especificada. Deshabilite (desmarque) esta opción para comprobar la tabla de enrutamiento configurada.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
de enrutamiento, utilizar la interfaz especificada)	
Count	Introduzca el número de solicitudes para enviar. El valor predeterminado es 5.
Don't fragment echo request packets (IPv4) (No fragmentar paquetes de solicitud de eco [IPv4])	Habilite esta opción para no fragmentar los paquetes de solicitud de eco para la prueba. Deshabilitar
Force to IPv6 destination (Forzar en destino de IPv6)	Habilite la opción para forzar la prueba en el destino de IPv6.
Intervalo	Especifique un retardo, en segundos, entre las solicitudes (el intervalo es de 1 a 2 000 000 000).
Source (Origen)	Introduzca la dirección de origen de la solicitud de eco.
Don't attempt to print addresses symbolically (No intentar imprimir direcciones simbólicamente)	Habilite esta opción para mostrar direcciones IP en los resultados de prueba y no resolver el nombre de host de la dirección IP. Deshabilite (desmarque) la opción para resolver nombres de host de dirección IP.
Patrón	Especifique la trama de relleno hexadecimal.
Tamaño	Introduzca el tamaño, en bytes, de los paquetes de solicitud (el intervalo es de 0 a 65 468).
Tos	Introduzca el valor de tipo de servicio IP (el intervalo es de 1 a 255).
TTL	Introduzca el valor del periodo de vida IP en saltos: valor de límite de salto IPv6 (el intervalo es de 1 a 255).
Display detailed output (Mostrar resultado detallado)	Habilite esta opción para ver los detalles de los resultados de la prueba.
Host	Introduzca el nombre del host o la dirección IP del host remoto.
RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada. (Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado: • Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico. • Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico. • Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)

	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Realizar seguimiento de ruta

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.
Use IPv4 (Usar IPv4)	Habilite la opción para usar la dirección IPv4 de los dispositivos seleccionados.
Use IPv6 (Usar IPv6)	Habilite la opción para usar la dirección IPv6 de los dispositivos seleccionados.
First TTL (Primer periodo de vida)	Introduzca el periodo de vida utilizado en el primer paquete sonda salientes (el intervalo es de 1 a 255).
Max TTL (Periodo de vida máximo)	Introduzca el valor máximo de saltos del periodo de vida (el intervalo es de 1 a 255).
Puerto	Introduzca el número de puerto base utilizado en la sonda.
Tos	Introduzca el valor de tipo de servicio IP (el intervalo es de 1 a 255).
Wait (Espera)	Introduzca la cantidad de segundos que se debe esperar una respuesta (el intervalo es de 1 a 99 999).
Pausa	Introduzca el tiempo, en milisegundos, para pausar entre las sondas (el intervalo es de 1 a 2 000 000 000).
Set the “don’t fragment” bit (Configurar el bit “no fragmentar”)	Habilite esta opción para no fragmentar el paquete ICMP en múltiples paquetes si la ruta no puede admitir la unidad de transmisión máxima configurada (Maximum Transmission Unit, MTU).

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Enable socket level debugging (Habilitar depuración de nivel de socket)	Habilite esta opción para poder depurar al nivel del socket.
Gateway	Especifique una cantidad de 8 puertas de enlace de ruta de origen no estricto.
Don't attempt to print addresses symbolically (No intentar imprimir direcciones simbólicamente)	Habilite esta opción para mostrar direcciones IP en los resultados de prueba y no resolver el nombre de host de la dirección IP. Deshabilite (desmarque) la opción para resolver nombres de host de dirección IP.
Bypass routing tables and send directly to a host (Omitir tablas de enrutamiento y enviar directamente a un host)	Habilite esta opción para omitir las tablas de enrutamiento configuradas y comprobar directamente con el host.
Source (Origen)	Introduzca una dirección de origen en los paquetes sonda salientes.
Host	Introduzca el nombre del host o la dirección IP del host remoto.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Conectividad de recopilador de logs

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales que se han seleccionado para la prueba.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Lista dinámica externa

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
(Solo Panorama) Selección del dispositivo	Seleccione **Select device/VSYS (Seleccionar dispositivo/sistema virtual)** para especificar los dispositivos y sistemas virtuales para los cuales comprobará la funcionalidad de la política. Los dispositivos y sistemas virtuales se presentan a los administradores y usuarios de grupos de dispositivos y plantillas en función de su dominio de acceso. Además, puede seleccionar el servidor de gestión Panorama como dispositivo.
(Solo Panorama) Dispositivos seleccionados	Enumera los dispositivos y sistemas virtuales seleccionados para la prueba.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Prueba de URL	Especifique la URL para comprobar la conexión.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

Actualizar servidor

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.

RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada.
	(Solo Panorama) Al ejecutar la prueba para varios dispositivos gestionados, la sección de resultados muestra la siguiente información para cada dispositivo evaluado:
	• Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico.
	• Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico.
	• Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`.
	• Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:
	  • `N/A (No corresponde)`: la prueba no corresponde al dispositivo.
	  • `Device not connected (Dispositivo no conectado)`: se interrumpió la conexión del dispositivo.

© 2020 Palo Alto Networks, Inc.

Comprobar el estado del servicio de logging en nube

Compruebe el estado de la conectividad con el servicio de creación de logs en la nube. Esta prueba solo está disponible en un servidor de gestión de Panorama que ejecute el complemento Cloud Services (Servicios en la nube) versión 1.3 o posterior.

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada. Al ejecutar la prueba para varios dispositivos gestionados, los resultados mostrarán la siguiente información para cada dispositivo evaluado: • Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico. • Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico. • Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`. • Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:

Comprobar el estado del servicio GP en nube

Compruebe el estado de la conectividad con GlobalProtect como servicio. Esta prueba solo está disponible en un servidor de gestión de Panorama que ejecute el complemento Cloud Services (Servicios en la nube) versión 1.3 o posterior.

Campo	Description (Descripción)
Seleccionar prueba	Seleccione la prueba de conectividad para ejecutar.
RESULTADOS	Seleccione esta opción para ver en detalle los resultados de la prueba ejecutada. Al ejecutar la prueba para varios dispositivos gestionados, los resultados mostrarán la siguiente información para cada dispositivo evaluado: • Device Group (Grupo de dispositivos): nombre del grupo de dispositivos al cual pertenece el cortafuegos que está procesando el tráfico. • Firewall (Cortafuegos): nombre del cortafuegos que está procesando el tráfico. • Status (Estado): indica el estado de la prueba: `Success (Correcta)` o `Failure (Incorrecta)`. • Result (Resultado): muestra el resultado de la prueba. Si la prueba no pudiera realizarse, se muestra una de las siguientes opciones:

© 2020 Palo Alto Networks, Inc.

Device > Virtual Systems

Un sistema virtual (vsys) es una instancia de cortafuegos (virtual) independiente que puede gestionar por separado dentro de un cortafuegos físico. Cada vsys puede ser un cortafuegos independiente con su propia política de seguridad, interfaces y administradores; un vsys le permite segmentar la administración de todas las políticas, informes y funciones de visibilidad que proporciona el cortafuegos.

Por ejemplo, si desea personalizar las características de seguridad para el tráfico asociado al departamento financiero, puede definir un vsys financiero y, a continuación, definir políticas de seguridad que pertenezcan únicamente a ese departamento. Para optimizar la administración de políticas, puede mantener cuentas de administrador distintas para todo el cortafuegos y las funciones de red, y crear a su vez cuentas de administrador de vsys que permitan el acceso a vsys individuales. Esto permite al administrador de vsys del departamento financiero gestionar la política de seguridad únicamente de dicho departamento.

Las funciones de red (como enrutamiento estático y dinámico, direcciones IP de interfaces y túneles IPSec) pertenecen a un cortafuegos completo y a todos sus sistemas virtuales. Una configuración de sistema virtual (**(Dispositivo** > **Sistemas virtuales**) no controla las funciones de nivel de cortafuegos y de red (como el enrutamiento estático y dinámico, las direcciones IP de interfaces, los túneles de IPSec, las VLAN, los cables virtuales, los enrutadores virtuales, los túneles de GRE, DHCP, DNS de proxy, QoS, LLDP y los perfiles de red). Para cada vsys puede especificar un conjunto de interfaces de cortafuegos físicas y lógicas (incluidas VLAN y Virtual Wire) y zonas de seguridad. Si necesita segmentación de rutas para cada vsys, debe crear y asignar enrutadores virtuales adicionales y asignar interfaces, VLAN y Virtual Wire, según corresponda.

Si usa una plantilla de Panorama para definir sus sistemas virtuales, puede configurar un vsys como predeterminado. El vsys predeterminado y la capacidad de varios sistemas virtuales determinan si un cortafuegos acepta configuraciones específicas de vsys durante una compilación de plantilla:

- Los cortafuegos que tienen habilitada la capacidad de varios sistemas virtuales aceptan configuraciones específicas de vsys para cualquier vsys que se defina en la plantilla.
- Los cortafuegos que no tienen habilitada la capacidad de varios sistemas virtuales aceptan configuraciones específicas de vsys solo para los vsys predeterminados. Si no configura un vsys predeterminado, estos cortafuegos no aceptarán configuraciones específicas de vsys.

Los cortafuegos PA-3200 Series, PA-5200 Series y PA-7000 Series admiten varios sistemas virtuales. Sin embargo, los cortafuegos PA-3200 Series requieren una licencia para habilitar varios sistemas virtuales. Los cortafuegos de la serie PA-220 y PA-800 no admiten varios sistemas virtuales.

Antes de habilitar varios sistemas virtuales, tenga en cuenta lo siguiente:

- Un administrador de vsys crea y gestiona todos los elementos necesarios para la política de seguridad por sistema virtual asignado.
- Las zonas son objetos dentro de vsys. Antes de definir una política o un objeto de política, seleccione el **Virtual System (Sistema virtual)** apropiado en la lista desplegable de la pestaña **Policies (Políticas)** u **Objects (Objetos)**.
- Puede establecer destinos de creación de logs remotos (SNMP, syslog y correo electrónico), aplicaciones, servicios y perfiles para que estén disponibles para todos los sistemas virtuales (compartido) o con un único vsys.
- Si tiene varios sistemas virtuales, puede seleccionar un vsys como un concentrador de User-ID para que comparta la información de asignación de dirección IP a nombre de usuario entre los sistemas virtuales.
- Puede configurar rutas de servicios globales (para todos los sistemas virtuales de un cortafuegos) o específicas de un vsys (Device [Dispositivo] > Setup [Configuración] > Services [Servicios]).
- Puede cambiar el nombre de un vsys solo en el cortafuegos local. En Panorama, no se permite. Si cambia el nombre de un vsys en Panorama, creará un vsys completamente nuevo o el nombre del nuevo vsys se asignará al vsys incorrecto en el cortafuegos.

© 2020 Palo Alto Networks, Inc.

Antes de definir un vsys, primero debe habilitar la funcionalidad de múltiples sistemas virtuales en el cortafuegos. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, edite la sección **General Settings (Configuración general)**, seleccione **Multi Virtual System Capability (Capacidad para múltiples sistemas virtuales)** y haga clic en **OK (Aceptar)**. Esto añade una página **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)**. Seleccione la página, haga clic en **Add (Añadir)** para añadir un sistema virtual y especifique la siguiente información.

Configuración de sistemas virtuales	Description (Descripción)
ID	Introduzca un identificador que sea un número entero para el vsys. Consulte la hoja de datos de su modelo de cortafuegos para obtener información sobre el número de sistemas virtuales admitidos. *Si usa una plantilla de Panorama para configurar el vsys, este campo no aparece.*
Nombre	Introduzca un nombre (hasta 31 caracteres) para identificar el vsys. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. *Si usa una plantilla de Panorama para enviar configuraciones vsys, el nombre vsys en la plantilla debe coincidir con el nombre de vsys en el cortafuegos.*
Allow Forwarding of Decrypted Content (Permitir reenvío de contenido descifrado)	Seleccione esta opción para permitir que el sistema virtual reenvíe el contenido descifrado a un servicio exterior durante el reflejo de puerto o el envío de archivos de WildFire para análisis. Consulte también Reflejo del puerto de descifrado.
Pestaña General	Seleccione un objeto de **DNS Proxy (Proxy de DNS)**si desea aplicar reglas de proxy de DNS a este vsys. (Network [Red] > DNS Proxy). Para incluir objetos de un tipo particular, seleccione ese tipo (Interfaz, VLAN, Virtual Wire, enrutador virtual o sistema virtual visible), haga clic en **Add (Añadir)** y seleccione el objeto en el menú desplegable. Puede añadir uno o más objetos de cualquier tipo. Para eliminar un objeto, selecciónelo y haga clic en **Delete (Eliminar)**.
Pestaña Recurso	Especifique los siguientes límites de recursos permitidos para este vsys. 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 vsys coincide con el límite del modelo de cortafuegos en cuestión. No obstante, el límite de un ajuste concreto no se reproduce en todos los vsys. 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. • **Sessions Limit (Límite de sesiones)**: número máximo de sesiones. *Si utiliza el comando CLI `show session meter`, el cortafuegos mostrará la cantidad máxima de sesiones permitidas por plano de datos, la cantidad actual de*

© 2020 Palo Alto Networks, Inc.

Configuración de sistemas virtuales	Description (Descripción)
	sesiones que está utilizando el sistema virtual y la cantidad acelerada de sesiones por sistema virtual. En los cortafuegos de la serie PA-5200 o PA-7000, la cantidad actual de sesiones que se utiliza puede ser mayor que el máximo configurado para el límite de sesiones, ya que existen varios planos de datos por cada sistema 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. • **Security Rules (Reglas de seguridad)**: número máximo de reglas de seguridad. • **NAT Rules (Reglas NAT)**: número máximo de reglas de NAT. • **Decryption Rules (Reglas de descifrado)**: número máximo de reglas de descifrado. • **QoS Rules (Reglas QoS)**: número máximo de reglas de QoS. • **Application Override Rules (Reglas de cancelación de aplicación)**: número máximo de reglas de cancelación de aplicaciones. • **Policy Based Forwarding Rules (Reglas de reenvío basado en políticas)**: número máximo de reglas de reenvío basado en políticas (Policy Based Forwarding, PBF). • **Captive Portal Rules (Reglas de portal cautivo)**: número máximo de reglas de portal cautivo (CP). • **DoS Protection Rules (Reglas de protección DoS)**: número máximo de reglas de denegación de servicio (Denial-of-Service, DoS). • **Site to Site VPN Tunnels (Túneles VPN de sitio a sitio)**: número máximo de túneles de VPN de sitio a sitio. • **Concurrent GlobalProtect Tunnels (Túneles de GlobalProtect concurrentes)**: número máximo de usuarios de GlobalProtect remotos concurrentes. • **Inter-Vsys User-ID Data Sharing (Uso compartido de datos de User-ID entre sistemas virtuales)**: seleccione **Make this vsys a User-ID data hub (Convertir este sistema virtual en un concentrador de datos de User-ID)** para permitir que todos los demás sistemas virtuales del cortafuegos accedan a la información de asignación de usuario compartida o seleccione **Change hub (Cambiar concentrador)** y seleccione un nuevo sistema virtual para reasignar ese sistema virtual como concentrador de datos de User-ID. Requiere privilegios de superusuario o administrador.

© 2020 Palo Alto Networks, Inc.

Device > Shared Gateways

Las puertas de enlace compartidas permiten a los sistemas virtuales múltiples compartir una única comunicación externa (tradicionalmente conectada a una red ascendente común como un proveedor de servicios de Internet). El resto de sistemas virtuales se comunican con el mundo exterior a través de la interfaz física mediante una única dirección IP. Se utiliza un único enrutador virtual para enrutar el tráfico de todos los sistemas virtuales a través de la puerta de enlace compartida.

Las puertas de enlace compartidas utilizan interfaces de capa 3 y, como mínimo, una interfaz de capa 3 debe configurarse como puerta de enlace compartida. Las comunicaciones que se originan en un sistema virtual y que salen del cortafuegos mediante una puerta de enlace compartida requieren una política similar para las comunicaciones que pasan entre dos sistemas virtuales. Puede configurar una zona "Vsys externa" para definir las reglas de seguridad en el sistema virtual.

Configuración de puertas de enlace compartidas	Description (Descripción)
ID	Identificador de la puerta de enlace (no utilizado por el cortafuegos).
Nombre	Introduzca un nombre para la puerta de enlace compartida (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. Solo se requiere el nombre.
Proxy Dns	(Opcional) Si hay un proxy DNS configurado, seleccione qué servidores DNS se deben utilizar para las consultas de nombre de dominio.
Interfaces	Seleccione las interfaces que utilizará la puerta de enlace compartida.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Gestión de certificados

- Device > Certificate Management > Certificates
- Device > Certificate Management > Certificate Profile
- Device > Certificate Management > OCSP Responder
- Device > Certificate Management > SSL/TLS Service Profile
- Device > Certificate Management > SCEP
- Device > Certificate Management > SSL Decryption Exclusion

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > Certificates

Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivos)** para gestionar (generar, importar, renovar, eliminar y revocar) certificados, los cuales se utilizan para asegurar la comunicación en la red. También puede exportar e importar la clave de alta disponibilidad (HA) que protege la conexión entre los peers de HA en la red. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Default Trusted Certificate Authorities (Entidades de certificación de confianza predeterminadas)** para ver, habilitar y deshabilitar las entidades de certificación (CA) en las que confía el cortafuegos.

Para obtener más información sobre cómo implementar certificados en el cortafuegos y Panorama, consulte Gestión de certificados.

- Gestión de certificación de cortafuegos y Panorama
- Gestión de entidades de certificación de confianza predeterminadas
- Device > Certificate Management > Certificate Profile
- Device > Certificate Management > OCSP Responder
- Device > Certificate Management > SSL/TLS Service Profile
- Device > Certificate Management > SCEP
- Device > Master Key and Diagnostics

Gestión de certificación de cortafuegos y Panorama

- Device > Certificate Management > Certificates > Device Certificates
- Panorama > Certificate Management > Certificates

Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivos)** o **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivos)** para mostrar los certificados que el cortafuegos o Panorama utilizan para tareas como garantizar el acceso a la interfaz web, el descifrado SSL o LSVPN.

A continuación se mencionan algunos usos de los certificados. Defina el uso del certificado después de generarlo (consulte Gestión de Default Trusted Certificate Authorities).

- **Forward Trust (Reenvío fiable)**: el cortafuegos utiliza este certificado para firmar una copia del certificado del servidor que el cortafuegos presenta a los clientes durante el descifrado de proxy SSL de reenvío cuando la entidad de certificación (CA) que firmó el certificado del servidor está en la lista de CA de confianza en el cortafuegos.
- **Forward Untrust (Reenvío no fiable)**: el cortafuegos utiliza este certificado para firmar una copia del certificado del servidor que el cortafuegos presenta a los clientes durante el descifrado de proxy SSL de reenvío cuando la CA que firmó el certificado del servidor no está en la lista de CA de confianza en el cortafuegos.
- **Trusted Root CA (CA raíz de confianza)**: el cortafuegos usa este certificado como una CA de confianza para el descifrado de proxy de reenvío de SSL, GlobalProtect, la cancelación de admin de URL y Portal cautivo. El cortafuegos tiene una extensa lista de CA de confianza existentes. El certificado de CA raíz de confianza es para CA adicionales en las que su empresa confía pero que no forman parte de la lista de CA fiables preinstalada.

© 2020 Palo Alto Networks, Inc.

- **SSL Exclude (Exclusión en SSL)**: el cortafuegos usa este certificado si configura las excepciones de descifrado para que excluyan servidores específicos del cifrado SSL/TLS.
- **Certificate for Secure Syslog (Certificado de Syslog seguro)**: el cortafuegos usa este certificado para asegurar la entrega de logs como mensajes syslog a un servidor syslog.

Para generar un certificado, haga clic en Generate (Generar) y complete los siguientes campos:

Después de generar un certificado, la página muestra otras acciones admitidas para administrar certificados.

Configuración de Generate Certificate	Description (Descripción)
Tipo de certificado	Seleccione la entidad que emite el certificado. **Local**: el cortafuegos o Panorama generan el certificado. **SCEP**: un servidor SCEP (Simple Certificate Enrollment Protocol [Protocolo de inscripción de certificados simple]) genera el certificado y lo envía al cortafuegos o a Panorama.
Nombre del certificado	(Obligatorio) Especifique un nombre (hasta 63 caracteres en el cortafuegos o hasta 31 caracteres en Panorama) para identificar el certificado. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Perfil SCEP	(Solo certificados SCEP) Seleccione un **SCEP Profile (Perfil SCEP)** para definir cómo se comunica el cortafuegos o Panorama con un servidor SCEP y la configuración del certificado SCEP. Para obtener más información, consulte Device > Certificate Management > SCEP. Puede configurar un cortafuegos que sirva como portal de GlobalProtect para solicitar certificados de SCEP bajo demanda e implementar automáticamente los certificados en los endpoints. Los campos restantes del cuadro de diálogo Generate Certificate (Generar certificado) no se aplican a los certificados SCEP. Después de especificar el **Certificate Name (Nombre del certificado)** y el **SCEP Profile (Perfil SCEP)**, haga clic en **Generate (Generar)**.
Nombre común	(Obligatorio) Introduzca la dirección IP o FQDN que aparecerá en el certificado.
Lugar	En un cortafuegos que tiene más de un sistema virtual (vsys), seleccione **Shared (Compartido)** si quiere que el certificado esté disponible en cada vsys.
Firmado por	Para firmar el certificado, puede utilizar un certificado de entidad de certificación (CA) que haya importado en el cortafuegos. El certificado también puede ser autofirmado, en cuyo caso el cortafuegos será la CA. Si está utilizando Panorama, también tiene la opción de generar un certificado autofirmado para Panorama. Si ha importado certificados de CA o los ha emitido en el propio cortafuegos (autofirmados), el menú desplegable incluye los CA disponibles para firmar el certificado que está creando.

© 2020 Palo Alto Networks, Inc.

Configuración de Generate Certificate	Description (Descripción)
	Para generar una solicitud de firma de certificado (CSR), seleccione una **External Authority (CSR) [Autoridad externa (CSR)]**. Una vez que el cortafuegos genera el certificado y el par de claves, puede exportar el CSR y enviarlo a la CA para que lo firme.
entidad de certificación	Seleccione esta opción si quiere que el cortafuegos emita el certificado. Marcar este certificado como CA le permitirá utilizarlo para firmar otros certificados en el cortafuegos.
OCSP responder	Seleccione un perfil de respondedor OCSP en el menú desplegable (consulte Device > Certificate Management > OCSP Responder). El nombre de host correspondiente aparece en el certificado.
Algoritmo	Seleccione un algoritmo de generación de claves para el certificado: **RSA** o **Elliptic Curve DSA (DSA de curva elíptica)** (ECDSA). ECDSA usa tamaños de clave más pequeños que el algoritmo RSA y, por lo tanto, ofrece una mejora del rendimiento para las conexiones SSL/TLS de procesamiento. ECDSA también ofrece una seguridad igual o superior a la de RSA. Se recomienda ECDSA para los navegadores de clientes y los sistemas operativos que lo admitan, pero es posible que deba seleccionar RSA para que sea compatible con los navegadores y los sistemas operativos anteriores. *Los cortafuegos que usan 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 usar un módulo de seguridad de hardware (HSM) para guardar claves ECDSA privadas utilizadas para el descifrado de SSL Forward Proxy (Proxy SSL de reenvío) o Inbound Inspection (Inspección entrante).
Número de bits	Seleccione la longitud de la clave del certificado. Si el cortafuegos está en modo FIPS-CC y el **Algorithm (Algoritmo)** de generación de claves es **RSA**, las claves RSA generadas deben ser de **2048** o **3027** bits. Si el **Algorithm (Algoritmo)** es **Elliptic Curve DSA (DSA de curva elíptica)**, son válidas ambas opciones de longitud (**256** y **384**).
Resumen	Seleccione el algoritmo de **Digest (Resumen)** del certificado. Las opciones disponibles dependen de la generación de claves de **algoritmos**: • **RSA**: **MD5**, **SHA1**, **SHA256**, **SHA384** o **SHA512** • **Elliptic Curve DSA (DSA de curva elíptica)**: **SHA256** o **SHA384** Si el cortafuegos está en modo FIPS-CC y el **Algorithm (Algoritmo)** de generación de claves es **RSA**, debe seleccionar **SHA256**, **SHA384** o **SHA512** como el algoritmo de **Digest (Resumen)**. Si el **Algorithm (Algoritmo)** es **Elliptic Curve DSA (DSA de curva elíptica)**, son válidos ambos algoritmos de **Digest (Resumen)** (**SHA256** y **SHA384**).

© 2020 Palo Alto Networks, Inc.

Configuración de Generate Certificate	Description (Descripción)
	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 inferior (como SHA384) o bien debe limitar la Max Version (Versión máx.) a TLSv1.1 al configurar los perfiles de servicios SSL/TLS de los servicios de cortafuegos (consulte Device > Certificate Management > SSL/TLS Service Profile*).*
Vencimiento (días)	Indique la cantidad de días (el valor predeterminado es 365) que el certificado será válido. *Si especifica un Validity Period (Período de validez) en una configuración del satélite de GlobalProtect, ese valor cancelará el valor introducido en este campo.*
Atributos del certificado	Haga clic en **Add (Añadir)** para especificar **Certificate Attributes (Atributos del certificado)** adicionales que se deben utilizar para identificar la entidad para la que está emitiendo el certificado. Puede añadir cualquiera de los siguientes atributos: **Country (País)**, **State (Estado)**, **Locality (Población)**, **Organization (Organización)**, **Department (Departamento)** y **Email (Correo electrónico)**. Además, puede especificar uno de los siguientes campos de nombre alternativo del asunto: **Host Name (Nombre de host)** (SubjectAltName:DNS), **IP** (SubjectAltName:IP), y **Alt Email (Correo electrónico alt)** (SubjectAltName:email). *Para añadir un país como atributo de certificado, seleccione Country (País) en la columna Type (Tipo) y, a continuación, haga clic en la columna Value (Valor) para ver los códigos de país ISO 6366.*

Si ha configurado un módulo de seguridad de hardware (HSM), las claves privadas se almacenan en un almacén HSM externo, no en el cortafuegos.

Otras acciones admitidas para administrar certificados

Tras generar el certificado, sus detalles se muestran en la página y están disponibles las siguientes acciones:

Otras acciones admitidas para administrar certificados	Description (Descripción)
delete	Seleccione el certificado y después **Delete (Borrar)**.

© 2020 Palo Alto Networks, Inc.

Otras acciones admitidas para administrar certificados	Description (Descripción)
	Si el cortafuegos tiene una política de descifrado, no puede eliminar un certificado cuyo uso esté establecido como Forward Trust Certificate (Certificado de reenvío fiable) o Forward Untrust Certificate (Certificado de reenvío no fiable). Para cambiar el uso del certificado, consulte Gestión de entidades de certificación de confianza predeterminadas*.*
revocación	Seleccione el certificado que desea revocar y haga clic en **Revoke (Revocar)**. El certificado se establecerá instantáneamente en estado revocado. No es necesario realizar una compilación.
renovación	En caso de que un certificado caduque o esté a punto de caducar, seleccione el certificado correspondiente y haga clic en **Renew (Renovar)**. Establezca el periodo de validez (en días) para el certificado y haga clic en **OK (Aceptar)**. 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. Si una entidad de certificación (CA) externa firmó el certificado y el cortafuegos utiliza el protocolo OCSP (Online Certificate Status Protocol) para verificar el estado de revocación de certificados, el cortafuegos utiliza la información del respondedor OCSP para actualizar el estado del certificado.
Importar	Seleccione **Import (Importar)** un certificado y configúrelo de la siguiente manera: • Introduzca el nombre del certificado para identificarlo. • Busque el archivo del certificado. Si importa un certificado **PKCS12** y clave privada, un único archivo contiene ambos. Si importa un certificado **PEM**, el archivo contiene solo el certificado. *Importe los certificados individualmente. Si selecciona una cadena de certificados, el cortafuegos importará el primer certificado de la cadena.* • Seleccione el formato de archivo del certificado en **File Format (Formato de archivo)**. • Seleccione **Private key resides on Hardware Security Module (La clave privada reside en el módulo de seguridad de hardware)** si HSM almacena la clave de este certificado. Para obtener más información sobre HSM, consulte Device > Setup > HSM. • **Import private key (Importar clave privada)** si procede (solo formato PEM). Si selecciona **PKCS12** como certificado **File Format (Formato de archivo)**, el **Certificate File (Archivo del certificado)** seleccionado incluye la clave. Si selecciona el formato **PEM**, busque el archivo de clave privada cifrado (generalmente denominado *.key). En ambos casos, introduzca la información en los campos **Passphrase (Frase de contraseña)** y **Confirm Passphrase (Confirmar frase de contraseña)**.

© 2020 Palo Alto Networks, Inc.

Otras acciones admitidas para administrar certificados	Description (Descripción)
	Al importar un certificado a un cortafuegos de Palo Alto Networks o un servidor Panorama que se encuentre en modo FIPS-CC, debe importar el certificado como un certificado codificado en Base64 (PEM) y debe cifrar la clave privada con AES. Además, debe utilizar SHA1 como el método de derivación de claves basado en contraseña. Para importar un certificado PKCS12, convierta el certificado al formato PEM (con una herramienta como OpenSSL); asegúrese de que la contraseña que utiliza durante la conversión tiene al menos seis caracteres.
Exportar	Seleccione el certificado que desea exportar, haga clic en **Export (Exportar)** y seleccione el formato de archivo en **File Format (Formato de archivo)**: • Encrypted Private Key and Certificate (PKCS12): Clave privada cifrada y certificado; el archivo exportado tendrá tanto el certificado como la clave privada. • Base64 Encoded Certificate (PEM): Certificado codificado en Base64; si desea exportar la clave privada también, seleccione Export Private Key (Exportar clave privada) e introduzca una frase de contraseña en Passphrase (Frase de contraseña) y Confirm Passphrase (Confirmar frase de contraseña). • Binary Encoded Certificate (DER): Certificado codificado binario; solo puede exportar el certificado, no la clave; ignore los campos Export Private Key (Exportar clave privada) y de frase de contraseña.
Importar clave de HA Exportar clave de HA	Las claves de HA se deben intercambiar entre ambos peers del cortafuegos; es decir, se debe exportar la clave del cortafuegos 1 y, a continuación, importarse al cortafuegos 2 y viceversa. Para importar claves para alta disponibilidad (HA), haga clic en **Import HA Key (Importar clave de HA)** y en **Browse (Buscar)** para especificar el archivo de clave que se importará. Para exportar claves para HA, haga clic en **Export HA Key (Exportar clave de HA).** y especifique una ubicación en la que guardar el archivo.
Defina el uso del certificado	En la columna Name, seleccione el certificado y las opciones de selección para indicar cómo planea utilizar el certificado.
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de configuración de certificado gestionado como **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla para elementos como las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.

© 2020 Palo Alto Networks, Inc.

Gestión de entidades de certificación de confianza predeterminadas

- Device > Certificate Management > Certificates > Default Trusted Certificate Authorities

Utilice esta página para ver, deshabilitar o exportar las entidades de certificación (CA) preincluidas en las que confía el cortafuegos. La lista de CA instalada previamente incluye los proveedores de certificados más comunes y de confianza responsables de emitir los certificados que requiere el cortafuegos para asegurar conexiones a internet. Para cada CA raíz de confianza, se muestra el nombre, asunto, emisor, fecha de vencimiento y estado de validez.

El cortafuegos no confía en CA intermedios de manera predeterminada debido a que no forman parte de una cadena de confianza entre el cortafuegos y la CA raíz de confianza. Debe añadir manualmente las CA intermedias en las que desee que el cortafuegos confíe, además de las CA empresariales de confianza adicionales que su organización requiera (**Device [Dispositivo]** > **Certificate Management [Gestión de certificados]** > **Certificates [Certificados]** > **Device Certificates [Certificados de dispositivos]**).

Configuración de entidades de certificación de confianza	Description (Descripción)
Habilitación	Si deshabilitó una entidad de certificación, puede volver a **habilitarla**.
Deshabilitar	Seleccione la entidad de certificación y **deshabilítela**. Es posible que use esta opción para confiar solo en entidades de certificación específicas o para deshabilitar todas ellas y confiar solo en su entidad de certificación local.
Exportar	Seleccione **Export** para exportar el certificado de CA. Puede importar el certificado a otro sistema o ver el certificado sin conexión.

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > Certificate Profile

- **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**
- **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)**

Los perfiles del certificado especifican qué certificados de la entidad de certificación (CA) deben utilizarse para verificar los certificados de clientes, cómo verificar el estado de revocación de certificados y cómo restringe el acceso dicho estado. Los perfiles se seleccionan al configurar la autenticación del certificado para el acceso de Captive Portal, GlobalProtect, VPN de sitio a sitio de IPSec, DNS dinámico (Dynamic DNS, DDNS) e interfaces web a cortafuegos y Panorama. Puede configurar un perfil de certificado independiente para cada uno de estos servicios.

Configuración de perfiles de certificado	Description (Descripción)
Nombre	(Obligatorio) Especifique un nombre para identificar el perfil (hasta 63 caracteres en el cortafuegos o hasta 31 caracteres en Panorama). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Campo de nombre de usuario	Si GlobalProtect usa solo certificados para la autenticación de portal y puerta de enlace, PAN-OS usa el campo de certificado que seleccione en el menú desplegable **Username Field (Campo de nombre de usuario)** como el nombre de usuario, y busca coincidencias con la dirección IP del servicio User-ID: • **Subject (Asunto)**: el nombre común. • **Subject Alt (Asunto alternativo)**: el correo electrónico o nombre principal • **None (Ninguno)**: Suele destinarse al dispositivo GlobalProtect o a la autenticación anterior al inicio de sesión.
Dominio	Introduzca el dominio NetBIOS, para que PAN-OS pueda asignar a los usuarios mediante User-ID.
Certificados de CA	(Obligatorio) Haga clic en **Add (Añadir)** para añadir un **CA Certificate (Certificado de CA)** para asignar al perfil. Opcionalmente, si el cortafuegos utiliza el protocolo de estado de certificado en línea (OCSP) para verificar el estado de revocación

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de certificado	Description (Descripción)
	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 la información de acceso a información de entidad emisora (Authority Information Access, AIA) del certificado para extraer la información del respondedor 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 diferente para la validación, selecciónelo en el campo **OCSP Verify CA Certificate (Verificación de certificado CA con OCSP)**. Además, introduzca un **Template Name (Nombre de plantilla)** para identificar la plantilla que se utilizó para firmar el certificado.
Utilizar CRL	Seleccione esta opción para utilizar la lista de revocación de certificados (CRL) y verificar el estado de revocación de los certificados.
Utilizar OCSP	Seleccione esta opción para utilizar OCSP y verificar el estado de revocación de los certificados. *Si selecciona OCSP y CRL, el cortafuegos primero intentará utilizar el OCSP y solamente retrocederá al método CRL si el respondedor OCSP no está disponible.*
Tiempo de espera de recepción de CRL	Especifique el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta del servicio CRL.
Tiempo de espera de recepción de OCSP	Especifique el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta del OCSP responder.
Tiempo de espera del estado del certificado	Especifique el intervalo (1-60 segundos) tras el cual el cortafuegos deja de esperar una respuesta de cualquier servicio de estado de certificados y aplica la lógica de bloqueo de sesión que defina.
Bloquear una sesión si el estado del certificado es desconocido	Seleccione esta opción si desea que el cortafuegos bloquee sesiones cuando el servicio OCSP o CRL devuelva un estado de revocación de certificados desconocido (*unknown*). De lo contrario, el cortafuegos continuará con la sesión.
Bloquear sesiones si no se puede recuperar el estado del certificado dentro del tiempo de espera	Seleccione esta opción si desea que el cortafuegos bloquee sesiones después de registrar un tiempo de espera de la solicitud de OCSP o CRL. De lo contrario, el cortafuegos continuará con la sesión.

© 2020 Palo Alto Networks, Inc.

Configuración de perfiles de certificado	Description (Descripción)
Block sessions if the certificate was not issued to the authenticating device (Bloquear sesión si el certificado no se emitió para un dispositivo de autenticación)	(Solo GlobalProtect) Seleccione esta opción si usted 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. De lo contrario, el cortafuegos permitirá las sesiones. Esta opción se aplica solo a la Autenticación de certificados de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > OCSP Responder

Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **OCSP Responder (Respondedor OCSP)** para definir un respondedor (servidor) del protocolo de estado de certificado en línea (Online Certificate Status Protocol, OCSP) que verifique el estado de la revocación de los certificados.

Además de añadir un OCSP responder, habilitar un OCSP requiere las siguientes tareas:

- Habilitar la comunicación entre el cortafuegos y el servidor de OCSP: seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, seleccione **HTTP OCSP** en Management Interface Settings (Configuración de interfaz de gestión) y haga clic en **OK (Aceptar)**.
- Si el cortafuegos descifra el tráfico SSL/TLS saliente, de manera opcional, configúrelo para verificar el estado de revocación de los certificados del servidor de destino: seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Sessions (Sesiones)**, haga clic en **Decryption Certificate Revocation Settings (Configuración de revocación de certificado de descifrado)**, seleccione **Enable (Habilitar)** en la configuración de OCSP, introduzca el valor de **Receive Timeout (Tiempo de espera de recepción)** (intervalo después del cual el cortafuegos deja de esperar una respuesta del OCSP) y, a continuación, haga clic en **OK (Aceptar)**.
- Opcionalmente, para configurar el cortafuegos como OCSP responder, añada un perfil de gestión de interfaz a la interfaz utilizada para servicios OCSP. En primer lugar, seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt** (Gestión de interfaz), haga clic en **Add (Añadir)**, seleccione **HTTP OCSP** y, a continuación, haga clic en **OK (Aceptar)**. En segundo lugar, seleccione **Network (Red)** > **Interfaces** haga clic en el nombre de la interfaz que utilizará el cortafuegos para los servicios del OCSP, seleccione **Advanced (Avanzado)** > **Other info (Otra información)**, seleccione el perfil de gestión de la interfaz que ha configurado y, a continuación, haga clic en **OK (Aceptar)** y **Commit (Confirmar)**.

Habilite un respondedor OCSP para que, si se revoca un certificado, usted reciba una notificación y pueda tomar las medidas apropiadas para establecer una conexión segura con el portal y las puertas de enlace.

Configuración de OCSP Responder	Description (Descripción)
Nombre	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.
Ubicación	Seleccione el ámbito en el que está disponible el respondedor. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido. Una vez guardado el respondedor, no puede cambiar su **Location (Ubicación)**.
Nombre de host	Especifique el nombre de host (recomendado) o la dirección IP del respondedor OCSP. A partir de este valor, PAN-OS deriva automáticamente una URL y la añade al certificado que se está verificando. Si configura el cortafuegos como respondedor OCSP,

© 2020 Palo Alto Networks, Inc.

Configuración de OCSP Responder	Description (Descripción)
	el nombre de host debe resolverse en una dirección IP de la interfaz que utiliza el cortafuegos para servicios de OCSP.

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > SSL/TLS Service Profile

- Device > Certificate Management > SSL/TLS Service Profile
- Panorama > Certificate Management > SSL/TLS Service Profile

Los perfiles de servicio SSL/TLS especifican un certificado de servidor y una versión o conjunto de versiones de protocolo para servicios de cortafuegos y Panorama que utilizan SSL/TLS (como el acceso administrativo a la interfaz web). Mediante la definición de versiones de protocolo, los perfiles le permiten restringir los conjuntos de cifras disponibles para proteger la comunicación con los sistemas clientes que solicitan los servicios.

En los sistemas cliente que solicitan servicios de cortafuegos o Panorama, 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 verán un error de certificado al solicitar los servicios. 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.

Para añadir un perfil, haga clic en **Add (Añadir)**, rellene los campos en la siguiente tabla.

Configuración de perfil de servicio SSL/TLS	Description (Descripción)
Nombre	Introduzca un nombre para identificar el perfil (de hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas. Debe ser exclusivo y utilizar únicamente letras, números, espacios, guiones y guiones bajos.
Lugar	Si el cortafuegos tiene más de un sistema virtual (vsys), puede seleccionar esta opción para que el perfil esté disponible en todos los sistemas virtuales. De manera predeterminada, esta opción no está seleccionada y el perfil está disponible solo para el vsys seleccionado en la pestaña **Device (Dispositivo)**, en el menú desplegable **Location (Ubicación)**.
Certificado	Seleccione, importar o generar un certificado de servidor para asociarlo con el perfil (consulte Manage Firewall and Panorama Certificates). *No use certificados de entidades de certificación (CA) para servicios SSL/TLS; use solo certificados firmados.*
Versión mín.	Seleccione las versiones más antiguo (**Min Version (Versión Mín.)**) y más reciente (**Max Version (Versión máx.)**) de TLS que los servicios pueden utilizar: **TLSv1.0**, **TLSv1.1**, **TLSv1.2** o **Max (Máx.)** (la versión más reciente disponible).
Versión máx.	

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de servicio SSL/TLS	Description (Descripción)
	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. *Los certificados de cliente que se utilizan al solicitar servicios de cortafuegos que dependen de TLSv1.2 no puede tener SHA512 como un 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.* *Utilice la versión más potente que pueda del protocolo para brindar la máxima seguridad a su red. Si puede, configure la Min Version (Versión mínima) en TLSv1.2 y la Max Version (Versión máxima) en Max (Máximo).*

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > SCEP

El protocolo de inscripción de certificados simple (simple certificate enrollment protocol, SCEP) ofrece un mecanismo para emitir un único certificado a puertas de enlace, endpoints y dispositivos satélite. Seleccione **Device (dispositivo)** > **Certificate Management (Gestión de certificados)** > **SCEP** para crear una configuración de SCEP.

Para obtener más información sobre cómo crear un perfil de SCEP, consulte Implementación de certificados utilizando SCEP

.

Para añadir una configuración de SCEP, haga clic en **Add (añadir)** y, a continuación, complete los siguientes campos.

Ajustes SCEP	Description (Descripción)
Nombre	Especifique un nombre descriptivo para identificar esta configuración de SCEP, por ejemplo, *SCEP*_Example. Este nombre distingue un perfil de SCEP de otras instancias que podría tener en los perfiles de configuración.
Ubicación	Seleccione una ubicación del perfil si el sistema posee múltiples sistemas virtuales. La ubicación identifica dónde está disponible la configuración de SCEP.
Contraseña de un uso (reto)	
Reto SCEP	(Opcional) Para que la generación de certificados basada en SCEP sea más segura, puede configurar un mecanismo de respuesta de reto de SCEP [una contraseña de una vez (one-time password, OTP)] entre la infraestructura de clave pública (key infrastructure, 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.* El mecanismo de comprobación que seleccione determina el origen de la OTP. Si selecciona **Fixed (Fijo)**, copie la contraseña de comprobación de inscripción del servidor SCEP para la PKI e introduzca la cadena en el cuadro de diálogo del portal **Password (Contraseña)** que aparece cuando se configura como **Fijo**. Cada vez que el portal solicita un certificado, utiliza esta contraseña para autenticarse con la PKI. Si selecciona **Dynamic (Dinámico)**: 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. Este nombre de usuario y contraseña permanecen igual mientras que el servidor SCEP genera una contraseña de OTP para el portal en cada solicitud de certificado. (Puede ver este cambio de OTP después de una actualización de pantalla en el campo "The enrollment challenge password is" [La contraseña de comprobación de inscripción es] en cada solicitud de certificado). La PKI aprueba cada contraseña nueva de manera

© 2020 Palo Alto Networks, Inc.

Ajustes SCEP	Description (Descripción)
	transparente en el portal, el cual luego utiliza la contraseña para su solicitud de certificado. *Para cumplir con el Estándar federal de procesamiento de información (Federal Information Processing Standard, FIPS) de EE. UU, seleccione Dynamic (Dinámico), especifique una Server URL (URL de servidor) que use HTTPS, y habilite SCEP Server SSL Authentication (Autenticación SSL del servidor SCEP). (La operación de FIPS-CC se indica en el inicio de sesión del cortafuegos y en la barra de estado el cortafuegos).*
Configuración	
URL del servidor	Introduzca la URL en la cual el portal solicite y reciba certificados de clientes del servidor SCEP. Ejemplo: `http://<hostname or IP>/certsrv/mscep/.`
Nombre de CA-IDENT	Introduzca la cadena para identificar el servidor SCEP. La longitud máxima es de 255 caracteres.
Asunto	Configure el Asunto para incluir información de identificación sobre el dispositivo y opcionalmente el usuario y proporcione esta información en la solicitud de firma de certificado (CSR) al servidor SCEP. Cuando se usa para solicitar certificados de cliente para endpoints, el endpoint envía información de identificación del dispositivo 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). Cuando se utiliza para solicitar certificados para dispositivos satélite, el valor de ID de host es el número de serie del dispositivo. Para especificar información adicional en el CSR, introduzca el nombre del sujeto. El nombre de asunto debe ser un nombre distinguido en el formato *<atributo>=<valor>* y debe incluir la clave de nombre común (CN). Por ejemplo: `O=acme,CN=acmescep` Hay dos formas de especificar el CN: • (Recomendado) **CN basado en token**: Introduzca uno de los tokens compatibles **`$USERNAME`**, **`$EMAILADDRESS`**, O **`$HOSTID`**. Utilice la variable de nombre de usuario o dirección de correo electrónico para garantizar que el portal solicite certificados para un usuario específico. Para solicitar certificados únicamente para el dispositivo, especifique la variable de hostid. 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, hostid o dirección de correo electrónico) del propietario del certificado. Por ejemplo:

© 2020 Palo Alto Networks, Inc.

Ajustes SCEP	Description (Descripción)

	`O=acme,CN=$HOSTID`
	• **CN estático**: El nombre común que especifique no se usará como asunto para todos los certificados que emita el servidor SCEP. Por ejemplo:
	`O=acme,CN=acmescep`

Tipo de nombre alternativo de asunto	*Utilice entradas estáticas para el tipo de Nombre Alternativo del Asunto. El cortafuegos no admite tokens dinámicos como* ***$USERNAME****.* Luego de seleccionar un tipo diferente a **None (Ninguno)**, se muestra un cuadro de diálogo para que introduzca el valor apropiado. • **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 (URI) [Identificador uniforme de recursos (URI)]**: ingrese el nombre del recurso URI desde el cual el cliente obtiene el certificado.
Configuración criptográfica	• **Number of Bits (Número de bits)**: Seleccione el número de bits de la clave en **Number of Bits (Número de bits)** para el certificado. Si el cortafuegos está en modo FIPS-CC, las claves generadas deben ser de al menos 2.048 bits. (La operación de FIPS-CC se indica en el inicio de sesión del cortafuegos y en la barra de estado el cortafuegos). • **Digest (Resumen)**: seleccione el algoritmo de resumen en **Digest (Resumen)** del certificado: **SHA1**, **SHA256**, **SHA384** o **SHA512**. Si el cortafuegos está en modo FIPS-CC, debe seleccionar **SHA256**, **SHA384** o **SHA512** como el algoritmo de resumen en **Digest (Resumen)**.
Usar como firma digital	Seleccione esta opción para que el extremo use la clave privada en el certificado para validar una firma digital.
Usar para el cifrado de clave	Seleccione esta opción para que el extremo del cliente use la clave privada en el certificado para cifrar los datos intercambiados en la conexión HTTPS establecida con los certificados emitidos por el servidor SCEP.
Huella digital de certificado CA	(Opcional) Para garantizar que el portal se conecte al servidor SCEP correcto, introduzca la **CA Certificate Fingerprint (Huella digital de certificado CA)**. Obtenga esta huella en la interfaz del servidor SCEP en el campo **Thumbprint (Huella digital)**. Inicie sesión en la interfaz de usuario administrativo del servidor SCEP (por ejemplo, en http://<hostname or IP>/CertSrv/mscep_admin/). Copie la huella e introdúzcala en **CA Certificate Fingerprint (Huella digital de certificado CA)**.

© 2020 Palo Alto Networks, Inc.

Ajustes SCEP	Description (Descripción)
Autenticación SSl de servidor SCEP	Para habilitar SSL, seleccione la raíz **CA Certificate (Certificado CA)** para el 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)**.

© 2020 Palo Alto Networks, Inc.

Device > Certificate Management > SSL Decryption Exclusion

Ver y administrar las Exclusiones de descifrado de SSL. Existen dos tipos de exclusiones de descifrado, exclusiones predefinidas y exclusiones personalizadas:

- Las exclusiones de descifrado predefinidas permiten que las aplicaciones y los servicios que pueden fallar cuando el cortafuegos los descifren permanezcan cifrados. Palo Alto Networks define las exclusiones de descifrado predefinidas y entrega actualizaciones y adiciones a la lista de exclusiones predefinidas a intervalos regulares como parte de la actualización de contenido de aplicaciones y amenazas. Las exclusiones predefinidas están habilitadas de forma predeterminada, pero puede optar por deshabilitar la exclusión según sea necesario.
- Puede crear exclusiones de descifrado personalizadas para excluir el tráfico de servidor del descifrado. Todo el tráfico proveniente o destinado al servidor de destino permanecerá cifrado.

Puede también excluir el tráfico del descifrado basándose en el origen, destino, categoría de URL y servicio.

Utilice los ajustes de esta página para Modificar o agregar una exclusión de descifrado y para Administrar exclusiones de descifrado.

Configuración de exclusiones de descifrado SSL	Description (Descripción)
Modificar o **Add (Añadir)** una exclusión de descifrado	
Nombre de host	Introducir un **Hostsname (Nombre de host)** para definir una exclusión de descifrado personalizada. El cortafuegos compara el nombre de host con el SNI solicitado por el cliente o con el CN presentado en el certificado del servidor. El cortafuegos excluye las sesiones en las que el servidor presenta un CN que contiene el dominio definido del descifrado. 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.

© 2020 Palo Alto Networks, Inc.

Configuración de exclusiones de descifrado SSL	Description (Descripción)
	• 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 no coincide con google.com porque una etiqueta (dev) no es un comodín.* Los nombres de host deben ser únicos para cada entrada: si se entrega una entrada predefinida al cortafuegos que coincide con una entrada personalizada existente, la entrada personalizada tendrá prioridad. No puede editar el nombre de host para una exclusión de descifrado predefinida.
Lugar	Seleccionar **Shared (Compartido)** para compartir una exclusión de descifrado en todos los sistemas virtuales en un cortafuegos de sistema virtual múltiple. Si bien las exclusiones de descifrado predefinidas se comparten de forma predeterminada, puede habilitar e inhabilitar entradas predefinidas y personalizadas para un sistema virtual específico.
Description (Descripción)	(Opcional) Describa la aplicación que está excluyendo del descifrado, incluyendo por qué la aplicación falla al descifrarse.
Excluir	Excluya la aplicación del descifrado. Deshabilite esta opción para iniciar el descifrado de una aplicación que anteriormente estaba excluida del descifrado.
Administrar exclusiones de descifrado	
Habilitación	**Enable (Habilitar)** una o más entradas para excluirlas del descifrado.
Deshabilitar	**Disable (Inhabilitar)** una o más exclusiones de descifrado predefinidas. Dado que las exclusiones de descifrado identifican las aplicaciones que fallan cuando se descifran, la desactivación de una de estas entradas hará que la aplicación no sea compatible. El cortafuegos intentará descifrar la aplicación y la aplicación fallará. Puede utilizar esta opción si desea asegurarse de que ciertas aplicaciones cifradas no entren en su red.
Mostrar obsoletos	**Show obsoletes (Mostrar obsoletos)** para ver entradas predefinidas que Palo Alto Networks ya no define como exclusiones de descifrado. **Más información sobre entradas obsoletas:**

© 2020 Palo Alto Networks, Inc.

Configuración de exclusiones de descifrado SSL	Description (Descripción)
	Las actualizaciones de las exclusiones de descifrado predefinidas (incluida la eliminación de una entrada predefinida) se envían al cortafuegos como parte de las actualizaciones de contenido de Aplicaciones y amenazas. Las entradas predefinidas con **Exclude from decryption (Excluir del descifrado)** habilitado se eliminan automáticamente de la lista de exclusiones de descifrado SSL cuando el cortafuegos recibe una actualización de contenido que ya no incluye esa entrada. Sin embargo, las entradas predefinidas con **Exclude from decryption (Excluir del descifrado)** desactivado permanecen en la lista de descifrado SSL incluso después de que el cortafuegos reciba una actualización de contenido que ya no incluya esa entrada. Cuando elija **Show obsoletes (Mostrar obsoletos)**, verá estas entradas predefinidas inhabilitadas que no se están aplicando actualmente; puede eliminar estas entradas manualmente según sea necesario.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Páginas de respuesta

Las páginas de respuesta personalizadas son las páginas web que se muestran cuando un usuario intenta acceder a una URL. Puede proporcionar un mensaje HTML personalizado que se descargará y mostrará en lugar del archivo o la página web que ha solicitado.

Cada sistema virtual puede tener sus propias páginas de respuesta personalizadas. La siguiente tabla describe los tipos de páginas de respuesta personalizadas que admiten mensajes del cliente.

Tipos de páginas de respuesta personalizadas	Description (Descripción)
Página de bloqueo de antivirus	Acceso bloqueado debido a una infección por virus.
Página de bloqueo de aplicación	Acceso bloqueado debido a que la aplicación está bloqueada por una regla de política de seguridad.
Página de comodidad de portal cautivo	El cortafuegos muestra esta página para que los usuarios puedan introducir las credenciales de inicio de sesión para acceder a los servicios sujetos a las reglas de políticas de autenticación (consulte Policies > Authentication). Introduzca un mensaje que indique a los usuarios cómo responder a este desafío de autenticación. El cortafuegos autentica a los usuarios basándose en el **Authentication Profile (Perfil de autenticación)** especificado en el objeto de cumplimiento de autenticación asignado a una regla de autenticación (consulte Objects > Authentication). *Puede mostrar instrucciones de autenticación únicas para cada regla de autenticación introduciendo un Message (Mensaje) en el objeto de aplicación de autenticación asociado. El mensaje definido en el objeto cancela el mensaje definido en la página Captive Portal Comfort.*
Página de bloqueo de filtrado de datos	El contenido se comparó con un perfil de filtrado de datos y se bloqueó, debido a que se detectó información confidencial.
Página de opción continua de bloqueo de archivo	Página para que los usuarios confirmen que la descarga debe continuar. Esta opción únicamente está disponible si la funcionalidad Continue (Continuar) está habilitada en el perfil de seguridad. Seleccione Objetos > Perfiles de seguridad > Bloqueo de archivo.
Página de bloqueo de bloqueo de archivo	Acceso bloqueado debido a que el acceso al archivo está bloqueado.
Página de ayuda de aplicación de GlobalProtect	Página de ayuda personalizada para los usuarios de GlobalProtect (disponible en el menú de configuración del panel de estado de GlobalProtect).
Página de inicio de sesión de portal de GlobalProtect	Página de inicio de sesión para los usuarios que intentan autenticarse en la página web del portal de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Tipos de páginas de respuesta personalizadas	Description (Descripción)
Página de inicio del portal de GlobalProtect	Página de inicio para los usuarios que se autentican correctamente en la página web del portal de GlobalProtect.
Página de bienvenida de aplicación de GlobalProtect	Página de bienvenida para los usuarios que se conectan correctamente a GlobalProtect.
Página de inicio de sesión de MFA	El cortafuegos muestra esta página para que los usuarios puedan responder a los desafíos de autenticación de múltiples factores (MFA) al acceder a los servicios sujetos a las reglas de la política de autenticación (consulte Policies > Authentication). Introduzca un mensaje que indique a los usuarios cómo responder a los desafíos del MFA.
Página de error interno de autenticación SAML	Página para informar a los usuarios de que la autenticación SAML ha fallado. La página incluye un enlace para que el usuario vuelva a intentar la autenticación.
Página de notificación de errores de certificado SSL	Notificación de que un certificado SSL se ha revocado.
Página de exclusión de descifrado de SSL	La página de advertencia de usuario que indica que el cortafuegos descifrará las sesiones SSL para una inspección.
Página de bloqueo de coincidencia de categoría y filtro de URL	Acceso bloqueado por un perfil de filtrado de URL o porque la categoría de URL está bloqueada por una regla de política de seguridad.
Página de continuación y cancelación de filtrado de URL	Página con política de bloqueo inicial que permite que los usuarios deriven el bloqueo. Por ejemplo, un usuario que piense que la página se bloqueó de manera inadecuada puede hacer clic en **Continue (Continuar)** para ir a la página. Con la página de cancelación, el usuario necesita una contraseña para cancelar la política que bloquea esta URL. Consulte la sección Cancelación de administrador de URL para obtener instrucciones sobre cómo configurar la contraseña de cancelación.
Página de bloqueo de aplicación de búsqueda segura de filtro 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 forzada de búsquedas seguras)**. El usuario ve esta página si se realiza una búsqueda con Bing, Google, Yahoo, Yandex o YouTube y la configuración de cuenta de su explorador o motor de búsqueda no está establecida como estricta. La página de bloque pedirá al usuario que establezca la configuración de búsqueda segura como estricta.
Página de bloqueo antiphishing	Se muestra a los usuarios cuando intentan introducir credenciales corporativas válidas (nombres de usuario o contraseñas) en una página web para la que se bloquea la presentación de credenciales. El usuario puede seguir accediendo al sitio, pero sigue sin poder enviar credenciales corporativas válidas a formularios web asociados.

© 2020 Palo Alto Networks, Inc.

Tipos de páginas de respuesta personalizadas	Description (Descripción)
	Seleccione Objects > Security Profiles > URL Filtering para permitir la detección de credenciales y controlar las solicitudes de credenciales a páginas web basadas en la categoría de URL.
Página de continuación antiphishing	Esta página advierte a los usuarios contra la presentación de credenciales corporativas (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. Los usuarios ven esta página cuando intentan enviar credenciales a un sitio para el cual los permisos de **User Credential Submission (Envío de credencial de usuario)** se establecen como **continue (continuar)** (ver Objects > Security Profiles > URL Filtering). Deben seleccionar **Continue (Continuar)** para introducir credenciales en el sitio.

Puede realizar cualquiera de las siguientes funciones para **Response Pages (Páginas de respuesta)**:

- Para importar una página de respuesta HTML personalizada, haga clic en el enlace del tipo de página que desee cambiar y, a continuación, haga clic en Importar o Exportar. Explore para ubicar la página. Se mostrará un mensaje para indicar si la importación se ha realizado con éxito. Para que la importación tenga éxito, el archivo debe estar en formato HTML.
- Para exportar una página de respuesta HTML personalizada, haga clic en **Export (Exportar)** del tipo de página. Seleccione si abrir el archivo o guardarlo en el disco y, si corresponde, seleccione **Always use the same option (Usar siempre la misma opción)**.
- Para habilitar o deshabilitar la página **Application Block (bloqueo de aplicación)** o las páginas **SSL Decryption Opt-out (Exclusión de descifrado SSL)**, haga clic en el enlace **Enable (Habilitar)** del tipo de página. Seleccione o anule la selección de **Enable (Habilitar)**, según corresponda.
- Para usar la página de respuesta predeterminada de una página personalizada cargada anteriormente, elimine la página de bloqueo personalizada y realice una compilación. Esto establecerá la página de bloqueo predeterminada como la nueva página activa.

© 2020 Palo Alto Networks, Inc.

Device > Log Settings

Seleccione **Device** > **Log Settings** (Dispositivo > Configuración de log) para configurar alarmas, borrar logs, o habilitar el reenvío de logs a Panorama, al servicio de creación de logs y a otros servicios externos.

- Selección de destinos de reenvío de logs
- Definición de la configuración de alarma
- Borrar logs

Selección de destinos de reenvío de logs

Device (Dispositivo) > Log Settings (Configuración de log)

La página Log Settings (Configuración de log) le permite configurar el reenvío de logs a los siguientes destinos:

- **Panorama, receptores de traps de SNMP, servidores de correo electrónico, servidores Syslog y servidores HTTP**: también puede añadir o eliminar etiquetas de una dirección IP de origen o de destino en una entrada de log; todos los tipos de logs, excepto los logs del sistema y los logs de configuración admiten el etiquetado.
- **Servicio de creación de logs:** si posee una suscripción al servicio de creación de logs y el servicio de creación de logs está habilitado (Device [Dispositivo] > Setup [Configuración] > Management [Gestión]), el cortafuegos enviará los logs al servicio de creación de logs cuando configure el reenvío de logs a Panorama/servicio de creación de logs. Panorama enviará consultas al servicio de creación de logs para acceder a los logs, mostrar los logs y generar informes.
- **Azure Security Center (Centro de seguridad de Azure):** la integración con el centro de seguridad de Azure está disponible solo en los cortafuegos serie VM en Azure.
  - Si inició un cortafuegos serie VM del centro de seguridad de Azure, se habilita automáticamente una regla de la política de seguridad con los perfiles de reenvío de logs.
  - Si inició un cortafuegos serie VM desde el mercado de Azure o utilizando plantillas Azure personalizadas, debe seleccionar manualmente **Azure-Security-Center-Integration** para reenviar logs del sistema, logs de User-ID y logs de coincidencias HIP al centro de seguridad de Azure, y utilizar el perfil de reenvío de logs de otros tipos de logs (consulte Objects [Objetos] > Log Forwarding [Reenvío de logs]).

    El nivel libre del centro de seguridad se habilita automáticamente en su suscripción de Azure.

Puede reenviar los siguientes tipos de logs : Sistema, Configuración, User-ID, HIP Match y Correlación. Para especificar destinos para cada tipo de log, seleccione **Add (Añadir)** uno o más perfiles de la lista de coincidencias (hasta 64) y complete los campos descritos en la siguiente tabla.

Para enviar logs de tráfico, amenazas, WildFire, filtrado de URL, filtrado de datos, inspección de túnel, GTP y autenticación, debe configurar un perfil de reenvío de logs (consulte Objects > Log Forwarding).

Configuración del perfil de la lista de coincidencias	Description (Descripción)
Nombre	Introduzca un nombre (hasta 31 caracteres) para el perfil de la lista de coincidencias. Un nombre válido debe empezar por un carácter

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de la lista de coincidencias	Description (Descripción)
	alfanumérico y puede contener ceros, caracteres alfanuméricos, guiones bajos, guiones, puntos o espacios.
Filter (Filtro)	De forma predeterminada, el cortafuegos envía **All Logs (Todos los logs)** del tipo para el que agrega el perfil de lista de coincidencias. Para enviar un subconjunto de logs, abra el menú desplegable y seleccione un filtro existente o seleccione **Filter Builder (Generador de filtro)** para añadir un nuevo filtro. En cada nueva aplicación de filtro, especifique los siguientes campos y haga clic en **Add (Añadir)** para incluir la consulta: • **Connector (Conector)**: seleccione la lógica del conector (AND/OR) para la consulta. Seleccione **Negate (Negar)** si desea aplicar la negación a la lógica. Por ejemplo, para evitar el reenvío de logs desde una zona no fiable, seleccione **Negate (Negar)**, **Zone (Zona)** como atributo, **equal (igual)** como operador e introduzca el nombre de la zona no fiable en la columna Value (Valor). • **Attribute (Atributo)**: seleccione un atributo de log. Los atributos disponibles varían según el tipo de log. • **Operator (Operador)**: seleccione el criterio para determinar si se aplica el atributo (como **equal [igual]**). Los criterios disponibles varían según el tipo de log. • **Value (Valor)**: Especifique el valor del atributo para coincidir. Para ver o exportar los logs que coinciden con el filtro, seleccione **View Filtered Logs (Ver logs filtrados)**. Esta pestaña ofrece las mismas opciones que las páginas de la pestaña **Monitoring** (Supervisión) (como **Monitoring [Supervisión]** > **Logs [Logs]** > **Traffic [Tráfico]**). *Configure el filtro para el reenvío de logs para todos los niveles de gravedad del evento (el filtro predeterminado es All Logs [Todos los logs]). Para crear métodos de reenvío de log separados para diferentes niveles de gravedad, especifique uno o varios niveles de gravedad en Filter (Filtro), configure un Forward Method (Método de reenvío) y luego repita el proceso para el resto de los niveles de gravedad.*
Description (Descripción)	Introduzca una descripción (hasta 1023 caracteres) para explicar el propósito de este perfil de lista de coincidencias.
Panorama/Logging Service (Servicio de creación de logs)	Seleccione **Panorama/Logging Service (Servicio de creación de logs)** si desea reenviar logs al servicio de creación de logs, a los recopiladores de logs o al servidor de gestión de Panorama. Si habilita esta opción, debe configurar el reenvío de logs a Panorama. *No puede reenviar logs de correlación desde los cortafuegos a Panorama. Panorama genera logs de correlación sobre la base de los logs de cortafuegos que recibe.*

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de la lista de coincidencias	Description (Descripción)
SNMP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de trampas SNMP para reenviar logs como trampas SNMP (consulte Device > Server Profiles > SNMP Trap).
EMAIL	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de correo electrónico para reenviar logs como notificaciones de correo electrónico (consulte Device > Server Profiles > Email).
Syslog	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor Syslog para reenviar logs como mensajes de syslog (consulte Device > Server Profiles > Syslog).
HTTP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor HTTP para reenviar logs como solicitudes HTTP (consulte Device > Server Profiles > HTTP).
Acciones integradas	Existen dos tipos de acciones integradas: • **Tagging (Etiquetado):** puede realizar una acción en todos los tipos de log que incluyan una dirección IP de origen o de destino en la entrada de log configurando los siguientes ajustes según sea necesario. *Solo puede etiquetar la dirección IP de origen en los logs de correlación y en los logs de coincidencias HIP. No puede configurar ninguna acción para los logs de sistema y de configuración porque el tipo de log no incluye una dirección IP en la entrada de log.* • Haga clic en **Add (Añadir)** para añadir una acción e introduzca un nombre que la describa. • Seleccione la dirección IP que desee etiquetar automáticamente: **Source Address (Dirección de origen)** o **Destination Address (Dirección de destino)**. • Seleccione la acción: **Add Tag (Añadir etiqueta)** o **Remove Tag (Eliminar etiqueta)**. • Seleccione si desea registrar la dirección IP y la asignación de etiquetas en el agente de **Local User-ID (User-ID local)** en este cortafuegos o en Panorama, o a un agente de **Remote User-ID (User-ID remoto)**. • Para registrar la dirección IP y la asignación de etiquetas en un agente **Remote User-ID (User-ID remoto)**, seleccione el perfil del servidor HTTP (Device > Server Profiles > HTTP) que habilitará el reenvío. • Configure la opción **Timeout (Tiempo de espera)** de la etiqueta IP para configurar, en minutos, el tiempo durante el que se mantendrá la asignación de dirección IP a etiqueta. Una configuración de tiempo de espera en 0 significa que el tiempo de espera de la asignación de la etiqueta IP no se agotará (el intervalo es de 0 a 43 200 [30 días]; el valor predeterminado es 0).

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de la lista de coincidencias	Description (Descripción)
	Solo puede configurar un tiempo de espera con la acción Add Tag (Añadir etiqueta). • Introduzca o seleccione las **Tags (Etiquetas)** que desea aplicar o quitar de la dirección IP objetivo de origen o de destino. • **Integration (Integración):** solo disponible en el cortafuegos serie VM en Azure. Haga clic en **Add (Añadir)** para añadir un nombre y utilice esta acción para reenviar los logs seleccionados al centro de seguridad de Azure. Si esta opción no está visible, es posible que su suscripción de Azure no sea compatible con el centro de seguridad de Azure.

Definición de la configuración de alarma

- Device > Log Settings

Use la configuración de alarma para configurar Alarmas para la CLI y la interfaz web. Puede configurar notificaciones para los siguientes eventos:

- Se ha encontrado una coincidencia con una regla de seguridad (o grupo de reglas) en un umbral especificado y dentro de un intervalo de tiempo especificado.
- Se ha alcanzado el umbral de fallos de cifrado/descifrado.
- La base de datos de logs de cada tipo de log está casi llena; la cuota predeterminada está configurada para notificar que se ha usado el 90% de la capacidad del disco. La configuración de alarmas permite actuar antes de que se llene el disco y se purguen los logs.

Cuando habilite las alarmas, puede ver la lista actual haciendo clic en **Alarms (Alarmas)** ( ) en la parte inferior de la interfaz web.

Para añadir una alarma, edite la configuración de alarma que se describe en la siguiente tabla:

Configuración del log Alarma	Description (Descripción)
Habilitar alarmas	Alarms (Alarmas) se visualizan cuando selecciona **Enable Alarms (Habilitar alarmas)**. *Si deshabilita las alarmas, el cortafuegos no le avisa de los eventos críticos que requieren acción. Por ejemplo, una alarma le indica cuando la tecla maestra está a punto de caducar; si la clave caduca antes de cambiarla, el cortafuegos se reinicia en el modo de mantenimiento y, a continuación, se requerirá un restablecimiento de fábrica.*
Habilitar notificaciones de alarmas por CLI	Habilite notificaciones de alarmas por CLI cuando se produzca una alarma.
Habilitar notificaciones de alarma web	Abra una ventana para mostrar alarmas en las sesiones de usuario, incluyendo el momento en que se producen y cuándo se reconocen.
Habilitar alarmas audibles	Se reproduce una alarma audible cada 15 segundos en el equipo del administrador cuando este inició sesión en la interfaz web y no aceptó la

© 2020 Palo Alto Networks, Inc.

Configuración del log Alarma	Description (Descripción)
	alarma. El tono de alarma se reproducirá hasta que el administrador acepte todas las alarmas. Para ver y aceptar alarmas, haga clic en **Alarms (Alarmas)**. Esta función solo está disponible cuando el cortafuegos está en el modo FIPS-CC.
Umbral de fallo de cifrado/descifrado	Especifique el número de fallos de cifrado/descifrado tras los cuales se genera una alarma.
<*Tipo de log*> Base de datos de log	Genere una alarma cuando una base de datos de logs alcance el porcentaje indicado del tamaño máximo.
Umbral de infracciones de seguridad / Período de tiempo de infracciones de seguridad	Se genera una alarma si un puerto o una dirección IP en concreto incumple una regla de denegación el número de veces especificado en el ajuste **Security Violations Threshold (Umbral de infracciones de seguridad)** dentro del período (segundos) especificado en el ajuste**Security Violations Time Period (Período de tiempo de infracciones de seguridad)**.
Umbral de infracciones / Periodo de tiempo de infracciones / Etiquetas política de seguridad	Se genera una alarma si el conjunto de reglas alcanza el número de infracciones del límite de reglas especificado en el campo **Violations Threshold (Umbral de infracciones)** durante el período especificado en el campo **Violations Time Period (Período de tiempo de infracciones)**. Los incumplimientos se cuentan cuando una sesión coincide con una política de denegación explícita. Utilice **Security Policy Tags (Etiquetas de política de seguridad)** para especificar las etiquetas con las que los umbrales de límite de reglas generarán alarmas. Estas etiquetas están disponibles para su especificación al definir políticas de seguridad.
Auditoría selectiva	Las opciones de auditoría selectiva solo están disponibles cuando los cortafuegos están en modo FIPS-CC. Especifique los siguientes ajustes: • **FIPS-CC Specific Logging (Logging específico de FIPS-CC)**: permite logs ampulosos necesarios para el cumplimiento de criterios comunes (CC). • **Packet Drop Logging (Logs de descarte de paquetes)**: los paquetes de logs omitidos por el cortafuegos. • **Suppress Login Success Logging (Suprimir log de inicio de sesión correcto)**: detiene los inicios de sesión correctos del administrador en el cortafuegos. • **Suppress Login Failure Logging (Suprimir log de fallo de sesión correcto)**: detiene los inicios de sesión fallidos del administrador en el cortafuegos. • **TLS Session Logging (Logging de sesión TLS)**: registra el establecimiento de sesiones TLS. • **CA (OCSP/CRL) Session Establishment Logging [Logging de CA de establecimiento de sesiones (OCSP/CRL)]**: registra el establecimiento de sesiones entre el cortafuegos y una entidad de certificación cuando el cortafuegos envía una solicitud para verificar el estado de revocación del

© 2020 Palo Alto Networks, Inc.

Configuración del log Alarma	Description (Descripción)
	certificado mediante el Protocolo de estado de certificado en línea o una solicitud de servidor de la Lista de revocación de certificados. (De forma predeterminada, esta opción está deshabilitada). • **IKE Session Establishment Logging (Logging de establecimiento de sesión IKE)**: registra el establecimiento de sesión IKE de IPSec cuando la puerta de enlace VPN en el cortafuegos se autentica con un peer. El peer puede ser un cortafuegos de Palo Alto Networks u otro dispositivo de seguridad para iniciar y finalizar las conexiones de VPN. El nombre de interfaz que se especifica en el log es la interfaz que se vincula a la puerta de enlace IKE. El nombre de la puerta de enlace IKE también se muestra si corresponde. Si deshabilitar esta opción, se detiene el registro de todos los eventos de logs de IKE. (De forma predeterminada, esta opción está habilitada). • **Suppressed Administrators (Administradores suprimidos)**: detiene el registro de cambios que realizan los administradores enumerados en la configuración del cortafuegos.

Borrar logs

- Device > Log Settings

Puede borrar logs en el cortafuegos cuando gestiona logs en la página Log Settings. Haga clic en el tipo de log que desea borrar y haga clic en **Sí** para confirmar la solicitud.

Para borrar automáticamente los logs e informes, puede configurar períodos de vencimiento. Para obtener más información, consulte Configuración de logging e informes.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Perfiles de servidor > Netflow

Los siguientes temas describen la configuración del perfil de servidor que puede configurar en el cortafuegos:

- Dispositivo > Perfiles de servidor > Trap SNMP
- Device > Server Profiles > Syslog
- Device > Server Profiles > Email
- Dispositivo > Perfiles de servidor > HTTP
- Device > Server Profiles > NetFlow (Dispositivo > Perfiles de servidor > Netflow)
- Device > Server Profiles > RADIUS
- Device > Server Profiles > TACACS+
- Device > Server Profiles > LDAP
- Device > Server Profiles > Kerberos
- Dispositivo > Perfiles de servidor > Proveedor de identidad SAML
- Device > Server Profiles > DNS
- Dispositivo> Perfiles de servidor> Autenticación de múltiples factores

© 2020 Palo Alto Networks, Inc.

Dispositivo > Perfiles de servidor > Trap SNMP

SNMP (Protocolo simple de administración de redes) es un protocolo estándar para la supervisión de los dispositivos de su red. Para avisarle de eventos o alertas del sistema en su red, los dispositivos supervisados envían traps SNMP a los gestores de SNMP (servidores trap). Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **SNMP Trap (Trap SNMP)** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **SNMP Trap (Trap SNMP)** para configurar el perfil de servidor que permite al cortafuegos o Panorama enviar traps a los gestores de SNMP. Para habilitar mensajes GET SNMP (solicitudes de estadísticas desde un gestor SNMP), consulte Enable SNMP Monitoring.

Tras crear el perfil del servidor, debe especificar qué tipos de logs activarán el cortafuegos para que envíe traps SNMP (consulte Device > Log Settings). Para obtener una lista de los MIB que debe cargar en el gestor de SNMP para que pueda interpretar los traps, consulte MIB compatibles.

No elimine perfiles de servidor usados por configuración de log Sistema o perfiles de logs.

Configuración de perfil de servidor de Trap SNMP	Description (Descripción)
Nombre	Introduzca un nombre para el perfil de SNMP (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
versión	Seleccione la versión de SNMP: **V2c** (predeterminado) o **V3**. Su selección controla los campos restantes que muestra el cuadro de diálogo. Para cada versión, puede añadir hasta cuatro gestores SNMP. *Utilice SNMPv3, que ofrece autenticación y otras características para mantener la seguridad de las conexiones de red.*
Para SNMP V2c	
Nombre	Especifique un nombre para el gestor SNMP. El nombre puede tener hasta 31 caracteres que pueden ser alfanuméricos, puntos, guiones bajos o guiones.
Gestor SNMP	Especifique el FQDN o dirección IP del gestor SNMP.
Comunidad	Introduzca la cadena de comunidad, que identifica a una *comunidad* SNMP de gestores SNMP y dispositivos supervisados, además de servir como contraseña para autenticar a los miembros de la comunidad entre sí durante el reenvío de traps. Esta cadena puede tener hasta 127 caracteres, admite todos los caracteres y distingue entre mayúsculas y minúsculas.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil de servidor de Trap SNMP	Description (Descripción)
	No utilice cadenas de comunidad predeterminadas (no configure la cadena de comunidad como public [pública] o private [privada]). Utilice cadenas de comunidad únicas, lo cual evita los conflictos si utiliza varios servicios SNMP. Dado que los mensajes SNMP contienen cadenas de comunidad en texto sin cifrar, tenga en cuenta los requisitos de seguridad de su red cuando defina la pertenencia a la comunidad (acceso de administradores).
Para SNMP V3	
Nombre	Especifique un nombre para el gestor SNMP. El nombre puede tener hasta 31 caracteres que pueden ser alfanuméricos, puntos, guiones bajos o guiones.
Gestor SNMP	Especifique el FQDN o dirección IP del gestor SNMP.
Usuario	Especifique un nombre de usuario para identificar la cuenta de usuario de SNMP (de hasta 31 caracteres). El nombre de usuario que configure en el cortafuegos debe tener el mismo nombre de usuario configurado en el gestor SNMP.
EngineID	Especifique el ID de motor del cortafuegos. Cuando un gestor SNMP y el cortafuegos se autentican entre sí, los mensajes trap usan este valor para identificar exclusivamente el cortafuegos. Si deja este campo en blanco, los mensajes usan el número de serie del cortafuegos como **EngineID**. Si introduce un valor, debe estar en formato hexadecimal, con el prefijo 0x, y con otros 10-128 caracteres para representar cualquier número de 5-64 bytes (2 caracteres por byte). Para cortafuegos en configuración de alta disponibilidad (HA), deje el campo en blanco, de modo que el gestor SNMP pueda identificar qué peer HA envió los traps; de lo contrario, el valor se sincroniza y ambos peers usarán el mismo **EngineID**.
Contraseña de autenticación	Especifique la contraseña de autenticación del usuario SNMP. El cortafuegos usa la contraseña para autenticar el gestor SNMP. El cortafuegos usa el algoritmo de hash seguro (SHA-1 160) para cifrar la contraseña. La contraseña debe tener entre 8 y 256 caracteres y todos están permitidos.
Contraseña priv.	Especifique la privacidad de autenticación del usuario SNMP. El cortafuegos usa la contraseña y el estándar de cifrado avanzado (AES-128) para cifrar traps SNMP. La contraseña debe tener entre 8 y 256 caracteres y todos están permitidos.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > Syslog

Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Syslog** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **Syslog** para configurar un perfil de servidor para el reenvío de cortafuegos, Panorama y recopiladores de logs como mensajes syslog a un servidor syslog. Para definir un perfil de servidor syslog, haga clic en **Add (Añadir)** y especifique los campos New Syslog Server.

- *Para seleccionar el perfil de servidor Syslog para los logs de correlación, sistema, configuración, User-ID y coincidencia HIP, consulte* Device > Log Settings*.*
- *Para seleccionar el perfil de servidor de Syslog para tráfico, amenaza, Wildfire, filtrado de URL, filtrado de datos, inspección de túnel, autenticación y logs de GTP, consulte* Objects > Log Forwarding*.*
- *No puede eliminar un perfil servidor que el cortafuegos utilice en algún ajuste del log Sistema o Configuración o perfil de reenvío de logs.*

Configuración de servidor Syslog	Description (Descripción)
Nombre	Introduzca un nombre para el perfil de Syslog (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Pestaña Servidores	
Nombre	Haga clic en **Add (Añadir)** e introduzca un nombre para el servidor Syslog (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Servidor	Introduzca la dirección IP o FQDN del servidor syslog.
Transporte	Elija si desea transportar los mensajes de Syslog en UDP, TCP o SSL. *Utilice SSL para cifrar y proteger los datos enviados a un servidor syslog. Los datos se envían por UDP o TCP como texto no cifrado y pueden leerse en tránsito.*
Puerto	Introduzca el número de puerto del servidor Syslog (el puerto estándar para UDP es 514; el puerto estándar para SSL es 6514; para TCP debe especificar un número de puerto).
format	Especifique el formato de Syslog que se debe utilizar: BSD (valor predeterminado) o IETF.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor Syslog	Description (Descripción)
Instalaciones	Seleccione uno de los valores estándar de Syslog. Seleccione el valor que asigna al modo en que su servidor Syslog usa el campo Instalaciones para gestionar mensajes. Para obtener más información sobre el campo Instalaciones, consulte RFC 3164 (formato BSD) o RFC 5424 (formato IETF).
Pestaña Formato de log personalizado	
Tipo de log	Haga clic en el tipo de log para abrir un cuadro de diálogo que le permitirá especificar un formato de log personalizado. En el cuadro de diálogo, haga clic en un campo para añadirlo al área Formato de log. Otras cadenas de texto se pueden editar directamente en el área Formato de log. Haga clic en **OK (Aceptar)** para guardar los ajustes. Vea una descripción de cada campo que se pueda usar para logs personalizados. Para obtener información detallada sobre los campos que se pueden utilizar para logs personalizados, consulte Device > Server Profiles > Email.
Escape	Especifique secuencias de escape. Utilice el cuadro **Escaped characters (Caracteres de escape)** para enumerar todos los caracteres que se escaparán sin espacios.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > Email

Seleccione **Dispositivo** > **Perfiles de servidor** > **Correo electrónico** o **Panorama** > **Perfiles de servidor** > **Correo electrónico** para realizar la Configuración de un perfil de servidor que reenvíe logs como notificaciones de correo electrónico. Para definir un perfil de servidor de correo electrónico, tiene que **Add (Añadir)** un perfil y especificar los Email Notification Settings (Ajustes de notificación por correo electrónico).

- *Para seleccionar el perfil de servidor Syslog para los logs de correlación, sistema, configuración, User-ID y coincidencia HIP, consulte* Device > Log Settings*.*
- *Para seleccionar el perfil de servidor de Syslog para tráfico, amenaza, Wildfire, filtrado de URL, filtrado de datos, inspección de túnel, autenticación y logs de GTP, consulte* Objects > Log Forwarding*.*
- *también puede consultar* Monitor > PDF Reports > Email Scheduler*.*
- *No puede eliminar un perfil servidor que el cortafuegos utilice en algún ajuste del log Sistema o Configuración o perfil de reenvío de logs.*

Configuración de notificaciones por correo electrónico	Description (Descripción)
Nombre	Introduzca un nombre para el perfil de servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Pestaña Servidores	
Servidor	Introduzca un nombre para identificar el servidor (hasta 31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente.
Mostrar nombre	Introduzca el nombre mostrado en el campo **De** del correo electrónico.
De	Introduzca la dirección de correo electrónico del remitente, por ejemplo, “alerta_seguridad@empresa.com”.
Para	Introduzca la dirección de correo electrónico del destinatario.
Destinatario adicional	También puede introducir la dirección de correo electrónico de otro destinatario. Solo puede añadir un destinatario adicional. Para añadir varios destinatarios, añada la dirección de correo electrónico de una lista de distribución.

