paloalto TECHDOCS

Guía del administrador de redes de PAN-OS®

Version 10.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

Last Revised

August 9, 2021

Table of Contents

Networking 9
- Introducción a las redes 10

Configuración de interfaces 13
- Interfaces de modo tap 14
- Interfaces de cable virtual 16
  - Paquetes de capa 2 y capa 3 en un cable virtual 17
  - Velocidad de puertos en las interfaces de cable virtual 18
  - LLDP en un cable virtual 18
  - Interfaces agregadas para un cable virtual 18
  - Compatibilidad del cable virtual con la alta disponibilidad 19
  - Protección de zona para una interfaz de cable virtual 19
  - Tráfico con etiqueta de VLAN 19
  - Subinterfaces de Virtual Wire 19
  - Configuración de cables virtuales 22
- Interfaces de capa 2 25
  - Interfaces de capa 2 sin LAN 25
  - Interfaces de capa 2 con LAN 26
  - Configure la interfaz de capa 2 27
  - Configuración de una interfaz de capa 2, una subinterfaz y una VLAN 28
  - Gestión de la reescritura de BPDU del árbol de conmutación por VLAN (Per-VLAN Spanning Tree, PVST+) 28
- Interfaces de capa 3 32
  - Configuración de interfaces de capa 3 32
  - Gestión de hosts IPv6 con NDP 39
- Configuración de los grupos de interfaces de agregación 45
- Configuración del reflector de Bonjour para la segmentación de red 49
- Uso de los perfiles de gestión de interfaz para restringir el acceso 52

Enrutadores virtuales 55
- Descripción general del enrutador virtual 56
- Configuración de los enrutadores virtuales 57

Rutas de servicio 59
- Información general sobre las rutas de servicio 60
- Configuración de las rutas de servicio 61

Rutas estáticas 63
- Descripción general de la ruta estática 64
- Eliminación de ruta estática basada en el control de ruta 65

Configuración de una ruta estática....68
Configuración del control de ruta para una ruta estática....70

RIP....73

Descripción general de RIP....74
Configurar RIP....75

OSPF....77

Conceptos de OSPF....78
OSPFv3....78
Vecinos OSPF....78
Áreas OSPF....79
Tipos de enrutadores OSPF....79
Configuración de OSPF....80
Configuración de OSPFv3....84
Configuración del reinicio correcto de OSPF....88
Confirmación del funcionamiento de OSPF....90
Visualización de la tabla de enrutamiento....90
Confirmación de adyacencias OSPF....90
Confirmación de que se han establecido conexiones OSPF....90

BGP....91

Descripción general del BGP....92
MP-BGP....93
Configuración de BGP....95
Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6....103
Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4....106
Confederaciones BGP....108

IP de multidifusión....115

IGMP....116
PIM....118
Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido....120
Mecanismo de imposición de PIM....122
Reenvío de ruta inversa....122
Configuración de IP de multidifusión....124
Visualización de información de IP de multidifusión....132

Redistribución de ruta....135

Descripción general sobre la redistribución de rutas....136
Configuración de la redistribución de rutas....137

Túneles GRE....141

Descripción general de los túneles de GRE 142
Creación de túneles de GRE 144

DHCP 149

Descripción general de DHCP 150
Cortafuegos como servidor y cliente DHCP 151
Mensajes DHCP 152
Direccionamiento DHCP 154
Métodos de asignación de direcciones DHCP 154
Concesiones DHCP 155
Opciones de DHCP 156
Opciones de DHCP predefinidas 156
Múltiples valores para una opción de DHCP 157
Opciones de DHCP 43, 55 y 60 y otras opciones personalizadas 158
Configure una interfaz como servidor DHCP 159
Configure una interfaz como cliente DHCP 164
Configuración de la interfaz de gestión como cliente DHCP 166
Configure una interfaz como agente de relé DHCP 169
Supervisión y resolución de problemas de DHCP 170
Ver información de servidor DHCP principal 170
Borrado de concesiones DHCP 171
Ver información de cliente DHCP 171
Recopilación de resultados de depuración sobre DHCP 171

DNS: 173

Descripción general del DNS 174
Objeto proxy DNS 176
Perfil de servidor DNS 177
Implementaciones de DNS multiusuario 178
Configuración de un objeto proxy DNS 180
Configuración de un perfil de servidor DNS 183
Caso de uso 1: el cortafuegos exige la resolución de DNS 185
Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual 188
Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor 192
Regla de proxy DNS y coincidencia FQDN 194

DDNS 199

Descripción general del DNS dinámico 200
Configuración del DNS dinámico en las interfaces de cortafuegos 203

NAT 207

Reglas de políticas NAT 208
Descripción general de la política de NAT 208
Grupos de direcciones NAT identificados como objetos de direcciones 209
ARP proxy para grupos de direcciones NAT 209
NAT de origen y destino 211
NAT de origen 211
NAT de destino 212
Casos de uso de NAT de destino con reescritura de DNS 214
Capacidades de regla NAT 220
Sobresuscripción de NAT de IP dinámica y puerto 221
Estadísticas de memoria NAT de plano de datos 223
Configuración de NAT 224
Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen) 225
Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino) 226
Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática) 228
Configuración de la NAT de destino con reescritura de DNS 229
Configuración de NAT de destino utilizando direcciones IP dinámicas 230
Modificación de la ratio de sobresuscripción para NAT DIPP 232
Reserva de direcciones NAT de IP dinámicas 232
Deshabilitación de NAT para un host o interfaz específico 233
Ejemplos de configuración de NAT 235
Ejemplos de NAT de destino: asignación de uno a uno 235
NAT de destino con ejemplo de traducción de puerto 236
Ejemplo de NAT de destino: asignación de uno a uno 237
Ejemplo de NAT de origen y destino 237
Ejemplo de NAT de origen de Virtual Wire 239
Ejemplo de NAT estática de Virtual Wire 240
Ejemplo de NAT de destino de Virtual Wire 240

NPTv6 243

Resumen de NPTv6 244
Direcciones locales exclusivas 244
Razones para usar NPTv6 245
Funcionamiento de NPTv6 246
Asignación neutral de suma de comprobación 247
Traducción bidireccional 247
NPTv6 aplicada a un servicio específico 247
Proxy NDP 248

Ejemplo de NPTv6 y Proxy NDP 250
Caché de ND en el ejemplo de NPTv6 250
Proxy ND en el ejemplo de NPTv6 250
La traducción NPTv6 en el ejemplo de NPTv6 251
Los vecinos en caché ND no se traducen 251
Creación de una política NPTv6 252

NAT64 255

Descripción general de NAT64 256
Dirección IPv6 integrada en la dirección IPv4 257
Servidor DNS64 258
Detección de MTU de ruta 259
Comunicación de Pv6 iniciada 260
Configuración de NAT64 para la comunicación iniciada por IPv6 262
Configuración de NAT64 para la comunicación iniciada por IPv4 265
Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto 268

ECMP 271

Algoritmos de equilibrio de carga de ECMP 272
Configuración de ECMP en un enrutador virtual 274
Habilitación de ECMP para varios sistemas BGP autónomos 277
Verificación de ECMP 278

LLDP 279

Descripción general de LLDP 280
TLV compatibles con LLDP 281
Mensajes de Syslog LLDP y capturas de SNMP 283
Configuración de LLDP 284
Visualización de estados y configuración de LLDP 286
Borrado de estadísticas de LLDP 288

BFD 289

Descripción general de BFD 290
Modelo, interfaz y soporte al cliente de BFD 291
Componentes RFC no compatibles de BFD 291
BFD para rutas estáticas 291
BFD para protocolos de enrutamiento dinámico 292
Configuración de BFD 293
Referencia: Detalles de BFD 300

Configuración de sesión y tiempos de espera de sesión 305

Sesiones de capa de transporte....306
TCP....307
Temporizadores de TCP semicerrado y de Tiempo de espera TCP....307
Temporizador RST sin verificar....309
Descarte de paquetes de protocolo de enlace dividido de TCP....309
Tamaño de segmento máximo (MSS)....310
UDP....312
ICMP....313
Reglas de la política de seguridad basadas en paquetes ICMP e ICMPv6....313
Límite de tasa ICMPv6....314
Control de tipos y códigos específicos de ICMP o ICMPv6....315
Configuración de los tiempos de espera de sesión....316
Configuración de los ajustes de sesión....319
Política de distribución de sesiones....324
Descripciones de las políticas de distribución de sesiones....324
Cambio de la política de distribución de sesiones y visualización de las estadísticas....327
Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP....329

Inspección del contenido del túnel....331

Descripción general de la inspección del contenido del túnel....332
Configuración de la inspección del contenido del túnel....336
Visualización de actividad de túneles inspeccionados....344
Visualización de información del túnel en logs....345
Creación de un informe personalizado basado en el tráfico de túnel etiquetado....347
Deshabilitación de aceleración de túneles....348

Agente de paquetes de red....349

Descripción general del agente de paquetes de red....350
Cómo funciona el agente de paquetes de red....353
Preparación para implementar el agente de paquetes de red....355
Configuración de las cadenas de seguridad de puente transparente....358
Configuración de cadenas de seguridad de capa 3 enrutadas....364
Compatibilidad con HA del agente de paquetes de red....370
Cambios en la interfaz de usuario para agente de paquetes de red....371
Limitaciones del agente de paquetes de red....373
Solución de problemas del agente de paquetes de red....376

Networking

Todos los cortafuegos de próxima generación de Palo Alto Networks® proporcionan una arquitectura de red flexible que incluye la compatibilidad con el enrutamiento dinámico, la conmutación y la conectividad de VPN, lo que le permite implementar el cortafuegos en prácticamente cualquier entorno de red.

> Introducción a las redes

Introducción a las redes

Las redes son el componente fundamental de los cortafuegos porque deben poder recibir datos, procesarlos y reenviarlos. Al configurar los puertos Ethernet del cortafuegos, podrá elegir entre una implementación de interfaz de cable virtual, capa 2. capa 3 o AE. Además, para permitirle integrar una variedad de segmentos de red, podrá configurar diferentes tipos de interfaces en diferentes puertos.

Para comenzar a establecer las redes, primero debe acceder al tema Introducción de la Guía del administrador de PAN-OS®. Con esta aprenderá a segmentar la red y configurar interfaces y zonas; en esa tarea inicial, se ilustra cómo configurar interfaces de capa 3 para conectarse a Internet, la red interna y las aplicaciones del centro de datos.

En esta Guía del administrador de redes de PAN-OS, se desarrolla esa información con temas sobre cómo configurar las interfaces tap, cable virtual, capa 2, capa 3 y AE. Tras configurar las interfaces de red, puede realizar la Exportación de los datos de la tabla de configuración como PDF o CSV para realizar una revisión o una auditoría internas.