© 2020 Palo Alto Networks, Inc.

Configuración de notificaciones por correo electrónico	Description (Descripción)
Gateway	Introduzca la dirección IP o el nombre de host del servidor Simple Mail Transport Protocol (SMTP) utilizado para enviar el correo electrónico.
Pestaña Formato de log personalizado	
Tipo de log	Haga clic en el tipo de log para abrir un cuadro de diálogo que le permitirá especificar un formato de log personalizado. En el cuadro de diálogo, haga clic en un campo para añadirlo al área Formato de log. Haga clic en **OK (Aceptar)** para guardar los ajustes.
Escape	Incluya los caracteres de escape y especifique el carácter o los caracteres de escape.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Perfiles de servidor > HTTP

Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **HTTP** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **HTTP** para configurar un perfil de servidor para reenviar logs. Puede configurar el cortafuegos para que envíe los logs a un destino HTTP (S) o para integrarse con cualquier servicio basado en HTTP que exponga una API y modifique la URL, el encabezado HTTP, los parámetros y la carga útil en la solicitud HTTP para satisfacer sus necesidades. También puede utilizar el perfil del servidor HTTP para acceder a cortafuegos que ejecutan el agente User-ID de PAN-OS integrado y registrar una o varias etiquetas en una dirección IP de origen o de destino en los logs que generó un cortafuegos.

Para usar el perfil del servidor HTTP para reenviar los logs:

- *Consulte* Device > Log Settings *para los logs de sistema, configuración, User-ID, coincidencia HIP y correlación.*
- *Consulte* Objects > Log Forwarding *para los logs de tráfico, amenaza, WildFire, filtrado de URL, filtrado de datos, inspección de túnel, autenticación y GTP.*

No puede eliminar un perfil de servidor HTTP si se utiliza para reenviar logs. Para eliminar un perfil de servidor en el cortafuegos o Panorama, debe eliminar todas las referencias al perfil del perfil Device (Dispositivo) > Log Settings (Configuración del log) u Objects (Objetos) > Log Forwarding (Reenvío de registros).

Para definir un perfil de servidor HTTP, debe **Add (Añadir)** un nuevo perfil y configurar los ajustes en la tabla siguiente.

Ajustes de servidor HTTP	Description (Descripción)
Nombre	Introduzca un nombre para el perfil de servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Un nombre válido debe empezar por un carácter alfanumérico y puede contener ceros, caracteres alfanuméricos, guiones bajos '_', guiones '-', puntos '.' o espacios
Ubicación	Seleccione el ámbito en el que este perfil está disponible. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar la **Location (Ubicación)**.
Registro de etiquetas	El registro de etiquetas le permite agregar o quitar una etiqueta en una dirección IP de origen o de destino en una entrada de log y registrar la dirección IP y la asignación de etiquetas al agente de User-ID en un cortafuegos mediante HTTP (S). A continuación, puede definir grupos de direcciones dinámicas que utilizan estas etiquetas como criterios de filtrado para determinar sus miembros y aplicar reglas de políticas a una dirección IP basada en etiquetas. **Add (Añadir)** los detalles de conexión para habilitar el acceso HTTP (S) en el agente User-ID en un cortafuegos. Para registrar etiquetas en el agente de User-ID en Panorama, no necesita un perfil de servidor. Además, no puede utilizar el perfil de servidor HTTP

© 2020 Palo Alto Networks, Inc.

Ajustes de servidor HTTP	Description (Descripción)
	para registrar etiquetas en un agente de User-ID que se ejecuta en un servidor Windows.
Pestaña Servidores	
Nombre	Debe **Add (Añadir)** un servidor HTTP (s) e introducir un nombre (hasta 31 caracteres) o un agente de User-ID remoto. Un nombre válido debe ser único y comenzar con un carácter alfanumérico; el nombre puede contener ceros, caracteres alfanuméricos, guiones bajos, guiones, puntos o espacios. Un perfil de servidor puede incluir hasta cuatro servidores.
Dirección	Introduzca la dirección IP del servidorHTTP. Para el registro de etiquetas, especifique la dirección IP del cortafuegos configurado como un agente de User-ID.
PROTOCOL	Seleccione el protocolo: HTTP o HTTPS.
Puerto	Introduzca el número de puerto para acceder al servidor o cortafuegos. El puerto predeterminado para HTTP es 80 y para HTTPS es 443. Para el registro de etiquetas, el cortafuegos utiliza HTTP o HTTPS para conectarse al servidor web en los cortafuegos configurados como agentes User-ID.
Versión de TLS	Seleccione la versión de TLS admitida en el servidor. El valor predeterminado es **1.2**.
Perfil del certificado	Seleccione el Perfil de Certificado que usar para la conexión TLS con el servidor. El cortafuegos utiliza el Perfil de Certificado especificado para validar el certificado del servidor cuando se establece una conexión segura con el servidor.
Método HTTP	Seleccione el método HTTP que admite el servidor. Las opciones son GET, PUT, POST (predeterminado) y DELETE. Para el agente User-ID, utilice el método GET.
Nombre de usuario	Introduzca el nombre de usuario que tiene privilegios de acceso para completar el método HTTP que seleccionó. Si está registrando etiquetas en el agente de User-ID en un cortafuegos, el nombre de usuario debe ser el de un administrador con una función de superusuario.
Contraseña	Introduzca la contraseña para autenticarse en el servidor o en el cortafuegos.
Probar conexión de servidor	Seleccione un servidor y seleccione **Test Server Connection (Probar conexión de servidor)** para probar la conectividad de red con el servidor.

© 2020 Palo Alto Networks, Inc.

Ajustes de servidor HTTP	Description (Descripción)
	Esta prueba no prueba conectividad a un servidor que ejecuta el agente User-ID.
Pestaña Formato de payload	
Tipo de log	Se muestra el tipo de log disponible para el reenvío de HTTP. Haga clic en el tipo de log para abrir un cuadro de diálogo que le permitirá especificar un formato de log personalizado.
format	Muestra si el tipo de log utiliza el formato predeterminado, un formato predefinido o un formato de carga útil personalizado definido por usted.
Formatos predefinidos	Seleccione el formato para su servicio o proveedor para el envío de logs. Los formatos predefinidos se envían junto con las actualizaciones de contenido y pueden cambiar cada vez que se instala una nueva actualización de contenido en el cortafuegos o Panorama.
Nombre	Introduzca un nombre para el formato de log personalizado.
Formato de URl	Especifique el recurso al que desea enviar logs utilizando HTTP (S). 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 petición.
Cabecera de HTTP	Añada un Encabezado y su valor correspondiente.
Parámetros	Incluya los parámetros y valores opcionales.
Payload	Seleccione los atributos de log que desea incluir como carga útil en el mensaje HTTP al servidor web externo.
Enviar log de prueba	Haga clic en este botón para validar que el servidor web externo recibe la solicitud y en el formato de carga útil correcto.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > NetFlow (Dispositivo > Perfiles de servidor > Netflow)

Los cortafuegos de Palo Alto Networks pueden exportar estadísticas sobre el tráfico IP en sus interfaces como campos 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 agregar interfaces Ethernet, puede exportar registros para el grupo agregado, pero no para las interfaces individuales dentro del grupo. Los cortafuegos admiten plantillas NetFlow estándar y empresariales (específicas de PAN-OS), que los recopiladores NetFlow utilizan para descifrar los campos NetFlow. 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.

Para configurar exportaciones de datos NetFlow, seleccione **Add (Añadir)**un perfil de servidor NetFlow para especificar los servidores NetFlow que recibirán los datos exportados y los parámetros de exportación. Después de asignar el perfil a una interfaz (consulte Network > Interfaces), el cortafuegos exporta los datos NetFlow para todo el tráfico en la interfaz a los servidores especificados.

Configuración de Netflow	Description (Descripción)
Nombre	Introduzca un nombre para el perfil de servidor Netflow (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Tasa de actualización de plantilla	El cortafuegos actualiza periódicamente las plantillas NetFlow 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. Especifique la velocidad a la que el cortafuegos actualiza las plantillas de NetFlow en **Minutes (Minutos)** (intervalo: 1-3.600; predeterminado es 30) y **Packets (Paquetes)** (registros exportados: intervalo es 1-600 y el predeterminado es 20), de acuerdo con los requisitos de su recopilador NetFlow. El cortafuegos actualiza la plantilla después de pasar cualquiera de los umbrales. La frecuencia de actualización necesaria depende del recopilador de NetFlow. Si añade varios recopiladores de flujo de red al perfil del servidor, utilice el valor del recopilador con la velocidad de actualización más rápida.
Tiempo de espera activo	Especifique la frecuencia (en minutos) a la que el cortafuegos exporta registros de datos para cada sesión (el intervalo es 1-60 y el predeterminado es 5). Establezca la frecuencia basada en cuántas veces quiere que el recopilador del flujo de datos actualice las estadísticas de tráfico.
Tipos de campos de PAN-OS	Exporte campos específicos de PAN-OS para App-ID y el servicio de User-ID en registros de Netflow.
los servidores	

© 2020 Palo Alto Networks, Inc.

Configuración de Netflow	Description (Descripción)
Nombre	Especifique un nombre para identificar el servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Servidor	Especifique el nombre de host o la dirección IP del servidor. Puede añadir un máximo de dos servidores por perfil.
Puerto	Especifique el número de puerto para el acceso al servidor (predeterminado: 2055).

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > RADIUS

Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **RADIUS** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **RADIUS** para configurar los ajustes de los servidores de Servicio de autenticación remota telefónica de usuario (Remote Authentication Dial-In User Service, RADIUS) a los que hacen referencia los perfiles de autenticación (consulte Device [Dispositivo] > Authentication Profile [Perfil de autenticación]). Puede utilizar RADIUS para autenticar a los usuarios finales que acceden a sus recursos de red (a través de GlobalProtect o portal cautivo), para autenticar a los administradores definidos localmente en el cortafuegos o Panorama y para autenticar y autorizar administradores definidos externamente en el servidor RADIUS.

Configuración de servidor RADIUS	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el perfil de servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Únicamente uso de administrador	Seleccione esta opción para especificar que solo las cuentas de administrador puedan usar el perfil para la autenticación. Para cortafuegos que tienen varios sistemas virtuales, la opción aparece solo si **Location (Ubicación)** es **Shared (Compartida)**.
Tiempo de espera	Introduzca un intervalo en segundos después del cual la solicitud de autenticación vence (el intervalo es de 1 a 120, el valor predeterminado es 3). *Si utiliza el perfil del servidor RADIUS para integrar el cortafuegos con un servicio MFA, introduzca un intervalo que proporcione a los usuarios tiempo suficiente para responder al desafío de autenticación. 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.*
Protocolos de autenticación	Seleccione el **Authentication Protocol (Protocolo de autenticación)** que el servidor de seguridad utiliza para proteger una conexión al servidor RADIUS: • **PEAP-MSCHAPv2**: (valor predeterminado) el EAP protegido (PEAP) con el Protocolo de autenticación por desafío mutuo de Microsoft (Microsoft Challenge-Handshake Authentication Protocol,

© 2020 Palo Alto Networks, Inc.

Configuración de servidor RADIUS	Description (Descripción)
	MSCHAPv2) brinda seguridad mejorada al PAP o CHAP transmitiendo el nombre de usuario y la contraseña en un túnel cifrado. • **PEAP with GTC (PEAP con GTC)**: seleccione EAP protegido (PEAP) con la Tarjeta de token genérico (Generic Token Card, GTC) para utilizar tokens únicos en un túnel cifrado. • **EAP-TTLS with PAP (EAP-TTLS con PAP)**: seleccione EAP con Seguridad con capa de transporte de túnel (Tunneled Transport Layer Security, TTLS) y PAP para transportar credenciales de texto sin formato en un túnel cifrado. • **CHAP**: seleccione el Protocolo de autenticación por desafío mutuo (Challenge-Handshake Authentication Protocol, CHAP) si el servidor RADIUS no admite EAP o PAP o si no está configurado para ello. • **PAP**: seleccione el Protocolo de autenticación de contraseña (Password Authentication Protocol, PAP) si el servidor RADIUS no admite EAP o CHAP, o si no está configurado para ello.
Allow users to change passwords after expiry (Permitir a los usuarios cambiar contraseñas tras el vencimiento)	(PEAP-MSCHAPv2 con GlobalProtect 4.1 o posterior) Seleccione esta opción para permitir a los usuarios de GlobalProtect cambiar las contraseñas vencidas.
Make Outer Identity Anonymous (Hacer anónima la identidad externa)	(PEAP-MSCHAPv2, PEAP con GTC o EAP-TTLS con PAP) Esta opción se habilita de manera predeterminada para hacer anónima la identidad del usuario en el túnel externo que crea el cortafuegos tras la autenticación en el servidor. *Es posible que algunas configuraciones de servidor RADIUS no admitan ID externas anónimas y que deba anular esta selección. Cuando se deshabilita esta opción, los nombres de usuario se transmiten sin formato.*
Perfil del certificado	(PEAP-MSCHAPv2, PEAP con GTC o EAP-TTLS con PAP) Seleccione o configure un perfil de certificado para asociarlo a un perfil de servidor RADIUS. El cortafuegos utiliza el Perfil de Certificado para autenticar el servidor RADIUS.
Reintentos	Especifique el número de veces que se volverá a intentar después de un tiempo de espera (el intervalo es de 1 a 5; el valor predeterminado es 3).
los servidores	Configure información para cada servidor en el orden preferido. • **Name (Nombre)**: introduzca un nombre para identificar el servidor. • **RADIUS Server (Servidor RADIUS)**: Introduzca la dirección IP del servidor o FQDN. • **Secret/Confirm Secret (Secreto/Confirmar secreto)**: Introduzca y confirme una clave para verificar y cifrar la conexión entre el cortafuegos y el servidor RADIUS. • **Puerto**: introduzca el puerto del servidor (intervalo es de 1 a 65 535; el valor predeterminado es 1812) para solicitudes de autenticación.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > TACACS+

Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **TACACS+** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **TACACS+** para realizar la Configuración de los ajustes que definen la forma en que el cortafuegos o Panorama se conecta a los servidores del sistema mejorado de control de acceso del controlador de acceso a terminales (Terminal Access Controller Access-Control System Plus, TACACS+) (consulte Device [Dispositivo] > Authentication Profile [Perfil de autenticación]). Puede utilizar TACACS+ para autenticar a los usuarios finales que acceden a sus recursos de red (a través de GlobalProtect o portal cautivo), para autenticar a los administradores definidos localmente en el cortafuegos o Panorama y para autenticar y autorizar administradores definidos externamente en el servidor TACACS+.

Configuración de servidor de TACACS+	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el perfil de servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Únicamente uso de administrador	Seleccione esta opción para especificar que solo las cuentas de administrador puedan usar el perfil para la autenticación. Para cortafuegos de vsys múltiples, esta opción aparece solo si la **Location (Ubicación)** es **Shared (Compartida)**.
Tiempo de espera	Introduzca un intervalo en segundos después del cual la solicitud de autenticación vence (intervalo: 1-20, el predeterminado es 3).
Protocolos de autenticación	Seleccione el **Authentication Protocol (Protocolo de autenticación)** que el cortafuegos usa para asegurar una conexión con el servidor TACACS+: • **CHAP**: el Protocolo de autenticación por desafío mutuo (CHAP) es el protocolo predeterminado y preferido porque es más seguro que PAP. • **PAP**: seleccione el Protocolo de autenticación de contraseña (PAP) si el servidor TACACS+ no admite CHAP o si no está configurado para ello. • **Auto (automático)**: el cortafuegos primero intenta autenticar usando CHAP. Si el servidor TACACS+ no responde, el cortafuegos vuelve a PAP.
Utilizar conexión única para toda la autenticación	Seleccione esta opción para usar la misma sesión TCP para todas las autenticaciones. Esta opción mejora el rendimiento al evitar el procesamiento que requiere iniciar y eliminar una sesión TCP diferente para cada evento de autenticación.
los servidores	Haga clic en **Add (Añadir)** y especifique los siguientes parámetros para cada servidor TACACS+: • **Name (Nombre)**: introduzca un nombre para identificar el servidor.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor de TACACS+	Description (Descripción)
	• **TACACS+ Server (Servidor TACACS+)**: introduzca la dirección IP o FQDN del servidor TACACS+. • **Secret/Confirm Secret (Secreto/Confirmar secreto)**: introduzca y confirme una clave para verificar y cifrar la conexión entre el cortafuegos y el servidor TACACS+. • **Port**: Introduzca el puerto del servidor (predeterminado: 49) para solicitudes de autenticación.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > LDAP

- **Device (Dispositivo)** > **Server Profiles (Perfil de servidor)** > **LDAP**
- **Panorama** > **Server Profiles (Perfil de servidor)** > **LDAP**

Seleccione **Add (Añadir)** para añadir o seleccione un perfil de servidor LDAP para configurar los ajustes de los servidores del protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP) a los que hacen referencia los perfiles de autenticación (consulte Device [Dispositivo] > Authentication Profile [Perfil de autenticación]). Puede utilizar LDAP para autenticar a los usuarios finales que acceden a sus recursos de red (a través de GlobalProtect o portal cautivo) y a los administradores definidos localmente en el cortafuegos o Panorama.

Configuración de servidor LDAP	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el perfil (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Únicamente uso de administrador	Seleccione esta opción para especificar que solo las cuentas de administrador puedan usar el perfil para la autenticación. Para cortafuegos que tienen varios sistemas virtuales, la opción aparece solo si **Location (Ubicación)** es **Shared (Compartida)**.
Use this profile for serial number check (Utilizar este perfil para la comprobación de número de serie)	Seleccione esta opción para habilitar este perfil de servidor LDAP para recolectar números de serie de los endpoints gestionados. Esta información la utilizan el portal y la puerta de enlace de GlobalProtect para verificar si el endpoint es gestionado (si el número de serie existe en Active Directory) o no.
Server List (Lista de servidores)	Para cada servidor LDAP, haga clic en **Add (Añadir)** e introduzca el **Name (Nombre)** del host, la dirección IP o FQDN (**LDAP Server [Servidor LDAP]**) y **Port (Puerto)** (el valor predeterminado es 389). *Configure al menos dos servidores LDAP para proporcionar redundancia.*
Tipo	Seleccione el tipo de servidor del menú desplegable.
DN base	Especifique el contexto raíz del servidor de directorio para acotar la búsqueda de información de usuario o grupo.
Enlazar DN	Especifique el nombre de inicio de sesión (nombre distintivo) del servidor de directorio.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor LDAP	Description (Descripción)
	La cuenta Bind DN debe tener permiso para leer el directorio LDAP.
Contraseña/Confirmar contraseña	Especifique la contraseña de la cuenta de enlace. El agente guardará la contraseña cifrada en el archivo de configuración.
Tiempo de espera de enlace	Especifique el límite de tiempo (en segundos) impuesto al conectar con el servidor de directorio (intervalo es 1-30 s; predeterminado: 30 s).
Tiempo de espera de búsqueda	Especifique el límite de tiempo (en segundos) impuesto al realizar búsquedas en el directorio (intervalo es 1-30 s; predeterminado: 30 s).
Intervalo de reintento	Especifique el intervalo en segundos tras el cual el sistema intentará conectarse al servidor LDAP después de un intento fallido anterior (intervalo: 1-3.600; predeterminado: 60).
Solicitar conexión SSL/ TLS protegida	Seleccione esta opción si quiere que el cortafuegos use SSL o TLS para comunicarse con el servidor de directorio. El protocolo depende del puerto del servidor: • 389 (predeterminado): TLS (específicamente, el cortafuegos usa la operación Start TLS, que actualiza la conexión de texto no cifrado con TLS). • 636—SSL • Cualquier otro puerto: El cortafuegos primero intenta usar TLS. Si el servidor de directorio no admite TLS, el cortafuegos cambia a SSL. *Se recomienda esta opción, ya que aumenta la seguridad y está seleccionada de forma predeterminada.*
Verificar certificado de servidor para sesiones SSL	Seleccione esta opción (sin marcar de manera predeterminada) si quiere que el cortafuegos verifique el certificado que presenta el servidor de directorio para conexiones SSL/TLS. El cortafuegos verifica el certificado en dos aspectos: • El certificado es fiable y válido. Para que el cortafuegos confíe en el certificado, su entidad de certificación (certificate authority, CA) raíz y cualquier certificado intermedio debe estar en la tienda de certificados en **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados de dispositivos)**. • El nombre del certificado debe coincidir con el **Name (Nombre)** del host del servidor LDAP. El cortafuegos comprueba primero la coincidencia del atributo Subject AltName del certificado y, a continuación, prueba el atributo Subject DN. Si el certificado usa el FQDN del servidor de directorio, debe usar FQDN en el campo **LDAP Serve (Servidor LDAP)** para que se consiga la coincidencia de nombre. Si la verificación falla, la conexión también. Para habilitar esta verificación, debe seleccionar también **Require SSL/TLS secured connection (Solicitar conexión SSL/TLS protegida)**.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor LDAP	Description (Descripción)
	Habilite el cortafuegos para verificar el certificado del servidor para las sesiones SSL para aumentar la seguridad.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > Kerberos

Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **Kerberos** o **Panorama** > **Server Profiles (Perfiles de servidor)** > **Kerberos** para configurar un perfil de servidor que permita a los usuarios autenticarse de manera nativa en un controlador de dominio de Active Directory o un servidor de autenticación compatible con Kerberos V5. Después de configurar un perfil de servidor Kerberos, puede asignarlo al perfil de autenticación (consulte Device > Authentication Profile). Puede utilizar Kerberos para autenticar a los usuarios finales que acceden a sus recursos de red (a través de GlobalProtect o portal cautivo) y a los administradores definidos localmente en el cortafuegos o en Panorama.

Para usar autenticación de Kerberos, debe poderse acceder a su servidor Kerberos de back-end a través de una dirección IPv4. Las direcciones IPv6 no son compatibles.

Configuración de servidor Kerberos	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Únicamente uso de administrador	Seleccione esta opción para especificar que solo las cuentas de administrador puedan usar el perfil para la autenticación. Para cortafuegos que tienen varios sistemas virtuales, la opción aparece solo si **Location (Ubicación)** es **Shared (Compartida)**.
los servidores	En el caso de cada servidor Kerberos, haga clic en **Add (Añadir)** y especifique los siguientes ajustes: • **Name (Nombre)**: introduzca un nombre para el servidor. • **Kerberos Server (Servidor Kerberos)**: introduzca la dirección IPv4 del servidor o FQDN. • **Port (Puerto)**: introduzca un número de puerto opcional (intervalo: 1-65.535; predeterminado: 88) para la comunicación con el servidor.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Perfiles de servidor > Proveedor de identidad SAML

Utilice esta página para registrar un proveedor de identidad (IdP) 2.0 con el cortafuegos o Panorama. El registro es un paso necesario para que el cortafuegos o Panorama funcione como un proveedor de servicios SAML, que controla el acceso a los recursos de red. Cuando los administradores y los usuarios finales solicitan recursos, el proveedor de servicios redirige a los usuarios a IdP para la autenticación. Los usuarios finales pueden ser usuarios de GlobalProtect o portal cautivo. Los administradores pueden administrarse localmente en el cortafuegos y en Panorama o administrarse externamente en el almacén de identidad IdP. Puede configurar el inicio de sesión único (SSO) de SAML para que cada usuario pueda acceder automáticamente a varios recursos después de iniciar sesión en uno. También puede configurar el inicio de sesión único de SAML (SLO) para que cada usuario pueda desconectarse simultáneamente de cada servicio habilitado para SSO cerrando sesión de un solo servicio.

Las secuencias de autenticación no admiten perfiles de autenticación que especifiquen los perfiles de servidor SAMP IdP.

En la mayoría de los casos, no puede utilizar SSO para acceder a varias aplicaciones en el mismo dispositivo móvil.

No puede habilitar SLO para los usuarios del portal cautivo.

La forma más sencilla de crear un perfil de servidor SAMP IdP es **Import (Importar)** un archivo de metadatos que contiene la información de registro del IdP. Después de guardar un perfil de servidor con valores importados, puede editar el perfil para modificar los valores. Si el IdP no proporciona un archivo de metadatos, puede **Add (Añadir)** el perfil del servidor e introducir manualmente la información. Después de crear un perfil de servidor, asígnelo a un perfil de autenticación (consulte Device > Authentication Profile) para servicios específicos de cortafuegos o Panorama.

Configuración de servidor de proveedor de identidad SAML	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el perfil. En el contexto de un cortafuegos con múltiples sistemas virtuales (vsys), seleccione un sistema virtual o seleccione **Shared (Compartido)** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Únicamente uso de administrador	Seleccione esta opción para especificar que solo las cuentas de administrador puedan usar el perfil para la autenticación. Para cortafuegos que tienen varios sistemas virtuales, la opción aparece solo si **Location (Ubicación)** es **Shared (Compartida)**.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor de proveedor de identidad SAML	Description (Descripción)
ID de proveedor de identidad	Introduzca un identificador para el IdP. Su IdP proporciona esta información.
Certificado de proveedor de identidad	Seleccione el certificado que el IdP utiliza para firmar mensajes SAML que envía al cortafuegos. Debe seleccionar un certificado IdP para garantizar la integridad de los mensajes que el IdP envía al cortafuegos. Para validar el certificado IdP en relación con la emisión de la entidad de certificación (CA), debe especificar un **Perfil de Certificado** en cualquier perfil de autenticación que haga referencia al perfil del servidor IdP (consulte Dispositivo > Perfil de Autenticación). Al generar o importar un certificado y su clave privada asociada, recuerde que los atributos de uso de clave especificados en el certificado controlan para qué puede utilizar la clave. Si el certificado enumera explícitamente atributos de uso de clave, uno de los atributos debe ser Firma digital, que no está disponible en los certificados que genera en el cortafuegos En este caso, debe Importar el certificado y la clave de su entidad emisora de certificados de empresa (CA) o de una entidad emisora de certificados de terceros. Si el certificado no especifica los atributos de uso de clave, puede utilizar la clave para cualquier propósito, incluida la firma de mensajes. En este caso, puede utilizar cualquier método para Obtener el certificado y la clave para firmar mensajes SAML. Los certificados IdP admiten 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.
URL SSO de proveedor de identidad	Introduzca la URL que el IdP anuncia para su servicio de inicio de sesión único (SSO). Si crea el perfil de servidor importando un archivo de metadatos y el archivo especifica varias URL de SSO, el cortafuegos utiliza la primera dirección URL que especifica un método de vinculación POST o redireccionamiento. *Palo Alto Networks recomienda encarecidamente el uso de una URL que dependa de HTTPS, aunque SAML también es compatible con HTTP.*
URL SLO de proveedor de identidad	Introduzca la URL que el IdP anuncia para su servicio de cierre de sesión único (SLO). Si crea el perfil de servidor importando un archivo de metadatos y el archivo especifica varias URL de SLO, el cortafuegos utiliza la primera dirección URL que especifica un método de vinculación POST o redireccionamiento.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor de proveedor de identidad SAML	Description (Descripción)
	Palo Alto Networks recomienda encarecidamente el uso de una URL que dependa de HTTPS, aunque SAML también es compatible con HTTP.
Enlace SSO SAML HTTP	Seleccione el enlace HTTP asociado con el **Identity Provider SSO URL (Proveedor de Identidad URL de SSO)**. El cortafuegos utiliza el enlace para enviar mensajes SAML al IdP. Las opciones son las siguientes: • **POST**: el cortafuegos envía mensajes utilizando formularios HTML codificados en base64. • **Redirect (Redireccionar)**: el cortafuegos envía mensajes SSO codificados en base64 y codificados con URL dentro de los parámetros de URL. *Si importa un archivo de metadatos IdP que tiene varias URL SSO, el cortafuegos utiliza el enlace de la primera dirección URL que utiliza el método POST o de redireccionamiento. El cortafuegos ignora las URL que usan otros enlaces.*
Enlace SLO SAML HTTP	Seleccione el enlace HTTP asociado con el **Identity Provider SLO URL (URL SLO de proveedor de identidad)**. El cortafuegos utiliza el enlace para enviar mensajes SAML al IdP. Las opciones son las siguientes: • **POST**: el cortafuegos envía mensajes utilizando formularios HTML codificados en base64. • **Redirect (Redireccionar)**: el cortafuegos envía mensajes SSO codificados en base64 y codificados con URL dentro de los parámetros de URL. *Si importa un archivo de metadatos IdP que tiene varias URL SLO, el cortafuegos utiliza el enlace de la primera dirección URL que utiliza el método POST o de redireccionamiento. El cortafuegos ignora las URL que usan otros enlaces.*
Metadatos de proveedor de identidad	Este campo solo se muestra si selecciona **Import (Importar)** un archivo de metadatos IdP que subió al cortafuegos desde el IdP. El archivo especifica los valores y el certificado de firma para un nuevo perfil de servidor IdL de SAML. **Browse (Busque)** el archivo, especifique el Nombre de perfil y Sesgo máximo de reloj y luego haga clic en **OK (Aceptar)** para crear el perfil. Opcionalmente, puede editar el perfil para cambiar los valores importados.
Validar certificado de proveedor de identidad	Seleccione esta opción para validar la cadena de confianza y, opcionalmente, el estado de la revocación del certificado de firma IdP. Para habilitar esta opción, una entidad de certificación (CA) debe emitir el certificado de firma de su IdP. Debe crear un Perfil de 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 de Certificado para validar el certificado IdP (consulte Dispositivo > Perfil de Autenticación). 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

© 2020 Palo Alto Networks, Inc.

Configuración de servidor de proveedor de identidad SAML	Description (Descripción)
	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 9.1.3 o una versión 9.1 posterior para reducir la exposición a CVE-2020-2021.
Firma del mensaje SAML en IdP	Seleccione esta opción para especificar que el cortafuegos firme los mensajes que envía al IdP. El cortafuegos utiliza la **Certificate for Signing Requests (Solicitud de firma de certificado)** que especifique en un perfil de autenticación (consulte Device > Authentication Profile). *El uso de un certificado de firma garantiza la integridad de los mensajes enviados al IdP.*
Sesgo máximo de reloj	Introduzca la diferencia de tiempo máxima aceptable en segundos entre el IdP y los tiempos del sistema del cortafuegos en el momento en que el cortafuegos valida un mensaje que recibe del IdP (el intervalo es de 1-900; predeterminado es 60). Si la diferencia de tiempo excede este valor, la validación (y por tanto la autenticación) falla.

© 2020 Palo Alto Networks, Inc.

Device > Server Profiles > DNS

Para simplificar la configuración para un sistema virtual, un perfil de servidor de DNS le permite especificar el sistema virtual que se está configurando, un origen de herencia o las direcciones DNS primarias y secundarias para los servidores de DNS, así como la interfaz y la dirección de origen (ruta de servicio) que se usará en los paquetes enviados al servidor de DNS. La interfaz y la dirección de origen se usan como interfaz y dirección destino en la respuesta desde el servidor de DNS.

Un perfil de servidor de DNS solo sirve para un sistema virtual; no sirve para la ubicación compartida global.

Configuración de perfil de servidor de DNS	Description (Descripción)
Nombre	Asigne un nombre al perfil de servidor de DNS.
Ubicación	Seleccione el sistema virtual al que pertenece el perfil.
Origen de herencia	Seleccione **None (Ninguno)** si las direcciones del servidor de DNS no son heredadas. De lo contrario, especifique el servidor de DNS desde el que el perfil debería heredar la configuración.
Comprobar estado de origen de herencia	Haga clic para ver la información de origen de herencia.
DNS principal	Especifique la dirección IP del servidor DNS primario.
DNS secundario	Especifique la dirección IP del servidor DNS secundario.
Ruta de servicio IPv4	Seleccione esta opción si desea especificar que los paquetes dirigidos al servidor de DNS tienen su origen en una dirección IPv4.
Interfaz de origen	Especifique la interfaz de origen que usarán los paquetes dirigidos al servidor de DNS.
Dirección de origen	Especifique la dirección de origen IPv4 desde la que se originan los paquetes dirigidos al servidor de DNS.
Ruta de servicio IPv6	Seleccione esta opción si desea especificar que los paquetes dirigidos al servidor de DNS tienen su origen en una dirección IPv6.
Interfaz de origen	Especifique la interfaz de origen que usarán los paquetes dirigidos al servidor de DNS.
Dirección de origen	Especifique la dirección de origen IPv6 desde la que se originan los paquetes dirigidos al servidor de DNS.

© 2020 Palo Alto Networks, Inc.

Dispositivo> Perfiles de servidor> Autenticación de múltiples factores

Utilice esta página para configurar un perfil de servidor de autenticación de múltiples factores (MFA) que define cómo se conecta el servidor de seguridad a un servidor MFA. MFA puede proteger sus recursos más sensibles al asegurar que los atacantes no puedan acceder a su red y moverse lateralmente a través de ella comprometiendo un único factor de autenticación (por ejemplo, robar credenciales de inicio de sesión). Después de configurar el perfil de servidor, asígnelo a perfiles de autenticación para los servicios que requieren autenticación (consulte Device > Authentication Profile).

En los siguientes casos de uso de autenticación, el cortafuegos se integra con proveedores de autenticación de múltiples factores (multi-factor authentication, MFA) utilizando RADIUS y SAML:

- Autenticación de usuario remoto a través de portales y puertas de enlace de GlobalProtect™.
- Autenticación de administrador en la interfaz web de PAN-OS y Panorama™.
- Autenticación a través de la política de autenticación.

Además, el cortafuegos se puede integrar con MFA vendors (Proveedores de MFA) utilizando la API para aplicar la MFA a través de la política de autenticación solo para la autenticación de usuarios finales (no para autenticación de GlobalProtect o de administrador).

El Procedimiento completo para configurar MFA requiere tareas adicionales además de crear un perfil de servidor.

Las secuencias de autenticación no admiten perfiles de autenticación que especifiquen perfiles de servidor MFA.

Si el cortafuegos se integra con su proveedor MFA a través de RADIUS, configure un perfil de servidor RADIUS (consulte Device > Server Profiles > RADIUS). El cortafuegos admite todos los proveedores de MFA a través de RADIUS.

Configuración de servidor MFA	Description (Descripción)
Nombre de perfil	Introduzca un nombre para identificar el servidor (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o la ubicación **Shared (Compartida)**. Una vez guardado el perfil, no puede cambiar su **Location (Ubicación)**.
Perfil del certificado	Selecciona el **Certificate Profile (Perfil del certificado)** que especifica el certificado de la autoridad de certificación (CA) y que el cortafuegos utilizará para validar el certificado del servidor MFA al configurar una conexión segura con el servidor. Para obtener más información, consulte Device > Certificate Management > Certificate Profile.
MFA Vendor / Value (Proveedor/Valor de MFA)	Seleccione un proveedor de MFA en **MFA Vendor (Proveedor de MFA)** e introduzca un **Value (Valor)** para cada atributo de proveedor. Los atributos varían según el proveedor. Consulte la documentación de su proveedor para obtener los valores correctos.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor MFA	Description (Descripción)

	• **Duo v2**:
	  • **Host API**: el nombre de host del servidor Duo v2.
	  • **Integration Key (Clave de integración)** y **Secret Key (Clave secreta)**: el cortafuegos utiliza estas claves para autenticarse en el servidor Duo v2 y para firmar las solicitudes de autenticación que envía al servidor. Para proteger estas claves, la clave maestra del cortafuegos las cifra automáticamente para que sus valores de texto sin formato no se expongan en ninguna parte del almacenamiento del cortafuegos. Póngase en contacto con su administrador de Duo v2 para obtener las claves.
	  • **Timeout (Tiempo de espera)**: introduzca el tiempo en segundos después del cual el cortafuegos deja de intentar comunicarse con el **API Host (Host API)** (intervalo 5-600; predeterminado es 30). Este intervalo debe ser mayor que el tiempo de espera entre el host API y el dispositivo de endpoint del usuario.
	  • **Base URI**: si su organización aloja un servidor proxy de autenticación local para el servidor Duo v2, introduzca el URI del servidor proxy (predeterminado / auth / v2).
	• **Okta Adaptive**:
	  • **Host API**: el nombre de host del servidor Okta.
	  • **Base URI**: si su organización aloja un servidor proxy de autenticación local para el servidor Okta, introduzca el URI del servidor proxy (predeterminado / api / v1).
	  • **Token**: el cortafuegos utiliza este token para autenticarse en el servidor Okta y para firmar las solicitudes de autenticación que envía al servidor. Para proteger el token, la clave maestra del cortafuegos lo cifra automáticamente para que su valor de texto sin formato no quede expuesto en ningún lugar del almacenamiento del cortafuegos. Póngase en contacto con su administrador de Okta para obtener el token.
	  • **Organization (Organización)**: el subdominio para su organización en el **API Host (Host API)**.
	  • **Timeout (Tiempo de espera)**: introduzca el tiempo en segundos después del cual el cortafuegos deja de intentar comunicarse con el **API Host (Host API)** (intervalo 5-600; predeterminado es 30). Este intervalo debe ser mayor que el tiempo de espera entre el host API y el dispositivo de endpoint del usuario.
	• **PingID**:
	  • **Base URI**: si su organización aloja un servidor proxy de autenticación local para el servidor PingID, introduzca el URI del servidor proxy (predeterminado / pingid / rest / 4).
	  • **Host name (Nombre de host)**: Introduzca el nombre del servidor PingID (predeterminado idpxnyl3m.pingidentity.com).
	  • **Use Base64 Key (Utilizar clave Base64)** y **Token**: el cortafuegos utiliza la clave y el token para autenticarse en el servidor PingID y firmar las solicitudes de autenticación que envía al servidor. Para proteger la clave y el token, la clave maestra del cortafuegos los cifra automáticamente para que sus valores de texto sin formato no se expongan en ningún lugar del almacenamiento del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Configuración de servidor MFA	Description (Descripción)
	Póngase en contacto con su administrador PingID para obtener los valores. • **PingID Client Organization ID (ID de organización de cliente PingID)**: el identificador PingID de su organización. • **Timeout (Tiempo de espera)**: introduzca el tiempo en segundos después del cual el cortafuegos deja de intentar comunicarse con el servidor PingID especificado en el campo **Host name (Nombre de host)** (intervalo 5-600; predeterminado es 30). Este intervalo debe ser más largo que el tiempo de espera entre el servidor PingID y el dispositivo de endpoint del usuario.

© 2020 Palo Alto Networks, Inc.

Device > Local User Database > Users

Puede configurar una base de datos local en el cortafuegos para almacenar información de autenticación para el cortafuegos Administradores, Usuarios finales del portal cautivo y los usuarios finales que se autentican en un Portal de GlobalProtect y una Puerta de enlace de GlobalProtect. La autenticación de base de datos local no requiere ningún servicio de autenticación externa; se realiza toda la gestión de cuentas en el cortafuegos. Después de crear la base de datos local y (opcionalmente) asignar los usuarios a los grupos (consulte Device > Local User Database > User Groups), usted puede Device > Authentication Profile basado en la base de datos local.

No se puede configurar Device > Password Profiles para cuentas administrativas que utilizan autenticación de base de datos local.

Para **Add (Añadir)** un usuario local a la base de datos, configure la configuración descrita en la siguiente tabla.

Configuración de usuario local	Description (Descripción)
Nombre	Introduzca un nombre para identificar al usuario (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible la cuenta de usuario. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardada la cuenta de usuario, no puede cambiar su **Location (Ubicación)**.
Modo	Utilice este campo para especificar la opción de autenticación: • **Password (Contraseña)**: Introduzca y confirme una contraseña para el usuario. • **Password Hash (Contraseña con hash)**: introduzca una cadena de contraseña con hash. Esto puede ser útil si, por ejemplo, desea reutilizar las credenciales de una cuenta Unix existente pero no conoce la contraseña de texto sin formato, sólo la contraseña hash. El cortafuegos acepta cualquier cadena de hasta 63 caracteres independientemente del algoritmo utilizado para generar el valor de hash. El comando CLI operativo `request password-hash password` Utiliza el algoritmo MD5 cuando el cortafuegos está en modo normal y el algoritmo SHA256 cuando el cortafuegos está en el modo CC / FIPS. *Cualquier parámetro de Complejidad mínima de la contraseña que defina para el cortafuegos (Device (Dispositivo) > Setup (Configuración) > Management (Gestión)) no se aplican a las cuentas que usan una Password Hash (Contraseña con hash).*
Habilitación	Seleccione esta opción para activar la cuenta de usuario.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Base de datos de usuario local > Grupos de usuarios

Seleccione **Device (Dispositivo)** > **Local User Database (Base de datos de usuario local)** > **User Groups (Grupos de usuarios)** para añadir información de grupo de usuario a la base de datos local.

Configuración de grupo de usuarios local	Description (Descripción)
Nombre	Introduzca un nombre para identificar el grupo (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	Seleccione el ámbito en el que está disponible el grupo de usuarios. En el contexto de un cortafuegos con más de un sistema virtual (vsys), seleccione un vsys o **Shared** (todos los sistemas virtuales). En cualquier otro contexto, no puede seleccionar la **Location (Ubicación)**; su valor se define previamente como Compartido (cortafuegos) o como Panorama. Una vez guardado el grupo de usuarios, no puede cambiar su **Location (Ubicación)**.
Todos los usuarios locales	Haga clic en **Add (Añadir)** para seleccionar a los usuarios que desee añadir al grupo.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Programación de la exportación de logs

Puede Programar exportaciones de logs y guardarlas en un servidor File Transfer Protocol (FTP) en formato CSV o utilizar Secure Copy (SCP) para transferir datos de manera segura entre el cortafuegos y un host remoto. Los perfiles de logs contienen la información de programación y servidor FTP. Por ejemplo, puede que un perfil especifique la recogida de los logs del día anterior cada día a las 3:00 y su almacenamiento en un servidor FTP específico.

Haga clic en **Add (Añadir)** y especifique los siguientes ajustes:

Configuración de la programación de la exportación de logs	Description (Descripción)
Nombre	Introduzca un nombre para identificar el perfil (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. No podrá cambiar el nombre después de crear el perfil.
Description (Descripción)	Introduzca una descripción opcional (de hasta 255 caracteres).
Habilitación	Seleccione esta opción para habilitar la programación de exportaciones de logs.
Tipo de log	Seleccione el tipo de log (**traffic [tráfico]**, **threat [amenaza]**, **gtp**, **sctp**, **tunnel [túnel]**, **User-ID**, **auth [autenticación]**, **url**, **data [datos]**, **hipmatch [coincidencia HIP]** o **WildFire**). El valor predeterminado es Tráfico.
Scheduled Export Start Time (Hora de inicio de exportación programada) (diario)	Introduzca la hora del día (hh:mm) a la que comenzará la exportación en el formato de 24 horas (00:00 - 23:59).
PROTOCOL	Seleccione el protocolo que debe utilizarse para exportar logs desde el cortafuegos a un host remoto: • **FTP**: este protocolo no es seguro. • **SCP**: este protocolo es seguro. Después de completar los campos restantes, deberá hacer clic en **Test SCP server connection (Conexión de servidor SCP de prueba)** para probar la conectividad entre el cortafuegos y el servidor SCP. Además, deberá verificar y aceptar la clave de host del servidor SCP.
Nombre de host	Introduzca el nombre de host o dirección IP del servidor FTP que se utilizará para la exportación.
Puerto	Introduzca el número de puerto que utilizará el servidor FTP. El valor predeterminado es 21.

© 2020 Palo Alto Networks, Inc.

Configuración de la programación de la exportación de logs	Description (Descripción)
Ruta	Especifique la ruta ubicada en el servidor FTP que se utilizará para almacenar la información exportada.
Enable FTP Passive Mode (Habilitar modo pasivo de FTP)	Seleccione esta opción para utilizar el modo pasivo para la exportación. De manera predeterminada, esta opción está seleccionada.
Nombre de usuario	Introduzca el nombre de usuario para acceder al servidor FTP. El valor predeterminado es anónimo.
Contraseña/Confirmar contraseña	Introduzca la contraseña para acceder al servidor FTP. No se necesita contraseña si el usuario es anónimo.
Conexión de servidor SCP de prueba (Solo protocolo SCP)	Si establece el **Protocol (Protocolo)** a **SCP**, debe hacer clic en el botón para probar la conectividad entre el cortafuegos y el servidor SCP, y a continuación verificar y aceptar la clave de host del 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).*

© 2020 Palo Alto Networks, Inc.

Device > Software

Seleccione **Device (Dispositivo)** > **Software** para ver las versiones de software disponibles, descargar o cargar una versión, instalar una versión (se requiere una licencia de asistencia), eliminar una imagen de software del cortafuegos o ver las notas de la versión.

Antes de actualizar la versión de su software o volver a una versión anterior:

- Revise las Release Notes (Notas de la versión) actual para ver descripciones de las nuevas funciones y los cambios del comportamiento predeterminado en una versión, y ver la ruta de migración para actualizar el software.
- Revise las consideraciones de actualización y vuelta a una versión anterior y las instrucciones de actualización la Guía de funciones nuevas de PAN-OS® 9.1.
- Asegúrese de que la configuración de fecha y hora en el cortafuegos esté actualizada. El software PAN-OS está firmado digitalmente y el cortafuegos comprueba la firma antes de instalar una nueva versión. Si la configuración de fecha y hora del cortafuegos no está actualizada y el cortafuegos percibe que la firma del software es futura (de manera errónea), mostrará el siguiente mensaje:

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

En la siguiente tabla se proporciona ayuda para utilizar la página de **Software**.

Campos de opciones de software	Description (Descripción)
versión	Muestra las versiones de software que están disponibles actualmente en el servidor de actualizaciones de Palo Alto Networks. Para comprobar si hay una nueva versión de software disponible en Palo Alto Networks, haga clic en **Check Now (Comprobar ahora)**. El cortafuegos utiliza la ruta del servicios para conectar al servidor de actualizaciones y comprueba la existencia de nuevas versiones. Si hay actualizaciones disponibles, las muestra al principio de la lista.
Tamaño	Indica el tamaño de la imagen de software.
Release date	Indica la fecha y hora en la que Palo Alto Networks publicó la versión.
Disponible	Indica la versión correspondiente de la imagen de software cargada o descargada en el cortafuegos.
Instalado actualmente	Indica si la versión correspondiente de la imagen de software está activada y si se ejecuta actualmente en el cortafuegos.
Acción	Indica la acción actual que puede realizar para la imagen de software correspondiente de la siguiente forma: • **Download (Descargar)**: la versión de software correspondiente está disponible en el servidor de actualizaciones de Palo Alto Networks; haga clic en **Download (Descargar)** para descargar la versión disponible del software. • **Install (Instalar)**: se ha descargado o cargado la versión de software correspondiente en el cortafuegos; haga clic en **Install (Instalar)** para

© 2020 Palo Alto Networks, Inc.

Campos de opciones de software	Description (Descripción)
	instalar el software. Se necesita reiniciar para completar el proceso de actualización. • **Reinstall (Reinstalar)**: previamente se instaló la versión de software correspondiente; haga clic en **Reinstall (Reinstalar)** para volver a instalar la misma versión.
Notas de versión	Proporciona un enlace a las notas de la versión de la actualización de software correspondiente. Este enlace solo está disponible para actualizaciones que descargue del servidor de actualizaciones de Palo Alto Networks: no está disponible para actualizaciones cargadas.
☒	Elimina la imagen de software cargada o descargada anteriormente del cortafuegos. Únicamente puede eliminar la imagen base en el caso de versiones anteriores que no necesiten actualizarse. Por ejemplo, si ejecuta 7.0, puede eliminar la imagen base de 6.1 a menos que crea que pueda necesitar una versión anterior en algún momento.
Comprobar ahora	Comprueba si hay nuevas actualizaciones de software en Palo Alto Networks.
Carga	Importa una imagen de actualización de software desde un ordenador al que tiene acceso el cortafuegos. Se suele utilizar esta opción si el cortafuegos no tiene acceso a Internet, que es necesario al descargar actualizaciones desde el servidor de actualizaciones de Palo Alto Networks. En el caso de las cargas, use un equipo conectado a Internet para visitar el sitio web de Palo Alto Networks, descargue la imagen de software del sitio de Asistencia técnica (Actualizaciones de software), descargue la actualización en su equipo, seleccione **Device (Dispositivo)** > **Software** en el cortafuegos y luego **Upload (Cargar)** para cargar la imagen de software. En una configuración de alta disponibilidad (HA), puede seleccionar **Sync To Peer (Sincronizar en el peer)** para enviar la imagen de software importada al peer HA. Una vez cargada, la página**Software** muestra la misma información (p. ej., versión y tamaño) y las opciones **Install (Instalar)**/**Reinstall (Reinstalar)** para software cargado y descargado. La opción de **Release Notes (Notas de la versión)** no está activa para el software cargado.

© 2020 Palo Alto Networks, Inc.

Device > Dynamic Updates

- Device > Dynamic Updates
- Panorama > Dynamic Updates

Palo Alto Networks publica periódicamente actualizaciones que incluyen aplicaciones nuevas y modificadas, protección frente a amenazas y archivos de datos de GlobalProtect mediante actualizaciones dinámicas. El cortafuegos puede recuperar estas actualizaciones y usarlas para aplicar una política, sin necesidad de cambios en la configuración. Las actualizaciones de aplicaciones y algunos antivirus están disponibles sin suscripción; otras dependen de sus suscripciones.

Puede ver las actualizaciones más recientes, leer las notas de versión de cada actualización y, a continuación, seleccionar la actualización que desee descargar e instalar. También puede revertir a una versión de una actualización instalada anteriormente.

La configuración de un cronograma para las actualizaciones dinámicas le permitirá definir la frecuencia con la que el cortafuegos comprobará, descargará o instalará las actualizaciones nuevas. En particular, para las actualizaciones de contenido de aplicaciones y amenazas, es posible establecer un programa que alterne actualizaciones de aplicaciones nuevas y modificadas detrás de las actualizaciones de amenazas; esto le brinda más tiempo para evaluar cómo afectan las aplicaciones nuevas y modificadas a la política de seguridad, mientras que garantiza que el cortafuegos siempre cuente con la protección contra amenazas más reciente.

Opciones de las actualizaciones dinámicas	Description (Descripción)
versión	Muestra las versiones disponibles actualmente en el servidor de actualizaciones de Palo Alto Networks. Para comprobar si hay una nueva versión de software disponible en Palo Alto Networks, haga clic en **Check Now (Comprobar ahora)**. El cortafuegos utiliza la ruta del servicios para conectar al servidor de actualizaciones y comprueba la existencia de nuevas versiones de publicación de contenido. Si hay actualizaciones disponibles, las muestra al principio de la lista.
Última comprobación	Muestra la fecha y hora en la que el cortafuegos se conectó por última vez al servidor de actualizaciones y comprobó si había alguna actualización disponible.
Programa	Le permite programar la frecuencia de recuperación de actualizaciones. Puede definir la frecuencia y el momento en que se producen las actualizaciones de contenido dinámico (l**Recurrence [Periodicidad]** y hora), y las opciones de **Download Only (Solo descargar)** o **Download and Install (Descargar e instalar)** para las actualizaciones programadas. En el caso de las actualizaciones de antivirus, y de aplicaciones y amenazas, puede configurar un umbral mínimo de tiempo durante el cual la actualización de contenido debe estar disponible antes de que el cortafuegos la instale. Rara vez, es posible que se produzca un error en una actualización de contenido y este umbral garantiza que el cortafuegos solo descargue versiones de contenido que hayan estado disponibles y en funcionamiento en entornos de cliente durante un período de tiempo concreto. Para las actualizaciones de contenido de aplicaciones y amenazas, también puede establecer un umbral que se aplique específicamente a las

© 2020 Palo Alto Networks, Inc.

Opciones de las actualizaciones dinámicas	Description (Descripción)
	actualizaciones de contenido con aplicaciones nuevas y modificadas. Un umbral extendido para las aplicaciones le brinda más tiempo para evaluar y adaptar su política de seguridad en función de los cambios que introduzcan las aplicaciones nuevas o modificadas. *Para obtener una orientación sobre cómo habilitar mejor las actualizaciones de contenido de aplicaciones y amenazas para lograr la disponibilidad constante de la aplicación y la protección contra las amenazas más recientes, consulte las* Prácticas recomendadas de actualización de contenido de aplicaciones y amenazas*.*
Nombre de archivo	Muestra el nombre de archivo; incluye información de la versión de contenido.
Features	Enumera el tipo de firmas que puede incluir la versión de contenido. En las versiones de publicaciones de contenido de Aplicaciones y amenazas, este campo podría mostrar una opción para revisar **Apps, Threats (Aplicaciones, Amenazas)**. Haga clic en esta opción para ver nuevas firmas de aplicaciones disponibles por primera vez desde la última versión de publicación de contenido instalada en el cortafuegos. También puede usar el cuadro de diálogo **New Applications (Nuevas aplicaciones)** para **Enable/Disable (Habilitar/Deshabilitar)** nuevas aplicaciones. Puede elegir deshabilitar una nueva aplicación incluida en una publicación de contenido si quiere evitar cualquier impacto en la política desde aplicación que se identifique exclusivamente (una aplicación se puede tratar de manera diferente antes y después de una instalación de contenido si una aplicación desconocida anteriormente se identifica y categoriza de manera de diferente).
Tipo	Indica si la descarga incluye una actualización completa o una actualización incremental.
Tamaño	Muestra el paquete de actualización de contenido.
Release date	Fecha y hora en la que Palo Alto Networks publicó la versión.
Descargado	Una marca de verificación en esta columna indica que se ha descargado la versión correspondiente de la publicación de contenido en el cortafuegos.
Instalado actualmente	Una marca de verificación en esta columna indica que se ha descargado la versión correspondiente de la publicación de contenido que se está ejecutando actualmente en el cortafuegos.
Acción	Indica la acción actual que puede realizar para la imagen de software correspondiente de la siguiente forma: • **Download (Descargar)**: la versión de contenido correspondiente está disponible en el servidor de actualizaciones de Palo Alto Networks; haga clic en **Download (Descargar)** para descargar la versión de contenido. Si el cortafuegos no tiene acceso a internet, utilice un ordenador conectado a internet para ir al Portal de asistencia al cliente y seleccione **Dynamic Updates (Actualizaciones dinámicas)**. Busque la versión de contenido que

© 2020 Palo Alto Networks, Inc.

Opciones de las actualizaciones dinámicas	Description (Descripción)
	desee y haga clic en **Download (Descargar)** para guardar el paquete de actualización en su ordenador local. Luego, haga clic en **Upload (Cargar)** para cargar manualmente el software en el cortafuegos. Asimismo, al descargar una versión de publicación de contenido de Aplicaciones y Amenazas se habilita la opción de **Review Policies (Revisar políticas)** afectadas por las nuevas firmas de aplicaciones incluidas en la publicación. • **Review Policies (Revisar políticas)** [solamente contenido de aplicaciones y amenazas]: revisa cualquier impacto en políticas de nuevas aplicaciones incluidas en una versión de publicación de contenido. Use esta opción para evaluar el tratamiento que recibe una aplicación antes y después de instalar una actualización de contenido. También puede usar el cuadro de diálogo Revisión de políticas para añadir o eliminar una aplicación pendiente (una aplicación que se descarga con una versión de publicación de contenido pero no se instala en el cortafuegos) de una regla de política de seguridad existente; los cambios en políticas para aplicaciones pendientes no tienen efecto hasta que se instala la versión de publicación de contenido correspondiente. • **Review Apps (Revisar aplicaciones)** (solo contenido de aplicación y amenazas): observe las firmas de aplicaciones nuevas y modificadas disponibles por primera vez desde la última versión de publicación de contenido instalada en el cortafuegos. Cuando una actualización de contenido introduzca cambios que podrían afectar la aplicación de aplicaciones críticas, esas aplicaciones se marcan como recomendadas para la revisión de la política. Haga clic en Review Policies (Revisar políticas) para ver cómo las actualizaciones de contenido afectan su política de seguridad existente o puede deshabilitar una aplicación hasta que tenga tiempo para revisar el impacto de la política de la aplicación. • **Install (Instalar)**: se descargó la versión de contenido correspondiente en el cortafuegos; haga clic en **Install (Instalar)** para instalar la actualización. Al instalar una nueva versión de publicación de contenido en Aplicaciones y amenazas, verá la opción de **Disable new apps in content update (Deshabilitar nuevas aplicaciones en actualización de contenido)**. Esta opción ofrece protección contra las amenazas más recientes y al mismo tiempo, le concede la flexibilidad de habilitar aplicaciones tras preparar las actualizaciones de cualquier política, debido al impacto de nuevas firmas de aplicaciones (para habilitar aplicaciones que ha deshabilitado previamente, seleccione **Apps, Threats [Aplicaciones, amenazas]** en la página Dynamic Updates [Actualizaciones dinámicas] o seleccione **Objects [Objetos]** > **Applications [Aplicaciones]**). • **Revert (Revertir)**: anteriormente se ha descargado la versión de publicación de contenido correspondiente. Para volver a instalar la misma versión, haga clic en **Revert (Revertir)**.
Documentación	Proporciona un enlace a las notas de la versión de la versión correspondiente.
☒	Elimine la versión de publicación de contenido descargada anteriormente del cortafuegos.
Carga	Si el cortafuegos no tiene acceso al servidor de actualizaciones de Palo Alto Netwoks, puede descargar manualmente las actualizaciones dinámica del sitio de asistencia técnica de Palo Alto Networks en la sección Actualizaciones

© 2020 Palo Alto Networks, Inc.

Opciones de las actualizaciones dinámicas	Description (Descripción)
	dinámicas. Luego de descargar una actualización en su equipo, haga clic en **Upload (Cargar)** para cargar la actualización al cortafuegos. Luego, seleccione **Install From File (Instalar desde el archivo)** y seleccione el archivo que descargó.
Instalar desde archivo	Luego de cargar manualmente un archivo de actualización al cortafuegos, use esta opción para instalar el archivo. En el menú desplegable **Package Type (Tipo de paquete)**, seleccione el tipo de actualización que instala (**Application and Threats (Aplicaciones y Amenazas)**, **Antivirus** o **WildFire**), haga clic en **OK (Aceptar)**, seleccione el archivo que desea instalar y luego haga clic en **OK (Aceptar)** de nuevo para iniciar la instalación.

© 2020 Palo Alto Networks, Inc.

Device > Support

- Device > Support
- Panorama > Support

Seleccione **Device (Dispositivo)** > **Support (Soporte)** o **Panorama** > **Support (Soporte)** para acceder a las opciones relacionadas con la asistencia técnica. Puede ver la información de contacto de Palo Alto Networks, la fecha de vencimiento y alertas de producto y seguridad de Palo Alto Networks, según el número de serie de su cortafuegos.

Realice cualquiera de las siguientes funciones en esta página:

- **Soporte**: proporciona información sobre el estado de soporte del dispositivo y proporciona un enlace para activar el soporte mediante un código de autorización.
- **Alertas de producción/Alertas de aplicación y amenazas**: estas alertas se recuperarán desde los servidores de actualización de Palo Alto Networks cuando se acceda a esta página o se actualice. Para ver los detalles de las alertas de producción o las alertas de aplicación y amenazas, haga clic en el nombre de la alerta. Las alertas de producción se publicarán si hay una recuperación a gran escala o un problema urgente relacionado con una determinada publicación. Se publicarán alertas de aplicación y amenazas si se descubren alertas de importancia.
- **Enlaces**: proporciona enlaces de soporte comunes para ayudarle a gestionar su dispositivo y para acceder a la información de contacto de soporte.
- **Archivo de asistencia técnica**: haga clic en **Generate Tech Support File (Generar archivo de asistencia técnica)** para generar un archivo del sistema que pueda utilizar el equipo de asistencia técnica para facilitar la resolución de los problemas que pudiera estar experimentando el cortafuegos. Después de generar el archivo, haga clic en **Download Tech Support File (Descargar archivo de asistencia técnica)** y, a continuación, envíelo al departamento de asistencia técnica de Palo Alto Networks.

  Si su navegador está configurado para abrir automáticamente archivos luego de la descarga, debe desactivar esa opción de modo que el navegador descargue el archivo de asistencia técnica en lugar de intentar abrirlo y extraerlo.
- **Archivo de volcado de estadísticas** (solo cortafuegos): haga clic en **Generate Stats Dump File (Generar archivo de volcado de estadísticas)** para generar un conjunto de informes de XML que resuma el tráfico de red en los últimos 7 días. Luego de que se genere el informe, puede hacer clic en **Download Stats Dump File (Descargar archivo de volcado de estadísticas)**. El ingeniero de sistemas de Palo Alto Networks o de un socio autorizado utiliza el reporte para generar un Informe de Ciclo de Vida de Seguridad (SRL). El SRL resalta lo que se ha encontrado en la red y los riesgos asociados con la empresa o de seguridad que pueden existir. Tradicionalmente se utiliza como parte del proceso de evaluación. Para obtener más información sobre SRL, póngase en contacto con el ingeniero de sistemas de Palo Alto Networks o de un socio autorizado.
- **Archivos core**: si su cortafuegos experimenta un fallo del proceso del sistema, generará un archivo core que contiene detalles sobre el proceso y por qué falló. Haga clic en el enlace **Download Core Files (Descargar archivos core)** para ver una lista de los archivos principales disponibles y, a continuación, haga clic en un nombre de archivo core para descargarlo. Después de descargar el archivo, cárguelo en un caso de soporte de Palo Alto Networks para obtener asistencia para resolver el problema.

  El contenido de los archivos core solo puede ser interpretado por un ingeniero de soporte de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Device > Master Key and Diagnostics

- **Device (Dispositivo)** > **Master Key and Diagnostics (Clave maestra y diagnóstico)**
- **Panorama** > **Master Key and Diagnostics (Clave maestra y diagnóstico)**

Edite la clave maestra que cifra todas las contraseñas y claves privadas en el cortafuegos o Panorama (como la clave RSA para autenticar a los administradores que acceden a la CLI). El cifrado de contraseñas y claves mejora la seguridad asegurando que sus valores de texto sin formato no se expongan en ningún lugar del cortafuegos o Panorama.

La única manera de restaurar la clave maestra predeterminada es realizar un restablecimiento de fábrica.

Palo Alto Networks recomienda configurar una nueva clave maestra en lugar de utilizar la clave predeterminada, almacenar la clave en un lugar seguro y cambiarla periódicamente. Para mayor privacidad, puede utilizar un módulo de seguridad de hardware para cifrar la clave maestra (consulte Dispositivo> Configuración> HSM). La configuración de una clave maestra única en cada cortafuegos o servidor de gestión Panorama garantiza que un atacante que aprenda la clave maestra de un dispositivo no pueda acceder a las contraseñas y las claves privadas de cualquiera de sus otros dispositivos. Sin embargo, debe utilizar la misma clave maestra en varios dispositivos en los siguientes casos:

- **Configuraciones de alta disponibilidad (HA)**: si implementa cortafuegos o Panorama en una configuración de alta disponibilidad, utilice la misma clave maestra en los cortafuegos o en los servidores de administración Panorama del par. De lo contrario, la sincronización HA no funcionará.
- **Panorama envía configuraciones a cortafuegos**: si utiliza Panorama para enviar configuraciones a cortafuegos gestionados, utilice la misma clave maestra para Panorama y los cortafuegos gestionados. De lo contrario, las operaciones de envío de Panorama fallarán.

Para configurar una clave maestra, edite la configuración de Clave maestra mediante la siguiente tabla para determinar los valores correctos:

Configuración de clave maestra y diagnóstico	Description (Descripción)
Clave maestra	Habilítela para configurar una clave maestra única. Deshabilite (desmarque) esta opción para usar la clave maestra predeterminada.
Clave maestra actual	Especifique la clave que se utiliza actualmente para cifrar todas las claves privadas y contraseñas del cortafuegos.
Nueva clave principal Confirmar clave maestra	Para cambiar la clave maestra, introduzca una cadena de 16 caracteres y confirme la nueva clave.
Duración	Especifique el número de **Días** y **Horas** tras los cuales caduca la clave maestra. El intervalo es de 1 a 438 000 días (50 años). *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. A continuación, debe realizar un restablecimiento de fábrica.*

© 2020 Palo Alto Networks, Inc.

Configuración de clave maestra y diagnóstico	Description (Descripción)
Tiempo para el recordatorio	Introduzca el número de **Days (Días)** y **Hours (Horas)** Antes de que la clave maestra expire cuando el cortafuegos genere una alarma de caducidad. El cortafuegos abre automáticamente el cuadro de diálogo System Alarms (Alarmas de sistema) para mostrar la alarma. *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).*
Almacenado en HSM	Habilite esta opción si la clave maestra se cifra en un módulo de seguridad de hardware (HSM). No puede utilizar HSM en una interfaz dinámica como un cliente DHCP o PPPoE. La configuración HSM no está sincronizada entre cortafuegos peer en modo de alta disponibilidad. Por lo tanto, cada peer del par de HA se puede conectar a un origen HSM diferente. Si utiliza Panorama y necesita mantener sincronizada la configuración en ambos peers, utilice las plantillas de Panorama para configurar el origen de HSM en los cortafuegos gestionados. PA-220 no admite HSM.
Renovación automática de la clave maestra	Habilite esta opción para renovar automáticamente la clave maestra durante una cantidad especificada de días y horas. Deshabilite (desmarque) esta opción para permitir que la clave maestra caduque después del periodo de vida útil configurado para la clave. Seleccione **Auto Renew with Same Master Key (Renovación automática con la misma clave maestra)** y especifique la cantidad de **Days (Días)** y **Hours (Horas)** a los cuales extender el cifrado de la clave maestra (el intervalo es de 1 hora a 730 días).
Criterios comunes	En el modo Criterios comunes, hay disponibles opciones adicionales para ejecutar una prueba automática de algoritmos criptográficos y una prueba automática de integridad del software. También se incluye un programador para especificar los momentos en los que se ejecutarán las dos pruebas automáticas.

Implementar clave maestra

Implemente una clave maestra o actualice una clave maestra existente en un cortafuegos gestionado, el Recopilador de logs o un dispositivo WF-500 directamente desde Panorama.

Campo	Description (Descripción)
Implementar clave maestra	
Filter (Filtro)	Filtro para mostrar los dispositivos gestionados en función de la plataforma, el grupo de dispositivos, las plantillas, las etiquetas, el estado de HA o la versión de software.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Device Name (Nombre del dispositivo)	Nombre del cortafuegos gestionado.
Versión de software	Versión de software que se ejecuta en el dispositivo gestionado.
estado	Estado de conexión del dispositivo gestionado: puede ser `Connected (Conectado)`, `Disconnected (Desconectado)` o `Unknown (Desconocido)`.
Estado de la tarea de implementación de clave maestra	
Device Name (Nombre del dispositivo)	Nombre del cortafuegos gestionado.
estado	Estado de la tarea de implementación de clave maestra.
Resultado	Resultado de la tarea de implementación de clave maestra. Puede ser `OK (CORRECTO)` o `FAIL (ERROR)`.
Progreso	Progreso (%) de la tarea de implementación de clave maestra.
Detalles	Detalles sobre la tarea de implementación de clave maestra. Si la tarea no se puede realizar, los detalles que describen el motivo del error se mostrarán aquí.
Resumen	
Progreso	Muestra una barra de progreso que indica el avance de la tarea de implementación de clave maestra. Se muestra la siguiente información: • **Results Succeeded (Resultados satisfactorios)**: cantidad de dispositivos en los que la clave maestra se implementó correctamente. • **Results Pending (Resultados pendientes)**: cantidad de dispositivos para los cuales la tarea de implementación de clave maestra está pendiente. • **Results Failed (Resultados erróneos)**: cantidad de dispositivos para los cuales no se pudo llevar a cabo la tarea de implementación de clave maestra.

Identificación de usuarios

La identificación de usuario (User-ID™) es una función del cortafuegos de nueva generación de Palo Alto Networks® que se integra sin problemas con una variedad de servicios de terminal y directorio empresarial para vincular las políticas y la actividad de la aplicación con los nombres de usuarios y grupos en lugar de solo con las direcciones IP. La configuración de User-ID habilita el centro de comando de aplicación (ACC), App Scope, los informes y los logs para incluir nombres de usuarios además de direcciones IP.

> Device > User Identification > User Mapping
> Dispositivo > Identificación de usuarios > Seguridad de conexión
> Device > User Identification > User-ID Agents
> Dispositivo > Identificación de usuarios > Agentes de servidor de terminal
> Device > User Identification > Group Mapping Settings
> Device > User Identification > Captive Portal Settings

¿Busca más información?

Consulte User-ID

© 2020 Palo Alto Networks, Inc.

Device > User Identification > User Mapping

Configure el agente integrado de User-ID de PAN-OS que se ejecuta en el servidor de seguridad para asignar direcciones IP a nombres de usuario.

¿Qué está buscando?	Consulte:
Configurar el agente integrado de User-ID de PAN-OS	Configuración del agente User-ID de Palo Alto Networks
Para gestionar el acceso a los servidores que el agente User-ID supervisa para la información de asignación de usuario, consulte:	Supervisión de servidores
Para gestionar las subredes que el cortafuegos incluye o excluye al recopilar información de asignación de usuario, consulte:	Incluir o excluir subredes para la asignación de usuarios
¿Busca más información?	Configuración de la asignación de usuarios mediante el agente de User-ID integrado en PAN-OS.

Configuración del agente User-ID de Palo Alto Networks

Esta configuración define los métodos que el agente User-ID usa para llevar a cabo la asignación de usuario.

¿Qué está buscando?	Consulte:
Habilite el agente de User-ID para utilizar la instrumentación de gestión de Windows (Windows Management Instrumentation, WMI) para sondear los sistemas cliente o la administración remota de Windows (Windows Remote Management, WinRM) en HTTP o HTTPS para supervisar los servidores con el fin de obtener información de asignación de usuarios.	Cuenta de supervisor del servidor
Supervisar logs del servidor para obtener información de asignación de usuarios con el agente de User-ID.	Monitorización de servidor

© 2020 Palo Alto Networks, Inc.

¿Qué está buscando?	Consulte:
Habilite el agente User-ID para sondear los sistemas del cliente para la información de asignación de usuario.	Sondeo de cliente
Asegúrese de que el cortafuegos tenga la información de asignación de usuario más actual a medida que los usuarios se desplazan y obtienen las nuevas direcciones IP.	Caché
Habilite la autenticación de NT LAN Manager (NTLM) para la asignación de usuario a través del Portal cautivo.	Autenticación NTLM
Habilite los cortafuegos para compartir la información de asignación de usuario y grupo para simplificar la gestión lUser-ID.	Redistribución
Habilite el agente User-ID para analizar los mensajes de Syslog para la información de asignación de usuario.	Filtrados de Syslog
Configure el agente User-ID para omitir los nombres de usuario específicos del proceso de asignación.	Lista de usuarios ignorados

Cuenta de supervisor del servidor

- **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **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)**

Para configurar el agente User-ID integrado en PAN-OS para que utilice la instrumentación de gestión de Windows (Windows Management Instrumentation, WMI) para sondear los sistemas cliente o la Administración remota de Windows (Windows Remote Management, WinRM) en HTTP o HTTPS para supervisar los servidores con el fin de obtener información de asignación de usuarios, complete los campos a continuación.

También puede Configuración de acceso a servidores supervisados al configurar un servidor de Kerberos para autenticar la supervisión de servidores usando la Administración remota de Windows (WinRM) en HTTP o HTTPS.

Debido a que el sondeo de WMI confía en los datos que se informan de un endpoint, Palo Alto Network recomienda que no utilice este método para obtener información de asignación de User-ID en una red de alta seguridad. Si configura el agente User-ID para obtener información de asignación analizando los registros de sucesos de seguridad de Active Directory (AD) o los mensajes syslog, o utilizando la API XML, Palo Alto Networks recomienda desactivar el sondeo WMI.

Si utiliza el sondeo de WMI, no lo habilite en interfaces externas que no son de confianza. Al hacerlo, el agente envía sondas WMI que contienen información confidencial, como el nombre de usuario, el nombre de dominio y el hash de contraseña de la cuenta de servicio del agente de User-ID, fuera de su red. Un atacante podría explotar esta información para penetrar y obtener más acceso a su red.

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación de Active Directory	Description (Descripción)
Nombre de usuario	Introduzca las credenciales de dominio (**User Name [Nombre de usuario]** y **Password [Contraseña]**) de la cuenta que el cortafuegos utilizará para acceder a los recursos de Windows. La cuenta requiere permisos para llevar a cabo consultas de WMI en computadoras de cliente y para supervisar servidores Microsoft Exchange y controladores de dominio. Utilice la sintaxis domain\username para el **User Name (Nombre de usuario)**. Si Configuración de acceso a servidores supervisados usando Kerberos para la autenticación de servidor, introduzca el nombre principal de usuario (User Principal Name, UPN) de Kerberos.
Nombre de DNS del dominio	Introduzca el nombre DNS del servidor supervisado. Si Configuración de acceso a servidores supervisados usando Kerberos para la autenticación de servidor, introduzca el dominio de Kerberos (Kerberos Realm). Debe configurar este ajuste si está utilizando **WinRM-HTTP** como el protocolo de transporte cuando Configuración de acceso a servidores supervisados.
Contraseña/Confirmar contraseña	Introduzca y confirme la contraseña de la cuenta que el cortafuegos utiliza para acceder a los recursos de Windows.
Perfil de servidor Kerberos	Seleccione el perfil de servidor Kerberos para el servidor Kerberos que controla el acceso al dominio con el fin recuperar logs de seguridad e información de la sesión del servidor supervisado con WinRM en HTTP o HTTPS.

El procedimiento completo para configurar el agente User-ID integrado con PAN-OS para supervisar los servidores y sondear a los clientes requiere tareas adicionales además de la definición de la configuración de autenticación de Active Directory.

Monitorización de servidor

- **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Server Monitor (Supervisión de servidores)**

Para habilitar al agente de User-ID para asignar direcciones IP a nombres de usuario mediante la búsqueda de sucesos de inicio de sesión en los logs de eventos de seguridad de los servidores, configure los valores descritos en la tabla siguiente.

Si la carga de consultas es alta para los logs de servidor de Windows, las sesiones del servidor de Windows o servidores eDirectory, el retardo observado entre consultas puede superar considerablemente el intervalo o frecuencia especificados.

El procedimiento completo para configurar el agente User-ID integrado con PAN-OS para supervisar a los servidores requiere tareas adicionales además de la definición de la configuración de la supervisión de servidores.

© 2020 Palo Alto Networks, Inc.

Configuración de Supervisión de servidor	Description (Descripción)
Habilitar log de seguridad	Seleccione esta opción para habilitar la monitorización de logs de seguridad en los servidores de Windows
Frecuencia de monitorización de log de servidor (en segundos)	Especifique la frecuencia en segundos en la que el cortafuegos solicitará los logs de seguridad al servidor de Windows para la información de asignación de usuarios (intervalo: 1-3600; predeterminado: 2). Este es el intervalo en el cual el cortafuegos termina de procesar la última consulta y envía la siguiente. *Si la supervisión de logs no se produce con la frecuencia suficiente, es posible que la asignación de dirección IP a usuario más reciente no esté disponible. Si el cortafuegos crea logs con demasiada frecuencia, el controlador de dominio, la memoria, la CPU y la aplicación de la política de User-ID pueden verse afectados. Comience con un valor en el intervalo de 2 a 30 segundos y luego revise el valor en función del impacto en el rendimiento o la frecuencia con la que se actualizan las asignaciones de usuario.*
Habilitar sesión	Seleccione esta opción para habilitar la monitorización de sesiones de usuario en los servidores supervisados. Cada vez que un usuario se conecta a un servidor, se crea una sesión y el cortafuegos puede utilizar esta información para identificar la dirección IP del usuario. *No haga clic en Enable Session (Habilitar sesión). 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 las fuentes 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 NAC.*
Frecuencia de lectura de sesión de servidor (en segundos)	Especifique la frecuencia en segundos en la que el cortafuegos solicitará a las sesiones de usuario del servidor de Windows la información de asignación de usuarios (intervalo: 1-3600; predeterminado: 10). Este es el intervalo entre cuando el cortafuegos termina de procesar la última solicitud y cuando comienza con la siguiente.
Intervalo de consulta de Novell eDirectory (en segundos)	Especifique la frecuencia en segundos en la que el cortafuegos solicitará a los servidores de Novell eDirectory la información de asignación de usuarios (intervalo: 1-3600; predeterminado: 30). Este es el intervalo entre cuando el cortafuegos termina de procesar la última solicitud y cuando comienza con la siguiente.

© 2020 Palo Alto Networks, Inc.

Configuración de Supervisión de servidor	Description (Descripción)
Perfil de servicio Syslog	Seleccione un perfil de servicio SSL/TLS que especifica el certificado y las versiones SSL/TLS permitidas para las comunicaciones entre el cortafuegos y cualquier emisor Syslog que supervisa el servicio User-ID. Para obtener más información, consulte Device (Dispositivo) > Certificate Management (Gestión de certificados) > SSL/TLS Service Profile (Perfil de servicio SSL/TLS) y Syslog Filters (Filtros de Syslog). Si selecciona **none (ninguno)**, el cortafuegos usa su certificado preconfigurado y autofirmado.

Sondeo de cliente

- **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Client Probing (Sondeo de clientes)**

Puede configurar el agente User-ID para llevar a el sondeo de clientes de WMI para cada sistema de cliente que el proceso de asignación de usuario identifica. El agente User-ID sondeará periódicamente cada dirección IP obtenida para verificar si el mismo usuario sigue conectado. Cuando el cortafuegos se encuentre en una dirección IP para la que no tenga una asignación de usuarios, enviará la dirección al agente User-ID para un sondeo inmediato. Para configurar las opciones de sondeo del cliente, complete los siguientes campos.

No habilite el sondeo de clientes en redes de alta seguridad. No habilite el sondeo de clientes en interfaces externas no fiables. El sondeo de clientes puede generar una gran cantidad de tráfico de red, puede suponer una amenaza para la seguridad cuando se configura incorrectamente y, si está habilitado en una zona externa no fiable, puede permitir que un atacante envíe una sonda fuera de su red y así podría divulgarse el nombre de la cuenta de servicio del agente de User-ID, el nombre de dominio y el hash de contraseña cifrado. 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, y no solo para clientes de Windows.

El procedimiento completo para configurar el agente User-ID integrado con PAN-OS para sondear a los clientes requiere tareas adicionales además de la definición de la configuración del sondeo de clientes.

El agente User-ID integrado en PAN-OS no admite el sondeo de NetBIOS, pero sí lo admite el Agente User-ID basado en Windows.

Configuración de Sondeo de cliente	Description (Descripción)
Habilitar pruebas	Seleccione esta opción para habilitar el sondeo WMI.
Intervalo de sondeo (min)	Introduzca el intervalo de sondeo en minutos (intervalo: 1-1440; predeterminado: 20). Este es el intervalo entre cuando el cortafuegos termina de procesar la última solicitud y cuando comienza con la siguiente.

© 2020 Palo Alto Networks, Inc.

Configuración de Sondeo de cliente	Description (Descripción)
	En implementaciones de gran tamaño, es importante establecer el intervalo correctamente para proporcionar tiempo para sondear cada cliente que el proceso de asignación de usuarios identificó. Por ejemplo, si dispone de 6.000 usuarios y un intervalo de 10 minutos, puede necesitar 10 consultas WMI por segundo de cada cliente. *Si la carga de solicitud de sonda es alta, el intervalo observado entre solicitudes puede superar considerablemente el intervalo que especifique.*

Caché

- **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)** > **Cache (Caché)**

Para asegurarse de que el cortafuegos tenga la información de asignación de usuarios más reciente como los desplazamientos de los usuarios y la obtención de nuevas direcciones IP, configure los tiempos de espera para eliminar las asignaciones de usuarios desde el caché de cortafuegos: Este tiempo de espera se aplica a las asignaciones de usuarios obtenidas a través de cualquier método excepto portal cautivo. En las asignaciones obtenidas a través de Captive Portal, establezca el tiempo de espera en la configuración de Captive Portal (Device [Dispositivo] > User Identification [Identificación de usuarios] > Captive Portal Settings [Configuración de Captive Portal], campos **Timer [Temporizador]** y **Idle Timer [Temporizador de inactividad]**).

Para buscar coincidencias de los nombres de usuario recopilados en los orígenes de User-ID, incluso si no se incluye un dominio, configure el cortafuegos para que permita la coincidencia de nombres de usuario sin dominios. Solo debe utilizar esta opción si los nombres de usuarios en su organización no se duplican en los dominios.

Configuración del caché	Description (Descripción)
Habilitar identificación de usuario	Seleccione esta opción para habilitar un valor de tiempo de espera para las entradas de asignación de usuarios. Al obtener el valor de tiempo de espera para una entrada, el cortafuegos lo elimina y recopila información de asignación nueva. Eso garantiza que el cortafuegos tenga la información más reciente sobre los desplazamientos de los usuarios y la obtención de nuevas direcciones IP. *Habilite el tiempo de espera para garantizar que el cortafuegos tenga la información de asignación de usuario a dirección IP más actualizada.*
Tiempo de espera de identificación de usuario (minutos)	Establezca el valor de tiempo de espera en minutos para las entradas de asignación de usuarios (el intervalo es 1-3.600; predeterminado: 45). *Configure el valor del tiempo de espera en la media vida de la concesión DHCP o la duración válida del vale de Kerberos.*

© 2020 Palo Alto Networks, Inc.

Configuración del caché	Description (Descripción)
	Si configura cortafuegos para redistribuir la información de asignación, cada cortafuegos borra las entradas de asignación que recibe en función del tiempo de espera establecido en ese cortafuegos, no en los tiempos de espera establecidos en los cortafuegos de reenvío.
Allow matching usernames without domains (Permitir nombres de usuario coincidentes sin dominios)	Seleccione esta opción para permitir que el cortafuegos busque coincidencias para los usuarios si no se proporciona el dominio en el origen de User-ID. Para evitar que los usuarios se identifiquen erróneamente, solo seleccione esta opción si sus nombres de usuario no se duplican en los dominios. *Antes de habilitar esta opción, compruebe que el cortafuegos haya obtenido las asignaciones de grupo del servidor de LDAP.*

Autenticación NTLM

- **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)** > **NTLM**

Puede usar NT LAN Manager (NTLM) para autenticar solo a usuarios de Windows. Cuando una solicitud web de cliente coincide con una regla de política de autenticación en la que el objeto de imposición de autenticación especifica un desafió de navegador (consulte Policies > Authentication), un desafío NTLM autentica de forma transparente al cliente. El cortafuegos recopila entonces la información de asignación de usuarios desde el dominio NTLM.

Solo puede habilitar el proceso de autenticación NTLM en un sistema virtual según el cortafuegos, el cual selecciona en el menú desplegable **Location (Ubicación)** en la parte superior de la página **User Mapping (Asignación de usuarios)**.

De forma opcional, puede utilizar el cortafuegos para llevar a cabo el proceso de autenticación NTLM para otros cortafuegos añadiéndolo como un agente User-ID a esos cortafuegos. Para obtener más información, consulte Configuración de acceso a agentes User-ID.

Si usa el agente de User-ID basado en Windows, las respuestas NTLM van directamente al controlador de dominio en el que ha instalado el agente. Para obtener más información, consulte el campo **NTLM Authentication (Autenticación NTLM)** en Device > User Identification > Captive Portal Settings.

Configure reglas de autenticación para usar Inicio de sesión único de Kerberos en lugar de autenticación NTLM. Kerberos es un método de autenticación más potente y robusto que NTLM y no requiere que el cortafuegos tenga una cuenta administrativa para unirse al dominio. Para obtener información detallada sobre la configuración de los métodos de autenticación para las reglas de autenticación, consulte Objects > Authentication.

Los procedimientos completos para configurar el portal cautivo o Agentes User-ID basados en Windows requieren tareas adicionales.

Para configurar el procesamiento de autenticación NTLM, especifique la configuración descrita en la siguiente tabla.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Habilitar procesamiento de autenticación NTLM	Seleccione esta opción para habilitar el proceso de autenticación NTLM.
Dominio Ntlm	Introduzca el nombre de dominio NTLM.
Nombre de usuario del administrador (para el dominio NTLM)	Introduzca la cuenta del administrador que tiene acceso al dominio NTLM. *No incluya el dominio en el campo Admin User Name (Nombre de usuario del administrador) De lo contrario, el cortafuegos no podrá unirse al dominio.*
Contraseña/Confirmar contraseña (para el dominio NTLM)	Introduzca la contraseña de la cuenta del administrador que tiene acceso al dominio NTLM.

Redistribución

- **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)** > **Redistribution (Redistribución)**

Para habilitar un cortafuegos o un sistema virtual para servir como un agente User-ID que redistribuye información de asignación de usuarios junto con las marcas de tiempo asociadas con desafíos de autenticación, configure los valores descritos en la siguiente tabla. Cuando más tarde conecte este cortafuegos a un dispositivo (como Panorama) que recibirá la información de asignación y las marcas de tiempo, el dispositivo utilizará estos campos para identificar el cortafuegos o el sistema virtual como un agente de User-ID.

El procedimiento completo para configurar cortafuegos para redistribuir información de asignación de usuarios y marcas de tiempo de autenticación requiere tareas adicionales además de especificar la configuración de redistribución.

De forma predeterminada, un servidor de seguridad con varios sistemas virtuales no redistribuye la información de asignación de usuarios a través de sus sistemas virtuales, aunque puede configurarlos para su redistribución.

Configuración de redistribución	Description (Descripción)
Nombre del recopilador	Introduzca el Nombre del recopilador (hasta 255 caracteres alfanuméricos) que identifica al cortafuegos o sistema virtual como agente de User-ID.
Clave precompartida/ Confirmar clave precompartida	Introduzca una clave precompartida (hasta 255 caracteres alfanuméricos) para identificar al cortafuegos o el sistema virtual como un agente User-ID.

© 2020 Palo Alto Networks, Inc.

Filtrados de Syslog

- **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User Mapping (Asignación de usuarios)** > **Palo Alto Networks User-ID Agent Setup (Configuración de agente de User-ID de Palo Alto Networks)** > **Syslog Filters (Filtros de Syslog)**

El agente de User-ID utiliza perfiles de análisis de Syslog para filtrar mensajes de syslog enviados desde los remitentes de syslog que supervisa el agente en búsqueda de información de asignación de dirección IP a nombre de usuario (consulte Configuración de acceso a servidores supervisados). Cada perfil puede analizar mensajes de syslog para cualquiera de los siguientes tipos de eventos, pero no ambos:

- Eventos de autenticación (inicio de sesión): se utilizan para añadir asignaciones de usuario al cortafuegos.
- Eventos de cierre de sesión: se utilizan para eliminar asignaciones de usuarios obsoletas. La eliminación de asignaciones obsoletas es útil en entornos en los que las asignaciones de direcciones IP cambian con frecuencia.

Palo Alto Networks proporciona al cortafuegos perfiles predefinidos de análisis de Syslog a través de actualizaciones de contenido de aplicaciones. Para actualizar dinámicamente la lista de perfiles a medida que los proveedores desarrollan nuevos filtros, programe actualizaciones de contenido dinámico (consulte Device [Dispositivo] > Dynamic Updates [Actualizaciones dinámicas]). Los perfiles predefinidos son globales para el cortafuegos, mientras que los perfiles personalizados que el usuario configura se aplican solo al sistema virtual (**Location [Ubicación]**) seleccionado en **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User Mapping (Asignación de usuarios)**.

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. Una nueva línea (\n) o un retorno de carro más una nueva línea (\r\n) son los delimitadores de los saltos de línea.
- El tamaño máximo permitido de un mensaje de syslog individual es de 2048 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.

Para configurar un perfil personalizado, haga clic en **Add (Añadir)** y especifique la configuración que se describe en la siguiente tabla. Las descripciones de campos de esta tabla utilizan un ejemplo de evento de inicio de sesión de un mensaje de syslog con el formato siguiente:

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```

El procedimiento completo de configuración del agente de User-ID para analizar la información de asignación de usuarios de un remitente de syslog requiere tareas adicionales, además de crear un perfil de análisis de syslog.

Campo	Description (Descripción)
Perfil de análisis de Syslog	Introduzca un nombre para el perfil (hasta 63 caracteres alfanuméricos).
Description (Descripción)	Introduzca una descripción del perfil (hasta 255 caracteres alfanuméricos).
Tipo	Especifique el tipo de análisis que se debe utilizar para filtrar la información de asignación de usuarios: • **Regex Identifier (Identificador Regex)**: use los campos **Event Regex (Regex de eventos)**, **Username Regex (Regex de nombre de usuario)** y **Address Regex (Regex de dirección)** para especificar expresiones

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	regulares (regex) que describan patrones de búsqueda para identificar y extraer la información de asignación de usuarios de los mensajes de syslog. El cortafuegos utiliza las regex para hacer coincidir los eventos de autenticación o de cierre de sesión de los mensajes de syslog y los nombres de usuario y las direcciones IP con los mensajes de coincidencia. • **Field Identifier (Identificador de campo)**: use los campos **Event String (Cadena de eventos)**, **Username Prefix (Prefijo de nombre de usuario)**, **Username Delimiter (Delimitador de nombre de usuario)**, **Address Prefix (Prefijo de dirección)** y **Address Delimiter (Delimitador de dirección)** para especificar las cadenas y hacer coincidir el evento de autenticación o de cierre de sesión, y para identificar la información de asignación de usuarios en los mensajes de syslog. Los campos restantes del cuadro de diálogo varían en función de su selección. Configure los campos como se describe en las siguientes filas.
Regex de eventos	Introduzca la regex para identificar los eventos de autenticación o de cierre de sesión correctos. En el ejemplo de mensaje de esta tabla, la regex **`(authentication\ success) {1}`** extrae la primera instancia **`{1}`** de la cadena `authentication success`. 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.
Regex de nombre de usuario	Introduzca la regex para identificar el campo de nombre de usuario en los mensajes de autenticación o de cierre de sesión correctos. En el mensaje de ejemplo de esta tabla, la regex **`User:([a-zA-Z0-9\\\._]+)`** coincidiría con la cadena `User:johndoe_4` y extraería acme\johndoe1 como nombre de usuario.
Regex de dirección	Introduzca la regex para identificar la parte de la dirección IP de los mensajes de autenticación correcta o de cierre de sesión. En el mensaje de ejemplo de esta tabla, 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:192.168.0.212` y añade 192.168.0.212 como la dirección IP en la asignación de nombres de usuario.
Cadena de eventos	Introduzca una cadena coincidente para identificar los mensajes de autenticación correcta o de cierre de sesión. En el mensaje de ejemplo de esta tabla, introduciría la cadena **`authentication success`**.
Prefijo de nombre de usuario	Introduzca la cadena coincidente para identificar el principio del campo del nombre de usuario en los mensajes de syslog de autenticación o de cierre de sesión. Este campo no admite regex como \s (para un espacio) o \t (para una pestaña). En el mensaje de ejemplo de esta tabla, `User:(Usuario:)` identifica el inicio del campo del nombre de usuario.
Delimitador de nombre de usuario	Introduzca el delimitador que marca el final del campo del nombre de usuario en un mensaje de autenticación o de cierre de sesión. Utilice \s para indicar un espacio independiente (como en el mensaje de ejemplo) y \t para indicar una pestaña.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Prefijo de dirección	Introduzca una cadena coincidente que marque 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 el mensaje de ejemplo de esta tabla, `Source: (Fuente:)` identifica el inicio del campo de dirección.
Delimitador de dirección	Introduzca la cadena coincidente que marca el final del campo de dirección IP en los mensajes de autenticación correcta o de cierre de sesión. Por ejemplo, introduzca \n para indicar que el delimitador es un salto de línea.

Lista de usuarios ignorados

- **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)** > **Ignore User List (Lista de usuarios ignorados)**

La lista de usuarios ignorados define qué cuentas de usuario no requieren la asignación de dirección IP a nombre de usuario (por ejemplo, cuentas de kiosk). Para configurar la lista, haga clic en **Add (Añadir)** e introduzca un nombre de usuario. 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***coincide 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.

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.

Supervisión de servidores

- Device > User Identification > User Mapping

Use la sección Supervisión de servidores para definir los servidores Microsoft Exchange, los controladores de dominio Active Directory (AD), los servidores Novell eDirectory o los emisores syslog que el agente User-ID supervisará para los eventos de inicio de sesión.

- Configuración de acceso a servidores supervisados
- Gestión de acceso a servidores supervisados
- Incluir o excluir subredes para la asignación de usuarios

Configuración de acceso a servidores supervisados

Utilice la sección Supervisión del servidor para **Add (Añadir)** perfiles de servidor que especifican los servidores que supervisará el cortafuegos.

Configure al menos dos servidores supervisados de User-ID, para que, si un servidor se desactiva, el cortafuegos pueda seguir obteniendo las asignaciones de dirección IP a nombre de usuario.

El procedimiento completo para configurar el agente User-ID integrado en PAN-OS para supervisar los servidores requiere tareas adicionales aparte de la creación de perfiles.

© 2020 Palo Alto Networks, Inc.

Configuración de Supervisión de servidor	Description (Descripción)
Nombre	Introduzca un nombre para el servidor.
Description (Descripción)	Introduzca una descripción del servidor.
Habilitado	Seleccione esta opción para habilitar la monitorización de log para este servidor.
Tipo	Seleccione el tipo de servidor. Su selección determina cuáles otros campos muestra este diálogo. • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Emisor de syslog**
Protocolo de transporte (Microsoft Active Directory y Microsoft Exchange solamente)	Seleccione el protocolo de transporte: • **WMI**: (valor predeterminado) Utilice la instrumentación de gestión de Windows (Windows Management Instrumentation, WMI) para sondear cada dirección IP obtenida y verificar que el mismo usuario siga conectado. • **Win-RM-HTTP**: utilice la administración remota de Windows (Windows Remote Management, WinRM) en HTTP para supervisar los logs de seguridad y la información de sesión en el servidor. Esta opción requiere el **nombre de DNS del dominio** de Kerberos en Cuenta de supervisor del servidor. • **Win-RM-HTTP**: utilice la administración remota de Windows (WinRM) en HTTP para supervisar los logs de seguridad y la información de sesión en el servidor. Para exigir la validación del certificado del servidor con el servidor de Windows al usar la autenticación de Kerberos, asegúrese de configurar NTP en Configuración de servicios globales y seleccione la CA raíz como el perfil de certificado (Device [Dispositivo] > User Identification [Identificación del usuario] > Connection Security [Seguridad de conexión]).
Dirección de red	Introduzca la dirección IP o FQDN del servidor correspondiente al servidor supervisado. Si utiliza Kerberos para la autenticación del servidor, debe introducir un FQDN. Esta opción no es compatible si el **Type (Tipo)** es **Novell eDirectory**.
Perfil de servidor (Solo Novell eDirectory)	Seleccione un perfil de servidor LDAP para conectarse al servidor Novell eDirectory (Device > Server Profiles > LDAP
Tipo de conexión (Solo Emisor Syslog)	Seleccione si el agente de User-ID escucha los mensajes de Syslog en el puerto **UDP** (514) o en el puerto **SSL** (6514). Si selecciona **SSL**, la opción de **Syslog Service Profile (Perfil de servicio de Syslog)** que seleccione cuando habilite la Supervisión de servidor determinará las versiones SSL/TLS que se permiten y el certificado que utiliza el cortafuegos para garantizar una conexión al emisor syslog. *Como práctica recomendada de seguridad, seleccione SSL cuando utilice el agente User-ID integrado en PAN-OS para asignar direcciones IP a nombres de usuario. Si selecciona UDP, asegúrese de que tanto el emisor syslog como el cliente estén en*

© 2020 Palo Alto Networks, Inc.

Configuración de Supervisión de servidor	Description (Descripción)
	una red dedicada y segura para evitar que hosts no fiables puedan enviar tráfico UDP al cortafuegos.
Filter (Filtro) (Solo Emisor Syslog)	Si el **Type (Tipo)** de servidor es **Syslog Sender (Emisor Syslog)**, entonces seleccione **Add (Añadir)** uno o más perfiles de análisis de Syslog para usar en la extracción de nombres de usuario y direcciones IP de los mensajes de syslog recibidos desde este servidor. Puede añadir un perfil personalizado (consulte Filtros de Syslog) o un perfil predefinido. Para cada perfil, establezca el **Event Type (Tipo de evento)**: • **login (iniciar sesión)**: El agente User-ID analiza los mensajes syslog para los eventos de inicio de sesión para crear asignaciones de usuario. • **Logout (cerrar sesión)**: El agente User-ID analiza los mensajes syslog para los eventos de cierre de sesión para eliminar asignaciones de usuarios que ya no están actualizadas. En redes en las que la asignación de direcciones IP es dinámica, la eliminación automática mejora la precisión de las asignaciones de usuarios al garantizar que el agente correlaciona cada dirección IP únicamente con el usuario asociado actualmente. *Si agrega un perfil de análisis de Syslog predefinido, compruebe su nombre para determinar si está destinado a la búsqueda de coincidencias de eventos de inicio de sesión o cierre de sesión.*
Nombre de dominio predeterminado (Solo Emisor Syslog)	(Opcional) Si el tipo de servidor en **Type (Tipo)** es **Syslog Sender (Emisor syslog)**, introduzca un nombre de dominio para anular el nombre de dominio actual en el nombre de usuario de syslog o para que el dominio preceda al nombre de usuario si su mensaje syslog no contiene un dominio.

Gestión de acceso a servidores supervisados

Realice las siguientes tareas en la sección Monitorización de servidor para gestionar el acceso a servidores que el agente User-ID monitorizará para la información de asignación de usuarios.

Tarea	Description (Descripción)
Ver información del servidor	La página User Mapping (Asignación de usuarios) muestra el estado de conexión del agente de User-ID a cada servidor supervisado. Luego de **Add (Añadir)** un servidor, el cortafuegos intenta conectarse a este. Si la conexión se establece correctamente, la sección Server Monitoring (Supervisión de servidor) muestra Connected (Conectado) en la columna Status (Estado). Si el cortafuegos no puede conectarse, la columna Status (Estado) mostrará un error, como `Connection refused` (Conexión rechazada) o `Connection timeout` (Tiempo de espera de la conexión). Para obtener más información sobre otros campos que se muestran en la sección Server Monitoring, consulte Configuración de acceso a los servidores supervisados.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Añadir	Para configurar el acceso a los servidores supervisados, haga clic en **Add (Añadir)** para añadir cada servidor cuya información de asignación de usuarios supervisará el agente de User-ID.
delete	Para eliminar un servidor del proceso de asignación de usuarios (descubrimiento), seleccione el servidor y haga clic en **Delete (Eliminar)**. **Consejo**: Para eliminar un servidor desde descubrimiento sin borrar su configuración, edite la entrada del servidor y borre **Enabled (Habilitado)**.
Descubra	Puede **Discover (Descubrir)** automáticamente los controladores de dominio de Microsoft Active Directory con DNS. El cortafuegos descubrirá los controladores de dominio según el nombre de dominio introducido en la página **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**, sección **General Settings (Configuración general)**, campo **Domain (Dominio)**. Después de descubrir un controlador de dominio, el cortafuegos crea una entrada para este en la lista de Monitorización de servidor, por lo que usted puede habilitar el servidor para la monitorización. *La función Discover (Descubrir) funciona solo para controladores de dominio y no para servidores Exchange o eDirectory.*

Incluir o excluir subredes para la asignación de usuarios

- Device > User Identification > User Mapping

Utilice la lista Incluir/Excluir redes para definir las subredes que el agente User-ID incluirá o excluirá al llevar a cabo la asignación de dirección IP a nombre de usuario (detección). De manera predeterminada, si no añade ninguna subred a la lista, el agente User-ID ejecuta una tarea para descubrir desde dónde se identifican los usuarios en todas las subredes excepto cuando se emplea el sondeo WMI en los sistemas de clientes con direcciones IPv4 públicas. (Las direcciones IPv4 públicas son aquellas que están fuera del alcance de RFC 1918 y RFC 3927).

Para habilitar el sondeo WMI para las direcciones IPv4 públicas, debe añadir sus subredes a la lista y establecer su opción de **Discovery (Descubrimiento)** a incluir con **Include (Incluir)**. Si realiza la Configuración del cortafuegos para redistribuir información de asignación de usuarios a otros cortafuegos, los límites de descubrimiento que especifique en la lista se aplicarán a la información redistribuida.

Utilice las listas de inclusión y exclusión para definir las subredes en las cuales el cortafuegos realiza la asignación de usuarios.

Puede llevar a cabo las siguientes tareas en la lista Incluir/excluir redes:

Tarea	Description (Descripción)
Añadir	Para limitar el descubrimiento en una subred específica, haga clic en **Add (Añadir)** para añadir un perfil de subred y complete los siguientes campos. • **Name (Nombre)**: introduzca un nombre para identificar la subred. • **Enabled (Habilitado)**: seleccione esta opción para habilitar la inclusión o exclusión de la subred para la monitorización del servidor.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	• **Discovery (Descubrimiento)**: seleccione si el agente User-ID will **Include (Incluirá)** o **exclude (excluirá)** a subred. • **Network Address (Nueva dirección)**: ingrese el intervalo de dirección IP de la subred. El agente de ID de usuario aplica una exclusión implícita de todas las reglas a la lista. Por ejemplo, si agrega una subred 10.0.0.0/8 con la opción **Include (Incluir)**, el agente User-ID excluye todas las demás subredes, pero no las añade a la lista. Añada entradas con la opción **Exclude (Excluir)** únicamente si desea que el agente de ID de usuario excluya un subconjunto de las subredes que ha incluido explícitamente. Por ejemplo, si añade 10.0.0.0/8 con la opción **Include (Incluir)** y añade 10.2.50.0/22 a la opción **Exclude (Excluir)**, el agente de ID de usuario realizará el descubrimiento de 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 en **Exclude (Excluir)** sin añadir ningún perfil en **Include (Incluir)**, el agente User-ID excluye todas las subredes, no solo las que ha añadido.
delete	Para eliminar una subred de la lista, selecciónela y haga clic en **Delete (Eliminar)**. **Consejo**: Para eliminar una subred desde la lista de Incluir/excluir redes sin borrar su configuración, edite el perfil de subred y borre **Enabled (Habilitado)**.
Red de inclusión/ exclusión personalizada	Por defecto, el agente User-ID evalúa las subredes en el orden en el que las añade, desde la primera la última. Para cambiar el orden de evaluación, haga clic en **Custom Include/Exclude Network Sequence (Secuencia de red de inclusión exclusión personalizada)**. Puede hacer clic en **Add (Añadir)**, **Delete (Eliminar)**, **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para añadir, eliminar, mover hacia arriba o mover hacia abajo las subredes para crear un orden de evaluación personalizado.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Identificación de usuarios > Seguridad de conexión

Edite ( ) la configuración de seguridad de conexión de User-ID para seleccionar el perfil de certificado utilizado por el cortafuegos para validar el certificado presentado por agentes de User-ID de Windows. El cortafuegos utiliza el perfil de certificado seleccionado para verificar la identidad del agente de User-ID a través de la validación del certificado del servidor presentado por el agente.

Tarea	Description (Descripción)
Perfil de certificado de User-ID	En el menú desplegable, seleccione el perfil de certificado que se utilizará al autenticar los agentes de User-ID de Windows o seleccione Nuevo perfil de certificado para crear un nuevo perfil de certificado. Seleccione **None (Ninguna)** para eliminar el perfil de certificado y utilizar la autenticación predeterminada en su lugar. Para exigir la validación del certificado del servidor con el servidor de Windows cuando Configuración de acceso a servidores supervisados utiliza Kerberos para la autenticación de servidor, asegúrese de configurar NTP en Configuración de servicios globales y seleccione la CA raíz como el perfil de certificado.
Eliminar todo (Sólo configuración de plantilla)	Elimina el perfil de certificado asociado a la configuración de seguridad de conexión de User-ID para la plantilla seleccionada.

© 2020 Palo Alto Networks, Inc.

Device > User Identification > User-ID Agents

Para asignar nombres de usuario a direcciones IP, los agentes de User-ID supervisan diversas fuentes, como servidores de directorios. Los agentes envían las asignaciones de usuario a cortafuegos, recopiladores de logs o Panorama y cada uno de estos dispositivos puede servir como *Puntos de redistribución* que reenvían las asignaciones a otros cortafuegos, recopiladores de logs o Panorama. Para un cortafuegos (**Device (Dispositivo)** > **User Identification (Identificación del usuario)** > **User-ID Agents (Agentes de User-ID)**) o Panorama (**Panorama** > **User Identification (Identificación del usuario)**) para recopilar las asignaciones de usuario, debe configurar sus conexiones a los agentes de User-ID o puntos de redistribución.

Para configurar los recopiladores de logs dedicados para conectarse a agentes de User-ID o puntos de redistribución, defina Configuración del agente de User-ID. No puede configurar los recopiladores de logs locales para conectarse a agentes de User-ID o puntos de redistribución.

Aunque puede configurar un recopilador de logs o Panorama para redistribuir las asignaciones de usuarios, estos dispositivos no pueden asignar direcciones IP a nombres de usuario. Sólo los agentes de User-ID basados en Windows y los agentes integrados de User-ID de PAN-OS pueden realizar la asignación de usuarios.

El procedimiento completo para configurar la asignación de usuarios requiere tareas adicionales además de configurar las conexiones con los agentes de User-ID.

- Configuración de acceso a agentes User-ID
- Gestión de acceso a agentes User-ID

Configuración de acceso a agentes User-ID

Cada cortafuegos y servidor de gestión Panorama pueden conectarse a un máximo de 100 agentes de User-ID o puntos de redistribución de User-ID (o una combinación de ambos). Para añadir una conexión, haga clic en **Add (Añadir)** y complete los siguientes campos.

Configuración del User-ID de usuarios	Description (Descripción)
Nombre	Introduzca un nombre descriptivo (hasta 31 caracteres) para el agente User-ID o el punto de redistribución. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. *Para un cortafuegos o sistema virtual que actúa como punto de redistribución, este campo no tiene que coincidir con el campo Nombre del recopilador.*
Añadir un agente que utiliza (Solo cortafuegos)	Seleccione cómo el cortafuegos identifica al agente User-ID o el punto de redistribución: • **Serial Number (Número de serie)**: Seleccione esta opción para un servidor de gestión Panorama que redistribuya las asignaciones de User-ID. • **Host and Port (Host y puerto)**: Seleccione esta opción para los agentes User-ID basados en Windows o para cortafuegos, sistemas virtuales y recopiladores de logs que redistribuyan las asignaciones de User-ID.

© 2020 Palo Alto Networks, Inc.

Configuración del User-ID de usuarios	Description (Descripción)
Serial Number (Solo cortafuegos)	Seleccione el servidor de gestión Panorama que redistribuye las asignaciones de usuario al cortafuegos. Para implementaciones de alta disponibilidad (HA), puede seleccionar Panorama activo (**panorama**) o Panorama pasivo (**Panorama2**). *No es necesario especificar el host, el puerto u otra información de conexión porque los ha definido durante la configuración inicial del cortafuegos.*
Host	• **Agentes User-ID basados en Windows**: Introduzca la dirección IP del host de Windows en el que está instalado el agente User-ID. • **Cortafuegos**Agente integrado de User-ID de PAN-OS**)**: Introduzca la dirección IP de la interfaz MGT o la ruta de servicio que el cortafuegos utiliza para enviar asignaciones de usuario. Para la interfaz MGT, puede introducir un nombre de host en lugar de la dirección IP. • **Recopiladores de logs que redistribuyen las asignaciones de usuarios**: introduzca el nombre de host o la dirección IP de la interfaz que el recopilador de logs utiliza para enviar asignaciones de usuario.
Puerto	Introduzca el número de puerto en el que el agente de User-ID escucha solicitudes de User-ID. El valor predeterminado es 5007, pero puede especificar cualquier puerto disponible y diferentes agentes de User-ID pueden utilizar puertos diferentes. *El puerto predeterminado para algunas versiones anteriores del agente de User-ID es 2010.*
Nombre del recopilador Clave precompartida del recopilador / Confirmar clave precompartida del recopilador	Introducir el **Collector Name (Nombre del recopilador)** y la **Pre-Shared Key (Clave precompartida)** que identifican al cortafuegos o sistema virtual como agente de User-ID. Introduzca los mismos valores que cuando configuró el cortafuegos o sistema virtual para redistribuir las asignaciones de usuario (consulte Redistribución). *El recopilador al que se refieren estos campos es el agente de User-ID, no un recopilador de logs y los campos son configurables solo cuando el agente es un cortafuegos o un sistema virtual.*
Utilizar como Proxy LDAP (Solo cortafuegos)	Seleccione esta opción para utilizar este agente de User-ID como proxy para supervisar el servidor de directorio para asignar nombres de usuario a grupos. Para utilizar esta opción, debe configurar la asignación de grupo en el cortafuegos (Device > User Identification > Group Mapping Settings). El cortafuegos envía esa configuración al agente de User-ID para habilitarla para asignar nombres de usuario a grupos. Esta opción es útil en implementaciones en donde el cortafuegos no puede directamente acceder al servidor del directorio. También es útil en implementaciones que se benefician de reducir el número de consultas que el servidor de directorio debe procesar; varios cortafuegos pueden recibir la información de asignación de grupo desde el caché en un único agente User-ID en lugar de requerir que cada cortafuegos consulte al servidor directamente.

© 2020 Palo Alto Networks, Inc.

Configuración del User-ID de usuarios	Description (Descripción)
Utilizar para autenticación NTLM (Solo cortafuegos)	Seleccione esta opción para utilizar este agente de User-ID como proxy para realizar la autenticación de NT LAN Manager (NTLM) cuando la solicitud web de un cliente coincida con una regla de política de autenticación. El agente de User-ID supervisa el controlador de dominio para obtener información de asignación de usuarios y reenvía la información al cortafuegos. Para usar esta opción, también debe habilitar la Autenticación NTLM en el agente de User-ID. Esta opción es útil en implementaciones en donde el cortafuegos no puede directamente acceder al controlador del dominio para realizar la autenticación NTLM. También es útil en implementaciones que se benefician de reducir el número de consultas de autenticación que el controlador de dominio debe procesar; varios cortafuegos pueden recibir la información de asignación de grupo desde el caché en un único agente de User-ID en lugar de solicitar que cada cortafuegos consulte al controlador de dominio directamente. *Configure reglas de autenticación para usar Inicio de sesión único de Kerberos en lugar de autenticación NTLM. Kerberos es un método de autenticación más potente y robusto que NTLM y no requiere que el cortafuegos tenga una cuenta administrativa para unirse al dominio. Para obtener información detallada sobre la configuración de los métodos de autenticación para las reglas de autenticación, consulte Objects > Authentication.*
Habilitado	Seleccione esta opción para permitir que el cortafuegos o Panorama se comuniquen con el agente de User-ID o punto de redistribución.
Informe HIP	Seleccione esta opción para habilitar este cortafuegos para que reciba informes HIP de otros cortafuegos que estén configurados como agentes User-ID (incluidas las puertas de enlace de GlobalProtect, los recopiladores de logs distribuidos [Distributed Log Collectors, DLC], cortafuegos y Panorama). Así el cortafuegos podrá utilizar la información de los informes HIP para la aplicación de políticas basadas en HIP.

Gestión de acceso a agentes User-ID

Lleve a cabo las siguientes tareas para gestionar las conexiones del cortafuegos de los agentes de User-ID o los puntos de redistribución.

Tarea	Description (Descripción)
Mostrar información/ Actualizar conectados	Seleccione **Device (Dispositivo)** > **User Identification (Identificación de usuarios)** > **User-ID Agents (Agentes de User-ID)** o **Panorama** > **User Identification (Identificación de usuarios)** para conocer si el cortafuegos o Panorama están conectados a cada agente de User-ID o punto de redistribución. La columna Connected (Conectado) indica con un icono verde una conexión correcta, con un icono amarillo una conexión deshabilitada y con un icono rojo una conexión fallida. Si piensa que el estado de conexión puede haber cambiado desde la primera vez que lo vio, haga clic en **Refresh Connected (Actualizar conectados)** para actualizar la visualización del estado. En el caso del resto de campos que se muestran, consulte Configuración de acceso a agentes de User-ID.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Añadir	Pulse **Add (Añadir)** y configure el acceso a los agentes de User-ID.
delete	Para borrar la configuración que permite al cortafuegos conectarse a un agente de User-ID o a un punto de redistribución, haga clic en **Delete (Eliminar)** para eliminar el agente o el punto. *Para deshabilitar el acceso a un agente de User-ID o un punto de redistribución sin eliminar su configuración, edítelo y desmarque la opción Enabled (Habilitado).*
Secuencia de agente personalizada	Si habilita agentes de User-ID para llevar a cabo la autenticación de NT LAN Manager (NTLM) en nombre del cortafuegos, entonces este se comunica de forma predeterminada con los agentes para añadirlos por orden descendente (para conocer cómo, consulte el campo **Use for NTLM Authentication [Utilizar para autenticación NTLM]** en Configuración de acceso a agentes User-ID). Para cambiar el orden en que el cortafuegos se comunica con los agentes, haga clic en **Custom Agent Sequence (Secuencia de agente personalizada)**, añada cada agente con **Add (Añadir)**, use **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)** para reordenar a los agentes y haga clic en **OK (Aceptar)**.
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de configuración de agente de User-ID como **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla para elementos como las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Identificación de usuarios > Agentes de servidor de terminal

En un sistema que admite varios usuarios que comparten la misma dirección IP, un agente de servidor de terminal (TS) identifica a los usuarios individuales asignándoles rangos de puertos a cada uno. El agente TS informa a cada cortafuegos conectado sobre del rango de puerto asignado de modo que los cortafuegos puedan aplicar políticas basadas en usuarios y grupos de usuarios.

Todos los modelos de cortafuegos pueden recopilar información de asignaciones de nombre de usuario a puerto de hasta 5.000 sistemas multiusuario. El número de agentes TS desde los que un cortafuegos puede recopilar la información de asignación varía según el modelo de cortafuegos.

Debe instalar y configurar los agentes de TS antes de configurar el acceso a ellos. El procedimiento completo para configurar la asignación de usuarios para usuarios de servidores de terminal requiere tareas adicionales además de configurar las conexiones con los agentes TS.

Puede realizar las siguientes tareas para gestionar el acceso a los agentes de TS.

Tarea	Description (Descripción)
Mostrar información/ Actualizar conectados	En la página **Agentes de servidor de terminal**, la columna Connected muestra el estado de las conexiones desde el cortafuegos a los agentes TS. Un icono verde indica una conexión satisfactoria, un icono amarillo indica una conexión desactivada y un icono rojo indica una conexión fallida. Si piensa que el estado de conexión podría haber cambiado desde que abrió la página, haga clic en **Refresh Connected (Actualizar conectados)** para actualizar la visualización del estado.
Añadir	Para configurar el acceso a un agente TS, haga clic en **Add (Añadir)** agente y configure los siguientes campos: • **Name (Nombre)**: introduzca un nombre para identificar el agente de TS (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. • **Host**: introduzca la dirección IP estática o el nombre de host del servidor del terminal en el que está instalado el agente de TS. • **Port (Puerto)**: introduzca el número de puerto (el predeterminado es 5009) que el servicio del agente de TS usa para comunicarse con el cortafuegos. • **Alternative IP Addresses (Direcciones IP alternativas)**: si el servidor de terminal donde está instalado el agente TS tiene varias direcciones IP que pueden aparecer como la dirección IP de origen para el tráfico saliente, haga clic en **Add (Añadir)** e introduzca hasta ocho direcciones IP o nombres de host adicionales. • **Enabled (Habilitado)**: seleccione esta opción para permitir que el cortafuegos se comunique con este agente TS.
delete	Para eliminar la configuración que habilita el acceso al agente TS, seleccione el agente y haga clic en **Delete (Eliminar)**.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	Para deshabilitar el acceso a un agente TS sin eliminar su configuración, edítelo y desactive la opción Enabled (Habilitado).
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de configuración del dispositivo como **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla para elementos como las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.

© 2020 Palo Alto Networks, Inc.

Device (Dispositivo) > User Identification (Identificación del usuario) > Pestaña Group Mapping Settings (Ajustes de asignación de grupos)

- **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Configuración de asignación de grupo)**

Para definir las políticas e informes de seguridad basándose en usuarios o grupos, el cortafuegos debe recuperar la lista de grupos y la lista de miembros correspondiente que se mantienen en su servidor de directorio. El cortafuegos admite una variedad de servidores de directorio LDAP, incluidos Microsoft Active Directory (AD), Novell eDirectory y Sun ONE Directory Server.

El número de grupos de usuarios distintos que cada cortafuegos o Panorama puede hacer referencia en todas las políticas varía según el modelo. No obstante, independientemente del modelo, debe configurar un perfil de servidor LDAP (Device [Dispositivo] > Server Profiles [Perfiles de servidor] > LDAP) para poder crear una configuración de asignación de grupos.

El procedimiento completo para asignar nombres de usuario a grupos requiere tareas adicionales además de crear configuraciones de asignaciones de grupo.

Haga clic en **Add (Añadir)** y configure los campos siguientes según fuera necesario para crear una configuración de asignación de grupos. Para eliminar una configuración de asignación de grupo, selecciónela y haga clic en **Delete (Eliminar)**. Si desea deshabilitar una configuración de asignación de grupo sin eliminarla, edite la configuración y borre la opción **Enabled (Habilitado)**.

Configuración de asignación de grupo: Perfil de servidor	Configurado en	Description (Descripción)
Nombre	**Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Configuración de asignación de grupo)**	Introduzca un nombre para identificar la configuración de asignación de grupo (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Perfil de servidor	**Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Configuración de asignación de grupo)** > **Server Profile (Perfiles de servidor)**	Seleccione el perfil de servidor LDAP que se debe utilizar para la asignación de grupos en este cortafuegos.
Intervalo de actualización		Especifique el intervalo en segundos tras el cual el cortafuegos iniciará una conexión con el servidor de directorios LDAP para obtener actualizaciones realizadas a los grupos que se utilizan en las políticas de cortafuegos (el intervalo de 60-86.400).

© 2020 Palo Alto Networks, Inc.

Configuración de asignación de grupo: Perfil de servidor	Configurado en	Description (Descripción)
Dominio de usuario		De manera predeterminada, el campo **User Domain (Dominio de usuario)** está en blanco: el cortafuegos detecta automáticamente los nombres de dominio para los servidores de Active Directory. Si introduce un valor, este sobrescribirá cualquier nombre de dominio que el cortafuegos recupera en el origen LDAP. Su entrada debe ser el nombre NetBIOS. *Este campo solo afecta a los nombres de usuarios y los nombres de grupo recuperados desde el origen LDAP. Para anular el dominio asociado con un nombre de usuario para la autenticación del usuario, configure el User Domain (Dominio de usuario) y el Username Modifier (Modificador de nombre de usuario) para el perfil de autenticación que asigna a ese usuario (consulte Device > Authentication Profile).*
Group Objects (Objetos de grupo)		• **Search Filter (Filtro de búsqueda)**: ingrese una consulta LDAP especifique qué grupos se recuperan y siguen. • **Object Class (Clase de objeto)**: ingrese una definición de grupo. El valor predeterminado es objectClass=group, lo que especifica que el sistema recupera todos los objetos en el directorio que coinciden con el filtro de grupo **Search Filter (Filtro de búsqueda)** y cuentan con objectClass=group.
Objetos de usuario		• **Search Filter (Filtro de búsqueda)**: ingrese una consulta LDAP especifique qué usuarios se recuperan y siguen. • **Object Class (Clase de objeto)**: ingrese una definición de objeto de usuario. Por ejemplo, en Active Directory, el objectClass es *usuario*.
Habilitado		Seleccione esta opción para habilitar el perfil de servidor para la asignación de grupo.

© 2020 Palo Alto Networks, Inc.

Configuración de asignación de grupo: Perfil de servidor	Configurado en	Description (Descripción)
Recuperar lista de dispositivos gestionados		Para las implementaciones de GlobalProtect, seleccione esta opción para permitir que el cortafuegos recupere los números de serie de un servidor de directorio (como Active Directory). Esto permite que GlobalProtect identifique el estado de los endpoint que se conecta y aplique las políticas de seguridad basadas en HIP, en función de la presencia del número de serie del endpoint.
User Attributes (Atributos de usuario)	**Device (Dispositivo) > User Identification (Identificación de usuario) > Group Mapping Settings (Configuración de asignación de grupos) > User and Group Attributes (Atributos de usuario y grupo)**	Especifique los atributos del directorio para identificar a los usuarios: • **Primary Username (Nombre de usuario principal)**: especifique el atributo que el origen de User-ID proporciona para el nombre de usuario (por ejemplo, **`userPrincipalName`** o **`sAMAccountName`**) *El nombre de usuario principal es la manera en que el cortafuegos identifica al usuario en los logs, informes y configuraciones de política, incluso si el cortafuegos recibe otros formatos de los orígenes de User-ID. Si no especifica un formato, el cortafuegos utiliza el formato `sAMAccountName` de manera predeterminada para Active Directory y el formato `uid` para Novell eDirectory y Sun ONE Directory Server.* • **E-Mail (Correo electrónico)**: especifique el atributo que el origen de User-ID proporciona para la dirección de correo electrónico. El valor predeterminado es **`mail`** (correo electrónico). • **Alternate Username 1-3 (Nombre de usuario alternativo 1-3)**: especifique hasta tres atributos adicionales que se correspondan con los formatos que los orígenes de User-ID pueden enviar. *Si configura un servidor de Active Directory, el nombre de usuario alternativo 1 es*

© 2020 Palo Alto Networks, Inc.

Configuración de asignación de grupo: Perfil de servidor	Configurado en	Description (Descripción)
		`userPrincipalName` *de forma predeterminada.*
Group Attributes (Atributos de grupo)		Especifique los atributos que los orígenes de User-ID utilizan para identificar a los grupos: • **Group Name (Nombre de grupo)**: especifique el atributo que el origen de User-ID utiliza para el atributo del nombre de grupo. El valor predeterminado para Active Directory es `name` y el valor predeterminado para Novell eDirectory o Sun ONE Directory Server es `cn`. • **Group Member (Miembro de grupo)**: especifique el atributo que el origen de User-ID utiliza para el atributo del nombre de grupo. El valor predeterminado es `member` (miembro). • **E-Mail (Correo electrónico)**: especifique el atributo que el origen de User-ID utiliza para la dirección de correo electrónico. El valor predeterminado es `mail` (correo electrónico).
Grupos disponibles Grupos incluidos	**Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Configuración de asignación de grupo)** > **Group Include List (Lista de inclusión de grupos)**	Use estos campos para limitar el número de grupos que el cortafuegos muestra cuando crea una regla de seguridad. Busque en el árbol de LDAP los grupos que desea usar en las reglas. Para incluir un grupo, seleccione y añada (⊞) en la lista de Grupos disponibles. Para eliminar un grupo de la lista, seleccione y elimine (⊟) de la lista de Grupos incluidos. El máximo combinado para las listas **Included groups (Grupos incluidos)** y **Custom Group (Grupo personalizado)** es de 640 entradas para cada configuración de asignación de grupo. *Incluya solo los grupos que necesite, de manera que el cortafuegos recupere las asignaciones de grupo de usuarios únicamente para los grupos necesarios y no para todo el árbol del directorio LDAP.*
Nombre Filtro LDAP	**Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **Group Mapping Settings (Ajustes de asignación**	Cree los grupos personalizados basados en los filtros LDAP de modo que puede basar las políticas de cortafuegos en atributos de usuario

© 2020 Palo Alto Networks, Inc.

Configuración de asignación de grupo: Perfil de servidor	Configurado en	Description (Descripción)
	de grupo) > **Custom Group (Grupo personalizado)**	que no coinciden con los grupos de usuarios existentes en un directorio LDAP. El servicio de ID de usuario asigna todos los usuarios de directorio LDAP que aplica el filtro al grupo personalizado. Si crea un grupo personalizado con el mismo nombre distinguido (Distinguished Name, DN) que un nombre de dominio de grupo Active Directory existente, el cortafuegos usa el grupo personalizado en todas las referencias a ese nombre (por ejemplo, en políticas y logs). Para crear un grupo personalizado, haga clic en **Add (Añadir)** y configure los siguientes campos: • **Name (Nombre)**: introduzca un nombre de grupo personalizado que sea única en la configuración de asignación de grupo para el cortafuegos o sistema virtual actual. • **LDAP Filter (Filtro LDAP)**: ingrese un filtro de hasta 2048 caracteres. *Utilice únicamente atributos indexados en el filtro para agilizar las búsquedas LDAP y minimizar el impacto de rendimiento en el servidor de directorio LDAP; el cortafuegos no valida los filtros LDAP.* El máximo combinado para las listas **Included Groups (Grupos incluidos)** y **Custom Group (Grupo personalizado)** es de 640 entradas. Para eliminar un grupo personalizado, selecciónelo y haga clic en **Delete (Eliminar)**. Para realizar una copia de un grupo personalizado, selecciónelo, haga clic en **Clone (Duplicar)** y edite los campos según corresponda. *Después de agregar o duplicar un grupo personalizado, debe Commit (Confirmar) sus cambios antes de que su nuevo grupo personalizado esté disponible en directivas y objetos.*

© 2020 Palo Alto Networks, Inc.

Device > User Identification > Captive Portal Settings

Editar) el portal cautivo configuración para configurar el cortafuegos para autenticar a los usuarios cuyo tráfico coincide con una regla de política de autenticación.

Si Captive Portal utiliza un perfil de servicio SSL/TLS (Device [Dispositivo] > Certificate Management [Gestión de certificados] > SSL/TLS Service Profile [Perfil de servicio SSL/TLS]), un perfil de autenticación (Device [Dispositivo] > Authentication Profile [Perfil de autenticación]) o un perfil de certificado (Device [Dispositivo] > Certificate Management [Gestión de certificados] > Certificate Profile [Perfil de certificado]), configure el perfil antes de comenzar. El procedimiento completo para configurar Captive Portal requiere tareas adicionales además de configurar estos perfiles.

Debes Enable Captive Portal (Habilitar el portal cautivo) para aplicar la política de autenticación (consulte Policies > Authentication).

Campo	Description (Descripción)
Habilitar portal cautivo	Seleccione esta opción para habilitar el Portal cautivo
Temporizador de inactividad (minutos)	Introduzca el tiempo de vida (TTL) del usuario en minutos para una sesión de portal cautivo (el intervalo es 1-1.440; el predeterminado es 15). Este temporizador se reinicia cada vez que hay actividad de un usuario de Captive Portal. Si el tiempo de inactividad de un usuario supera el valor en el **Idle Timer (Temporizador de inactividad)**, PAN-OS quita la asignación de usuarios del portal cautivo y el usuario debe iniciar sesión de nuevo.
Temporizador (min)	Este es el TTL máximo en minutos, que es el tiempo máximo que cualquier sesión del portal cautivo puede permanecer asignada (el intervalo es 1-1.440; el predeterminado es 60) Después de de que transcurra el tiempo, PAN-OS elimina la asignación y los usuarios deben volver a autenticarse aunque la sesión esté activa. Este temporizador evita las asignaciones obsoletas y cancela el valor del **Idle Timer (Temporizador de inactividad)**. *Se recomienda que establezca el valor de Timer (Temporizador) más alto que el de Idle Timer (Temporizador de inactividad).*
Perfil de servicio SSL/TLS	Para especificar un certificado y los protocolos permitidos para asegurar las solicitudes de redirección, seleccione un perfil de servicio SSL/TLS (consulte Device > Certificate Management > SSL/TLS Service Profile). Si selecciona **None (Ninguno)**, el cortafuegos utiliza el certificado local predeterminado para las conexiones SSL/TLS. *En el perfil de servicio SSL/TLS, configure Min Version (Versión mín.) en TLSv1.2 y configure Max Version (Versión máx.) en Max (Máx.) para proporcionar la máxima seguridad contra las vulnerabilidades del protocolo SSL/TLS. La configuración de Max*

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Version (Versión máx.) en Max (Máximo) garantiza que, a medida que haya protocolos más seguros disponibles, el cortafuegos use siempre la versión más reciente. Para redirigir a los usuarios de forma transparente sin mostrar los errores de certificado, asigne un perfil asociado con un certificado que haga coincidir la dirección IP en la interfaz a la que desea redirigir las solicitudes web.
Perfil de autenticación	Puede seleccionar un perfil de autenticación (Device > Authentication Profile) para autenticar usuarios cuando su tráfico coincide con una regla de política de autenticación (Policies > Authentication). Sin embargo, el perfil de autenticación que seleccione en la configuración del portal cautivo solo se aplica a las reglas que hacen referencia a uno de los objetos de imposición de autenticación predeterminadosObjects > Authentication). Esto suele ser el caso justo después de una actualización a PAN-OS 8.0 porque todas las reglas de autenticación hacen referencia inicialmente a los objetos predeterminados. Para las reglas que hacen referencia a objetos de cumplimiento de autenticación personalizados, seleccione el perfil de autenticación al crear el objeto.
Puerto de red de GlobalProtect para solicitudes de autenticación entrantes (UDP)	Especifique el puerto que utiliza GlobalProtect™ para recibir las solicitudes de autenticación de entrada de las puertas de enlace de varios factores (multi-factor, MFA). (Intervalo: 1-65.536; predeterminado: 4.501). Para admitir la autenticación de múltiples factores, un endpoint de GlobalProtect debe recibir y confirmar las solicitudes UDP que se reciben desde la puerta de enlace de MFA. Cuando un endpoint de GlobalProtect recibe un mensaje UDP en el puerto de red especificado y el mensaje UDP proviene de un cortafuegos o puerta de enlace de confianza, GlobalProtect muestra el mensaje de autenticación (consulte Personalizar la aplicación de GlobalProtect).
Modo	Seleccione cómo captura el cortafuegos solicitudes web para la autenticación: • **Transparent (Transparente)**: el cortafuegos intercepta la solicitud web conforme a la regla de autenticación y representa a la URL de destino original, emitiendo un mensaje de HTTP 401 para solicitar la autenticación del usuario. 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, solo use este modo cuando sea absolutamente necesario, como en implementaciones de capa 2 o cable virtual (Virtual Wire). • **Redirect (Redireccionar)**: el cortafuegos intercepta las solicitudes web de acuerdo con la regla de autenticación y las redirecciona al Host de redireccionamiento. El cortafuegos utiliza una redirección HTTP 302 para pedir al usuario que se autentique. Se recomienda usar **Redirect (Redirigir)**, ya que ofrece una mejor experiencia de usuario final (no muestra certificados de error y permite las cookies de sesión que permiten optimizar la navegación, debido a que **Redirect [Redirigir]** no se reasigna cuando finaliza el tiempo de espera). Sin embargo, este requiere que habilite las páginas de respuesta en el perfil de gestión de interfaz asignado a la interfaz de capa 3 de entrada (para obtener más información, consulte Network > Network Profiles > Interface Mgmt e interfaz de capa 3 de PA-7000 Series). 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 vez que venza el tiempo de espera. Esto es de especial utilidad para

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	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. *El modo Redirect (Redireccionar) es necesario si el portal cautivo utiliza autenticación Kerberos SSO o NTLM porque el navegador proporciona credenciales solo a sitios de confianza. El modo Redirect (Redireccionar) también es necesario si el portal cautivo utiliza la autenticación de múltiples factores (MFA).*
Cookie de sesión (Solo modo de redireccionamiento)	• **Enable (Habilitar)**: seleccione esta opción para habilitar las cookies de sesión. • **Timeout (Tiempo de espera)**: si hace clic en **Enable (Habilitar)**, habilita las cookies de sesión, este temporizador especifica el número de minutos durante los que la cookie es válida (el intervalo es 30-10.080; el predeterminado es 1.440). *Configure un valor del tiempo de espera lo suficientemente bajo como para que no derive en entradas de asignación de usuario obsoletas en las cookies, pero lo suficientemente extenso como para permitir una buena experiencia del usuario al no indicar a los usuarios que se registren varias veces durante una sesión. Comience con un valor menor o igual que 480 minutos (8 horas) y vaya ajustándolo según fuera necesario.* • **Roaming (Movilidad)**: seleccione esta opción para conservar la cookie si la dirección IP cambia mientras la sesión está activa (como cuando el endpoint cambia de una red con cable a una red inalámbrica). El usuario debe volver a autenticarse solo si la cookie agota el tiempo de espera o el usuario cierra el explorador.
Redirigir host (Solo modo de redireccionamiento)	Especifique el nombre de host de intranet que resuelve a la dirección IP de la interfaz de capa3 a la que el cortafuegos redirige las solicitudes web. *Si los usuarios se autentican mediante el inicio de sesión único (SSO) de Kerberos, Redirect Host (Host de redireccionamiento) debe ser el mismo que el nombre de host especificado en el Kerberos keytab.*
Perfil del certificado	Puede seleccionar un perfil de certificado (Device > Certificate Management > Certificate Profile) para autenticar usuarios cuando su tráfico coincide con cualquier regla de política de autenticación (Policies > Authentication). Para este tipo de autenticación, Captive Portal solicita al explorador de endpoint del usuario que presente un certificado de cliente. Por lo tanto, debe implementar certificados de cliente en cada sistema de usuario. Además, en el cortafuegos, debe instalar el certificado de autoridad de certificación (CA) que emitió los certificados de cliente y asignar el certificado de CA al perfil de certificado. Este es el único método de autenticación que habilita una autenticación **Transparent (Transparente)** para endpoints de Mac OS y Linux.
Autenticación NTLM	Cuando el portal cautivo se configura para la autenticación NTLM, el cortafuegos utiliza un mecanismo de respuesta por desafío cifrado para obtener de forma transparente las credenciales de usuario del explorador sin preguntar al usuario.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Para invocar la autenticación NTLM, las reglas de política de autenticación deben especificar un objeto de **Authentication Enforcement (Aplicación de la autenticación)** con el **Authentication Method (Método de autenticación)** establecido en **browser-challenge (desafío del navegador)** o **default-browser-challenge (desafío del navegador predeterminado)** (Objects > Authentication). Si el objeto especifica una **Authentication Profile (Perfil de autenticación)** con el inicio de sesión único (SSO) de Kerberos habilitado, el cortafuegos primero intenta la autenticación Kerberos antes de volver a NTLM. Si el explorador no puede realizar la autenticación NTLM o esta falla, el cortafuegos retrocederá a **web-form** o **default-web-form** como **Authentication Method (Método de identificación)** De manera predeterminada, Internet Explorer admite NTLM. Puede configurar Firefox y Chrome para utilizarlo también, pero no puede utilizar NTLM para autenticar a endpoints que no sean de Windows. *Seleccione la autenticación transparente de Kerberos SSO sobre la autenticación NTLM al configurar el Portal cautivo. Kerberos es un método de autenticación más potente y robusto que NTLM y no requiere que el cortafuegos tenga una cuenta administrativa para unirse al dominio.* *Estas opciones solo se aplican a los agentes User-ID con Windows. Al utilizar el agente User-ID integrado en PAN-OS, el cortafuegos debe poder resolver correctamente el nombre de DNS de su controlador de dominio para que se una al dominio. A continuación, puede habilitar la Autenticación de NTLM en la configuración de agente de User-ID integrado en PAN-OS y proporcionar las credenciales para que el cortafuegos se una al dominio. NTLM está disponible solo para Windows Server versión 2003 y versiones anteriores.* Para configurar NTLM para su uso con agentes User-ID basados en Windows, defina lo siguiente: • **Attempts (Intentos)**: el número de intentos antes de que falle la autenticación NTLM (el intervalo es 1-60; el valor predeterminado es 1). • **Timeout (Tiempo de espera)**: el número de segundos antes de que se agote el tiempo para la autenticación NTLM (el intervalo es 1-60; el valor predeterminado es 2). • **Reversion Time (Tiempo de revisión)**: el número de segundos después de los cuales el cortafuegos intentará comunicarse con el primer agente User-ID detallado en la página **Device (Dispositivo)** > **User Identification (Identificación de usuario)** > **User-ID Agents (Agentes de User-ID)** después de que el agente no esté disponible (el intervalo es 60-3.600; el valor predeterminado es 300).

© 2020 Palo Alto Networks, Inc.

GlobalProtect

GlobalProtect™ ofrece una completa infraestructura para la gestión de su fuerza de trabajo itinerante para garantizar a todos sus usuarios un acceso seguro, independientemente de los dispositivos que usen o de donde se encuentren. Las siguientes páginas de interfaz web de cortafuegos le permiten configurar y gestionar componentes de GlobalProtect:

> Red > GlobalProtect > Portales
> Red > GlobalProtect > Puertas de enlace
> Red > GlobalProtect > MDM
> Network > GlobalProtect > Device Block List
> Red> GlobalProtect> Aplicaciones sin cliente
> Red> GlobalProtect> Grupos de aplicaciones sin cliente
> Objetos > GlobalProtect > Objetos HIP
> Objetos > GlobalProtect > Perfiles HIP
> Dispositivo > Cliente de GlobalProtect

¿Busca más información?

Consulte la Guía del administrador de GlobalProtect para obtener más información sobre GlobalProtect, incluyendo detalles sobre cómo configurar la infraestructura de GlobalProtect, cómo utilizar la información del host para aplicar la política e instrucciones paso a paso para configurar implementaciones comunes de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Red > GlobalProtect > Portales

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** para configurar y gestionar un portal de GlobalProtect™. El portal proporciona las funciones de gestión para la infraestructura de GlobalProtect. Todos los endpoints que participan en la red de GlobalProtect reciben su configuración desde el portal, incluso la información sobre las puertas de enlace disponibles y los certificados de cliente necesarios para conectarse a las puertas de enlace. Además, el portal controla el comportamiento y la distribución del software de la aplicación de GlobalProtect para los endpoints con Mac OS y Windows. En los endpoints de Linux, debe obtener el software del sitio de asistencia; en el caso de los dispositivos móviles, la aplicación de GlobalProtect se distribuye a través de la App Store de Apple (para dispositivos iOS), Google Play (para dispositivos Android) y Microsoft Store (para Windows Phone y otros dispositivos de Windows UWP). En las Chromebooks, la aplicación GlobalProtect se distribuye a través de la consola de gestión de Chromebook o Google Play.

Para añadir una configuración de portal, haga clic en **Add (Añadir)** para abrir el cuadro de diálogo Portal de GlobalProtect.

¿Qué está buscando?	Consulte:
¿Qué configuración general debo configurar para el portal GlobalProtect?	Pestaña general de Portales de GlobalProtect
¿Cómo puedo asignar un perfil de autenticación a una configuración de portal?	Pestaña GlobalProtect Portals Authentication (Autenticación de portales de GlobalProtect)
¿Cómo puedo definir los datos que la aplicación de GlobalProtect recopila de los endpoints?	Pestaña Portal Data Collection (Recopilación de datos de portal) de los portales de GlobalProtect
¿Qué opciones de autenticación de cliente puedo configurar?	Pestaña Autenticación de agente de Portales de GlobalProtect
¿Cómo puedo asignar una configuración a un grupo específico de dispositivos en función de un sistema operativo, usuario o grupo de usuarios?	Pestaña Criterios de selección de configuración de agente de portales de GlobalProtect
¿Cómo puedo configurar los ajustes y la prioridad de las puertas de enlace internas?	Pestaña interna de agente de Portales de GlobalProtect
¿Cómo puedo configurar los ajustes y la prioridad de las puertas de enlace externas?	Pestaña externa de agente de Portales de GlobalProtect
¿Cómo puedo crear configuraciones de cliente diferentes para diferentes tipos de usuarios?	Pestaña GlobalProtect Portals Agent (Agente de portales de GlobalProtect)
¿Qué configuraciones puedo personalizar en la apariencia y	Pestaña de la aplicación de agente de Portales de GlobalProtect

© 2020 Palo Alto Networks, Inc.

¿Qué está buscando?	Consulte:
funcionamiento de la aplicación de GlobalProtect?	
¿Cómo puedo configurar las opciones de recopilación de datos HIP?	Pestaña Recopilación de datos HIP de agente de portales de GlobalProtect
¿Cómo puedo configurar el portal de GlobalProtect para permitir el acceso a las aplicaciones web sin necesidad de instalar una aplicación de GlobalProtect?	Pestaña VPN sin cliente de portales GlobalProtect
¿Cómo puedo ampliar la conectividad VPN a un cortafuegos que actúa como satélite?	Pestaña Satélite del portal de GlobalProtect
¿Busca más información?	Para obtener instrucciones detalladas sobre cómo configurar el portal, consulte Configurar un portal de GlobalProtect (en inglés) en la *guía del administrador de GlobalProtect*.

Pestaña general de Portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **General (General)**

Seleccione la pestaña **General** para definir los ajustes de red que la aplicación de GlobalProtect utiliza para conectarse al portal GlobalProtect. Opcionalmente, puede deshabilitar la página de inicio de sesión o especificar una página de inicio de sesión y de ayuda personalizadas para GlobalProtect. Para obtener información sobre cómo crear e importar páginas personalizadas, consulte la sección sobre Personalización de las páginas de inicio de sesión de portal, bienvenida y ayuda de portal en la Guía del administrador de GlobalProtect.

Configuración del portal de GlobalProtect	Description (Descripción)
Nombre	Escriba un nombre para el portal (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	En el caso de un cortafuegos que esté en modo de sistema virtual múltiple, **Location (Ubicación)** es el sistema virtual (virtual system, vsys) en el que el portal de GlobalProtect está disponible. Para un cortafuegos que no está en modo vsys múltiple, **Location (Ubicación)** no está disponible. Una vez guardado el portal, no puede cambiar **Location (Ubicación)**.
Configuración de red	
Interface (Interfaz)	Seleccione el nombre de la interfaz de cortafuegos que será la entrada de las comunicaciones de endpoints y cortafuegos remotos.

© 2020 Palo Alto Networks, Inc.

Configuración del portal de GlobalProtect	Description (Descripción)
	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. Consulte Prácticas recomendadas de seguridad del acceso administrativo *para obtener información detallada sobre cómo proteger el acceso a su red de gestión.*
Dirección IP	Especifique la dirección IP en la que se ejecutará el servicio web del portal GlobalProtect. Seleccione el **IP Address Type (Tipo de dirección IP)** y luego introduzca la **IP Address (Dirección IP)**. • El tipo de dirección IP puede ser **IPv4** (Sólo para el tráfico IPv4), **IPv6** (Sólo para tráfico IPv6), 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 IPv4 o 21DA:D3:0:2F3b para IPv6). • Si selecciona **IPv4 e IPv6**, introduzca el tipo de dirección IP apropiado para cada uno.
Apariencia	
Página de inicio de sesión de portal	(Opcional) Seleccione una página de inicio de sesión personalizada para el acceso de usuario al portal. Puede seleccionar la página **factory-default (predeterminada de fábrica)** o **Import (Importar)** para importar una página personalizada. El valor predeterminado es **None (Ninguno)**. Para evitar el acceso a esta página desde un navegador web, debe **Disable (Inhabilitar)** esta página.
Página de inicio del portal	(Opcional) Seleccione una página de inicio personalizada para el portal. Puede seleccionar la página **factory-default (predeterminada de fábrica)** o **Import (Importar)** para importar una página personalizada. El valor predeterminado es **None (Ninguno)**.
Página de ayuda de aplicación	(Opcional) Seleccione una página de ayuda personalizada para asistir al usuario con GlobalProtect. Puede seleccionar la página **factory-default (predeterminada de fábrica)** o **Import (Importar)** para importar una página personalizada. La página de ayuda predeterminada de fábrica se brinda con el software de la aplicación de GlobalProtect. Si selecciona una página de ayuda personalizada, el portal de GlobalProtect brinda la página de ayuda con la configuración del portal de GlobalProtect. Cuando conserva el valor predeterminado **None (Ninguno)**, la aplicación de GlobalProtect suprime la página y elimina la opción del menú.

Pestaña GlobalProtect Portals Authentication (Autenticación de portales de GlobalProtect)

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Authentication (Autentificación)**

© 2020 Palo Alto Networks, Inc.

Seleccione la pestaña **Authentication (Autenticación)** para configurar los diversos ajustes del portal de GlobalProtect™:

- Un perfil de servicio SSL/TLS que el portal y los servidores usan para la autenticación. El perfil de servicio es independiente de las demás configuraciones en la autenticación.
- Esquemas de autenticación únicos que están basados principalmente en el sistema operativo de los endpoints de usuario y de forma secundaria en un perfil de autenticación opcional.
- (Opcional) Un **Certificate Profile (Perfil de certificado)**, que permite a GlobalProtect utilizar un perfil de certificado específico para autenticar al usuario. El certificado del cliente debe coincidir con el perfil del certificado (si los certificados del cliente son parte del esquema de seguridad).

Configuración de autenticación en portales de GlobalProtect	Description (Descripción)
Autenticación de servidor	
Perfil de servicio SSL/TLS	Seleccione un perfil de servicio SSL/TLS existente. El perfil especifica un certificado y los protocolos permitidos para asegurar el tráfico en la interfaz de gestión. El campo Nombre común (Common Name, CN) y, si corresponde, el campo Nombre alternativo del asunto (Subject Alternative Name, SAN) del certificado asociado al perfil deben coincidir con la dirección IP o FQDN de la **Interface (Interfaz)** seleccionada en la pestaña **General**. *En las configuraciones VPN de GlobalProtect, utilice un perfil asociado a un certificado de una CA externa de confianza o un certificado generado por su CA empresarial interna.*
Autenticación de cliente	
Nombre	Introduzca un nombre para identificar la configuración de autenticación del cliente. (La configuración de autenticación de cliente es independiente del perfil de servicio SSL/TLS). Puede crear múltiples configuraciones de autenticación de cliente y diferenciarlas principalmente por sistema operativo y también por perfiles de autenticación (para el mismo SO). Por ejemplo, puede añadir configuraciones de autenticación de cliente para diferentes sistemas operativos y también tener configuraciones diferentes para el SO que estén diferenciadas por perfiles de autenticación únicos. (Debe ordenar estos perfiles manualmente desde el más específico al más general. Por ejemplo, todos los usuarios y cualquier SO es el más general). También puede crear configuraciones que GlobalProtect implementa a las aplicaciones en modo **pre-logon (anterior al inicio de sesión)** (antes de que el usuario haya iniciado sesión en el sistema) o que se aplican a cualquier usuario. (El pre-logon establece un túnel VPN a una puerta de enlace GlobalProtect antes de que el usuario inicie sesión en GlobalProtect).
SO	Para implementar el perfil de autenticación de cliente concreto para el sistema operativo (SO) en un endpoint, **añada** el SO (**Cualquiera**, **Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** o **WindowsUWP**). El SO es el diferenciador principal entre configuraciones. (Consulte el perfil de autenticación para comprender las diferenciaciones).

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación en portales de GlobalProtect	Description (Descripción)
	Las opciones adicionales de **Browser (Navegador)** y **Satellite (Satélite)** le permiten especificar el perfil de autenticación para usarlo en escenarios específicos. Seleccione **Browser (Navegador)** para especificar el perfil de autenticación a utilizar para autenticar un usuario que acceda al portal desde un navegador web con la intención de descargar la aplicación de GlobalProtect (Windows y Mac). Seleccione **Satellite (Satélite)** para especificar el perfil de autenticación a usar para autenticar el satélite (LSVPN).
Perfil de autenticación	Además de distinguir la configuración de autenticación de cliente en función del SO, puede diferenciar aún más especificando un perfil de autenticación. (Puede crear un nuevo perfil de autenticación en **New Authentication Profile (Nuevo perfil de autenticación)** o seleccionar uno existente). Para configurar múltiples opciones de autenticación para un SO, puede crear múltiples perfiles de autenticación de cliente. *Si configura un LSVPN en Gateways (Puertas de enlace), no puede guardar esa configuración salvo que seleccione un perfil de autenticación aquí. Además, si planea usar números de serie para autenticar satélites, el portal debe tener un perfil de autenticación disponible cuando no pueda localizar o validar el número de serie de un cortafuegos.* Consulte también Device > Authentication Profile.
Username Label (Etiqueta de nombre de usuario)	Especifique un nombre de usuario personalizado para el inicio de sesión en el portal de GlobalProtect. Por ejemplo, un **nombre de usuario (únicamente)** o una **dirección de correo electrónico (username@domain)**.
Password Label (Etiqueta de contraseña)	Especifique una etiqueta de contraseña personalizada para el inicio de sesión en el portal de GlobalProtect. Por ejemplo, una **contraseña (Turkish)** o un **código de contraseña** (para autenticación basada en token de dos factores).
Mensaje de autenticación	Para ayudar a los usuarios finales a conocer el tipo de credenciales que necesitan para iniciar sesión, ingrese un mensaje o conserve el mensaje predeterminado. La longitud máxima del mensaje es de 256 caracteres.
Permitir autenticación con credencial de usuario O certificado de cliente	Si selecciona **No**, los usuario deberán autenticarse en la puerta de enlace usando credenciales de usuario y certificados de cliente. Si selecciona **Yes (Sí)**, los usuario podrán autenticarse en la puerta de enlace usando credenciales de usuario o certificados de cliente.
Perfil del certificado	
Perfil del certificado	(Opcional) Seleccione el perfil de certificado que usa el portal en **Certificate Profile (Perfil de certificado)** para hacer coincidir aquellos certificados de cliente que provienen de los endpoints. Con un perfil de certificado, el portal autentica el usuario solo si el certificado del cliente coincide con este perfil. Si configura la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credencial de usuario O certificado de**

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación en portales de GlobalProtect	Description (Descripción)
	cliente) en **No**, debe seleccionar un **Certificate Profile (Perfil de certificado)**. Si configura la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credencial de usuario O certificado de cliente)** en **Yes (Sí)**, el **Certificate Profile (Perfil de certificado)** es optativo. El perfil del certificado es independiente del SO. Además, este perfil está activo incluso si habilita Cancelación de autenticación, lo cual cancela el perfil de autenticación para permitir la autenticación con cookies cifradas.

Pestaña Portal Data Collection (Recopilación de datos de portal) de los portales de GlobalProtect

Seleccione **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > **<portal-config>** > **Portal Data Collection (Recopilación de datos de protal)** para definir los datos que la aplicación de GlobalProtect recopila de los endpoints y envía en los datos de los criterios de selección de configuración, una vez que los usuarios inician sesión correctamente en el portal.

Configuración de recopilación de datos del portal de GlobalProtect	Description (Descripción)
Perfil del certificado	Seleccione el perfil de certificado que el portal de GlobalProtect utiliza para hacer coincidir con el certificado del equipo enviado por la aplicación de GlobalProtect.
Comprobaciones personalizadas	Defina información de host personalizada que desee que recopile la aplicación: • **Windows**: haga clic en **Add (Añadir)** para añadir una comprobación de una clave de registro determinada o un valor clave. • **Mac**: haga clic en **Add (Añadir)** para añadir una comprobación de una clave de plist determinada o un valor clave.

Pestaña GlobalProtect Portals Agent (Agente de portales de GlobalProtect)

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)**

Seleccione la pestaña **Agent (Agente)** para definir los ajuste de configuración del agente. El portal GlobalProtect implementa la configuración en el dispositivo después de que la conexión se establece por primera vez.

También puede especificar que el portal implemente automáticamente los certificados de entidad de certificación (CA) raíz de confianza y los certificados intermedios. Si los endpoints no confían en los certificados del servidor que usan las puertas de enlace de GlobalProtect y el gestor de seguridad móvil de

© 2020 Palo Alto Networks, Inc.

GlobalProtect, los endpoints necesitan estos certificados para establecer conexiones HTTPS en las puertas de enlace o el gestor de seguridad móvil. El portal envía los certificados que especifica aquí al cliente junto con la configuración de cliente.

Para añadir un certificado de CA raíz de confianza, seleccione **Add (Añadir)** un certificado existente o **Import (Importar)** uno nuevo. Para instalar (de manera transparente) los certificados CA raíz de confianza que se requieren para el cifrado de proxy de reenvío SSL en el almacén de certificados del cliente, seleccione **Install in Local Root Certificate Store (Instalar en el almacén local de certificados raíz)**.

Especifique el certificado de raíz de CA de confianza que la aplicación utiliza para verificar la identidad del portal y las puertas de enlace de GlobalProtect. Si el portal o la puerta de enlace presentan un certificado que no ha sido firmado o emitido por la misma autoridad del certificado que emitió la CA de raíz de confianza, la aplicación de GlobalProtect no puede establecer una conexión con el portal o la puerta de enlace.

Si tiene tipos de usuarios distintas que necesitan distintas configuraciones, puede crear una configuración de agente distinta para cada uno. El portal entonces utilizará el nombre de usuario/nombre de grupo o el sistema operativo del cliente para determinar qué configuración cliente implementar. Como con la evaluación de reglas de seguridad, el portal busca una coincidencia empezando por la parte superior de la lista. Cuando el portal encuentra una coincidencia, proporciona la configuración correspondiente para la aplicación. Por lo tanto, si tiene varias configuraciones de agente, es importante ordenarlas, para que las más específicas (configuraciones para usuarios o sistemas operativos concretos) estén por encima de configuraciones más genéricas. Utilice los botones **Move Up (Mover hacia arriba)** y **Move Down (Mover hacia abajo)** para volver a ordenar las configuraciones. Según sea necesario, seleccione **Add (Añadir)** una nueva configuración de agente. Para obtener información detallada sobre cómo configurar el portal y crear configuraciones de agente, consulte Portales del GlobalProtect en la Guía del administrador de GlobalProtect. Cuando hace clic en **Add (Añadir)** para añadir una nueva configuración de agente o modificar una ya existente, se abrirá el cuadro de diálogo **Configs** (Configuración) y mostrará cinco pestañas que se describen en las tablas siguientes:

- Pestaña Autenticación de agente de Portales de GlobalProtect
- Pestaña Criterios de selección de configuración de agente de portales de GlobalProtect
- Pestaña interna de agente de Portales de GlobalProtect
- Pestaña externa de agente de Portales de GlobalProtect
- Pestaña de la aplicación de agente de Portales de GlobalProtect
- Pestaña Recopilación de datos HIP de agente de portales de GlobalProtect

Pestaña Autenticación de agente de Portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **Authentication (Autentificación)**

Seleccione la pestaña **Authentication** para configurar los ajustes de autenticación que se aplican a la configuración del agente.

Ajustes de Configuración de autenticación de clientes del portal de GlobalProtect	Description (Descripción)
Pestaña Autenticación	
Nombre	Introduzca un nombre descriptivo para esta configuración para la autenticación del cliente.

© 2020 Palo Alto Networks, Inc.

Ajustes de Configuración de autenticación de clientes del portal de GlobalProtect	Description (Descripción)
Certificado de cliente	(Opcional) Seleccione el origen que distribuye el certificado del cliente a un endpoint, que entonces presenta el certificado a las puertas de enlace. Se requiere un certificado de cliente si usted configura la autenticación SSL mutua. Si SCEP está configurado para el pre-logon en la configuración del portal del cliente, el portal genera un certificado de la máquina que se guarda en el almacén de certificados del sistema para las conexiones y la autenticación de la puerta de enlace. Para usar un certificado que es **Local** para el cortafuegos en lugar de un certificado generado a partir de PKI a través de **SCEP**, seleccione un certificado que ya esté cargado en el cortafuegos. Si utiliza una CA interna para distribuir certificados a los endpoints, seleccione **None (Ninguno)** (predeterminado). Cuando selecciona **None (Ninguno)**, el portal no envía un certificado al endpoint.
Save User Credentials (Guardar credenciales de usuario)	Seleccione **Yes (Sí)** para guardar el nombre de usuario y la contraseña en la aplicación o seleccione **No** para forzar a los usuarios a proporcionar la contraseña (así sea de manera transparente a través del endpoint o de manera manual ingresando una) cada vez que se conectan. Seleccione **Save Username Only (Guardar solo nombre de usuario)** para guardar solo el nombre de usuario cada vez que un usuario se conecta. Seleccione **Solo con huella digital de usuario** para permitir el inicio de sesión biométrico. Cuando el inicio de sesión biométrico está habilitado en un endpoint, GlobalProtect usa las credenciales de usuario guardadas cuando un escaneo de huellas digitales coincide con una plantilla de huellas digitales fiable en el endpoint. *No guarde las credenciales del usuario, ya que facilita el acceso a recursos delicados e información confidencial por parte de usuarios no autorizados. Los usuario deben introducir manualmente sus credenciales cada vez que se conectan a GlobalProtect.*
Cancelación de autenticación	
Generar cookie para cancelación de autenticación	Seleccione esta opción para configurar que el portal genere cookies específicas de endpoint cifradas. El portal envía esta cookie al endpoint después de que el usuario primero se autentica con el portal.
Aceptar cookie para anulación de autenticación	Seleccione esta opción para establecer que el portal autentique los endpoints mediante una cookie cifrada válida.

© 2020 Palo Alto Networks, Inc.

Ajustes de Configuración de autenticación de clientes del portal de GlobalProtect	Description (Descripción)
	Cuando el endpoint presenta una cookie válida, el portal verifica que la cookie fue cifrada por el portal, descifra la cookie y luego autentica el usuario.
Vida útil de la cookie	Especifique las horas, los días o las semanas que la cookie será válida. El vencimiento normal es 24 horas. Los intervalos son 1–72 horas, 1–52 semanas o 1–365 días. Después de que una cookie vence, el usuario debe introducir las credenciales de inicio de sesión y el portal consecuentemente cifra una nueva cookie para enviarla al endpoint del usuario.
Certificado para cifrar/descifrar cookie	Seleccione el certificado a usar para cifrar y descifrar la cookie. *Asegúrese de que el portal y las puertas de enlace usan el mismo certificado para cifrar y descifrar cookies. (Configure el certificado como parte de una configuración de cliente de puerta de enlace. consulte* Network > GlobalProtect > Gateways*).*
Componentes que requieren contraseñas dinámicas (autenticación de dos factores)	
Para configurar GlobalProtect para que admita contraseñas dinámicas, como las contraseñas de una vez (OTP), especifique los tipos de puerta de enlace o portal que requieren que los usuarios introduzcan contraseñas dinámicas. Cuando no se habilita la autenticación de dos factores, GlobalProtect usa la autenticación regular usando las credenciales de inicio de sesión (como AD) y un certificado. Cuando habilite un tipo de puerta de enlace o portal para la autenticación de dos factores, ese portal o puerta de enlace solicita al usuario tras la autenticación del portal inicial que introduzca credenciales y una segunda OTP (u otra contraseña dinámica)- Sin embargo, si también habilita la cancelación de autenticación, se utiliza una cookie cifrada para autenticar al usuario (después de que el usuario se autenticó primero para la nueva sesión) y, por lo tanto, anticipa el requisito para que el usuario reingrese las credenciales (siempre que la cookie sea válida). Por lo tanto, el usuario inicia sesión de manera transparente cuando sea necesario siempre que la cookie sea válida. Especifique la duración de la cookie.	
Portal	Seleccione esta opción para usar contraseñas dinámicas para conectarse al portal.
Internal gateways - all	Seleccione esta opción para usar contraseñas dinámicas para conectarse a puertas de enlaces internas.
Puertas de enlace externas (solo manual)	Seleccione esta opción para usar contraseñas dinámicas para conectarse a las puertas de enlace externas que están configuradas como puertas de enlace manuales en **Manual**.
External gateways-auto discovery	Seleccione esta opción para utilizar contraseñas dinámicas para conectarse a cualquier puerta de enlace externa restante

© 2020 Palo Alto Networks, Inc.

Ajustes de Configuración de autenticación de clientes del portal de GlobalProtect	Description (Descripción)
	que la aplicación pueda descubrir automáticamente (puertas de enlaces que no estén configuradas en **Manual**).

Pestaña Criterios de selección de configuración de agente de portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **Config Selection Criteria (Criterios de selección de configuración)**

Seleccione la pestaña **Config Selection Criteria (Criterios de selección de configuración)** para configurar los criterios de coincidencia utilizados para identificar el tipo de endpoint en las implementaciones con endpoints gestionados y no gestionados. El portal puede enviar configuraciones especificadas al endpoint según el tipo de endpoint.

Ajustes de los criterios de selección de configuración del portal de GlobalProtect	Description (Descripción)
Pestaña Usuario/grupo de usuarios	
SO	Seleccione **Add (Añadir)** para añadir uno o varios sistemas operativos (SO) de endpoint y especificar qué endpoints recibirán esta configuración. El portal automáticamente detecta el SO del endpoint e incorpora detalles para ese SO en la configuración del cliente. Puede seleccionar **cualquier** SO o un SO específico (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** o **WindowsUWP**).
Usuario/grupo de usuarios	Seleccione **Add (Añadir)** para añadir usuarios o grupos de usuarios específicos a los cuales se aplica esta configuración. *Debe configurar la asignación de grupo (Device [Dispositivo] > User Identification [Identificación de usuarios] > Group Mapping Settings [Configuración de asignación de grupos]) para poder seleccionar los grupos de usuarios.* Para implementar esta configuración en todos los usuarios, seleccione **any (cualquiera)** en la lista desplegable **User/User Group (Usuario/Grupo de usuarios)**. Para implementar esta configuración únicamente en los usuarios con aplicaciones GlobalProtect en el modo previo al inicio de sesión, seleccione **pre-logon (anterior al inicio de sesión)**

© 2020 Palo Alto Networks, Inc.

Ajustes de los criterios de selección de configuración del portal de GlobalProtect	Description (Descripción)
	en la lista desplegable **User/User Group (Usuario/ Grupo de usuarios)**.
Comprobación de dispositivos	
La cuenta de máquina existe con un número de serie del dispositivo	Configure los criterios de coincidencia según si el número de serie del endpoint existe en Active Directory.
Perfil del certificado	Seleccione el perfil de certificado que el portal de GlobalProtect utiliza para hacer coincidir con el certificado del equipo enviado por la aplicación de GlobalProtect.
Comprobaciones personalizadas	
Comprobaciones personalizadas	Seleccione esta opción para definir la información de host personalizada con la cual comparar.
Clave de registro	Para buscar en los endpoints de Windows una clave de registro determinada, haga clic en **Add (Añadir)** e introduzca la **Registry Key (Clave de registro)** para buscar las coincidencias. Para buscar coincidencias solo en los endpoints a los que les falta la clave de registro específica o el valor de la clave, habilite la opción **Key does not exist or match the specified value data (La clave no existe o no coincide con datos de valor especificados)**. Para buscar coincidencias con valores concretos, haga clic en **Add (Añadir)** e introduzca el **Registry Value (Valor de registro)** y los **Value Data (Datos de valor)**. Para buscar coincidencias en endpoints que explícitamente no tengan el valor o los datos de valor especificados, seleccione **Negate (Negar)**.
Plist	Para verificar los endpoints de macOS para encontrar una entrada específica en la lista de propiedades (plist), haga clic en **Add (Añadir)** e introduzca el nombre de **Plist**. Para buscar coincidencias solo en endpoints que no tengan la plist especificada, seleccione **Plist does not exist (La lista de propiedades no existe)**. Para buscar coincidencias en pares de clave-valor concretos dentro de la plist, haga clic en **Add (Añadir)** e introduzca la clave en **Key (Clave)** y el valor correspondiente en **Value (Valor)**. Para buscar coincidencias en endpoints que explícitamente no tengan la clave o el valor especificados, seleccione **Negate (Negar)**.

© 2020 Palo Alto Networks, Inc.

Pestaña interna de agente de Portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **Internal (Interna)**

Seleccione la pestaña **Internal (Interna)** para configurar los ajustes de puerta de enlace interna para una configuración de agente.

Configuración interna de portales de GlobalProtect	Description (Descripción)
Detección de host interno	
Detección de host interno	Seleccione esta opción para permitir a la aplicación de GlobalProtect determinar si está dentro de la red empresarial. Esta opción se aplica solo a los endpoints que están configurados para comunicarse con las puertas de enlace internas y es la opción recomendada para estos endpoints. Cuando el usuario intenta iniciar sesión, la aplicación realiza una búsqueda de DNS inversa de un host interno utilizando el valor especificado de **Hostname (Nombre de host)** para **IP Address (Dirección IP)**. El host sirve como un punto de referencia que se puede alcanzar si el endpoint está dentro de la red empresarial. Si la aplicación encuentra el host, el endpoint está dentro de la red y la aplicación se conecta a una puerta de enlace interna; si la aplicación no encuentra el host interno, el endpoint está afuera de la red y la aplicación establece un túnel en una de las puertas de enlace externas. • El tipo de dirección IP puede ser **IPv4** (solo tráfico IPv4), **IPv6** (solo tráfico IPv6) o ambos. Utilice **IPv4** e **IPv6** si su red admite dos configuraciones de pila, donde IPv4 y 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 IPv4 o 21DA:D3:0:2F3b para IPv6). • Si selecciona **IPv4** e **IPv6**, introduzca el tipo de dirección IP apropiado para cada uno.
Nombre de host	Introduzca el **Hostname (Nombre de host)** que lleva a la dirección IP en la red interna.
Puertas de enlace internas	
Especifique las puertas de enlace internas a las cuales una aplicación puede solicitar acceso y también proporcione informes HIP (si el HIP está habilitado en Pestaña Recopilación de datos de agente de Portales de GlobalProtect).	Haga clic en **Add (Añadir)** para añadir puertas de enlace internas que incluyan esta información para cada una de las siguientes: • **Name (Nombre)**: etiqueta de hasta 31 caracteres para identificar la puerta de enlace. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. • **Address (Dirección)**: la dirección IP o FQDN de la interfaz del cortafuegos para la puerta de enlace. Este valor debe coincidir con el Nombre común (Common Name, CN) y SAN (si está especificado) en el certificado del servidor de puerta de enlace. Por ejemplo, si utilizó un FQDN para generar el certificado, debe introducir el FQDN aquí. • **Source Address (Dirección de origen)**: una dirección de origen o un grupo de direcciones para endpoints. Cuando los usuarios se conectan,

© 2020 Palo Alto Networks, Inc.