En esta guía, también se explica cómo el cortafuegos admite varios enrutadores virtuales para obtener rutas de capa 3 de otras subredes y para mantener conjuntos de rutas distintos. En los capítulos restantes, se describen las rutas estáticas, los protocolos de enrutamiento dinámico y las principales funciones que admiten la creación de redes en el cortafuegos.

- Configuración de interfaces
- Enrutadores virtuales
- Rutas de servicio
- Rutas estáticas
- RIP
- OSPF
- BGP
- IP de multidifusión
- Redistribución de ruta
- Túneles GRE
- DHCP
- DNS:
- DDNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD
- Configuración de sesión y tiempos de espera de sesión

- Inspección del contenido del túnel
- Agente de paquetes de red

Configuración de interfaces

Un cortafuegos de última generación de Palo Alto Networks® puede funcionar en varias implementaciones a la vez porque estas se producen en el nivel de la interfaz. Por ejemplo, puede configurar algunas interfaces para que las interfaces de capa 3 integren el cortafuegos a su entorno de enrutamiento dinámico y configurar otras interfaces de modo que se integren en su red de conmutación de capa 2. En los siguientes temas, se describe cada tipo de implementación de interfaz y cómo configurarlo, además de cómo configurar Bonjour Reflector y cómo usar los perfiles de gestión de interfaz.

> Interfaces de modo tap
> Interfaces de cable virtual
> Interfaces de capa 2
> Interfaces de capa 3
> Configuración de los grupos de interfaces de agregación
> Configuración del reflector de Bonjour para la segmentación de red
> Uso de los perfiles de gestión de interfaz para restringir el acceso

Interfaces de modo tap

Un tap de red es un dispositivo que proporciona acceso a los datos que atraviesan una red de equipos. La implementación del modo tap permite supervisar de forma pasiva los flujos de tráfico a través de una red mediante un conmutador SPAN o un puerto espejo.

El puerto SPAN o de espejo permite copiar el tráfico de otros puertos en el conmutador. Al configurar una interfaz del cortafuegos como interfaz de modo tap y conectarla con un puerto SPAN de conmutación, este puerto proporciona al cortafuegos un reflejo del tráfico. De esta forma es posible visualizar la aplicación en la red sin necesidad de estar en el flujo del tráfico de red.

Al implementar el cortafuegos en modo tap, obtiene visibilidad sobre las aplicaciones que están ejecutando en la red sin tener que realizar ningún cambio en su diseño. En este modo, el cortafuegos también puede identificar las amenazas que se ciernen sobre la red. No obstante, tenga en cuenta que no hay tráfico en el cortafuegos en este modo, por lo que no puede realizar ninguna acción sobre él, como bloquear el tráfico con amenazas o aplicar el control del tráfico con QoS.

Para configurar una interfaz de modo tap y empezar a supervisar las aplicaciones de la red y las amenazas que se ciernen sobre ella:

STEP 1 | Decida el puerto que desea utilizar como interfaz de modo tap y conéctelo a un conmutador configurado con SPAN, RSPAN o reflejo de puertos.

El tráfico de la red se envía desde el puerto SPAN de destino por el cortafuegos, de modo que obtenga visibilidad sobre las aplicaciones de la red y las amenazas que se ciernen sobre ella.

STEP 2 | En la interfaz web del cortafuegos, configure la interfaz que desea utilizar en el modo tap de la red.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz que corresponde al puerto que acaba de cablear.
2. Seleccione **Tap** en **Interface Type (Tipo de interfaz)**.
3. En la pestaña **Config (Configuración)**, expanda **Security Zone (Zona de seguridad)** y seleccione **New Zone (Nueva zona)**.
4. En el cuadro de diálogo Zone (Zona), introduzca el nombre de la zona en **Name (Nombre)** (por ejemplo, TapZone [ZonaTap]) y haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Cree los perfiles de reenvío que desea utilizar.

- Configure el reenvío de logs.
- Configure la supervisión de syslog.

STEP 4 | Cree perfiles de seguridad para analizar el tráfico de red en busca de amenazas:

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)**.
2. En cada uno de los tipos de perfiles de seguridad, haga clic en **Add (Añadir)** para añadir un perfil nuevo y configure la acción en **alert (alertar)**.

   Como el cortafuegos no está en línea con el tráfico, no se pueden especificar las acciones de bloqueo ni de restablecimiento. Al configurar la alerta como acción, ve todas las amenazas que detecta el cortafuegos en los logs y en el centro de control de aplicaciones (application command center, ACC).

STEP 5 | Cree una regla de la política de seguridad para permitir el tráfico en la interfaz de modo tap.

Cuando cree una regla de la política de seguridad para el modo tap, las zonas de origen y de destino deben ser la misma.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y haga clic en **Add (Añadir)**.
2. En la pestaña **Source (Origen)**, configure **Source Zone (Zona de origen)** en la zona TapZone (ZonaTap) que acaba de crear.
3. En la pestaña **Destination (Destino)**, configure **Destination Zone (Zona de destino)** también en la zona TapZone (ZonaTap).
4. Configure todos los criterios de coincidencia con la regla, **Applications (Aplicaciones)**, **User (Usuario)**, **Service (Servicio)** y **Address Dirección)**, en **any (cualquiera)**.
5. En la pestaña **Actions (Acciones)** establezca la **Action Setting (Configuración de acción)** en **Allow (Permitir)**.
6. Configure **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)** y seleccione todos los perfiles de seguridad que ha creado para alertar sobre las amenazas.
7. Verifique que **Log at Session End** esté habilitado.
8. Haga clic en **OK (Aceptar)**.
9. Coloque la regla al principio de la base de reglas.

STEP 6 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

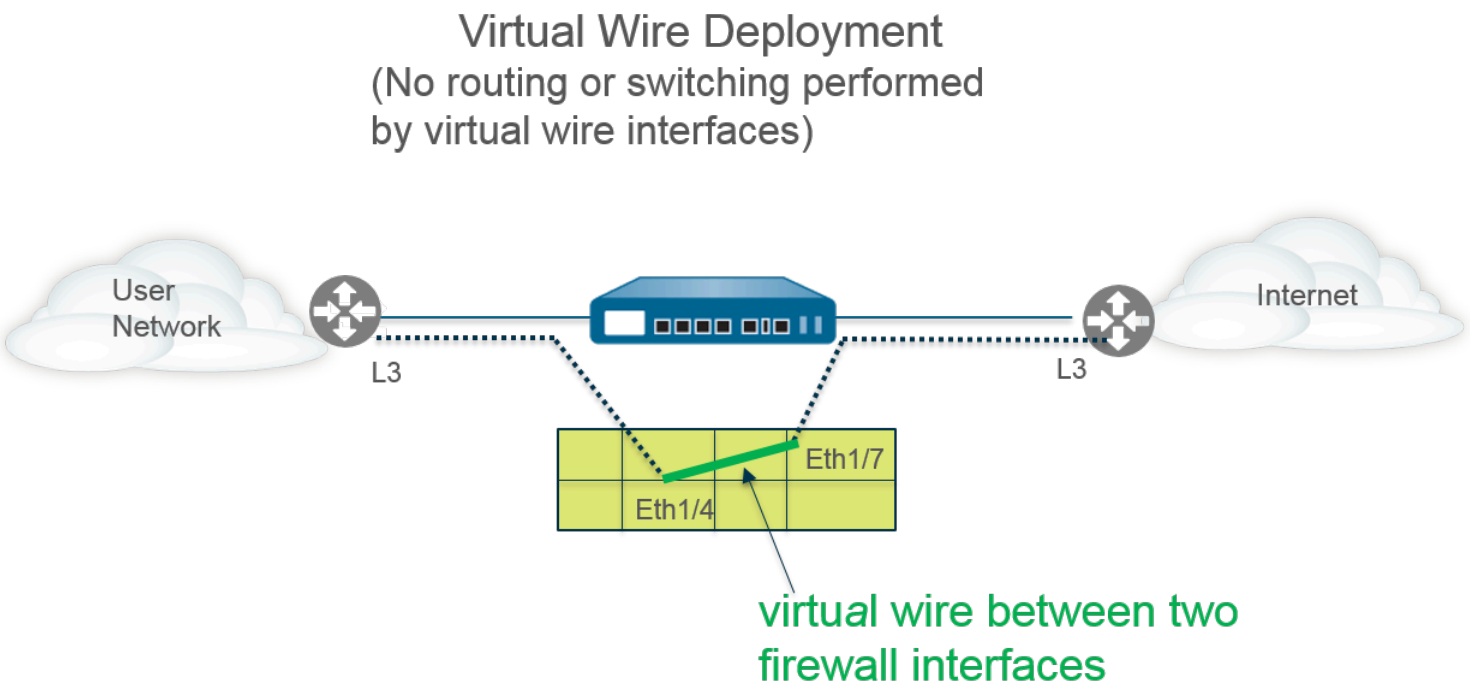
STEP 7 | Supervise los logs del cortafuegos con **Monitor (Supervisar)** > **Logs (Logs)** y el **ACC** para obtener información sobre las aplicaciones de la red y las amenazas que se ciernen sobre ella.

Interfaces de cable virtual

En una implementación de cable virtual, debe instalar un cortafuegos de forma transparente en un segmento de red uniendo dos puertos (interfaces) del cortafuegos. Evidentemente, el cable virtual conecta dos interfaces; por lo tanto, el cable virtual es un componente interno del cortafuegos.

Utilice una implementación de cable virtual solo cuando desee integrar sin inconvenientes un cortafuegos en una topología y las dos interfaces conectadas en el cortafuegos no deben llevar a cabo conmutación o enrutamiento. En el caso de estas dos interfaces, el cortafuegos se considera como ***puesto en el cable (bump-in-the-wire)***.

Una implementación de cable virtual simplifica la instalación y la configuración del cortafuegos debido a que puede insertar el cortafuegos en una topología existente sin asignar direcciones MAC o IP a las interfaces, rediseñar la red o reconfigurar los dispositivos de red alrededor. El cable virtual admite el bloqueo o el permiso de tráfico en función de etiquetas de la LAN virtual (VLAN), además de admitir reglas de la política de seguridad, App-ID, Content-ID, User-ID, cifrado, LLDP, HA activa/pasiva y activa/activa, QoS, protección de zona (con algunas excepciones), protección de protocolo no IP, protección contra DoS, protección del búfer de paquetes, inspección del contenido del túnel y NAT.