Configuración interna de portales de GlobalProtect	Description (Descripción)
	GlobalProtect reconoce la dirección de origen del dispositivo. Solo las aplicaciones de GlobalProtect con direcciones IP que se incluyen en el grupo de direcciones de origen pueden autenticarse con esta puerta de enlace y enviar informes HIP. • **DHCP Option 43 Code (Código de opción 43 de DHCP)** (Sólo para Windows y Mac): códigos de subopción DHCP para la selección de puerta de enlace. Especifique uno o más códigos de subopción (en decimal). La aplicación de GlobalProtect lee la dirección de puerta de enlace de los valores definidos por los códigos de subopción.

Pestaña externa de agente de Portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **External (Externa)**

Seleccione la pestaña **External (Externa)** para configurar los ajustes de puerta de enlace externa para una configuración de agente.

Configuración externa de portales de GlobalProtect	Description (Descripción)
Tiempo límite (seg.)	Especifique la cantidad de segundos que una aplicación espera para que todas las puertas de enlace disponibles respondan antes de que seleccione la mejor puerta de enlace. En las siguientes solicitudes de conexión, la aplicación intenta conectarse solo a aquellas puertas de enlace que respondieron antes del cierre. Un valor de 0 significa que la aplicación utiliza el **TCP Connection Timeout (Tiempo de espera de conexión TCP)** en **AppConfigurations (Ajustes de la aplicación)** en la pestaña **App (Aplicación)** (el intervalo es de 0 a 10; el valor predeterminado es 5).
Puertas de enlace externas	
Especifique la lista de cortafuegos a los que las aplicaciones pueden intentar conectarse cuando establecen un túnel mientras no están en la red corporativa.	Haga clic en **Add (Añadir)** para añadir puertas de enlace externas que incluyan esta información para cada una de las siguientes • **Name (Nombre)**: etiqueta de hasta 31 caracteres para identificar la puerta de enlace. El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos. • **Address (Dirección)**: la dirección IP o FQDN de la interfaz del cortafuegos donde la puerta de enlace se configura. El valor debe coincidir con el CN (y SAN, si está especificado) en el certificado del servidor de puerta de enlace. Por ejemplo, si utilizó un FQDN para generar el certificado, también debe introducir el FQDN aquí. • **Source Region (Región de origen)**: región de origen de los endpoints. Cuando los usuarios se conectan, GlobalProtect reconoce la región del endpoint y solo permite que los usuarios se conecten a las puertas de enlace configuradas para esa región. Para las opciones de puertas de enlace, la región de origen se considera primero, luego la prioridad de la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Configuración externa de portales de GlobalProtect	Description (Descripción)
	• **Priority (Prioridad)**: seleccione un valor (**Highest [Más alto]**, **High [Alto]**, **Medium [Medio]**, **Low [Bajo]**, **Lowest [Más bajo]** o **Manual only [Solo manual]**) para ayudar a la aplicación a determinar qué puerta de enlace utilizar. La opción **Manual only (Solo manual)** evita que la aplicación de GlobalProtect intente conectarse a esta puerta de enlace cuando **Auto Discovery (Detección automática)** esté habilitado en el endpoint. En primer lugar, la aplicación contactará a todas las puertas de enlace especificadas con la prioridad **Highest (Más alta)**, **High (Alta)** o **Medium (Media)** y establecerá un túnel con la puerta de enlace que proporcione una respuesta más rápida. Si no es posible comunicarse con las puertas de enlace de mayor prioridad, la aplicación se comunica con las puertas de enlace adicionales con valores de prioridad más bajos (excluye las puertas de enlace **Manual only [Solo manual]**). • **Manual**: seleccione esta opción para permitirles a los usuarios seleccionar manualmente (o cambiar a) la puerta de enlace. La aplicación de GlobalProtect puede conectarse a cualquier puerta de enlace externa configurada en **Manual**. Cuando la aplicación se conecta a otra puerta de enlace, el túnel existente se desconecta y se establece un nuevo túnel. A diferencia de la puerta de enlace principal, las puertas de enlace manuales pueden también tener un mecanismo de autenticación diferente. Si se reinicia un endpoint o si se realiza un redescubrimiento, la aplicación de GlobalProtect se conecta a la puerta de enlace principal. Esta función es muy útil si un grupo de usuarios necesita conectarse de forma temporal a una puerta de enlace específica para acceder a un segmento seguro de su red.
VPN externo	
VPN externo	Para indicar a la aplicación de GlobalProtect que ignore los clientes VPN externos seleccionados, de modo que GlobalProtect no entre en conflicto con ellos, haga clic en **Add (Añadir)** para añadir el nombre del cliente de VPN: Seleccione el nombre de la lista o ingrese el nombre en el campo suministrado. GlobalProtect ignora la configuración de la ruta para los clientes VPN especificados si configura esta función.

Pestaña de la aplicación de agente de Portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **App (Aplicación)**

Seleccione la pestaña **App (Aplicación)** para especificar la forma en la que interactúan los usuarios finales con las aplicaciones de GlobalProtect instaladas en sus sistemas. Puede definir configuraciones de aplicaciones diferentes para las distintas configuraciones de agente de GlobalProtect que cree.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Página de bienvenida	Seleccione la página de bienvenida para presentar a los usuarios finales después de que se conecten a GlobalProtect. Puede seleccionar la página **factory-default (predeterminada**

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	de fábrica) o **Import (Importar)** para importar una página personalizada. El valor predeterminado es **None (Ninguno)**.
Configuraciones de aplicación	
Connect Method (Método de conexión)	• **On-demand (Bajo demanda) (Manual user initiated connection [Conexión iniciada manualmente por el usuario])**: los usuarios deben iniciar la aplicación de GlobalProtect y luego iniciar una conexión al portal e introducir sus credenciales de GlobalProtect. Esta opción se utiliza principalmente para conexiones con acceso remoto. • **User-logon (Inicio de sesión del usuario) (Always On [Siempre activado])**: la aplicación de GlobalProtect automáticamente establece una conexión al portal después de que el usuario inicia sesión en un endpoint. El portal responde brindando el cliente la aplicación con la configuración de agente apropiada. De manera subsiguiente, la aplicación configura un túnel a una de las puertas de enlace especificadas en la configuración de agente que recibió del portal. • **Pre-logon (Anterior al inicio de sesión)**: el modo anterior al inicio de sesión asegura que los usuarios remotos de Windows y Mac siempre estén conectados a la red corporativa, y habilita los scripts de inicio de sesión de usuario y la aplicación de directivas de dominio cuando el usuario inicia sesión en el endpoint. Debido a que el endpoint puede conectarse a la red corporativa como si fuera interna, los usuarios pueden iniciar sesión con nuevas contraseñas cuando sus contraseñas caducan o recibir ayuda con la recuperación de contraseñas si olvidan su contraseña. Con el modo anterior al inicio de sesión, la aplicación de GlobalProtect establece un túnel VPN para una puerta de enlace de GlobalProtect antes de que el usuario inicie sesión en el endpoint; el endpoint solicita autenticación enviando un certificado preinstalado de la máquina a la puerta de enlace. A continuación, en los endpoints de Windows, la puerta de enlace reasigna el túnel VPN del usuario anterior al inicio de sesión al nombre de usuario que inició sesión en el enpoint; en los endpoints de Mac, la aplicación se desconecta y crea un nuevo túnel VPN para el usuario. Existen dos métodos de conexión anteriores al inicio de sesión, cualquiera de los cuales permite la misma funcionalidad anterior al de sesión que tiene lugar antes de que los usuarios inicien sesión en el endopoint. Sin embargo, después de que los usuarios inicien sesión en el enpoint, el método de conexión anterior al inicio de sesión determina cuándo se establece la conexión de la aplicación de GlobalProtect:

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	• **Pre-logon (Anterior al inicio de sesión) (Always On [Siempre activado])**: la aplicación de GlobalProtect intenta automáticamente conectarse y volver a conectarse a las puertas de enlace de GlobalProtect. Los dispositivos móviles no admiten la funcionalidad de anterior al inicio de sesión y, por consiguiente, utilizarán de forma predeterminada el método de conexión **User-Logon (Always On) (Inicio de sesión de usuario - siempre activado)** si se especifica este método de conexión. • **Pre-logon then On-demand (Antes del inicio de sesión y, a continuación, bajo demanda)**: los usuarios deben iniciar la aplicación de GlobalProtect e iniciar la conexión manualmente. Los dispositivos móviles no admiten la funcionalidad anterior al inicio de sesión y, por consiguiente, utilizarán de forma predeterminada el método de conexión **On-demand (Manual user initiated connection) (Bajo demanda - conexión manual iniciada por el usuario)** si se especifica este método de conexión.
GlobalProtect App Config Refresh Interval (hours) (Intervalo de actualización de configuración para la aplicación de GlobalProtect [horas])	Especifique el número de horas que el portal de GlobalProtect espera antes de iniciar la siguiente actualización de la configuración de una aplicación (el intervalo es de 1 a 168; el valor predeterminado es 24).
Allow User to Disable GlobalProtect App (Permitir al usuario desactivar la aplicación de GlobalProtect)	Especifica si los usuarios pueden deshabilitar la aplicación de GlobalProtect y, si es así, qué (en todo caso) deben hacer antes de deshabilitar la aplicación: • **Allow (Permitir)**: permite que cualquier usuario deshabilite la aplicación de GlobalProtect según sea necesario. • **Disallow (No permitir)**: no permite que los usuarios finales deshabiliten la aplicación de GlobalProtect. • **Allow with Comment (Permitir con comentario)**: permite que los usuarios deshabiliten la aplicación de GlobalProtect en su endpoint, pero requiere que ingresen el motivo para deshabilitar la aplicación. • **Allow with Passcode (Permitir con contraseña)**: permite que los usuarios ingresen un código de contraseña para deshabilitar la aplicación de GlobalProtect. Esta opción requiere que el usuario ingrese y confirme un valor de código de contraseña que, como una contraseña, no se muestra cuando se escribe. En general, los administradores brindan un código de contraseña a los usuarios antes de eventos no planificados o no anticipados para evitar que los usuarios se conecten a la red utilizando la VPN de GlobalProtect. Puede enviar el código de acceso por correo electrónico o como una publicación en el sitio web de su organización. • **Allow with Ticket (permitir con vale)**: esta opción habilita un mecanismo de respuesta de reto donde, después de

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	los intentos de un usuario de deshabilitar GlobalProtect, el endpoint muestra un número de solicitud de vale de 8 caracteres hexadecimales. El usuario debe comunicarse con el administrador del cortafuegos o el equipo de asistencia técnica (preferentemente, por teléfono para mayor seguridad) y brindar este número. En el cortafuegos (**Network [Red]** > **GlobalProtect** > **Portals [Portales]**), el administrador o técnico pueden hacer clic en **Generate Ticket (Generar vale)** e introducir el número de **Request (Solicitud)** del vale para obtener el número **Ticket (Vale)** (también es un número de 8 caracteres hexadecimales). El administrador o técnico indica este número de vale al usuario, que lo ingresa en el campo de reto para deshabilitar la aplicación.
Permitir al usuario desinstalar la aplicación de GlobalProtect	Especifica si los usuarios pueden desinstalar la aplicación de GlobalProtect y, si es así, qué (en todo caso) deben hacer antes de desinstalar la aplicación: • **Permitir**: permite que cualquier usuario desinstalar la aplicación de GlobalProtect según sea necesario. • **No permitir**: no permite que los usuarios finales desinstalen la aplicación de GlobalProtect. • **Permitir con contraseña**: aplica una contraseña para desinstalar la aplicación de GlobalProtect. Esta opción requiere que el usuario especifique y confirme una contraseña para poder continuar con la desinstalación. Puede enviar la contraseña por correo electrónico o como una publicación en el sitio web de su organización. Esta opción necesita la versión de contenido 8196-5685 o una versión posterior.
Permitir al usuario actualizar la aplicación GlobalProtect	Especifique si los usuarios finales pueden actualizar el software de la aplicación de GlobalProtect y, si es así, si pueden elegir cuándo actualizarlo: • **Disallow (No permitir)**: impide que los usuarios actualicen el software de la aplicación. • **Allow Manually (Permitir manualmente)**: permite que los usuarios comprueben e inicien las actualizaciones manualmente seleccionando **Check Version (Comprobar versión)** en la aplicación de GlobalProtect. • **Allow with Prompt (Permitir con solicitud)**(predeterminado): indica a los usuarios cuando una versión está activa en el cortafuegos y permite a los usuarios actualizar su software cuando es conveniente. • **Allow Transparently (Permitir de manera transparente)**: actualiza automáticamente el software de la aplicación cuando hay una nueva versión disponible en el portal. • **Internal (Interno)**: actualiza automáticamente el software de la aplicación siempre que una nueva versión esté

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	disponible en el portal, pero espera hasta que el enpoint esté conectado internamente a la red corporativa. Esto evita retrasos causados por actualizaciones sobre conexiones de bajo ancho de banda.
Permitir al usuario cerrar sesión desde la aplicación de GlobalProtect (Solo Windows, macOS, iOS, Android y Chrome)	Permite especificar si se permite a los usuarios cerrar sesión manualmente en la aplicación de GlobalProtect. • **Sí** (valor predeterminado): permite que cualquier usuario cierre sesión en la aplicación de GlobalProtect según sea necesario. • **No**: no permite que los usuarios finales cierren sesión en la aplicación de GlobalProtect. Esta opción necesita la versión de contenido 8196-5685 o una versión posterior.
Usar inicio de sesión único (Windows)	Seleccione **No** para deshabilitar el inicio de sesión único (single sign-on, SSO). Si habilita SSO (predeterminado), la aplicación de GlobalProtect usa automáticamente las credenciales de inicio de sesión de Windows para autenticar y luego conectarse a la puerta de enlace y el portal de GlobalProtect. GlobalProtect también permite ajustar credenciales de terceros para asegurar que los usuarios de Windows puedan autenticarse y conectarse, incluso si el proveedor de credenciales de terceros se usa para ajustar las credenciales de inicio de sesión de Windows.
Usar inicio de sesión único (macOS)	Seleccione **No** para deshabilitar el inicio de sesión único (single sign-on, SSO). Si habilita SSO (predeterminado), la aplicación de GlobalProtect usa automáticamente las credenciales de inicio de sesión de macOS para autenticar y luego conectarse a la puerta de enlace y el portal de GlobalProtect. Esta opción necesita la versión de contenido 8196-5685 o una versión posterior.
Clear Single Sign-On Credentials on Logout (Solo Windows)	Seleccione **No** para conservar credenciales de inicio de sesión único cuando el usuario cierra sesión. Seleccione **Yes (Sí)** (valor por defecto) para borrarlas y forzar al usuario a introducir las credenciales en el próximo inicio de sesión.
Use Default Authentication on Kerberos Authentication Failure Utilizar autenticación predeterminada si falla la autenticación Kerberos	Seleccione **No** para usar solo la autenticación Kerberos. Seleccione **Yes (Sí)** (predeterminado) para volver a intentar la autenticación usando el método de autenticación predeterminado después de una falla para autenticar con Kerberos. Esta opción es compatible únicamente con endpoints Windows y Mac.
Automatic Restoration of VPN Connection Timeout (Restauración	Introduzca un valor de tiempo de espera, en minutos, de 0 a 180 para especificar la acción que realiza la aplicación de GlobalProtect cuando el túnel está desconectado debido a la

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
automática del tiempo de espera de conexión VPN)	inestabilidad de la red o los cambios en el estado del endpoint debido al ingreso de un valor; el valor predeterminado es 30. • 0: deshabilite esta opción de modo que GlobalProtect no intente restablecer el túnel luego de que se desconecte el túnel. • 1 a 180: habilite esta opción de modo que GlobalProtect intente restablecer la conexión del túnel si el túnel no funciona por un período de tiempo que no supera el valor de tiempo de espera que especifica aquí. Por ejemplo, si el valor de tiempo de espera es de 30 minutos, GlobalProtect no intenta restablecer el túnel si el túnel permanece desconectado por 45 minutos. Sin embargo, si el túnel se desconecta durante 15 minutos, GlobalProtect intenta volver a conectarse porque el número de minutos no ha excedido el valor de tiempo de espera. *Con la opción de VPN siempre activada, si un usuario cambia de una red externa a una red interna antes de que caduque el valor de tiempo de espera, GlobalProtect no realiza la detección de la red. Como resultado, GlobalProtect restablece el túnel a la última puerta de enlace externa conocida. Para activar la detección interna del host, el usuario debe seleccionar la opción Volver a detectar red desde la consola de GlobalProtect.*
Wait Time Between VPN Connection Restore Attempts (Tiempo de espera entre intentos de restauración de conexión VPN)	Introduzca el período de tiempo, en segundos, que la aplicación de GlobalProtect espera entre intentos de restablecer la conexión con la última puerta de enlace conectada cuando habilita **Automatic Restoration of VPN Connection Timeout (Restauración automática del tiempo de espera de conexión VPN)**. Especifique un tiempo de espera más prolongado o breve según la condición de su red. El intervalo es de 1 a 60; el valor predeterminado es 5. Este intervalo de tiempo se utiliza como tiempo de espera de TCP para el intento de restauración en el caso de un túnel VPN SSL; y se utiliza como tiempo de espera UDP keepalive para el intento de restauración en caso de túnel IPSec. *En el modo Always-On (Siempre activo), la aplicación de GlobalProtect seguirá re-intentando indefinidamente en el tiempo de espera entre intentos de restauración de la conexión VPN configurado. Sin embargo, en el modo On-Demand (A petición), la aplicación de GlobalProtect lo intentará una vez durante el tiempo de espera configurado en Tiempo de espera entre intentos de restauración de conexión VPN y si no lo consigue dentro del*

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	periodo de espera, parará, cambiará al estado desconectado y no volverá a intentarlo.
Enforce GlobalProtect Connection for Network Access	Seleccionar **Sí** Para obligar a todo el tráfico de red a recorrer un túnel de GlobalProtect. Seleccionar **No** (predeterminado) si GlobalProtect no es obligatorio para el acceso de red, lo que significa que los usuarios aún pueden acceder a Internet si GlobalProtect está desactivado o desconectado. Para proporcionar instrucciones a los usuarios antes de que el tráfico se bloquee, configure un mensaje de notificación de bloqueo de tráfico con la opción **Traffic Blocking Notification Message (Mensaje de notificación de bloqueo de tráfico)** y opcionalmente especifique cuándo mostrar el mensaje (**Traffic Blocking Notification Delay [Retraso de notificación de bloqueo de tráfico]**). Para permitir el tráfico necesario para establecer una conexión con un portal cautivo, especifique un **Captive Portal Exception Timeout (Tiempo de espera de excepción del portal cautivo)**. El usuario debe autenticarse con el portal antes de que finalice el tiempo de espera. Para proporcionar instrucciones adicionales, configure un **Captive Portal Detection Message (Mensaje de detección de portal cautivo)** y opcionalmente especifique cuándo mostrar el mensaje (**Captive Portal Notification Delay (Retraso de notificación de portal cautivo]**). *En la mayoría de los casos, utilice la selección predeterminada No. Si selecciona Yes (Sí), se bloqueará todo el tráfico de red hacia y desde el endpoint, hasta que la aplicación se conecte con una puerta de enlace interna dentro de la empresa, o con una puerta de enlace externa fuera la red de la empresa.*
Permitir el tráfico a hosts/redes especificados cuando la opción Aplicar conexión de GlobalProtect para acceso de red está habilitada y la opción Conexión de GlobalProtect no está establecida	Si lo desea, puede configurar hasta diez direcciones IP o segmentos de red para los que desee permitir el acceso cuando aplique GlobalProtect para el acceso a la red, pero no se establezca la conexión. Separe varios valores con comas. Las exclusiones pueden mejorar la experiencia del usuario, ya que les permite acceder a los recursos locales cuando GlobalProtect está desconectado. Por ejemplo, cuando GlobalProtect no está conectado, GlobalProtect puede excluir direcciones de enlace local para permitir el acceso a un segmento de red local o dominio de transmisión. Esta opción necesita la versión de contenido 8196-5685 o una versión posterior.
Portal Connection Timeout (sec)	Para aplicar a GlobalProtect el acceso a la red, pero proporciona un período de gracia para permitir a los usuarios tiempo suficiente para conectarse a un portal cautivo, especifique el tiempo de espera en segundos (el intervalo está

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	entre 0 y 3600). Por ejemplo, un valor de 60 significa que el usuario debe iniciar sesión en el portal cautivo en el intervalo temporal de un minuto después de que GlobalProtect detecte el portal cautivo. Un valor de 0 significa que GlobalProtect no permite a los usuarios conectarse a un portal cautivo e inmediatamente bloquea el acceso.
Iniciar automáticamente la página web en el navegador predeterminado tras la detección del portal cautivo	Para iniciar automáticamente su navegador web predeterminado después de la detección del portal cautivo para que los usuarios puedan iniciar sesión sin problemas en él, especifique el nombre de dominio completo (FQDN) o la dirección IP del sitio web que desee utilizar para el intento de conexión inicial que activa el tráfico web cuando se inicia el navegador web predeterminado (la longitud máxima es de 256 caracteres). El portal cautivo intercepta este intento de conexión del sitio web y redirige el navegador web predeterminado a la página de inicio de sesión del portal cautivo. Si este campo está vacío (predeterminado), GlobalProtect no inicia el navegador web predeterminado automáticamente al detectar el portal cautivo.
Traffic Blocking Notification Delay (sec)	Especifique un valor, en segundos, para determinar cuándo mostrar el mensaje de notificación. GlobalProtect inicia la cuenta regresiva para mostrar la notificación después de que la red sea accesible (el intervalo está entre 5 y 120, y el predeterminado es 15).
Display Traffic Blocking Notification Message	Especifica si un mensaje aparece cuando se requiere GlobalProtect para el acceso a la red. Seleccionar **No** para desactivar el mensaje. Seleccionar **Yes (Sí)** para activar el mensaje (GlobalProtect muestra el mensaje cuando se desconecta GlobalProtect pero detecta que la red está accesible).
Traffic Blocking Notification Message	Personalizar un mensaje de notificación para mostrar a los usuarios cuando se requiere GlobalProtect para el acceso a la red. GlobalProtect muestra el mensaje cuando se desconecta GlobalProtect, pero detecta que la red está accesible. El mensaje puede indicar el motivo del bloqueo del tráfico y proporcionar instrucciones sobre cómo conectarse. Por ejemplo: `To access the network, you much first connect to GlobalProtect.` El mensaje debe tener 512 caracteres o menos.
Allow User to Dismiss Traffic Blocking Notifications	Seleccionar **No** Para mostrar siempre las notificaciones de bloqueo de tráfico. De forma predeterminada, el valor se establece en **Yes (Sí)**, lo que significa que los usuarios pueden desestimar las notificaciones.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Display Captive Portal Detection Message	Especifica si aparece un mensaje cuando GlobalProtect detecta un portal cautivo. Seleccionar **Yes (Sí)** para mostrar el mensaje. Seleccionar **No** (predeterminado) para suprimir el mensaje (GlobalProtect no muestra un mensaje cuando GlobalProtect detecta un portal cautivo). *Si habilita un mensaje de detección de portal cautivo, el mensaje aparecerá 85 segundos antes del tiempo de espera de excepción de portal cautivo. Por lo tanto, si el tiempo de espera de excepción del portal de captura es de 90 segundos o menos, el mensaje aparecerá 5 segundos después de que se detecta un portal cautivo.*
Captive Portal Detection Message	Personalizar un mensaje de notificación para mostrar a los usuarios cuando GlobalProtect detecta la red que proporciona instrucciones adicionales para conectarse a un portal cautivo. Por ejemplo: `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.` El mensaje debe tener 512 caracteres o menos.
Retraso de detección del portal cautivo	Si habilita un mensaje de detección del portal cautivo, puede especificar el retraso en segundos después de la detección del portal cautivo en el que GlobalProtect muestra el mensaje de detección (el intervalo es de 1 a 120; el valor predeterminado es 5).
Client Certificate Store Lookup (Búsqueda del almacén de certificados de cliente)	Seleccione el tipo de certificado o certificados que una aplicación busca en su almacén de certificados personal. La aplicación de GlobalProtect utiliza el certificado para autenticarse en el portal o en una puerta de enlace, y luego establecer un túnel VPN a la puerta de enlace de GlobalProtect. • **User (Usuario)**: autentique usando el certificado que es local para la cuenta del usuario. • **Machine (Equipo)**: autentique usando el certificado que es local para el endpoint. Este certificado se aplica en todas las cuentas de usuario con permiso para usar el endpoint. • **User and machine [Usuario y equipo]** (predeterminado): autentique usando el certificado de usuario y el certificado de la máquina.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
SCEP Certificate Renewal Period (days) (Periodo de renovación del certificado SCEP [días])	Este mecanismo es para revisar un certificado generado por SCEP antes de que el certificado realmente venza. Especifique la cantidad máxima de días antes de que el certificado venza durante los que el portal podrá solicitar un nuevo certificado desde el servidor SCEP en su sistema PKI (el intervalo está entre 0 y 30; el predeterminado es 7). Un valor de 0 significa que el portal no renueva automáticamente el certificado de cliente cuando actualiza una configuración de cliente. Para que una aplicación obtenga el nuevo certificado, el usuario debe iniciar sesión durante el período de renovación (el portal no solicita el nuevo certificado para un usuario durante este período de renovación salvo que el usuario inicie sesión). Por ejemplo, supongamos que el certificado de cliente tiene una duración de 90 días y este período de renovación de certificado es de 7 días. Si un usuario inicia sesión durante los 7 días finales de la duración del certificado, el portal genera el certificado y lo descarga junto con una configuración de cliente actualizada. Consulte GlobalProtect App Config Refresh Interval (hours).
Extended Key Usage OID for Client Certificate (OID de uso de clave extendida para certificado de cliente)	Ingrese el uso de clave extendido de un certificado de cliente especificando su identificador de objeto (object identifier, OID). Esta configuración garantiza que la aplicación de GlobalProtect seleccione únicamente un certificado que es para la autenticación del cliente y permite a GlobalProtect guardar el certificado para uso futuro.
Retain Connection on Smart Card Removal (Solo Windows)	Seleccionar **Yes (Sí)** para retener la conexión cuando un usuario elimina una tarjeta inteligente que contiene un certificado de cliente. Seleccionar **No** (predeterminado) para finalizar la conexión cuando un usuario quita una tarjeta inteligente.
Permitir anular el nombre de usuario del certificado de cliente	Seleccione **No** para obligar a GlobalProtect a utilizar el nombre de usuario del certificado de cliente y evitar que GlobalProtect lo anule (habilitado de forma predeterminada).
Enable Advanced View (Habilitar vista avanzada)	Seleccione **No** para restringir la interfaz del usuario en la aplicación a la vista mínima básica (habilitada de manera predeterminada).
Allow User to Dismiss Welcome Page (Permitir al usuario descartar la página de bienvenida)	Seleccione **No** para forzar la aparición de la Página de bienvenida cada vez que un usuario inicie una conexión. Esto restricción evita que el usuario desestime información importante, como las condiciones que puedan ser obligatorias para mantener el cumplimiento según su organización.
Enable Rediscover Network Option (Habilitar la opción de redescubrir red)	Seleccione **No** para evitar que los usuarios inicien manualmente un redescubrimiento de red.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Enable Resubmit Host Profile Option (Habilitar la opción Reenviar perfil de host)	Seleccione **No** para impedir que los usuarios activen manualmente el reenvío del último HIP.
Allow User to Change Portal Address (Permitir al usuario cambiar la dirección del portal)	Seleccione **No** para deshabilitar el campo **Portal** en la pestaña **Home (Inicio)** de la aplicación de GlobalProtect. Sin embargo, como el usuario no podrá entonces especificar un portal al que conectarse, debe proporcionar la dirección predeterminada del portal en el registro de Windows o plist de Mac: • **Registro de Windows**:`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` con la clave `Portal` • **Plist de Mac**—`/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` con clave `Portal` Para obtener más información sobre la implementación previa de la dirección del portal, consulte Configuración personalizable de la aplicación en la guía del administrador de GlobalProtect.
Allow User to Continue with Invalid Portal Server Certificate (Permitir al usuario continuar con certificado no válido de portal)	Seleccione **No** para impedir a la aplicación establecer una conexión con el portal si el certificado de portal no es válido.
Display GlobalProtect Icon (Mostrar icono GlobalProtect)	Seleccione **No** para ocultar el icono de GlobalProtect en el endpoint. Si el icono está oculto, los usuarios no pueden llevar a cabo determinadas tareas, como ver la información de resolución de problemas, cambiar contraseñas, redescubrir la red o llevar a cabo una conexión a demanda. Sin embargo, los mensajes de notificación HIP, las solicitudes de inicio de sesión y los diálogos de certificado sí muestran cuándo es necesaria la interacción de usuario.
User Switch Tunnel Rename Timeout (sec) (Tiempo de espera del switch del usuario para cambiar nombre del túnel [s]) (Solo Windows)	Especifique el número de segundos que un usuario remoto tiene para ser autenticado por una puerta de enlace de GlobalProtect tras iniciar sesión en un endpoint utilizando el Protocolo de escritorio remoto (RDP) de Microsoft (el intervalo está entre 0 y 600; el predeterminado es 0). Exigirle al usuario remoto que se autentica dentro de una cantidad de tiempo límite conserva la seguridad. Después de autenticar el nuevo usuario y cambiar al túnel para el usuario, al puerta de enlace vuelve a nombrar el túnel. Un valor de 0 significa que el túnel del usuario actual no se renombra pero, en cambio, se finaliza de inmediato. En este caso, el usuario remoto obtiene un nuevo túnel y no tiene límite de tiempo para autenticar una puerta de enlace (diferente al tiempo de espera de TCP configurado)

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Tiempo de renombrado del túnel de inicio de sesión anterior (seg) (Sólo Windows)	Esta configuración controla cómo GlobalProtect gestiona el túnel anterior al inicio de sesión que conecta un enpoint a la puerta de enlace. Un valor -1 significa que el túnel anterior al inicio de sesión no se agota después de que un usuario inicie sesión en el enpoint; GlobalProtect cambia el nombre del túnel para reasignarlo al usuario. Sin embargo, el túnel persiste incluso si el cambio de nombre falla o si el usuario no inicia sesión en la puerta de enlace de GlobalProtect. Un valor 0 significa que, cuando el usuario inicia sesión en el enpoint, GlobalProtect termina inmediatamente el túnel de inicio de sesión en lugar de cambiarlo de nombre. En este caso, GlobalProtect inicia un nuevo túnel para el usuario en lugar de permitir que el usuario se conecte a través del túnel anterior al inicio de sesión. Normalmente, este ajuste es muy útil cuando se ajusta el **Connect Method (Método de conexión)** a **Pre-logon then On-demand (Anterior al inicio de sesión a continuación, bajo demanda)**, que obliga al usuario a iniciar manualmente la conexión después del inicio de sesión inicial. Un valor de 1 a 600 indica el número de segundos en los que el túnel anterior al inicio de sesión puede permanecer activo después de que un usuario inicie sesión en el enpoint. Durante este tiempo, GlobalProtect aplica las directivas en el túnel anterior al inicio de sesión. Si el usuario se autentica con la puerta de enlace GlobalProtect dentro del período de tiempo de espera, GlobalProtect reasigna el túnel al usuario. Si el usuario no se autentica con la puerta de enlace GlobalProtect antes del tiempo de espera, GlobalProtect finaliza el túnel anterior al inicio de sesión.
Conservar el túnel en el tiempo de espera de cierre de sesión del usuario (segundos)	Para permitir que GlobalProtect conserve el túnel VPN existente después de que los usuarios cierren sesión en su endpoint, especifique un valor **Conservar túnel cuando el usuario se desconecte** (el intervalo es de 0 a 600 segundos; el valor predeterminado es 0 segundos). Si acepta el valor predeterminado de 0, GlobalProtect no conserva el túnel después del cierre de sesión del usuario.
Show System Tray Notifications (Mostrar notificaciones en la bandeja del sistema) (Solo Windows)	Seleccione **No** para ocultar las notificaciones de usuario. Seleccione **Yes (Sí)** (predeterminado) para mostrar las notificaciones en el área de la bandeja del sistema.
Custom Password Expiration Message (Sólo autenticación LDAP)	Cree un mensaje personalizado para mostrar a los usuarios cuándo sus contraseñas están a punto de vencer. La longitud máxima del mensaje es de 200 caracteres.
Usar SSL automáticamente cuando IPSec no es fiable (horas)	Si marca **Usar SSL automáticamente si IPSec es inestable**, especifique el número de horas durante las que debe hacerlo

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	la aplicación de GlobalProtect; el intervalo va de 0 a 168 horas. Si configura esta opción, la aplicación de GlobalProtect no intenta establecer ningún túnel de IPSec durante el período especificada. Este temporizador se pone en marcha cada vez que se queda inactivo un túnel de IPSec por haberse agotado el tiempo de espera de su conexión permanente. Si acepta el valor predeterminado de **0**, la aplicación no recurre a un túnel de SSL si puede establecer un túnel de IPSec. Solo recurre al primero si no logra establecer el túnel de IPSec.
Conectar solo con SSL	Especifique si necesita que los usuarios se conecten a las puertas de enlace de GlobalProtect mediante SSL en lugar de IPSec. Las opciones son las siguientes: • Sí: impone el uso de SSL para conectarse a las puertas de enlace configuradas en el portal. • No: (valor predeterminado) utiliza el protocolo configurado en la puerta de enlace. • El usuario puede cambiar: proporciona al usuario la flexibilidad de usar SSL o IPSec, si la configuración de la puerta de enlace admite el uso de cualquiera de los protocolos. Cuando se establece en **El usuario puede cambiar**, en la aplicación GP, el usuario puede habilitar o desmarcar la casilla de verificación para **VPN: Conéctese solo con SSL** para seleccionar el protocolo que habilita la mejor opción de conectividad para un acceso seguro.
Maximum Internal Gateway Connection Attempts (Máximos intentos de conexión al gateway interno)	Introduzca el número máximo de veces que el agente GlobalProtect debe reintentar la conexión con una puerta de enlace interna después de que el primer intento falle (el intervalo es de 0 a 100; el valor predeterminado es 0, lo que significa que la aplicación de GlobalProtect no reintenta la conexión). Si aumenta el valor, le permite a la aplicación conectarse automáticamente a una puerta de enlace interna que esté temporalmente desactivada o que no se pueda alcanzar durante el primer intento de conexión, pero que vuelve a activarse antes de agotar el número especificado de reintentos. Aumentar el valor también garantiza que la puerta de enlace interna recibe la información de host y usuario más actualizada.
Portal Connection Timeout (sec) (Tiempo de espera de la conexión al portal [s])	El número de segundos (entre 1 y 600) antes de una solicitud de conexión al portal se agota debido a que no hay respuesta del portal. Cuando su cortafuegos ejecuta versiones de contenido de aplicaciones y amenazas anteriores a 777-4484, el valor predeterminado es 30. A partir de la versión de contenido 777-4484, el valor predeterminado es 5.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
TCP Connection Timeout (sec) (Tiempo de espera de la conexión TCP [s])	La cantidad de segundos (de 1 a 600) antes de que se agote el tiempo de espera de la solicitud de conexión TCP debido a que no hay respuesta en un extremo de la conexión. Cuando su cortafuegos ejecuta versiones de contenido de aplicaciones y amenazas anteriores a 777-4484, el valor predeterminado es 60. A partir de la versión de contenido 777-4484, el valor predeterminado es 5.
TCP Receive Timeout (sec) (Tiempo de espera de la recepción TCP [s])	El número de segundos antes de que una conexión TCP se agote debido a la falta de alguna respuesta parcial de una solicitud TCP (el intervalo está entre 1 y 600; el predeterminado es 30).
Resolver todas las FQDN use los servidores DNS asignados por el túnel (solo Windows)	(GlobalProtect 4.0.3 y versiones posteriores) Configure las preferencias de resolución de DNS cuando el túnel de GlobalProtect esté conectado a los endpoints de Windows: • Seleccione **Yes (Sí)** (predeterminado) para acceder a que la aplicación de GlobalProtect permita a los endpoints de Windows resolver todas las consultas DNS con los servidores DNS que configura en la puerta de enlace en lugar de permitir que el endpoint envíe algunas consultas DNS a los servidores DNS establecidos en el adaptador físico. • Seleccione **No** para permitir que los endpoints de Windows envíen consultas DNS al servidor DNS configurado en el adaptador físico si el servidor DNS configurado en la puerta de enlace no resuelve la consulta inicial. Esta opción conserva el comportamiento nativo de Windows para consultar todos los servidores DNS en todos los adaptadores recursivamente, pero puede dar lugar a largos tiempos de espera para resolver algunas consultas DNS. Para configurar los ajustes de DNS para la aplicación GlobalProtect 4.0.2 y versiones anteriores, utilice la opción **Update DNS Settings at Connect (Actualizar la configuración de DNS al conectarse)**
Update DNS Settings at Connect (Solo Windows) (obsoleto)	(GlobalProtect 4.0.2 y versiones anteriores) Configure las preferencias de servidor DNS para el túnel de GlobalProtect: • Seleccione **No** (predeterminado) para permitir que los endpoints de Windows envíen consultas DNS al servidor DNS establecido en el adaptador físico si la consulta inicial al servidor DNS configurado en la puerta de enlace no se resuelve. Esta opción conserva el comportamiento nativo de Windows para consultar todos los servidores DNS en todos los adaptadores recursivamente, pero puede dar lugar a largos tiempos de espera para resolver algunas consultas DNS. • Seleccione **Yes (Sí)** para permitir que los endpoints de Windows resuelvan todas las consultas DNS con los

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	servidores DNS que configura en la puerta de enlace en lugar de los servidores DNS establecidos en el adaptador físico en el endpoint. Cuando habilita esta opción, GlobalProtect aplica estrictamente la configuración DNS de la puerta de enlace y anula las configuraciones estáticas para todos los adaptadores físicos. *Cuando esta opción se habilita, (se establece en Yes [Sí]), es posible que GlobalProtect no pueda restaurar la configuración de DNS guardada previamente y, como resultado, es posible que evite que el endpoint resuelva las consultas DNS. Esta función es obsoleta y se reemplaza con una implementación mejorada, de modo que no se produzca esta situación. Si utilizaba esta función, le recomendamos actualizar a la aplicación de GlobalProtect 4.0.3 o posterior.* Para configurar los ajustes de DNS para la aplicación de GlobalProtect 4.0.3 y posterior, utilice la opción **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Resolver todos los FQDN utilizando servidores DNS asignados por el túnel)**.
Detect Proxy for Each Connection (Solo Windows)	Seleccione **No** para detectar automáticamente el proxy de la conexión del portal y usarlo para conexiones posteriores. Seleccione **Yes (Sí)** (valor por defecto) para detectar automáticamente el proxy en cada conexión.
Configure el túnel en proxy (Solo Windows y Mac)	Especifique si GlobalProtect debe usar u omitir los proxies. Seleccione **No** para que GlobalProtect omita los proxies. Seleccione **Yes (Sí)** para que GlobalProtect use los proxies. En función del uso del proxy de GlobalProtect, el SO del endpoint y el tipo de túnel, el tráfico de la red se comportará de diferente manera.
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Solo Windows)	Seleccione **No** para evitar que la aplicación de GlobalProtect envíe datos HIP cuando cambia el estado del Centro de seguridad de Windows (Windows Security Center, WSC). Seleccione **Yes (Sí)** (valor por defecto) para enviar inmediatamente datos HIP cuando cambia el estado de WSC.
Enable Inbound Authentication Prompts from MFA Gateways	Para admitir la autenticación de múltiples factores (multi-factor authentication, MFA), un endpoint de GlobalProtect debe recibir y confirmar las solicitudes UDP que se reciben desde la puerta de enlace. Seleccione **Yes (Sí)** para permitir que un endpoint de GlobalProtect reciba y confirme la solicitud. Seleccionar **No** (predeterminado) para que GlobalProtect bloquee las solicitudes UDP desde la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Network Port for Inbound Authentication Prompts (UDP)	Especifica el número de puerto que un endpoint de GlobalProtect utiliza para recibir mensajes de autenticación de entrada desde las puertas de enlace de MFA. El puerto predeterminado es 4501. Para cambiar el puerto, especifique un número de 1 a 65535.
Trusted MFA Gateways	Especifica la lista de cortafuegos o puertas de enlace de autenticación que un endpoint de GlobalProtect confía en la autenticación de múltiples factores. Cuando un endpoint de GlobalProtect recibe un mensaje UDP en el puerto de red especificado, GlobalProtect muestra un mensaje de autenticación sólo si el mensaje UDP proviene de una puerta de enlace de confianza.
Inbound Authentication Message (Mensaje de autenticación entrante)	Personalizar un mensaje de notificación para mostrar cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional. Cuando los usuarios intentan acceder a un recurso que requiere autenticación adicional, GlobalProtect recibe un paquete UDP que contiene la solicitud de autenticación de entrada y muestra este mensaje. El paquete UDP también contiene la dirección URL para la página del portal de autenticación que especifica cuando realiza la Configuración de autenticación de múltiples factores. GlobalProtect adjunta automáticamente la URL al mensaje. Por ejemplo: `You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` El mensaje debe tener 255 caracteres o menos.
IPv6 preferido	Especifica el protocolo preferido para las comunicaciones de endpoint de GlobalProtect. Seleccionar **No** para cambiar el protocolo preferido a IPv4.Seleccione Sí (predeterminado) para hacer de IPv6 la conexión preferida un entorno de doble pila.
Cambiar el mensaje de la contraseña	Personalice un mensaje para especificar las políticas o requisitos de contraseña cuando los usuarios cambien su contraseña de Active Directory (AD). Por ejemplo: `Passwords must contain at least one number and one uppercase letter.` El mensaje debe tener 255 caracteres o menos para los idiomas de dos bytes en Unicode como el chino simplificado. En el caso del japonés, el mensaje debe tener 128 caracteres o menos.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
Mostrar panel de estado al inicio (solo Windows)	Seleccione **Yes (Sí)** para mostrar automáticamente el panel de estado de GlobalProtect cuando los usuarios establezcan una conexión por primera vez. Seleccione **No** para suprimir el panel de estado de GlobalProtect cuando los usuarios establezcan una conexión por primera vez.
Deshabilitar aplicación de GlobalProtect	
Código de acceso/Confirmar código de acceso	Ingrese y luego confirme un código de contraseña si la configuración de **Allow User to Disable GlobalProtect App (Permitir al usuario desactivar la aplicación de GlobalProtect)** es **Allow with Passcode (Permitir con contraseña)**. Registre y guarde el código de acceso en un lugar seguro. Puede distribuir el código de contraseña a los nuevos usuarios de GlobalProtect por correo electrónico o publicarlo en un área de asistencia técnica del sitio web de su empresa. Si las circunstancias impiden al endpoint establecer una conexión VPN y esta función se encuentra habilitada, un usuario puede introducir este código de contraseña en la interfaz de la aplicación para deshabilitar la aplicación de GlobalProtect y obtener acceso a internet sin usar la VPN.
Máximo número de veces que el usuario puede desactivar	Especifique el número máximo de veces que un usuario puede desactivar GlobalProtect antes de que deba conectarse a un cortafuegos. El valor predeterminado de 0 significa que los usuarios no tienen límite en el número de veces que pueden deshabilitar la aplicación.
Tiempo de espera de deshabilitación (min)	Especifique el número máximo de minutos que la aplicación de GlobalProtect puede deshabilitarse. Después de que el tiempo especificado se cumple, la aplicación intenta conectarse al cortafuegos. El valor predeterminado de 0 indica que el período de deshabilitación es ilimitado. *Configure un valor de tiempo de espera de deshabilitación para limitar el tiempo durante el cual los usuarios pueden deshabilitar la aplicación. Esto garantiza que GlobalProtect continúe y establezca la VPN cuando el tiempo de espera finalice, para proteger al usuario y el acceso del usuario a los recursos.*
Desinstalar la aplicación de GlobalProtect	
Contraseña/Confirmar contraseña	Especifique y luego confirme una contraseña si la configuración de **Permitir al usuario desinstalar la aplicación de GlobalProtect** es **Permitir con contraseña**. Registre y guarde la contraseña en un lugar seguro. Utilice esta configuración para evitar que sus usuarios desinstalen la aplicación de GlobalProtect. Una vez

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de la aplicación de GlobalProtect	Description (Descripción)
	configurado, el usuario debe especificar esta contraseña en la interfaz de la aplicación de GlobalProtect para desinstalar dicha aplicación.
Configuración del gestor de seguridad móvil	
Gestor de seguridad móvil	Si está utilizando el gestor de seguridad móvil de GlobalProtect para la gestión del dispositivo móvil (mobile device management, MDM), introduzca la dirección IP o FQDN de la interfaz de registro (inscripción) del dispositivo en el dispositivo GP-100.
Puerto de inscripción	Número de puerto que debe utilizar el endpoint móvil al conectar al gestor de seguridad móvil de GlobalProtect para la inscripción. De manera predeterminada, el gestor de seguridad móvil escucha en el puerto 443. *Se recomienda conservar este número de puerto de modo que no se pida a los usuarios de endpoint móvil un certificado de cliente durante el proceso de inscripción (otros valores posibles son 443, 7443 y 8443).*

Pestaña Recopilación de datos HIP de agente de portales de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Agent (Agente)** > *<agent-config>* > **HIP Data Collection (Recopilación de datos HIP)**

Seleccione la pestaña **HIP Data Collection (Recopilación de datos HIP)** para definir los datos que la aplicación recopilará del endpoint en el informe HIP:

Ajustes de configuración de recopilación de datos HIP de GlobalProtect	Description (Descripción)
Recopilar datos HIP	Borre esta opción para evitar que la aplicación recopile y envíe datos HIP. *Habilite GlobalProtect para que recopile datos HIP para la aplicación de la política basada en HIP, de manera que el cortafuegos pueda comparar los datos HIP de endpoints con los objetos HIP o perfiles HIP que usted defina, y luego aplicar la política correspondiente.*
Max Wait Time (Tiempo máx. de espera) (segundos)	Especifique durante cuántos segundos la aplicación debe buscar los datos HIP antes de enviar los datos disponibles (el intervalo es de 10 a 60; el valor predeterminado es 20).

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de recopilación de datos HIP de GlobalProtect	Description (Descripción)
Perfil del certificado	Seleccione el perfil de certificado que el portal de GlobalProtect utiliza para hacer coincidir con el certificado del equipo enviado por la aplicación de GlobalProtect.
Excluir categorías	Seleccione **Exclude Categories (Excluir categorías)** para especificar las categorías de información de host para las que no desee que la aplicación recopile datos HIP. Seleccione **Category (Categoría)** (como prevención de pérdida de datos) para excluir de la recopilación HIP. Después de seleccionar una categoría, puede hacer clic en **Add (Añadir)** para añadir un proveedor particular y luego puede seleccionar **Add (Añadir)** para añadir productos específicos del proveedor y restringir más la exclusión, según fuera necesario. Haga clic en **OK (Aceptar)** para guardar la configuración de cada diálogo.
Comprobaciones personalizadas	Seleccione **Custom Checks (Comprobaciones personalizadas)** para definir la información de host personalizada que desea que recopile la aplicación. Por ejemplo, si tiene aplicaciones necesarias que no estén incluidas en la lista de productos o de proveedores para crear objetos HIP, puede crear una comprobación personalizada para determinar si se ha instalado esa aplicación (tiene un registro de Windows o clave plist de Mac que corresponde) o se está ejecutando actualmente (tiene un proceso en ejecución que corresponde). • **Windows**: haga clic en **Add (Añadir)** para añadir una comprobación de una clave de registro determinada o un valor clave. • **Mac**: haga clic en **Add (Añadir)** para añadir una comprobación de una clave de plist determinada o un valor clave. • **Process List (Lista de procesos)**: haga clic en **Add (Añadir)** para añadir los procesos que desea comprobar en los endpoints de usuario para ver si se están ejecutando. Por ejemplo, para determinar si una aplicación de software se está ejecutando, agregue el nombre del archivo ejecutable a la lista de procesos. Puede añadir un proceso a la pestaña **Windows** o **Mac** o a ambas.

Pestaña VPN sin cliente de portales GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales)** > *<portal-config>* > **Clientless VPN (VPN sin cliente)**

Ahora puede configurar el portal GlobalProtect para proporcionar acceso remoto seguro a aplicaciones web empresariales comunes que utilizan tecnologías HTML, HTML5 y JavaScript. Los usuarios tienen la ventaja de un acceso seguro desde los navegadores web habilitados para SSL sin instalar el software de GlobalProtect. Esto es útil cuando necesita habilitar el acceso de socios o contratistas a aplicaciones y para habilitar de manera segura activos no administrados, incluidos dispositivos personales. Esta característica requiere que instale una suscripción de GlobalProtect en el cortafuegos que aloja la VPN sin cliente desde el portal GlobalProtect. Seleccione la pestaña **Clientless VPN (VPN sin cliente)** para configurar los ajustes de VPN sin cliente de GlobalProtect en el portal, según se describe en la siguiente tabla:

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración sin cliente del portal GlobalProtect	Description (Descripción)
Pestaña General	
VPN sin cliente	Seleccionar **Clientless VPN (VPN sin cliente)** para especificar información general acerca de la sesión VPN sin cliente:
Nombre de host	La dirección IP o FQDN del portal GlobalProtect que aloja la página de destino de las aplicaciones web. La VPN de GlobalProtect sin cliente vuelve a escribir las URL de la aplicación con este nombre de host. *Si utiliza Network Address Translation (NAT) para proporcionar acceso al portal GlobalProtect, la dirección IP o FQDN que introduzca debe coincidir (o resolverse) con la dirección IP NAT del portal GlobalProtect (la dirección IP pública).*
Zona de seguridad	La zona para la configuración VPN sin cliente. Las reglas de seguridad definidas en esta zona controlan a qué aplicaciones pueden acceder los usuarios.
Proxy Dns	El servidor DNS que resuelve los nombres de las aplicaciones. Seleccionar un servidor **DNS Proxy (Proxy de DNS)** o configurar una **New DNS Proxy (Proxy de DNS nueva)** (Network > DNS Proxy).
Duración de inicio de sesión	El número de **Minutes (Minutos)** (el intervalo es de 60 a 1440) o de **Hours (Horas)** (el intervalo es de 1 a 24, el valor predeterminado es 3) por el que una sesión VPN SSL sin cliente es válida. Después de la hora especificada, los usuarios deben volver a autenticarse e iniciar una nueva sesión VPN sin cliente.
Tiempo de espera de inactividad	El número de **Minutes (Minutos)** (el intervalo es de 5 a 1440, el valor predeterminado es 30) o de **Hours (Horas)** (el intervalo es de 1 a 24) por el que una sesión VPN SSL sin cliente puede permanecer inactiva. Si no hay actividad de usuario durante la cantidad de tiempo especificada, el usuario debe volver a autenticarse e iniciar una nueva sesión VPN sin cliente.
Máx. de usuarios	La cantidad máxima de usuarios que pueden iniciar sesión en el portal al mismo tiempo (el valor predeterminado es 10, el intervalo es de 1 a sin máximo). Cuando se alcanza el número máximo de usuarios, los usuarios VPN sin cliente adicionales no pueden iniciar sesión en el portal.
Pestaña Aplicaciones	
Asignación de aplicaciones a usuario	**Add (Añadir)** uno o mas **Applications to User Mapping (Aplicaciones a la asignación de usuarios)** para hacer coincidir los usuarios con las aplicaciones publicadas. Esta asignación controla qué usuarios o grupos de usuarios pueden usar una VPN sin cliente para acceder a las aplicaciones. Debe definir las aplicaciones y los grupos de aplicaciones antes de asignarlos a los usuarios (Network > GlobalProtect > Clientless Apps y Network > GlobalProtect > Clientless App Groups).

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración sin cliente del portal GlobalProtect	Description (Descripción)
	• **Name (Nombre)**: introduzca un nombre para asignación (de hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos. • **Display application URL address bar (Mostrar la barra de direcciones URL de aplicaciones)**: seleccione esta opción para mostrar una barra de direcciones URL de aplicaciones desde la cual los usuarios pueden iniciar aplicaciones inéditas en la página de inicio de aplicaciones. Cuando esta opción está habilitada, los usuarios pueden hacer clic en el enlace **Application URL (URL de aplicación)** en la página y especificar una dirección URL.
Usuario/grupo de usuarios	Puede añadir usuarios individuales o grupos de usuarios con **Add (Añadir)**, a los cuales se aplique la configuración de aplicación actual. Estos usuarios tienen permiso para iniciar las aplicaciones configuradas utilizando una VPN sin cliente de GlobalProtect. *Debe configurar la asignación de grupo (Device (Dispositivo) > User Identification (Identificación de usuario) > Group Mapping Settings (Configuración de asignación de grupo)) antes de poder seleccionar los grupos.* Además de los usuarios y grupos, puede usar el menú desplegable para especificar cuando esta configuración se aplique a los usuarios o grupos: • **any (cualquiera)**: la configuración de la aplicación se aplica a todos los usuarios (no es necesario **Add (Añadir)** usuarios o grupos de usuarios). • **select (seleccionar)**: la configuración de la aplicación se aplica solo a usuarios y grupos de usuarios que usted añade a esta lista con **Add (Añadir)**.
applications	Usted puede **Add (Añadir)** aplicaciones individuales o grupos de aplicaciones a la asignación. Los **Source Users (Usuarios de origen)** que incluyó en la configuración pueden utilizar la VPN GlobalProtect sin cliente para iniciar las aplicaciones que añade.
Pestaña Configuración de perfil criptográfico	
Versiones de protocolo	Seleccione las versiones TLS/SSL mínimas y máximas requeridas. Cuanto mayor sea la versión TLS, más segura será la conexión. Las opciones incluyen **SSLv3**, **TLSv1.0**, **TLSv1.1**, o **TLSv1.2**.
Algoritmos de intercambio de clave	Seleccione los tipos de algoritmos compatibles para el intercambio de claves. Las opciones incluyen **RSA**, Diffie-Hellman (**DHE**), o Curva Elíptica Efímera Diffie-Hellman (**ECDHE**).
Algoritmos de cifrado	Seleccione los algoritmos de cifrado compatibles. Se recomienda **AES128** o superior.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración sin cliente del portal GlobalProtect	Description (Descripción)
Algoritmos de autenticación	Seleccione los algoritmos de autenticación compatibles. Las opciones son: **MD5**, **SHA1**, **SHA256** y **SHA384**. Se recomienda **SHA256** o superior.
Verificación de certificado de servidor	Habilitar qué acciones emprender para los siguientes problemas que pueden ocurrir cuando una aplicación presenta un certificado de servidor: • **Block sessions with expired certificate (Bloquear sesiones con certificado caducado)**: si el certificado del servidor ha caducado, bloquee el acceso a la aplicación. • **Block sessions with untrusted issuers (Bloquear sesiones con emisores no fiables)**: si el certificado de servidor se emite desde una autoridad con certificado no fiable, bloquee el acceso a la aplicación. • **Block sessions with unknown certificate status (Bloquear sesiones con estado de certificado desconocido)**: si el servicio OCSP o CRL devuelve el estado de revocación de certificado `desconocido`, bloquear el acceso a la aplicación. • **Block sessions on certificate status check timeout (Bloquear sesiones en el tiempo de espera de comprobación de estado del certificado)**: si la comprobación del estado del certificado se agota antes de recibir una respuesta de cualquier servicio de estado del certificado, bloquee el acceso a la aplicación.
Pestaña Proxy	
Nombre	Una etiqueta de hasta 31 caracteres para identificar el servidor proxy que utiliza el portal GlobalProtect para acceder a las aplicaciones publicadas. El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos.
Dominios	Añada los dominios servidos por el servidor proxy.
Usar proxy	Seleccione esta opción para permitir que el portal GlobalProtect utilice el servidor proxy para acceder a las aplicaciones publicadas.
Servidor Puerto	Especifique el nombre de host (o dirección IP) y el número de puerto del servidor proxy.
Usuario Contraseña	Especifique el nombre de usuario y la contraseña necesarios para iniciar sesión en el servidor proxy. Introduzca la contraseña nuevamente para verificación.
Pestaña Configuración avanzada	
Reescribir lista de dominios excluidos	(Opcional) **Add (Añadir)** nombres de dominio, nombres de host o direcciones IP a **Rewrite Exclude Domain List (Reescribir lista de dominios excluidos)**. La VPN sin cliente actúa como un proxy inverso, y modifica las páginas devueltas por las aplicaciones publicadas. Cuando un usuario remoto accede a la URL, las solicitudes pasan por el portal GlobalProtect. En algunos casos, la aplicación puede tener páginas a las que no se necesita acceder a través

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración sin cliente del portal GlobalProtect	Description (Descripción)
	del portal. Especifique los dominios que deben excluirse de las reglas de reescritura y no se pueden volver a escribir. Las rutas no se admiten en los nombres de host y dominio. El carácter comodín (*) para los nombres de host y dominio sólo puede aparecer al principio del nombre (por ejemplo, * .etrade.com).

Pestaña Satélite del portal de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Satellite (Satélite)**

Un satélite es un cortafuegos de Palo Alto Networks® (tradicionalmente en una sucursal) que actúa como aplicación de GlobalProtect para permitir que el satélite establezca conectividad de VPN con una puerta de enlace de GlobalProtect. Como una aplicación de GlobalProtect, un satélite recibe su configuración inicial del portal, que incluye certificados e información sobre la ruta de configuración de VPN y le permite al satélite conectarse a todas las puertas de enlace configuradas para establecer conectividad de VPN.

Antes de configurar los ajustes de satélite de GlobalProtect en el cortafuegos de la sucursal, debe configurar una interfaz con conectividad de WAN y establecer una política y una zona de seguridad para que la LAN de la sucursal pueda comunicarse con Internet. Puede seleccionar la pestaña **Satellite (Satélite)** para configurar los ajustes del satélite de GlobalProtect en el portal, según se describe en la siguiente tabla.

Ajustes de configuración del satélite del portal de GlobalProtect	Description (Descripción)
General	• **Name (Nombre)**: un nombre para esta configuración de satélite en el portal de GlobalProtect. • **Configuration Refresh Interval (hours) [Intervalo de actualización de la configuración (horas)]**: especifique la frecuencia con la que el satélite debe comprobar el portal para obtener actualizaciones de la configuración (el intervalo es 1-48; el predeterminado es 24).
Dispositivos	Haga clic en **Add (Añadir)** para añadir un satélite usando el **Serial Number (Número de serie)** del cortafuegos. El portal no puede aceptar un número de serie o credenciales de inicio de sesión para identificar quién solicita una conexión; si el portal no recibe un número de serie, solicita las credenciales de inicio de sesión. Si identifica el satélite por su número de serie de cortafuegos, no debe brindar las credenciales de inicio de sesión del usuario cuando el satélite se conecta primero para adquirir el certificado de autenticación y su configuración inicial. Después de que el satélite se autentica por un número de serie o las credenciales de inicio de sesión, el **Satellite Hostname (Nombre del host del satélite)** se añade automáticamente al portal.
Usuario de inscripción/ Grupo de usuarios	El portal puede usar los ajustes **Enrollment User/User Group (Usuario de inscripción/Grupo de usuarios)** con o sin los números de serie de Dispositivos para hacer coincidir un satélite con una configuración. Los

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración del satélite del portal de GlobalProtect	Description (Descripción)
	satélites que no coinciden en el número de serie deberán autenticarse como un usuario individual o un miembro de grupo. Haga clic en **Add (Añadir)** para añadir un usuario o grupo que desee recibir esta configuración. *Antes de que pueda restringir la configuración a los grupos específicos, debe habilitar la asignación de grupo en el cortafuegos (Device [Dispositivo] > User Identification [Identificación de usuario] > Group Mapping Settings [Configuración de asignación de grupos]).*
Gateways	Haga clic en **Add (Añadir)** para introducir la dirección IP o nombre de host de los satélites de las puertas de enlace con los que esta configuración puede establecer túneles de IPSec. Introduzca el FQDN o la dirección IP de la interfaz donde está configurada la puerta de enlace en el campo **Gateways (Puertas de enlace)**. Las direcciones IP pueden especificarse como **IPv6**, **IPv4** o ambos. Seleccione **IPv6 Preferred (IPv6 preferido)** para especificar la preferencia de las conexiones IPv6 en un entorno de doble pila. (Opcional) Si está añadiendo dos o más puertas de enlace a la configuración, la **Routing Priority (Prioridad del enrutador)** ayuda al satélite a seleccionar la puerta de enlace preferida (el intervalo es 125). Los números menores tienen mayor prioridad (para las puertas de enlace que están disponibles). El satélite multiplica la prioridad de enrutamiento por 10 para determinar la medida de enrutamiento. *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 una puerta de enlace, asegúrese también de establecer la prioridad de enrutamiento de modo que las rutas anunciadas por puertas de enlace de reserva tienen medidas más altas que las mismas rutas anunciadas por puertas de enlace 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.* El satélite también comparte su información de red y enrutador con las puertas de enlace si selecciona **Publish all static and connected routes to Gateway (Publicar todas las rutas estáticas y conectadas a la puerta de enlace)** (**Network [Red]** > **IPSec tunnels [Túneles IPSec]** > **<tunnel [túnel]** > **Advanced [Avanzado]**, disponible únicamente cuando selecciona **GlobalProtect Satellite [Satélite de GlobalProtect] en <tunnel [túnel]** > **General**).
CA raíz de confianza	Haga clic en **Add (Añadir)** y, a continuación, seleccione el certificado de CA para emitir los certificados de servidor de la puerta de enlace. Los

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración del satélite del portal de GlobalProtect	Description (Descripción)
	certificados de CA raíz de confianza del satélite se envían a los endpoints al mismo tiempo que la configuración de agente del portal. *Especifique un CA de raíz de confianza para verificar los certificados de servidor de puerta de enlace y establecer conexiones de túnel VPN seguras con las puertas de enlace de GlobalProtect. Todas las puertas de enlace deberían usar el mismo emisor.* *Puede Import (Importar) o Generate (Generar) a un certificado CA raíz para emitir su certificado de servidor de puerta de enlace si no existe uno en el portal.*
Certificado de cliente	
Local	• **Issuing Certificate (Emisor del certificado)**: seleccione el CA raíz que emite el certificado que el portal utiliza para emitir certificados para un satélite después de que se autentica con éxito. Si el certificado necesario no existe en el cortafuegos, puede **Import (Importar)** o **Generate (Generar)** el certificado. *Si un certificado no está en el cortafuegos, puede importar o generar un certificado de emisión con las opciones Import (Importar) o Generate (Generar).* • **OCSP Responder**: seleccione el respondedor OCSP que deben usar el satélite para verificar el estado de revocación de los certificados presentados por el portal y las puertas de enlace. Seleccione **None (Ninguno)** para indicar que OCSP no se utiliza para verificar la revocación de un certificado. *Habilite un respondedor OCSP satélite para que, si se revoca un certificado, usted reciba una notificación y pueda tomar las medidas apropiadas para establecer una conexión segura con el portal y las puertas de enlace. Para habilitar un respondedor OCSP satélite, también debe habilitar CRL y OCSP en la configuración de Comprobación de revocación de certificado (Device [Dispositivo] > Setup [Configuración] > Session [Sesión] > Decryption Settings [Configuración de descifrado]).* • **Validity Period [Periodo de validez]** (días): especifique la duración del certificado de satélite de GlobalProtect (el intervalo es 7-365; el predeterminado es 7). • **Certificate Renewal Period [Período de renovación del certificado]** (días): especifique el número de días antes del vencimiento en el que el certificado puede automáticamente renovarse (el intervalo es 3-30; el valor predeterminado es 3).

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración del satélite del portal de GlobalProtect	Description (Descripción)
SCEP	• **SCEP**: seleccione un perfil SCEP para generar certificados de cliente. Si el perfil no está en el menú desplegable, puede crear un perfil nuevo en **New (Nuevo)**. • **Certificate Renewal Period [Período de renovación del certificado]** (días): especifique el número de días antes del vencimiento en el que el certificado puede automáticamente renovarse (el intervalo es 3-30; el valor predeterminado es 3).

© 2020 Palo Alto Networks, Inc.

Red > GlobalProtect > Puertas de enlace

Seleccione **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** para configurar una puerta de enlace de GlobalProtect. Una puerta de enlace puede brindar conexiones VPN para las aplicaciones de GlobalProtect o para los satélites de GlobalProtect.

En el cuadro de diálogo Gateways (Puertas de enlace) de GlobalProtect, haga clic en **Add (Añadir)** para añadir una nueva configuración de puerta de enlace o seleccione una existente para modificarla.

¿Qué está buscando?	Consulte:
¿Qué configuración general puedo configurar para la puerta de enlace GlobalProtect?	Pestaña general de Puertas de enlace de GlobalProtect
¿Cómo configuro la autenticación de cliente de la puerta de enlace?	Pestaña Autenticación de Puerta de enlace de GlobalProtect
¿Cómo defino la configuración del túnel y la red que permiten a una aplicación establecer un túnel VPN con la puerta de enlace?	Pestaña Agente de Puertas de enlace de GlobalProtect
¿Cómo defino la configuración del túnel y la red para habilitar los satélites para establecer conexiones VPN con una puerta de enlace que actúa como satélite?	Pestaña Satélite de la puerta de enlace de GlobalProtect
¿Busca más información?	Para obtener instrucciones detalladas sobre cómo configurar el portal, consulte Configuración de las puertas de enlace de GlobalProtect en la guía del administrador de GlobalProtect.

Pestaña general de Puertas de enlace de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **General (General)**

Seleccione la pestaña **General** para definir la interfaz de la puerta de enlace a la que se conectarán las aplicaciones y especificar de qué manera la puerta de enlace autentica los endpoints.

Configuración general de la puerta de enlace de GlobalProtect	Description (Descripción)
Nombre	Introduzca un nombre para la puerta de enlace (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	En el caso de un cortafuegos que esté en modo de Sistema virtual múltiple, **Location (Ubicación)** es el sistema virtual (vsys) en el que la puerta de enlace de GlobalProtect está disponible. En el caso de un cortafuegos que

© 2020 Palo Alto Networks, Inc.

Configuración general de la puerta de enlace de GlobalProtect	Description (Descripción)
	no esté en modo de Sistema virtual múltiple, el campo **Location (Ubicación)** no aparecerá en el cuadro de diálogo Puerta de enlace de GlobalProtect. *Una vez guardada la configuración de la puerta de enlace, no puede cambiar el campo Location (Ubicación).*
Área de configuración de red	
Interface (Interfaz)	Seleccione el nombre de la interfaz de cortafuegos que servirá como la interfaz de salida para los endpoints remotos. (Estas interfaces ya deben existir). *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. Consulte* Prácticas recomendadas de seguridad del acceso administrativo *para obtener información detallada sobre cómo proteger el acceso a su red de gestión.*
Dirección IP	(Opcional) Seleccione la dirección IP para el acceso a la puerta de enlace. Selecciona el **IP Address Type (Tipo de dirección IP)**,luego introduzca la **IP Address (Dirección IP)**. • El tipo de dirección IP puede ser **IPv4** (solo tráfico IPv4), **IPv6** (solo tráfico IPv6), o **IPv4 e IPv6**. Utilice **IPv4 e IPv6** si su red admite dos configuraciones de pila, donde IPv4 y 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 IPv4 o 21DA:D3:0:2F3b para IPv6). Si selecciona **IPv4 e IPv6**, introduzca el tipo de dirección IP apropiado para cada uno.

Pestaña Autenticación de Puerta de enlace de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Authentication (Autenticación)**

Seleccione la pestaña **Authentication (Autenticación)** para identificar el perfil de servicio SSL/TLS y configurar los detalles de la autenticación del cliente. Puede añadir múltiples configuraciones de autenticación de cliente.

Configuración de autenticación de la puerta de enlace de GlobalProtect	
Perfil de servicio SSL/TLS	Seleccione un perfil de servicio SSL/TLS para asegurar esta puerta de enlace GlobalProtect. Para obtener información detallada sobre los contenidos de un perfil de servicio, consulte Device (Dispositivo) > Certificate Management (Gestión de certificados) > SSL/TLS Service Profile (Perfil de servicio de SSL/TLS).

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación de la puerta de enlace de GlobalProtect	
Área de autenticación de cliente	
Nombre	Introduzca un nombre único para identificar esta configuración.
SO	Por defecto, la configuración se aplica a todos los endpoints. Puede restringir la lista de endpoints del cliente por SO (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** o **WindowsUWP**), por dispositivos **Satélites** o por clientes VPN de IPSec de terceros (**X-Auth**). El SO es el diferenciador principal entre configuraciones múltiples. Si necesita múltiples configuraciones para un sistema operativo, puede distinguir las configuraciones por su elección del perfil de autenticación. *Ordene las configuraciones de la más específica en la parte superior de la lista a la más general en la parte inferior.*
Perfil de autenticación	Seleccione un perfil o una secuencia de autenticación del menú desplegable para autenticar el acceso a la puerta de enlace. Consulte Device (Dispositivo) > Authentication Profile (Perfil de autenticación). *Para la autenticación de cliente, asegúrese de que el perfil de autenticación utilice RADIUS o SAML con autenticación de dos factores. Si no utiliza RADIUS o SAML, debe configurar un perfil de certificado además de un perfil de autenticación.*
Username Label (Etiqueta de nombre de usuario)	Especifique una etiqueta de nombre de usuario personalizada para el inicio de sesión a la puerta de enlace de GlobalProtect. Por ejemplo, un **nombre de usuario (únicamente)** o una **dirección de correo electrónico (username@domain)**.
Password Label (Etiqueta de contraseña)	Especifique una etiqueta de contraseña personalizada para el inicio de sesión a la puerta de enlace de GlobalProtect. Por ejemplo, una **contraseña (Turkish)** o un **código de contraseña** (para autenticación basada en token de dos factores).
Mensaje de autenticación	Para ayudar a los usuarios finales a saber qué credenciales deben usar para iniciar sesión en esta puerta de enlace, puede introducir un mensaje o conservar el mensaje predeterminado. El mensaje puede tener un máximo de 256 caracteres.
Permitir autenticación con credencial de usuario O certificado de cliente	Si selecciona **No**, los usuario deberán autenticarse en la puerta de enlace usando credenciales de usuario y certificados de cliente. Si selecciona **Yes (Sí)**, los usuario podrán autenticarse

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación de la puerta de enlace de GlobalProtect	
	en la puerta de enlace usando credenciales de usuario o certificados de cliente.
Perfil del certificado	
Perfil del certificado	(Opcional) Seleccione el **Certificate Profile (Perfil de certificado)** que usa la puerta de enlace para hacer coincidir aquellos certificados de cliente que provienen de los endpoints de usuarios. Con un perfil de certificado, la puerta de enlace autentica al usuario solo si el certificado del cliente coincide con este perfil. Si configura la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credencial de usuario O certificado de cliente)** en **No**, debe seleccionar un **Certificate Profile (Perfil de certificado)**. Si configura la opción **Allow Authentication with User Credentials OR Client Certificate (Permitir autenticación con credencial de usuario O certificado de cliente)** en **Yes (Sí)**, el **Certificate Profile (Perfil de certificado)** es optativo. El perfil del certificado es independiente del SO.

Pestaña Agente de Puertas de enlace de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Portals (Portales de GlobalProtect)** > *<portal-config>* > **Agent (Agente)**

Seleccione la pestaña **Agent (Agente)** para configurar los ajustes de túnel que permiten a la aplicación establecer un túnel de VPN con la puerta de enlace. Además, esta pestaña le permite especificar lo tiempos de espera para las VPN, los servicios de red de DNS y WINS, y los mensajes de notificación HIP para los usuarios finales en la coincidencia o no coincidencia de un perfil HIP adjunto a una regla de política de seguridad.

Configure los parámetros del agente en las siguientes pestañas:

- Pestaña Ajustes de túnel
- Pestaña Configuración de cliente
- Pestaña Grupo de IP de cliente
- Pestaña Servicios de red
- Pestaña Ajustes de conexión
- Pestaña Tráfico de vídeo
- Pestaña Notificación HIP

Pestaña Ajustes de túnel

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Tunnel Settings (Configuración de túnel)**

Seleccione la pestaña **Tunnel Settings (Configuración de túnel)** para habilitar la tunelización y configure los parámetros del túnel.

Los parámetros del túnel son necesarios si configura una puerta de enlace externa. Si configura una puerta de enlace interna, los parámetros del túnel son opcionales.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de modo de túnel de cliente de puerta de enlace de GlobalProtect	Description (Descripción)

Modo de túnel	Seleccione **Tunnel Mode (Modo de túnel)** para activar el modo túnel y especifique los siguientes ajustes:
	• **Tunnel Interface (Interfaz de túnel)**: seleccione la interfaz de túnel para acceder a esta puerta de enlace.
	• **Max User (Usuarios máx.)**: especifique el número máximo de usuarios que pueden acceder a la puerta de enlace simultáneamente para autenticación, actualizaciones HIP y actualizaciones de aplicación de GlobalProtect. Si se alcanza el número máximo de usuarios, se negará el acceso a los usuarios siguientes con un mensaje de error que indica que se ha alcanzado el número máximo de usuarios (el intervalo varía según la plataforma y se muestra cuando el campo está vacío).
	• **Enable IPSec (Habilitar IPSec)**: seleccione esta opción para habilitar el modo IPSec para el tráfico de endpoint, lo que convierte a IPSec en el método principal y a SSL-VPN en el método alternativo. Las opciones restantes no están disponibles hasta que se habilita IPSec.
	• **GlobalProtect IPSec Crypto (Criptográfico de IPSec de GlobalProtect)**: seleccione un perfil criptográfico de IPSec de GlobalProtect que especifique algoritmos de autenticación y cifrado para los túneles de VPN. El perfil **default (predeterminado)** utiliza un cifrado AES-128-CBC y una autenticación SHA1. Para obtener más información, consulte Red > Perfiles de red > Criptográfico IPSec de GlobalProtect.
	• **Enable X-Auth Support (Habilitar compatibilidad con X-Auth)**: seleccione esta opción para activar la compatibilidad con Extended Authentication (X-Auth) en la puerta de enlace de GlobalProtect cuando se activa IPSec. Con la compatibilidad de X-Auth, los clientes externos de VPN de IPSec compatibles con X-Auth (como el cliente VPN de IPSec en dispositivos Apple iOS y Android y el cliente VPNC en Linux) pueden establecer un túnel VPN con la puerta de enlace de GlobalProtect. La opción X-Auth proporciona acceso remoto desde el cliente VPN a una puerta de enlace de GlobalProtect específica. Como el acceso de X-Auth proporciona funciones de GlobalProtect limitadas, considere el uso de la aplicación de GlobalProtect para un acceso simplificado a todo el conjunto de funciones de seguridad que proporciona GlobalProtect en dispositivos iOS y Android.
	Seleccionar la casilla de verificación de **X-Auth Support (Compatibilidad con X-Auth)** activa las opciones **Group Name (Nombre de grupo)** y **Group Password (Contraseña de grupo)**:
	  • Si se especifica el nombre de grupo y la contraseña de grupo, la primera fase de autenticación requiere ambas informaciones para utilizar esta credencial para autenticar. La segunda fase requiere una contraseña y un nombre de usuario válidos, que se comprobarán mediante el perfil de autenticación configurado en la sección Autenticación.
	  • Si no se definen un nombre de grupo y una contraseña de grupo, la primera fase de autenticación se basa en un certificado válido presentado por el cliente de VPN externo. Este certificado se valida

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de modo de túnel de cliente de puerta de enlace de GlobalProtect	Description (Descripción)
	después a través del perfil de certificado configurado en la sección de autenticación. • De forma predeterminada, no es necesario que el usuario vuelva a autenticarse cuando caduque la clave utilizada para establecer el túnel de IPSec. Para volver a solicitar la autenticación, borre la opción **Skip Auth on IKE Rekey (Saltar autenticación de clave de registro de IKE)**.

Pestaña Configuración de cliente

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Client Settings (Configuración del cliente)**

Seleccione la pestaña **Client Settings (Configuración del cliente)** para configurar los ajustes del adaptador de red virtual en el endpoint cuando la aplicación de GlobalProtect establezca un túnel con la puerta de enlace.

Algunas opciones de la Configuración de cliente están disponibles solo después de que habilite el modo túnel y defina una interfaz de túnel en la Pestaña Ajustes de túnel *.*

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
Pestaña Config Selection Criteria (criterios de selección de configuración)	
Nombre	Introduzca un nombre para identificar la configuración de opciones del cliente (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Source User (Usuario de origen)	Seleccione **Add (Añadir)** para añadir usuarios o grupos de usuarios específicos a los cuales se aplica esta configuración. *Debe configurar la asignación de grupo (Device [Dispositivo] > User Identification [Identificación de usuarios] > Group Mapping Settings [Configuración de asignación de grupos]) antes de que pueda seleccionar los grupos y usuarios.* Para implementar esta configuración en todos los usuarios, seleccione **any (cualquiera)** en la lista desplegable **Source User (Usuario de origen)**. Para implementar esta configuración únicamente en los usuarios con aplicaciones GlobalProtect en el modo previo al inicio de sesión, seleccione **pre-logon (anterior al inicio de sesión)** en la lista desplegable **Source User (Usuario de origen)**.

© 2020 Palo Alto Networks, Inc.

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
	La configuración de ajustes del cliente se implementa en los usuarios únicamente si el usuario coincide con los criterios para Source User (Usuario de origen), OS (Sistema operativo) Y Source Address (Dirección de origen).
SO	Para implementar esta configuración en función del sistema operativo del endpoint, **añada** un SO (**Android**, **Chrome**, **iOS**, **IoT**, **Linux**, **Mac**, **Windows** o **WindowsUWP**). De manera alternativa, puede dejar este valor configurado en **Any (Cualquiera)** para que la implementación de la configuración se base únicamente en el usuario o grupo de usuarios, y no en el sistema operativo del endpoint. *La configuración de ajustes del cliente se implementa en los usuarios únicamente si el usuario coincide con los criterios para Source User (Usuario de origen), OS (Sistema operativo) Y Source Address (Dirección de origen).*
Dirección de origen	Para implementar esta configuración en función de la ubicación del usuario, seleccione **Add (Añadir)** para añadir una **Region (Región)** de origen o una **IP Address (Dirección IP)** local (IPv4 y IPv6). Para implementar esta configuración en todas las ubicaciones de usuario, no especifique una **región** ni una **dirección IP**. También debe dejar estos campos en blanco si sus usuarios ejecutan una aplicación GlobalProtect 4.0 y versiones anteriores, ya que esta función no es compatible con las versiones anteriores de GlobalProtect. *La coincidencia de Source Address (Dirección de origen) es correcta si la ubicación del usuario que se conecta coincide con la región o la dirección IP que usted configuró.* *La configuración de ajustes del cliente se implementa en los usuarios únicamente si el usuario coincide con los criterios para Source User (Usuario de origen), OS (Sistema operativo) Y Source Address (Dirección de origen).*
Pestaña de anulación de autenticación	
Cancelación de autenticación	Habilite la puerta de enlace para usar cookies seguras, cifradas y específicas para el dispositivo con el fin de autenticar el usuario después de que este autentica primero usando el

© 2020 Palo Alto Networks, Inc.

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
	esquema de autenticación especificado por la autenticación o perfil de certificado. • **Generate cookie for authentication override (Generar cookie para anulación de autenticación)**: durante la duración de la cookie, el agente presenta esta cookie cada vez que el usuario se autentica con la puerta de enlace. • **Cookie Lifetime (Duración de la cookie)**: especifique las horas, los días o las semanas que la cookie será válida. El vencimiento normal es 24 horas. Los intervalos son 1–72 horas, 1–52 semanas o 1–365 días. Después de que expire la cookie, el usuario debe introducir las credenciales de inicio de sesión y el portal consecuentemente cifra una nueva cookie para enviarla al dispositivo del usuario. • **Accept cookie for authentication override (Aceptar cookie para anulación de autenticación)**: seleccione esta opción para configurar la puerta de enlace y aceptar la autenticación mediante la cookie cifrada. Cuando el agente presente la cookie, la puerta de enlace valida que la cookie fue cifrada por la puerta de enlace antes de autenticar al usuario. • **Certificate to Encrypt/Decrypt Cookie (Certificado para cifrar/descifrar cookie)**: seleccione el certificado que la puerta de enlace usa para usar al cifrar y descifrar la cookie. *Asegúrese de que la puerta de enlace y el portal usan el mismo certificado para cifrar y descifrar cookies.*
Pestaña IP Pools	
Recuperar atributo de dirección IP entramada desde el servidor de autenticación	Seleccione esta opción para permitir que la puerta de enlace de GlobalProtect asigne direcciones IP fijas mediante un servidor de autenticación externo. Cuando esta opción está habilitada, la puerta de enlace de GlobalProtect asigna la dirección IP a dispositivos que se estén conectando mediante el atributo IP entramada del servidor de autenticación.
Grupo de IP de servidores de autenticación	Seleccione **Add (Añadir)** para crear una subred o un intervalo de direcciones IP que se asignarán a los usuarios remotos. Cuando el túnel esté establecido, la puerta de enlace de GlobalProtect asignará la dirección IP de este intervalo a dispositivos que se estén conectando mediante el atributo IP entramada del servidor de autenticación. Puede añadir direcciones IPv4 (como 192.168.74.0/24 y 192.168.75.1-192.168.75.100) o direcciones IPv6 (como 2001:aa::1-2001:aa::10). Puede habilitar y configurar **Authentication Server IP Pool (Grupo de IP de servidores de autenticación)** solo si habilita **Retrieve Framed-IP-Address attribute from authentication**

© 2020 Palo Alto Networks, Inc.

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
	server (Recuperar atributo de dirección IP entramada desde el servidor de autenticación). *El grupo de IP de servidores de autenticación debe ser lo suficientemente grande para abarcar todas las conexiones actuales. La asignación de dirección IP es fija y se mantiene cuando se desconecta el usuario. La configuración de varias gamas de diferentes subredes permitirá al sistema ofrecer a los clientes una dirección IP que no entra en conflicto con otras interfaces en el cliente.* Los servidores y enrutadores en las redes debe dirigir el tráfico para este grupo de IP en el cortafuegos. Por ejemplo, para la red 192.168.0.0/16, un usuario remoto puede recibir la dirección 192.168.0.10.
Grupo de IP	Seleccione **Add (Añadir)** para crear un intervalo de direcciones IP que se asignarán a los usuarios remotos. Cuando se establece el túnel, se crea una interfaz en el endpoint del usuario remoto con una dirección de esta rango. Puede añadir direcciones IPv4 (como 192.168.74.0/24 y 192.168.75.1-192.168.75.100) o direcciones IPv6 (como 2001:aa::1-2001:aa::10). *Para evitar conflictos, el grupo de IP debe ser lo suficientemente grande para abarcar todas las conexiones actuales. La puerta de enlace mantiene un índice de clientes y direcciones IP para que el cliente reciba automáticamente la misma dirección IP la próxima vez que se conecte. La configuración de varias gamas de diferentes subredes permitirá al sistema ofrecer a los clientes una dirección IP que no entra en conflicto con otras interfaces en el cliente.* Los servidores y enrutadores en las redes debe dirigir el tráfico para este grupo de IP en el cortafuegos. Por ejemplo, para la red 192.168.0.0/16, se puede asignar la dirección 192.168.0.10 a un usuario remoto.
Pestaña Split Tunnel	
Pestaña de rutas de acceso	
No direct access to local network (Sin acceso directo a la red local)	Seleccione esta opción para deshabilitar los túneles divididos, que incluye el acceso directo a las redes locales en endpoints Windows y Mac OS. Esta función evita que los usuarios envíen tráfico a proxies o recursos locales, como una impresora

© 2020 Palo Alto Networks, Inc.

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
	doméstica. Cuando el túnel esté establecido, todo el tráfico se enrutará a través del túnel y estará sujeto a la aplicación de la política por parte del cortafuegos.
Incluir	**Add (Añadir)** rutas para incluir en el túnel VPN. Estas son las rutas que la puerta de enlace empuja al endpoint de los usuarios remotos para especificar qué endpoints de usuario se pueden enviar a través de la conexión VPN. *Para incluir todas las subredes de destino o todos los objetos de dirección, seleccione Include (Incluir) para incluir 0.0.0.0/0 y ::/0 como rutas de acceso.*
Excluir	**Add (Añadir)** rutas para excluirlas del túnel VPN. Estas rutas se envían a través del adaptador físico en los endpoints en lugar de a través del adaptador virtual (el túnel). Puede definir las rutas que envía a través del túnel VPN como rutas que incluye en el túnel, las rutas que excluye del túnel o una combinación de ambas. Por ejemplo, puede establecer túneles divididos para permitir a los usuarios remotos acceder a internet sin pasar por el túnel de VPN. Las rutas excluidas deben ser más específicas que las rutas incluidas para evitar excluir más tráfico del que se pretende excluir. Si no se incluye o excluye rutas, todas las solicitudes se dirigirán a través del túnel (sin división de túneles). En este caso, cada solicitud de internet pasa a través del cortafuegos y luego a la red. Éste método puede evitar la posibilidad de acceso a los endpoints del usuario por parte de terceros externos y por lo tanto la obtención de acceso a la red interna (utilizando el endpoint de usuario como puente).
Pestaña Domain and Application (Dominio y aplicación)	
Include Domain (Incluir dominio)	Añada las aplicaciones de software como servicio (software as a service, SaaS) o de nube pública que desea incluir en el túnel VPN utilizando el dominio y el puerto (opcional). Estas son las aplicaciones que la puerta de enlace envía al endpoint de los usuarios remotos para especificar qué endpoints de usuario se pueden enviar a través de la conexión VPN. *Puede configurar una lista de puertos para cada dominio. Si no se configuran puertos, todos los puertos del dominio especificado están sujetos a esta política.*
Exclude Domain (Excluir dominio)	Añada las aplicaciones de software como servicio (software as a service, SaaS) o de nube pública que desea excluir del túnel VPN utilizando el dominio y el puerto (opcional). Estas

© 2020 Palo Alto Networks, Inc.

Configuración de red y opciones del cliente de puerta de enlace GlobalProtect	Description (Descripción)
	aplicaciones se envían a través del adaptador físico en los endpoints en lugar de a través del adaptador virtual (el túnel). *Puede configurar una lista de puertos para cada dominio. Si no se configuran puertos, todos los puertos del dominio especificado están sujetos a esta política.* Si no incluye ni excluye dominios, todas las solicitudes se dirigirán a través del túnel (sin división de túneles). En este caso, cada solicitud de internet pasa a través del cortafuegos y luego a la red. Este método puede evitar que terceros accedan a endpoints del usuarios con el fin de obtener acceso a la red interna.
Include Client Application Process Name (Incluir nombre de proceso de la aplicación cliente)	Añada las aplicaciones de software como servicio (software as a service, SaaS) o de nube pública que desea incluir en el túnel VPN utilizando el nombre de proceso de la aplicación. Estas son las aplicaciones que la puerta de enlace envía al endpoint de los usuarios remotos para especificar qué endpoints de usuario se pueden enviar a través de la conexión VPN.
Exclude Client Application Process Name (Excluir nombre de proceso de la aplicación cliente)	Añada las aplicaciones de software como servicio (software as a service, SaaS) o de nube pública que desea excluir del túnel VPN utilizando el nombre de proceso de la aplicación. Estas aplicaciones se envían a través del adaptador físico en los endpoints en lugar de a través del adaptador virtual (el túnel). Si no incluye ni excluye aplicaciones, todas las solicitudes se dirigirán a través del túnel (sin división de túneles). En este caso, cada solicitud de internet pasa a través del cortafuegos y luego a la red. Este método puede evitar que terceros accedan a endpoints del usuarios con el fin de obtener acceso a la red interna.
Pestaña Network Services (Servicios de red)	
Servidor DNS	Especifique la dirección IP en el servidor DNS al que enviará las consultas DNS la aplicación de GlobalProtect con esta configuración de cliente. Puede añadir varios servidores DNS separando cada dirección IP con una coma.
Sufijo DNS	Especifique el sufijo DNS que el endpoint debe utilizar de forma local cuando se introduce un nombre de host sin restricciones que el endpoint no puede resolver. Para introducir varios sufijos DNS (hasta 100), sepárelos con una coma.

© 2020 Palo Alto Networks, Inc.

Pestaña Grupo de IP de cliente

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Client IP Pool (Grupo de IP del cliente)**

Seleccione la pestaña **Client IP Pool (Grupo de IP del cliente)** para configurar el grupo de IP global que se utiliza para asignar direcciones IPv4 o IPv6 a todos los endpoints que se conectan a la puerta de enlace de GlobalProtect™.

Ajustes de configuración del grupo de IP del cliente de la puerta de enlace de GlobalProtect	Description (Descripción)
Grupo de IP	Seleccione **Add (Añadir)** para crear un intervalo de direcciones IPv4 o IPv6 que se asignarán a los usuarios remotos. Tras establecer el túnel, la puerta de enlace de GlobalProtect asigna direcciones IP en este intervalo a todos los endpoints que se conectan a través de ese túnel. *Si configura grupos IP en el nivel de la puerta de enlace (Network [Red] > GlobalProtect > Gateways [Puerta de enlace] > <gateway-config> > GlobalProtect Gateway Configuration [Configuración de puerta de enlace de GlobalProtect] > Agent [Agente] > Client IP Pool [Grupo de IP de cliente]), no configure grupos IP en el nivel del cliente (Network [Red] > GlobalProtect > Gateways [Puerta de enlace] > <gateway-config> > GlobalProtect Gateway Configuration [Configuración de puerta de enlace de GlobalProtect] > Agent [Agente] > Client Settings [Configuración de cliente] > <client-setting> > Configs [Configuración] > IP Pools [Grupos IP]).*

Pestaña Servicios de red

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Network Services (Servicios de red)**

Seleccione la pestaña **Network Services (Servicios de red)** para configurar los ajustes DNS que se asignarán al adaptador de red virtual en el endpoint cuando la aplicación de GlobalProtect establezca un túnel con la puerta de enlace.

Las opciones de Network Services (Servicios de red) solamente están disponibles si ha habilitado el modo de túnel y ha definido una interfaz de túnel en la pestaña Tunnel Settings*.*

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de servicios de red de cliente de puerta de enlace de GlobalProtect	Description (Descripción)
Origen de herencia	Seleccione un origen para propagar un servidor DNS y otras configuraciones desde la interfaz del cliente DHCP o PPPoE seleccionados en la configuración de la aplicación de GlobalProtect. Con esta configuración, se heredan todas las configuraciones de red del cliente, como servidores DNS y servidores WINS, de la configuración de la interfaz seleccionada en el Origen de herencia.
Comprobar estado de origen de herencia	Haga clic Inheritance Source para ver la configuración del servidor asignada actualmente a las interfaces del cliente.
DNS principal DNS secundario	Introduzca las direcciones IP de los servidores principal y secundario que proporcionan DNS a los clientes.
WINS principal WINS secundario	Introduzca las direcciones IP de los servidores principal y secundario que proporciona el Servicio de nombres de internet de Windows (Windows Internet Naming Service, WINS) a los endpoints.
Heredar sufijos DNS	Seleccione esta opción para heredar los sufijos de DNS del origen de herencia.
Sufijo DNS	Haga clic en **Add (Añadir)** para añadir un sufijo que el endpoint pueda utilizar de forma local cuando se introduce un nombre de host no calificado que no puede resolver. Puede introducir múltiples sufijos (hasta 100) separándolos con comas.

Pestaña Ajustes de conexión

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Connection Settings (Configuración de conexiones)**

Seleccione la pestaña **Connection Settings (Configuración de conexiones)** para definir los ajustes de tiempo de espera y las restricciones de uso de cookies de autenticación para la aplicación de GlobalProtect™.

Ajustes de conexión del modo túnel del cliente de la puerta de enlace de GlobalProtect	Description (Descripción)
Configuración de tiempo de espera	
Duración de inicio de sesión	Especifique el número de días, horas o minutos permitido para una sesión de inicio de sesión de puerta de enlace única.
Cierre de sesión por inactividad	Especifique el número de días, horas y minutos tras el que se cierra automáticamente una sesión inactiva.

© 2020 Palo Alto Networks, Inc.

Ajustes de conexión del modo túnel del cliente de la puerta de enlace de GlobalProtect	Description (Descripción)
Disconnect on Idle (Desconectar cuando esté inactivo)	Especifique la cantidad de tiempo (en minutos) antes de que se cierre la sesión de un endpoint en la aplicación de GlobalProtect después de que la aplicación deja de enrutar tráfico a través del túnel de VPN.
Restricciones de uso de cookies de autenticación	
Disable Automatic Restoration of SSL VPN (Deshabilitar la restauración automática de la VPN SSL)	Habilite esta opción para evitar la restauración automática de los túneles de VPN SSL. *Si habilita esta opción, GlobalProtect no admitirá la VPN resiliente.*
Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) to (Restringir uso de cookies de autenticación [para la restauración automática del túnel de VPN o la cancelación de la autenticación] para)	Habilite esta opción para restringir el uso de las cookies de autenticación en función de una de las siguientes condiciones: • **The original Source IP for which the authentication cookie was issued (IP original para la cual se emitió las cookies de autenticación)**: restringe el uso de la cookie de autenticación a los endpoints con la misma dirección IP de origen público del endpoint para el cual la cookie se emitió en un principio. • **The original Source IP network range (Intervalo de red IP original)**: restringe el uso de las cookies de autenticación a los endpoints con direcciones IP de origen público dentro del intervalo de direcciones IP de red designadas. Introduzca una **Source IPv4 Netmask (Máscara de red IPv4 de origen)** para especificar un intervalo de direcciones IPv4 o introduzca una **Source IPv6 Netmask (Máscara de red IPv6 de origen)** para especificar un intervalo de direcciones IPv6. Si configura una máscara de red en `0`, esta opción estará deshabilitada para el tipo de dirección IP especificada. Por ejemplo, puede configurar una máscara de red en `0` si su portal o puerta de enlace admiten solo un tipo de dirección IP (IPv4 o IPv6), o si desea habilitar esta opción únicamente para un tipo de dirección IP (cuando su portal o puerta de enlace admiten IPv4 e IPv6). Puede configurar únicamente una máscara de red en `0` en una configuración de puerta de enlace dada; no puede configurar simultáneamente ambas máscaras de red en `0`. Si acepta el valor predeterminado de **Source IPv4 Netmask (Máscara de red IPv4 de origen)** de `32`, el uso de la cookie de autenticación se restringe a la misma dirección IPv4 pública del endpoint para el cual la cookie se emitió en primer lugar. Si acepta el valor predeterminado de **Source IPv6 Netmask (Máscara de red IPv6 de origen)** de `128`, el uso de la cookie de autenticación se restringe a la misma dirección IPv4 pública del endpoint para el cual la cookie se emitió en primer lugar.

Pestaña Tráfico de vídeo

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **Video Traffic (Tráfico de vídeo)**

© 2020 Palo Alto Networks, Inc.

Seleccione la pestaña **Video Traffic (Tráfico de vídeo)** para excluir el tráfico de transmisión de vídeo del túnel VPN.

Ajustes de configuración de tráfico de vídeos de puerta de enlace de GlobalProtect	Description (Descripción)
Excluir aplicaciones de vídeo del túnel	Seleccione esta opción para permitir el tráfico de transmisión de vídeo para que se excluya del túnel de VPN.
applications	Haga clic en **Add (Añadir)** o **Browse (Explorar)** para añadir o explorar las aplicaciones de transmisión de vídeo que desea excluir del túnel de VPN. El redireccionamiento de este vídeo se aplica a cualquier tipo de tráfico de vídeo de las siguientes aplicaciones: • Youtube • Dailymotion • Netflix En el caso de las otras aplicaciones de transmisión de vídeo, solo los siguientes tipos de vídeos se pueden redireccionar: • MP4 • WebM • MPEG El tráfico de transmisión de vídeo solo puede excluirse del túnel de VPN. Si no excluye aplicaciones de transmisión de vídeo, todas las solicitudes se envían a través del túnel (sin túnel dividido). En este caso, cada solicitud de internet pasa a través del cortafuegos y luego a la red. Este método puede evitar que terceros accedan a endpoints del usuarios con el fin de obtener acceso a la red interna.

Pestaña Notificación HIP

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Agent (Agente)** > *<agent-config>* > **HIP Notification (Notificación HIP)**

Seleccione la pestaña **HIP Notification (Notificación HIP)** para definir los mensajes de notificación que verán los usuarios finales cuando se aplique una regla de seguridad con un perfil de información de host (HIP).

Estas opciones están disponibles solo si creó perfiles HIP y los agregó a sus políticas de seguridad.

Configuración de las notificaciones HIP de agente de GlobalProtect	Description (Descripción)
Notificación HIP	Haga clic en **Add (Añadir)** para añadir notificaciones HIP y configurar las opciones. Puede habilitar las notificaciones con **Enable (Habilitar)** en el campo **Match Message (Coincidir mensaje)**, **Not Match Message (No coincidir mensaje)** o ambos, y luego indicar en **Show Notification As**

© 2020 Palo Alto Networks, Inc.

Configuración de las notificaciones HIP de agente de GlobalProtect	Description (Descripción)
	(Mostrar notificación como) si desea mostrar las notificaciones como **System Tray Balloon (Icono en la barra de tareas)** o **Pop Up Message (Mensaje emergente)**. Luego especifique el mensaje para coincidir o no coincidir. Utilice esta configuración para notificar al usuario final el estado de la máquina, por ejemplo, para proporcionar un mensaje de advertencia que indica que el sistema host no tiene la aplicación necesaria instalada. En el caso de la opción Match Message (Coincidir mensaje), también puede habilitar la opción **Include Mobile App List (Incluir lista de aplicaciones móviles)** para indicar qué aplicaciones activan la coincidencia HIP. *Los mensajes de notificación HIP pueden tener el formato HTML enriquecido, que puede incluir enlaces a recursos y sitios web externos. Haga clic en el hipervínculo en la barra de herramientas de configuración de texto enriquecido para añadir enlaces.*

Pestaña Satélite de la puerta de enlace de GlobalProtect

- **Network (Red)** > **GlobalProtect** > **Gateways (Puertas de enlace)** > *<gateway-config>* > **Satellite (Satélite)**

Un satélite es un cortafuegos de Palo Alto Networks (tradicionalmente, en una sucursal) que actúa como una aplicación de GlobalProtect para permitir que establezca conectividad de VPN con una puerta de enlace de GlobalProtect. Seleccione la pestaña **Satellite (Satélite)** para definir la configuración del túnel de la puerta de enlace y de la red para permitir que los dispositivos satélite establezcan conexiones VPN con él. También puede configurar las rutas anunciadas por los satélites.

- Pestaña Ajustes de túnel
- Pestaña Configuración de red
- Pestaña Filtro de ruta

Ajustes de configuración de satélite de puerta de enlace de GlobalProtect	Description (Descripción)
Pestaña Ajustes de túnel	
Configuración de túnel	Seleccione **Tunnel Configuration (Configuración de túnel)** y luego una interfaz de túnel existente en **Tunnel Interface (Interfaz de túnel)** o una nueva en **New Tunnel Interface (Nueva interfaz de túnel)** desde el menú desplegable. Para más información, consulte **Network > Interfaces > Tunnel** • **Replay attack detection (Detección de reproducción de ataques)**: protege frente a la reproducción de ataques. *Habilite Replay attack detection (Detección de ataque de reproducción) para proteger los dispositivos satélites de GlobalProtect contra los ataques de reproducción, si habilita la configuración del túnel del satélite.*

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de satélite de puerta de enlace de GlobalProtect	Description (Descripción)
	• **Copy TOS (Copiar TOS)**: copie el encabezado de Tipo de servicio (Type of Services, ToS) desde el encabezado IP interno en el encabezado IP externo de los paquetes resumidos con el fin de preservar la información original de ToS. • **Configuration Refresh Interval (hours) [Intervalo de actualización de la configuración (horas)]**: especifique la frecuencia con la que los satélites deben comprobar el portal para obtener actualizaciones de la configuración (el intervalo es 1-48, el predeterminado es 2).
Monitorización de túnel	Seleccione **Tunnel Monitoring (Supervisión de túnel)** para habilitar los satélites 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. • **Destination Address (Dirección de destino)**: especifique una dirección **IPv4** o **IPv6** que utilizará el supervisor de túnel para determinar si hay conectividad a la puerta de enlace (por ejemplo, una dirección IP en la red protegida por la puerta de enlace). 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. • **Tunnel Monitor Profile (Perfil de monitor de túnel):Failover (Conmutación por error)** en la conmutación por error a otra puerta de enlace es el único tipo de perfil de monitorización de túnel permitido con LSVPN. *Habilite Tunnel Monitoring (Supervisión de túnel) y configure un* Perfil de supervisión de túnel *para controlar la acción de conmutación por error si habilita la configuración del túnel del satélite.*
Perfiles criptográficos	Seleccione un **IPSec Crypto Profile (Perfil criptográfico IPSec)** o cree uno nuevo. Un perfil criptográfico determinará los protocolos y algoritmos para la identificación, la autenticación y el cifrado de los túneles de VPN. Dado que ambos endpoints del túnel de una LSVPN son cortafuegos fiables de su organización, por lo general utiliza el perfil predeterminado, que utiliza el protocolo ESP, el grupo DH 2, el cifrado AES 128 CVC y la autenticación SHA-1. Para más información, consulte Red> Perfiles de red> GlobalProtect IPSec Crypto.
Pestaña Configuración de red	
Origen de herencia	Seleccione un origen para propagar un servidor DNS y otras configuraciones desde el cliente DHCP o cliente PPPoE seleccionados en la configuración del satélite de GlobalProtect. Con esta configuración, se heredan todas las configuraciones de red, como servidores DNS, de la configuración de la interfaz seleccionada en el Origen de herencia.
DNS principal DNS secundario	Introduzca las direcciones IP de los servidores principal y secundario que proporcionan DNS a los satélites.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de satélite de puerta de enlace de GlobalProtect	Description (Descripción)
Sufijo DNS	Haga clic en **Add (Añadir)** para introducir un sufijo que el satélite puede utilizar de forma local cuando se introduce un nombre de host sin restricciones que no puede resolver. Puede introducir varios sufijos separándolos con comas.
Heredar sufijo DNS	Seleccione esta opción para enviar el sufijo de DNS a los satélites para uso local cuando se introduce un nombre de host sin restricciones que no puede resolver.
Grupo de IP	Seleccione **Add (Añadir)**para crear un rango de direcciones IP que se pueden asignar a la interfaz del túnel en los satélites al establecer el túnel VPN. Puede especificar direcciones IPv6 o IPv4. *El grupo de IP debe ser lo suficientemente grande para abarcar todas las conexiones actuales. La asignación de dirección IP es dinámica y no se mantiene cuando se desconecta el satélite. La configuración de varias gamas de diferentes subredes permitirá al sistema ofrecer a los satélites una dirección IP que no entra en conflicto con otras interfaces en los satélites.* Los servidores y enrutadores en las redes debe dirigir el tráfico para este grupo de IP en el cortafuegos. Por ejemplo, para la red 192.168.0.0/16, se puede asignar la dirección 192.168.0.10 a un satélite. Si está utilizando el enrutamiento dinámico, asegúrese de que el grupo de direcciones IP que designe a los satélites no se solape con las direcciones IP que asignó manualmente a las interfaces de túnel de sus puertas de enlace y satélites.
Acceder a ruta	Haga clic en **Add (Añadir)** y, a continuación, introduzca las rutas de la siguiente forma: • Si desea enrutar todo el tráfico desde los satélites a través del túnel, deje este campo en blanco. • 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 enruta el tráfico no destinado a una ruta de acceso especificada mediante su propia tabla de rutas. Por ejemplo, puede seleccionar 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.
Pestaña Filtro de ruta	
Aceptar las rutas publicadas	Active **Accept published routes (Aceptar rutas publicadas)** para aceptar rutas publicadas por el satélite en la tabla de ruta de la puerta de enlace.

© 2020 Palo Alto Networks, Inc.

Ajustes de configuración de satélite de puerta de enlace de GlobalProtect	Description (Descripción)
	Si no selecciona esta opción, la puerta de enlace no aceptará ninguna ruta publicada por los satélites.
Subredes permitidas	Si desea ser más restrictivo al aceptar rutas publicadas por los satélites, haga clic en **Add (Añadir)** en la sección de subredes permitidas y defina las subredes cuyas rutas pueden aceptar la puerta de enlace; las subredes publicadas por los satélites que no sean parte de la lista no pasarán el filtro. Por ejemplo, si todos los satélites están configurados con la subred 192.168.x.0/24 en la LAN, puede permitir la ruta 192.168.0.0/16 en la puerta de enlace. De esta forma, la puerta de enlace solo aceptará las rutas del satélite que estén en la subred 192.168.0.0/16.

© 2020 Palo Alto Networks, Inc.

Red > GlobalProtect > MDM

Si utiliza un gestor de seguridad móvil para gestionar endpoints móviles de usuario final y además aplica las políticas habilitadas para HIP, debe configurar la puerta de enlace para comunicarse con el gestor de seguridad móvil si desea recuperar los informes HIP para los endpoints gestionados.

Haga clic en **Add (Añadir)** para añadir información de MDM para que Mobile Security Manager permita que la puerta de enlace se comunique con Mobile Security Manager.

Configuración de MDM en GlobalProtect	Description (Descripción)
Nombre	Introduzca un nombre para Mobile Security Manager (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
	En el caso de un cortafuegos que esté en modo de sistema virtual múltiple, la configuración de MDM mostrará los sistemas virtuales (vsys) donde el gestor de seguridad móvil está disponible. En el caso de un cortafuegos que no esté en modo vsys múltiple, este campo no aparecerá en el cuadro de diálogo de MDM. Una vez guardado el gestor de seguridad móvil, no puede cambiar su ubicación.
Configuración de conexión	
Servidor	Introduzca la dirección IP o FQDN de la interfaz en el gestor de seguridad móvil donde la puerta de enlace se conecta para recuperar informes HIP. Asegúrese de contar con una ruta de servicio a esta interfaz.
Puerto de conexión	El puerto de conexión es donde el gestor de seguridad móvil escucha las solicitudes de informes HIP. El puerto predeterminado es 5008, es el mismo puerto en el que se escucha el gestor de seguridad móvil de GlobalProtect. Si utiliza un gestor de seguridad móvil de terceros, introduzca el número de puerto en el que escucha las solicitudes de informe HIP ese servidor.
Certificado de cliente	Seleccione el certificado de cliente que debe presentar la puerta de enlace al gestor de seguridad móvil al establecer una conexión HTTPS. Este certificado solo es necesario si el gestor de seguridad móvil se configura para utilizar autenticación mutua.
CA raíz de confianza	Haga clic en **Add (Añadir)** y seleccione el certificado de CA raíz que se usó para emitir el certificado para la interfaz a la que se conecta la puerta de enlace para recuperar los informes HIP. (Este certificado de servidor puede ser diferente del certificado emitido para la interfaz de registro del endpoint en el gestor de seguridad móvil). Debe importar el certificado de CA raíz y agregarlo a esta lista.

© 2020 Palo Alto Networks, Inc.

Network > GlobalProtect > Device Block List

Seleccione **Network (Red)** > **GlobalProtect** > **Device Block List (Lista de bloqueo de dispositivos)** (solo cortafuegos) para añadir endpoints a la lista de dispositivos bloqueados de GlobalProtect. No está permitido que los endpoints de esta lista establezcan una conexión VPN con GlobalProtect.

Configuración de Device Block List	Description (Descripción)
Nombre	Introduzca un nombre para la lista de bloqueos dinámicos (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	En el caso de un cortafuegos que esté en modo de Sistema virtual múltiple, **Location (Ubicación)** es el sistema virtual (vsys) en el que la puerta de enlace de GlobalProtect está disponible. En el caso de un cortafuegos que no esté en modo de Sistema virtual múltiple, el campo **Location (Ubicación)** no aparecerá en el cuadro de diálogo Puerta de enlace de GlobalProtect. Una vez guardada la configuración de la puerta de enlace, no puede cambiar el campo **Location (Ubicación)**.
ID de host	Ingrese el ID único que identifica al endpoint, una combinación de nombre de host e ID de dispositivo única. Para cada ID de host, especifique el nombre de host correspondiente.
Nombre de host	Introduzca un nombre de host para identificar el dispositivo (de hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.

© 2020 Palo Alto Networks, Inc.

Red> GlobalProtect> Aplicaciones sin cliente

Seleccione **Network (Red)** > **GlobalProtect** > **Clientless Apps (Aplicaciones sin cliente)** para añadir aplicaciones accesibles a través de la VPN de GlobalProtect sin clientes. Puede añadir aplicaciones individuales sin cliente y, luego, seleccionar **Network (Red)** > **GlobalProtect** > **Clientless App Groups (Grupos de aplicaciones sin cliente)** para definir los grupos de aplicaciones.

GlobalProtect Clientless VPN proporciona acceso remoto seguro a aplicaciones web empresariales comunes que utilizan tecnología HTML, HTML5 y JavaScript. Los usuarios tienen la ventaja de un acceso seguro desde los navegadores web habilitados para SSL sin instalar el software de GlobalProtect. Resulta útil cuando necesita habilitar el acceso de socios o contratistas a aplicaciones y habilitar de forma segura activos no gestionados, como los dispositivos personales.

Necesita las actualizaciones dinámicas de **GlobalProtect Clientless VPN (VPN sin cliente de GlobalProtect)** para usar esta función. Esta función también requiere instalar una suscripción de GlobalProtect en el cortafuegos que aloje la VPN sin cliente desde el portal de GlobalProtect.

Configuración de aplicaciones sin cliente	Description (Descripción)
Nombre	Introduzca un nombre descriptivo para la aplicación (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Ubicación	En el caso de un cortafuegos que esté en modo de Sistema virtual múltiple, **Location (Ubicación)** es el sistema virtual (vsys) en el que la puerta de enlace de GlobalProtect está disponible. En el caso de un cortafuegos que no esté en modo de Sistema virtual múltiple, el campo **Location (Ubicación)** no aparecerá en el cuadro de diálogo Puerta de enlace de GlobalProtect. Una vez guardada la configuración de la puerta de enlace, no puede cambiar el campo **Location (Ubicación)**.
URL de inicio de la aplicación	Introduzca la dirección URL en la que se encuentra la aplicación (hasta 4095 caracteres).
Descripción de la aplicación	(Opcional) Introduzca una descripción de la aplicación (hasta 255 caracteres). Utilice solamente letras, números, espacios, guiones y guiones bajos.
Icono de aplicación	(Opcional) Cargue un icono para identificar la aplicación en la página de la aplicación publicada. Puede examinar el contenido del disco para cargar el icono.

© 2020 Palo Alto Networks, Inc.

Red> GlobalProtect> Grupos de aplicaciones sin cliente

Seleccione **Network (Red)** > **GlobalProtect** > **Clientless App Groups (Grupos de aplicaciones sin cliente)** para agrupar las aplicaciones accesibles a través de la VPN GlobalProtect sin cliente. Puede añadir aplicaciones sin cliente existentes a un grupo o configurar nuevas aplicaciones sin clientes para el grupo. Los grupos son útiles para trabajar con varias aplicaciones a la vez. Por ejemplo, puede que tenga un conjunto estándar de aplicaciones SaaS (como Workday, JIRA o Bugzilla) que desee configurar para acceder a la VPN sin cliente.

Configuración de Clientless App Groups	Description (Descripción)
Nombre	Introduzca un nombre descriptivo para el grupo de aplicaciones (hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos.
Ubicación	En el caso de un cortafuegos que esté en modo de Sistema virtual múltiple, **Location (Ubicación)** es el sistema virtual (vsys) en el que la puerta de enlace de GlobalProtect está disponible. En el caso de un cortafuegos que no esté en modo de Sistema virtual múltiple, el campo **Location (Ubicación)** no aparecerá en el cuadro de diálogo Puerta de enlace de GlobalProtect. Una vez guardada la configuración de la puerta de enlace, no puede cambiar el campo **Location (Ubicación)**.
applications	Haga clic en **Add (Añadir)** para añadir una **Application (Aplicación)** desde el menú desplegable o configure una nueva aplicación sin cliente y añádala al grupo. Para configurar una nueva aplicación sin cliente, consulte Network > GlobalProtect > Clientless Apps.

© 2020 Palo Alto Networks, Inc.

Objetos > GlobalProtect > Objetos HIP

Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** para definir objetos de un perfil de información de host (host information profile, HIP). Los objetos HIP brindan los criterios coincidentes para filtrar los datos sin procesar por una aplicación que desea utilizar para aplicar la política. Por ejemplo, si los datos del host sin procesar incluyen información de varios paquetes antivirus en un endpoint, es posible que le interese una aplicación en particular porque su organización requiere ese paquete. En este caso, cree un objeto HIP que coincida con la aplicación específica que desea aplicar.

La mejor forma de determinar los objetos HIP necesita es determinar cómo utilizará la información de host para aplicar la política. Tenga en cuenta que los objetos HIP son solo los ladrillos que le permiten crear los perfiles HIP que puede utilizar en sus políticas de seguridad. Por lo tanto, es posible que desee mantener la sencillez de sus objetos, de forma que solo coincidan con un elemento, como la presencia de un tipo concreto de software necesario, la pertenencia a un dominio específico o la presencia del SO de un endpoint determinado. De esta manera, tiene la flexibilidad de crear una política aumentada HIP muy granular.

Para crear un objeto HIP, haga clic en **Add (Añadir)** para abrir el cuadro de diálogo Objeto HIP. Para obtener una descripción sobre qué introducir en un campo determinado, consulte las siguientes tablas.

- Pestaña general de Objetos HIP
- Pestaña Dispositivo móvil de Objetos HIP
- Pestaña Administración de parches de Objetos HIP
- Pestaña de cortafuegos de Objetos HIP
- Pestaña Antimalware de Objetos HIP
- Pestaña de copia de seguridad de disco de Objetos HIP
- Pestaña de cifrado de disco de Objetos HIP
- Pestaña de prevención de pérdida de datos de objetos HIP
- Pestaña Certificado de objetos HIP
- Pestaña de comprobaciones personalizadas de objetos HIP

Para obtener información más detallada sobre cómo crear políticas de seguridad aumentadas HIP, consulte Configuración de la aplicación de políticas basadas en HIP en la *guía del administrador de GlobalProtect*.

Pestaña general de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **General (General)**

Seleccione la pestaña **General** para especificar un nombre para el nuevo objeto HIP y configurar el objeto para que coincida con la información de host general, como el dominio, el sistema operativo o el tipo de conectividad de red que tiene.

Configuración general de HIP Objects	Description (Descripción)
Nombre	Introduzca un nombre para el objeto HIP (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Lugar	Si selecciona **Shared (Compartido)**, los objetos HIP actuales están disponibles para lo siguiente: Todos los sistemas virtuales (vsys) del cortafuegos, si inició sesión en un cortafuegos que esté en modo de sistema virtual múltiple. Si cancela esta

© 2020 Palo Alto Networks, Inc.

Configuración general de HIP Objects	Description (Descripción)
	selección, el objeto únicamente estará disponible en el vsys seleccionado en el menú desplegable **Virtual System (Sistema virtual)** de la pestaña **Objects (Objetos)**. En el caso de un cortafuegos que no esté en modo vsys múltiple, esta opción no está disponible en el diálogo de objeto HIP. Todos los grupos de dispositivos de Panorama™. Si cancela esta selección, el objeto únicamente estará disponible en el grupo de dispositivos seleccionado en el menú desplegable **Device Group (Grupo de dispositivos)** de la pestaña **Objects (Objetos)**. Una vez guardado el objeto, no puede cambiar su ajuste **Shared (Compartido)**. Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** para ver la ubicación actual en **Location (Ubicación)**.
Description (Descripción)	(Opcional) Incluya una descripción.
Información de host	Seleccione esta opción para activar las opciones para configurar la información de host.
Gestionado	Filtre según si el endpoint es gestionado o no. Para hacer coincidir endpoints gestionados, seleccione **Yes (Sí)**. Para hacer coincidir endpoints no gestionados, seleccione **No**.
Deshabilitar anulación (Panorama únicamente)	Controla el acceso de cancelación al objeto HIP en grupos de dispositivos descendientes del **Device Group (Grupo de dispositivos)** seleccionado en la pestaña **Objects (Objetos)**. Seleccione esta opción para impedir que los administradores creen copias locales del objeto en grupos de dispositivos descendientes cancelando sus valores heredados. Esta opción no está seleccionada de manera predeterminada (la cancelación está habilitada).
Dominio	Para coincidir con el nombre de un dominio, seleccione un operador en el menú desplegable e introduzca una cadena para la coincidencia.
SO	Para buscar coincidencias con el SO de un host, seleccione **Contains (Contiene)** en el primer menú desplegable, seleccione un proveedor en el segundo menú desplegable y, a continuación, seleccione una versión de SO concreta en el tercer menú desplegable, o puede seleccionar **All (Todas)** para que la coincidencia sea con cualquier versión de SO del proveedor seleccionado.
Versión de cliente	Para buscar la coincidencia con un número de versión concreto, seleccione un operador en el menú desplegable y, a continuación, introduzca la cadena que debe coincidir (o no coincidir) en el cuadro de texto.
Nombre de host	Para buscar la coincidencia con un nombre de host específico o parte de él, seleccione un operador en el menú desplegable y, a continuación, introduzca la cadena que debe coincidir (o no coincidir, según el operador seleccionado) en el cuadro de texto.
ID de host	El ID de host es un identificador único que GlobalProtect asigna para identificar el host. El valor del ID de host varía según el tipo de dispositivo:

© 2020 Palo Alto Networks, Inc.

Configuración general de HIP Objects	Description (Descripción)
	• **Windows:** GUID de la máquina almacenada en el registro de Windows (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid). • **macOS:** dirección MAC de la primera interfaz de red física incorporada. • **Android:** ID de Android. • **iOS:** UDID • **Linux**: UUID del producto recuperado de la tabla DMI del sistema. • **Chrome**: GlobalProtect asigna cadenas alfanuméricas únicas de 32 caracteres. Para buscar la coincidencia con un ID de host específico, seleccione el operador en el menú desplegable e introduzca en el cuadro de texto la cadena que debe coincidir (o no coincidir, según el operador seleccionado).
Número de serie	Para buscar una coincidencia total o parcial del número de serie de un endpoint, seleccione un operador en la lista desplegable e introduzca la cadena para buscar coincidencias.
network	Utilice este campo para habilitar el filtrado en la configuración de red de un dispositivo móvil específico. Estos criterios de coincidencia se aplican únicamente a dispositivos móviles. Seleccione un operador en el menú desplegable y, a continuación, seleccione el tipo de conexión de red que se debe filtrar en el segundo menú desplegable: **Wifi**, **Mobile (Móvil)**, **Ethernet** (solo disponible para los filtros **Is Not (No es)**) o **Unknown (Desconocido)**. Después de seleccionar un tipo de red, introduzca cadenas adicionales con las que buscar coincidencias, si están disponibles, como el **Carrier (Operador)** móvil o **SSID** de Wifi.

Pestaña Dispositivo móvil de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **Mobile Device (Dispositivo móvil)**

Seleccione **Mobile Device (Dispositivo móvil)** para habilitar la coincidencia de HIP con datos recopilados de dispositivos móviles que ejecutan la aplicación GlobalProtect.

Para recopilar atributos de dispositivos móviles y utilizarlos en políticas de aplicación de HIP, GlobalProtect requiere un servidor MDM. Actualmente, GlobalProtect admite la integración de HIP con el servidor MDM de AirWatch.

Configuración de Mobile Device en HIP Objects	Description (Descripción)
Dispositivo móvil	Seleccione esta opción para habilitar el filtrado de los datos de host recopilados de los dispositivos móviles que se ejecutan en la aplicación de GlobalProtect y habilitar las pestañas Device, Settings y Apps.
PestañaDevice (Dispositivo)	• **Model (Modelo)**: para buscar la coincidencia con un modelo de dispositivo determinado, seleccione un operador en la lista desplegable e introduzca una cadena.

© 2020 Palo Alto Networks, Inc.

Configuración de Mobile Device en HIP Objects	Description (Descripción)
	• **Tag (Etiqueta)**: para buscar la coincidencia con un valor de etiqueta definido en el gestor de seguridad móvil de GlobalProtect, seleccione un operador en el primer menú desplegable y, a continuación, seleccione una etiqueta en el segundo menú desplegable. • **Phone Number (Número de teléfono)**: para buscar una coincidencia total o parcial del número de teléfono de un dispositivo, seleccione un operador en el menú desplegable e introduzca la cadena cuya coincidencia se debe buscar. • **IMEI**: para buscar una coincidencia total o parcial del IMEI (Identidad Internacional de Equipo Móvil) de un dispositivo, seleccione un operador en el menú desplegable e introduzca la cadena cuya coincidencia se debe buscar.
Pestaña Settings	• **Passcode (Contraseña)**: filtro basado en la existencia de un código de acceso en el dispositivo. Para hacer coincidir dispositivos que tengan un código de acceso establecido, seleccione **Yes (Sí)**. Para hacer coincidir dispositivos sin códigos de acceso establecidos, seleccione No. • **Rooted/Jailbroken (Modificado/Bloqueado)**: filtro basado en la modificación o bloqueo del dispositivo. Para hacer coincidir dispositivos que se hayan modificado o bloqueado, seleccione **Yes (Sí)**. Para hacer coincidir dispositivos que no se hayan modificado o bloqueado, seleccione **No**. • **Disk Encryption (Cifrado de disco)**: filtro basado en el cifrado del dispositivo. Para hacer coincidir dispositivos con el cifrado de disco habilitado, seleccione Yes (Sí). Para hacer coincidir dispositivos sin el cifrado de disco habilitado, seleccione No. • **Time Since Last Check-in (Tiempo desde el último registro)**: filtro en el momento en que MDM comprobó el dispositivo por última vez. Seleccione un operador en el menú desplegable y, a continuación, especifique el número de días para la ventana de comprobación. Por ejemplo, podría definir el objeto que se debe hacer coincidir con los dispositivos que no se hayan comprobado en los últimos 5 días.

Pestaña Apps	• **Apps**: (solo dispositivos Android) Seleccione esta opción para permitir el filtrado basado en las aplicaciones instaladas en el dispositivo y en la presencia de alguna aplicación instalada infectada por software malintencionado en el dispositivo.
	• Pestaña **Criteria (Criterios)**
	  • **Has Malware (Tiene malware)**: seleccione **Yes (Sí)** para hacer coincidir dispositivos con aplicaciones instaladas infectadas con malware. Seleccione **No** para hacer coincidir dispositivos sin aplicaciones instaladas infectadas con malware. Seleccione **None (Ninguna)** para no aplicar **Has Malware (Tiene malware)** como criterio de coincidencia.
	• Pestaña **Include (Incluir)**
	  • **Package (Paquete)**: para hacer coincidir dispositivos con aplicaciones específicas instaladas, añada una aplicación mediante **Add (Añadir)** e indique el nombre exclusivo de la aplicación en formato DNS inverso. Por ejemplo, com.netflix.mediaclient, y escriba el **Hash**

© 2020 Palo Alto Networks, Inc.

Configuración de Mobile Device en HIP Objects	Description (Descripción)
	correspondiente de la aplicación, que la aplicación de GlobalProtect calcula y envía junto con el informe HIP del dispositivo.

Pestaña Administración de parches de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **Patch Management (Administración de parches)**

Seleccione la pestaña **Patch Management (Administración de parches)** para habilitar la coincidencia HIP en el estado del parche de los endpoints de GlobalProtect.

Configuración de Patch Management en HIP Objects	Description (Descripción)
Administración de parches	Seleccione esta opción para habilitar la coincidencia del estado de la administración de los parches del host y habilitar las pestañas Criteria y Vendor.
Pestaña Criteria	Especifique los siguientes ajustes: • **Is Installed (Está instalado)**: busca coincidencias si el software de administración de parches está instalado en el host. • **Is Enabled (Está habilitado)**: busca coincidencias si el software de administración de parches está habilitado en el host. Si **Is Installed (Está instalado)** no está marcado, este campo se establece automáticamente como **none** y no se puede editar. • **Severity (Gravedad)**: seleccione de la lista de operadores lógicos para buscar coincidencias si al host le faltan parches del valor de gravedad especificado. Use las siguientes asignaciones entre los valores de gravedad de GlobalProtect y la escala de gravedad de OPSWAT para comprender lo que significa cada valor: • **0**—Low (Bajo) • **1**—Moderate (Moderado) • **2**—Important (Importante) • **3**—Critical (Crítico) • **Check (Comprobar)**: busca coincidencias en el endpoint si faltan parches. • **Patches (Parches)**: busca coincidencias si el host cuenta con determinados parches. Haga clic en **Add (Añadir)** e introduzca los ID de artículo de KB para los parches específicos que se deben buscar. Por ejemplo, introduzca `3128031` para comprobar la actualización de Microsoft Office 2010 (KB3128031), edición de 32 bits.
Pestaña Vendor	Defina los proveedores de software de gestión de parches y productos concretos que se deben buscar en el endpoint para determinar una coincidencia. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor** en el menú desplegable. También puede hacer clic

© 2020 Palo Alto Networks, Inc.

Configuración de Patch Management en HIP Objects	Description (Descripción)
	en Add (Añadir) para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar los ajustes.

Pestaña de cortafuegos de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > <*hip-object*> > **Firewall (Cortafuegos)**

Seleccione la pestaña **Firewall (Cortafuegos)** para habilitar la coincidencia HIP basada en el estado del software del cortafuegos de los endpoints de GlobalProtect.

Configuración de Firewall en HIP Objects
Seleccione la casilla de verificación **Firewall (Cortafuegos)** para habilitar la coincidencia en el estado del software del cortafuegos del host: • **Is Installed (Está instalado)**: busca coincidencias si el software del cortafuegos está instalado en el host. • **Is Enabled (Está habilitado)**: busca coincidencias si el software del cortafuegos está habilitado en el host. Si **Is Installed (Está instalado)** no está marcado, este campo se establece automáticamente como **none** y no se puede editar. • **Vendor and Product (Proveedor y producto)**: define proveedores o productos de software de cortafuegos concretos que se deben buscar en el host para determinar una coincidencia. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor** en el menú desplegable. También puede hacer clic en **Add (Añadir)** para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar los ajustes. • **Exclude Vendor (Excluir proveedor)**: seleccione esta opción para hacer coincidir hosts que no tengan software de un determinado proveedor.

Pestaña Antimalware de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > <*hip-object*> > **Anti-Malware**

Seleccione la pestaña **Anti-Malware** para habilitar la coincidencia HIP basada en la cobertura del antivirus o antispyware en los endpoints de GlobalProtect.

Configuración de antispyware en objetos HIP
Seleccione **Anti-Malware** para habilitar la coincidencia basada en la cobertura antivirus o antispyware en el host. Defina los criterios de evaluación adicionales de la coincidencia como se indica: • **Is Installed (Está instalado)**: busca coincidencias si el software antivirus o antispyware está instalado en el host. • **Real Time Protection (Protección en tiempo real)**: busca coincidencia si la protección antivirus o antispyware en tiempo real está habilitada en el host. Si **Is Installed (Está instalado)** no está marcado, este campo se establece automáticamente como **None (ninguno)** y no se puede editar. • **Virus Definition Version (Versión de definición de virus)**: busca coincidencias basándose en la actualización de las definiciones de virus dentro de un número especificado de días o versiones.

© 2020 Palo Alto Networks, Inc.

Configuración de antispyware en objetos HIP
• **Product Version (Versión de producto)**: busca coincidencias de una versión concreta del software antivirus o antispyware. Para especificar una versión, seleccione un operador en el menú desplegable y, a continuación, introduzca una cadena que represente la versión del producto. • **Last Scan Time (Última hora de análisis)**: especifique si la búsqueda de coincidencias debe basarse en el momento en el que se ejecutó el último análisis del antivirus o antispyware. Seleccione un operador en el menú desplegable y, a continuación, especifique el número de días en **Days (Días)** o de horas en **Hours (Horas)** con los que se buscarán coincidencias. • **Vendor and Product (Proveedor y Producto)**: defina proveedores o productos de software antivirus o antispyware concretos que se deben buscar en el host para determinar una coincidencia. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor (Proveedor)** en el menú desplegable. También puede hacer clic en **Add (Añadir)** para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar los ajustes. • **Exclude Vendor (Excluir proveedor)**: seleccione esta opción para hacer coincidir hosts que no tengan software de un determinado proveedor.

Pestaña de copia de seguridad de disco de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > <*hip-object*> > **Disk Backup (Copia de seguridad de disco)**

Seleccione la pestaña **Disk Backup (Copia de seguridad de disco)** para habilitar la coincidencia HIP basada en el estado de la copia de seguridad del disco de los endpoints de GlobalProtect.

Configuración de Disk Backup en HIP Objects
Seleccione **Disk Backup (Copia de seguridad de disco)** para habilitar la coincidencia con el estado de la copia de seguridad del disco en el host y, a continuación, defina criterios de coincidencia adicionales para la búsqueda de la siguiente forma: • **Is Installed (Está instalado)**: Busca coincidencias si el software de copia de seguridad del disco está instalado en el host. • **Last Backup Time (Última fecha de copia de seguridad)**: Especifica si la búsqueda de coincidencias debe basarse en el momento en el que se ejecutó la última copia de seguridad del disco. Seleccione un operador en el menú desplegable y, a continuación, especifique el número de días en **Days (Días)** o las horas en **Hours (Horas)** con los que buscar coincidencias. • **Vendor and Product (Proveedor y Producto)**: Define proveedores o productos de software de copia de seguridad de disco concretos que se deben buscar en el host. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor** en el menú desplegable. También puede hacer clic en **Add (Añadir)** para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar los ajustes. • **Exclude Vendor (Excluir proveedor)**: seleccione esta opción para hacer coincidir hosts que no tengan software de un determinado proveedor.

Pestaña de cifrado de disco de Objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > <*hip-object*> > **Disk Encryption (Cifrado de disco)**

Seleccione la pestaña **Disk Encryption (Cifrado de disco)** para habilitar la coincidencia HIP basada en el estado de cifrado del disco de los endpoints de GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Configuración de Disk Encryption en HIP Objects	Description (Descripción)
Cifrado de disco	Seleccione **Disk Encryption (Cifrado de disco)** para habilitar la coincidencia según el estado de cifrado del disco en el host.
Criterios	Especifique los siguientes ajustes: • **Is Installed (Está instalado)**: busca coincidencias si el software de cifrado del disco está instalado en el host. • **Encrypted Locations (Ubicaciones cifradas)**: haga clic en **Add (Añadir)** para especificar la unidad o la ruta que se debe comprobar para el cifrado del disco cuando se determine una coincidencia: • **Encrypted Locations (Ubicaciones cifradas)**: introduzca las ubicaciones concretas que se deben comprobar para el cifrado del host. • **State (Estado)**: especifique cómo hacer coincidir el estado de la ubicación cifrada seleccionando un operador en el menú desplegable y, a continuación, seleccionando un posible estado (**full (completo)**, **none (ninguno)**, **partial (parcial)**, **not-available (no disponible)**). Haga clic en **OK (Aceptar)** para guardar los ajustes.
Proveedor	Define proveedores y productos de software de cifrado del concretos que se deben buscar en el endpoint. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor** en el menú desplegable. También puede hacer clic en **Add (Añadir)** para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar la configuración y volver a la pestaña **Disk Encryption (Cifrado de disco)**.

Pestaña de prevención de pérdida de datos de objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **Data Loss Prevention (Prevención de pérdida de datos)**

Seleccione la pestaña **Data Loss Prevention (Prevención de pérdida de datos)** para configurar la coincidencia HIP que está basada en si los endpoints de GlobalProtect ejecutan el software de prevención de pérdida de datos.

Configuración de Data Loss Prevention en HIP Objects
Seleccione **Data Loss Prevention (Prevención de pérdida de datos)** para habilitar la coincidencia con el estado de la prevención de pérdida de datos (DLP) en el host (solo hosts de Windows) y defina de la siguiente forma criterios de coincidencia adicionales para la búsqueda: • **Is Installed (Está instalado)**: busca coincidencias si el software DPL está instalado en el host. • **Is Enabled (Está habilitado)**: busca si el software DLP está habilitado en el host. Si **Is Installed (Está instalado)** no está marcado, este campo se establece automáticamente como **none** y no se puede editar. • **Vendor and Product (Proveedor y Producto)**: Define proveedores o productos de software DPL concretos que se deben buscar en el host para determinar una coincidencia. Haga clic en **Add (Añadir)** y, a continuación, seleccione un proveedor en **Vendor** en el menú desplegable. También puede hacer clic en **Add (Añadir)** para elegir un producto específico en **Product (Producto)**. Haga clic en **OK (Aceptar)** para guardar los ajustes.

© 2020 Palo Alto Networks, Inc.

Configuración de Data Loss Prevention en HIP Objects
• **Exclude Vendor (Excluir proveedor)**: seleccione esta opción para hacer coincidir hosts que no tengan software de un determinado proveedor.

Pestaña Certificado de objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **Certificate (Certificado)**

Seleccione la pestaña **Certificate (Certificado)** para habilitar la coincidencia de HIP en función del perfil del certificado y otros atributos del certificado.

Configuración de certificado de objeto HIP
Seleccione **Validate Certificate (Validar certificado)** para habilitar la coincidencia en función de los perfiles del certificado y los atributos del certificado. A continuación, defina los criterios de coincidencia de la siguiente manera: • **Certificate Profile (Perfil del certificado)**: seleccione el perfil del certificado que la puerta de enlace de GlobalProtect usará para validar el certificado de equipo enviado en el informe HIP. • **Certificate Field (Campo de certificado)**: seleccione un atributo de certificado utilizado para la comparación con el certificado del equipo. • **Value (Valor)**: establezca el valor para el atributo.

Pestaña de comprobaciones personalizadas de objetos HIP

- **Objects (Objetos)** > **GlobalProtect** > **HIP Objects (Objetos HIP)** > *<hip-object>* > **Custom Checks (Comprobaciones personalizadas)**

Seleccione la pestaña **Custom Checks (Comprobaciones personalizadas)** para habilitar las coincidencias HIP en cualquier comprobación personalizada que haya definido en el portal de GlobalProtect. Para obtener información sobre cómo añadir comprobaciones personalizadas a la colección HIP, consulte Network (Red) > GlobalProtect > Portals (Portales).

Configuración de Custom Checks en HIP Objects	Description (Descripción)
Comprobaciones personalizadas	Seleccione **Custom Checks (Comprobaciones personalizadas)** para habilitar la coincidencia con cualquier comprobación personalizada que haya definido en el portal de GlobalProtect.
Lista de procesos	Para comprobar el sistema de host para un proceso específico, haga clic en **Add (Añadir)** y, a continuación, introduzca el nombre del proceso. De forma predeterminada, la aplicación comprueba los procesos en ejecución; si desea comprobar si un proceso concreto no se está ejecutando, elimine la marca de **Running (En ejecución)**. Los procesos pueden ser procesos en el nivel del sistema operativo o procesos de aplicación en el espacio del usuario.
Clave de registro	Para buscar en los hosts de Windows una clave de registro determinada, haga clic en **Add (Añadir)** e introduzca la **Registry Key (Clave de registro)** con la que buscar la coincidencia. Para buscar coincidencias solo en los

© 2020 Palo Alto Networks, Inc.

Configuración de Custom Checks en HIP Objects	Description (Descripción)
	hosts a los que les falta la clave de registro específica o el valor de la clave, marque la casilla **Key does not exist or match the specified value data (La clave no existe o coincide con datos de valor especificados)**. Para buscar coincidencias con valores concretos, haga clic en **Add (Añadir)** y, a continuación, introduzca el **Registry Value (Valor de registro)** y los **Value Data (Datos de valor)**. Para buscar coincidencias en hosts que explícitamente no tengan el valor o datos de valor especificados, seleccione **Negate (Negar)**. Haga clic en **OK (Aceptar)** para guardar los ajustes.
Plist	Para buscar en los hosts de Mac una entrada específica en la lista de propiedades (plist), haga clic en **Add (Añadir)** e introduzca el nombre **Plist**. Para buscar coincidencias solamente en hosts que no tengan la plist especificada, seleccione **Plist does not exist (Plist no existe)**. Para buscar coincidencias con un par clave-valor concreto dentro de la plist, haga clic en **Add (Añadir)** y, a continuación, introduzca la clave en **Key (Clave)** y el valor correspondiente en **Value (Valor)** que se debe hacer coincidir. Para buscar coincidencias en hosts que explícitamente no tengan la clave o el valor especificados, seleccione **Negate (Negar)**. Haga clic en **OK (Aceptar)** para guardar los ajustes.

© 2020 Palo Alto Networks, Inc.

Objetos > GlobalProtect > Perfiles HIP

Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Profiles (Perfiles HIP)** para crear perfiles HIP (una recopilación de objetos HIP que se evaluarán juntos para la supervisión o la aplicación de políticas de seguridad) que el usuario utiliza para configurar las políticas de seguridad habilitadas con HIP. Cuando crea perfiles HIP, puede combinar objetos HIP que haya creado previamente (así como otros perfiles HIP) usando lógica booleana como la que se usa cuando un flujo de tráfico se evalúa con respecto al perfil HIP resultante con el que tendrá, o no, coincidencia. Si coincide, la regla de política correspondiente se aplica; si no coincide, el flujo se evalúa con respecto a la siguiente regla (como con cualquier otro criterio de coincidencia de política).

Para crear un perfil HIP, haga clic en **Add (Añadir)**. En la siguiente tabla se proporciona información sobre qué introducir en los campos del cuadro de diálogo Perfil HIP. Para obtener información más detallada sobre cómo configurar GlobalProtect y el flujo de trabajo para crear políticas de seguridad aumentadas HIP, consulte Configuración de la aplicación de políticas basadas en HIP en la *guía del administrador de GlobalProtect*.

Configuración de perfil HIP	Description (Descripción)
Nombre	Introduzca un nombre para el perfil (de hasta **31** caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	(Opcional) Incluya una descripción.
Lugar	Seleccione **Shared (Compartido)** para que el perfil HIP actual esté disponible para los siguientes: • Todos los sistemas virtuales (vsys) del cortafuegos, si inició sesión en un cortafuegos que esté en modo de sistema virtual múltiple. Si cancela esta selección, el perfil únicamente está disponible en el vsys seleccionado en el menú desplegable **Virtual System (Sistema virtual)** de la pestaña **Objects (Objetos)**. En el caso de un cortafuegos que no esté en modo vsys múltiple, esta opción no aparece en el diálogo de perfil HIP. • Todos los grupos de dispositivos en Panorama. Si cancela esta selección, el perfil únicamente está disponible en el grupo de dispositivos seleccionado en el menú desplegable **Device Group (Grupo de dispositivos)** de la pestaña **Objects (Objetos)**. Una vez guardado el perfil, no puede cambiar su ajuste **Shared (Compartido)**. Seleccione **Objects (Objetos)** > **GlobalProtect** > **HIP Profiles (Perfiles HIP)** para ver la **Location (Ubicación)** actual.
Deshabilitar anulación (Panorama únicamente)	Controla el acceso de cancelación al perfil HIP en grupos de dispositivos descendientes de **Device Group (Grupo de dispositivos)** en la pestaña **Objects (Objetos)**. Seleccione esta opción si desea impedir que los administradores creen copias locales del perfil en grupos de dispositivos descendientes cancelando sus valores heredados. Esta opción no está seleccionada de manera predeterminada (la cancelación está habilitada).
Coincidencia	Haga clic en **Add Match Criteria (Añadir criterio de coincidencia)** para abrir el generador de objetos/perfiles HIP.

© 2020 Palo Alto Networks, Inc.

Configuración de perfil HIP	Description (Descripción)
	Seleccione el primer objeto o perfil HIP que desee utilizar como criterio de coincidencia y añádalo (⊞) al cuadro de texto **Match (Coincidencia)** del cuadro de diálogo HIP Objects/Profiles Builder (Generador de objetos/perfiles HIP). Tenga en cuenta que, si desea que el perfil HIP evalúe el objeto como una coincidencia solo cuando el criterio del objeto no sea verdadero para un flujo, seleccione **NOT** antes de añadir el objeto. Continúe añadiendo criterios de coincidencia como corresponda para el perfil que está creando, y asegúrese de seleccionar el operador booleano apropiado (**AND** u **OR**) cada vez que añada un elemento (y usando la casilla de el operador **NOT** cuando corresponda). Para crear una expresión booleana compleja, debe añadir manualmente el paréntesis en los lugares adecuados del cuadro de texto **Match (Coincidir)** para asegurarse de que el perfil HIP se evalúa usando la lógica que desea. Por ejemplo, la siguiente expresión indica que el perfil HIP buscará coincidencias con el tráfico desde un host que tenga cifrado de disco FileVault (en sistemas macOS) o TrueCrypt (en sistemas Windows), que pertenezca al dominio requerido y que también tenga instalado un cliente antivirus de Symantec: `(("MacOS" and "FileVault") or ("Windows" and "TrueCrypt")) and "Domain" and "SymantecAV"` Cuando haya terminado de añadir objetos y perfiles al nuevo perfil HIP, haga clic en **OK (Aceptar)**.

© 2020 Palo Alto Networks, Inc.

Dispositivo > Cliente de GlobalProtect

Los temas siguientes describen cómo configurar y gestionar la aplicación GlobalProtect.

¿Qué está buscando?	Consulte:
Obtener más información sobre las versiones de software de GlobalProtect.	Gestión del software del agente de GlobalProtect
Instalar el software GlobalProtect.	Configuración del agente de GlobalProtect
Usar el software GlobalProtect.	Uso del agente de GlobalProtect
¿Busca más información?	Para obtener instrucciones detalladas sobre cómo configurar el software de GlobalProtect, consulte Implementación del software de aplicación de GlobalProtect en la guía del administrador de GlobalProtect.

Gestión del software de la aplicación de GlobalProtect

Seleccione **Device (Dispositivo)** > **GlobalProtect Client (Cliente de GlobalProtect)** (solo cortafuegos) para descargar y activar el software de aplicación de GlobalProtect en el cortafuegos que aloja el portal. Luego, los endpoints que se conectan al portal descargan el software de la aplicación. En las configuraciones del agente que especifica en el portal, defina cómo y cuándo el portal aplica el software a los endpoints. Su configuración determina si las actualizaciones se producen automáticamente cuando la aplicación se conecta, si a los usuarios finales se les solicita actualizar, o si actualizar está prohibido para todos o un conjunto especial de usuarios. Consulte Allow User to Upgrade GlobalProtect App para obtener más información. Para obtener información sobre las opciones que existen para distribuir el software de la aplicación de GlobalProtect y leer instrucciones detalladas sobre cómo implementarlo, consulte Implementación del software de aplicación de GlobalProtect en la guía del administrador de GlobalProtect.

Para la instalación y descarga inicial de la aplicación de GlobalProtect, el usuario del endpoint debe iniciar sesión con derechos de administrador. Para las actualizaciones siguientes, no se requieren los derechos de administrador.

Configuración del cliente de GlobalProtect	Description (Descripción)
versión	Este número de versión es el software de la aplicación de GlobalProtect disponible en el servidor de actualizaciones de Palo Alto Networks. Para ver si hay disponible alguna nueva versión de software de aplicación en Palo Alto Networks, haga clic en **Check Now (Comprobar ahora)**. El cortafuegos utiliza su ruta del servicios para conectarse al servidor de actualizaciones y determinar si hay nuevas versiones. Si hay actualizaciones disponibles, las muestra al principio de la lista.
Tamaño	El tamaño del paquete de software de la aplicación.
Release date	Fecha y hora en la que Palo Alto Networks publicó la versión.

© 2020 Palo Alto Networks, Inc.

Configuración del cliente de GlobalProtect	Description (Descripción)
Descargado	Una marca de comprobación en esta columna indica que se ha descargado la versión correspondiente del paquete de software de aplicación en el cortafuegos.
Activado actualmente	Una marca de comprobación en esta columna indica que se ha activado la versión correspondiente del software de aplicación en el cortafuegos y que las aplicaciones que se conecten pueden descargarla. Solo se puede activar una versión del software.
Acción	Indica la acción actual que puede realizar para el paquete de software de aplicación de la siguiente forma: • **Download (Descargar)**: la versión de software de aplicación correspondiente está disponible en el servidor de actualizaciones de Palo Alto Networks. Haga clic en **Download (Descargar)** para iniciar la descarga. Si el cortafuegos no tiene acceso a Internet, utilice un ordenador conectado a Internet para ir al sitio de Asistencia al cliente y luego seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)** para buscar y **Download (Descargar)** las nuevas versiones de software de aplicación en su ordenador local. Luego, haga clic en **Upload (Cargar)** para cargar manualmente el software de aplicación al cortafuegos. • **Activate (Activar)**: se ha descargado la versión de software de aplicación correspondiente al cortafuegos, pero las aplicaciones no la pueden descargar todavía. Haga clic en **Activate (Activar)** para activar el software y habilitar la actualización de la aplicación. Para activar una actualización de software que haya cargado manualmente en el cortafuegos, haga clic **Activate from File (Activar desde archivo)** y seleccione la versión que desea activar en el menú desplegable (puede que necesite actualizar la pantalla para que aparezca como **Currently Activated (Activado actualmente)**). • **Reactivate (Reactivar)**: se ha activado el software de aplicación correspondiente y está listo para que lo descarguen los endpoints. Dado que solo puede estar activa una versión del software de aplicación de GlobalProtect en el cortafuegos, si los usuarios finales necesitan acceder a una versión distinta a la actual, tendrá que hacer clic en **Activate (Activar)** para activar la otra versión y que se convierta en la versión **Currently Active (Activada actualmente)**.
Notas de versión	Proporciona un enlace a las notas de la versión de GlobalProtect para la versión de aplicación correspondiente.
☒	Elimine la imagen de software de la aplicación descargada anteriormente del cortafuegos.

Configuración de aplicación de GlobalProtect

GlobalProtect es una aplicación que se instala en el endpoint (generalmente, un portátil) para admitir conexiones de GlobalProtect con portales y puertas de enlace. La aplicación recibe el respaldo del servicio GlobalProtect (PanGP Service).

© 2020 Palo Alto Networks, Inc.

Asegúrese de seleccionar la opción de instalación correcta para su sistema operativo de host (32 bits o 64 bits). Si se realiza la instalación en un host de 64 bits, utilice una combinación de explorador/Java de 64 bits para la instalación inicial.

Para instalar la aplicación, abra el archivo de instalador y siga las instrucciones que aparecen en pantalla.

Uso de la aplicación de GlobalProtect

Las pestañas en el panel **GlobalProtect Settings (Configuración de GlobalProtect)**, que se abre cuando inicia la aplicación de GlobalProtect y selecciona **Settings (Configuración)** del menú **Settings (Configuración)** en el panel de estado de GlobalProtect, contienen información útil sobre el estado y la configuración, y brindan información para asistir en la resolución de problemas de conexión.

- Pestaña General: muestra el nombre de usuario y los portales asociados a la cuenta de GlobalProtect. También puede añadir, eliminar o modificar los portales desde esta pestaña.
- **Pestaña Connection (Conexión)**: muestra las puertas de enlace configuradas para la aplicación de GlobalProtect y brinda la siguiente información sobre cada puerta de enlace:
  - Gateway name (Nombre de la puerta de enlace)
  - Tunnel status (Estado del túnel)
  - Authentication status (Estado de autenticación)
  - Connection type (Tipo de conexión)
  - Gateway IP address or FQDN (Dirección IP o FQDN de la puerta de enlace) (solo disponible en el modo externo)

  En el modo interno, la pestaña Connection (Conexión) muestra la lista completa de puertas de enlace disponibles. En el modo externo, la pestaña Connection (Conexión) muestra la puerta de enlace a la que se conecta y los detalles adicionales sobre la puerta de enlace (como la dirección IP y el tiempo activo de la puerta de enlace).
- **Pestaña Host Profile (Perfil de host)**: muestra los datos de endpoint que utiliza GlobalProtect para supervisar y aplicar políticas a través del perfil de información de host (Host Information Profile, HIP). Haga clic en **Resubmit Host Profile (Reenviar perfil de host)** para reenviar manualmente los datos de HIP a la puerta de enlace.
- **Pestaña Troubleshooting (Resolución de problemas)**: en los endpoints Mac OS, esta pestaña le permite **Collect Logs (Recopilar logs)** y establecer el **Logging Level (Nivel de creación de logs)**. En los endpoints Windows, esta pestaña le permite **Collect Logs (Recopilar logs)**, establecer el **Logging Level (Nivel de creación de logs)** y ver la siguiente información para asistir durante la resolución de problemas:
  - **Network Configurations (Configuración de red)**: muestra la configuración actual del sistema.
  - **Routing Table**: Muestra información acerca del enrutamiento actual de la conexión de GlobalProtect.
  - **Sockets**: Muestra información de socket de las conexiones actualmente activas.
  - **Logs**: le permite al usuario mostrar logs de la aplicación y el servicio de GlobalProtect. Seleccione el tipo de log y el nivel de depuración. Haga clic en **Start (Iniciar)** para comenzar los logs y **Stop (Detener)** para finalizar los logs.
- **Pestaña Notification (Notificación)**: muestra la lista de notificaciones activadas en la aplicación de GlobalProtect. Para acceder a más detalles sobre una notificación específica, haga doble clic en la notificación.

© 2020 Palo Alto Networks, Inc.

Interfaz web de Panorama

Panorama™ es el sistema de gestión centralizado de la familia de cortafuegos de nueva generación de Palo Alto Networks®. Panorama proporciona una única ubicación desde la que puede supervisar todas las aplicaciones, usuarios y contenido de su red, y emplear esta información para crear políticas que controlen y protejan toda la red. Si se usa Panorama para gestionar de forma centralizada las políticas y cortafuegos, es posible aumentar la eficiencia operativa al gestionar una red distribuida de cortafuegos. Panorama está disponible como plataforma de hardware dedicada (M-Series) y como dispositivo virtual VMware (que se ejecuta en un servidor ESXi o en la plataforma vCloud Air).

Si bien muchas vistas y ajustes de la interfaz web de Panorama son idénticos a los de la interfaz web del cortafuegos, los siguientes temas describen las opciones disponibles exclusivamente en la interfaz web de Panorama para administrar Panorama, cortafuegos y recopiladores de logs.

> Uso de la interfaz web de Panorama
> Conmutador de contexto
> Operaciones de compilación de Panorama
> Definición de políticas en Panorama
> Particiones de almacenamiento de log para un dispositivo virtual de Panorama en modo Legado
> Panorama > Configuración > Interfaces
> Panorama > Alta disponibilidad
> Panorama > Clústeres Wildfire gestionados
> Panorama > Administradores
> Panorama > Funciones de administrador
> Panorama > Access Domains
> Panorama > Managed Devices > Summary (Panorama > Dispositivos gestionados > Resumen)
> Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)
> Panorama > Plantillas
> Panorama > Grupos de dispositivos
> Panorama > Recopiladores gestionados
> Panorama > Grupos de recopiladores
> Panorama> Complementos
> Panorama > VMware NSX
> Panorama > Perfil de ingestión de logs
> Panorama > Configuración de log
> Panorama > Exportación de configuración programada
> Panorama > Software
> Panorama > Implementación de dispositivo

¿Busca más información?

Consulte la Guía del administrador de Panorama para obtener detalles sobre cómo configurar y utilizar Panorama para una gestión centralizada.

© 2020 Palo Alto Networks, Inc.

Uso de la interfaz web de Panorama

Las interfaz web en Panorama y el cortafuegos tienen la misma apariencia. Sin embargo, la interfaz web de Panorama incluye opciones adicionales y una pestaña específica de Panorama para gestionarlo y usarlo con el fin de administrar cortafuegos y recopiladores de logs.

Los siguientes campos comunes aparecen en el encabezado o pie de página de varias páginas del interfaz web de Panorama.

Campo común	Description (Descripción)
Contexto	Puede usar el menú desplegable **Context (Contexto)** situado sobre el menú lateral para cambiar entre la interfaz web de Panorama y la interfaz web de un cortafuegos (consulte Conmutador de contexto).
	En las **Dashboard (Panel)** y **Monitor (Supervisar)**, haga clic en actualizar ( ) en el encabezado de pestaña para actualizar manualmente los datos en esas pestañas. También puede utilizar el menú desplegable sin etiqueta en el lado derecho del encabezado de la pestaña para seleccionar un intervalo de actualización automática en minutos (**1 min**, **2 min** o **5 min**); para deshabilitar la actualización automática, seleccione **Manual**.
Dominio de acceso	Un dominio de acceso define el acceso a grupos específicos de dispositivos, plantillas y cortafuegos individuales (a través del menú desplegable **Context (Contexto)**). Si inicia sesión como administrador con varios dominios de acceso asignados a su cuenta, las pestañas **Dashboard (Panel)**, **ACC** y **Monitor (Supervisar)** muestran información (como datos de log) solo para el **Acces Domain (Dominio de acceso)** que seleccione en el pie de página de la interfaz web. *Si sólo se ha asignado un dominio de acceso a su cuenta, la interfaz web no muestra el menú desplegable Access Domain (Dominio de acceso).*
Grupo de dispositivos	Un grupo de dispositivos incluye cortafuegos y sistemas virtuales que gestiona como un grupo (consulte Panorama > Device Groups). Las pestañas **Dashboard (Panel)**, **ACC** y **Monitor (Supervisor)** muestran información (como datos de registro) solo para el **Device Group (Grupo de dispositivos)** que selecciona en el encabezado de pestaña. En las pestañas **Policies (Políticas)** y **Objects (Objetos)**, puede configurar los ajustes para un **Device Group (Grupo de dispositivos)** o para todos los grupos de dispositivos (seleccione **Shared [Compartido]**).
Plantilla	Una plantilla es un grupo de cortafuegos con configuraciones comunes de red y dispositivo, y una pila de plantillas es una combinación de plantillas (consulte Panorama > Templates). En las pestañas **Network (Red)** y **Device (Dispositivo)**, se configuran las configuraciones de una **Template (Plantilla)** o pila de plantillas. Debido a que puede editar configuraciones solo en plantillas individuales, la configuración de estas pestañas es de sólo lectura si selecciona una pila de plantillas.

© 2020 Palo Alto Networks, Inc.

Campo común	Description (Descripción)
Ver por: Dispositivo Modo	De forma predeterminada, las pestañas **Network (Red)** y **Device (Dispositivo)** muestran las configuraciones y valores disponibles para cortafuegos que están en modo operativo normal y que soportan múltiples sistemas virtuales y VPNs. Sin embargo, puede utilizar las siguientes opciones para filtrar las pestañas para mostrar solo la configuración de modo específico que desea editar: • En el menú desplegable **Mode (Modo)**, seleccione o cancele las opciones **Multi VSYS (VSYS múltiple)**, **Operational Mode (Modo operativo)** y **VPN Mode (Modo VPN)**. • Configure todas las opciones de Modo para reflejar la configuración de modo de un cortafuegos determinado seleccionándolo en el menú desplegable **View by (Ver por): Device (Dispositivo)**.

La pestaña **Panorama** proporciona las siguientes páginas para administrar los recopiladores de datos y Panorama.

Páginas de Panorama	Description (Descripción)
Configuración	Seleccione **Panorama** > **Setup (Configuración)** para las siguientes tareas: • Especifique la configuración general (como el nombre de host de Panorama) y los valores de autenticación, logs, informes, AutoFocus ™, banners, el mensaje del día y la complejidad de la contraseña. Estos ajustes son similares a los que se configuran para cortafuegos: seleccione Device > Setup > Management. • Haga copias de seguridad y restaure configuraciones, reinicie Panorama y apague Panorama. Estas operaciones son similares a las que realiza para cortafuegos: seleccione Device > Setup > Operations. • Defina conexiones de servidor para actualizaciones de DNS, NTP y Palo Alto Networks. Estos ajustes son similares a los que se configuran para cortafuegos: seleccione Device > Setup > Services. • Defina los ajustes de red para las interfaces Panorama. Seleccione Panorama > Setup > Interfaces. • Especifique la configuración del dispositivo WildFire™ Estos ajustes son similares a los que configura para los cortafuegos: seleccione Device > Setup > WildFire. • gestionar la configuración del Módulo de seguridad de hardware (HSM). Estos ajustes son similares a los que se configuran para cortafuegos: seleccione Device > Setup > HSM.
High Availability	Le permite configurar la alta disponibilidad (HA) de un par de servidores de gestión Panorama. Seleccione Panorama > High Availability.
Auditoría de configuraciones	Le permite ver las diferencias entre los archivos de configuración. Seleccione Device > Config Audit.
Perfiles de la contraseña	Le permite definir perfiles de contraseña para los administradores de Panorama. Seleccione Device > Password Profiles.
Administradores	Le permite configurar las cuentas de administrador de Panorama. Seleccione Panorama > Administrators.

© 2020 Palo Alto Networks, Inc.

Páginas de Panorama	Description (Descripción)
	Si la cuenta de administrador se bloquea, la página Administrators (Administradores) muestra el icono de un candado en la columna Locked User (Usuario bloqueado). Puede hacer clic en el candado para desbloquear la cuenta.
Funciones de gestor	Le permite definir funciones administrativas que controlan los privilegios y responsabilidades de los administradores que acceden a Panorama. Seleccione Panorama > Admin Roles.
Dominio de acceso	Le permite controlar el acceso de los administradores a los grupos de dispositivos, plantillas, pilas de plantillas y la interfaz web de los cortafuegos. Seleccione Panorama > Access Domains.
Perfil de autenticación	Le permite especificar un perfil de acceso de autenticación a Panorama. Seleccione Device > Authentication Profile.
Secuencia de autenticación	Le permite especificar una serie de perfiles de autenticación que se usan para permitir el acceso a Panorama. Seleccione Device > Authentication Sequence.
Identificación de usuarios	Permite configurar Panorama para recibir información de asignación de usuarios de los agentes de User-ID ™. Seleccione Dispositivo > Identificación de usuarios > Agentes de User-ID.
Dispositivos gestionados	Le permite gestionar cortafuegos, que incluye añadir cortafuegos a Panorama como *dispositivos gestionados*, mostrar la conexión del cortafuegos y el estado de licencia, etiquetar cortafuegos, actualizar el contenido y software del cortafuegos y cargar copias de seguridad de la configuración. Seleccione Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen).
Plantillas	Le permite gestionar opciones de configuración en las pestañas **Device (Dispositivo)** y **Network (Red)**. Las plantillas y las pilas de plantillas le permiten reducir la carga de trabajo administrativo que supone implementar varios cortafuegos con la misma o configuraciones similares. Seleccione Panorama > Templates.
Grupos de dispositivos	Le permite configurar grupos de dispositivos, que agrupa cortafuegos basándose en la función, segmentación de red o ubicación geográfica. Los grupos de dispositivos pueden incluir cortafuegos físicos, virtuales y sistemas virtuales. Tradicionalmente, los cortafuegos de un grupo de dispositivos necesitan configuraciones de política parecidas. Cuando use las pestañas **Policies (Políticas)** y **Objects (Objetos)** de Panorama, los grupos de dispositivos le permitirán implementar un método por capas para gestionar políticas en una red de cortafuegos gestionados. Puede anidar grupos de dispositivos en una jerarquía de árbol de hasta cuatro niveles. Los grupos sucesores heredan automáticamente las políticas y objetos de los grupos antecesores y de la ubicación compartida. Seleccione Panorama > Device Groups.
Recopiladores gestionados	Le permite gestionar recopiladores de logs. Dado que usa Panorama para configurar recopiladores de logs, también reciben el nombre de *recopiladores gestionados*. Un recopilador gestionado puede ser local para el servidor de administración Panorama (dispositivo M-Series o dispositivo virtual Panorama

© 2020 Palo Alto Networks, Inc.

Páginas de Panorama	Description (Descripción)
	en modo Panorama) o un recopilador de logs dedicado (dispositivo M-Series en modo recopilador de logs). Seleccione Panorama > Recopiladores gestionados. También puede instalar Actualizaciones de software para recopiladores de logs dedicados. *Puede* Convertir un servidor de gestión de Panorama en un recopilador de logs dedicado.
Grupos de recopiladores	Le permite gestionar Grupos de recopiladores. Un grupo de recopiladores lógicamente agrupa recopiladores de logs de modo que pueda aplicar las mismas opciones de configuración y asignar cortafuegos a ellos. Panorama distribuye uniformemente los logs entre todos los discos de un recopilador de logs y entre todos los miembros del grupo de recopiladores. Seleccione Panorama > Grupos de recopiladores.
Complementos	Le permite administrar complementos para la integración de terceros, como VMware NSX. Seleccione Panorama > VMware NSX.
VMware NSX	Le permite automatizar el aprovisionamiento de cortafuegos VM-Series permitiendo la comunicación entre Panorama y el administrador NSX. Seleccione Panorama > VMware NSX.
Gestión de certificados	Le permite configurar y gestionar certificados, perfiles de certificados y claves. Seleccione Manage Firewall and Panorama Certificates.
Configuración de log	Le permite reenviar logs a receptores de traps del Protocolo simple de administración de redes (Simple Network Management Protocol, SNMP), servidores Syslog, servidores de correo electrónico y servidores HTTP. Seleccione Device > Log Settings.
Perfiles de servidores	Le permite configurar perfiles para los diferentes tipos de servidores que prestan servicios a Panorama: Seleccione cualquiera de los siguientes para configurar un tipo de servidor específico: • Device > Server Profiles > Email • Dispositivo > Perfiles de servidor > HTTP • Dispositivo > Perfiles de servidor > Trap SNMP • Device > Server Profiles > Syslog • Device > Server Profiles > RADIUS • Device > Server Profiles > TACACS+ • Device > Server Profiles > LDAP • Device > Server Profiles > Kerberos • Dispositivo > Perfiles de servidor > Proveedor de identidad SAML
Exportación de configuración programada	Le permite exportar configuraciones de Panorama y de cortafuegos a un servidor FTP o un servidor Secure Copy (SCP) a diario. Seleccione Panorama > Scheduled Config Export.
Software	Le permite actualizar el software Panorama. Seleccione Panorama > Software.

© 2020 Palo Alto Networks, Inc.

Páginas de Panorama	Description (Descripción)
Actualizaciones dinámicas	Le permite visualizar las definiciones de la aplicación y la información sobre amenazas de seguridad como firmas antivirus más actualizadas (se requiere licencia de prevención de amenazas), así como actualizar Panorama con nuevas definiciones. Seleccione Device > Dynamic Updates (Dispositivo > Actualizaciones dinámicas).
Soporte	Le permite acceder a alertas sobre el producto y seguridad de Palo Alto Networks. Seleccione Device > Support.
Implementación de dispositivo	Le permite implementar software y actualizaciones de contenido a los cortafuegos y recopiladores de logs. Seleccione Panorama > Device Deployment.
Clave maestra y diagnóstico	Le permite especificar una clave maestra para cifrar claves privadas en Panorama. De forma predeterminada, Panorama almacena las claves privadas en forma cifrada aunque no especifique una nueva clave maestra. Seleccione Device > Master Key and Diagnostics.

© 2020 Palo Alto Networks, Inc.

Conmutador de contexto

En el encabezado de cada página de interfaz web de Panorama, puede usar el menú desplegable **Context (Contexto)** situado sobre el menú lateral izquierdo para cambiar entre la interfaz web de Panorama y la interfaz web de un cortafuegos. Cuando selecciona un cortafuegos, la interfaz web se actualiza para mostrar todas las páginas y opciones del cortafuegos seleccionado de modo que pueda gestionarlo de manera local. El menú desplegable muestra solo los cortafuegos en los que tiene acceso como administrador (consulte Panorama > Access Domains) y que están conectados a Panorama.

Puede utilizar los filtros para buscar cortafuegos por plataformas (modelo), grupos de dispositivos, plantillas, etiquetas o estado de HA. También puede introducir una cadena de texto en la barra de filtros para buscar por Nombre de dispositivo.

Los iconos de los cortafuegos en modo de alta disponibilidad (HA) tienen el fondo de color para indicar que están en estado de HA.

© 2020 Palo Alto Networks, Inc.

Operaciones de compilación de Panorama

Haga clic en **Commit (Compilar)** en la parte superior derecha de la interfaz web y seleccione una operación para los cambios pendientes en la configuración de Panorama y los cambios que Panorama envía al cortafuegos, recopiladores de log, y clústeres y dispositivos WildFire:

- **Commit (Compilar)** > **Commit to Panorama (Compilar en Panorama)**: activa los cambios realizados en la configuración del servidor de gestión Panorama. Esta acción también compila los cambios al grupo de dispositivos, plantilla, grupo de recopiladores y clúster y dispositivo WildFire en la configuración de Panorama sin enviar los cambios a los cortafuegos, recopiladores de logs ni clústeres y dispositivos WildFire. Compilar solo la configuración de Panorama le permite guardar los cambios que aún no quiere activar en los cortafuegos, recopiladores de logs, y clústeres y dispositivos WildFire.