Cada interfaz de cable virtual está conectada directamente a un dispositivo o host de red de capa 2 o capa 3. Las interfaces de cable virtual no tienen direcciones de capa 2 o capa 3. Cuando una de las interfaces de cable virtual recibe una trama o paquete, ignora cualquier dirección de capa 2 o de capa 3 con fines de conmutación o enrutamiento, pero se aplica a sus reglas de la política de seguridad o de NAT antes de pasar una trama o paquete permitida en el cable virtual a la segunda interfaz y hacia el dispositivo de red conectado a ella.

No debe utilizar una implementación de cable virtual para las interfaces que deben admitir conmutación, túneles VPN o enrutamiento debido a que requieren una dirección de capa 2 o capa 3.

Una interfaz de cable virtual no utiliza un perfil de gestión de interfaces, que controla servicios como HTTP y ping, y, por lo tanto, requiere que la interfaz cuente con una dirección IP.

Todos los cortafuegos que se envían desde la fábrica cuentan con dos puertos Ethernet (puerto 1 y 2) preconfigurados como interfaces de cable virtual, y estas interfaces permiten todo el tráfico sin etiquetas.

Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Si el cortafuegos está en alguno de esos modos, puede inspeccionar el tráfico etiquetado y ofrecer prevención contra amenazas.

Si no desea utilizar el cable virtual preconfigurado, debe eliminar esta configuración para evitar que interfiera con otra configuración del cortafuegos. Consulte el Establecimiento de acceso a la red para servicios externos**.**

- Paquetes de capa 2 y capa 3 en un cable virtual
- Velocidad de puertos en las interfaces de cable virtual
- LLDP en un cable virtual
- Interfaces agregadas para un cable virtual
- Compatibilidad del cable virtual con la alta disponibilidad
- Protección de zona para una interfaz de cable virtual
- Tráfico con etiqueta de VLAN
- Subinterfaces de Virtual Wire
- Configuración de cables virtuales

Paquetes de capa 2 y capa 3 en un cable virtual

Una interfaz de cable virtual permitirá que los paquetes de capa 2 y capa 3 procedentes de dispositivos conectados pasen de manera transparente siempre que las políticas que se aplican a la zona o a la interfaz permitan el tráfico. Las interfaces de cable virtual no participan en el enrutamiento o la conmutación.

Por ejemplo, el cortafuegos no reduce el TTL en un paquete de traceroute hacia el enlace virtual debido a que el enlace es transparente y no cuenta como un salto. Los paquetes como las unidades de datos de protocolo (PDU) de operaciones, administración y mantenimiento (OAM), por ejemplo, no finalizan en el cortafuegos. Por lo tanto, el cable virtual permite que el cortafuegos mantenga una presencia transparente actuando como un enlace de paso, mientras que proporciona servicios de seguridad, NAT y QoS.

Con el fin de que las unidades de datos para protocolo puente (BPDU) y otros paquetes de control de capa 2 (que, por lo general, no se etiquetan) pasen por un cable virtual, las interfaces deben adjuntarse a un objeto de cable virtual que permita el tráfico no etiquetado. Esta es la configuración predeterminada. Si el campo **Tag Allowed (Etiqueta permitida)** del objeto de cable virtual está vacío, el cable virtual permite tráfico no etiquetado. (Las reglas de la política de seguridad no se aplican a los paquetes de capa 2).

Para que los paquetes de control (de capa 3) de enrutamiento pasen por un cable virtual, debe aplicar una regla de la política de seguridad que permita el paso de tráfico. Por ejemplo, aplique una regla de la política de seguridad que permita una aplicación como BGP o OSPF.

Si desea poder aplicar reglas de la política de seguridad a una zona para el tráfico IPv6 que llega a una interfaz de cable virtual en el cortafuegos, habilite el cortafuegos IPv6. De lo contrario, el tráfico IPv6 se reenviará de manera transparente por el cable.

Si habilita el cortafuegos de multidifusión para un objeto de cable virtual y lo aplica a una interfaz de cable virtual, el cortafuegos inspecciona el tráfico multidifusión y lo reenvía o no, en función de las reglas de la política de seguridad. Si no habilita el cortafuegos de multidifusión, el cortafuegos reenviará el tráfico de multidifusión de manera transparente.

La fragmentación en un cable virtual se produce de igual manera que en otros modos de implementación de la interfaz.

Velocidad de puertos en las interfaces de cable virtual

Los diferentes modelos de cortafuegos proporcionan varios puertos de cobre y de fibra óptica, que funcionan a diferente velocidad. Un cable virtual puede unir dos puertos Ethernet del mismo tipo (ambos de cobre o ambos de fibra óptica) o unir un puerto de cobre con un puerto de fibra óptica. De manera predeterminada, la **Link Speed (Velocidad del enlace)** de los puertos de cobre en el cortafuegos se establece en **auto (automático)**, lo que significa que el cortafuegos negocia automáticamente su velocidad y modo de transmisión (**Link Duplex [Dúplex de enlace]**). Cuando realiza la Configuración de cables virtuales, también puede seleccionar una **Link Speed (Velocidad del enlace)** y un **Link Duplex (Dúplex de enlace)** específicos, pero los valores de estos ajustes deben ser iguales en ambos puertos de cualquier cable virtual.

LLDP en un cable virtual

Las interfaces de cable virtual pueden utilizar LLDP para encontrar dispositivos vecinos y sus capacidades, y el LLDP permite a los dispositivos vecinos detectar la presencia del cortafuegos en la red. LLDP facilita la resolución de problemas, especialmente en el caso de implementaciones de cable virtual donde el cortafuegos suele pasar desapercibido debido a un ping o traceroute que pasa por un cable virtual. LLDP proporciona un método para que los dispositivos detecten el cortafuegos en la red. Sin el LLDP, es prácticamente imposible que los sistemas de gestión de redes detecten la presencia de un cortafuegos mediante el enlace virtual.

Interfaces agregadas para un cable virtual

Puede Configurar un grupo de interfaces agregadas de interfaces de cable virtual, pero los cables virtuales no utilizan el LACP. Si configura el LACP en dispositivos que se conectan el cortafuegos a otras redes, el cable virtual pasará paquetes del LACP de manera transparente sin realizar las funciones del LACP.

Para que los grupos de interfaces agregados funcionen correctamente, asegúrese de que todos los enlaces del mismo grupo de LACP en el mismo lado del cable virtual se asignen a la misma zona.

Compatibilidad del cable virtual con la alta disponibilidad

Si configura el cortafuegos para realizar la supervisión de rutas para la alta disponibilidad utilizando un grupo de rutas de cable virtual, el cortafuegos intenta resolver el ARP de la dirección IP de destino configurada enviando paquetes de ARP de ambas interfaces de cable virtual. La dirección IP de destino que supervisa debe permanecer en la misma subred que uno de los dispositivos alrededor del cable virtual.

Las interfaces de cable virtual admiten HA activa/pasiva y activa/activa. En implementaciones de HA activa/activa con un cable virtual, los paquetes examinados deben devolverse al cortafuegos de destino para conservar la ruta de reenvío. Por lo tanto, si un cortafuegos recibe un paquete que pertenece a la sesión que el cortafuegos de HA del peer posee, lo devuelve mediante el enlace HA3 al peer.

Puede configurar el cortafuegos pasivo en un par de HA para permitir que los dispositivos del par en ambos lados del cortafuegos negocien con anterioridad el LLDP y LACP mediante un cable virtual antes de que se produzca una conmutación de error de HA. Una configuración que garantice la Negociación previa de LACP y LLDP para HA activa/pasiva acelera las conmutaciones por error de HA.

Protección de zona para una interfaz de cable virtual

Puede aplicar protección de zona a una interfaz de cable virtual, pero, dado que las interfaces de cable virtual no realizan el enrutamiento, no puede aplicar protección de ataques basados en paquetes a los paquetes provenientes de una dirección IP falsa ni suprimir los paquetes de error vencidos de TTL ICMP ni los paquetes que requieren fragmentación de ICMP.

De manera predeterminada, una interfaz de cable virtual reenvía todo el tráfico no IP que recibe. Sin embargo, puede aplicar un perfil de protección de zona con protección de protocolos para bloquear o permitir determinados paquetes de protocolo no IP entre las zonas de seguridad en un cable virtual.

Tráfico con etiqueta de VLAN

Las interfaces de cable virtual predeterminadas permiten todo el tráfico sin etiquetas. No obstante, puede utilizar un cable virtual para conectar dos interfaces y configurarlas para que bloqueen o permitan el tráfico basándose en las etiquetas de LAN virtual (VLAN). La etiqueta VLAN 0 indica el tráfico sin etiquetar.

También puede crear varias subinterfaces, añadirlas a diferentes zonas y, a continuación, clasificar el tráfico de acuerdo con una etiqueta VLAN, o una combinación de una etiqueta VLAN con clasificadores IP (dirección, intervalo o subred) para aplicar un control detallado de las políticas para etiquetas VLAN específicas o para etiquetas VLAN de una dirección IP de origen, intervalo o subred en concreto.

Subinterfaces de Virtual Wire

Las implementaciones de cable virtual pueden usar subinterfaces de cable virtual para separar el tráfico en zonas. Las subinterfaces de Virtual Wire ofrecen flexibilidad a la hora de aplicar distintas políticas cuando necesita gestionar el tráfico de varias redes de clientes. Las subinterfaces le permiten separar y clasificar el tráfico en diferentes zonas (las zonas pueden pertenecer a sistemas virtuales separados, si es necesario) utilizando los siguientes criterios:

- **Etiquetas de la VLAN**: el ejemplo de Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN) muestra un ISP que utiliza subinterfaces de Virtual Wire con etiquetas VLAN para separar el tráfico para dos clientes diferentes.
- **Etiquetas VLAN junto con clasificadores IP (dirección, intervalo o subred)**: el siguiente ejemplo muestra un ISP con dos sistemas virtuales separados en un cortafuegos que gestiona el tráfico de dos clientes diferentes. En cada sistema virtual, el ejemplo ilustra cómo se utilizan las subinterfaces de Virtual Wire con etiquetas VLAN y clasificadores IP para clasificar el tráfico en zonas separadas y aplicar la política relevante para los clientes de cada red.

Flujo de trabajo de subinterfaces de Virtual Wire

- Configure dos interfaces Ethernet con el tipo Virtual Wire y asigne estas interfaces a un Virtual Wire.

- Cree subinterfaces en el Virtual Wire principal para separar el tráfico del cliente A del cliente B. Asegúrese de que las etiquetas VLAN definidas en cada par de subinterfaces configuradas como Virtual Wire sean idénticas. Esto es esencial, porque un Virtual Wire no conmuta etiquetas VLAN.

- Cree nuevas subinterfaces y defina clasificadores IP. Esta tarea es opcional y solamente es necesaria si desea añadir subinterfaces adicionales con clasificadores IP para gestionar de manera más exhaustiva el tráfico de un cliente basándose en la combinación de etiquetas VLAN y una dirección IP de origen, intervalo o subred en concreto.

También puede utilizar clasificadores IP para gestionar el tráfico sin etiquetar. Para ello, debe crear una subinterfaz con la etiqueta VLAN "0" y definir subinterfaces con clasificadores IP para gestionar el tráfico sin etiquetar mediante clasificadores IP.

La clasificación de IP solamente puede utilizarse en las subinterfaces asociadas con un lado del Virtual Wire. Las subinterfaces definidas en el lado correspondiente del Virtual Wire deben utilizar la misma etiqueta VLAN, pero no deben incluir un clasificador IP.

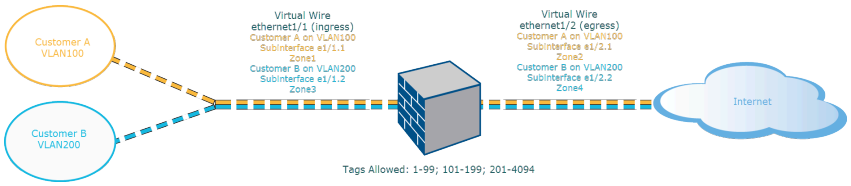


Figure 1: Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN)

Implementación de Virtual Wire con subinterfaces (únicamente etiquetas VLAN) muestra al cliente A y al cliente B conectados al cortafuegos mediante una interfaz física, Ethernet 1/1, configurada como Virtual Wire, que es la interfaz de entrada. Una segunda interfaz física, Ethernet1/2, también forma parte del Virtual Wire y se utiliza como la interfaz de salida que proporciona acceso a internet.

Para el cliente A, también tiene las subinterfaces Ethernet 1/1.1 (entrada) y Ethernet 1/2.1 (salida). Para el cliente B, tiene las subinterfaces Ethernet 1/1.2 (entrada) y Ethernet 1/2.2 (salida). Cuando configure las subinterfaces, debe asignar la etiqueta VLAN y la zona correctas para aplicar las políticas a cada uno de los clientes. En este ejemplo, las políticas del cliente A se crean entre la zona 1 y la zona 2, y las políticas del cliente B se crean entre la zona 3 y la zona 4.

Cuando el tráfico entre en el cortafuegos desde el cliente A o el cliente B, la etiqueta VLAN del paquete entrante primero deberá coincidir con la etiqueta VLAN definida en las subinterfaces de entrada. En este ejemplo, solo una subinterfaz coincide con la etiqueta VLAN en el paquete entrante, por lo que se seleccionará esa subinterfaz. Las políticas definidas para la zona se evalúan y aplican antes de que el paquete salga de la subinterfaz correspondiente.

*No debe definirse la misma etiqueta VLAN en la interfaz del Virtual Wire principal y la subinterfaz. Verifique que las etiquetas VLAN definidas en la lista Tag Allowed (Etiquetas permitidas) de la interfaz de Virtual Wire principal (**Network [Red] > Virtual Wires [Cables virtuales]**) no se incluyan en una subinterfaz.*

Implementación de Virtual Wire con subinterfaces (etiquetas VLAN y clasificadores IP) muestra al cliente A y al cliente B conectados a un cortafuegos físico que tiene dos sistemas virtuales (vsys), además del sistema virtual predeterminado (vsys1). Cada sistema virtual es un cortafuegos virtual independiente que se gestiona por separado para cada cliente. Cada vsys tiene adjuntadas interfaces/subinterfaces y zonas de seguridad que se gestionan de manera independiente.

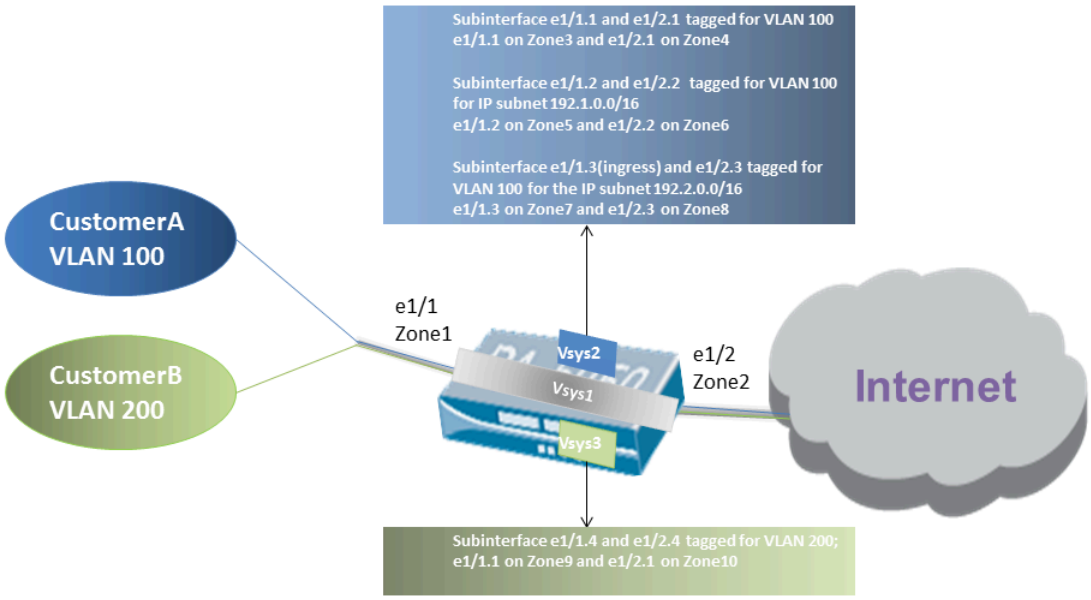


Figure 2: Implementación de Virtual Wire con subinterfaces (etiquetas VLAN y clasificadores IP)

Vsys1 está configurado para utilizar las interfaces físicas Ethernet 1/1 y Ethernet 1/2 como Virtual Wire; Ethernet 1/1 es la interfaz de entrada y Ethernet 1/2 es la interfaz de salida que proporciona el acceso a Internet. Este Virtual Wire está configurado para aceptar todo el tráfico etiquetado y sin etiquetar a excepción de las etiquetas VLAN 100 y 200, que están asignadas a las subinterfaces.

El cliente A se gestiona en vsys2 y el cliente B se gestiona en vsys3. En vsys2 y vsys3, se crean las siguientes subinterfaces de Virtual Wire con las etiquetas VLAN y las zonas adecuadas para aplicar las medidas incluidas en las políticas.

Cliente	Vsys	Subinterfaces de Vwire	Zona	Etiqueta VLAN	Clasificador IP
A	2	e1/1.1 (entrada) e1/2.1 (salida)	Zone3 Zone4	100 100	ninguno
	2	e1/1.2 (entrada) e1/2.2 (salida)	Zone5 Zone6	100 100	Subred IP 192.1.0.0/16
	2	e1/1.3 (entrada) e1/2.3 (salida)	Zone7 Zone8	100 100	Subred IP 192.2.0.0/16
B	3	e1/1.4 (entrada) e1/2.4 (salida)	Zone9 Zone10	200 200	ninguno

Cuando el tráfico entre en el cortafuegos desde el cliente A o el cliente B, la etiqueta VLAN del paquete entrante primero deberá coincidir con la etiqueta VLAN definida en las subinterfaces de entrada. En este caso, para el cliente A, hay varias subinterfaces que utilizan la misma etiqueta VLAN. De este modo, el cortafuegos primero acota la clasificación a una subinterfaz basándose en la dirección IP de origen del paquete. Las políticas definidas para la zona se evalúan y aplican antes de que el paquete salga de la subinterfaz correspondiente.

Para el tráfico de ruta de retorno, el cortafuegos compara la dirección IP de destino del modo definido en el clasificador IP en la subinterfaz del cliente y selecciona el Virtual Wire adecuado para enrutar el tráfico a través de la subinterfaz precisa.

*No debe definirse la misma etiqueta VLAN en la interfaz del Virtual Wire principal y la subinterfaz. Verifique que las etiquetas VLAN definidas en la lista Tag Allowed (Etiquetas permitidas) de la interfaz de Virtual Wire principal (**Network [Red] > Virtual Wires [Cables virtuales]**) no se incluyan en una subinterfaz.*

Configuración de cables virtuales

La siguiente tarea muestra cómo configurar dos Interfaces de cable virtual (Ethernet 1/3 y Ethernet 1/4 en este ejemplo) para crear un cable virtual. Las dos interfaces deben tener la misma **Link Speed (Velocidad de enlace)** y el mismo modo de transmisión (**Link Duplex [Dúplex de enlace]**). Por ejemplo, un puerto de cobre de 1000 Mbps de dúplex completo se corresponde con un puerto de fibra óptica de 1 Gbps de dúplex completo.

STEP 1 | Cree la primera interfaz de cable virtual.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz que haya conectado por cable (**ethernet1/3** en este ejemplo).
2. Establezca el **Interface Type (Tipo de interfaz)** en **Virtual Wire (Cable virtual)**.

STEP 2 | Conecte la interfaz a un objeto de cable virtual.

1. En la misma interfaz de Ethernet, seleccione **Virtual Wire (Cable virtual)** en la pestaña **Config (Configuración)** y haga clic en **New Virtual Wire (Nuevo cable virtual)**.
2. Introduzca un **Name (Nombre)** para el cable virtual.
3. Para **Interface1**, seleccione la interfaz que acaba de configurar (**ethernet1/3**). En la lista solo aparecen las interfaces configuradas como interfaces de cable virtual.
4. Para **Tag Allowed (Etiqueta permitida)**, introduzca **0** para indicar que el tráfico sin etiquetar (como BPDU y otro tráfico de control de capa 2) está permitido. La ausencia de una etiqueta implica una etiqueta de 0. Ingrese números enteros de etiquetas permitidas adicionales o intervalos de etiquetas, separados por coma (el valor predeterminado es 0; el intervalo es de 0 a 4094).
5. Seleccione **Multicast Firewalling (Cortafuegos de multidifusión)** si desea poder aplicar reglas de política de seguridad al tráfico de multidifusión que atraviesa el cable virtual. De lo contrario, el tráfico de multidifusión se envía de manera transparente por el cable virtual.
6. Seleccione **Link State Pass Through (Paso del estado del enlace)**, para que el cortafuegos pueda funcionar de manera transparente. Cuando el cortafuegos detecta un estado inactivo para un enlace de cable virtual, desactiva la otra interfaz en el par de cable virtual. Por lo tanto, los dispositivos en ambos lados del cortafuegos ven un estado de enlace constante, como si no hubiera un cortafuegos entre ellos. Si no selecciona esta opción, el estado del enlace no se propaga por el cable virtual.
7. Haga clic en **OK (Aceptar)** para guardar el objeto de cable.