  Al enviar configuraciones a dispositivos gestionados, Panorama 8.0 y versiones posteriores implementan la configuración en ejecución, que es la configuración compilada en Panorama. Panorama 7.1 y versiones anteriores implementan la configuración candidata, que incluye cambios no compilados. Por lo tanto, Panorama 8.0 y versiones posteriores no le permiten enviar los cambios a dispositivos gestionados hasta que los compile en Panorama.
- **Commit (Compilar)** > **Push to Devices (Enviar a dispositivos)**: envía la configuración en ejecución de Panorama a grupos de dispositivos, plantillas, grupos de recopiladores, y clústeres y dispositivos WildFire.
- **Commit (Compilar)** > **Commit and Push (Compilar y enviar)**: compila todos los cambios de configuración en la configuración local de Panorama y después envía la configuración en ejecución de Panorama a grupos de dispositivos, plantillas, grupos de recopiladores, y clústeres y dispositivos WildFire.

Puede filtrar los cambios pendientes por administrador o *ubicación* y, a continuación, compilar, enviar, validar o previsualizar solo esos cambios. La ubicación puede ser grupos de dispositivos, plantillas, grupos de recopiladores, recopiladores de logs, dispositivos y clústeres WildFire, y configuraciones compartidas específicos, o el servidor de gestión Panorama.

Al compilar los cambios, estos se convierten en parte de la configuración en ejecución. Los cambios que no haya compilado son parte de la configuración candidata. Panorama pone en cola las solicitudes de compilación de modo que pueda iniciar nuevas compilaciones mientras una previa está en curso. Panorama compila en el orden en que se inician las solicitudes, pero prioriza las compilaciones automáticas iniciadas por Panorama (como las actualizaciones de FQDN). Sin embargo, si la cola ya tiene el número máximo de compilaciones iniciadas por el administrador, debe esperar a que Panorama termine de procesar una compilación pendiente antes de iniciar una nueva. Puede usar el Gestor de tareas (Tasks) para limpiar la cola de compilación o ver los detalles de estas. Para obtener más información sobre los cambios de configuración, los procesos de compilación, las validaciones de compilación y la cola de compilación, consulte Operaciones de compilación y validación de Panorama. También puede Guardar configuraciones candidatas, Revertir cambios, e importar, exportar o cargar configuraciones (Device > Setup > Operations).

Las siguientes opciones están disponibles para compilar, validar o previsualizar los cambios de configuración.

Campo/Botón	Description (Descripción)
Las siguientes opciones se aplican cuando realiza una confirmación en Panorama seleccionando **Commit (Confirmar)** > **Commit to Panorama (Confirmar en Panorama)** o **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)**.	
Commit All Changes	Compila todos los cambios para los que tiene privilegios administrativos (predeterminado). No puede filtrar manualmente

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	el ámbito de los cambios de configuración que Panorama compila cuando se selecciona esta opción. En su lugar, la función de administrador asignada a la cuenta utilizada para iniciar sesión determina el ámbito de compilación: • **Función de superusuario**: Panorama compila los cambios de todos los administradores. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan el ámbito de compilación (consulte Panorama > Admin Roles). Si el perfil incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, Panorama compila los cambios configurados por cualquiera de los administradores. Si su perfil de función de administración no incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, Panorama compila solo sus cambios y no los de los demás administradores. Si ha implementado dominios de acceso, Panorama aplica automáticamente esos dominios para filtrar el ámbito de compilación (consulte Panorama > Access Domain). Independientemente de su función administrativa, Panorama compila solo los cambios de configuración en los dominios de acceso asignados a su cuenta.
Commit Changes Made By	Filtra el ámbito de los cambios de configuración que Panorama compila. La función administrativa asignada a la cuenta utilizada para iniciar sesión determina las opciones de filtrado: • **Función de superusuario**: puede limitar el ámbito de compilación a los cambios realizados por administradores específicos y a los cambios en ubicaciones específicas. • **Función personalizada**: los privilegios del perfil de función de administración asignado a su cuenta determinan las opciones de filtrado (consulte Panorama > Admin Roles). Si el perfil incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, puede limitar el ámbito de compilación a cambios configurados por administradores específicos y a cambios en ubicaciones específicas. Si su perfil de función de administración no incluye el privilegio **Commit For Other Admins (Compilar por otros administradores)**, solo puede limitar el ámbito de compilación a los cambios realizados por usted mismo en ubicaciones específicas. Filtre el ámbito de compilación de la siguiente manera: • **Filtrar por administrador**: incluso si su función permite compilar los cambios de otros administradores, el ámbito de compilación incluye solo sus cambios de forma predeterminada. Para añadir otros administradores al ámbito de confirmación, haga clic en el enlace <*usernames*>, seleccione los administradores y haga clic en **OK (Aceptar)**. • **Filtrar por ubicación**: seleccione los cambios en ubicaciones específicas para incluir en la compilación Include in Commit. Si ha implementado dominios de acceso, Panorama filtra automáticamente el ámbito de compilación en función de dichos dominios (consulte Panorama > Access Domain). Independientemente

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	de su función administrativa y de sus opciones de filtrado, el ámbito de compilación solo incluye los cambios de configuración en los dominios de acceso asignados a su cuenta. *Tras cargar una configuración (Device > Setup > Operations), debe Commit All Changes (Compilar todos los cambios).* Al compilar cambios en un grupo de dispositivos, debe incluir los cambios de todos los administradores que añadieron, eliminaron o cambiaron reglas para la misma base de reglas en ese grupo de dispositivos.
Commit Scope	Enumera las ubicaciones donde hay cambios que compilar. Que la lista incluya todos los cambios o un subconjunto de ellos depende de varios factores, tal como se describe en las opciones Commit All Changes y Commit Changes Made By. Las ubicaciones pueden ser cualquiera de las siguientes opciones: • **shared-object (objeto compartido)**: ajustes definidos en la ubicación compartida. • *<device-group>*: el nombre del grupo de dispositivos en el que se definen objetos o reglas de la política. • *<template>*: el nombre de la plantilla o pila de plantillas en la que se definen los ajustes. • *<log-collector-group>*: el nombre del grupo de recopiladores en el que se definen los ajustes. • *<log-collector>*: el nombre del recopilador de log en el que se definen los ajustes. • *<wildfire-appliances>*: el número de serie del dispositivo Wildfire en el que definen los ajustes. • *<wildfire-appliance-clusters>*: el nombre del clúster WildFire en el que definen los ajustes.
Tipo de ubicación	Esta columna categoriza las ubicaciones de los cambios pendientes: • **Panorama**: Los ajustes específicos de la configuración del servidor de gestión Panorama. • **Device Group (Grupo de dispositivos)**: configuraciones definidas en un grupo de dispositivos específico. • **Template (Plantilla)**: configuraciones definidas en una plantilla o pila de plantillas específica. • **Log Collector Group (Grupo de recopiladores de log)**: ajustes específicos de una configuración de grupo de recopiladores. • **Log Collector (Recopiladores de log)**: ajustes específicos de una configuración de recopiladores de log. • **WildFire Appliance Clusters (Clústeres de dispositivos WildFire)**: ajustes específicos de una configuración de clúster de dispositivos WildFire. • **WildFire Appliances (Dispositivos WildFire)**: ajustes específicos de un dispositivo WildFire.

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Other Changes (Otros cambios)**: ajustes que no son específicos de ninguna de las áreas de configuración anteriores (como los objetos compartidos).
Include in Commit (compilación parcial únicamente)	Permite seleccionar los cambios que desea compilar. De manera predeterminada, se seleccionan todos los cambios en **Commit Scope (Ámbito de compilación)**. Esta columna solo se muestra tras elegir compilar los cambios realizados por administradores específicos (**Commit Changes Made By**). *Puede haber dependencias que afecten a los cambios que incluya en la compilación. Por ejemplo, si añade un objeto y otro administrador, a continuación, modifica ese objeto, no puede compilar el cambio del otro administrador sin compilar su propio cambio.*
Group by Type	Agrupa la lista de cambios de configuración en **Commit Scope (Ámbito de compilación)** por **Location Type (Tipo de ubicación)**.
Vista previa de cambios	Permite comparar las configuraciones seleccionadas en **Commit Scope (Ámbito de compilación)** con la configuración en ejecución. La ventana de vista previa utiliza codificación de colores para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo). Para ayudarle a comparar los cambios con las secciones de la interfaz web, puede configurar la ventana de vista previa para que muestre **Lines of Context (Líneas de contexto)** antes y después de cada cambio. Este contexto proviene de los archivos de las configuraciones candidata y en ejecución que está comparando. *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.*
Cambiar resumen	Enumera los ajustes individuales en los que está compilando cambios. La lista **Change Summary (Resumen de los cambios)** muestra la siguiente información para cada ajuste: • **Object Name (Nombre de objeto)**: el nombre que identifica la política, el objeto, el ajuste de red o la configuración del dispositivo. • **Type (Tipo)**: el tipo de ajuste (como Dirección, Regla de seguridad o Zona). • **Location Type (Tipo de ubicación)**: indica si el ajuste se encuentra definido en **Device Groups (Grupos de dispositivos)**, **Templates (Plantillas)**, **Collector Groups (Grupos de recopiladores)**, **WildFire Appliances (Dispositivos WildFire)**, o **Wildfire Appliance Clusters (Clústeres de dispositivos Wildfire)**. • **Location (Ubicación)**: el nombre del grupo de dispositivos, plantilla, grupo de recopiladores, clúster WildFire o dispositivo WildFire donde se define la configuración. La columna muestra **Shared**

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	(Compartido) en los ajustes que no son específicos de estas ubicaciones. • **Operations (Operaciones)**: indica todas las operaciones (crear, editar o eliminar) realizadas en la configuración desde la última compilación. • **Owner (Propietario)**: el administrador que realizó el último cambio en el ajuste. • **Will Be Committed (Se compilará)**: indica si la compilación incluirá el ajuste. • **Previous Owners (Propietarios anteriores)**: administradores que realizaron cambios en el ajuste antes del último cambio. Opcionalmente, puede agrupar por nombre de columna con **Group By (Agrupar por)** (como, por ejemplo, **Type [Tipo]**).
Validar compilación	Valida si la configuración de Panorama tiene una sintaxis correcta y está completa semánticamente. Los resultados muestran los mismos errores y advertencias que una compilación, incluidas las advertencias de dependencia de aplicaciones y la observación de reglas. 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.
Las siguientes opciones se aplican cuando se envía cambios de configuración a dispositivos gestionados mediante la selección de **Commit (Compilar)** > **Push to Devices (Enviar a dispositivos)** o **Commit (Compilar)** > **Commit and Push (Compilar y enviar)**.	
Ámbito de envío	Enumera las ubicaciones donde hay cambios que enviar. Las ubicaciones incluidas en el ámbito de forma predeterminada dependen de cuál de las siguientes opciones seleccione: • **Commit (Compilar)** > **Commit and Push (Compilar y enviar)**: el ámbito incluye todas las ubicaciones con cambios que requieren compilación de Panorama. • **Compilar** > **Enviar a dispositivos**: el ámbito incluye todas las ubicaciones asociadas con entidades (cortafuegos, sistemas virtuales, recopiladores de logs, clústeres de WildFire, dispositivos de WildFire) que están `No sincronizados` con la configuración en ejecución de Panorama (consulte Panorama > Dispositivos gestionados > Resumen y Panorama > Recopiladores gestionados para obtener información sobre el estado de sincronización). Para ambas opciones, Panorama filtra el **Push Scope (Ámbito de envío)** de la siguiente manera: • **Administradores**: Panorama aplica los mismos filtros que para **Commit Scope (Ámbito de compilación)** (consulte Commit All Changes o Commit Changes Made By). • **Dominios de acceso**: si ha implementado dominios de acceso, Panorama filtra automáticamente el **Push Scope (Ámbito de envío)** en función de dichos dominios (ver Panorama > Access Domains). Independientemente de su función administrativa y

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	de sus opciones de filtrado, el ámbito solo incluye los cambios de configuración en los dominios de acceso asignados a su cuenta. Puede editar la selección (Edit Selections) de **Push Scope (Ámbito de envío)** en lugar de aceptar las ubicaciones predeterminadas.
Tipo de ubicación	Esta columna categoriza las ubicaciones de los cambios pendientes: • **Device Groups (Grupos de dispositivos)**: configuraciones definidas en un grupo de dispositivos específico. • **Template (Plantilla)**: configuraciones definidas en una plantilla o pila de plantillas específica. • **Log Collector Groups (Grupos de recopiladores de log)**: ajustes específicos de una configuración de grupo de recopiladores. • **WildFire Clusters (Clústeres WildFire)**: ajustes específicos de una configuración de clúster WildFire. • **WildFire Appliances (Dispositivos WildFire)**: ajustes específicos de una configuración de un dispositivo WildFire.
Entidades	Para cada grupo de dispositivos o plantilla, esta columna muestra los cortafuegos (por nombre de dispositivo o número de serie) o sistemas virtuales (por nombre) incluidos en el envío. *Si envía cambios en un grupo de recopiladores, la operación incluye todos los recopiladores de logs que pertenecen al grupo, aunque no se enumeran.*
Editar selecciones	Haga clic para seleccionar las entidades que incluir en el envío: • Device Groups and Templates • Grupos de recopiladores de logs • Clústeres y dispositivos WildFire *Panorama no le permitirá enviar cambios que aún no se hayan compilado en la configuración de Panorama.*
Device Groups and Templates	Haga clic en **Edit Selections (Editar selecciones)** y seleccione **Device Groups (Grupos de dispositivos)** o **Templates (Plantillas)** para ver las opciones de las filas a continuación.
Filtros	Filtre la lista de plantillas, pilas de plantillas o grupos de dispositivos y los sistemas virtuales y cortafuegos asociados.
Nombre	Seleccione plantillas, pilas de plantillas, grupos de dispositivos, cortafuegos o sistemas virtuales que incluir en el envío.
Último estado de compilación	Indica si la configuración del sistema virtual y el cortafuegos están sincronizados con la configuración del grupo de dispositivos o la plantilla en Panorama.
Estado HA	Indica el estado de alta disponibilidad (HA) de los cortafuegos detallados:

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	• **Active (Activo)**: estado operativo de gestión de tráfico normal. • **Sassive (Pasivo)**: estado de copia de seguridad normal. • **Initiating (Iniciándose)**: el cortafuegos se encuentra en este estado por hasta 60 segundos desde el arranque. • **Non-functional (No funcional)**: estado de error. • **Suspended (Suspendido)**: un administrador deshabilitó el cortafuegos. • **Tentative (Tentativo)**: para una monitorización de enlace o ruta en una configuración activo/activo.
Cambios con compilación pendiente (Panorama)	Indica si la compilación en Panorama es (`sí`) o no es (`no`) necesaria antes de enviar los cambios a los cortafuegos y sistemas virtuales seleccionados.
Columna Preview Changes	Haga clic en **Preview Changes (Vista previa de cambios)** para comparar las configuraciones seleccionadas en **Push Scope (Ámbito de envío)** con la configuración en ejecución en Panorama. Panorama filtra los resultados y solo muestra los de los cortafuegos y sistemas virtuales seleccionados en la pestaña **Device Groups (Grupos de dispositivos)** o **Templates (Plantillas)**. La ventana de vista previa utiliza codificación de colores para indicar qué cambios son adiciones (verde), modificaciones (amarillo) o eliminaciones (rojo). *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.*
Seleccionar todo	Selecciona todas las entradas de la lista.
Anular selección	Anula la selección de todas las entradas de la lista.
Expandir todo	Muestra los cortafuegos y sistemas virtuales asignados a las plantillas, pilas de plantillas o grupos de dispositivos.
Contraer todo	Muestra solo las plantillas, pilas de plantillas o grupos de dispositivos, no muestra los cortafuegos o sistemas virtuales asignados a estos.
Agrupar Peers HA	Agrupa cortafuegos que son peers en una configuración de alta disponibilidad (HA). La lista resultante muestra primero el cortafuegos activo (o activo-principal en una configuración activo/activo) y luego el cortafuegos pasivo (o activo-secundario en una configuración activo/activo) entre paréntesis. Esto le permite identificar fácilmente los cortafuegos en el modo HA. Al enviar políticas compartidas, puede implementar el par agrupado, en lugar de peers individuales. *Para los peers HA en una configuración de activo/pasivo, tenga en cuenta que puede añadir ambos cortafuegos o sus sistemas virtuales al mismo grupo, plantilla o pila de plantillas de modo que pueda*

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
	aplicar la configuración a ambos peers de manera simultánea.
Validar	Haga clic para validar las configuraciones que va a enviar a los cortafuegos y sistemas virtuales seleccionados. El Administrador de tareas se abre automáticamente para mostrar el estado de validación.
Filtro seleccionado	Si desea que la lista muestre solo cortafuegos o sistemas virtuales específicos, selecciónelos y, a continuación, **Filter Selected (Filtrar seleccionados)** .
Combinar con configuración de candidato	(Seleccionado de manera predeterminada) Combina los cambios de configuración enviados de Panorama con los cambios de configuración pendientes implementados localmente por administradores en el cortafuegos de destino. El envío obliga a PAN-OS® a compilar los cambios combinados. Si borra esta selección, la compilación excluirá la configuración candidata en el cortafuegos. *Borre esta selección si permite que los administradores de cortafuegos compilen los cambios localmente en un cortafuegos y no desea incluir esos cambios locales al compilar cambios de Panorama.* Otra práctica recomendada es realizar una auditoría de configuración en el cortafuegos para revisar los cambios locales antes de enviar cambios de Panorama (consulte Device > Config Audit).
Incluir plantillas dispositivo y red (Solo en la pestaña Grupos de dispositivos)	(Seleccionado de manera predeterminada) Envía los cambios de grupo de dispositivos y los de plantilla asociados a los cortafuegos y sistemas virtuales seleccionados en una sola operación. Deje esta opción en blanco para enviar estos cambios en operaciones diferentes.
Forzar valores de plantilla	(Deshabilitado de manera predeterminada) Anula toda la configuración local y elimina todos los objetos de los cortafuegos seleccionados que no existen en la plantilla o pila de plantillas, o que están anulados en la configuración local. El envío revierte toda la configuración existente del cortafuegos y garantiza que el cortafuegos solamente herede los ajustes definidos en la plantilla o pila de plantillas. *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.*

© 2020 Palo Alto Networks, Inc.

Campo/Botón	Description (Descripción)
Grupos de recopiladores de logs	Haga clic en **Edit Selections (Editar selecciones)** y seleccione **Log Collector Groups (Grupos de recopiladores de logs)** para incluirlos en el envío. Esta pestaña muestra las siguientes opciones: • **Select All (Seleccionar todo)**: selecciona todos los grupos de recopiladores de la lista. • **Deselect All (Anular selección)**: anula la selección de todos los grupos de recopiladores de la lista.
Clústeres y dispositivos WildFire	Haga clic en **Edit Selections (Editar selecciones)** y seleccione **WildFire Appliances and Clusters (Clústeres y dispositivos WildFire)** para mostrar las siguientes opciones.
Filtros	Filtra la lista de dispositivos y clústeres WildFire.
Nombre	Seleccione los dispositivos y clústeres WildFire a los que Panorama enviará los cambios.
Último estado de compilación	Indica si la configuración del dispositivo y clúster WildFire está sincronizada con Panorama.
Eliminar selecciones	Permite eliminar todos los cortafuegos que aparecen en el ámbito de envío.
Validar envío de grupo de dispositivos	Valida las configuraciones que está enviando a los grupos de dispositivos en la lista Push Scope. El Administrador de tareas se abre automáticamente para mostrar el estado de validación.
Validar envío de plantilla	Valida las configuraciones que está enviando a las plantillas en la lista Push Scope. El Administrador de tareas se abre automáticamente para mostrar el estado de validación.
Group by Location Type	Seleccione para usar el criterio **Location Type (Tipo de ubicación)** para agrupar la lista Push Scope.
Las siguientes opciones se aplican cuando compila la configuración de Panorama o envía cambios a los dispositivos.	
Description (Descripción)	Introduzca una descripción (hasta 512 caracteres) para ayudar a otros administradores a comprender los cambios realizados. *El log del sistema corta las descripciones de compilación si superan los 512 caracteres.*
Commit / Push / Commit and Push	Comienza la compilación o, si existen otras compilaciones pendientes, añade la solicitud a la cola de compilación.

© 2020 Palo Alto Networks, Inc.

Definición de políticas en Panorama

Los grupos de dispositivos en Panorama™ le permiten gestionar políticas de cortafuegos de forma centralizada. En Panorama, las políticas se crean como *Pre Rules (Reglas previas)* o *Post Rules (Reglas posteriores)*; las reglas previas y las reglas posteriores le permiten crear un sistema de capas para la implementación de la política.

Puede definir las reglas previas o posteriores en un contexto compartido como políticas compartidas para todos los cortafuegos gestionados o, en un grupo de dispositivos, como específicas para un grupo de dispositivos concreto. Debido a que las reglas previas y posteriores se definen en Panorama y, a continuación, se envían de Panorama a los cortafuegos gestionados, podrá ver las reglas en los cortafuegos gestionados, pero solo podrá editar las reglas previas y posteriores en Panorama.

- **Pre Rules (Reglas previas)**: reglas añadidas a la parte superior del orden de las reglas y que se evalúan en primer lugar. Puede utilizar las reglas previas para aplicar la política de uso aceptable de una organización. Por ejemplo, puede bloquear el acceso a categorías URL concretas o permitir el tráfico DNS para todos los usuarios.
- **Post Rules (Reglas posteriores)**: reglas que se añaden al final del orden de reglas y que se evalúan después de las reglas previas y de las reglas definidas localmente en el cortafuegos. Las reglas posteriores suelen incluir reglas para impedir el acceso al tráfico basado en App-ID™, User-ID™ o servicio.
- **Default Rules (Reglas predeterminadas)**: reglas que especifican al cortafuegos cómo gestionar el tráfico que no coincide con ninguna regla previa, regla posterior o regla local de un cortafuegos. Estas reglas son parte de la configuración predefinida de Panorama. Para **Override (Cancelar)** y habilitar la edición de los ajustes seleccionados en estas reglas, consulte Cancelación o reversión de una regla de política de seguridad.

Utilice **Preview Rules (Vista previa de reglas)** para ver una lista de las reglas antes de enviarlas a los cortafuegos gestionados. En cada base de reglas, la jerarquía de las mismas se marca visualmente para cada grupo de dispositivos (y cortafuegos gestionado), lo que permite revisarlas entre un gran número de reglas.

Cuando añade una regla nueva, se muestran los datos operativos estáticos para la regla. La columna del identificador único universal (Universal Unique Identifier, UUID) muestra el UUID de 36 caracteres para la regla. El cortafuegos genera el UUID según cada regla. Sin embargo, si está enviando reglas desde Panorama, estas reglas poseen el mismo UUID, que también se muestra en la vista previa de reglas combinadas. La columna **Created (Creada)** muestra la hora y fecha en que la regla se añadió a la base de reglas. Además, la columna **Modified (Modificada)** muestra la hora y fecha de la última vez que se editó la regla. Si se creó una regla de política antes de la actualización a PAN-OS 9.0, se utilizan los datos de **First Hit (Primer resultado)** para establecer la fecha **Created (Creada)**. Si no hay datos de **First Hit (Primer resultado)** disponibles para la regla, se usará la fecha y hora en que se actualizó el servidor de gestión de Panorama o el cortafuegos con PAN-OS 9.0 para establecer la fecha **Created (Creada)**.

Cuando agrega o edita una regla en Panorama, se muestra una pestaña **Target (Objetivo)**. Puede usar esta pestaña para aplicar la regla a cortafuegos específicos o a grupos de dispositivos descendientes **Device Group (Grupo de dispositivos)** (u ubicación compartida) donde se define la regla. En la pestaña **Target (Objetivo)**, puede seleccionar **Any (Cualquiera)** (predeterminado), lo que significa que la regla se aplica a todos los cortafuegos y los grupos de dispositivos descendientes. Para actuar sobre cortafuegos o grupos de dispositivos concretos, anule la selección de **Any (Cualquiera)** y selecciónelos por nombre. Para excluir cortafuegos o grupos de dispositivos específicos, anule la selección de **Any (Cualquiera)**, selecciónelos por nombre y seleccione **Target to all but these specified devices (Todos excepto estos dispositivos concretos)**. Si la lista de grupos de dispositivos y cortafuegos es larga, puede aplicar Filtros para buscar las entradas por atributos (como Plataformas) o por una cadena de texto para nombres coincidentes.

Después de añadir y enviar correctamente una regla a Panorama, **Rule Usage (Uso de reglas)** muestra si a la regla la Utilizan todos los dispositivos en el grupo de dispositivos, la Utilizan parcialmente algunos dispositivos en el grupo de dispositivos o No la utilizan los dispositivos en el grupo de dispositivos.

© 2020 Palo Alto Networks, Inc.

Panorama determina la utilización de la regla basado en los cortafuegos gestionados con la opción Policy Rule Hit Count (Conteo de resultados de reglas de la política) (habilitada de manera predeterminada). En el contexto de Panorama, puede ver la utilización de reglas para una regla de la política compartida en todos los grupos de dispositivos. Además, puede cambiar el contexto a un grupo individual de dispositivos y ver la utilización total de la regla de la política en todos los dispositivos en el grupo de dispositivos. **Preview Rules (Vista previa de las reglas)** mostrará el **Hit Count (Recuento de resultados)**, **Last Hit (Último resultado)** y **First Hit (Primer resultado)** para cada regla de política del grupo de dispositivos. El conteo total de resultados de tráfico, además de las marcas de tiempo del primer y el último resultado, permanecen tras los reinicios, las actualizaciones y los eventos de reinicio del plano de datos. Consulte Monitor Policy Rule Usage (Supervisar la utilización de las regla de la política).

Seleccione **Group Rules by Tag (Agrupar reglas por etiquetas)** para aplicar una etiqueta que le permita agrupar reglas de políticas similares para una mejor visualización de las funciones de la regla, y para proporcionar una gestión más sencilla de las reglas de política en su base de reglas. Las reglas agrupadas por etiquetas muestran la lista de grupos de etiquetas, pero mantienen el listado de prioridad de las reglas. Puede anexar reglas al final de un grupo de etiquetas, mover las reglas a un grupo de etiquetas diferente, aplicar etiquetas adicionales a las reglas en un grupo de etiquetas y filtrar o buscar usando el grupo de etiquetas.

Para registrar los cambios a las reglas de política, añada un **Audit Comment (Comentario de auditoría)** para describir los cambios que realice y por qué se creó o modificó una regla. Después de introducir un comentario de auditoría y de confirmar el cambio de la configuración, el comentario de auditoría se mantiene en el **archivo de comentario de auditoría**, donde puede ver todos los comentarios de auditoría anteriores para la regla seleccionada. Puede buscar el comentario de auditoría en Global Find. El archivo de comentario de auditoría es de solo lectura.

Los usuarios administrativos con acceso a la pestaña Policies (Políticas) pueden exportar las reglas de la política que se muestran en la interfaz web como **PDF/CSV**. Consulte Datos de la tabla de configuración de exportación.

Para crear políticas, consulte la sección relevante de cada base de reglas.

- Políticas > Seguridad
- Políticas > NAT
- Políticas > QoS
- Políticas > Reenvío basado en políticas
- Políticas > Descifrado
- Policies > Application Override
- Políticas > Autenticación
- Políticas > Protección DoS
- Políticas > SD-WAN

© 2020 Palo Alto Networks, Inc.

Particiones de almacenamiento de log para un dispositivo virtual de Panorama en modo Legado

- Panorama > Setup > Operations

De forma predeterminada, un dispositivo virtual Panorama en modo Legacy cuenta con una sola partición de disco para todos los datos, en la que se asignan 10,89 GB para el almacenamiento de logs. Incrementar el tamaño del disco no aumenta la capacidad de almacenamiento de logs. Sin embargo, puede modificar la capacidad de almacenamiento de logs mediante las siguientes opciones:

- **Network File System (NFS) (Sistema de archivos de red [NFS])**: la opción para montar el almacenamiento NFS solo está disponible para un dispositivo virtual Panorama en modo Legacy que se ejecute en un servidor VMware ESXi. Para montar un almacenamiento NFS, seleccione **Storage Partition Setup (Configuración de partición de almacenamiento)** en la sección Miscellaneous (Varios), configure **Storage Partition (Partición de almacenamiento)** en **NFS V3** y realice los ajustes como se indica en la Tabla: de la configuración de almacenamiento NFS.
- **Almacenamiento interno predeterminado**: revierta las opciones a la partición predeterminada de almacenamiento interno (solo en Panorama en un servidor ESXi o en la plataforma vCloud Air donde previamente haya configurado otro disco de logs virtual o montado en un NFS). Para volver a la partición predeterminada de almacenamiento interno, seleccione **Storage Partition Setup (Configuración de partición de almacenamiento)** en la sección Miscellaneous (Varios) y configure la **Storage Partition (Partición de almacenamiento)** en **Internal (Interno)**.
- **Disco de logs virtual**: puede añadir otro disco virtual (de hasta 8 TB) para Panorama si se ejecuta en VMware ESXi versión 5.5 y posteriores o para Panorama si se ejecuta en la plataforma VMware vCloud Air. Sin embargo, Panorama deja de utilizar el almacenamiento de logs predeterminado de 10,89 GB en el disco original y copia los logs existentes en el disco nuevo. Las versiones anteriores de ESXi solo admiten discos virtuales de hasta 2 TB.

Debe reiniciar Panorama después de cambiar la configuración de la partición de almacenamiento: seleccione Panorama > Setup (Configuración) > Operations (Operaciones) y Reboot Panorama (Reiniciar Panorama).

El almacenamiento NFS no está disponible para el dispositivo virtual Panorama en modo Panorama ni en los dispositivos M-Series.

Table 1: Tabla: Configuración de almacenamiento NFS

Configuración de la partición de almacenamiento de Panorama: NFS V3	Description (Descripción)
Servidor	Especifique el FQDN o dirección IP del servidor NFS.
Directorio de log	Especifique el nombre de ruta completo del directorio en el que se almacenarán los logs.
PROTOCOL	Especifique el protocolo (UDP o TCP) para la comunicación con el servidor NFS.

© 2020 Palo Alto Networks, Inc.

Configuración de la partición de almacenamiento de Panorama: NFS V3	Description (Descripción)
Puerto	Especifique el puerto para la comunicación con el servidor NFS.
Tamaño de lectura	Especifique el tamaño máximo en bytes (el intervalo es de 256 a 32 768) para las operaciones de lectura de NFS.
Tamaño de escritura	Especifique el tamaño máximo en bytes (el intervalo es de 256 a 32 768) para las operaciones de escritura de NFS.
Copy on Setup (Copiar al configurar)	Seleccione esta opción para montar la partición NFS y copiar los logs existentes al directorio de destino del servidor cuando se inicie Panorama.
Partición de logs de prueba	Seleccione esta opción para realizar una prueba que monta la partición NFS y muestra un mensaje de acción satisfactoria o fallida.

© 2020 Palo Alto Networks, Inc.

Panorama > Configuración > Interfaces

Seleccione **Panorama** > **Setup (Configuración)** > **Interfaces (Interfaces)** para configurar las interfaces que utiliza Panorama para gestionar cortafuegos y recopiladores de logs, implementar software y actualizaciones de contenido en cortafuegos y recopiladores de logs, recopilar logs de cortafuegos y comunicarse con grupos de recopiladores. De forma predeterminada, Panorama utiliza la interfaz MGT para comunicarse con el cortafuegos y los recopiladores de logs.

Para reducir el tráfico en la interfaz MGT, configure otras interfaces para implementar actualizaciones, recopilar logs y comunicarse con los grupos de recopiladores. En un entorno con mucho tráfico de logs, puede configurar varias interfaces para la recopilación de logs. Además, para mejorar la seguridad del tráfico de gestión, puede definir una subred independiente (Netmask [Máscara de red] IPv4 o Prefix Length [Longitud del prefijo] IPv6) para la interfaz MGT que sea más privada que las subredes de las otras interfaces.

Las interfaces disponibles dependen del modelo de Panorama.

Interface (Interfaz)	Velocidad máxima	Dispositivo M-500	Dispositivo virtual Panorama
Gestión (Management, MGT)	1Gbps	✓	✓
Ethernet1 (Eth1)	1Gbps	✓	—
Ethernet2 (Eth2)	1Gbps	✓	—
Ethernet3 (Eth3)	1Gbps	✓	—
Ethernet4 (Eth4)	10Gbps	✓	—
Ethernet5 (Eth5)	10Gbps	✓	—

Para configurar una interfaz, haga clic en el nombre de la interfaz y configure los ajustes como se describe en la siguiente tabla.

Siempre debe especificar la dirección IP, la máscara de red (para IPv4) o la longitud de prefijo (para IPv6), y la puerta de enlace predeterminada para la interfaz MGT. Si omite los valores de algunos ajustes (por ejemplo, la puerta de enlace predeterminada), solo puede acceder a Panorama a través del puerto de la consola para futuros cambios de configuración. No puede compilar la configuración de otras interfaces a menos que especifique los tres ajustes.

Configuración de interfaz	Description (Descripción)
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Debe habilitar una interfaz para configurarla. Excepto la interfaz MGT, habilitada de forma predeterminada.

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz	Description (Descripción)
Dirección IP pública	Si sus cortafuegos se conectan a Panorama mediante una dirección IP pública que se traduce en una dirección IP privada (NAT), especifique la dirección IP pública en la interfaz.
Dirección IP (IPv4)	Si su red utiliza IPv4, asigne una dirección IPv4 a la interfaz.
Máscara de red (IPv4)	Si ha asignado una dirección IPv4 a la interfaz, debe introducir también una máscara de red (por ejemplo, 255.255.255.0).
Default Gateway (IPv4)	Si ha asignado una dirección IPv4 a la interfaz, también debe asignar una dirección IPv4 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz).
Dirección IPv6/ longitud de prefijo	Si su red utiliza IPv6, asigne una dirección IPv6 a la interfaz. Para indicar la máscara de red, introduzca una longitud de prefijo IPv6 (por ejemplo, 2001:400:f00::1/64). *Se admite una dirección IPv6 para la interfaz MGT en todos los dispositivos M-Series y dispositivos virtuales Panorama implementados en un entorno de nube privada (ESXi, vCloud Air, KVM y Hyper-V). No se admite una dirección IPv6 para la interfaz MGT en un dispositivo virtual Panorama implementado en un entorno de nube pública (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure y Google Cloud Platform).*
Puerta de enlace IPv6 predeterminada	Si ha asignado una dirección IPv6 a la interfaz, también debe asignar una dirección IPv6 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz). *Se admite una dirección IPv6 para la interfaz MGT en todos los dispositivos M-Series y dispositivos virtuales Panorama implementados en un entorno de nube privada (ESXi, vCloud Air, KVM y Hyper-V). No se admite una dirección IPv6 para la interfaz MGT en un dispositivo virtual Panorama implementado en un entorno de nube pública (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure y Google Cloud Platform).*
Velocidad	Establezca la velocidad de la interfaz a 10Mbps, 100Mbps, 1Gbps o 10Gbps (Eth4 y Eth5 solamente) a dúplex completo o medio. Utilice el ajuste de negociación automática predeterminado para que Panorama determine la velocidad de interfaz. *Este ajuste debe coincidir con la configuración de la interfaz del equipo de red vecino. Para garantizar que los ajustes coinciden, seleccione auto-negotiate si el equipo vecino admite esa opción.*

© 2020 Palo Alto Networks, Inc.

Configuración de interfaz	Description (Descripción)
MTU	Introduzca la unidad máxima de transmisión (MTU, por sus siglas en inglés) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 1500 y el valor predeterminado, 1500).
Recopilación de logs de dispositivo y de gestión de dispositivos	Habilite la interfaz (habilitada de manera predeterminada en la interfaz MGT) para gestionar cortafuegos y recopiladores de logs y recolectar sus logs. Puede habilitar varias interfaces para que realicen estas funciones.
Comunicación del grupo de recopiladores	Habilite la interfaz para la comunicación del grupo de recopiladores (la interfaz predeterminada es MGT). Esta función solo la puede realizar una interfaz.
Implementación de dispositivo	Habilite la interfaz para implementar software y actualizaciones de contenido en cortafuegos y recopiladores de logs (la interfaz predeterminada es MGT). Esta función solo la puede realizar una interfaz.
Servicios de gestión administrativa	• **HTTP**: habilita el acceso a la interfaz web de Panorama. HTTP usa texto sin formato, lo cual no es tan seguro como HTTPS. *Habilite HTTPS en lugar de HTTP para la gestión del tráfico en la interfaz.* • **Telnet**: habilita el acceso a la CLI de Panorama. Telnet usa texto sin formato, lo cual no es tan seguro como SSH. • **HTTPS**: habilita el acceso seguro a la interfaz web de Panorama. *Habilite SSH en lugar de Telnet para la gestión del tráfico en la interfaz.* • **SSH**: permite el acceso seguro a la CLI de Panorama.
Servicios de conectividad de red	El servicio de **Ping** está disponible en cualquier interfaz. Puede utilizar el ping para probar la conectividad entre la interfaz de Panorama y los servicios externos. En una implementación de alta disponibilidad (HA), los peers de HA usan el ping para intercambiar información de copias de seguridad de heartbeat. Los siguientes servicios solo están disponibles en la interfaz MGT: • **SNMP**: permite a Panorama procesar consultas de estadísticas desde un gestor SNMP. Para obtener más información, consulte Habilitación de supervisión de SNMP. • **User-ID**: permite que Panorama redistribuya la información de asignación de usuario recibida de los agentes de User-ID.
Direcciones IP permitidas	Introduzca las direcciones IP desde las que los administradores pueden acceder a Panorama en esta interfaz. Una lista vacía (predeterminada) especifica que el acceso está disponible desde cualquier dirección IP. *No deje esta lista en blanco; especifique las direcciones IP de los administradores de Panorama (solo) para evitar accesos no autorizados.*

© 2020 Palo Alto Networks, Inc.

Panorama > Alta disponibilidad

Para habilitar la alta disponibilidad (HA) en Panorama, configure los ajustes como se describe en la siguiente tabla.

Configuración de HA de Panorama	Description (Descripción)
Configuración Haga clic en Edit ( ) para configurar los siguientes ajustes.	
Habilitar HA	Seleccione esta opción para activar la alta disponibilidad.
Dirección IP HA del peer	Introduzca la dirección IP de la interfaz de gestión del peer.
Habilitar cifrado	Cuando está habilitada, la interfaz de gestión cifra la comunicación entre los peers HA. Antes de habilitar el cifrado, exporte la clave de HA de cada peer HA e importe la clave en el otro peer. Puede importar y exportar la clave HA en la página **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** (consulte Gestión de certificación de cortafuegos y Panorama). *La conectividad de HA utiliza el puerto TCP 28 con el cifrado habilitado y el puerto TCP 28769 cuando el cifrado no está habilitado.*
Tiempo de espera para monitorización (ms)	Introduzca la cantidad de milisegundos que el sistema esperará antes de reaccionar ante un fallo de un enlace de control (el intervalo es de 1000 a 60 000; el valor predeterminado es 3000).
Configuración de elección Haga clic en Edit ( ) para configurar los siguientes ajustes.	
Prioridad (Requerido en el dispositivo virtual de Panorama)	Esta configuración determina qué peer es el destinatario principal de los logs del cortafuegos. Asigne un peer como **Primary (Primario)** y otro como **Secondary (Secundario)** en el par HA. Cuando configure Particiones de almacenamiento de logs para un dispositivo virtual de Panorama en modo Legacy, puede utilizar su disco interno (predeterminado) o un sistema de archivos de red (NFS) para el almacenamiento de logs. Si configura un NFS, solo el destinatario principal recibe los logs del cortafuegos. Si configura el almacenamiento en disco interno, los cortafuegos envían los logs a los peers principal y secundario de forma predeterminada, pero puede cambiarlo si activa **Only Active Primary Logs to Local Disk (Solo logs principales activos al disco local)** en Logging and Reporting Settings (Configuración de log e informes).
Preferente	Seleccione esta opción para habilitar el dispositivo Panorama principal con el fin de reanudar el funcionamiento activo tras recuperarse de un fallo. Si está

© 2020 Palo Alto Networks, Inc.

Configuración de HA de Panorama	Description (Descripción)
	desactivado, el dispositivo Panorama secundario permanecerá activo incluso después de que el dispositivo Panorama principal se recupere de un fallo.
Configuración del temporizador HA	Su selección determina los valores para las opciones de elección de HA restantes, las cuales controlan la velocidad de la conmutación por error. • **Recommended (Recomendado)**: seleccione esta opción para la configuración de temporizador de conmutación por error típica (predeterminada). Para ver los valores asociados, seleccione **Advanced (Avanzado)** y **Load Recommended (Carga recomendada)**. • **Aggressive (Agresivo)**: seleccione esta opción para la configuración de temporizador de conmutación por error más rápida. Para ver los valores asociados, seleccione **Advanced (Avanzado)** y **Load Aggressive (Carga intensiva)**. • **Advanced (Avanzado)**: seleccione esta opción para mostrar la configuración de elección de HA restante de modo que pueda personalizar sus valores. Consulte los valores **Recommended (Recomendado)** y **Aggressive (Agresivo)** para las siguientes configuraciones.
Tiempo de espera de promoción (ms)	Introduzca la cantidad de milisegundos (el intervalo es de 0 a 60 000) que el peer secundario de Panorama espera antes de tomar el control después de que el peer principal tenga un fallo. El valor recomendado (predeterminado) es 2.000; el valor intensivo es 500.
Hello Interval (ms)	Introduzca la cantidad de milisegundos (el intervalo es de 8000 a 60 000) entre los paquetes de saludo enviados para verificar que el otro peer funciona. El valor recomendado (predeterminado) e intensivo es 8.000.
Intervalo de heartbeat (ms)	Especifique la frecuencia en milisegundos (el intervalo es de 1000 a 60 000) con la que Panorama envía pings ICMP al peer de HA. El valor recomendado (predeterminado) es 2.000; el valor intensivo es 1.000.
Preemption Hold Time (min)	Este campo se aplica solamente si también selecciona **Preemptive (Preferente)**. Introduzca la cantidad de minutos (el intervalo es de 1 a 60) que el peer pasivo de Panorama tiene que esperar antes de recuperar el estado activo tras recuperarse de un evento que provoque una conmutación por error. El valor recomendado (predeterminado) e intensivo es 1.
Tiempo de espera ascendente tras fallo de supervisor (ms)	Especifique la cantidad de milisegundos (el intervalo es de 0 a 60 000) que Panorama espera después de un fallo del supervisor de ruta antes de intentar volver al estado pasivo. Durante este período, el peer pasivo no está disponible para tomar el control como peer activo en el caso de fallo. Este intervalo permite que Panorama evite una conmutación por error debido a los flaps ocasionales de los dispositivos vecinos. El valor recomendado (predeterminado) e intensivo es 0.
Tiempo de espera principal adicional (ms)	Especifique la cantidad de milisegundos (el intervalo es de 0 a 60 000) durante los cuales el peer de prevención permanece en el estado pasivo antes de tomar el control como peer activo. El valor recomendado (predeterminado) es 7.000; el valor intensivo es 5.000.

© 2020 Palo Alto Networks, Inc.

Configuración de HA de Panorama	Description (Descripción)
Monitorización de rutas Haga clic en Edit ( ) para configurar la supervisión de rutas de HA.	
Habilitado	Seleccione esta opción para habilitar la supervisión de rutas. La monitorización de rutas permite que Panorama supervise direcciones IP de destino especificadas enviando mensajes de ping ICMP para verificar que responden.
Condición de fallo	Seleccione si se produce una conmutación por error cuando **Any (Cualquiera)** o **All (Todos)** los grupos de rutas supervisados presentan fallos al responder.
Grupo de rutas Para crear un grupo de rutas para la monitorización de ruta HA, haga clic en **Add (Añadir)** y complete los siguientes campos.	
Nombre	Especifique un nombre para el grupo de rutas.
Habilitado	Seleccione esta opción para habilitar el grupo de rutas.
Condición de fallo	Seleccione si se produce un fallo cuando **Any (Cualquiera)** o **All (Todas)** las direcciones de destino especificadas presentan fallos al responder.
intervalo de pings	Especifique la cantidad de milisegundos entre los mensajes ICMP de eco que verifican que la ruta a la dirección IP de destino está activa (el intervalo es de 1000 a 60 000; el valor predeterminado es 5000).
Recuento de pings	Especifique la cantidad de pings fallidos antes de declarar un fallo (el intervalo es de 3 a 10 pings; el valor predeterminado es 3).
IP de destino	Introduzca una o más direcciones IP de destino a supervisar. Utilice comas para separar múltiples direcciones.

© 2020 Palo Alto Networks, Inc.

Panorama > Clústeres Wildfire gestionados

- Panorama > Clústeres Wildfire gestionados
- Panorama > Managed WildFire Appliances

Puede gestionar dispositivos WildFire en clústeres o como dispositivos independientes desde una M-Series o dispositivo virtual de Panorama. La gestión de clústeres (**Panorama** > **Managed WildFire Clusters [Clústeres Wildfire gestionados]**) y la gestión de dispositivos independientes (**Panorama** > **Managed WildFire Appliances [Dispositivos Wildfire gestionados]**) comparten muchas tareas administrativas y de configuración comunes por lo que ambas se incluyen en los siguientes temas.

Tras añadir dispositivos WildFire a Panorama, utilice la interfaz web para añadir dichos dispositivos y gestionarlos como clústeres o para gestionarlos como dispositivos independientes.

- Tareas de clústeres Wildfire gestionados
- Tareas de dispositivos Wildfire gestionados
- Información de Wildfire gestionada
- Clúster WildFire gestionado y administración de dispositivos

Tareas de clústeres Wildfire gestionados

Puede crear en Panorama clústeres de dispositivos WildFire, así como eliminarlos. Además, puede ahorrar tiempo de configuración gracias a la función de importación de configuración de un clúster a otro.

Tarea	Description (Descripción)
Crear clúster	Según sea necesario, cree un clúster (**Create Cluster [Crear clúster]**), escriba un nombre para el nuevo clúster y haga clic en **OK (Aceptar)**. Los clústeres existentes configurados localmente y añadidos a Panorama mediante la incorporación de nodos individuales de dispositivo WildFire aparecen junto con sus nodos y funciones de nodo de WildFire (**Panorama** > **Managed WildFire Appliances [Dispositivos WildFire gestionados]**). El nombre del clúster debe ser un nombre de subdominio válido que empiece por un caracter en minúscula o un número y solo puede contener guiones que no sean el primer ni el último carácter del nombre del clúster (no se admiten espacios ni otros caracteres). La longitud máxima de un nombre de clúster es de 63 caracteres. Después de crearlo, al clúster puede agregar dispositivos gestionados de WildFire y administrarlos en Panorama. Cuando agrega un dispositivo WildFire a Panorama, registra automáticamente el dispositivo con Panorama. Puede crear hasta 10 clústeres WildFire gestionados en Panorama y cada uno de ellos puede tener hasta 20 nodos de dispositivo WildFire. Panorama puede gestionar hasta un total agregado de 200 dispositivos independientes y nodos de clústeres.
Importar configuración de clúster	Seleccione la opción **Import Cluster Config (Importar configuración de clúster)** para importar una configuración de clúster existente. Si selecciona un clúster antes de importar una configuración de clúster (**Import Cluster Config [Importar configuración de clúster]**), el **Controller (Controlador)** y el **Cluster** se rellenan automáticamente con la información oportuna del clúster seleccionado. Si no selecciona ningún clúster antes de seleccionar

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	Import Cluster Config (Importar una configuración de clúster), entonces debe seleccionar el **Controller (Controlador)** y el **Cluster (Clúster)** se rellenará automáticamente en función del nodo de controlador que seleccione. Tras importar la configuración, seleccione **Commit to Panorama (Compilar en Panorama)** para guardar la configuración candidata importada en la configuración de Panorama en ejecución.
Eliminar de Panorama	Si ya no necesita gestionar ningún clúster WildFire desde Panorama, haga clic en **Remove From Panorama (Eliminar de Panorama)** y seleccione **Yes (Sí)** para confirmar la acción. Después de eliminar un clúster de la gestión de Panorama, puede administrar el clúster localmente desde un nodo Controller. Puede volver a añadir el clúster al dispositivo de Panorama en cualquier momento si desea volver a gestionarlo de forma centralizada en lugar de local.
Encrypt WildFire Cluster Appliance-to-Appliance Communications (Cifrar comunicaciones de dispositivo a dispositivo dentro de un clúster de WildFire)	Para cifrar la comunicación de datos entre los dispositivos de WildFire en un clúster, haga clic en **Enable (Habilitar)** para habilitar el cifrado en **Secure Cluster Communication (Comunicación segura del clúster)**. WildFire utiliza un certificado predefinido o un certificado personalizado para comunicarse entre los dispositivos. Los certificados personalizados solo se utilizan cuando selecciona la opción **Customize Secure Server Communication (Personalizar comunicación segura del servidor)** y habilita **Custom Certificate Only (Certificado personalizado únicamente)**. Se requiere el cifrado en los clústeres de WildFire para funcionar en modo FIPS-CC. Los certificados personalizados utilizados en modo FIPS-CC deben cumplir con los requisitos de FIPS-CC. Después de habilitar la comunicación segura del clúster, puede añadir dispositivos de WildFire gestionados adicionales al clúster. Los dispositivos añadidos más recientes utilizan automáticamente la configuración de comunicación segura del clúster.

Tareas de dispositivos Wildfire gestionados

Puede agregar, eliminar y gestionar dispositivos WildFire independientes en un dispositivo de Panorama. Después de añadir dispositivos independientes, puede añadirlos a clústeres de dispositivos WildFire como nodos de clúster o gestionarlos como dispositivos independientes separados.

Tarea	Description (Descripción)
Añadir dispositivo	**Add Appliance** para añadir uno o más dispositivos WildFire a un dispositivo de Panorama y llevar una gestión centralizada. Introduzca el número de serie de cada dispositivo WildFire en una fila aparte (una nueva línea). Panorama puede gestionar hasta un total agregado de 200 nodos de clúster WildFire y dispositivos WildFire independientes. Configure la dirección IP o FQDN del dispositivo de Panorama (servidor Panorama) en cada dispositivo WildFire que desee gestionar en Panorama y, opcionalmente, el servidor de Panorama de copia de seguridad utilizando los siguientes comandos de la CLI del dispositivo WildFire:

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	`set deviceconfig system panorama-server <ip-address | FQDN>` `set deviceconfig system panorama-server-2 <ip-address | FQDN>`
Importar configuración	Seleccione un dispositivo WildFire y haga clic en **Import Config (Importar configuración)** para importar solo la configuración en ejecución de ese dispositivo a Panorama. Tras importar la configuración, seleccione **Commit to Panorama (Compilar en Panorama)** para guardar la configuración candidata importada en la configuración de Panorama en ejecución.
Eliminar	Si ya no necesita gestionar ningún dispositivo WildFire desde Panorama, haga clic en **Remove (Eliminar)** para eliminar el dispositivo y seleccione **Yes (Sí)** para confirmar la acción. Tras eliminar un dispositivo de la gestión de Panorama, puede gestionar el dispositivo de forma local con su CLI. Si es necesario, puede volver a añadir el dispositivo al dispositivo de Panorama en cualquier momento si desea volver a gestionar el dispositivo de forma centralizada en lugar de local.

Información de Wildfire gestionada

Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres Wildfire gestionados)** para mostrar la siguiente información de cada clúster gestionado (también puede seleccionar dispositivos independientes de esta página y mostrar su información) o seleccione **Panorama** > **Managed WildFire Appliances (Dispositivos WildFire gestionados)** para mostrar la información de los dispositivos independientes.

A menos que se indique lo contrario, la información de la siguiente tabla se aplica tanto a los clústeres de WildFire como a los dispositivos independientes. La información previamente configurada para un clúster o un dispositivo está propagada.

Información de Wildfire gestionada	Description (Descripción)
Dispositivo	El nombre del dispositivo. La vista Managed WildFire Clusters (Clústeres Wildfire gestionados) muestra los dispositivos agrupados por clústeres, incluye los dispositivos independientes que se pueden agregar a un clúster e incluye el número de serie (entre paréntesis) y el nombre de cada dispositivo (el número de serie no forma parte del nombre).
Número de serie (Solo en la vista Managed WildFire Appliances)	El número de serie del dispositivo. La vista Managed WildFire Clusters (Clústeres Wildfire gestionados) muestra el número de serie en la misma columna que el nombre del dispositivo (el número de serie no forma parte del nombre).
Versión de software	La versión de software instalada y en ejecución en el dispositivo.

© 2020 Palo Alto Networks, Inc.

Información de Wildfire gestionada	Description (Descripción)
Dirección IP	La dirección IP del dispositivo.
Conectado	El estado de la conexión entre el dispositivo y Panorama: Connected (Conectado) o Disconnected (Desconectado).
Nombre de clústeres	El nombre del clúster en el que se incluye el dispositivo como nodo; aquí no se muestra nada de dispositivos independientes.
Entorno de análisis	El entorno de análisis (vm1, vm2, vm3, vm4 o vm5). Cada entorno de análisis representa un conjunto de sistemas operativos y aplicaciones: • vm-1 es compatible con Windows XP, Adobe Reader 9.3.3, Flash 9, PE, PDF y Office 2003 y versiones anteriores de Office. • vm-2 es compatible con Windows XP, Adobe Reader 9.4.0, Flash 10n, PE, PDF y Office 2007 y versiones anteriores de Office. • vm-3 es compatible con Windows XP, Adobe Reader 11, Flash 11, PE, PDF y Office 2010 y versiones anteriores de Office. • vm-4 es compatible con Windows 7 de 32 bits, Adobe Reader 11, Flash 11, PE, PDF y Office 2010 y versiones anteriores de Office. • vm-5 es compatible con Windows 7 de 64 bits, Adobe Reader 11, Flash 11, PE, PDF y Office 2010 y versiones anteriores de Office.
Contenido	El número de versión de la versión de publicación de contenido.
Función	La función del dispositivo: • **Standalone (Independiente)**: el dispositivo no es un nodo de clúster. • **Controller (Controlador)**: el dispositivo es el nodo Controller del clúster. • **Controller Backup (Backup de controlador)**: el dispositivo es el nodo Controller Backup del clúster. • **Worker (Trabajador)**: el dispositivo es un nodo Worker del clúster.
Estado de configuración	El estado de sincronización de la configuración del dispositivo. El dispositivo de Panorama comprueba la configuración del dispositivo WildFire e informa de las diferencias de configuración entre la configuración del dispositivo y aquella guardada en Panorama para dicho dispositivo. • **In Sync (Sincronizado)**: la configuración del dispositivo está sincronizada con la configuración guardada en Panorama. • **Out of Sync (Sin sincronización)**: la configuración del dispositivo no está sincronizada con la configuración guardada en Panorama. Puede pasar el ratón por la lupa para mostrar la causa del fallo de sincronización.

Estado de clúster
(Solo en la página Managed WildFire Clusters)
	Cluster Status (Estado de clúster) muestra tres tipos de información de cada nodo de clúster:
	• Los servicios disponibles (en condiciones normales de funcionamiento):
	  • **wfpc** (WildFire Private Cloud): el servicio de análisis de muestras de malware y de generación de informes.
	  • **signature (firma)**: el servicio local de generación de firmas.

© 2020 Palo Alto Networks, Inc.

Información de Wildfire gestionada	Description (Descripción)

	• Progreso de las operaciones: el nombre de la operación seguido de dos puntos (:) y el estado:
	  • **Operations (Operaciones)**: el estado de las operaciones de desactivación, suspensión y reinicio.
	  • **Progress status (Progreso)**: las notificaciones de estado de la operación son las mismas para cada operación: requested (solicitada), ongoing (en curso), denied (denegada), success (con éxito) o fail (fallida).
	  Por ejemplo, si suspende un nodo y la operación está en curso, Cluster Status (Estado de clúster) mostrará `suspend:ongoing`, o si reinicia un nodo y se ha solicitado la operación, pero aún no se ha iniciado, Cluster Status muestra `reboot:requested`.
	• Condiciones de error:
	  Cluster Status (Estado de clúster) muestra las siguientes condiciones de error:
	  • **Cluster**: `cluster:offline` o `cluster:splitbrain`.
	  • **Service (Servicio)**: `service:suspended` or `service:none`.

Último estado de compilación	`Commit succeeded (Compilación correcta)` si la compilación más reciente se realizó correctamente o `commit failed (Fallo de compilación)` si falló. Seleccione cada estado para conocer más información sobre la última compilación.
Utilization > View	

Ver	La opción **View (Ver)** le permite ver estadísticas de uso del clúster o del dispositivo. Solo puede ver dispositivos individuales (**Panorama** > **Managed WildFire Appliances [Dispositivos WildFire gestionados]**) o solo estadísticas de clústeres (**Panorama** > **Managed WildFire Clusters [Clústeres Wildfire gestionados]**).
	• **Appliance (Dispositivo)**: (solo vista de dispositivos independientes) el número de serie del dispositivo.
	• **Cluster**: (solo vista de clústeres) el nombre del clúster. También puede seleccionar un clúster diferente para verlo.
	• **Duration (Duración)**: muestra el periodo de tiempo durante el que se recopilan y se muestran las estadísticas. Puede seleccionar diferentes duraciones:
	  • **15 min.**
	  • **Última hora**
	  • **Last 24 Hours (predeterminada)**
	  • **Últimos 7 días**
	  • **All (Todas)**
	La **View (Vista) Utilization (Utilización)** tiene cuatro pestañas y cada una determina qué se muestra en función de su configuración **Duration (Duración)**.

© 2020 Palo Alto Networks, Inc.

Información de Wildfire gestionada	Description (Descripción)

Pestaña General	La pestaña **General** muestra estadísticas de utilización de recursos agregados de un clúster o un dispositivo. Las otras pestañas muestran información más detallada sobre la utilización de recursos por tipo de archivo:
	• **Total Disk Usage (Uso total del disco)**: la utilización total del disco del clúster o del dispositivo.
	• **Verdict (Veredicto)**: la cantidad **Total** de veredictos, el número de cada tipo de veredicto asignado a los archivos —**Malware**, **Grayware** y **Benign (Benigno)**— y cuántos veredictos eran de **Error**.
	• **Sample Statistics (Estadísticas de muestras)**: la cantidad total de muestras **Submitted (Enviadas)** y **Analyzed (Analizadas)** y cuantas muestras hay **Pending (Pendientes)** de análisis.
	• **Analysis Environment & System Utilization (Entorno de análisis y utilización del sistema)**:
	  • **File Type Analyzed (Tipo de archivo analizado)**: el tipo de archivo que se analizó —**Executable (Ejecutable)**, **Non-Executable (No ejecutable)** o **Links (Enlaces)**—.
	  • **Virtual Machine Usage (Uso de máquinas virtuales)**: la cantidad de máquinas virtuales utilizadas para cada tipo de archivo analizado y cuántas máquinas virtuales están disponibles para analizar cada tipo de archivo. Por ejemplo, para archivos Executables, el uso de máquinas virtuales podría ser de 6/10 (seis máquinas virtuales utilizadas y diez máquinas virtuales disponibles).
	  • **Files Analyzed (Archivos analizados)**: la cantidad de archivos de cada tipo que se analizaron.

Pestañas Executable, Non-Executable y Links	Las pestañas **Executable (Ejecutable)**, **Non-Executable (No ejecutable)** y **Links (Enlaces)** ofrecen información similar de cada tipo de archivo:
	• **Verdict (Veredicto)**: detalles de veredictos por cada tipo de archivo. Puede filtrar los resultados:
	  • **Search box (Cuadro de búsqueda)**: introduzca los términos de búsqueda por los que desea filtrar los veredictos. El cuadro de búsqueda indica la cantidad de tipos de archivo (elementos) de la lista. Después de introducir los términos de búsqueda, aplique el filtro ( ) o bórrelo ( ) y escriba otros términos distintos.
	  • **File Type (Tipo de archivo)**: enumera los archivos según el tipo. Por ejemplo, la pestaña **Executable (Ejecutable)** muestra los tipos de archivo .exe y .dll; **Non-Executable (No ejecutable)** muestra los tipos de archivo .pdf, .jar, .doc, .ppt, .xls, .docx, .pptx, .xlsx, .rtf, class y .swf; y **Links (Enlaces)** muestra información sobre el tipo de archivo elink.
	  • De cada **File Type (Tipo de archivo)**, en cada pestaña se muestra el total de veredictos de archivos **Malware**, **Greyware** y **Benign (Benigno)**, la cantidad de veredictos con **Error** y el **Total** de veredictos .
	• **Sample Statistics (Estadísticas de muestras)**: ofrece detalles sobre el análisis de muestras de cada tipo de archivo.
	  • **Search box (Cuadro de búsqueda)**: igual que en el cuadro de búsqueda **Verdict (Veredicto)**.

© 2020 Palo Alto Networks, Inc.

Información de Wildfire gestionada	Description (Descripción)
	• **File Type (Tipo de archivo)**: igual que **Verdict (Veredicto) File Type (Tipo de archivo)**. • De cada **File Type (Tipo de archivo)**, en cada pestaña se muestra el total de archivos **Submitted (Enviados)** para su análisis, el total de archivos **Analyzed (Analizados)** y el total de archivos **Pending (Pendientes)**.
Firewalls Connected > View	
Ver	Mediante la opción **View (Ver)** puede acceder a la información sobre los cortafuegos conectados al clúster o al dispositivo. Solo puede ver dispositivos individuales (**Panorama** > **Managed WildFire Appliances [Dispositivos WildFire gestionados]**) o solo estadísticas de clústeres (**Panorama** > **Managed WildFire Clusters [Clústeres Wildfire gestionados]**). • **Appliance (Dispositivo)**: (solo vista de dispositivos independientes) el número de serie del dispositivo. • **Cluster**: (solo en la vista Cluster) el nombre de un clúster, y también puede seleccionar o clúster para verlo. • **Refresh (Actualizar)**: actualiza la pantalla.
Pestañas Registered y Submitting Samples	La pestaña **Registered (Registrados)** muestra información sobre los cortafuegos registrados en el clúster o el dispositivo, independientemente de si los cortafuegos están enviando muestras. La pestaña **Submitting Samples (Enviando muestras)** muestra información sobre los cortafuegos que están enviando muestras activamente al clúster o al dispositivo WildFire. El tipo de información que se muestra en estas pestañas y cómo filtrar la información es similar en ambas: • **Search box (Cuadro de búsqueda)**: introduzca los términos de búsqueda por los que desea filtrar la lista de cortafuegos. El cuadro de búsqueda indica la cantidad de cortafuegos (elementos) de la lista. Después de introducir los términos de búsqueda, aplique el filtro ( ) o bórrelo ( ) y escriba otros términos distintos. • **S/N**: el número de serie del cortafuegos. • **IP address (Dirección IP)**: dirección IP del cortafuegos. • **Model (Modelo)**: el número del modelo del cortafuegos • **Software Version (Versión de software)**: la versión de software instalada y en ejecución en el cortafuegos.

Clúster WildFire gestionado y administración de dispositivos

Seleccione **Panorama** > **Managed WildFire Clusters (Clústeres Wildfire gestionados)** y un clúster para gestionarlo o seleccione un dispositivo WildFire (**Panorama** > **Managed WildFire Appliances [Dispositivos WildFire gestionados]**) para gestionar un dispositivo independiente. La vista **Panorama** > **Managed WildFire Cluster (Clústeres Wildfire gestionados)** enumera los nodos de clústeres (dispositivos WildFire que son miembros del clúster) y los dispositivos independientes de modo que pueda añadir dispositivos disponibles a un clúster. Dado que el clúster gestiona los nodos, la selección de un nodo de clúster solo proporciona una capacidad de gestión limitada.

© 2020 Palo Alto Networks, Inc.

A menos que se indique lo contrario, las configuraciones y las descripciones de la siguiente tabla se aplican tanto a los clústeres como a los dispositivos independientes de WildFire. La información previamente configurada en el clúster o dispositivo se rellena previamente. En primer lugar, debe confirmar los cambios y la información nueva en Panorama, e insertar la configuración nueva en los dispositivos.

setting	Description (Descripción)
Pestaña General	
Nombre	El **Name (Nombre)** del clúster o dispositivo o su número de serie.
Habilitar DNS (Solo clústeres de WildFire)	Use la opción **Enable DNS (Habilitar DNS)** para habilitar el servicio DNS del clúster.
Registrar cortafuegos en	El nombre de dominio en el que registra los cortafuegos. El formato debe ser **`wfpc.service.`**<*cluster-name*>**`.`**<*domain*>. Por ejemplo, el nombre de dominio predeterminado es **`wfpc.service.mycluster.paloaltonetworks.com`**.
Servidor de actualizaciones de contenido	Indique la ubicación del **Content Update Server (Servidor de actualizaciones de contenido)** o utilice el valor predeterminado **`wildfire.paloaltonetworks.com`** de modo que el clúster o el dispositivo reciban actualizaciones de contenido del servidor más cercano de la infraestructura de Content Delivery Network (Red de entrega de contenido). La conexión con la nube global le brinda la ventaja de acceder a las firmas y a las actualizaciones basadas en el análisis de amenazas de todas las fuentes conectadas a la nube en lugar de confiar únicamente en el análisis de las amenazas locales.
Comprobar identidad de servidor	Use la opción **Check Server Identity (Comprobar identidad de servidor)** para confirmar la identidad del servidor de actualizaciones haciendo coincidir el nombre común (CN) del certificado con la dirección IP o FQDN del servidor.
Servidor cloud de WildFire	Indique la ubicación global del **WildFire Cloud Server (Servidor cloud de WildFire)** o utilice el valor predeterminado **`wildfire.paloaltonetworks.com`** para que el clúster o el dispositivo pueda enviar información al servidor más cercano. Puede elegir si desea enviar información y de qué tipo a la nube global (**Servicios en la nube de WildFire [Servicios en la nube de WildFire]**).
Imagen de análisis de muestras	Seleccione la imagen de VM que el clúster o el dispositivo utilizan para el análisis de muestras (la predeterminada es vm-5). Puede Obtener un archivo de prueba de malware (API de WildFire) para conocer el resultado del análisis de la muestra.
Servicios en la nube de WildFire	Si el clúster o el dispositivo están conectados al servidor en la nube global de WildFire, puede elegir si desea **Send Analysis Data (Enviar datos de análisis)**, **Send Malicious Samples (Enviar muestras de malware)** o **Send Diagnostics (Enviar diagnósticos)** a la nube global, o una combinación de las tres opciones. También puede elegir si desea realizar una **Verdict Lookup (Búsqueda de veredictos)** en la nube global. El envío de información a la nube global presenta ventajas para toda la comunidad de usuarios de WildFire, ya

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	que la información compartida aumenta la capacidad de cada dispositivo de identificar tráfico malicioso y evitar que cruce la red.
Sample Data Retention	Cantidad de días que se retienen muestras benignas o de greyware y muestras maliciosas: • Muestras de **Benign/Grayware (Benigno/Grayware)**: el intervalo es de 1 a 90 y el valor predeterminado, 14. • Muestras de **Malicious (Malicioso)**: el mínimo es uno y no existe máximo (indefinido); el valor predeterminado es indefinido.
Servicios de entorno de análisis	**Environment Networking (Redes de entorno)** permite que las máquinas virtuales se comuniquen con Internet. Puede seleccionar la opción **Anonymous Networking (Redes anónimas)** para que la comunicación de red sea anónima, pero para poder habilitarla debe seleccionar **Environment Networking (Redes de entorno)**. Los distintos entornos de red generan diferentes tipos de cargas de análisis en función de si se necesitan analizar más documentos o se deben analizar más archivos ejecutables. Según las necesidades de su entorno de análisis preferido, puede configurarlo para asignar más recursos a **Executables (Ejecutables)** o a **Documents (Documentos)**. La asignación **Default (Predeterminada)** se reparte entre las categorías **Executables (Ejecutables)** y **Documents (Documentos)**. La cantidad de recursos disponibles depende de cuántos nodos WildFire haya en el clúster.
Generación de firma	Seleccione si desea que el clúster o el dispositivo genere firmas para AV, DNS, URL, o una combinación de los tres.
Pestaña Appliance (Dispositivo)	
Nombre de host (Solo dispositivo independiente de WildFire)	Introduzca el nombre de host del dispositivo WildFire.
Servidor de Panorama	Introduzca la dirección IP o el FQDN del dispositivo o del Panorama principal que gestiona el clúster.
Servidor 2 de Panorama	Introduzca la dirección IP o el FQDN del dispositivo o del Panorama de respaldo que gestiona el clúster.
Dominio	Introduzca el nombre de dominio del clúster del dispositivo o del propio dispositivo.
Servidor DNS principal	Introduzca la dirección IP del servidor DNS principal.
Servidor DNS secundario	Introduzca la dirección IP del servidor DNS secundario.
timezone	Seleccione la zona horaria que desea configurar en el clúster o el dispositivo.

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
Latitud (Solo dispositivo independiente de WildFire)	Introduzca la latitud del dispositivo WildFire.
Longitud (Solo dispositivo independiente de WildFire)	Introduzca la longitud del dispositivo WildFire.
Servidor NTP principal	Introduzca la dirección IP del servidor NTP principal y establezca Authentication Type (Tipo de autenticación) en **None (Ninguna)** (predeterminado), **Symmetric Key (Clave simétrica)** o **Autokey (Clave automática)**. Al configurar Authentication Type en **Symmetric Key (Clave simétrica)** se muestran cuatro campos más: • **Key ID (ID de clave)**: introduzca el ID de la clave de autenticación. • **Algorithm (Algoritmo)**: establezca el algoritmo de autenticación en **SHA1** o **MD5**. • **Authentication Key (Clave de autenticación)**: introduzca la clave de autenticación. • **Confirm Authentication Key (Confirmar clave de autenticación)**: vuelva a escribir la clave de autenticación para confirmarla.
Servidor NTP secundario	Introduzca la dirección IP del servidor NTP secundario y establezca Authentication Type (Tipo de autenticación) en **None (Ninguna)** (predeterminado), **Symmetric Key (Clave simétrica)** o **Autokey (Clave automática)**. Al configurar Authentication Type en **Symmetric Key (Clave simétrica)** se muestran cuatro campos más: • **Key ID (ID de clave)**: introduzca el ID de la clave de autenticación. • **Algorithm (Algoritmo)**: establezca el algoritmo de autenticación en **SHA1** o **MD5**. • **Authentication Key (Clave de autenticación)**: introduzca la clave de autenticación. • **Confirm Authentication Key (Confirmar clave de autenticación)**: vuelva a escribir la clave de autenticación para confirmarla.
Banner de inicio de sesión	Escriba un mensaje de banner que se muestra cuando los usuarios inician sesión en el clúster o el dispositivo.
Pestaña Logging (Creación de logs) (incluye las pestañas System [Sistema] y Configuration [Configuración])	
Añadir	Haga clic en **Add (Añadir)** para añadir perfiles de reenvío de logs (**Panorama** > **Managed WildFire Clusters [Clústeres Wildfire gestionados]** > *<cluster>* > **Logging [Creación de logs]** > **System [Sistema]** o **Panorama** > **Managed**

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	WildFire Clusters [Clústeres Wildfire gestionados] > *<cluster>* > **Logging [Creación de logs]** > **Configuration [Configuración]**) para reenviarlos: • Sistema o logs de configuración como trampas SNMP a receptores de trampas SNMP. • Mensajes syslog a servidores syslog. • Notificaciones por correo electrónico a los servidores de correo electrónico. • Solicitudes HTTP a los servidores HTTP. No se admiten otros tipos de logs (consulte Device > Log Settings). Los perfiles de reenvío de logs especifican qué logs se deben reenviar y a qué servidores de destino. En cada perfil, complete lo siguiente: • **Name (Nombre)**: un nombre que identifica la configuración del log (hasta 31 caracteres) que consta de caracteres alfanuméricos y guiones bajos solamente; no se permiten espacios ni caracteres especiales. • **Filter (Filtrar)**: de forma predeterminada, el dispositivo de Panorama reenvía **All Logs (Todos los logs)** del perfil especificado. Para reenviar un subconjunto de logs, seleccione un filtro (**severity eq critical [Gravedad de EQ crítica]**, **severity eq high [Gravedad de EQ elevada]**, **severity eq informational [Gravedad de EQ informativa]**, **severity eq low [Gravedad de EQ baja]** o **severity eq medium [Gravedad de EQ media]**) o seleccione **Filter Builder (Generador de filtros)** para crear un filtro nuevo. • **Description (Descripción)**: escriba una descripción (hasta 1023 caracteres) para explicar el propósito del perfil.
Add > Filter > Filter Builder	Use **Filter Builder (Generador de filtro)** para crear nuevos filtros de logs. Seleccione **Create Filter (Crear filtro)** para crear filtros y, en cada consulta en un nuevo filtro, realice los siguientes ajustes y haga clic en **Add (Añadir)** para añadir la consulta: • **Connector (Conector)**: seleccione el conector lógico (**and [y]** u **or [o]**). Seleccione **Negate (Negar)** si desea aplicar la negación. Por ejemplo, para evitar el reenvío de un subconjunto de descripciones de logs, seleccione **Description (Descripción)** como atributo, seleccione **contains (Contiene)** como operador e introduzca la cadena de descripción como valor para identificar la descripción o las descripciones que no desea reenviar. • **Attribute (Atributo)**: seleccione un atributo de log. Las opciones varían según el tipo de log. • **Operator (Operador)**: seleccione el criterio para determinar cómo se debe aplica el atributo (como **contains [contiene]**). Las opciones varían según el tipo de log. • **Value (Valor)**: Especifique el valor del atributo para coincidir. • **Add (Añadir)**: agrega el nuevo filtro. Para ver o exportar los logs que coinciden con el filtro, seleccione **View Filtered Logs (Ver logs filtrados)**. • Para buscar entradas del logos coincidentes, puede añadir artefactos al campo de búsqueda, como direcciones IP o un intervalo de tiempo. • Seleccione el período de tiempo de logs que desea ver: **Last 15 Minutes (Últimos 15 minutos)**, **Last Hour (Última hora)**, **Last 6 Hrs (Últimas 6 horas)**, **Last 12 Hrs (Últimas 12 horas)**, **Last 24 Hrs (Últimas 24 horas)**,

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)

	Last 7 Days (Últimos 7 días), **Last 30 Days (Últimos 30 días)** o **All (Todos)** (predeterminado).
	• Utilice las opciones a la derecha de la lista desplegable de período de tiempo para aplicar, borrar, añadir, guardar y cargar filtros:
	  • **Apply filters (Aplicar filtros)** ( ): muestra las entradas de log que coinciden con los términos del campo de búsqueda.
	  • **Clear filters (Borrar filtros)** ( ): restablece el campo del filtro.
	  • **Add a new filter (Añadir un filtro nuevo)** ( ): define nuevos criterios de búsqueda (le lleva a Add Log Filter [Añadir filtro de log], similar a la creación de filtros).
	  • **Save a filter (Guardar un filtro)** ( ): asigne un nombre al filtro y haga clic en **OK (Aceptar)**.
	  • **Use a saved filter (Usar un filtro guardado)** ( ): añada un filtro guardado al campo de filtro.
	  • **Export to CSV (Exportar a CSV)** ( ): exporta logs a un informe con formato CSV y a través de **Download file (Descargar archivo)** descarga el informe. De manera predeterminada, el informe contiene hasta 2000 líneas de logs. Para cambiar el límite de línea de los informes CSV generados, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Logging and Reporting Settings (Configuración de log e informes)** > **Log Export and Reporting (Exportación e informes de logs)** e introduzca un nuevo valor en **Max Rows in CSV Export (Máx. de filas en exportación CSV)**.
	Puede cambiar el número y el orden de las entradas mostradas por página y puede utilizar los controles de paginación en la parte inferior izquierda de la página para navegar por la lista de logs. Las entradas de logs se recuperan en bloques de 10 páginas.
	• **per page (por página)**: utilice el menú desplegable para cambiar el número de entradas de log por página (**20**, **30**, **40**, **50**, **75** o **100**).
	• **ASC** o **DESC**: seleccione **ASC** para ordenar los resultados en orden ascendente (primero la entrada de log más antigua) o **DESC** para ordenarlos en orden descendente (primero la entrada de log más reciente). El valor predeterminado es **DESC**.
	• **Resolve Hostname (Resolver nombre de host)**: seleccione esta opción para resolver direcciones IP externas en nombres de dominio.
	• **Highlight Policy Actions (Resaltar acciones de política)**: especifique una acción y selecciónela para resaltar las entradas de log que coincidan con la acción. Los logs filtrados se resaltan en estos colores:
	  • Verde: allow (permitir)
	  • Amarillo: continue (continuar) u override (anular)
	  • Rojo: deny (denegar), drop (descartar), drop-icmp (descartar icmp), rst-client (rst cliente), reset-server (restablecer servidor), reset-both (restablecer ambos), block-continue (bloquear y continuar), block-override (bloquear y anular), block-url (bloquear URL), drop-all (descartar todo), sinkhole

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
delete	Seleccione el ajuste de reenvío de logs que desea eliminar y haga clic en **Delete (Eliminar)** para eliminarlo de la lista de logs de sistema o de configuración.
Pestaña Autenticación	
Remote Authentication (Autenticación remota)	Seleccione **Authentication Profile (Perfil de autenticación)** para acceder. El valor predeterminado es **None (Ninguno)**. Si no hay perfiles de autenticación que elegir, puede configurar una secuencia y un perfil de autenticación.

Autenticación local	Configure la autenticación local del administrador:
	• **Administrator (Administrador)**: es siempre **admin** porque solo hay un usuario de nivel administrativo en cada dispositivo de Panorama.
	• **Mode (Modo)**: establezca el modo de autenticación local en **Password (Contraseña)** o **Password Hash (Contraseña con hash)**:
	  • **Password (Contraseña)**: introduzca y confirme la nueva contraseña.
	  • **Password Hash (Contraseña con hash)**: introduzca una cadena de contraseña con hash. Por ejemplo, una contraseña con hash es útil si desea reutilizar las credenciales de una cuenta Unix existente, pero no conoce la contraseña de texto sin formato y sin embargo sí recuerda la contraseña con hash. El dispositivo acepta cualquier cadena de hasta 63 caracteres, independientemente del algoritmo empleado para generar el valor de hash. Los parámetros de complejidad mínima de contraseña que establezca en el cortafuegos (**Panorama** > **Setup [Configuración]** > **Management [Gestión]**) no se aplican a las cuentas que utilizan contraseña con hash.

Configuración de tiempo de espera	Configurar los tiempos de espera de autenticación de clústeres: • **Idle Timeout (min) (Tiempo de inactividad [min])**: establezca el tiempo de inactividad en minutos. Cuando un usuario permanece inactivo durante más tiempo de espera que el de inactividad especificado, el sistema finaliza la sesión del usuario. El valor predeterminado es **None (Ninguno)** (sin tiempo de espera). • **Failed Attempts (Intentos fallidos)**: establezca el número de intentos fallidos de inicio de sesión para que el sistema impida a un usuario entrar en el sistema. El valor predeterminado es de 10 intentos fallidos. • **Lockout Time (min) (Tiempo de bloqueo [min.])**: establezca los minutos que un usuario bloqueado debe esperar para poder iniciar sesión. El valor predeterminado es de 5 minutos.
Pestaña Clustering (Agrupación en clústeres) (solo clústeres de WildFire gestionados) y pestaña Interfaces (Interfaces) (solo dispositivos de WildFire gestionados) Debe añadir dispositivos a Panorama para gestionar interfaces y añadir dispositivos a clústeres para gestionar interfaces de nodos.	
Dispositivo (Solo pestaña Clustering [Agrupación en clústeres])	Seleccione un nodo de clúster para acceder a las pestañas Appliance e Interfaces de ese nodo. La información del nodo de la pestaña Appliance (Dispositivo) se rellena previamente y no se puede configurar excepto por el nombre de host. La pestaña Interfaces enumera las interfaces de nodo.

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	Seleccione una interfaz para gestionarla como se describe en las siguientes secciones: • Interface Name Management • Interface Name Analysis Environment Network • Interface Name Ethernet2 • Interface Name Ethernet3

Interface Name Management	La interfaz de gestión es Ethernet0. Configure o consulte la configuración de la interfaz de gestión:
	• **Speed and Duplex (Velocidad y dúplex)**: seleccione entre **auto-negotiate (negociación automática)** (predeterminado), **10Mbps-half-duplex (dúplex medio de 10 Mbps)**, **10Mbps-full-duplex (dúplex completo de 10 Mbps)**, **100Mbps-half-duplex (dúplex medio de 100 Mbps)**, **100Mbps-full-duplex (dúplex completo de 100 Mbps)**, **1Gbps-half-duplex (dúplex medio de 1 Gbps)** o **1Gbps-full-duplex (dúplex completo de 1 Gbps)**.
	• **IP Address (Dirección IP)**: introduzca la dirección IP del servidor.
	• **Netmask (Máscara de red)**: introduzca la máscara de red de la interfaz.
	• **Default Gateway (Puerta de enlace predeterminada)**: introduzca la dirección IP de la puerta de enlace predeterminada.
	• **MTU**: introduzca la MTU en bytes (el intervalo es de 576 a 1500; el valor predeterminado es 1500).
	• **Management Services (Servicios de administración)**: habilite los servicios de administración que desea admitir. Puede admitir servicios **Ping**, **SSH** y **SNMP**.
	Si utiliza un servidor proxy, configúrelo para conectarse a Internet:
	• **Server (Servidor)**: dirección IP del servidor proxy.
	• **Port (Puerto)**: número de puerto configurado en el servidor proxy para escuchar las solicitudes de dispositivos de Panorama.
	• **User (Usuario)**: nombre de usuario de autenticación configurado en el servidor proxy.
	• **Password (Contraseña)** y **Confirm Password (Confirmar contraseña)**: contraseña de autenticación configurada en el servidor proxy.
	• **Clustering Services (Servicios de clúster)** (solo en la pestaña Clustering): seleccione el servicio de HA:
	  • **HA (Alta disponibilidad)**: si hay dos nodos del controlador en el clúster, puede configurar la interfaz de gestión como una interfaz de HA para que la información de gestión esté disponible en ambos nodos del controlador. Si el nodo del clúster que está configurando es el nodo controlador principal, márquelo como interfaz **HA**.
	  En función de cómo utilice las interfaces Ethernet del dispositivo WildFire, también podrá, de manera alternativa, configurar Ethernet2 o Ethernet3 como interfaces de HA y de HA de respaldo en los nodos controladores principal y de respaldo, respectivamente. Por ejemplo, puede utilizar Ethernet2 como interfaz de HA y HA Backup. Las interfaces HA y HA Backup deben tener la misma interfaz (gestión, Ethernet2 o Ethernet3) en los nodos controladores principal y de respaldo. No puede utilizar Ethernet1 como interfaz de copia HA o HA Backup.