STEP 3 | Determine la velocidad del enlace de la interfaz de cable virtual.

1. Mientras esté en la misma interfaz Ethernet, seleccione **Advanced (Avanzado)** y registre o cambie la **Link Speed (Velocidad de enlace)**. El tipo de puerto condiciona los ajustes de velocidad disponibles en la lista. De manera predeterminada, los puertos de cobre se configuran en **auto (automático)** para negociar la velocidad del enlace. Ambas interfaces de cable virtual deben tener la misma velocidad de enlace.
2. Haga clic en **OK (Aceptar)** para guardar la interfaz de Ethernet.

STEP 4 | Configure la segunda interfaz de cable virtual (**ethernet1/4** en este ejemplo) repitiendo los pasos anteriores.

Cuando selecciona el objeto de **Virtual Wire (Cable virtual)** que creó, el cortafuegos añade automáticamente la segunda interfaz de cable virtual como **Interface2**.

STEP 5 | Cree una zona de seguridad diferente para cada una de las interfaces de cable virtual.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y **Add (Añadir)** para añadir una zona.
2. Introduzca un nombre para la zona en **Name (Nombre)**, (como **`internet`**).
3. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica la zona.
4. Para **Type (Tipo)**, seleccione **Virtual Wire (Cable virtual)**.
5. Haga clic en **Add (Añadir)** para añadir la **Interface (Interfaz)** que pertenezca a la zona.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | (Opcional) Cree reglas de política de seguridad para permitir el paso del tráfico de capa 3.

Para permitir el tráfico de capa 3 en el cable virtual, cree una regla de política de seguridad para permitir el tráfico desde la zona de usuario a la zona de Internet, y otra para permitir el tráfico desde la zona de Internet a la zona de usuario, al seleccionar las aplicaciones que desea permitir, tal como BGP u OSPF.

STEP 7 | (Opcional) Habilite los cortafuegos IPv6.

Si desea poder aplicar reglas de política de seguridad al tráfico IPv6 que llega a la interfaz de cable virtual, habilite los cortafuegos IPv6. De lo contrario, el tráfico IPv6 se enviará de manera transparente.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

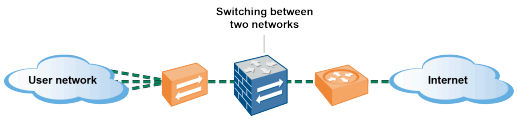
STEP 8 | **Commit (Confirmar)** los cambios.

STEP 9 | (Opcional) Configure un perfil LLDP y aplíquelo a las interfaces de cable virtual (consulte Configuración de LLDP).

STEP 10 | (Opcional) Aplique el control de protocolo no IP a las zonas de cable virtual (consulte Configuración de la protección de protocolos). De lo contrario, todo el tráfico no IP se reenviará por el cable virtual.

Interfaces de capa 2

En una implementación de capa 2, el cortafuegos permite cambiar entre dos o más redes. Los dispositivos se conectan a una trama de capa 2; el cortafuegos reenvía las tramas al puerto adecuado, que se asocia a la dirección MAC que se identifica en la trama. Realice la Configuración de una interfaz de capa 2 cuando se requiera la conmutación.



Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Si el cortafuegos está en alguno de esos modos, puede inspeccionar el tráfico etiquetado y ofrecer prevención contra amenazas.

Los siguientes temas describen los diferentes tipos de interfaces de capa 2 que puede configurar para cada tipo de implementación que necesita, lo que incluye los detalles sobre la utilización de LAN virtuales (VLAN) para la separación del tráfico y la política en los grupos. En otro tema se describe cómo el cortafuegos reescribe el número de ID de VLAN del puerto entrante en un árbol de conmutación por VLAN (PVST+) de Cisco o una unidad de datos para protocolo puente (BPDU) de PVST+ rápido.

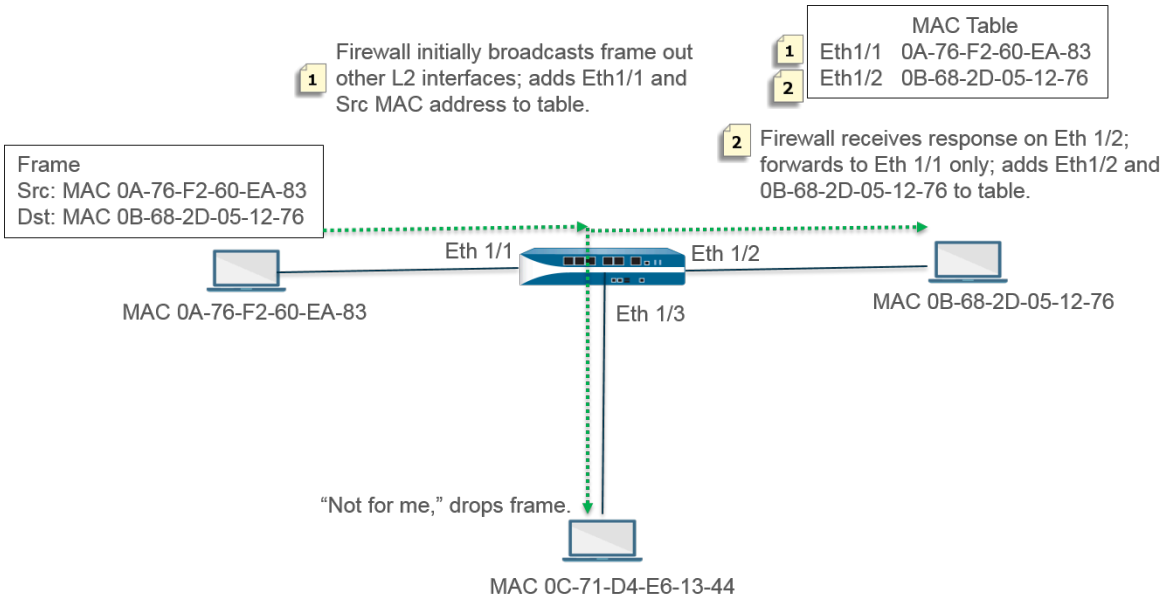
- Interfaces de capa 2 sin LAN
- Interfaces de capa 2 con LAN
- Configure la interfaz de capa 2
- Configuración de una interfaz de capa 2, una subinterfaz y una VLAN
- Gestión de la reescritura de BPDU del árbol de conmutación por VLAN (Per-VLAN Spanning Tree, PVST+)

Interfaces de capa 2 sin LAN

Realice la Configuración de una interfaz de capa 2 en el cortafuegos, de modo que pueda actuar como un conmutador en su red de capa 2 (no en el borde de la red). Probablemente, los hosts de capa 2 se encuentran cercanos geográficamente y pertenecen a un dominio de difusión único. El cortafuegos proporciona seguridad entre los hosts de capa 2 cuando asigna las interfaces a las zonas de seguridad y aplica las reglas de seguridad a las zonas.

Los hosts se comunican con el cortafuegos y entre sí en la capa 2 del modelo OSI intercambiando tramas. Una trama contiene un encabezado Ethernet que incluye una dirección de control de acceso a los medios (MAC), que es una dirección de hardware físico. Las direcciones MAC son números hexadecimales de 48 bits con formato de seis octetos separados por dos puntos o guiones (por ejemplo, 00-85-7E-46-F1-B2).

La siguiente figura tiene un cortafuegos con interfaces de capa 2 que se conectan a un host de capa 2 en una asignación de uno a uno.



El cortafuegos comienza con una tabla MAC vacía. Cuando el host con dirección de origen 0A-76-F2-60-EA-83 envía una trama al cortafuegos, el cortafuegos no cuenta con una dirección de destino 0B-68-2D-05-12-76 en su tabla MAC, de modo que no sabe a qué interfaz reenviar la trama y difunde la trama a todas sus interfaces de capa 2. El cortafuegos introduce la dirección de origen 0A-76-F2-60-EA-83 y la dirección Eth1/1 asociada en su tabla MAC.

El host en 0C-71-D4-E6-13-44 recibe la difusión, pero la dirección MAC de destino no es su propia dirección MAC y, por lo tanto, descarta la trama.

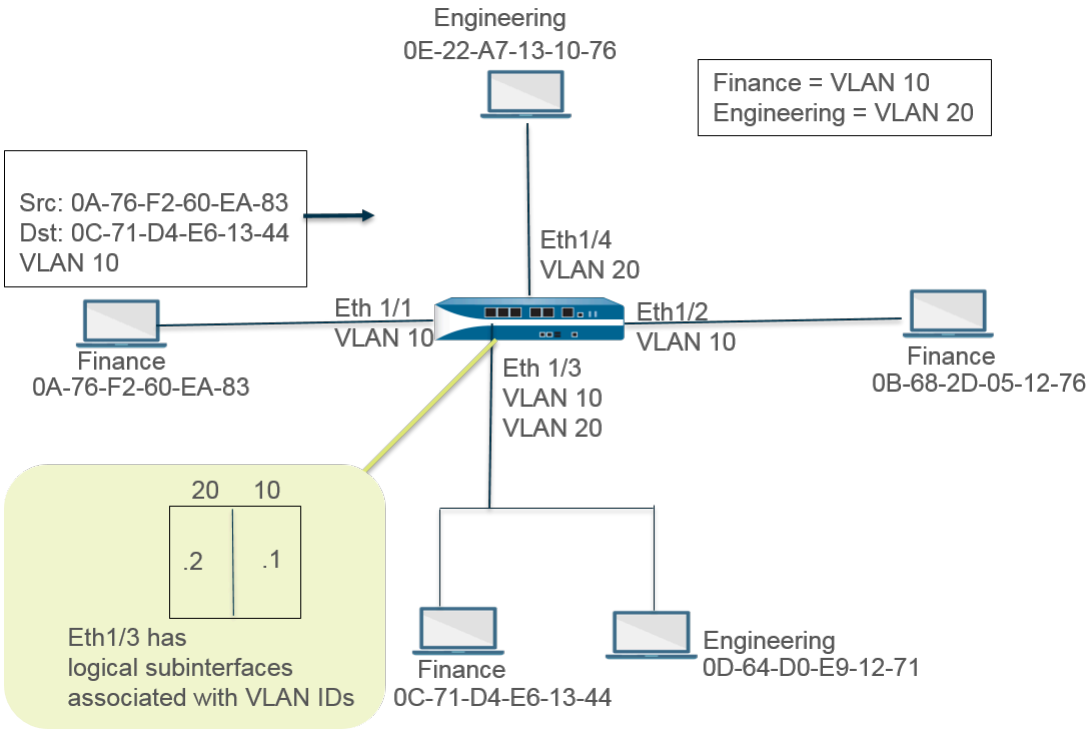
La interfaz de destino Ethernet 1/2 reenvía la trama a su host. Cuando el host 0B-68-2D-05-12-76 responde, utiliza la dirección de destino 0A-76-F2-60-EA-83 y el cortafuegos añade Ethernet 1/2 como la interfaz en su tabla MAC para alcanzar la dirección 0B-68-2D-05-12-76.