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	• **HA Backup**: si el nodo del clúster que está configurando es el nodo controlador de respaldo, márquelo como interfaz **HA Backup**. Especifique las direcciones IP permitidas en la interfaz: • **Search box (Cuadro de búsqueda)**: introduzca los términos de búsqueda para filtrar la lista de direcciones IP permitidas. El cuadro de búsqueda indica el número de direcciones IP (elementos) de la lista para conocer la longitud de la lista. Después de introducir los términos de búsqueda, aplique el filtro ( ) o bórrelo ( ) y escriba otros términos distintos. • **Add (Añadir)**: haga clic en **Add (Añadir)** para añadir una dirección IP permitida. • **Delete (Eliminar)**: seleccione las direcciones IP que desea eliminar del acceso a la interfaz de administración y haga clic en esta opción.
Interface Name Analysis Environment Network	Configure la interfaz de red de entorno para el análisis del clúster de dispositivos WildFire o de un dispositivo WildFire independiente (Ethernet1, también conocida como interfaz de VM): • **Speed and Duplex (Velocidad y dúplex)**: establezca esta opción en **auto-negotiate (negociación automática)** (predeterminado), **10Mbps-half-duplex (dúplex medio de 10 Mbps)**, **10Mbps-full-duplex (dúplex completo de 10 Mbps)**, **100Mbps-half-duplex (dúplex medio de 100 Mbps)**, **100Mbps-full-duplex (dúplex completo de 100 Mbps)**, **1Gbps-half-duplex (dúplex medio de 1 Gbps)** o **1Gbps-full-duplex (dúplex completo de 1 Gbps)**. • **IP Address (Dirección IP)**: introduzca la dirección IP del servidor. • **Netmask (Máscara de red)**: introduzca la máscara de red de la interfaz. • **Default Gateway (Puerta de enlace predeterminada)**: introduzca la dirección IP de la puerta de enlace predeterminada. • **MTU**: introduzca la MTU en bytes (el intervalo es de 576 a 1500; el valor predeterminado es 1500). • **DNS Server (Servidor DNS)**: introduzca la dirección IP del servidor DNS. • **Link State (Estado de enlace)**: establezca el estado del enlace en **Up (Activo)** o **Down (Inactivo)**. • Management Services (Servicios de gestión): habilite **Ping** si desea que la interfaz admita este tipo de servicio. Especifique las direcciones IP permitidas en la interfaz: • **Search box (Cuadro de búsqueda)**: introduzca los términos de búsqueda para filtrar la lista de direcciones IP permitidas. El cuadro de búsqueda indica el número de direcciones IP (elementos) de la lista para conocer la longitud de la lista. Después de introducir los términos de búsqueda, aplique el filtro ( ) o bórrelo ( ) y escriba otros términos distintos. • **Add (Añadir)**: haga clic en **Add (Añadir)** para añadir una dirección IP permitida. • **Delete (Eliminar)**: seleccione las direcciones IP que desea eliminar del acceso a la interfaz de administración y haga clic en esta opción.
Interface Name Ethernet2	Puede configurar los mismos parámetros para las interfaces Ethernet2 y Ethernet3:

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)

Interface Name Ethernet3	• **Speed and Duplex (Velocidad y dúplex)**: establezca esta opción en **auto-negotiate (negociación automática)** (predeterminado), **10Mbps-half-duplex (dúplex medio de 10 Mbps)**, **10Mbps-full-duplex (dúplex completo de 10 Mbps)**, **100Mbps-half-duplex (dúplex medio de 100 Mbps)**, **100Mbps-full-duplex (dúplex completo de 100 Mbps)**, **1Gbps-half-duplex (dúplex medio de 1 Gbps)** o **1Gbps-full-duplex (dúplex completo de 1 Gbps)**.
	• **IP Address (Dirección IP)**: introduzca la dirección IP del servidor.
	• **Netmask (Máscara de red)**: introduzca la máscara de red de la interfaz.
	• **Default Gateway (Puerta de enlace predeterminada)**: introduzca la dirección IP de la puerta de enlace predeterminada.
	• **MTU**: introduzca la MTU en bytes (el intervalo es de 576 a 1500; el valor predeterminado es 1500).
	• Management Services (Servicios de gestión): habilite **Ping** si desea que la interfaz admita este tipo de servicio.
	• **Clustering Services (Servicios de clúster)**: seleccione los servicios de clúster:
	  • **HA (Alta disponibilidad)**: si hay dos nodos del controlador en el clúster, puede configurar las interfaces Ethernet2 o Ethernet3 como interfaces de HA para que la información de gestión esté disponible en ambos nodos del controlador. Si el nodo del clúster que está configurando es el nodo controlador principal, márquelo como interfaz **HA**.
	  En función de cómo utilice las interfaces Ethernet del dispositivo WildFire, también puede configurar la interfaz de gestión (Ethernet1) como interfaces HA y HA Backup en los nodos controladores principal y de respaldo, respectivamente. Las interfaces HA y HA Backup deben tener la misma interfaz (gestión, Ethernet2 o Ethernet3) en los nodos controladores principal y de respaldo. No puede utilizar Ethernet1 como interfaz de copia HA o HA Backup.
	  • **HA Backup**: si el nodo del clúster que está configurando es el nodo controlador de respaldo, márquelo como interfaz **HA Backup**.
	  • **Cluster Management (Gestión de clústeres)**: configure las interfaces Ethernet2 o Ethernet3 para la gestión y la comunicación de todo el clúster.

Función (Solo pestaña Clustering [Agrupación en clústeres])	Cuando un clúster tiene dispositivos miembros, las funciones del dispositivo pueden ser Controller (Controlador), Controller Backup (Backup de controlador), o Worker (Trabajador). Seleccione **Controller** o **Backup Controller** para cambiar el dispositivo WildFire utilizado en cada función de los dispositivos del clúster. Al cambiar los resultados del controlador, se produce una pérdida de datos durante el cambio de función.
Examinar (Solo pestaña Clustering [Agrupación en clústeres])	La pestaña **Clustering (Agrupación en clústeres)** muestra los nodos del dispositivo WildFire en el clúster. Use **Browse (Examinar)** para ver y agregar dispositivos WildFire independientes que ya gestiona el dispositivo de Panorama: • **Search box (Cuadro de búsqueda)**: introduzca los términos de búsqueda que desea filtrar de la lista de nodos. El cuadro de búsqueda indica el número de dispositivos (elementos) de la lista para conocer la longitud de

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	la lista. Después de introducir los términos de búsqueda, aplique el filtro ( ) o bórrelo ( ) y escriba otros términos distintos. • **Add Nodes (Añadir nodos)**: añada ( ) nodos al clúster. El primer dispositivo WildFire que agregue a un clúster se convierte automáticamente en el nodo Controller. El segundo dispositivo WildFire que agregue a un clúster se convierte automáticamente en el nodo Controller Backup. Puede agregar hasta 20 dispositivos WildFire a un clúster. Después de agregar los nodos Controller y Controller Backup, todos los nodos agregados posteriormente serán nodos Worker.
delete (Solo pestaña Clustering [Agrupación en clústeres])	Seleccione uno o más dispositivos de la lista y haga clic en **Delete (Eliminar)** para eliminarlos del clúster. Puede eliminar un nodo Controller solo si hay dos nodos Controller en el clúster.
Gestionar controlador (Solo pestaña Clustering [Agrupación en clústeres])	Seleccione **Manage Controller (Gestionar controlador)** para especificar un **Controller (Controlador)** y un **Controller Backup (Backup de controlador)** de entre los nodos del dispositivo WildFire que pertenecen al clúster. Los nodos Controller y Controller Backup actuales se seleccionan de forma predeterminada. El nodo Controller Backup no puede ser el mismo que el nodo Controller principal.
Pestaña Communication (Comunicación)	

Customize Secure Server Communication (Personalizar comunicación del servidor segura)	• **SSL/TLS Service Profile (Perfil del servicio SSL / TLS)**: seleccione un perfil de servicio SSL / TLS del menú desplegable. Este perfil define el certificado y las versiones SSL / TLS admitidas que utilizan los dispositivos conectados para comunicarse con WildFire.
	• **Certificate Profile (Perfil de certificado)**: seleccione el perfil de certificado del menú desplegable. Este perfil de certificado define la conducta de la comprobación de revocación de certificados y la CA raíz utilizada para autenticar la cadena de certificados presentada por el cliente.
	• **Custom Certificate Only (Certificado personalizado únicamente)**: cuando esta opción está habilitada, WildFire sólo acepta certificados personalizados para la autenticación de dispositivos conectados.
	• **Check Authorization List (Comprobar lista de autorización)**: los dispositivos de cliente que se conectan a WildFire se comprueban con la lista de autorizaciones. Un dispositivo debe coincidir solo con un elemento de la lista para ser autorizado. Si no se encuentra ninguna coincidencia, el dispositivo no está autorizado.
	• **Authorization List (Lista de autorización)**: seleccione **Add (Añadir)** para añadir una lista de autorización y complete los siguientes campos para establecer criterios de autorización para dispositivos cliente. La Authorization List (Lista de autorización) admite un máximo de 16 entradas.
	  • **Identifier (Identificador)**: seleccione **Subject (Asunto)** o **Subject Alt. (Asunto Alt.) Name (Nombre)** como el identificador de autorización.
	  • **Type (Tipo)**: si seleccionó **Subject Alt. (Asunto Alt.) Name (Nombre)** como el Identificador, luego seleccione **IP**, **hostname (nombre de**

© 2020 Palo Alto Networks, Inc.

setting	Description (Descripción)
	host) o **e-mail (correo electrónico)** como el tipo del identificador. Si ha seleccionado **Subject (Asunto)**, entonces common-name (nombre común) es el tipo de identificador. • **Value (Valor)**: introduzca el valor del identificador.

Comunicación de cliente segura	Si utiliza **Secure Client Communication (Comunicación segura del cliente)**, garantizará que WildFire utilice certificados personalizados configurados (en lugar de certificados predefinidos predeterminados) para autenticar las conexiones SSL con otro dispositivo WildFire.
	• **Predefined (Predefinido)** (predeterminado): no se configuran certificados de dispositivos; WildFire utiliza el certificado predefinido predeterminado.
	• **Local**: WildFire utiliza un certificado de dispositivo local y la clave privada correspondiente generada en el cortafuegos o importada de un servidor PKI empresarial existente.
	  • **Certificate (Certificado)**: Seleccione el certificado del dispositivo local.
	  • **Certificate Profile (Perfil del certificado)**: Seleccione el perfil de certificado en la lista desplegable.
	• **SCEP**: WildFire utiliza un certificado de dispositivo y una clave privada generada por un servidor de protocolo de inscripción de certificados simple (Simple Certificate Enrollment Protocol, SCEP).
	  • **SCEP Profile (Perfil SCEP)**: Seleccione un perfil SCEP del menú desplegable.
	  • **Certificate Profile (Perfil del certificado)**: Seleccione el perfil de certificado en la lista desplegable.

Secure Cluster Communication (Comunicación segura del clúster)	Seleccione **Enable (Habilitar)** para cifrar las comunicaciones entre dispositivos de WildFire. El certificado predeterminado utiliza el tipo de certificado predefinido. Para utilizar un certificado personalizado definido por el usuario, debe realizar la configuración **Customize Secure Server Communication (Personalizar comunicación del servidor segura)** y habilitar la opción **Custom Certificate Only (Certificado personalizado únicamente)**.

© 2020 Palo Alto Networks, Inc.

Panorama > Administradores

Seleccione **Panorama** > **Administrators (Administradores)** para crear y gestionar cuentas para los administradores de Panorama.

Si inicia sesión en Panorama como administrador con una función de superusuario, puede desbloquear las cuentas de otros administradores haciendo clic en los iconos de candado de la columna Locked User (Usuario bloqueado). Los administradores bloqueados no tienen acceso a Panorama. Panorama bloquea a los administradores que exceden el número permitido de intentos sucesivos fallidos de acceder a Panorama según se define en la opción **Authentication Profile (Perfil de autenticación)** asignada a sus cuentas (consulte Device > Authentication Profile).

Para crear una cuenta de administrador, haga clic en **Add (Añadir)** y configure los ajustes como se describe en la siguiente tabla.

Configuración de cuentas de administrador	Description (Descripción)
Nombre	Introduzca un nombre de usuario de inicio de sesión para el administrador (hasta 15 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, guiones y guiones bajos.
Perfil de autenticación	Seleccione una secuencia o perfil de autenticación para autenticar este administrador. Para obtener más información, consulte Device > Authentication Profile o Device > Authentication Sequence.
Use only client certificate authentication (Web)	Seleccione esta opción para utilizar la autenticación con certificado de cliente para el acceso a la interfaz web. Si selecciona esta opción, no se requiere nombre de usuario (**Name**) ni contraseña (**Password**).
Contraseña/Confirmar contraseña	Introduzca y confirme una contraseña que haga distinción entre mayúsculas y minúsculas para el administrador (de hasta 15 caracteres). Por motivos de seguridad, Palo Alto Networks recomienda que los administradores cambien periódicamente las contraseñas administrativas. Estas contraseñas deben utilizar una combinación de minúsculas, mayúsculas y números. Asegúrese de seguir las prácticas recomendadas sobre seguridad de la contraseña para garantizar que la contraseña sea segura. Los administradores de grupos de dispositivos y plantillas no pueden acceder a la página **Panorama** > **Administrators (Administradores)**. Para cambiar su contraseña local, estos administradores deben hacer clic en su nombre de usuario junto al enlace **Logout (Cierre de sesión)** en la parte inferior de la interfaz web. Esto también se aplica a los administradores con una función personalizada de Panorama en la que está deshabilitado el acceso a **Panorama** > **Administrators (Administradores)**. Puede utilizar la autenticación de contraseña junto con un **Authentication Profile (Perfil de autenticación)** (o secuencia) o con la autenticación de base de datos local. Puede configurar los parámetros de caducidad de la contraseña mediante la selección de una opción en **Password Profile (Perfil de**

© 2020 Palo Alto Networks, Inc.

Configuración de cuentas de administrador	Description (Descripción)
	la contraseña) (consulte Device > Password Profiles) y establecer los parámetros de complejidad mínima (consulte Device > Setup > Management), pero únicamente para las cuentas administrativas autenticadas localmente por Panorama.
Utilizar autenticación de clave pública (SSH)	Seleccione esta opción para usar la autenticación de clave pública SSH: haga clic en **Import Key (Importar clave)** y en **Browse (Examinar)** para seleccionar el archivo de clave pública y, a continuación, en **OK (Aceptar)**. El cuadro de diálogo Administrador muestra la clave actualizada en el área de texto de solo lectura. Los formatos de archivo de clave admitidos son IETF SECSH y OpenSSH. Los algoritmos de clave admitidos son DSA (1.024 bits) y RSA (de 768 a 4.096 bits). *Si falla la autenticación de clave pública, Panorama muestra un mensaje de nombre de usuario y contraseña.*
Tipo de administrador	El tipo de selección determina las opciones de las funciones administrativas: • **Dynamic (Dinámico)**: estas funciones proporcionan acceso a Panorama y a los cortafuegos gestionados. Al añadir nuevas funciones, Panorama actualiza automáticamente las definiciones de funciones dinámicas; no necesitará actualizarlas manualmente en ningún momento. • **Custom Panorama Admin (Administrador de Panorama personalizado)**: funciones configurables con acceso de lectura y escritura, acceso de solo lectura o sin acceso a funciones de Panorama. • **Device Group and Template Admin (Administrador de grupo de dispositivo y plantillas)**: funciones configurables con acceso de lectura y escritura, acceso de solo lectura o sin acceso a las funciones de los grupos de dispositivos y plantillas asignados a los dominios de acceso seleccionados para este administrador.

función de administración
 	
(tipo de administrador dinámico)
	Seleccione una función predefinida:
	
	• **Superuser (Superusuario)**: acceso de lectura y escritura completo a Panorama y a todos los grupos de dispositivos, plantillas y cortafuegos gestionados.
	• **Superuser (Read Only) [Superusuario (solo lectura)]**: acceso de solo lectura a Panorama y a todos los grupos de dispositivos, plantillas y cortafuegos gestionados.
	• **Panorama administrator (Administrador de Panorama)**: acceso completo a Panorama a excepción de las siguientes acciones:
	  • Crear, modificar o eliminar los administradores y funciones de Panorama o el cortafuegos.
	  • Exportar, validar, revertir, guardar, cargar o importar una configuración (**Dispositivo** > **Configuración** > **Operaciones**).

© 2020 Palo Alto Networks, Inc.

Configuración de cuentas de administrador	Description (Descripción)
	• Configure **Scheduled Config Export (Exportación de configuración programada)** en la pestaña **Panorama**.
Perfil (Tipo de administrador Administrador de Panorama personalizado)	Seleccione una función personalizada de Panorama (consulte Panorama > Managed Devices [Dispositivos gestionados] > Summary [Resumen]).
Dominio de acceso a rol de administrador (Tipo de administrador Administrador de grupo de dispositivos y plantillas)	Para cada dominio de acceso (hasta 25) que desee asignar al administrador, haga clic en **Add (Añadir)** y seleccione un **Access Domain (Dominio de acceso)** del menú desplegable (consulte Panorama > Access Domains [Dominios de acceso]). A continuación, haga clic en la celda adyacente Admin Role (Función de gestión) y seleccione una función personalizada de administrador de grupo de dispositivos y plantilla en el menú desplegable (consulte Panorama > Managed Devices [Dispositivos gestionados] > Summary [Resumen]). Cuando los administradores con acceso a más de un dominio inician sesión en Panorama, aparece un menú desplegable **Access Domain (Dominio de acceso)** en el pie de página de la interfaz web. Los administradores pueden seleccionar cualquier **Access Domain (Dominio de acceso)** asignado para filtrar los datos de monitorización y configuración que muestra Panorama. La selección de **Access Domain (Dominio de acceso)** también filtra los cortafuegos que muestra el menú desplegable **Context (Contexto)**. *Si utiliza un servidor RADIUS para autenticar administradores, debe asignar las funciones de administrador y dominios de acceso a VSA de RADIUS. Debido a que las cadenas VSA admiten un número limitado de caracteres, si configura para un administrador el número máximo (25) de pares de dominio de acceso/función, los valores de Nombre de cada dominio de acceso y función no deben superar los 9 caracteres de media.*
perfil de contraseña	Seleccione un **Password Profile (Perfil de la contraseña)** (consulte Device > Password Profiles).

© 2020 Palo Alto Networks, Inc.

Panorama > Funciones de administrador

Los perfiles de función de administración son funciones personalizadas que definen los privilegios de acceso y las responsabilidades de los administradores. Por ejemplo, las funciones asignadas a un administrador establecen los informes que puede generar y los grupos de dispositivos o las configuraciones de plantilla que el administrador puede ver o cambiar.

En el caso de un administrador de grupo de dispositivos y plantilla, puede asignar una función independiente a cada dominio de acceso asignado a la cuenta administrativa (consulte Panorama > Access Domains). La asignación de funciones a dominios de acceso le permite obtener un control muy detallado sobre la información a la que pueden acceder los administradores en Panorama. Por ejemplo, imagine una situación en la que configura un dominio de acceso que incluye todos los grupos de dispositivos de los cortafuegos en sus centros de datos y que asigna ese dominio de acceso a un administrador que tenga permiso para supervisar el tráfico del centro de datos pero que no pueda configurar los cortafuegos. En este caso, asignaría el dominio de acceso a una función que proporcione todos los privilegios de supervisión, pero que no dé acceso a la configuración del grupo de dispositivos.

Para crear un perfil de función de administración, haga clic en **Add (Añadir)** para agregar un perfil y configure los ajustes como se describe en la siguiente tabla.

Si usa un servidor RADIUS para autenticar administradores, asigne las funciones de administrador y dominios de acceso a Atributos específicos de proveedor (Vendor Specific Attributes, VSA) RADIUS.

Configuración de funciones de administrador de Panorama	Description (Descripción)
Nombre	Introduzca un nombre para identificar esta función de administrador (hasta 31 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	(Opcional) Introduzca una descripción de la función.
Función	Seleccione el ámbito de responsabilidad administrativa: **Panorama** o **Device Group and Template (Grupo de dispositivos y plantilla)**.
Interfaz web	Seleccione entre las siguientes opciones para configurar el tipo de acceso permitido para las funciones específicas en el contexto de Panorama (**Web UI list [Lista de IU web]**) y en el contexto del cortafuegos (**Context Switch UI list [Lista de IU del conmutador de contexto]**): • **Enable (Habilitar)** ( ): acceso de lectura y escritura • **Read Only (Solo lectura)** ( ): acceso de solo lectura • **Disable (Deshabilitar)** ( ): sin acceso
API REST/XML (Función exclusiva de Panorama)	Seleccione el tipo de acceso de XML/REST API (**Enable [Habilitar]**, **Read Only [Solo lectura]** o **Disable [Deshabilitar]**) para Panorama y los cortafuegos gestionados: • **Report (Informes)**: acceso a los informes de cortafuegos y Panorama. • **Log**: acceso a los logs de cortafuegos y Panorama.

© 2020 Palo Alto Networks, Inc.

Configuración de funciones de administrador de Panorama	Description (Descripción)
	• **Configuration (Configuración)**: concede permisos para recuperar o modificar configuraciones del cortafuegos y Panorama. • **Operational Requests (Solicitudes de operación)**: concede permisos para ejecutar comandos de operaciones en Panorama y cortafuegos. • **Commit (Compilar)**: concede permisos para compilar configuraciones de Panorama y cortafuegos. • **User-ID Agent (Agente de User-ID)**: acceso al agente de User-ID. • **Export (Exportar)**: concede permisos para exportar archivos de Panorama y cortafuegos (como configuraciones, páginas de respuesta o bloque, certificados y claves). • **Import (Importar)**: concede permisos para importar a Panorama y cortafuegos (como actualizaciones de software, actualizaciones de contenido, licencias, configuraciones, certificados, páginas de bloque y logs personalizados).

Línea de comandos
 	
(Función exclusiva de Panorama)
	Seleccione el tipo de función para el acceso al CLI:
	• **None (Ninguno)**: (predeterminado) no se permite el acceso al CLI de Panorama.
	• **superuser (superusuario)**: acceso completo a **Panorama**.
	• **superreader (superlector)**: acceso de solo lectura a **Panorama**.
	• **panorama-admin (administrador de Panorama):** acceso completo a **Panorama** excepto para las siguientes acciones:
	  • Crear, modificar o eliminar los administradores y funciones de Panorama.
	  • Exportar, validar, revertir, guardar, cargar o importar una configuración.
	  • Exportaciones de configuración programadas

© 2020 Palo Alto Networks, Inc.

Panorama > Access Domains

Los dominios de acceso controlan el acceso que tienen los administradores de grupo de dispositivos y plantillas a grupos específicos de dispositivos (para gestionar políticas y objetos), plantillas (para gestionar la configuración de red y del dispositivo) e interfaz web de cortafuegos gestionados (mediante el cambio de contexto). Puede definir hasta 4000 dominios de acceso y gestionarlos localmente o usar Atributos específicos de proveedor de RADIUS (VSA), TACACS+ VSA o atributos SAML. Para crear un dominio de acceso, haga clic en **Add (Añadir)** y configure los ajustes como se describe en la siguiente tabla.

Configuración de dominio de acceso	Description (Descripción)
Nombre	Introduzca un nombre para el dominio de acceso (hasta 31 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, guiones y guiones bajos.
Objetos compartidos	Seleccione uno de los siguientes privilegios de acceso para los objetos que los grupos de dispositivos en este dominio de acceso heredan de la ubicación compartida. Independientemente de los privilegios, los administradores no pueden cancelar los objetos compartidos o predeterminados (predefinidos). • **read (lectura)**: los administradores pueden mostrar y duplicar objetos compartidos pero no pueden realizar otras operaciones con ellos. Al añadir objetos no compartidos o duplicar objetos compartidos, el destino debe ser un grupo de dispositivos dentro del dominio de acceso, no Compartido. • **write (escritura)**: los administradores pueden realizar todas las operaciones con objetos compartidos. Es el valor predeterminado. • **shared-only (solo compartidos)**: los administradores pueden añadir objetos solo a Compartido. Los administradores también pueden mostrar, editar y eliminar objetos compartidos pero no pueden moverlos o duplicarlos. Si elige esta opción, los administradores no podrán realizar operaciones con objetos no compartidos excepto mostrarlos.
Grupos de dispositivos	Habilite o deshabilite el acceso de lectura y escritura para grupos específicos de dispositivos en el dominio de acceso. También puede hacer clic en **Enable All (Habilitar todo)** o **Disable All (Deshabilitar todo)**. Al habilitar el acceso de lectura y escritura para un grupo de dispositivos, se habilita automáticamente el mismo acceso para sus sucesores. Si deshabilita manualmente un sucesor, el acceso a su antecesor máximo cambia automáticamente a solo lectura. El acceso está deshabilitado para todos los grupos de dispositivos de manera predeterminada. Si quiere que la lista de dispositivos muestre solo grupos de dispositivos específicos, seleccione los nombres de grupos de dispositivos y haga clic en **Filter Selected (Filtrar seleccionados)**. *Si define el acceso para objetos compartidos como shared-only (solo compartidos), Panorama aplica acceso de solo lectura a cualquier grupo de*

© 2020 Palo Alto Networks, Inc.

Configuración de dominio de acceso	Description (Descripción)
	dispositivos para el que especifique acceso de lectura y escritura.
Plantillas	Para cada plantilla o pila de plantillas que quiera asignar, haga clic en **Add (Añadir)** y selecciónela del menú desplegable.
Contexto de dispositivo (Corresponde a la columna Device/Virtual Systems en la página Access Domain)	Seleccione los cortafuegos en los que el administrador puede cambiar el contexto para llevar a cabo la configuración local. Si la lista es larga, puede filtrar por **Device State (Estado de dispositivo)**, **Platforms (Plataformas)**, **Device Groups (Grupos de dispositivos)**, **Plantillas**, **Tags (Etiquetas)** y **HA Status (Estado de HA)**.
Grupos de recopiladores de logs	Para cada grupo de recopiladores que desee asignar, haga clic en **Add (Añadir)** y selecciónelo en la lista desplegable.

© 2020 Palo Alto Networks, Inc.

Panorama > Managed Devices > Summary (Panorama > Dispositivos gestionados > Resumen)

Un cortafuegos de Palo Alto Networks gestionado por Panorama se denomina *dispositivo gestionado*. Panorama puede gestionar cortafuegos que se ejecutan con la misma versión principal o en versiones principales anteriores, pero no gestiona cortafuegos con una versión principal posterior. Por ejemplo, Panorama con PAN-OS 9.1 puede gestionar cortafuegos con PAN-OS 9.1 y versiones anteriores. Además, no se recomienda gestionar cortafuegos con una versión de mantenimiento posterior que Panorama, ya que puede provocar que algunas funciones no se comporten según lo esperado. Por ejemplo, no se recomienda gestionar cortafuegos con PAN-OS 9.1.1 o versiones de mantenimiento posteriores si Panorama funciona con PAN-OS 9.1.0. Para obtener más información sobre la información de la versión, consulte las Notas de la versión de PAN-OS 9.1. Para obtener más información sobre versiones de PAN-OS compatibles, consulte el Resumen de fin de vida útil.

- Administración de cortafuegos gestionado
- Información del cortafuegos gestionado
- Software de cortafuegos y actualizaciones de contenido
- Copias de seguridad de cortafuegos

Administración de cortafuegos gestionado

Puede realizar las siguientes tareas administrativas en los cortafuegos.

Tarea	Description (Descripción)
Añadir	Haga clic en **Add (Añadir)** para añadir los cortafuegos e introduzca los números de serie (uno por cada fila) para añadirlos como dispositivos gestionados. En la ventana **Managed Devices (Dispositivos gestionados)** se mostrará entonces la información del cortafuegos gestionado, incluido el estado de conexión, las actualizaciones instaladas y las propiedades que se establecieron durante la configuración inicial. Marque la casilla **Associate Devices (Asociar dispositivos)** para asociar los cortafuegos con un grupo de dispositivos o una pila de plantillas. Seleccione **Import (Importar)** para importar varios cortafuegos con formato CSV para que sean gestionados por el servidor de gestión de Panorama. Un archivo CSV se encuentra disponible para la descarga. A continuación, escriba la dirección IP del servidor de gestión Panorama en cada cortafuegos (consulte Device > Setup > Management) para que Panorama pueda gestionarlos. *El cortafuegos se registra con Panorama en una conexión SSL con cifrado AES-256. Panorama y el cortafuegos se autentican entre sí utilizando certificados de 2048 bits y usan la conexión SSL para la gestión de configuración y la recopilación de logs.*

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Reassosciate (Volver a asociar)	Reasigne uno o varios cortafuegos seleccionados a un grupo de dispositivos o pila de plantillas diferente.
delete	Seleccione uno o varios cortafuegos y haga clic en **Delete (Eliminar)** para eliminarlos de la lista de cortafuegos que gestiona Panorama.
Tag (Etiqueta)	Seleccione uno o más cortafuegos, haga clic en **Tag (Etiqueta)** e introduzca una cadena de texto de hasta 31 caracteres o seleccione una etiqueta existente. No utilice espacios en blanco. Dondequiera que la interfaz web muestre una lista extensa de cortafuegos (por ejemplo, en el cuadro de diálogo de instalación de software), las etiquetas permiten filtrar la lista. Por ejemplo, puede usar una etiqueta denominada sucursal para filtrar todos los cortafuegos de la sucursal de su red.
Instalación	**Instale** actualizaciones de contenido y software del cortafuegos.
Agrupar Peers HA	Seleccione **Group HA Peers (Agrupar Peers HA)** si desea que la página **Managed Devices (Dispositivos gestionados)** agrupe los cortafuegos que son peers en una configuración de alta disponibilidad (HA). Puede seleccionar solo llevar a cabo las acciones en ambos peers o en ningún peer en cada par de HA.
Gestión (copias de seguridad)	**Gestione** copias de seguridad del cortafuegos.
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de cortafuegos gestionados como **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla para elementos como las auditorías. Únicamente las columnas visibles en la interfaz web se exportarán. Consulte Exportación de la tabla de configuración.
Implementar clave maestra	Implemente una nueva clave maestra o actualice una clave maestra existente en uno o varios dispositivos.

Información del cortafuegos gestionado

Seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** para mostrar la siguiente información de cada cortafuegos gestionado.

Información del cortafuegos gestionado	Description (Descripción)
Grupo de dispositivos	Muestra el nombre del grupo de dispositivos del que es miembro el cortafuegos. De forma predeterminada, esta columna está oculta, aunque puede verla seleccionando el menú desplegable de cualquier encabezado de la columna y seleccionando **Columns (Columnas)** > **Device Group (Grupo de dispositivos)**. La página muestra los cortafuegos en clústeres según su grupo de dispositivos. Cada grupo tiene una fila de encabezado que muestra el nombre del grupo de dispositivos, el número total de cortafuegos

© 2020 Palo Alto Networks, Inc.

Información del cortafuegos gestionado	Description (Descripción)
	asignados, el número de cortafuegos conectados y la ruta del grupo de dispositivos en la jerarquía. Por ejemplo, **Data center (Centro de datos) (2/4 Devices Connected [2/4 de dispositivos conectados]): Shared (Uso compartido)** > **Europe (Europa)** > **Datacenter (Centro de datos)** indica que un grupo de dispositivos llamado **Data center (Centro de datos)** tiene cuatro cortafuegos (dos de ellos conectados) y pertenece a su vez a un grupo de dispositivos llamado **Europe (Europa)**. Puede contraer o expandir cualquier grupo de dispositivos para ocultar o mostrar sus cortafuegos.
Device Name (Nombre del dispositivo)	Muestra el nombre de host o número de serie del cortafuegos. Para el cortafuegos VM-Series edición NSX, el nombre del cortafuegos se adjunta al nombre de host del host ESXi. Por ejemplo, PA-VM: Host-NY5105
Sistema virtual	Muestra los sistemas virtuales disponibles en un cortafuegos en modo para sistemas virtuales múltiples.
Modelo	Muestra el modelo de cortafuegos.
Etiquetas	Muestra las etiquetas definidas para cada sistema virtual/cortafuegos.
Número de serie	Muestra el número de serie del cortafuegos.
Modo de operación	Muestra el modo de operación del cortafuegos. Puede ser FIPS-CC o Normal.
Dirección IP	Muestra la dirección IP del sistema virtual o cortafuegos.
	IPv4: dirección IPv4 del sistema virtual/cortafuegos.
	IPv6: dirección IPv6 del sistema virtual/cortafuegos.
Variables	Cree definiciones de variables para dispositivos específicos copiándolas de un dispositivo en la pila de plantillas o haga clic en Edit (Editar) para editar definiciones de variables existentes y crear variables únicas para el dispositivo. Esta columna estará vacía si el dispositivo no se asocia a una pila de plantillas. De manera predeterminada, las variables se heredan de la pila de plantillas. Consulte Creación o edición de una definición de variable en un dispositivo.
Plantilla	Muestra la pila de plantillas a la que se asigna el cortafuegos.
estado	**Device State**: indica el estado de conexión entre Panorama y el cortafuegos: conectado o desconectado. Un cortafuegos VM-Series puede tener dos estados adicionales: • **Deactivated (Deshabilitado)**: indica que deshabilitó una máquina virtual directamente en el cortafuegos o seleccionando **Deactivate VMs (Deshabilitar VM)** (**Panorama** > **Device Deployment**

© 2020 Palo Alto Networks, Inc.

Información del cortafuegos gestionado	Description (Descripción)
	[Implementación de dispositivo] > **Licenses [Licencias]**) y que eliminó todas las licencias y derechos del cortafuegos. Un cortafuegos deshabilitado ya no está conectado a Panorama porque el proceso de deshabilitación elimina el número de serie en el cortafuegos VM-Series. • **Partially deactivated**: indica que inició un proceso de deshabilitación de licencia desde Panorama que no se ha completado porque el cortafuegos no está conectado y Panorama no se puede comunicar con él.
	HA Status: indica si el cortafuegos está en uno de los siguientes estados: • **Active**: estado operativo de gestión de tráfico normal. • **Passive**: estado de copia de seguridad normal. • **Initiating**: el cortafuegos se encuentra en este estado por hasta 60 segundos desde el arranque. • **Non-functional**: estado de error. • **Suspended**: un administrador deshabilitó el cortafuegos. • **Tentative**: para una monitorización de enlace o ruta en una configuración activo/activo.
	Shared Policy: indica si las configuraciones de política y objeto en el cortafuegos están sincronizadas con Panorama.
	Template: indica si las configuraciones de red y dispositivo en el cortafuegos están sincronizadas con Panorama.
Status (Estado) (cont)	**Certificate (Certificado)**: indica el estado del certificado de cliente del dispositivo gestionado. • **Pre-defined (Predefinido)**: el dispositivo gestionado utiliza un certificado predefinido para autenticarse con Panorama. • **Deployed (Implementada)**: el certificado personalizado se implementa correctamente en el dispositivo gestionado. • **Expires in N days N hours (Vence en N días N horas)**: el certificado actualmente instalado vencerá en menos de 30 días. • **Expires in N minutes (Vence en N minutos)**: el certificado actualmente instalado vencerá en menos de un día. • **Client Identity Check Passed (Comprobación de identidad de cliente aprobada)**: el nombre común del certificado coincide con el número de serie del dispositivo que se conecta. • **OCSP Status Unknown (Estado OCSP desconocido)**: Panorama no puede obtener el estado del OCSP responder. • **OCSP Status Unavailable (Estado OCSP no disponible)**: Panorama no puede contactar con el OCSP responder. • **CRL Status Unknown (Estado CRL desconocido)**: Panorama no puede obtener el estado de revocación de la base de datos de CRL. • **CRL Status Unavailable (Estado CRL no disponible)**: Panorama no puede ponerse en contacto con la base de datos de CRL.

© 2020 Palo Alto Networks, Inc.

Información del cortafuegos gestionado	Description (Descripción)
	• **OCSP/CRL Status Unknown (Estado OCSP/CRL desconocido)**: Panorama no puede obtener el estado OCSP o de revocación cuando ambos están habilitados. • **OCSP/CRL Status Unavailable (Estado OCSP/CRL no disponible)**: Panorama no puede ponerse en contacto con la base de datos OCSP o CRL cuando ambos están habilitados. • **Untrusted Issuer (Emisor no fiable)**: el dispositivo gestionado tiene un certificado personalizado, pero el servidor no lo valida. **Last Commit State**: indica si la última compilación del cortafuegos tuvo éxito o no.
Software Version | Apps and Threat | Antivirus | URL Filtering | GlobalProtect™ Client | WildFire	Muestra las versiones de software y contenido instaladas actualmente en el cortafuegos. Para obtener más información, consulte Software de cortafuegos y actualizaciones de contenido.
Copias de seguridad	En la compilación de cada cortafuegos, PAN-OS automáticamente envía una copia de seguridad de la configuración del cortafuegos a Panorama. Haga clic en **Manage (Gestionar)** para ver las copias de seguridad de la configuración disponible y, de manera opcional, cargue una. Para obtener más información, consulte Copias de seguridad del cortafuegos.
Última inserción de clave maestra	Muestra el estado de la implementación de la clave maestra desde Panorama en el cortafuegos.
	Status (Estado): muestra el último estado de envío de la clave maestra. Puede ser `Success (Correcto)` o `Failed (Fallido)`. `Unknown (Desconocido)` se muestra si una clave maestra no se ha enviado al cortafuegos desde Panorama.
	Timestamp (Marca de tiempo): muestra la fecha y hora del último envío de clave maestra desde Panorama.

Creación de definición de variables de dispositivo

Cuando se añade un dispositivo por primera vez en una pila de plantillas, puede crear definiciones de variables para dispositivos específicos copiadas de dispositivos en la pila de plantillas o puede editar las definiciones de variables de la plantilla a través de **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)**. De manera predeterminada, todas las definiciones de variables se heredan de la pila de plantillas y solo puede anular (no eliminar) las definiciones de variables para un dispositivo individual. Puede utilizar variables para reemplazar objetos de la dirección IP y elementos literales de la dirección IP (máscara de red IP, intervalo IP, FQDN) en todas las áreas de la configuración, las interfaces de la configuración de puerta de enlace de IKE (interfaz) y la configuración de HA (ID de grupo).

© 2020 Palo Alto Networks, Inc.

Creación de la información de definición de variables de dispositivo	Description (Descripción)
Clone device variable definition from another device in the template stack? (¿Clonar definición de variable de dispositivo desde otro dispositivo en la pila de plantillas?)	
No	Observe las definiciones de variable existentes y edítelas según sea necesario. Consulte Panorama > Templates (Plantillas) > Template Variables (Variables de plantilla).
yes (sí)	Seleccione un dispositivo en el menú desplegable que se utilizará para clonar las definiciones de variables y seleccione las definiciones de variables específicas que desea clonar.

Software de cortafuegos y actualizaciones de contenido

Para instalar una actualización de contenido o software en un cortafuegos gestionado, primero utilice las páginas **Panorama** > **Device Deployment (Implementación de dispositivo)** para descargar o cargar la actualización en Panorama. Luego, seleccione la página **Panorama** > **Managed Devices (Dispositivos gestionados)**, haga clic en **Install (Instalar)** y complete los siguientes campos.

Para reducir el tráfico en la interfaz de gestión (MGT), puede configurar Panorama para utilizar una interfaz independiente para implementar actualizaciones (consulte Panorama > Setup > Interfaces).

Opciones de instalación de actualización de contenido/ software del cortafuegos	Description (Descripción)
Tipo	Seleccione el tipo de actualización que desea instalar: **Software** PAN-OS, software del **GlobalProtect Client (cliente de GlobalProtect)**, firmas de **Apps and Threats (Aplicaciones y amenazas)**, firmas de **antivirus**, **WildFire** o **URL Filtering (Filtrado de URL)**.
Archivo	Seleccione la imagen de actualización. El menú desplegable solo incluye las imágenes que ha descargado o cargado en Panorama mediante las páginas **Panorama** > **Device Deployment (Implementación de dispositivo)**.
Filtros	Seleccione Filters (Filtros) para filtrar la lista de dispositivos.
Dispositivos	Seleccione los cortafuegos en los que desea instalar la imagen.
Device Name (Nombre del dispositivo)	El nombre del cortafuegos.
Versión actual	La versión de actualización del **Type (Tipo)** seleccionado que está actualmente instalado en el cortafuegos.
Estado HA	Indica si el cortafuegos está en uno de los siguientes estados: • **Active**: estado operativo de gestión de tráfico normal.

© 2020 Palo Alto Networks, Inc.

Opciones de instalación de actualización de contenido/ software del cortafuegos	Description (Descripción)
	• **Passive**: estado de copia de seguridad normal. • **Initiating**: el cortafuegos se encuentra en este estado por hasta 60 segundos desde el arranque. • **Non-functional**: estado de error. • **Suspended**: un administrador deshabilitó el cortafuegos. • **Tentative**: para una monitorización de enlace o ruta en una configuración activo/activo.
Agrupar Peers HA	Seleccione esta opción para agrupar cortafuegos que son peers en una configuración de alta disponibilidad (HA).
Filtro seleccionado	Si quiere que la lista de dispositivos muestre solo cortafuegos específicos, seleccione los correspondientes nombres de dispositivos y **Filter Selected (Filtrar seleccionados)**.
Cargar solo al dispositivo	Seleccione para cargar la imagen en el cortafuegos pero no reiniciar automáticamente el cortafuegos. La imagen se instala cuando reinicia manualmente el cortafuegos.
Reiniciar dispositivo después de la instalación (solo el software)	Seleccione esta opción para cargar e instalar la imagen del software. El proceso de instalación provoca un reinicio.
Deshabilitar nuevas aplicaciones en la actualización de contenido (solo aplicaciones y amenazas)	Seleccione esta opción para deshabilitar aplicaciones en la actualización que son nuevas en relación con la última actualización instalada. Esto lo protege contra las últimas amenazas y le brinda la flexibilidad de habilitar aplicaciones después de preparar cualquier actualización de políticas. Luego, para habilitar las aplicaciones, inicie sesión en el cortafuegos, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, haga clic en **Apps (Aplicaciones)** en la columna Features (Funciones) para mostrar las nuevas aplicaciones y luego haga clic en **Enable/Disable (Habilitar/Deshabilitar)** en cada aplicación que desee habilitar.

Copias de seguridad de cortafuegos

- Panorama > Dispositivos gestionados

Panorama realiza automáticamente una copia de seguridad de todos los cambios de configuración que se confirman en los cortafuegos gestionados. Para gestionar las copias de seguridad de un cortafuegos, seleccione **Panorama** > **Managed Devices (Dispositivos gestionados)**, haga clic en **Manage (Gestionar)** en la columna Backups (Copias de seguridad) del cortafuegos, y lleve a cabo alguna de las siguientes tareas.

Para configurar el número de copias de seguridad de la configuración del cortafuegos que se guardan en Panorama, seleccione Panorama > Setup (Configuración) > Management (Gestión), edite la configuración de creación de logs e informes, seleccione Log Export and Reporting (Exportación e informes de logs), e ingrese el número de versiones en Number of Versions for Config Backups (Número de versiones para copias de seguridad de Configuración) (el valor predeterminado es 100).

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Vea los detalles sobre una configuración confirmada o guardada.	En la columna Version de la copia de seguridad, haga clic en el nombre de archivo de la configuración guardada o en el número de versión de la configuración confirmada para mostrar el contenido del archivo XML asociado.
Restaure una configuración guardada o confirmada a la configuración candidata.	En la columna Action de la copia de seguridad, haga clic en **Load (Cargar)** y **Commit (Confirmar)**.
Borre una configuración guardada.	En la columna Action de la copia de seguridad, haga clic en Delete ( ).

Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen)

Panorama™ le permite supervisar los recursos y el rendimiento del hardware de los cortafuegos gestionados. Panorama centraliza información de rendimiento (CPU, memoria, CPS y rendimiento), de rendimiento en la creación de logs y del entorno (como ventiladores, estado de RAID y fuentes de alimentación) en tendencias de tiempo, correlaciona eventos (como confirmaciones, instalaciones de contenido y actualizaciones de software) con los datos de estado. Cuando un cortafuegos se desvía de su referencia calculada, Panorama lo informa como un Deviating Device (Dispositivo desviado) con el fin de identificar, diagnosticar y resolver los problemas de hardware con rapidez.

También puede usar esta página para:

View Detailed Device Health (Ver el estado detallado del dispositivo)	Vea las métricas de estado de los dispositivos que gestiona Panorama.
Agrupar Peers HA	Vea qué cortafuegos están agrupados para permitir identificar problemas potenciales y determinar si y a cuales los problemas de recursos de hardware o de rendimiento los afecta.
PDF/CSV	Las funciones administrativas con un mínimo de acceso solo de lectura pueden exportar la tabla de cortafuegos gestionados en formato **PDF/CSV**. Es posible aplicar filtros para crear resultados más específicos de la configuración de la tabla cuando sea necesario para elementos como las auditorías. Únicamente se exportan las columnas visibles en la interfaz web. Consulte Datos de la tabla de configuración de exportación.

Panorama > Managed Devices (Dispositivos gestionados) > Summary (Resumen) > All Devices (Todos los dispositivos)

Utilice esta página para ver la siguiente información de cada cortafuegos.

© 2020 Palo Alto Networks, Inc.

Información de estado	Description (Descripción)
Device Name (Nombre del dispositivo)	Nombre de host o número de serie del cortafuegos. Para el cortafuegos VM-Series edición NSX, el nombre del cortafuegos se adjunta al nombre de host del host ESXi. Por ejemplo, PA-VM: Host-NY5105
Modelo	Modelo del cortafuegos.
Dispositivo	
Throughput (Rendimiento) (Kbps)	El rendimiento de los datos en el tiempo (media de cinco minutos) que se mide en kilobytes por segundo.
CPS	Total de conexiones por segundo del cortafuegos en el tiempo (media de cinco minutos).
session	
Counts (Recuentos) (Sesiones)	Recuento total de sesiones en el tiempo (media de cinco minutos).
PLANO DE DATOS	
CPU (%)	Utilización total de CPU en el plano de datos.
Plano de administración	
CPU (%)	Utilización total de CPU en el plano de gestión.
MEM (%)	Utilización total de memoria en el plano de gestión.
Logging Rate (Tasa de creación de logs) (logs por segundo)	Tasa de reenvío de logs desde los cortafuegos a Panorama o el recopilador de logs (media de un minuto)
Fans (Ventiladores)	Muestra la presencia, el estado actual, las RPM y el último fallo de los ventiladores en cada placa de ventiladores. El estado del ventilador se muestra como *A*/*B*, donde *A* es el número de ventiladores aceptables y en funcionamiento, y *B* es el número total de ventiladores en el cortafuegos. Los cortafuegos virtuales muestran `N/A (N/D)`.
Power Supplies (Fuentes de alimentación)	Muestra la presencia, el estado actual y la última marca de tiempo de fallo. El estado de las fuentes de alimentación se muestra como *A*/*B*, donde *A* es el número de fuentes de alimentación aceptables y en funcionamiento, y *B* es el número total de fuentes de alimentación el cortafuegos. Los cortafuegos virtuales muestran `N/A (N/D)`.
Ports (Puertos)	Número total de puertos en uso en el cortafuegos Los puertos se muestran como *A*/*B*, donde *A* es el número de puertos aceptables y en funcionamiento, y *B* es el número total de puertos en el dispositivo.

© 2020 Palo Alto Networks, Inc.

Panorama > Managed Devices (Dispositivos gestionados) > Health (Estado) > Deviating Devices (Dispositivos desviados)

La pestaña Deviating Devices (Dispositivos desviados) muestra dispositivos que cuentan con métricas que se desvían de su referencia calculada y muestra estos dispositivos en rojo. Una referencia de estado de métrica se determina calculando la media del rendimiento de estado para una métrica concreta en un período de siete días más la desviación estándar.

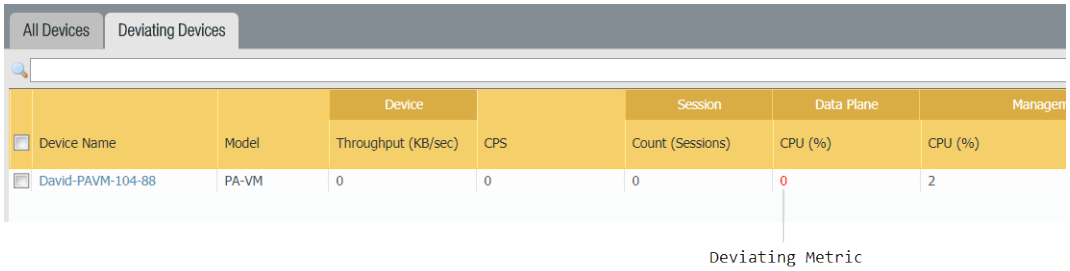


Figure 1: Ejemplo de una métrica desviada

Estado detallado de dispositivos en Panorama

Puede ver un historial detallado del estado del dispositivo de un cortafuegos individual haciendo clic en el nombre del dispositivo en la pestaña All Devices (Todos los dispositivos) o la pestaña Deviating Devices (Dispositivos desviados). La vista Detailed Device (Detalles de dispositivo) brinda el historial de estado de salud utilizando un filtro de tiempo y muestra los metadatos asociados al dispositivo. La información del estado del dispositivo se muestra como una tabla o un widget cuando sea posible para brindar una representación gráfica de datos en tendencias de tiempo.

Gestión de la vista detallada de dispositivos

Además de los metadatos descriptivos asociados al cortafuegos, la vista Detailed Device (Detalles de dispositivo) muestra la información detallada del estado del cortafuegos. Cuando corresponda, puede configurar los ajustes ( ) para añadir opciones al widget o hacer clic en Maximizar Panel ( ) para agrandar el widget.

Campo	Description (Descripción)
Acciones	
Time Filter (Filtro de tiempo)	Seleccione el filtro de tiempo para ver el historial de estado del dispositivo de la lista desplegable. Puede seleccionar **Last 12 hours (Últimas 12 horas)**, **24 hours (24 horas)**, **7 days (7 días)**, **15 days (15 días)**, **30 days (30 días)** o **90 days (90 días)**.
Show Average (Mostrar media)	Seleccione la distribución media y estándar que se muestra en los widgets en tendencias de tiempo. Puede seleccionar **None (Ninguno)**, **Last 24 hours (Últimas 24 horas)**, **7 days (7 días)** o **15 days (15 días)**.
Actualizar	Actualiza la información que se muestra con los datos más recientes.
Print PDF (Imprimir PDF)	Genera un PDF de la pestaña que se muestra actualmente.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	Debe habilitar las ventanas emergentes para seleccionar una ubicación de descarga y acceder al PDF.
System Information (Información del sistema)	
System Information (Información del sistema)	Los metadatos asociados al dispositivo: dirección IP, versión de software, versión de antivirus, estado de HA, número de serie, versión de aplicación y amenaza, versión de WildFire, modo de VSYS, modelo y modo de dispositivo.

Sesiones

La pestaña Sessions (Sesiones) muestra la información de sesión que pasa a través del cortafuegos. Esta información se muestra en seis gráficos individuales.

Campo	Description (Descripción)
Throughput (Rendimiento)	El rendimiento de los datos en el tiempo (media de cinco minutos) medida en kilobits por segundo (Kbps).
Número de sesiones	Recuento total de sesiones en el tiempo (media de cinco minutos).
Connections per Second (Conexiones por segundo)	Total de CPS del dispositivo en el tiempo (media de cinco minutos).
Packets per Second (Paquetes por segundo)	Total de paquetes por segundo (media de cinco minutos) que pasaron a través del dispositivo.
Global Session Table Utilization (Utilización de la tabla de sesión global) (Solo en dispositivos de la serie PA-7000 y PA-5200)	Porcentaje de la tabla de sesión global en el tiempo para cortafuegos con una tabla de sesión global (media de cinco minutos).
Session Table Utilization (Utilización de la tabla de sesión)	Muestra el porcentaje de la utilización de la tabla de sesión para cada plano de datos del cortafuegos en el tiempo (media de cinco minutos).
SSL Decrypted Sessions Info (Información de sesiones SSL descifradas)	Muestra el número de sesiones SSL descifradas en el tiempo (media de cinco minutos).
SSL Proxy Session Utilization (Utilización de sesión de proxy SSL)	Muestra el porcentaje de utilización de las sesiones de proxy en el tiempo (media de cinco minutos).

© 2020 Palo Alto Networks, Inc.

Entornos

La pestaña **Environments (Entornos)** muestra la presencia, estado y condición operativa del hardware, como fuentes de alimentación, placas de ventiladores y unidades de disco. Esta tabla solo muestra información sobre cortafuegos basados en hardware:

Campo	Description (Descripción)
Fan Status (Estado del ventilador)	Muestra la presencia, el estado actual, las RPM y el último fallo de los ventiladores en cada placa de ventiladores. El estado del ventilador se muestra como *A*/*B*, donde *A* es el número de ventiladores aceptables y en funcionamiento, y *B* es el número total de ventiladores en el cortafuegos. Los cortafuegos virtuales muestran `N/A (N/D)`.
Fuente de alimentación	Muestra la presencia, el estado actual y la última marca de tiempo de fallo. El estado de las fuentes de alimentación se muestra como *A*/*B*, donde *A* es el número de fuentes de alimentación aceptables y en funcionamiento, y *B* es el número total de fuentes de alimentación el cortafuegos. Los cortafuegos virtuales muestran `N/A (N/D)`.
Thermal Status (Estado térmico)	Muestra si existen alarmas térmicas asociadas a cada ranura del dispositivo. Si existe una alarma activa, el cortafuegos también muestra más información concreta sobre la temperatura y la ubicación exactas.
System Disk Status (Estado del disco del sistema)	Muestra el porcentaje disponible, en uso y para utilizar de los montajes root, pancfg, panlogs y panrepo. Esta sección también muestra el nombre del disco, el tamaño y el estado de RAID en los cortafuegos con RAID habilitado.

Interfaces

La pestaña Interfaces muestra el estado y las estadísticas de todas las interfaces físicas del cortafuegos.

Campo	Description (Descripción)
Nombre de interfaz	El nombre de la interfaz. Seleccione una interfaz para ver los gráficos de la tasa de bits, paquetes por segundo, errores y descartes de la interfaz seleccionada.
estado	El estado de la interfaz: `Administrador habilitado`, `Administrador deshabilitado`, `Operación habilitada`, u `Operación deshabilitada`.
Bit Rate (Tasa de bits)	Muestra la tasa de bits (bps) de datos recibidos y transmitidos.
Packets per Second (Paquetes por segundo)	Muestra el número de paquetes de datos recibidos y transmitidos por segundo.
Errores	Muestra el número de errores en datos recibidos y transmitidos.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Drops (Conexiones descartadas)	Muestra el número de conexiones descartadas de datos recibidos y transmitidos.

de creación de logs

La pestaña Logging (Creación de logs) muestra la tasa de creación de logs y las conexiones en los cortafuegos gestionados.

Campo	Description (Descripción)
Tasa de log	Muestra la tasa media de un minuto del reenvío de logs del dispositivo a Panorama o a un recopilador de logs.
Logging Connections (Conexiones de logs)	Muestra todas las conexiones de reenvío de logs disponibles, que incluye su estado activo o inactivo.
External Log Forwarding (Reenvío de logs externos)	Muestra la cantidad de logs enviados y descartados, y la tasa de reenvío media de logs (logs por segundo) de varios tipos de métodos de reenvío de logs externos.

FUENTES

La pestaña Resources (Recursos) muestra la estadística de CPU y memoria del cortafuegos.

Campo	Description (Descripción)
Management Plane Memory (Memoria de plano de gestión)	Muestra la media de cinco minutos en tendencias de tiempo de la memoria de plano de gestión como un porcentaje.
Packet Buffers (Búferes de paquetes)	Muestra la media de cinco minutos en tendencias de tiempo de la utilización del búfer de paquetes como un porcentaje. En un sistema con múltiples planos de datos, incluye los diferentes planos de datos, la CPU y los búferes de paquetes en diferentes colores.
Descriptores de paquetes	Muestra la media de cinco minutos en tendencias de tiempo de la utilización del descriptor de paquetes como un porcentaje. En un sistema con múltiples planos de datos, incluye los diferentes planos de datos, la CPU y los búferes de paquetes en diferentes colores.
CPU Management Plane (Plano de gestión de la CPU)	Muestra la media de cinco minutos en tendencias de tiempo de la CPU del plano de gestión.
CPU Data Plane (Plano de datos de la CPU)	Muestra la media de cinco minutos en tendencias de tiempo de la utilización por núcleo de la CPU del plano de datos. En los sistemas con múltiples planos de datos, puede seleccionar el plano de datos que desea ver en el selector.
Mounts (Montajes)	Muestra la información de los archivos del sistema del dispositivo. Esto incluye Name (Nombre), espacio Allocated (Asignado) (KB), Used

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	(Utilizado) (KB) y Avail (Disponible) (KB), además del porcentaje de Utilization (Utilización).

High Availability

La pestaña High Availability (Alta disponibilidad) muestra el estado de HA del cortafuegos y su peer de HA. El widget superior muestra la configuración y la versión de contenido del dispositivo y sus peers. El widget inferior brinda información sobre las conmutaciones por error de HA previas y los motivos asociados a ellas, e incluye qué cortafuegos experimentó un fallo.

© 2020 Palo Alto Networks, Inc.

Panorama > Plantillas

A través de las pestañas **Device (Dispositivo)** y **Network (Red)**, puede implementar una configuración básica común en múltiples cortafuegos que requieren configuraciones similares mediante una plantilla o una pila de plantillas (una combinación de plantillas). Al gestionar configuraciones de cortafuegos con Panorama, se usa una combinación de grupos de dispositivos (para gestionar políticas y objetos compartidos) y plantillas (para gestionar configuraciones de red y dispositivos compartidos).

Además de los ajustes disponibles en los cuadros de diálogo para crear Plantillas o Pilas de plantillas, **Panorama** > **Templates (Plantillas)** muestra las siguientes columnas:

- **Type**: identifica las entradas de la lista como plantillas o pilas de plantillas.
- **Stack**: enumera las plantillas asignadas a una pila de plantillas.

¿Qué desea hacer?	Consulte:
Agregar, clonar, editar o eliminar una plantilla	Plantillas
Agregar, clonar, editar o eliminar una pila de plantillas	Pilas de plantillas
¿Busca más información?	Plantillas y pilas de plantillas
	Gestión de plantillas y pilas de plantillas

Plantillas

Panorama admite hasta 1.024 plantillas. Es posible hacer clic en **Add (Añadir)** para añadir una plantilla y configurar los ajustes como se describe en la siguiente tabla. Después de crear una plantilla, debe realizar la Configuración de una pila de plantillas y añadir las plantillas y los cortafuegos a la pila de plantillas antes de gestionar sus cortafuegos. Después de configurar una plantilla, debe confirmar los cambios en Panorama (consulte Operaciones de confirmación de Panorama).

Si elimina una plantilla, no se eliminan los valores que Panorama ha enviado al cortafuegos.

Configuración de plantillas	Description (Descripción)
Nombre	Introduzca un nombre de plantilla (de hasta 31 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, espacios, puntos, guiones y guiones bajos. En las pestañas **Device (Dispositivo)** y **Network (Red)**, este nombre aparecerá en el menú desplegable **Template (Plantilla)**. Las configuraciones que modifique en estas plantillas se aplicarán solamente a la **Plantilla** seleccionada.
Description (Descripción)	Introduzca una descripción para la plantilla.

© 2020 Palo Alto Networks, Inc.

Pilas de plantillas

Puede configurar una pila de plantillas o asignar plantillas a una pila de plantillas. Asignar cortafuegos a una pila de plantillas le permite enviar toda la configuración necesaria a los cortafuegos, en lugar de añadir cada una a cada plantilla individualmente. Panorama admite hasta 1.024 pilas. Puede hacer clic en **Add (Añadir)** para crear una nueva pila de plantillas y configurar los ajustes como se describe en la siguiente tabla. Después de configurar una pila de plantilla, debe confirmar los cambios en Panorama (consulte Operaciones de confirmación de Panorama). Además, después de configurar la red y las opciones de dispositivos de los cortafuegos asignados a la pila de plantillas, debe realizar una confirmación para enviar la configuración a los cortafuegos.

La eliminación de una pila de plantillas o la eliminación de un cortafuegos de una pila de plantillas no elimina los valores que Panorama previamente envió a ese cortafuegos; sin embargo, al quitar un cortafuegos de una pila de plantillas, Panorama ya no envía las nuevas actualizaciones a ese cortafuegos.

Configuración de pilas de plantillas	Description (Descripción)
Nombre	Introduzca un nombre para la pila (de hasta 31 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, debe comenzar con una letra, y solo puede contener letras, números y guiones bajos. En las pestañas **Device (Dispositivo)** y **Network (Red)**, el menú desplegable **Template (Plantilla)** muestra el nombre de la pila y las plantillas asignadas a ella.
Description (Descripción)	Introduzca una descripción para la pila.
Plantillas	**Add (Añadir)** cada plantilla que desea incluir en la pila (hasta 8). Si las plantillas tienen configuraciones duplicadas, Panorama envía solo las configuraciones de la plantilla de mayor nivel en la lista a los cortafuegos asignados. Por ejemplo, si Plantilla_A está antes que Plantilla_B en la lista y ambas plantillas definen la interfaz ethernet1/1, Panorama envía la definición de ethernet1/1 desde Plantilla_A y no desde Plantilla_B. Para cambiar el orden de las plantillas de la lista, seleccione una plantilla y seleccione **Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. *Panorama no valida combinaciones de plantillas en pilas, por lo que deberá planificar el orden de modo que se eviten las relaciones no válidas.*
Dispositivos	Seleccione cada cortafuegos que desee añadir a la pila de plantillas. Si la lista de cortafuegos es larga, puede filtrar por **Platforms (Plataformas)**, **Device Groups (Grupos de dispositivos)**, **Tags (Etiquetas)** y **HA Status (Estado de HA)**. *Puede asignar cortafuegos con modos no coincidentes (modo VPN, modo de sistemas virtuales múltiples o modo de operación) a la misma pila de plantillas. Panorama envía la configuración específica del modo solo a los cortafuegos compatibles con el modo.*

© 2020 Palo Alto Networks, Inc.

Configuración de pilas de plantillas	Description (Descripción)
Seleccionar todo	Selecciona todos los cortafuegos de la lista.
Anular selección	Anula la selección de todos los cortafuegos de la lista.
Agrupar Peers HA	Agrupe cortafuegos que son peers de alta disponibilidad (HA). Esta opción le permite identificar fácilmente cortafuegos que tienen una configuración de HA. Al enviar configuraciones de la pila de plantillas, puede enviar el par agrupado, en lugar de cada cortafuegos individualmente.
Filtro seleccionado	Para mostrar solo los cortafuegos específicos, selecciónelos y luego seleccione **Filter Selected (Filtrar seleccionados)**.

Panorama > Templates (Plantillas) > Template Variables (Variables de plantilla)

- Creación de nueva variable de plantilla
- Edición de una variable de plantilla existente
- Creación o edición de una definición de variable en un dispositivo

Puede definir variables (**Panorama** > **Templates [Plantillas]**) para las plantillas o las pilas de plantillas, o puede editar variables existentes para un dispositivo individual (**Panorama** > **Managed Devices [Dispositivos gestionados]** > **Summary [Resumen]**). Las variables son componentes de configuración definidos en la plantilla o en la pila de plantillas que brindan flexibilidad o reutilización cuando utiliza Panorama para gestionar configuraciones de cortafuegos. Puede utilizar variables para reemplazar lo siguiente:

- Una dirección IP (incluye máscara de red IP, rango IP y FQDN) en todas las áreas de la configuración.
- Interfaces en una configuración de puerta de enlace IKE (interfaz) y una configuración de HA (ID de grupo).

Cuando añade cortafuegos a una pila de plantillas, estos heredan automáticamente las variables que crea para una plantilla o pila de plantillas.

Información de variables de plantillas	Description (Descripción)
Nombre	El nombre de la definición de la variable.
Template (device and template stack) (Plantilla [dispositivo y pila de plantillas])	Muestra el nombre de la plantilla a la que pertenece la definición de la variable.
Tipo	Muestra el tipo de definición de variable: • **IP Netmask (Máscara de red IP)**: defina una dirección de red o dirección IP estática. • **IP Range (Intervalo de IP)**: defina un intervalo de IP. Por ejemplo, 192.168.1.10-192.168.1.20. • **FQDN**: defina un nombre de dominio completo.

© 2020 Palo Alto Networks, Inc.

Información de variables de plantillas	Description (Descripción)
	• **Group ID (ID de grupo)**: defina la ID de grupo de alta disponibilidad. Para obtener más información, consulte Pautas de configuración de HA activa/pasiva. • **Interface (Interfaz)**: defina una interfaz de cortafuegos en el cortafuegos. Solo puede utilizarse con una configuración de puerta de enlace IKE.
Valor	Muestra el valor configurado para la definición de variable.
Add (Añadir) (plantilla y pila de plantillas)	Añada una nueva definición de variable de plantilla.
delete	Elimine una definición de variable de plantilla existente.
Duplicar	Duplique una definición de variable de plantilla existente.
Override (Anular) (pila de plantillas y dispositivo)	Anula una definición de variable de plantilla existente heredada de la pila de plantillas o el dispositivo. No puede cambiar el tipo o el nombre de la variable y no puede anular variables de dispositivos concretos.
Revert (Revertir) (pila de plantillas y dispositivo)	Para eliminar los valores anulados en el nivel de la pila de plantillas o el dispositivo; revierte la variable anulada a la definición de variable de plantilla original.
Get values used on device only (Obtener valores utilizados solo en el dispositivo) (solo en dispositivos)	Rellene la variable seleccionada con el valor utilizado en el cortafuegos. Requiere que ya se haya definido una variable de plantilla o pila de plantillas y se haya enviado al cortafuegos antes de que Panorama pueda recuperar el valor. Los valores que se obtienen del cortafuegos **Override (Anularán)** la variable de plantilla o pila de plantillas para crear una variable para un dispositivo concreto. Si no se han enviado definiciones de variables al cortafuegos, Panorama enviará el mensaje `Value not found` (Valor no encontrado) para esa variable.

Creación de nueva variable de plantilla

Haga clic en **Add (Añadir)** para añadir una nueva definición de variable de plantilla.

Información de nueva definición de variable de plantilla	Description (Descripción)
Nombre	Brinde un nombre a la definición de la variable. Todos los nombres de definición de variable deben comenzar con el caracter de signo de dólar ("$").
Tipo	Seleccione el tipo de definición de variable: **IP Netmask (Máscara de red IP)**, **IP Range (Intervalo IP)**, **FQDN**, **Group ID (ID de grupo)** o **Interface (Interfaz)**.

© 2020 Palo Alto Networks, Inc.

Información de nueva definición de variable de plantilla	Description (Descripción)
Valor	Introduzca el valor deseado para la definición de variable.

Edición de una variable de plantilla existente

Puede editar una variable de definición de plantilla para una plantilla o pila de plantillas en cualquier momento después de que se crea la variable (**Panorama** > **Templates [Plantillas]**). Haga clic en **Manage (Gestionar)** para gestionar las variables de plantilla, y seleccionar una variable y editar los valores disponibles como sea necesario.

Creación o edición de una definición de variable en un dispositivo

Vaya a **Panorama** > **Managed Devices (Dispositivos gestionados)** > **Summary (Resumen)** para crear definiciones de variables o anular variables de plantilla enviadas desde una plantilla o pila de plantillas de Panorama. Las variables de plantilla incluyen lo siguiente:

- Una dirección IP (máscara de red IP, rango IP o FQDN) en todas las áreas de la configuración.
- Interfaces en una configuración de puerta de enlace IKE (interfaz) o una configuración de HA (ID de grupo).

La creación de una variable de dispositivo le permite copiar variables de dispositivos concretos anuladas desde un dispositivo en la misma pila de plantillas en lugar de recrearlas individualmente. De manera predeterminada, todas las definiciones de variables se heredan de la plantilla o pila de plantillas, y solo se pueden anular (no puede eliminar ni crear nuevas definiciones de variable para un dispositivo individual.

Haga clic en **Create (Crear)** para crear definiciones de variables de dispositivo copiando definiciones de variables de dispositivos existentes en la pila de plantillas o haga clic en **Edit (Editar)** para editar las definiciones de variables de dispositivo existentes.

© 2020 Palo Alto Networks, Inc.

Panorama > Grupos de dispositivos

Los grupos de dispositivos están formados por cortafuegos y sistemas virtuales que desea gestionar como grupo, como los cortafuegos que gestionan un grupo de sucursales o departamentos individuales de una empresa. Panorama trata cada grupo como una sola unidad al aplicar políticas. Los cortafuegos solo pueden pertenecer a un único grupo de dispositivos pero, puesto que los sistemas virtuales se consideran entidades independientes en Panorama, puede asignar sistemas virtuales dentro de un cortafuegos a diferentes grupos de dispositivos.

Puede anidar grupos de dispositivos en un árbol jerárquico de hasta cuatro niveles en la ubicación compartida para implementar un método por capas para la gestión de políticas en toda la red de cortafuegos. En el nivel inferior, un grupo de dispositivos puede tener grupos de dispositivos primarios, primarios principales y primarios principales superiores en niveles sucesivamente mayores (lo que en conjunto se denomina *antecesores*), de los cuales el grupo de dispositivos de nivel inferior hereda políticas y objetos. En el nivel superior, un grupo de dispositivos puede tener grupos de dispositivos secundarios, secundarios de segundo nivel y secundarios de tercer nivel (lo que en conjunto se denomina *descendientes*). Cuando selecciona **Panorama** > **Device Groups (Grupos de dispositivos)**, la columna Name muestra esta jerarquía de grupos de dispositivos.

Después de añadir, editar o eliminar un grupo de dispositivos, debe realizar una compilación de Panorama y una compilación del grupo de dispositivos (consulte Operaciones Commit de Panorama). Panorama envía los cambios de configuración a los cortafuegos asignados al grupo de dispositivos; Panorama admite hasta 1024 grupos de dispositivos.

Para configurar un grupo de dispositivos, haga clic en **Add (Añadir)** y configure los ajustes como se describe en la siguiente tabla.

Configuración de grupos de dispositivos	Description (Descripción)
Nombre	Introduzca un nombre para identificar el grupo (de hasta 31 caracteres). El nombre debe ser único en toda la jerarquía del grupo de dispositivos, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, espacios, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción para el grupo de dispositivos.
Dispositivos	Seleccione cada cortafuegos que desee añadir al grupo de dispositivos. Si la lista de cortafuegos es larga, puede filtrar por **Device State (Estado de dispositivo)**, **Platforms (Plataformas)**, **Templates (Plantillas)** o **Tags (Etiquetas)**. La sección Filtros muestra (entre paréntesis) el número de dispositivos gestionados para cada una de estas categorías. Si el objetivo de un grupo de dispositivos es puramente organizativo (es decir, contener otros grupos de dispositivos), no es necesario que le asigne cortafuegos.
Seleccionar todo	Selecciona todos los cortafuegos y sistemas virtuales de la lista.
Anular selección	Anula la selección de todos los cortafuegos y sistemas virtuales de la lista.

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de dispositivos	Description (Descripción)
Agrupar Peers HA	Seleccione esta opción para agrupar cortafuegos que son peers en una configuración de alta disponibilidad (HA). A continuación, la lista muestra primero el cortafuegos activo (o activo-primario en una configuración activo/activo) y luego el cortafuegos pasivo (o activo-secundario en configuración activo/activo) entre paréntesis. Esto le permite identificar fácilmente los cortafuegos en el modo HA. Al enviar políticas compartidas, puede implementar el par agrupado, en lugar de peers individuales. *Para peers HA en configuración activo/pasivo, puede añadir ambos cortafuegos o sus sistemas virtuales al mismo grupo de dispositivos. Esto le permite enviar la configuración a ambos peers al mismo tiempo.*
Filtro seleccionado	Si quiere que la lista de dispositivos muestre solo cortafuegos específicos, seleccione los cortafuegos y luego **Filter Selected (Filtrar seleccionados)**.
Grupo de dispositivos primario	En relación con el grupo de dispositivos que está definiendo, seleccione el grupo de dispositivos (o la ubicación compartida) en el nivel inmediatamente superior de la jerarquía [la opción predeterminada es **Shared (Compartido)**].
Dispositivo principal	Para configurar las reglas de políticas y los informes por nombres de usuario y grupos de usuarios, debe seleccionar un **Master Device (Dispositivo maestro)**. Este es el cortafuegos que envía a Panorama los nombres de usuario, los nombres de grupo de usuarios y la información de asignación de nombre de usuario a grupo. *Cuando cambie el Master Device (Dispositivo maestro) o lo establezca en None (Ninguno), Panorama pierde toda la información de usuarios y grupos recibida de ese cortafuegos.*
Store users and groups from Master Device	Esta opción solo se muestra si selecciona un **Master Device (Dispositivo maestro)**. La opción permite a Panorama almacenar localmente nombres de usuario, nombres de grupo de usuarios e información de asignación de nombre de usuario a grupo que recibe del **Master Device (Dispositivo maestro)**. Para habilitar el almacenamiento local, también debe seleccionar **Panorama** > **Setup (Configuración)** > **Management (Gestión)**, editar la configuración de Panorama y realizar la Habilitación de informes y filtrado en grupos.
Propiedades de dispositivo añadidas dinámicamente: cuando se añade un nuevo dispositivo al grupo de dispositivos, Panorama aplica dinámicamente el código de autorización especificado y la versión del software PAN-OS al nuevo dispositivo. Solo se muestra cuando un grupo de dispositivos está asociado a una definición de servicio NSX en Panorama.	
Código de autorización	Introduzca el código de autorización que se aplicará a los dispositivos añadidos a este grupo de dispositivos.
Versión de software	Seleccione la versión de software que se aplicará a los dispositivos añadidos a este grupo de dispositivos.

© 2020 Palo Alto Networks, Inc.

Panorama > Recopiladores gestionados

El servidor de gestión de Panorama (dispositivo serie M o dispositivo virtual de Panorama en modo Panorama) puede gestionar los recopiladores de log dedicados (dispositivos serie M o dispositivos virtuales de Panorama en modo de recopilación de logs). Cada servidor de gestión de Panorama también tiene un recopilador de logs local predefinido (denominado predeterminado) para procesar los logs que recibe directamente de los cortafuegos. (Un dispositivo virtual de Panorama en modo heredado procesa los logs que recibe directamente de los cortafuegos sin usar un recopilador de logs dedicado).

Para usar Panorama para gestionar un Recopilador de logs dedicado, añada el Recopilador de logs como un *recopilador gestionado*.

¿Qué desea hacer?	Consulte:
Mostrar información del recopilador de logs	Información del recopilador de logs
Añadir, editar o eliminar un recopilador de logs	Configuración del recopilador de logs
Actualizar el software Panorama en un recopilador de logs	Actualizaciones de software para recopiladores de logs dedicados
¿Busca más información?	Creación centralizada de logs e informes
	Configurar un recopilador gestionado

Información del recopilador de logs

Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para mostrar la siguiente información de los recopiladores de logs. Se pueden configurar parámetros adicionales durante la configuración del recopilador de logs.

Información del recopilador de logs	Description (Descripción)
Nombre del recopilador	El nombre que identifica este recopilador de logs. Este nombre se muestra como el nombre de host del recopilador de logs.
Número de serie	El número de serie del dispositivo de Panorama que funciona como recopilador de logs. Si el recopilador de logs es local, este es el número de serie del servidor de gestión Panorama.
Versión de software	La versión de software de Panorama instalada en el recopilador de logs.
Dirección IP	La dirección IP de la interfaz de gestión en el recopilador de logs.
Conectado	El estado de la conexión entre el recopilador de logs y Panorama.

© 2020 Palo Alto Networks, Inc.

Información del recopilador de logs	Description (Descripción)
Estado/detalle de configuración	Indica si la configuración del recopilador de logs está sincronizada con Panorama.
Estado/detalle del tiempo de ejecución	El estado de la conexión entre este y otros recopiladores de logs en el grupo de recopiladores.
Estado de redistribución de logs	Ciertas acciones (por ejemplo, añadir discos) provocarán que el recopilador de logs redistribuya los logs entre sus pares de discos. Esta columna indica el estado de finalización del proceso de redistribución como un porcentaje.
Último estado de compilación	Indica si la última compilación del grupo de recopiladores realizada en el recopilador de logs falló o fue exitosa.
Estadísticas	Cuando finalice la configuración del recopilador de logs, haga clic en **Statistics (Estadísticas)** para ver la información del disco, el rendimiento de la CPU y la tasa media de logs por segundo. Para entender mejor el intervalo de logs que está revisando, también puede ver información en el log más antiguo que ha recibido el recopilador. *Si utiliza un gestor SNMP para supervisar de forma centralizada, también podrá ver las estadísticas de logs en el MIB de panLogCollector.*

Configuración del recopilador de logs

Seleccione **Panorama** > **Managed Collectors (Recopiladores gestionados)** para gestionar los recopiladores del logs. Al pulsar **Add (Añadir)** para añadir un nuevo recopilador de logs como uno gestionado, los ajustes que configure varían en función de la ubicación del recolector de logs y si ha implementado Panorama en una configuración de alta disponibilidad (HA):

- **Dedicated Log Collector (Recopilador de logs dedicado)**: al añadir el recolector de logs, al principio no se muestra la pestaña **Interfaces**. Debe introducir el número de serie del recopilador de logs (**Collector S/N [Nº serie del recopilador]**); después, haga clic en **OK (Aceptar)** y edite el recopilador de logs para visualizar la configuración de la interfaz.
- **Default Log Collector that is local to the solitary (non-HA) or active (HA) Panorama management server (Recopilador de logs predeterminado local para el servidor de gestión Panorama solitario [no HA] o activo [HA])**: al introducir el número de serie del servidor de gestión Panorama (**Collector S/N [Nº serie del recopilador]**), el cuadro de diálogo del recopilador solo muestra la configuración de **Disks (Discos)** y **Communication (Comunicación)**, y un subconjunto de ajustes generales (**General**). El recopilador de log deriva sus valores para todos los demás ajustes desde la configuración del servidor de gestión Panorama.
- (Solo HA) **Default Log Collector that is local to the passive Panorama management server (Recopilador de logs local predeterminado para el servidor de gestión Panorama pasivo)**: Panorama trata a este recopilador de logs como remoto, por lo que para configurarlo debe seguir los mismos pasos que en la configuración de un recopilador de logs dedicado.

El procedimiento completo para configurar un recopilador de logs requiere tareas adicionales.

© 2020 Palo Alto Networks, Inc.

¿Qué está buscando?	Consulte:
Identificar el recopilador de logs y definir sus conexiones con el servidor de gestión Panorama y con los servicios externos.	Ajustes del recopilador de logs general
Configure el acceso a el CLI del recopilador de logs.	Configuración de autenticación del CLI del recopilador de logs
Configurar las interfaces que utiliza el recopilador de logs dedicado para el tráfico de gestión, la comunicación del grupo de recopiladores y la recopilación de logs.	Configuración de la interfaz del recopilador de logs
Configure los discos RAID que almacenan los logs recopilados de los cortafuegos.	Configuración del disco RAID del recopilador de logs
Configurar el recopilador de logs para recibir información de asignación de usuarios por parte de los agentes de User-ID.	Configuración del User-ID de usuarios
Configurar el recopilador de logs para autenticarse con agentes de User-ID de Windows.	Seguridad de conexión
Configurar los ajustes de seguridad para comunicarse con Panorama, otros recopiladores de log y cortafuegos.	Configuración de comunicación

Ajustes del recopilador de logs general

- Panorama > Managed Collectors > General

Configure los ajustes como se describe en la siguiente tabla para identificar un recopilador de logs y definir sus conexiones al servidor de gestión de Panorama, los servidores DNS y los servidores NTP.

Configuración general del recopilador de logs	Description (Descripción)
Nº serie del recopilador	(Obligatorio) Introduzca el número de serie del dispositivo Panorama que funciona como recopilador de logs. Si el recopilador de logs es local, introduzca el número de serie del servidor de gestión Panorama.

© 2020 Palo Alto Networks, Inc.

Configuración general del recopilador de logs	Description (Descripción)
Nombre del recopilador	Introduzca un nombre para identificar al recopilador de logs (hasta 31 caracteres). El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos. Este nombre se muestra como el nombre de host del recopilador de logs.
Certificado entrante de Syslog seguro	Seleccione el certificado que debe usar el recopilador gestionado para asimilar de forma segura los logs del servidor Traps ™ ESM. Este certificado se denomina certificado entrante porque Panorama / recopilador gestionado es el servidor al que el Traps ESM (cliente) envía logs; el certificado es necesario si el protocolo de **Transport (Transporte)** para el perfil de ingestión de logs es **SSL**.
Certificado de Syslog seguro	Seleccione un certificado para el reenvío seguro de syslogs a un servidor Syslog externo. El certificado debe tener la opción **Certificate for Secure Syslog (Certificado de Syslog seguro)** seleccionada (consulte Gestión de certificados de cortafuegos y Panorama). Cuando asigna un perfil de servidor Syslog al grupo de recopiladores que incluye este recopilador de logs (consulte Panorama > Collector Groups [Grupos de recopiladores]), **Panorama** > **Collector Groups (Grupos de recopiladores)** > **Collector Log Forwarding (Reenvío de logs del recopilador**), el protocolo de **Transport (Transporte)** del perfil del servidor debe ser **SSL** (consulte Device [Dispositivo] > Server Profiles [Perfiles del servidor] > Syslog).
IP del servidor de Panorama	Especifique la dirección IP del servidor de gestión de Panorama que gestiona este recopilador de logs.
IP del servidor 2 de Panorama	Especifique la dirección IP del peer secundario si el servidor de gestión de Panorama está implementado en una configuración de alta disponibilidad (HA).
Dominio	Introduzca el nombre de dominio del recopilador de logs.
Servidor DNS principal	Introduzca la dirección IP del servidor DNS principal. El recopilador de logs usa este servidor para consultas de DNS (por ejemplo, para encontrar el servidor de gestión de Panorama).
Servidor DNS secundario	(Opcional) Introduzca la dirección IP o el servidor DNS secundario que deberá utilizarse si el servidor principal no está disponible.
Servidor NTP principal	Introduzca la dirección IP o el nombre de host del servidor NTP principal, si lo hubiera. Si no utiliza servidores NTP, puede establecer la hora del recopilador de logs manualmente.
Servidor NTP secundario	(Opcional) Introduzca la dirección IP o el nombre de host de los servidores NTP secundarios que deberán utilizarse si el servidor principal no está disponible.
timezone	Seleccione la zona horaria del recopilador de logs.
Latitud	Introduzca la latitud (de -90.0 a 90.0) del recopilador de logs. Los mapas de tráfico y amenazas usan la latitud de App Scope.