Interfaces de capa 2 con LAN

Cuando su organización desea dividir una LAN en LAN virtuales (VLAN) separadas para que el tráfico y las políticas de los diferentes departamentos permanezcan separados, puede agrupar los hosts de capa 2 en VLAN y, por lo tanto, dividir un segmento de red de capa 2 en dominios de difusión. Por ejemplo, puede crear VLAN para los departamentos de finanzas e ingeniería. Para ello, realice la Configuración de una interfaz de capa 2, una subinterfaz y una VLAN.

El cortafuegos actúa como conmutador para reenviar una trama con un encabezado Ethernet que contiene una ID de VLAN, y la interfaz de destino debe tener una subinterfaz con la ID de VLAN con el fin de recibir la trama y reenviarla al host. Puede configurar una interfaz de capa 2 en el cortafuegos y configurar una o más subinterfaces lógicas para el interfaz, cada una con una etiqueta (ID) de VLAN.

En la siguiente figura, el cortafuegos tiene cuatro interfaces de capa 2 que se conectan a hosts de capa 2 pertenecientes a diferentes departamentos dentro de una organización. La interfaz Ethernet 1/3 se configura con subinterfaz .1 (etiquetada con VLAN 10) y subinterfaz .2 (etiquetada con VLAN 20); por lo tanto, existen dos dominios de difusión en ese segmento. Los hosts en VLAN 10 pertenecen al departamento de finanzas; los hosts en VLAN 20 pertenecen al departamento de ingeniería.



En este ejemplo, el host en la dirección MAC 0A-76-F2-60-EA-83 envía una trama con VLAN ID 10 al cortafuegos y el cortafuegos lo difunde a sus otras interfaces de capa 2. La interfaz Ethernet 1/3 acepta la trama debido a que está conectada al host con la dirección de destino 0C-71-D4-E6-13-44 y se asigna la VLAN 10 a su subinterfaz .1. La interfaz Ethernet 1/3 reenvía la trama a su host de finanzas.

Configure la interfaz de capa 2

Configure las interfaces de capa 2 sin VLAN cuando desee una conmutación de capa 2 y no necesite un tráfico independiente en las VLAN.

STEP 1 | Configure la interfaz de capa 2.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz. El **Interface Name (Nombre de la interfaz)** es fijo, como ethernet1/1.
2. En **NAT Type (Tipo de NAT)**, seleccione **Layer2**.
3. Seleccione la pestaña **Config (Configuración)** y asigne la interfaz a una **Security Zone (Zona de seguridad)** o cree una **New Zone (Nueva zona)**.
4. Configure interfaces de capa 2 adicionales en el cortafuegos que se conecten a otros hosts de capa 2.

STEP 2 | Seleccione Confirmar.

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

Configuración de una interfaz de capa 2, una subinterfaz y una VLAN

Configure interfaces de capa 2 con VLAN cuando desee una conmutación de capa 2 y un tráfico independiente en las VLAN. De manera opcional, puede controlar protocolos no IP entre zonas de seguridad en una interfaz de capa 2 o entre interfaces dentro de una misma zona en una VLAN de capa 2.

STEP 1 | Configure una interfaz de capa 2 y una subinterfaz, y asigne una ID de VLAN.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz. El **Interface Name (Nombre de la interfaz)** es fijo, como ethernet1/1.
2. En **NAT Type (Tipo de NAT)**, seleccione **Layer2**.
3. Seleccione la pestaña **Config (Configuración)**.
4. En **VLAN**, conserve la configuración **None (Ninguno)**.
5. Asigne la interfaz a una **Security Zone (Zona de seguridad)** o cree una **New Zone (Nueva zona)**.
6. Haga clic en **OK (Aceptar)**.
7. Cuando la interfaz Ethernet esté resaltada, haga clic en **Add Subinterface (Añadir subinterfaz)**.
8. El campo **Interface Name (Nombre de interfaz)** permanece fijo. Tras el punto, introduzca el número de subinterfaz en el rango de 1 a 9999.
9. Introduzca una ID con una **Tag (Etiqueta)** de VLAN en el rango de 1 a 4094.
10. Asigne la interfaz a una **Security Zone (Zona de seguridad)**.
11. Haga clic en **OK (Aceptar)**.

STEP 2 | Seleccione Confirmar.

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

STEP 3 | (Opcional) Aplique un perfil de protección de zona con protección de protocolo para controlar paquetes de protocolo no IP entre zonas de capa 2 (o entre interfaces dentro de una zona de capa 2).

Configure la protección de protocolo.

Gestión de la reescritura de BPDU del árbol de conmutación por VLAN (Per-VLAN Spanning Tree, PVST+)

Cuando una interfaz del cortafuegos está configurada para una implementación de capa 2, el cortafuegos reescribe el número de ID de VLAN del puerto entrante (PVID) en un árbol de conmutación por VLAN (PVST+) Cisco o una unidad de datos para protocolo puente (BPDU) de PVST+ rápido con el número de ID de VLAN entrante adecuado y reenvía BPDU. Este comportamiento predeterminado a partir de PAN-OS 7.1 permite que el cortafuegos etiquete correctamente las tramas de PVST+ y PVST+ rápido de Cisco entre los conmutadores de Cisco en las VLAN a cada lado del cortafuegos para que la detección de bucle de árbol de expansión que utiliza Cisco PVST+ y PVST+ rápido pueda funcionar correctamente. El cortafuegos no participa en

el proceso de elección del protocolo de árbol de expansión (Spanning Tree Protocol, STP) y no hay ningún cambio de comportamiento para otros tipos de árbol de expansión.

El conmutador Cisco debe tener el loopguard deshabilitado para que PVST+ o la BPDU de PVST+ rápido reescriba la función correctamente en el cortafuegos.

Esta función solo es compatible con las interfaces Ethernet de capa 2 y de Ethernet de agregación (Aggregate Ethernet, AE). El cortafuegos admite un intervalo de PVID de 1 a 4094 con un ID de VLAN nativa de 1 para que sea compatible con la implementación de VLAN nativa de Cisco.

Para admitir la función de reescritura de BPDU de PVST+, PAN-OS admite el concepto de una VLAN nativa de PVST+. Las tramas enviadas a una VLAN nativa o enviadas desde ella no están etiquetadas con un PVID igual que la VLAN nativa. Todos los conmutadores y cortafuegos en la misma implementación de capa 2 deben tener la misma VLAN nativa para que PVST+ funcione correctamente. Aunque la VLAN nativa de Cisco se configura de forma predeterminada en vlan1, la ID de VLAN puede ser un número distinto de 1.

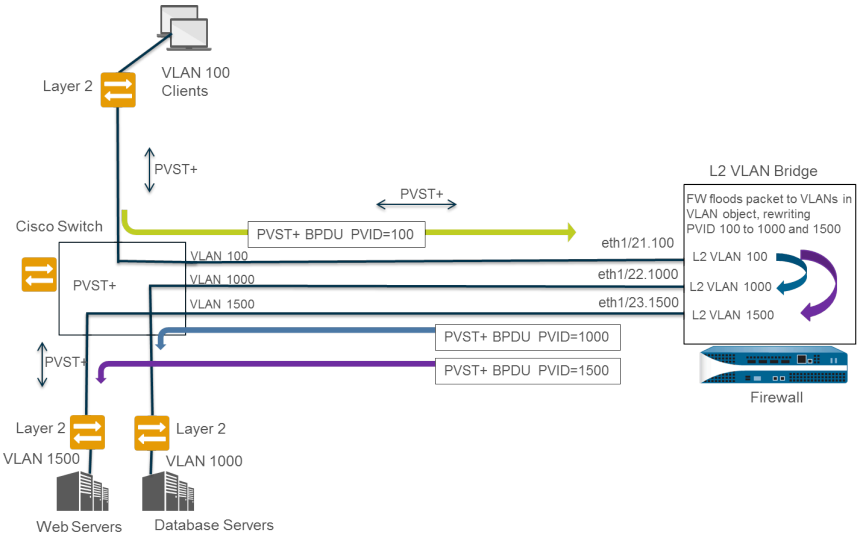
Por ejemplo, el cortafuegos está configurado con un objeto VLAN (denominado VLAN_BRIDGE), que describe las interfaces y subinterfaces que pertenecen a un conmutador o dominio de difusión. En este ejemplo, la VLAN incluye tres subinterfaces: ethernet1/21.100 con la etiqueta 100, ethernet1/22.1000 con la etiqueta 1000 y ethernet1/23.1500 con la etiqueta 1500.

Las subinterfaces que pertenecen a VLAN_BRIDGE tienen el siguiente aspecto:

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

En el siguiente gráfico y explicación se muestra la secuencia en la que el cortafuegos reescribe automáticamente la BPDU de PVST+:



1. El puerto del conmutador de Cisco que pertenece a la VLAN 100 envía una BPDUP de PVST+, con el PVID y la etiqueta VLAN 802.1Q establecida en 100, al cortafuegos.
2. Las interfaces y subinterfaces de cortafuegos están configuradas como un tipo de interfaz de capa 2. La subinterfaz de entrada en el cortafuegos tiene la etiqueta VLAN 100, que coincide con la etiqueta PVID y VLAN de la BPDU entrante, por lo que el cortafuegos acepta la BPDU. El cortafuegos inunda la BPDU de PVST+ en todas las demás interfaces que pertenecen al mismo objeto VLAN (en este ejemplo, ethernet1/22.1000 y ethernet1/23.1500). Si las etiquetas VLAN no coinciden, el cortafuegos descartará la BPDU.
3. Cuando el cortafuegos inunda la BPDU a través de otras interfaces (que pertenecen al mismo objeto VLAN), reescribe el PVID y cualquier etiqueta VLAN 802.1Q para que coincida con la etiqueta VLAN de la interfaz de salida. En este ejemplo, el cortafuegos reescribe el PVID de la BPDU de 100 a 1000 para una subinterfaz y de 100 a 1500 para la segunda subinterfaz cuando la BPDU atraviesa el puente de capa 2 en el cortafuegos.
4. Cada conmutador Cisco recibe la etiqueta PVID y VLAN correcta en la BPDU entrante y procesa el paquete PVST+ para detectar posibles bucles en la red.

Los siguientes comandos operativos de la CLI le permiten gestionar BPDU de PVST+ y PVST+ rápido.

- Deshabilite o vuelva a habilitar globalmente la reescritura de la BPDU de PVST+ y PVST+ rápido del PVID (el valor predeterminado es habilitado).

  `set session rewrite-pvst-pvid <yes|no>`

- Establezca la ID de VLAN nativa para el cortafuegos (el intervalo es de 1 a 4094; el valor predeterminado es 1).

  Si la ID de VLAN nativa en su conmutador es un valor distinto de 1, debe establecer la ID de VLAN nativa del cortafuegos en ese mismo número; de lo contrario, el cortafuegos eliminará los paquetes con esa ID de VLAN. Esto se aplica a las interfaces troncalizadas y no troncalizadas.

  `set session pvst-native-vlan-id <vid>`

- Descarte todos los paquetes de BPDU STP.

  set session drop-stp-packet <yes|no>

  Ejemplos de por qué es posible que quiera descartar todos los paquetes de BPDU STP:

  - Si solo hay un conmutador a cada lado del cortafuegos y no hay otras conexiones entre los conmutadores que puedan causar un bucle, no es necesario STP y puede desactivarse en el conmutador o que el cortafuegos lo bloquee.
  - Si hay un interruptor STP con un comportamiento erróneo que inunda de manera inapropiada las BPDU, puede detener los paquetes STP en el cortafuegos para detener la inundación de BPDU.

- Compruebe si la reescritura de BPDU de PVST+ está habilitada, vea el ID de VLAN nativa de PVST y determine si el cortafuegos está descartando todos los paquetes de BPDU STP.

  show vlan all

  ```
  pvst+ tag rewrite: disabled
  pvst native vlan id:     5
  drop stp:                disabled
  total vlans shown:       1
  name     interface           virtual interface
  bridge   ethernet1/1
           ethernet1/2
           ethernet1/1.1
           ethernet1/2.1
  ```

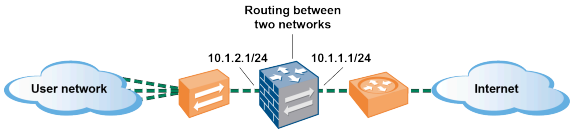
- Solucione los errores de la BPDU de PVST+.

  show counter global

  Observe contador **flow_pvid_inconsistent**, que registra la cantidad de veces que no coinciden los campos de etiqueta 802.1Q y PVID dentro de un paquete de BPDU de PVST+.

Interfaces de capa 3

En una implementación de capa 3, el cortafuegos enruta el tráfico entre múltiples puertos. Antes de que pueda Configurar las interfaces de capa 3, debe configurar los enrutadores virtuales que desea que el cortafuegos utilice para enrutar el tráfico a cada interfaz de capa 3.



Si utiliza etiquetas de grupos de seguridad (SGT, Security Group Tag) en una red Cisco TrustSec, se recomienda implementar cortafuegos en línea en los modos de capa 2 o cable virtual. Ahora bien, si debe utilizar un cortafuegos de capa 3 en una red Cisco TrustSec, tiene que implementarlo entre dos peers del protocolo de intercambio de SGT (SXP, SGT Exchange Protocol) y configurarlo de modo que permita el tráfico entre ellos.

Los siguientes temas describen cómo configurar interfaces de capa 3, y cómo utilizar el protocolo de detección de vecinos (NDP) para suministrar hosts IPv6 y visualizar las direcciones IPv6 de los dispositivos en la red local del enlace para ubicar dispositivos con rapidez.

- Configuración de interfaces de capa 3
- Gestión de hosts IPv6 con NDP

Configuración de interfaces de capa 3

El siguiente procedimiento es necesario para configurar interfaces de capa 3 (Ethernet, VLAN, bucle invertido e interfaces de túnel) con direcciones IPv4 o IPv6, de manera que el cortafuegos pueda realizar el enrutamiento en estas interfaces. Si un túnel se utiliza para el enrutamiento o si la supervisión de túnel está activada, el túnel necesita una dirección IP. Antes de realizar la siguiente tarea, defina uno o más enrutadores virtuales.

Habitualmente usaría el siguiente procedimiento para configurar una interfaz externa que se conecte con Internet y una interfaz para su red interna. Puede configurar ambas direcciones tanto IPv4 como IPv6 en una misma interfaz.

Los modelos de cortafuegos PAN-OS admiten un máximo de 16.000 direcciones IP asignadas a interfaces de capa 3 físicas o virtuales; este máximo incluye direcciones IPv4 e IPv6.

Si está utilizando rutas IPv6, puede configurar el cortafuegos para que proporcione anuncios de enrutador IPv6 para la configuración DNS. El cortafuegos proporciona a los clientes DNS IPv6 direcciones de servidor DNS recursivas (RDNS) y una lista de búsqueda DNS para que el cliente pueda resolver sus solicitudes DNS IPv6. Por lo tanto, el cortafuegos actúa como un servidor DHCPv6 para usted.

STEP 1 | Seleccione una interfaz y configúrela con una zona de seguridad.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**, según el tipo de interfaz que desee.
2. Seleccione la interfaz que desea configurar.
3. Seleccione **Interface Type**—**Layer3 (Tipo de interfaz: capa 3)**.
4. En la pestaña **Config**, para **Virtual Router (Enrutador virtual)**, seleccione el enrutador virtual que está configurando, tal como **default (predeterminado)**.
5. Para **Virtual System (Sistema virtual)**, seleccione el sistema virtual que está configurando, en el caso de un cortafuegos de sistema virtual múltiple.
6. Para **Security Zone (Zona de seguridad)**, seleccione la zona a la cual pertenece la interfaz o cree una **New Zone (Zona nueva)**.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure la interfaz con una dirección IPv4.

Para asignar la dirección IPv4 a una interfaz de capa 3, dispone de tres opciones:

- Estático
- Cliente DHCP: la interfaz del cortafuegos funciona como un cliente DHCP y recibe una dirección IP asignada dinámicamente. El cortafuegos también permite propagar los ajustes recibidos mediante la interfaz del cliente DHCP a un servidor DHCP activo en el cortafuegos. Esta opción se suele utilizar para propagar los ajustes del servidor DNS desde un proveedor de servicios de Internet a las máquinas cliente de la red que están protegidas por el cortafuegos.
- PPPoE: configure la interfaz como un punto de finalización del protocolo punto a punto sobre Ethernet (Point-to-Point Protocol over Ethernet, PPPoE) con el fin de permitir la conectividad en un entorno de línea de suscripción digital (DSL) en el que existe un módem DSL, pero ningún otro dispositivo PPPoE que finalice la conexión.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**, según el tipo de interfaz que desee.
2. Seleccione la interfaz que desea configurar.
3. Para configurar la interfaz con una dirección IPv4 estática, en la pestaña **IPv4**, configure **Type (Tipo)** en **Static (Estático)**.
4. Seleccione **Add (Añadir)** para añadir un nombre en **Name** y opcionalmente una descripción de la dirección en **Description**.

5. Para **Type (Tipo)**, seleccione una de las siguientes opciones:
   - **IP Netmask (Máscara de red IP)**: introduzca la dirección IP y la máscara de red para asignarla a la interfaz; por ejemplo, 208.80.56.100/24.

     Si utiliza una máscara de subred /31 para la dirección de interfaz de capa 3, la interfaz debe configurarse con la dirección .1/31, de modo que las utilidades, como ping, funcionen correctamente.

     Si está configurando una interfaz de bucle invertido con una dirección IPv4, debe tener una máscara de subred /32; por ejemplo, 192.168.2.1/32.
   - **IP Range (Intervalo IP)**: introduzca un intervalo de dirección IP, tal como 192.168.2.1-192.168.2.4.
   - **FQDN**: introduzca un nombre de dominio completo.
6. Seleccione **Tags (Etiquetas)** para aplicarlas a la dirección.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure una interfaz con el protocolo punto a punto sobre Ethernet (PPPoE). Consulte Interfaces de capa 3.

PPPoE no es compatible en modo HA activo/activo.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv4**, configure el **Type (Tipo)** en **PPPoE**.
4. En la pestaña **General**, seleccione **Enable (Habilitar)** para activar la interfaz para la finalización de PPPoE.
5. Introduzca el **Username (Nombre de usuario)** de la conexión de punto a punto.
6. Introduzca la **Password (Contraseña)** para el nombre de usuario y seleccione **Confirm Password (Confirmar contraseña)**.
7. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure una interfaz como cliente DHCP para que reciba la dirección IPv4 asignada de forma dinámica.

El cliente DHCP no es compatible en modo HA activo/activo.

STEP 5 | Configure una interfaz con una dirección IPv6 estática.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet**, **VLAN**, **loopback (bucle invertido)** o **Tunnel (Túnel)**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)** para permitir el direccionamiento de IPv6 en la interfaz.
4. Para **Interface ID (ID de interfaz)**, introduzca el identificador único ampliado de 64 bits (EUI-64) en formato hexadecimal (por ejemplo, 00:26:08:FF:FE:DE:4E:29). Si deja este campo en blanco, el cortafuegos utilizará el EUI-64 generado desde la dirección MAC de la interfaz física. Si activa la opción **Use interface ID as host portion (Usar la ID de interfaz como parte de host)** cuando se añade una dirección, el cortafuegos utiliza el ID de interfaz como la parte de host de esa dirección.
5. Seleccione **Add (Añadir)** para añadir la **Address (Dirección)** IPv6 o seleccione un grupo de direcciones.
6. Seleccione **Enable address on interface (Habilitar dirección en interfaz)** para habilitar la dirección IPv6 en la interfaz.
7. Seleccione **Use interface ID as host portion (Usar ID de interfaz como parte de host)** para utilizar el ID de interfaz como la parte de host de la dirección IPv6.
8. (Opcional) Seleccione **Anycast (Difusión por proximidad)** para que la dirección (ruta) IPv6 sea una dirección (ruta) de difusión por proximidad, lo que significa que varias ubicaciones pueden anunciar el mismo prefijo, e IPv6 envía el tráfico de difusión por proximidad al nodo que considera más cercano, según los costes del protocolo de enrutamiento y otros factores.
9. (Solo interfaz Ethernet) Seleccione **Send Router Advertisement (Enviar anuncio de enrutador,** RA) para habilitar el cortafuegos para que envíe esta dirección en anuncios de enrutador, en cuyo caso también debe habilitar la opción global **Enable Router Advertisement (Habilitar anuncio de enrutador)** en la interfaz (paso siguiente).
10. (Solo interfaz Ethernet) Introduzca la **Valid Lifetime (sec) (Duración válida [s])**, en segundos, por la que el cortafuegos considera la dirección como válida. La duración válida debe ser igual o superar la **Preferred Lifetime (sec) (Duración preferida [s])** (el valor predeterminado es 2 592 000).
11. (Solo interfaz Ethernet) Introduzca la **Preferred Lifetime (sec) (Duración preferida [s])** por la que se prefiere la dirección válida, lo que significa que el cortafuegos la puede utilizar para enviar y recibir tráfico. Cuando caduca la duración preferida, el cortafuegos deja de poder utilizar la dirección para establecer nuevas conexiones, pero cualquier conexión existente es válida hasta que caduque la **Valid Lifetime (Duración válida)** (el valor predeterminado es 604 800).
12. (Solo interfaz Ethernet) Seleccione **On-link (Enlace activo)** si se puede establecer comunicación con los sistemas con direcciones en el prefijo sin necesidad de un enrutador.
13. (Solo interfaz Ethernet) Seleccione **Autonomous (Autónomo)** si los sistemas pueden crear una dirección IP de forma independiente combinando el prefijo publicado con un ID de interfaz.
14. Haga clic en **OK (Aceptar)**.