© 2020 Palo Alto Networks, Inc.

Configuración general del recopilador de logs	Description (Descripción)
Longitud	Introduzca la longitud (de -180.0 a 180.0) del recopilador de logs. Los mapas de tráfico y amenazas usan la longitud de App Scope.

Configuración de autenticación del CLI del recopilador de logs

- Panorama > Managed Collectors > Authentication

Un dispositivo serie M en el modo de recopilador de logs (recopilador de logs dedicado) no tiene interfaz web, solo una CLI. Puede usar el servidor de gestión Panorama para configurar la mayor parte de las opciones de un recopilador de logs dedicado, pero algunas de ellas requieren acceso al CLI. Configure los ajustes de autenticación de acceso al CLI que se describen en esta tabla:

Configuración de autenticación del recopilador de logs	Description (Descripción)
Usuarios	Este campo siempre muestra `admin` y se utiliza para el nombre de inicio de sesión del CLI local del recopilador de logs.
Modo	Elija el modo de contraseña en **Mode (Modo)**: • **Password (Contraseña)**: escriba una contraseña en texto sin formato y haga clic en **Confirm Password (Confirmar contraseña)**. • **Password Hash (Contraseña con hash)**: introduzca una cadena de contraseña con hash. Puede serle útil si, por ejemplo, desea volver a usar la contraseña de una cuenta Unix existente, pero no conoce la contraseña de texto sin formato; solo la contraseña con hash. Panorama acepta cualquier cadena de hasta 63 caracteres, independientemente del algoritmo empleado para generar el valor de hash. El comando operativo de la CLI **`request password-hash password`** **<***password***>** emplea el algoritmo MD5. Cuando confirma los cambios, Panorama envía el nuevo valor de hash al recopilador de logs, y la contraseña del administrador será la que especificó en **<***password***>**.
Intentos fallidos	Introduzca el número de intentos fallidos de inicio de sesión que se permiten en la CLI hasta que se bloquea la cuenta de administrador (0 a 10). Un valor 0 significa que el número de intentos es ilimitado. El valor predeterminado es 0 en los recopiladores de logs en modo de operación normal y 10 en los recopiladores de logs en modo FIPS-CC. Al establecer un máximo de intentos de inicio de sesión, contribuye a proteger mejor el recolector de logs frente a los ataques de fuerza bruta. *Si configura cualquier valor distinto de 0 en Failed Attempts (Intentos fallidos), pero deja 0 en Lockout Time (Tiempo de bloqueo), se bloqueado al usuario administrativo por tiempo indefinido hasta que otro administrador lo desbloquee manualmente. Si no ha creado ningún otro administrador, debe volver a configurar los ajustes Failed Attempts (Intentos fallidos)*

© 2020 Palo Alto Networks, Inc.

Configuración de autenticación del recopilador de logs	Description (Descripción)
	y Lockout Time (Tiempo de bloqueo) en Panorama y enviar el cambio en la configuración al recopilador de logs. Para garantizar que nunca se bloquee al administrador, mantenga el valor predeterminado de 0 tanto en Failed Attempts (Intentos fallidos) como en Lockout Time (Tiempo de bloqueo).
Tiempo de bloqueo	Indique los minutos durante los que el recolector de logs bloquea al administrador tras alcanzar el máximo de **Failed Attempts (Intentos fallidos)** (el rango es de 0 a 60 y el valor predeterminado, 0). *Si configura cualquier valor distinto de 0 en Failed Attempts (Intentos fallidos), pero deja 0 en Lockout Time (Tiempo de bloqueo), se bloqueado al usuario administrativo por tiempo indefinido hasta que otro administrador lo desbloquee manualmente. Si no ha creado ningún otro administrador, debe volver a configurar los ajustes Failed Attempts (Intentos fallidos) y Lockout Time (Tiempo de bloqueo) en Panorama y enviar el cambio en la configuración al recopilador de logs. Para garantizar que nunca se bloquee al administrador, mantenga el valor predeterminado de 0 tanto en Failed Attempts (Intentos fallidos) como en Lockout Time (Tiempo de bloqueo).*

Configuración de la interfaz del recopilador de logs

- Panorama > Managed Collectors > Interfaces

Los recopiladores del logs dedicados (dispositivos M-Series en modo de recopilación de logs) utilizan de forma predeterminada la interfaz de gestión (MGT) para el tráfico, la recopilación de logs y la comunicación con el grupo de recopiladores. Sin embargo, Palo Alto Networks recomienda asignar interfaces separadas para la recopilación de logs y la comunicación con el grupo de recopiladores para reducir el tráfico en la interfaz MGT. Puede mejorar la seguridad si define una subred aparte para la interfaz MGT que sea más privada que las subredes del resto de interfaces. Para utilizar interfaces distintas, primero debe configurarlas en el servidor de gestión Panorama (consulte Device > Setup > Management). Las interfaces disponibles para la recopilación de logs y la comunicación con el grupo de recopiladores varían según el modelo de dispositivo de recopilación de logs. Por ejemplo, el dispositivo M-500 tiene las siguientes interfaces: Ethernet1 (1 Gbps), Ethernet2 (1 Gbps), Ethernet3 (1 Gbps), Ethernet4 (10 Gbps) Ethernet5 (10 Gbps)

Para configurar una interfaz, seleccione el enlace y realice los ajustes como se describe en la siguiente tabla.

Debe especificar la dirección IP, la máscara de red (para IPv4) o la longitud del prefijo (para IPv6) y la puerta de enlace predeterminada para acabar de configurar la interfaz de la interfaz MGT. Si confirma una configuración parcial (por ejemplo, podría omitir la puerta de enlace predeterminada), solo puede acceder al cortafuegos o Panorama a través del puerto de la consola para futuros cambios de configuración.

Compile siempre una configuración completa de la interfaz MGT. No puede compilar las configuraciones de otras interfaces a no ser que especifique la dirección IP, la máscara de red (para IPv4) o la longitud del prefijo (para IPv6) y la puerta de enlace predeterminada.

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz del recopilador de logs	Description (Descripción)
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Debe habilitar una interfaz para configurarla. Excepto la interfaz MGT, habilitada de forma predeterminada.
Velocidad y dúplex	Configure una tasa de datos y una opción de dúplex para la interfaz. Las opciones incluyen 10 Mbps, 100 Mbps,1 Gbps y 10Gbps (solo en Eth4 y Eth5) con dúplex completo o medio. Utilice el ajuste **auto-negotiate (negociación automática)** predeterminado para que el recopilador de logs determine la velocidad de interfaz. *Este ajuste debe coincidir con la configuración de la interfaz del equipo de red vecino.*
Dirección IP (IPv4)	Si su red utiliza IPv4, asigne una dirección IPv4 a la interfaz.
Máscara de red (IPv4)	Si ha asignado una dirección IPv4 a la interfaz, debe introducir también una máscara de red (por ejemplo, 255.255.255.0).
Default Gateway (IPv4)	Si ha asignado una dirección IPv4 a la interfaz, también debe asignar una dirección IPv4 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz MGT).
Dirección IPv6/ longitud de prefijo	Si su red utiliza IPv6, asigne una dirección IPv6 a la interfaz. Para indicar la máscara de red, introduzca una longitud de prefijo IPv6 (por ejemplo, 2001:400:f00::1/64).
Puerta de enlace IPv6 predeterminada	Si ha asignado una dirección IPv6 a la interfaz, también debe asignar una dirección IPv6 a la puerta de enlace predeterminada (la puerta de enlace debe estar en la misma subred que la interfaz).
MTU	Introduzca la unidad máxima de transmisión (MTU, por sus siglas en inglés) en bytes para los paquetes enviados en esta interfaz (el intervalo es de 576 a 1500 y el valor predeterminado, 1500).
Recopilación de logs del dispositivo	Habilite la interfaz para que recopile logs del cortafuegos. En una implementación con mucho tráfico de logs, puede habilitar múltiples interfaces para realizar esta función. Esta función está habilitada de forma predeterminada en la interfaz MGT.
Comunicación del grupo de recopiladores	Habilite la interfaz para la comunicación del grupo de recopiladores. Esta función solo la puede realizar una interfaz (la MGT de forma predeterminada).
Servicios de conectividad de red	El servicio **Ping** está disponible en cualquier interfaz y le permite probar la conectividad entre la interfaz del recopilador de logs y los servicios externos. Los siguientes servicios solo están disponibles en la interfaz MGT: • **SSH**: permite el acceso seguro a la CLI de Panorama. • **SNMP**: permite a la interfaz recibir consultas de estadísticas desde un gestor SNMP. Para obtener más información, consulte Habilitación de supervisión de SNMP.

© 2020 Palo Alto Networks, Inc.

Configuración de la interfaz del recopilador de logs	Description (Descripción)
	• **User-ID (ID de usuario)**: permite al recopilador de logs redistribuir la información de asignación de usuarios que recibe de los agentes de User-ID.
Direcciones IP permitidas	Introduzca las direcciones IP de los sistemas cliente que pueden acceder al recopilador de logs mediante esta interfaz. Una lista vacía de forma predeterminada especifica que el acceso está disponible en cualquier sistema cliente. *Palo Alto Networks recomienda no dejar esta lista en blanco. Especifique los sistemas cliente de los administradores de Panorama para evitar accesos no autorizados.*

Configuración del disco RAID del recopilador de logs

- Panorama > Managed Collectors > Disks

Tras configurar los discos de logs en el dispositivo M-Series o el dispositivo virtual Panorama, puede hacer clic en **Add (Añadir)** para añadirlos a la configuración del recopilador de logs.

De forma predeterminada, los dispositivos M-Series están equipados con el primer par de RAID 1 instalado en las bahías A1 y A2. En el software, el par de discos de las bahías A1 y A2 se denomina Disk Pair A (Par de discos A). El resto de bahías se nombran de forma secuencial: Disk Pair B, Disk Pair C, etc. Por ejemplo, el dispositivo M-500 admite hasta 12 pares de discos. Puede instalar pares de discos de 2 TB o 1 TB en el mismo dispositivo. Sin embargo, el tamaño del disco de las dos unidades de cada par debe ser el mismo.

El dispositivo virtual Panorama admite hasta 12 discos virtuales de logs para ofrecer una capacidad de almacenamiento de 24 TB.

Tras añadir pares de discos, el recopilador de logs redistribuye los logs existentes por todos los discos, lo que puede tardar varias horas por cada terabyte de logs. Durante el proceso de redistribución, se reduce la tasa máxima de ingestión de logs. En la página **Panorama** > **Managed Collectors (Recopiladores gestionados)**, la columna Log Redistribution State (Estado de redistribución de logs) indica el progreso con un porcentaje.

Si utiliza un gestor SNMP para supervisar de forma centralizada, podrá ver las estadísticas de logs en el MIB de panLogCollector.

Configuración del User-ID de usuarios

- Panorama> Managed Collectors> User-ID Agents

Un recopilador de logs dedicado puede recibir asignaciones de usuario de hasta 100 agentes de User-ID. Los agentes pueden ser agentes User-ID integrados de PAN-OS que se ejecutan en cortafuegos o agentes User-ID basados en Windows. En un cortafuegos con varios sistemas virtuales, cada sistema virtual puede servir como agente de User-ID independiente. El recopilador de logs puede entonces redistribuir las asignaciones de usuario a cortafuegos o al servidor de administración Panorama.

Los procedimientos completos para configurar la asignación de usuarios y habilitar la redistribución para la asignación de usuarios requieren tareas adicionales además de la conexión a agentes de User-ID.

© 2020 Palo Alto Networks, Inc.

Para configurar un recopilador de logs dedicado para conectarse a un agente de User-ID, haga clic en **Add (Añadir)** para añadir uno y configure los ajustes como se describe en la siguiente tabla.

Configuración del User-ID de usuarios	Description (Descripción)
Nombre	Introduzca un nombre (hasta 31 caracteres) para identificar al agente de User-ID. El nombre distingue entre mayúsculas y minúsculas, debe ser único y puede incluir sólo letras, números, espacios, guiones y guiones bajos. *Con un cortafuegos que actúe como agente de User-ID, este campo no tiene que coincidir con el campo* Nombre del recopilador*.*
Host	• **Windows-based User-ID agent (Agente de User-ID basado en Windows)**: introduzca la dirección IP del host de Windows en el que está instalado el agente de User-ID. • **Firewall (PAN-OS integrated User-ID agent) (Cortafuegos (agente integrado de usuario de PAN-OS))**: introduzca el nombre de host o la dirección IP de la interfaz que el cortafuegos utiliza para redistribuir las asignaciones de usuario.
Puerto	Introduzca el número de puerto en el que el agente User-ID escuchará solicitudes User-ID. El predeterminado es 5007, pero puede especificar cualquier puerto disponible. Los diferentes gentes User-ID pueden usar diferentes puertos. *Algunas versiones anteriores del agente de User-ID utilizan 2010 como puerto predeterminado.*
Nombre del recopilador	El recopilador al que se refieren estos campos es el agente de User-ID, no el Recopilador de logs. Los campos se aplican sólo si el agente es un cortafuegos o un sistema virtual que redistribuya las asignaciones de usuario al Recopilador de logs. Introducir el **Collector Name (Nombre del recopilador)** y la **Pre-Shared Key (Clave precompartida)** que identifican al cortafuegos o sistema virtual como agente de User-ID. Debe introducir los mismos valores que cuando configuró el cortafuegos o el sistema virtual para servir como agente de User-ID (consulte Redistribución).
Clave precompartida del recopilador / Confirmar clave precompartida del recopilador	
Habilitado	Seleccione esta opción para habilitar el Recopilador de logs y que pueda comunicarse con el agente de User-ID.

Seguridad de conexión

- Panorama > Recopiladores gestionados > Seguridad de conexión

Para configurar un perfil de certificado utilizado por el recopilador de logs para validar el certificado presentado por los agentes de User-ID de Windows. El recopilador de logs utiliza el perfil de certificado seleccionado para verificar la identidad del agente de User-ID mediante la validación del certificado de servidor presentado por el agente.

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
Perfil de certificado de User-ID	En el menú desplegable, seleccione el perfil de certificado utilizado para autenticarse con los agentes de User-ID de Windows o seleccione Nuevo perfil de certificado para crear uno. Seleccione Ninguno para quitar el perfil de certificado.

Configuración de comunicación

- Panorama > Managed Collectors > Communication

Para configurar la autenticación personalizada basada en certificados entre los recopiladores de logs y Panorama, los cortafuegos y otros recopiladores de logs, configure los ajustes como se describe en la siguiente tabla.

Configuración de comunicación	Description (Descripción)
Comunicación de servidor segura: Al habilitar la **Secure Server Communication (Comunicación del servidor segura)** valida la identidad de los dispositivos cliente que se conectan al recopilador de logs.	
Perfil de servicio SSL/TLS	Seleccione un perfil de servicio SSL / TLS en el menú desplegable. Este perfil define el certificado que presenta el recopilador de logs y especifica el rango de versiones SSL / TLS aceptables para la comunicación con el recopilador de logs.
Perfil del certificado	Seleccione un perfil de certificado en el menú desplegable. Este perfil de certificado define la conducta de la comprobación de revocación de certificados y la CA raíz utilizada para autenticar la cadena de certificados presentada por el cliente.
Certificado personalizado únicamente	Cuando está habilitado, el recopilador de logs solo acepta certificados personalizados para la autenticación con cortafuegos gestionados y recopiladores de logs.
Autorizar clientes según el número de serie	El recopilador de logs autoriza a los dispositivos cliente según el uso de un hash de su número de serie.
Comprobar lista de autorización	Los dispositivos cliente o grupos de dispositivos que se conectan a este recopilador de logs se comprueban en la lista de autorización.
Tiempo de espera de desconexión (min)	La cantidad de tiempo que el recopilador de logs espera antes de romper la conexión actual con sus dispositivos gestionados. El recopilador de logs vuelve a establecer conexiones con sus dispositivos gestionados utilizando la configuración de comunicaciones de servidor seguro configurada. El tiempo de espera comienza después de que se haya confirmado la configuración de comunicaciones del servidor seguro.
Authorization List	**Authorization List (Lista de autorización)**: Seleccione Añadir y complete los siguientes campos para establecer criterios. • **Identifier (Identificador)**: seleccione **Subject (Asunto)** o **Subject Alt. (Asunto Alt.) Name (Nombre)** como el identificador de autorización.

© 2020 Palo Alto Networks, Inc.

Configuración de comunicación	Description (Descripción)
	• **Type (Tipo)**: Si Asunto Alt. Nombre seleccionado como Identificador, seleccione **IP**, **hostname (nombre de host)** o **e-mail (correo electrónico)** como el tipo del identificador. Si se selecciona Asunto, se utiliza nombre común como el tipo de identificador. • **Value (Valor)**: introduzca el valor del identificador.
Secure Client Communication (Comunicación de cliente segura): La habilitación de **Secure Client Communication (Comunicación de cliente segura)** garantiza que el certificado de cliente especificado se utiliza para autenticar el recopilador de logs en las conexiones SSL con Panorama, cortafuegos u otros recopiladores de logs.	
Tipo de certificado	Seleccione el tipo de certificado de dispositivo (Ninguno, Local o SCEP) utilizado para asegurar la comunicación
ninguno	Si selecciona **None (Ninguno)**, no se ha configurado ningún certificado de dispositivo y no se utiliza la comunicación de cliente segura. Es el valor predeterminado.
Local	El recopilador de logs utiliza un certificado de dispositivo local y la clave privada correspondiente generada en el recopilador de logs o uno importado de un servidor PKI de empresa existente.
	Certificado: Seleccione el certificado del dispositivo local. Este certificado puede ser exclusivo para el cortafuegos (basado en un hash del número de serie del recopilador de logs) o un certificado de dispositivo común utilizado por recopiladores de logs que se conectan a Panorama.
	Perfil de certificado: Seleccione el perfil de certificado del menú desplegable. Este perfil de certificado se utiliza para definir la autenticación del servidor con el recopilador de logs.
SCEP	El recopilador de logs utiliza un certificado de dispositivo y la clave privada generada por el servidor de protocolo de inscripción de certificados simple (SCEP).
	Perfil de SCEP: Seleccione un perfil de SCEP del menú desplegable.
	Perfil de certificado: Seleccione el perfil de certificado del menú desplegable. Este perfil de certificado se utiliza para definir la autenticación del servidor con el recopilador de logs.
Comprobar identidad de servidor	El dispositivo cliente confirma la identidad del servidor haciendo coincidir el nombre común (CN) con la dirección IP o FQDN del servidor.

Actualizaciones de software para recopiladores de logs dedicados

- Panorama > Recopiladores gestionados

Para instalar una imagen de software en un dispositivo serie M en modo de recopilador de logs, descargue o cargue la imagen en Panorama (consulte Panorama > Device Deployment), haga clic en **Install (Instalar)** y complete los siguientes campos:

© 2020 Palo Alto Networks, Inc.

Dado que el servidor de gestión de Panorama comparte su sistema operativo con el recopilador de logs predeterminado local, actualiza ambos al instalar una actualización de software en el servidor de gestión de Panorama (consulte Panorama> Software).

Para Recopiladores de logs dedicados, también puede seleccionar Panorama > Device Deployment (Implementación de dispositivos) > Software para instalar actualizaciones (consulte Gestión de software y actualizaciones de contenido).

Para reducir el tráfico en la interfaz de gestión (MGT), puede configurar Panorama para utilizar una interfaz independiente para implementar actualizaciones (consulte Panorama > Setup > Interfaces).

Campos para la instalación de una actualización de software en un recopilador de logs	Description (Descripción)
Archivo	Seleccione una imagen de software descargada o cargada.
Dispositivos	Seleccione los recopiladores de logs en los que instalará el software. El diálogo muestra la siguiente información para cada recopilador de logs: • **Nombre de dispositivo**: el nombre del recopilador de logs dedicado. • **Versión actual**: la versión de software de Panorama actualmente instalada en el recopilador de logs. • **Estado de HA**: esta columna no se aplica a los recopiladores de logs. Los recopiladores de logs dedicados no admiten la alta disponibilidad.
Filtro seleccionado	Para mostrar solo recopiladores de logs específicos, seleccione los recopiladores de logs y luego **Filter Selected**.
Upload only to device (Cargar solamente en el dispositivo) (no instalar)	Seleccione para cargar el software al recopilador de logs sin reiniciarlo automáticamente. La imagen no se instala hasta que reinicie manualmente iniciando sesión en el CLI del recopilador de logs y ejecutando el comando operativo **`request restart system`**.
Reboot device after Install (Reiniciar dispositivo tras la instalación)	Seleccione cargar e instalar el software automáticamente. El proceso de instalación reinicia el recopilador de logs.

© 2020 Palo Alto Networks, Inc.

Panorama > Grupos de recopiladores

Cada grupo de recopiladores puede tener hasta 16 recopiladores de logs, a los cuales asigna cortafuegos para reenviar logs. Puede usar Panorama para solicitar a los recopiladores de logs la investigación y visualización de logs añadidos.

El grupo de recopiladores predefinido que se especifica como predeterminado contiene el recopilador de logs predefinido que es local para el servidor de gestión Panorama.

- Configuración del grupo de recopiladores
- Información del grupo de recopiladores

Configuración del grupo de recopiladores

Para configurar un grupo de recopiladores, haga clic en **Add (Añadir)** y complete los siguientes campos.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
Nombre	**Panorama** > **Collector Groups (Grupos de recopiladores)** > **General (General)**	Introduzca un nombre para identificar este Grupo de recopiladores (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, espacios, guiones y guiones bajos.
Almacenamiento de logs		Indica la cuota total de almacenamiento para los logs del cortafuegos que recibe el Grupo de recopiladores y el espacio disponible. Haga clic en el enlace de cuota de almacenamiento **Quota(%) [Cuota(%)]** para configurar el almacenamiento y el período de vencimiento (**Max Days (Días Máx.)**) para los siguientes tipos de log: • **Detailed Firewall Logs (Logs del cortafuegos detallados)**: incluye todos los tipos de logs en **Device (Dispositivo)** > **Setup (Configuración)** > **Logging and Reporting Settings (Configuración de logging e informes)**; por ejemplo, tráfico, amenaza, coincidencia HIP, direcciones IP registradas dinámicamente (etiqueta IP), PCAP extendidas, GTP y túnel, estadísticas de la aplicación, etc. • **Summary Firewall Logs (Resumen de los logs del cortafuegos)**: incluye todos los logs de resumen incluidos en **Device (Dispositivo)** > **Setup (Configuración)** > **Logging and Reporting Settings (Configuración de logging e informes)**; por ejemplo, resumen de tráfico, resumen de amenazas, resumen de URL, y resumen de GTP y túnel.

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
		• **Infrastructure and Audit Logs (Logs de infraestructura y auditoría)**:Incluye los logs de configuración, sistema, user-ID y autenticación. • **Palo Alto Networks Platform Logs (Logs de plataforma de Palo Alto Networks)**: ncluye logs de Traps y otros productos de Palo Alto Networks. • **3rd Party External Logs (Logs externos de terceros)**: Incluye logs de integraciones de otros proveedores proporcionados por Palo Alto Networks. Para usar la configuración predeterminada, haga clic en **Restore Defaults (Restablecer valores predeterminados)**.
Mín. de período de retención (días)		Introduzca el periodo de retención de logs mínimo en días (1-2.000) que Panorama mantiene en todos los recopiladores de logs en el grupo de recopiladores. Si la fecha actual menos la fecha de log más antigua es un valor inferior al periodo mínimo de retención definido, Panorama genera un log del sistema como una violación de la alerta.
Miembros de grupo de recopiladores		**Add (Añadir)** los recopiladores de logs que formarán parte de este Grupo de recopiladores (hasta 16). Puede añadir todos los Recopiladores de logs disponibles en la página **Panorama** > **Managed Collectors (Recopiladores gestionados)**. Todos los recopiladores de logs de un grupo de recopiladores en particular deben ser del mismo modelo: por ejemplo, todos los dispositivos M-500 o todos los dispositivos virtuales de Panorama. *Tras añadir recopiladores de logs a un grupo de recopiladores existente, Panorama redistribuye los logs existentes por todos los recopiladores de logs, lo que puede tardar varias horas por cada terabyte de logs. Durante el proceso de redistribución, se reduce la tasa máxima de logs. En la página Panorama > Collector Groups (Grupos de recopiladores), la columna Estado de redistribución de logs indica el estado de finalización del proceso con un porcentaje.*
Habilitar recopiladores en todas las redundancias de logs		Si selecciona esta opción, habrá dos copias de cada log en el grupo de recopiladores y cada copia residirá en un recopilador de logs distinto. Esta redundancia garantiza que si cualquiera de los recopiladores de logs deja de estar disponible, no se pierden los logs: puede ver todos

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
		los logs reenviados al grupo de recopiladores y ejecutar informes para todos los datos de logs. La redundancia de logs está disponible solo si el grupo de recopiladores tiene varios recopiladores de logs y cada recopilador de logs tiene el mismo número de discos. Tras habilitar la redundancia, Panorama redistribuye los logs existentes por todos los recopiladores de logs, lo que puede tardar varias horas por cada terabyte de logs. Durante el proceso de redistribución, se reduce la tasa máxima de logs. En la página **Panorama** > **Collector Groups (Grupos de recopiladores)**, la columna Estado de redistribución de logs indica el estado de finalización del proceso con un porcentaje. Todos los recopiladores de logs de un grupo de recopiladores en particular deben ser del mismo modelo: por ejemplo, todos los dispositivos M-500 o todos los dispositivos virtuales de Panorama. *Al habilitar la redundancia se crean más logs, por lo que esta configuración requiere más capacidad de almacenamiento. Al habilitar la redundancia se dobla el tráfico de procesamiento de logs en un grupo de recopiladores, que reduce su tasa de logs máxima a la mitad, ya que cada recopilador de logs debe distribuir una copia de cada log que reciba. (Si un grupo de recopiladores se queda sin espacio, elimina logs antiguos).*
Reenviar a todos los recopiladores de la lista de preferencias		(Solo los cortafuegos de las series PA-5200 y PA-7000) Seleccione para enviar logs a cada Recopilador de logs en la lista de preferencias. Panorama utiliza el equilibrio de carga por turnos para seleccionar qué Recopilador de logs recibe los logs en un momento dado. Esto está deshabilitado de forma predeterminada: los cortafuegos envían logs solo al primer Recopilador de logs de la lista, a menos que el Recopilador de logs deje de estar disponible (consulte Devices / Collectors).
Enable Secure Inter LC Communication (Habilitar comunicación segura entre LC)		Habilita el uso de certificados personalizados para la autenticación mutua de SSL entre recopiladores de logs en un grupo de recopiladores.

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
Ubicación	**Panorama** > **Collector Groups (Grupos de recopiladores)** > **Monitoring (Supervisión)**	Especifique la ubicación del Grupo de recopiladores.
Contacto		Especifique el contacto de correo electrónico (por ejemplo, la dirección de correo electrónico del administrador de SNMP que supervisará los recopiladores de logs).
versión		Especifique la versión SNMP para la comunicación con el servidor de gestión de Panorama: **V2c** o **V3**. SNMP le permite recopilar información sobre los recopiladores de logs, entre lo que se incluye estado de conexión, estadísticas sobre unidades de disco, versión de software, uso promedio de CPU, logs/segundo promedio y duración de almacenamiento por tipo de base de datos. La información de SNMP está disponible en cada grupo de recopiladores.
Cadena de comunidad de SNMP (solo V2c)		Introduzca la cadena de comunidad en **SNMP Community String (Cadena de comunidad de SNMP)**, la cual identifica una comunidad de gestores SNMP y dispositivos supervisados (recopiladores de logs, en este caso), y sirve como contraseña para autenticar a los miembros de la comunidad entre sí. *No utilice la cadena de comunidad predeterminada public; es muy conocida y, por lo tanto, no es segura.*
Vistas (solo V3)		**Add (Añada)** un grupo de vistas de SNMP y, en **Views (Vistas)**, ingrese el nombre del grupo. Cada vista es un Identificador de objeto (object identifier, OID) emparejado y una máscara binaria: el OID especifica una base de información gestionada (managed information base, MIB) y la máscara (en formato hexadecimal) especifica qué objetos SNMP son accesibles dentro (incluir coincidencias) o fuera (excluir coincidencias) del MIB. Para cada vista del grupo, haga clic en **Add (Añadir)** la siguiente configuración: • **View (Vista)**: especifique un nombre para una vista. • **OID**: introduzca el OID. • **Option (Opción)** (incluir o excluir): seleccione si la vista excluirá o incluirá el OID. • **Mask (Máscara)**: Especifique un valor de máscara para un filtro del OID (por ejemplo, 0xf0).

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
Usuario (V3 solamente)		Haga clic en **Add (Añadir)** la siguiente configuración para cada usuario de SNMP: • **Users (Usuarios)**: Introduzca un nombre de usuario para autenticar al usuario para el gestor de SNMP. • **View (Vista)**: Seleccione un grupo de vistas del usuario. • **Authpwd**: Introduzca una contraseña para autenticar al usuario para el gestor de SNMP (de ocho caracteres mínimo). Solo el algoritmo de hash seguro (Secure Hash Algorithm, SHA) es compatible para el cifrado de la contraseña. • **Prvpwd**: Introduzca una contraseña de privacidad para cifrar mensajes SNMP para el gestor de SNMP (de ocho caracteres mínimo). Únicamente se admite el estándar de cifrado avanzado (AES).
Dispositivos / Recopiladores	**Panorama** > **Collector Groups (Grupos de recopiladores)** > **Device Log Forwarding (Reenvío de logs del dispositivo)**	La lista de preferencias de reenvío de logs controla qué cortafuegos envían los logs a qué recopiladores de logs. Para cada entrada que **Add (Añada)** a la lista, **Modify (Modifique)** la lista de Dispositivos para asignar uno o más cortafuegos y **Add (Añada)** uno o más recopiladores de logs en la lista de recopiladores. De manera predeterminada, los cortafuegos que asigna en una entrada de lista enviarán logs solo al recopilador de logs principal (primero) siempre y cuando esté disponible. Si el recopilador principal falla, los cortafuegos envían los logs al recopilador de logs secundario. Si el secundario falla, los cortafuegos envían los logs al recopilador terciario, y así sucesivamente. Para cambiar el orden, seleccione un recopilador de logs y haga clic en**Move Up (Mover hacia arriba)** o **Move Down (Mover hacia abajo)**. *Puede anular el comportamiento predeterminado de reenvío de registros para los cortafuegos de las series PA-5200 y PA-7000 seleccionando* Reenviar a todos los recopiladores de la lista de preferencias *en la pestaña General.*
Sistema Configuración Coincidencia HIP	**Panorama** > **Collector Groups (Grupos de recopiladores)** > **Collector Log Forwarding (Reenvío de logs del recopilador)**	Para cada tipo de log del cortafuegos que desee reenviar desde este grupo de recopiladores a servicios externos, debe**Add (Añadir)** uno o más perfiles de la lista de coincidencias. Los perfiles especifican qué logs se deben reenviar y los servidores de destino. En cada perfil, complete lo siguiente:

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)

Tráfico
threat
WildFire
Correlación
GTP
Autenticación
User-ID
Túnel
Etiqueta IP
		• **Name (Nombre)**: Introduzca un nombre de hasta 31 caracteres para identificar el perfil de la lista de coincidencias.
		• **Filter (Filtrar)**: de manera predeterminada, el cortafuegos envía **All logs (Todos los logs)** del tipo al que se este perfil de lista de coincidencias pertenece. Para enviar un subconjunto de logs, seleccione un filtro existente o seleccione el **Filter Builder (Generador de filtros)** para añadir un nuevo filtro. En cada nueva aplicación de filtro, especifique los siguientes campos y haga clic en **Add (Añadir)** para incluir la consulta:
		  • **Connector (Conector)**: Seleccione la lógica del conector (y/o). Seleccione **Negate (Negar)** si desea aplicar la negación. Por ejemplo, para evitar el reenvío de logs desde una zona no fiable, seleccione **Negate (Negar)**, **Zone (Zona)** como atributo, **equal (igual)** como operador e introduzca el nombre de la zona no fiable en la columna Value (Valor).
		  • **Attribute (Atributo)**: seleccione un atributo de log. Las opciones varían según el tipo de log.
		  • **Operator (Operador)**: Seleccione el criterio para determinar cómo se aplica el atributo (por ejemplo **equal [igual]**).. Las opciones varían según el tipo de log.
		  • **Value (Valor)**: Especifique el valor del atributo para coincidir.
		Para ver o exportar los logs que coinciden con el filtro, seleccione **View Filtered Logs (Ver logs filtrados)**. Esta pestaña ofrece las mismas opciones que las páginas de la pestaña **Monitoring** (Supervisión) (como **Monitoring [Supervisión]** > **Logs [Logs]** > **Traffic [Tráfico]**).
		• **Description (Descripción)**: Introduzca una descripción de hasta 1.023 caracteres para explicar el propósito de este perfil de lista de coincidencias.
		• Servidores de destino: Para cada tipo de servidor, debe **Add (Añadir)** uno o más perfiles de servidor. Para configurar los perfiles del servidor, consulte Device > Server Profiles > SNMP Trap, Device > Server Profiles > Syslog, Device > Server Profiles > Email o Device > Server Profiles > HTTP.
		• Acciones integradas: Puede **Add (Añadir)** acciones para todos los tipos de logs excepto los logs de sistema y de configuración:
		  • Introduzca un nombre descriptivo para la **Action (Acción)**.

© 2020 Palo Alto Networks, Inc.

Configuración de grupos de recopiladores	Configurado en	Description (Descripción)
		• Seleccione la dirección IP que desea etiquetar: **Source Address (Dirección de origen)** o **Destination Address (Dirección de destino)**. Solo puede etiquetar la dirección IP de origen en los logs de correlación y en los logs de coincidencias HIP. • Seleccione la acción: **Add Tag (Añadir etiqueta)** o **Remove Tag (Eliminar etiqueta)**. • Seleccione si desea registrar la etiqueta con el agente de User-ID local en este Panorama o con un agente de User-ID remoto. Para registrar etiquetas con un **Remote device User-ID Agent (Agente User-ID de dispositivo remoto)**, seleccione el perfil de servidor HTTP que habilitará el reenvío. • Configure la opción **Timeout (Tiempo de espera)** de la etiqueta IP para configurar, en minutos, el tiempo durante el que se mantendrá la asignación de dirección IP a etiqueta. Una configuración de tiempo de espera en 0 significa que el tiempo de espera de la asignación de la etiqueta IP no se agotará (el intervalo es de 0 a 43 200 [30 días]; el valor predeterminado es 0). *Solo puede configurar un tiempo de espera con la acción Add Tag (Añadir etiqueta).* • Introduzca o seleccione las **Tags (Etiquetas)** que desea aplicar o quitar de la dirección IP objetivo de origen o de destino.
Perfil de ingestión	**Panorama** > **Collector Groups (Grupos de recopiladores)** > **Log Ingestion (Ingestión de logs)**	Seleccione **Add (Añadir)** uno o más perfiles de ingestión de logs que permitan que Panorama reciba logs del servidor ESM de Traps. Para configurar un nuevo perfil de ingestión de log, consulte Panorama > Log Ingestion Profile.

Información del grupo de recopiladores

Seleccione **Panorama** > **Collector Groups (Grupos de recopiladores)** para mostrar la siguiente información para los grupos de recopiladores. Los campos adicionales son configurables después de completar la Configuración del recopilador de logs.

© 2020 Palo Alto Networks, Inc.

Información del grupo de recopiladores	Description (Descripción)
Nombre	Un nombre que identifica el grupo de recopiladores.
Redundancia habilitada	Indica si la redundancia de logs está habilitada para el grupo de recopiladores. Puede habilitar la redundancia de log para un grupo de recopiladores una vez haya completado o modificado la Configuración del recopilador de logs.
Recopiladores	Los recopiladores de logs asignados al grupo de recopiladores.
Estado de redistribución de logs	Ciertas acciones (por ejemplo, habilitar la redundancia de logs) provocarán que el grupo de recopiladores redistribuya los logs entre los recopiladores de logs. Esta columna indica el estado de finalización del proceso de redistribución como un porcentaje.

© 2020 Palo Alto Networks, Inc.

Panorama> Complementos

- **Panorama** > **Plugins (Complementos)**
- **Device (Dispositivo)** > **Plugins (Complementos)**

Seleccione **Panorama** > **Plugins (Complementos)** para instalar, eliminar y gestionar los complementos que admiten la integración con terceros en Panorama.

(Solo disponible en los cortafuegos VM-Series) Seleccione **Dispositivo** > **Complementos** para instalar, eliminar y gestionar los complementos de los cortafuegos VM-Series.

Complementos	Description (Descripción)
Carga	Le permite cargar un archivo de instalación de complemento desde un directorio local. Esta acción no instala el complemento. Después de cargar el archivo de instalación, se activa el enlace Install.
Nombre de archivo	El nombre de archivo del complemento. Cuando instala el complemento **vm_series** en Panorama, la página **Device (Dispositivo)** > **VM-Series (Serie VM)** comienza a estar disponible para la gestión y confirmación de configuraciones de plantilla en los cortafuegos de la serie VM implementados en entornos de nube pública: AWS, Azure y Google.
versión	El número de versión del complemento.
Zero Trust	Los modelos compatibles con el complemento.
Release date (Fecha de versión)	La fecha de versión del complemento.
Tamaño	El tamaño de archivo del complemento.
Instalada	Proporciona el estado de instalación actual de cada complemento en Panorama.
Acciones	• **Install (Instalar)**: instala la versión especificada del complemento. La instalación de una nueva versión del complemento sobrescribe la versión instalada anteriormente. • **Delete (Borrar)**: elimina el archivo de complemento especificado. • **Remove Config (Eliminar configuración)**: borra todos los ajustes relacionados con el complemento. • **Uninstall (Desinstalar)**: elimina la instalación actual del complemento. Esta acción no borra el archivo de complemento de Panorama. Si desinstala el complemento, perderá cualquier configuración relacionada con este. Use la desinstalación solo cuando vaya a eliminar completamente la configuración relacionada.

© 2020 Palo Alto Networks, Inc.

Panorama > VMware NSX

Para automatizar el aprovisionamiento del cortafuegos VM-Series edición NSX, debe habilitar la comunicación entre NSX Manager y Panorama. Cuando Panorama registre el cortafuegos VM-Series como servicio en NSX Manager, este pasará a tener la configuración necesaria para abastecer una o más instancias de los cortafuegos VM-Series en cada host ESXi del clúster.

¿Qué desea saber?	Consulte:
¿Cómo se configura un grupo de notificación?	Configuración de una notificación a grupo
¿Cómo defino la configuración para el cortafuegos VM-Series edición NSX?	Creación de definiciones de servicio
¿Cómo configuro Panorama para que se comunique con NSX Manager?	Configuración de acceso al NSX Manager
¿Cómo defino las reglas de dirección para el cortafuegos VM-Series edición NSX?	Creación de reglas de dirección
¿Cómo configuro el cortafuegos para que ejecute la política de manera consistente en el entorno vSphere dinámico?	Seleccione Objects > Address Groups y Policies > Security Para permitir que Panorama y los cortafuegos reconozcan los cambios en el entorno virtual, use los grupos de direcciones dinámicas como objetos de dirección de origen y destino en las reglas previas de la política de seguridad.
¿Busca más información?	Consulte Configuración del cortafuegos VM-Series edición NSX

Configuración de una notificación a grupo

- Panorama > Notify Group

La siguiente tabla describe los ajustes de grupo de notificación de Panorama.

Ajustes de grupo de notificación	Description (Descripción)
Nombre	Introduzca un nombre descriptivo para el grupo de notificación.
Notify Device	Seleccione las casillas de los grupos de dispositivos a los que se debe notificar si se producen adiciones o modificaciones en las máquinas virtuales implementadas en la red. Conforme se abastecen las nuevas máquinas virtuales o se modifican las máquinas existentes, los cambios en la red virtual se aplican en forma de actualizaciones en Panorama. Cuando se configura de esta manera, Panorama completa y actualiza los objetos de direcciones dinámicas a los que se hace

© 2020 Palo Alto Networks, Inc.

Ajustes de grupo de notificación	Description (Descripción)
	referencia en las reglas de política, de manera que los cortafuegos en los grupos de dispositivos especificados reciban los cambios en las direcciones IP registradas en los grupos de direcciones dinámicas. Para habilitar las notificaciones, asegúrese de seleccionar cada grupo de dispositivos en el cual desee habilitar las notificaciones. Si no puede seleccionar un grupo de dispositivos (no está disponible la casilla de verificación), esto significa que el grupo de dispositivos está automáticamente incluido en virtud de la jerarquía del grupo de dispositivos. Este proceso de notificación crea visibilidad de contexto y mantiene la seguridad de la aplicación en la red. Si, por ejemplo, tiene un grupo de cortafuegos de perímetro basados en hardware que deben ser notificados cuando se implementa una nueva aplicación o servidor web, este proceso inicia una actualización automática de los grupos de direcciones dinámicas para el grupo de dispositivos especificado. Y todas las reglas de políticas que hacen referencia al objeto de dirección dinámica ahora incluyen automáticamente cualquier aplicación o servidores web recientemente modificados o implementados y se puede habilitar con seguridad basándose en sus criterios.

Creación de definiciones de servicio

- Panorama > VMware NSX > Service Definitions

Una definición de servicio le permite registrar el cortafuegos VM-Series como servicio de seguridad asociado en NSX Manager. Puede establecer hasta 32 definiciones de servicio en Panorama y sincronizarlas en NSX Manager.

En general, creará una definición de servicio para cada inquilino en un clúster ESXi. Cada definición de servicio especifica el OVF (versión PAN-OS) utilizado para implementar el cortafuegos e incluye la configuración de los cortafuegos VM-Series instalados en el clúster ESXi. Para especificar la configuración, una definición de servicio debe tener una plantilla única, un grupo de dispositivos único y los códigos de autorización de licencia para los cortafuegos que se implementarán usando la definición de servicio. Cuando el cortafuegos se implementa, se conecta a Panorama y recibe sus opciones de configuración (incluidas las zonas de cada inquilino o departamento que el cortafuegos asegurará) y su configuración de política del grupo de dispositivos especificado en la definición de servicio.

Para añadir una nueva definición de servicio, configure los ajustes según se describen en la siguiente tabla:

Campo	Description (Descripción)
Nombre	Introduzca el nombre del servicio que desea mostrar en NSX Manager.
Description (Descripción)	(Opcional) Introduzca una etiqueta para describir el objetivo o función de esta definición de servicio.
Grupo de dispositivos	Seleccione el grupo de dispositivos o la jerarquía del grupo de dispositivos a la que se asignarán estos cortafuegos VM-Series. Para obtener más información, consulte Panorama> VMware NSX.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
Plantilla	Seleccione la plantilla a la que se asignarán los cortafuegos VM-Series. Para obtener más información, consulte Panorama > Templates. Cada definición de servicio debe asignarse a una única plantilla o pila de plantillas. Una plantilla puede tener varias zonas (Zona de perfil de servicio para NSX para NSX) asociadas a ella. Para la implementación de una única tenencia, cree una zona (NSX Service Profile Zone) en la plantilla. Para la implementación de varias tenencias, cree una zona para cada subtenencia. Cuando cree una nueva Zona de perfil de servicio NSX, esta se adjunta automáticamente a un par de subinterfaces de cable virtuales. Para obtener más información, consulte Network > Zones.
URL de OVF de serie VM	Introduzca la URL (dirección IP o nombre de host y ruta) donde NSX Manager puede acceder al archivo OVF para abastecer a los nuevos cortafuegos VM-Series.
Notificar grupos	Seleccione un grupo de notificación del menú desplegable.

Configuración de acceso al NSX Manager

- Panorama > VMware NSX > Service Managers

Para que Panorama pueda comunicarse con el NSX Manager es necesario **Add (Añadir)** y configurar los ajustes tal y como se describe en la siguiente tabla.

Administradores de servicios	Description (Descripción)
Nombre del administrador de servicios	Introduzca un nombre para identificar el cortafuegos VM-Series como servicio. Este nombre se muestra en NSX Manager y se utiliza para implementar el cortafuegos VM-Series a petición. Admite hasta 63 caracteres; utilice solo letras, números, guiones y guiones bajos.
Description (Descripción)	(Opcional) Introduzca una etiqueta para describir el objetivo o función de este servicio.
URL de administrador NSX	Especifique la URL que Panorama utilizará para establecer una conexión con NSX Manager.
Inicio de sesión de administrador NSX	Introduzca las credenciales de autenticación (nombre de usuario y contraseña) configuradas en el administrador NSX. Panorama utiliza estas credenciales para autenticarse con NSX Manager.
Contraseña de administrador NSX	
Confirmar contraseña de	

© 2020 Palo Alto Networks, Inc.

Administradores de servicios	Description (Descripción)
administrador NSX	
Definiciones de servicio	Especifique las definiciones de servicio asociadas con este administrador de servicios. Cada administrador de servicios admite hasta 32 definiciones de servicio.

Después de compilar los cambios en Panorama, la ventana de VMware Service Manager muestra el estado de conexión entre Panorama y NSX Manager.

Estado de sincronización	Description (Descripción)
estado	Muestra el estado de conexión entre Panorama y el administrador NSX. Una conexión exitosa se muestra como Registered; Panorama y NSX Manager están sincronizados y el cortafuegos VM-Series está registrado como servicio en NSX Manager. En caso de una conexión no exitosa, el estado puede ser el siguiente: • **Connected Error**: no se ha podido alcanzar/establecer una conexión de red con NSX Manager. • **Not authorized**: las credenciales de acceso (nombre de usuario o contraseña) son incorrectas. • **Unregistered**: el administrador de servicios, la definición del servicio o el perfil del servicio no están disponibles o se eliminaron en NSX Manager. • **Out of sync**: los ajustes de configuración definidos en Panorama son distintos a lo que se definieron en NSX Manager. Haga clic en **Out of sync (Sin sincronización)** para obtener detalles sobre los motivos del fallo. Por ejemplo, NSX Manager puede tener una definición de servicio con el mismo nombre que se definió en Panorama. Para reparar el error, use el nombre de definición de servicio detallado en el mensaje de error para validar la definición del servicio en NSX Manager. Hasta que se sincronice la configuración en Panorama y NSX Manager, no puede añadir una nueva definición de servicio en Panorama.
Sincronizar objetos dinámicos	Haga clic en **Synchronize Dynamic Objects (Sincronizar objetos dinámicos)** para actualizar la información de objeto dinámico desde NSX Manager. La sincronización de objetos dinámicos le permite mantener el contexto en los cambios del entorno virtual y activar aplicaciones de forma segura, ya que actualiza de forma automática los grupos de direcciones dinámicas en las reglas de la política. *En Panorama, solo puede ver las direcciones IP que están registradas dinámicamente desde NSX Manager. Panorama no muestra las direcciones IP dinámicas registradas directamente en los cortafuegos. Si usa los Orígenes de información de VM (no admitidos en los cortafuegos VM-Series edición NSX) o XML API para registrar las direcciones IP dinámicamente en los cortafuegos, debe iniciar sesión en cada cortafuegos para ver la lista completa de direcciones IP dinámicas (aquellas que envían desde Panorama y que se registran localmente) en el cortafuegos.*

© 2020 Palo Alto Networks, Inc.

Estado de sincronización	Description (Descripción)
Sincronización de configuración de NSX	Seleccione **NSX Config-Sync (Sincronización de configuración de NSX)** para sincronizar las definiciones del servicio configuradas en Panorama con NSX Manager. Si tiene confirmaciones pendientes en Panorama, esta opción no está disponible. Si la sincronización falla, visualice los detalles en el mensaje de error para saber si el error está en Panorama o en NSX Manager. Por ejemplo, cuando elimina una definición de servicio en Panorama, la sincronización NSX Manager falla si se hace referencia a la definición de servicio en una regla en NSX Manager. Use la información en el mensaje de error para determinar el motivo del fallo y dónde debe tomar medidas correctivas (en Panorama o en NSX Manager).

Creación de reglas de dirección

- Panorama > VMware NSX > Steering Rules

Las reglas de dirección determinan qué tráfico y de qué invitados en el clúster se envía al cortafuegos de la VM-Series.

Campo	Description (Descripción)
Generación automática de reglas de dirección	Genera reglas de dirección basadas en una regla de seguridad configurada de la siguiente forma: • Pertenece a un grupo de dispositivos principal o secundario registrados con un Administrador de servicios NSX. • Tiene la misma zona que el origen y destino (no de cualquiera a cualquiera). • Tiene sólo una zona. • No tiene grupo de dirección estática, intervalo de IP o máscara de red configurada para la política. De forma predeterminada, las reglas de dirección generadas a través de Panorama no tienen Servicios NSX configurados y la dirección de tráfico NSX está establecida como dentro-fuera. Después de generar las reglas de dirección, puede actualizar reglas de dirección individuales para cambiar la dirección de tráfico NSX o agregar servicios NSX. Panorama automáticamente rellena los siguientes campos (excepto Descripción y Servicios NSX) al generar automáticamente reglas de dirección.
Nombre	Introduzca el nombre de la regla de dirección que desea mostrar en NSX Manager. Cuando se genera automáticamente, Panorama añade el prefijo auto_ a cada regla de dirección y reemplaza cualquier espacio en el nombre de la regla de política de seguridad con un subrayado (_).
Description (Descripción)	(Opcional) Introduzca una etiqueta para describir el objetivo o función de esta definición de servicio.
Dirección del tráfico NSX	Especifique la dirección del tráfico que se redirige al cortafuegos VM-Series. • **inout (dentro-fuera)**-Crea una regla INOUT en NSX. El tráfico del tipo especificado que va entre el origen y el destino se redirige al cortafuegos de la

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	serie VM. Panorama utiliza esta dirección de tráfico para las reglas de dirección generadas automáticamente. • **in (dentro)**-Crea una regla IN en NSX. El tráfico del tipo especificado que va al origen desde el destino se redirige al cortafuegos de la serie VM. • **out (fuera)**-Crea una regla OUT en NSX. El tráfico del tipo especificado que va del origen al destino se redirige al cortafuegos de la serie VM.
Servicios NSX	Seleccione el tráfico de la aplicación (Active Directory Server, HTTP, DNS, etc.) para redirigir al cortafuegos de la serie VM..
Grupo de dispositivos	Seleccione un grupo de dispositivos del menú desplegable. El grupo de dispositivos elegido determina qué políticas de seguridad se aplican a la regla de dirección. Los grupos de dispositivos deben estar asociados con una definición de servicio NSX.
Política de seguridad	La regla de política de seguridad en la que se basa la regla de dirección generada automáticamente.

© 2020 Palo Alto Networks, Inc.

Panorama > Perfil de ingestión de logs

Utilice el perfil de ingesta de log para permitir que Panorama reciba logs de fuentes externas. En PAN-OS 8.0.0, Panorama (en modo Panorama) puede servir como un receptor Syslog que puede ingerir logs desde el servidor Traps ESM mediante Syslog. Se añadirá compatibilidad con nuevas fuentes de logs externas y actualizaciones de las nuevas versiones Traps ESM mediante actualizaciones de contenido.

Para habilitar la ingesta de log, debe configurar Panorama como un receptor Syslog en el servidor Traps ESM, definir un perfil de ingesta de log en Panorama y adjuntar el perfil de ingesta de log a un grupo de recopiladores de logs.

Para añadir un nuevo perfil de ingesta de Syslog externo, haga clic en **Add (Añadir)** un perfil y configure los ajustes como se describe en la siguiente tabla.

Campo	Description (Descripción)
Nombre	Introduzca el nombre del perfil de ingesta de Syslog externo. Puede añadir hasta 255 perfiles.
Nombre de origen	Introduzca el nombre o la dirección IP de las fuentes externas que enviarán logs. Puede añadir hasta 4 fuentes por perfil.
Puerto	Introduzca el puerto mediante el que se podrá acceder a Panorama a través de la red y que Panorama utilizará para comunicarse y escuchar. Para Traps ESM, seleccione un valor entre el intervalo de 23000 a 23999. Debe configurar el mismo número de puerto en Traps ESM para habilitar la comunicación entre Panorama y el ESM.
Transporte	Seleccione TCP, UDP o SSL. Si selecciona SSL, debe configurar un certificado entrante para la comunicación segura de syslog en Panorama > Managed Collectors > General.
Tipo de log externo	Seleccione el tipo de log en el menú desplegable.
versión	Seleccione la versión en el menú desplegable.

Consulte Monitor > External Logs para obtener información sobre los logs ingeridos desde el servidor Traps ESM en Panorama.

© 2020 Palo Alto Networks, Inc.

Panorama > Configuración de log

Utilice la página **Log Settings (Configuración del log)** para enviar los siguientes tipos de log a servicios externos:

- Los logs de sistema, configuración, User-ID y correlación que el servidor de gestión Panorama (dispositivo M-Series o dispositivo virtual Panorama en modo Panorama) genera localmente.
- Los logs de todos los tipos que el dispositivo virtual Panorama en modo Legacy genera localmente o se recopila de cortafuegos.

Para los logs que los cortafuegos envían a los recopiladores de log, concluya la Configuración del recopilador de logs para permitir el reenvío a servicios externos.

Antes de empezar, defina perfiles de servidor para los servicios externos (consulte Device > Server Profiles > SNMP Trap, Device > Server Profiles > Syslog, Device > Server Profiles > Email, y Device > Server Profiles > HTTP). Después, haga clic en **Add (Añadir)** para agregar uno o más perfiles de lista de coincidencias y configure los ajustes como se describe en la siguiente tabla.

Configuración del perfil de la lista de coincidencias	Description (Descripción)
Nombre	Introduzca un nombre (hasta 31 caracteres) para el perfil de la lista de coincidencias.
Filter (Filtro)	De forma predeterminada, Panorama envía **All Logs (Todos los logs)** del tipo que está añadiendo al perfil de la lista de coincidencias. Para enviar un subconjunto de logs, abra el menú desplegable y seleccione un filtro existente o seleccione **Filter Builder (Generador de filtro)** para añadir un nuevo filtro. En cada nueva aplicación de filtro, especifique los siguientes campos y haga clic en **Add (Añadir)** para incluir la consulta: • **Connector (Conector)**: seleccione la lógica del conector (y/o) para la consulta. Seleccione **Negate (Negar)** si desea aplicar la negación a la lógica. Por ejemplo, para evitar el reenvío de logs desde una zona no fiable, seleccione **Negate (Negar)**, **Zone (Zona)** como atributo, **equal (igual)** como operador e introduzca el nombre de la zona no fiable en la columna Value (Valor). • **Attribute (Atributo)**: seleccione un atributo de log. Las opciones dependen del tipo de log. • **Operator (Operador)**: seleccione el criterio para determinar si se aplica el atributo (como **equal [igual]**). Las opciones disponibles dependen del tipo de log. • **Value (Valor)**: especifique un valor de atributo para que coincida con la consulta. Para ver o exportar los logs que coinciden con el filtro, seleccione **View Filtered Logs (Ver logs filtrados)**. Esta pestaña ofrece las mismas opciones que las páginas de la pestaña **Monitoring** (Supervisión) (como **Monitoring [Supervisión]** > **Logs [Logs]** > **Traffic [Tráfico]**).
Description (Descripción)	Introduzca una descripción de hasta 1024 caracteres para explicar el propósito de este perfil de lista de coincidencias.

© 2020 Palo Alto Networks, Inc.

Configuración del perfil de la lista de coincidencias	Description (Descripción)
SNMP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de trampas SNMP para reenviar logs como trampas SNMP (consulte Device > Server Profiles > SNMP Trap).
EMAIL	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor de correo electrónico para reenviar logs como notificaciones de correo electrónico (consulte Device > Server Profiles > Email).
Syslog	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor Syslog para reenviar logs como mensajes de syslog (consulte Device > Server Profiles > Syslog).
HTTP	Haga clic en **Add (Añadir)** para añadir uno o varios perfiles de servidor HTTP para reenviar logs como solicitudes HTTP (consulte Device > Server Profiles > HTTP).
Acciones integradas	Todos los tipos de log excepto los logs del sistema y los de configuración le permiten configurar acciones. • Haga clic en **Add (Añadir)** para añadir una acción e introduzca un nombre que la describa. • Seleccione la dirección IP que desea etiquetar: **Source Address (Dirección de origen)** o **Destination Address (Dirección de destino)**. • Seleccione la acción: **Add Tag (Añadir etiqueta)** o **Remove Tag (Eliminar etiqueta)**. • Seleccione si distribuir la etiqueta al agente de User-ID local en este dispositivo o a un agente de User-ID remoto. • Para distribuir etiquetas a un **Remote device User-ID Agent (Agente User-ID de dispositivo remoto)**, seleccione el perfil de servidor HTTP que habilitará el reenvío. • Configure la opción **Timeout (Tiempo de espera)** de la etiqueta IP para configurar, en minutos, el tiempo durante el que se mantendrá la asignación de dirección IP a etiqueta. Una configuración de tiempo de espera en 0 significa que el tiempo de espera de la asignación de la etiqueta IP no se agotará (el intervalo es de 0 a 43 200 [30 días]; el valor predeterminado es 0). *Solo puede configurar un tiempo de espera con la acción Add Tag (Añadir etiqueta).* • Introduzca o seleccione las **Tags (Etiquetas)** que desea aplicar o quitar de la dirección IP objetivo de origen o de destino. Solo puede etiquetar la dirección IP de origen en los logs de correlación y en los de coincidencias HIP.

© 2020 Palo Alto Networks, Inc.

Panorama > Exportación de configuración programada

Para programar una exportación de todas las configuraciones en ejecución en Panorama y cortafuegos, haga clic en **Add (Añadir)** para añadir una tarea de exportación y configure los ajustes como se describe en la siguiente tabla.

Si Panorama tiene una configuración de alta disponibilidad (HA), debe aplicar estas instrucciones en cada peer para asegurarse de que las exportaciones programadas continúen tras una conmutación por error. Panorama no sincroniza exportaciones de configuración programadas entre peers HA.

Configuración de la exportación de configuración programada	Description (Descripción)
Nombre	Introduzca un nombre para identificar el trabajo de exportación de configuración (hasta 31 caracteres). El nombre hace distinción entre mayúsculas y minúsculas y debe ser exclusivo. Utilice solamente letras, números, guiones y guiones bajos.
Description (Descripción)	Introduzca una descripción opcional.
Habilitación	Seleccione esta opción para habilitar el trabajo de exportación.
Hora de inicio de exportación programada (a diario)	Especifique la hora del día a la que se iniciará la exportación (reloj de 24 horas, formato HH:MM).
PROTOCOL	Seleccione el protocolo que debe utilizarse para exportar logs desde Panorama a un host remoto. Secure Copy (**SCP**) es un protocolo seguro; **FTP** no lo es.
Nombre de host	Introduzca la dirección IP o el nombre de host del servidor SCP o FTP de destino.
Puerto	Introduzca el número de puerto en el servidor de destino.
Ruta	Especifique la ruta a la carpeta o directorio en el servidor de destino que guardará la configuración exportada. Por ejemplo, si el lote de configuración está almacenado en una carpeta denominada exported_config dentro de una carpeta de nivel superior denominada Panorama, la sintaxis para cada tipo de servidor es la siguiente: • Servidor SCP://Panorama/exported_config • Servidor FTP://Panorama/exported_config Los siguientes caracteres: `.`(punto), `+`, `{` y `}`, `/`, `-`, `_`, `0-9`, `a-z` y `A-Z`. Los espacios no son compatibles con la **ruta** del archivo.

© 2020 Palo Alto Networks, Inc.

Configuración de la exportación de configuración programada	Description (Descripción)
Enable FTP Passive Mode (Habilitar modo pasivo de FTP)	Seleccione esta opción para utilizar el modo pasivo de FTP.
Nombre de usuario	Especifique el nombre de usuario necesario para acceder al sistema de destino.
Contraseña/Confirmar contraseña	Especifique la contraseña necesaria para acceder al sistema de destino. Utilice una contraseña con una extensión máxima de 15 caracteres. Si la contraseña supera los 15 caracteres, la conexión SCP de prueba mostrará un error, ya que el cortafuegos cifra la contraseña cuando intenta conectarse con el servidor SCP y la extensión de la contraseña cifrada puede ser de hasta 63 caracteres únicamente.
Conexión de servidor SCP de prueba	Seleccione esta opción para probar la comunicación entre Panorama y el host/servidor SCP. Para activar la transferencia segura de los datos, debe verificar y aceptar la clave de host del servidor SCP. La conexión no se establece hasta que acepte la clave de host. Si Panorama tiene una configuración de HA, debe realizar esta verificación en cada peer de HA para que cada uno acepte la clave de host del servidor SCP.

© 2020 Palo Alto Networks, Inc.

Panorama > Software

Use esta página para gestionar las actualizaciones del software de Panorama en el servidor de gestión de Panorama.

- Gestión de actualizaciones del software de Panorama
- Visualización de la información de actualización del software de Panorama

Gestión de actualizaciones del software de Panorama

Seleccione **Panorama** > **Software** para realizar las tareas descritas en la siguiente tabla.

De manera predeterminada, el servidor de gestión de Panorama guarda hasta dos versiones del software. Para dejar espacio libre para las actualizaciones más nuevas, el servidor elimina automáticamente la actualización más antigua. Puede cambiar el número de imágenes de software que Panorama guarda y eliminar imágenes manualmente para liberar espacio.

Consulte Instalación de actualizaciones de software y contenido de Panorama (en inglés) para obtener información importante sobre la compatibilidad de la versión.

Tarea	Description (Descripción)
Comprobar ahora	Si Panorama tiene acceso a Internet, haga clic en **Check Now (Comprobar ahora)** para mostrar la información de la actualización más reciente (consulte Visualización de la información de actualización del software de Panorama). Si Panorama no tiene acceso a la red externa, use un navegador para visitar el sitio de actualización de software para obtener información de la actualización.
Carga	Para cargar una imagen de software cuando Panorama no tiene acceso a Internet, utilice un navegador para visitar el sitio de actualización de software, localice la versión deseada y descargue la imagen de software en un ordenador al que Panorama pueda acceder, seleccione **Panorama** > **Software**, haga clic en **Upload (Cargar)**, **Browse (Examinar)** para seleccionar la imagen de software y haga clic en **OK (Aceptar)**. Cuando se complete la carga, la columna Available (Disponible) mostrará `Uploaded`.
DESCARGUE	Si Panorama tiene acceso a Internet, haga clic en **Download (Descargar)** en la columna Action de la versión deseada. Cuando se complete la descarga, la columna Available mostrará Downloaded.
Instalación	Instale (**Install [Instalar]** en la columna Action) la imagen del software. Cuando la instalación finaliza, Panorama cierra sesión mientras se reinicia. *Panorama ejecuta periódicamente una comprobación de integridad del sistema de archivos (file system integrity check, FSCK) para evitar daños en el sistema de archivos de Panorama. Esta comprobación se realiza cada 8 reinicios o tras un reinicio 90 días después de la última comprobación de integridad del sistema de archivos (file system integrity check, FSCK). Aparecerá una advertencia en la interfaz web y pantallas de inicio de sesión de SSH si una comprobación FSCK se está ejecutando y no*

© 2020 Palo Alto Networks, Inc.

Tarea	Description (Descripción)
	podrá iniciar sesión hasta que se complete. El tiempo necesario para completar el proceso depende del tamaño del sistema de almacenamiento; en un sistema grande, pueden pasar varias horas antes de que pueda iniciar sesión en Panorama. Para ver el progreso, configure el acceso de consola a Panorama.
Notas de versión	Si Panorama tiene acceso a Internet, haga clic en **Release Notes (Notas de versión)** para acceder a las notas de la versión para conocer la versión de software deseada y revise los cambios de la versión, correcciones, problemas conocidos, problemas de compatibilidad y cambios en el comportamiento predeterminado. Si Panorama no tiene acceso a Internet, use un navegador para visitar el sitio de actualización de software y descargue la versión correcta.
☒	Elimine una imagen de software cuando ya no sea necesaria o cuando desee liberar espacio para descargar más imágenes.

Visualización de la información de actualización del software de Panorama

Seleccione **Panorama** > **Software** para mostrar la siguiente información. Para mostrar la información más reciente de Palo Alto Networks, haga clic en **Check Now (Comprobar ahora)**.

Información sobre la actualización de contenido y software	Description (Descripción)
versión	La versión de software de Panorama
Tamaño	El tamaño en megabytes de la imagen del software.
Release date	La fecha y hora en la que Palo Alto Networks realizó la actualización.
Disponible	Indica si la imagen está disponible para la instalación.
Instalado actualmente	Una marca de verificación indica que la actualización está instalada.
Acción	Indica las acciones (**Download (Descargar)**, **Install (Instalar)** o **Reinstall (Reinstalar)**) que están disponibles para una imagen.
Notas de versión	Haga clic en **Release Notes (Notas de versión)** para acceder a las notas de la versión para la versión de software deseada y revise los cambios de la versión, correcciones, problemas conocidos, problemas de compatibilidad y cambios en el comportamiento predeterminado.
☒	Elimine una actualización cuando ya no sea necesaria o para liberar espacio para más descargas o cargas.

© 2020 Palo Alto Networks, Inc.

Panorama > Implementación de dispositivo

Puede utilizar Panorama para implementar software y actualizaciones de contenido en varios cortafuegos y recopiladores de logs y administrar licencias de cortafuegos.

¿Qué está buscando?	Consulte:
Implemente software y actualizaciones de contenido en los cortafuegos y recopiladores de logs.	Gestión de software y actualizaciones de contenido
Consulte qué software y actualizaciones de contenido están instaladas o disponibles para su descarga e instalación.	Visualización de la información sobre la actualización de contenido y software
Programar actualizaciones de contenido automáticas para los cortafuegos y recopiladores de logs	Programación de actualizaciones de contenido dinámico
Revertir las versiones de contenido de uno o más cortafuegos de Panorama.	Restablecimiento de las versiones de contenido de Panorama
Visualice, active, desactive y actualice licencias. Consulte el estado de las licencias del cortafuegos.	Gestión de licencias de cortafuegos
¿Busca más información?	Gestión de licencias y actualizaciones.

Gestión de software y actualizaciones de contenido

- Panorama > Device Deployment > Software

Panorama proporciona las siguientes opciones para implementar software y actualizaciones de contenido en cortafuegos y recopiladores de logs.

Para reducir el tráfico en la interfaz de gestión (MGT), puede configurar Panorama para utilizar una interfaz independiente para implementar actualizaciones (consulte Panorama > Setup > Interfaces*).*

© 2020 Palo Alto Networks, Inc.

Opciones de implementación de dispositivos de Panorama	Description (Descripción)
DESCARGUE	Para implementar una actualización de contenido o software cuando Panorama está conectado a Internet, haga clic en **Download (Descargar)** para descargar la actualización. Cuando se complete la descarga, la columna Available mostrará Downloaded. Entonces, puede realizar lo siguiente: • Instale la actualización de software o la de contenido de PAN-OS/Panorama. • Activar la actualización de software del cliente VPN de SSL o la aplicación de GlobalProtect™.
upgrade	Si está disponible la actualización de contenido de filtrado de URL de BrightCloud, haga clic en **Upgrade (Actualizar)**. Cuando finalice la actualización, puede instalar la actualización en el cortafuegos.
Instalación	Después de descargar o cargar un software de PAN-OS, un software de Panorama o una actualización de contenido, haga clic en **Install (Instalar)** en la columna Action y seleccione las siguientes opciones: • **Devices (Dispositivos)**: seleccione los cortafuegos o recopiladores de logs en los que instalará el software. Si la lista es extensa, use los filtros. Seleccione **Peers del grupo de HA** para agrupar los cortafuegos que son peers de alta disponibilidad (HA). Esta opción le permite identificar fácilmente cortafuegos que tienen una configuración de HA. Para mostrar solo los cortafuegos o recopiladores de logs específicos, selecciónelos y luego seleccione **Filter Selected (Archivos seleccionados)**. • **Upload only to device (Cargar solo al dispositivo)** (software solamente): seleccione esta opción para cargar el software sin instalarlo automáticamente. Debe instalar el software manualmente. • **Reboot device after install (Reiniciar dispositivo tras la instalación)** (software solamente): seleccione esta opción si desea que el proceso de instalación reinicie automáticamente los cortafuegos o los recopiladores de logs. La instalación no puede finalizar hasta que se produzca un reinicio. • **Disable new apps in content update (Deshabilitar nuevas aplicaciones en actualización de contenido)** (Aplicaciones y amenazas solamente): seleccione esta opción para desactivar aplicaciones en la actualización que son nuevas en relación con la última actualización instalada. Esto lo protege contra las últimas amenazas y le brinda la flexibilidad de habilitar aplicaciones después de preparar cualquier actualización de políticas. Luego, para habilitar las aplicaciones, inicie sesión en el cortafuegos, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, haga clic en **Apps (Aplicaciones)** en la columna Features (Funciones) para mostrar las nuevas aplicaciones y luego haga clic en **Enable/Disable (Habilitar/Deshabilitar)** en cada aplicación que desee habilitar. *También puede seleccionar Panorama > Managed Devices (Dispositivos gestionados) para instalar* software de cortafuegos y actualizaciones de contenido *o Panorama > Managed Collectors (Recopiladores gestionados) para instalar* actualizaciones de software para recopiladores de logs dedicados*.*

© 2020 Palo Alto Networks, Inc.

Opciones de implementación de dispositivos de Panorama	Description (Descripción)
Activar	Después de descargar o cargar una actualización de software de la aplicación de GlobalProtect, haga clic en **Activate (Activar)** en la columna Action (Acción) y seleccione las siguientes opciones: • **Devices (Dispositivos)**: seleccione los cortafuegos en los que activará la actualización. Si la lista es extensa, use los filtros. Seleccione **Peers del grupo de HA** para agrupar los cortafuegos que son peers de alta disponibilidad (HA). Esta opción le permite identificar fácilmente cortafuegos que tienen una configuración de HA. Para mostrar solo los cortafuegos específicos, selecciónelos y luego seleccione **Filter Selected (Filtrar seleccionados)**. • **Upload only to device (Cargar solo al dispositivo)**: seleccione esta opción si no desea que PAN-OS active automáticamente la imagen cargada. Debe iniciar sesión en el cortafuegos y activarla.
Notas de versión	Haga clic en **Release Notes (Notas de versión)** para acceder a las notas de la versión para la versión de software deseada y revise los cambios de la versión, correcciones, problemas conocidos, problemas de compatibilidad y cambios en el comportamiento predeterminado.
Documentación	Haga clic en **Documentation (Documentación)** para acceder a las notas de la versión para obtener la versión de contenido deseada.
☒	Elimine una actualización de contenido o software cuando ya no sea necesaria o cuando desee liberar espacio para realizar más descargas o cargas.
Comprobar ahora	Haga clic en **Check Now (Comprobar ahora)** para ver la información sobre la actualización de contenido y software.
Carga	Para implementar una actualización de contenido o software cuando Panorama no está conectado a Internet, descargue la actualización en su ordenador desde el sitio de actualizaciones de software o actualizaciones dinámicas, seleccione la página **Panorama** > **Device Deployment (Implementación de dispositivo)** que corresponda al tipo de actualización, haga clic en **Upload (Cargar)**, seleccione el tipo de actualización en **Type (Tipo)** (actualizaciones de contenido solamente), seleccione el archivo cargado y haga clic en **OK (Aceptar)**. Los pasos para instalar o activar la actualización dependen del tipo: • **Software de PAN-OS o Panorama**: cuando se complete la carga, la columna Available mostrará Uploaded. Entonces podrá instalar la actualización de software. • **GlobalProtect Client or SSL VPN Client software (Software de cliente de GlobalProtect o de cliente VPN de SSL)**: activar desde el archivo. • **Dynamic updates (Actualizaciones dinámicas)**: instalar desde el archivo.
Instalar desde archivo	Después de cargar una actualización de contenido, haga clic en **Install from File (Instalar desde archivo)**, seleccione el tipo de contenido en **Type (Tipo)**, seleccione el nombre de archivo de la actualización y luego seleccione los cortafuegos o los recopiladores de logs.

© 2020 Palo Alto Networks, Inc.

Opciones de implementación de dispositivos de Panorama	Description (Descripción)
Activar desde archivo	Después de cargar una actualización de software de aplicación de GlobalProtect, haga clic en **Activate from File (Activar desde archivo)**, seleccione el nombre de archivo de la actualización y seleccione los cortafuegos.
Programaciones	Seleccione esta opción para programar actualizaciones de contenido dinámico.

Visualización de la información sobre la actualización de contenido y software

- Panorama > Device Deployment > Software

Seleccione **Panorama** > **Device Deployment (Implementación de dispositivos)** > **Software** para mostrar PAN-OS **Software**, **GlobalProtect Client (Cliente de GlobalProtect)** software y **Dynamic Updates (Actualizaciones dinámicas)** (contenido) que están actualmente instaladas o disponibles para descargar e instalar. La página **Dynamic Updates (Actualizaciones dinámicas)** organiza la información por tipo de contenido (antivirus, aplicaciones y amenazas, filtrado de URL y WildFire) e indica la fecha y hora de la última verificación de información actualizada. Para mostrar la información más reciente de contenido y software de Palo Alto Networks, haga clic en **Check Now (Comprobar ahora)**.

Información sobre la actualización de contenido y software	
versión	La versión de actualización de contenido o software.
Nombre de archivo	El nombre del archivo de actualización.
Zero Trust	El modelo designado del cortafuegos o recopilador de logs para la actualización. Un número indica una plataforma de cortafuegos de hardware (por ejemplo, `7000` indica el cortafuegos serie PA-7000), `vm` indica el cortafuegos VM-Series y `m` indica el dispositivo serie M.
Features	(Contenido solamente) Enumera el tipo de firmas que puede incluir la versión de contenido.
Tipo	(Contenido solamente) Indica si la descarga incluye una actualización completa o una actualización incremental.
Tamaño	El tamaño del archivo de actualización.
Release date	La fecha y hora en la que Palo Alto Networks realizó la actualización.
Disponible	(Software PAN-OS o Panorama solamente) Indica que la actualización se cargó o descargó.

© 2020 Palo Alto Networks, Inc.

Información sobre la actualización de contenido y software	
Descargado	(Software de cliente de VPN de SSL, software de cliente de GlobalProtect o contenido solamente) Una marca de verificación indica que la actualización de descargó.
Acción	Indica la acción que puede realizar en la actualización: Descargar, Actualizar, Instalar o Habilitar.
Documentación	(Contenido solamente) Brinda un enlace a las notas de la revisión de la versión de contenido deseada.
Notas de versión	(Software solamente) Brinda un enlace a las notas de la revisión de la versión de software deseada.
☒	Elimine una actualización de cuando ya no sea necesaria o cuando desee liberar espacio para realizar más descargas o cargas.

Programación de actualizaciones de contenido dinámico

- Panorama > Implementación de dispositivo > Actualizaciones dinámicas

Para programar una descarga e instalación automática de una actualización, haga clic en **Schedules (Programas)**, luego en **Add (Añadir)** y configure los ajustes como se describe en la siguiente tabla.

Configuración de programación de actualizaciones dinámicas	
Nombre	Introduzca un nombre para identificar el trabajo programado (hasta 31 caracteres). El nombre debe ser único, distingue entre mayúsculas y minúsculas, y solo puede contener letras, números, guiones y guiones bajos.
Disabled (Deshabilitado)	Seleccione esta opción para deshabilitar el trabajo programado.
Tipo	Seleccione el tipo de actualización de contenido a programar: **App**, **App and Threat (Aplicación y amenaza)**, **Antivirus**, **WildFire** o **URL Database (Base de datos URL)**.
Periodicidad	Seleccione el intervalo en el que Panorama comprueba el servidor de actualizaciones. Las opciones de periodicidad varían según el tipo de actualización.
Time	Para realizar una actualización **Daily (Diaria)**, seleccione la **Time (Hora)** en el reloj de 24 horas. Para realizar una actualización **Weekly (Semanal)**, seleccione el **Day (Día)** de la semana y la **Time (Hora)** del reloj de 24 horas.
Deshabilitar nuevas aplicaciones en actualización de contenido	Puede deshabilitar nuevas aplicaciones en las actualizaciones de contenido si configura el tipo de actualización en **Type (Tipo)** a **App (Aplicación)** o **App and Threat (Aplicación y amenaza)** y solo si **Action (Acción)** está configurado como **Download and Install (Descargar e instalar)**. Seleccione esta opción para deshabilitar aplicaciones en la actualización que son nuevas en relación con la última actualización instalada. Esto lo protege contra las últimas amenazas y le brinda la flexibilidad de habilitar aplicaciones después de

© 2020 Palo Alto Networks, Inc.

Configuración de programación de actualizaciones dinámicas	
	preparar cualquier actualización de políticas. Luego, para habilitar las aplicaciones, inicie sesión en el cortafuegos, seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)**, haga clic en **Apps (Aplicaciones)** en la columna Features (Funciones) para mostrar las nuevas aplicaciones y luego haga clic en **Enable/Disable (Habilitar/Deshabilitar)** en cada aplicación que desee habilitar.
Acción	• **Download Only (Solo descargar)**: Panorama descargará la actualización programada. Debe instalar manualmente la actualización en los cortafuegos y recopiladores de logs. • **Download and Install (Descargar e instalar)**: Panorama descargará e instalará automáticamente la actualización programada.
Dispositivos	Seleccione **Devices (Dispositivos)** y luego seleccione los cortafuegos que recibirán las actualizaciones de contenido programadas.
Recopiladores de logs	Seleccione **Logs Collectors (Recopiladores de logs)** y luego seleccione los recopiladores gestionados que recibirán las actualizaciones de contenido programadas.

Restablecimiento de las versiones de contenido de Panorama

- Panorama > Implementación de dispositivo > Actualizaciones dinámicas

Realice rápidamente el **Restablecimiento de contenido** de las versiones de aplicaciones, aplicaciones y amenazas, antivirus, WildFire, y las actualizaciones de contenido de WildFire de uno o más cortafuegos a la versión de contenido instalada previamente desde Panorama. La versión de contenido que restablece debe ser una versión más antigua de la instalada actualmente en el cortafuegos. Esta función está disponible en Panorama con la versión 8.1. El contenido en los cortafuegos se puede restablecer si la función se encuentra disponible localmente en el cortafuegos.

Campo	Description (Descripción)
Filter (Filtro)	Filtra los dispositivos en los que desea restablecer el contenido. Puede filtrar por lo siguiente: • Estado del dispositivo • Plataformas • Grupos de dispositivos • Plantillas • Etiquetas • Estado HA • Software Version (Versión de software) (PAN-OS) • Versión de contenido actual
Dispositivos	Seleccione uno o más dispositivos para restablecer. Muestra la siguiente información de los dispositivos: • Device Name (Nombre del dispositivo): nombre del cortafuegos.

© 2020 Palo Alto Networks, Inc.

Campo	Description (Descripción)
	• Current version (Versión actual): versión de contenido actual instalada en el dispositivo. La columna mostrará 0 si no hay una versión de contenido instalada. • Previous version (Versión previa) (contenido): la versión de contenido instalada previamente en los cortafuegos con PAN 8.1 o posterior. La columna estará vacía si no se instalaron versiones de contenido o si el cortafuegos ejecuta una versión de PAN-OS anterior a 8.1. • Software Version (Versión de software): la versión actual de PAN-OS instalada en el dispositivo. • HA Status (Estado de HA): muestra el estado de HA cuando el dispositivo se encuentra en un par de HA. La columna estará vacía si el dispositivo no está en un par de HA.
Group HA pairs (Agrupar pares de HA)	Seleccione esta opción para agrupar pares de HA.

Cuando haya seleccionado los dispositivos que desea restablecer, haga clic en **OK (Aceptar)**.

Gestión de licencias de cortafuegos

- Panorama > Device Deployment > Licenses

Seleccione **Panorama** > **Device Deployment (Implementación de dispositivo)** > **Licenses (Licencias)** para llevar a cabo las siguientes tareas.

- Actualizar las licencias de los cortafuegos que no tienen acceso directo a Internet: haga clic en Refresh (Actualizar).
- Activar una licencia en un cortafuegos: haga clic en **Activate (Activar)**, seleccione el cortafuegos y, en la columna Auth Code (Código de autenticación), introduzca los códigos de autorización que Palo Alto Networks proporcionó para los cortafuegos.
- Desactivar todas las licencias y suscripciones/derechos instalados en los cortafuegos VM-Series: haga clic en **Deactivate VMs (Deshabilitar VM)**, seleccione los cortafuegos (la lista solo muestra los cortafuegos que ejecutan la versión PAN-OS 7.0 o superior) y haga clic en una de las siguientes opciones:
  - **Continue (Continuar)**: deshabilita las licencias y registra automáticamente los cambios con el servidor de licencias. Las licencias se devuelven a su cuenta y están disponibles para volver a utilizarlas.
  - **Complete Manually (Completar manualmente)**: genera un archivo de token. Use esta opción si Panorama no tiene acceso directo a Internet. Para completar el proceso de deshabilitación, debe iniciar sesión en el portal de asistencia técnica, seleccionar **Assets (Activos)**, hacer clic en **Deactivate License(s) (Deshabilitar licencias)**, cargar el archivo de token y hacer clic en **Submit (Enviar)**. Con esto habrá completado el proceso de desactivación.

También puede ver el estado de licencia actual de los cortafuegos gestionados. En el caso de los cortafuegos que tienen acceso directo a internet, Panorama realiza comprobaciones diarias automáticamente con el servidor de licencias, recupera actualizaciones y renovaciones de licencias, y las envía a los cortafuegos. La comprobación está programada para producirse entre la 1 y 2 a. m.; y no puede modificar esta programación.

© 2020 Palo Alto Networks, Inc.

Información de licencia del cortafuegos	
Dispositivo	El nombre del cortafuegos.
Sistema virtual	Indica si el cortafuegos admite o no múltiples sistemas virtuales.
Threat Prevention	Indica si la licencia está activa, inactiva o vencida (junto con la fecha de vencimiento).
URL	
Soporte	
Puerta de enlace GlobalProtect	
Portal GlobalProtect	
WildFire	
Capacidad VM-Series	Indica si este es o no un cortafuegos VM-Series.

© 2020 Palo Alto Networks, Inc.