STEP 6 | (Interfaz Ethernet o VLAN usando una dirección IPv6 únicamente) Habilite el cortafuegos para que envíe los anuncios de enrutador IPv6 (RA) desde una interfaz y, opcionalmente, para que ajuste los parámetros RA.

Ajuste los parámetros RA por cualquiera de estos motivos: Para interoperar con un enrutador/host que utilice diferentes valores. Para lograr una convergencia más rápida cuando haya varias puertas de enlace presentes. Por ejemplo, configure valores de ***Min Interval (Intervalo mínimo)***, ***Max Interval (Intervalo máximo)*** *y* ***Router Lifetime (Duración del enrutador)*** *más bajos para que el cliente/host IPv6 pueda cambiar rápidamente la puerta de enlace predeterminada después de que haya fallado la puerta de enlace principal, e iniciar el envío a otra puerta de enlace predeterminada en la red.*

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que desee configurar.
3. Seleccione **IPv6**.
4. Seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
5. En la pestaña **Router Advertisement (Anuncio de enrutador)**, seleccione **Enable Router Advertisement (Habilitar anuncio de enrutador)** (por defecto está deshabilitado).
6. (Opcional) Especifique el **Min Interval (sec) (Intervalo mínimo [s])**; es decir, el intervalo mínimo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 3 a 1350 y el valor predeterminado, 200). El cortafuegos envía los RA en intervalos aleatorios entre los valores mínimo y máximo que usted configure.
7. (Opcional) Especifique el **Max Interval (sec) (Intervalo máximo [s])**; es decir, el intervalo máximo (en segundos) entre los distintos RA que el cortafuegos enviará (el intervalo es de 4 a 1800 y el valor predeterminado, 600). El cortafuegos envía los RA en intervalos aleatorios entre los valores mínimo y máximo que usted configure.
8. (Opcional) Configure el **Hop Limit (Límite de salto)** que se debe aplicar a los clientes en los paquetes salientes (el intervalo es de 1 a 255, el valor predeterminado es 64). Introduzca 0 si no desea ningún límite de salto.
9. (Opcional) Configure **Link MTU (Unidad de transmisión máxima de enlace)**, la unidad de transmisión máxima (maximum transmission unit, MTU) de enlace para aplicar a los clientes (el intervalo es de 1280 a 9192; el valor predeterminado es **unspecified [no especificado]**). Seleccione **unspecified (no especificado)** para que no haya un MTU de enlace.
10. (Opcional) Configure el **Reachable Time (ms) (Tiempo alcanzable [s])**; es decir, el tiempo alcanzable (en milisegundos) que el cliente utilizará para asumir que un vecino es alcanzable después de recibir un mensaje de confirmación de esta condición. Seleccione **unspecified (no especificado)** si no desea establecer ningún valor de tiempo alcanzable (intervalo 0-3.600.000, predeterminado no especificado).
11. (Opcional) Configure el **Retrans Time (ms) (Tiempo de retransmisión [ms])**; el temporizador de retransmisión que determinará cuánto tiempo debe esperar el cliente, en milisegundos, antes de retransmitir los mensajes de convocatoria de vecinos. Seleccione **unspecified (no especificado)** si no desea ningún tiempo de retransmisión (intervalo 0-4.294.967.295, predeterminado no especificado).
12. (Opcional) Configure la **Router Lifetime (sec) (Duración de enrutador [s])** para especificar cuánto tiempo, en segundos, el cliente utilizará el cortafuegos como puerta de enlace

predeterminada (el intervalo es de 0 a 9000 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.

13. Configure la **Router Preference (Preferencia de enrutador)** que el cliente utiliza para seleccionar un enrutador preferido si el segmento de red tiene varios enrutadores IPv6. **High (Alta)**, **Medium (Intermedia)** (valor predeterminado) o **Low (Baja)** es la prioridad que el RA anuncia para indicar la prioridad relativa del enrutador virtual del cortafuegos en relación con otros enrutadores del segmento.
14. Seleccione **Managed Configuration (Configuración gestionada)** para indicar al cliente que las direcciones están disponibles a través de DHCPv6.
15. Seleccione **Other Configuration (Otra configuración)** para indicar al cliente que hay disponible otra información de dirección (por ejemplo, ajustes relacionados con DNS) a través de DHCPv6.
16. Seleccione **Consistency Check (Comprobación de consistencia)** si desea que el cortafuegos verifique que los RA enviados desde otros enrutadores están publicando información coherente en el enlace. El cortafuegos envía logs sobre cualquier incoherencia.
17. Haga clic en **OK (Aceptar)**.

STEP 7 | (Interfaz Ethernet o VLAN usando una dirección IPv6 únicamente) Especifique las direcciones del servidor DNS recursivo y la lista de búsqueda de DNS que el cortafuegos anunciará en los anuncios de enrutador ND desde esta interfaz.

Los servidores RDNS y la lista de búsqueda DNS son parte de la configuración DNS para el cliente DNS, de manera que el cliente pueda resolver las solicitudes DNS IPv6.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6** > **DNS Support (Soporte DNS)**.
4. Seleccione **Include DNS information in Router Advertisement (Incluir información DNS en el anuncio de enrutador)** para habilitar el cortafuegos para que envíe información DNS IPv6.
5. Para el **Server (Servidor)** DNS, seleccione **Add (Añadir)** para añadir la dirección IPv6 de un servidor DNS recursivo. Seleccione **Add (Añadir)** para añadir hasta ocho servidores DNS recursivos. El cortafuegos envía direcciones de servidor en un anuncio de enrutador ICMPv6 en orden descendente.
6. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el servidor RDNS específico para resolver nombres de dominio.
   - El intervalo de la **Lifetime (Duración)** es cualquier valor igual o entre el **Max Interval (Intervalo máximo)** (que configuró en la pestaña **Router Advertisement [Anuncio de enrutador]**) y dos veces ese **Max Interval (Intervalo máximo)**. Por ejemplo, si su intervalo máximo es de 600 segundos, el intervalo de duración es de 600 a 1200 segundos.
   - La **Lifetime (Duración)** predeterminada es de 1200 segundos.
7. Para el sufijo DNS, seleccione **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** (nombre de dominio de un máximo de 255 bytes). Seleccione **Add (Añadir)** para añadir hasta ocho

sufijos DNS. El cortafuegos envía sufijos en un anuncio de enrutador ICMPv6 en orden descendente.

8. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el sufijo. La duración posee el mismo intervalo y valor predeterminado que el **servidor**.
9. Haga clic en **OK (Aceptar)**.

STEP 8 | (Ethernet o interfaz de VLAN) Especifique las entradas de ARP. Las entradas de ARP estáticas reducen el procesamiento de ARP.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **ARP Entries (Entradas de ARP)**.
4. Haga clic en **Add (Añadir)** para añadir una **IP Address (Dirección IP)** y la **MAC Address (Dirección MAC)** correspondiente (dirección de control de acceso a medios o hardware). Para una interfaz de VLAN, también debe seleccionar la **Interface (Interfaz)**.

   Las entradas de ARP estáticas no agotan su tiempo de espera. Las entradas de ARP que se obtienen automáticamente en caché se agotan en 1800 segundos de manera predeterminada; debe personalizar el tiempo de espera de caché del ARP; consulte Configuración de los tiempos de espera de sesión.
5. Haga clic en **OK (Aceptar)**.

STEP 9 | (Ethernet o interfaz de VLAN) Especifique las entradas estáticas del Protocolo de detección de vecinos (Neighbor Discovery Protocol, NDP). NDP para IPv6 realiza funciones similares a las que ofrece ARP para IPv4.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **ND Entries (Entradas del ND)**.
4. Haga clic en **Add (Agregar)** para agregar una **IPv6 Address (Dirección IPv6)** y la **MAC Address (Dirección MAC)** correspondiente.
5. Haga clic en **OK (Aceptar)**.

STEP 10 | (Opcional) Habilite los servicios en la interfaz.

1. Para habilitar los servicios en la interfaz, seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**.
4. Expanda la lista **Management Profile (Perfil de gestión)** y seleccione un perfil o **New Management Profile (Nuevo perfil de gestión)**.
5. Introduzca un **Name (Nombre)** para el perfil.
6. Para **Permitted Services (Servicios permitidos)**, seleccione servicios, tales como **Ping**, y haga clic en **OK (Aceptar)**.

STEP 11 | **Commit (Confirmar)** los cambios.

STEP 12 | Conecte el cable de Internet.

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

STEP 13 | Verifique que la interfaz esté activa.

Desde la interfaz web, seleccione **Network (Red)** > **Interfaces** y verifique que el icono de la columna Link State (Estado de enlace) esté de color verde. También puede supervisar el estado de enlace desde el widget **Interfaces** en el **Dashboard (Panel)**.

STEP 14 | Configure rutas estáticas o un protocolo de enrutamiento dinámico (RIP, OSPF o BGP), para que el enrutador virtual pueda enrutar el tráfico.

- Configuración de una ruta estática
- RIP
- OSPF
- BGP

STEP 15 | Configuración de una ruta predeterminada.

Configure una ruta estática y establézcala como predeterminada.

Gestión de hosts IPv6 con NDP

Este tema describe cómo puede utilizar NDP para suministrar hosts IPv6; por lo tanto, no necesita un servidor DHCPv6 separado para este fin. Esto también explica cómo utilizar el NDP para supervisar direcciones IPv6, lo que le permite rastrear con rapidez la dirección IPv6 y la dirección MAC de un dispositivo y el usuario asociado que ha violado una regla de seguridad.

- Anuncios de enrutador IPv6 para la configuración del DNS
- Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6
- Monitorización NDP
- Habilitar supervisión NDP

Anuncios de enrutador IPv6 para la configuración del DNS

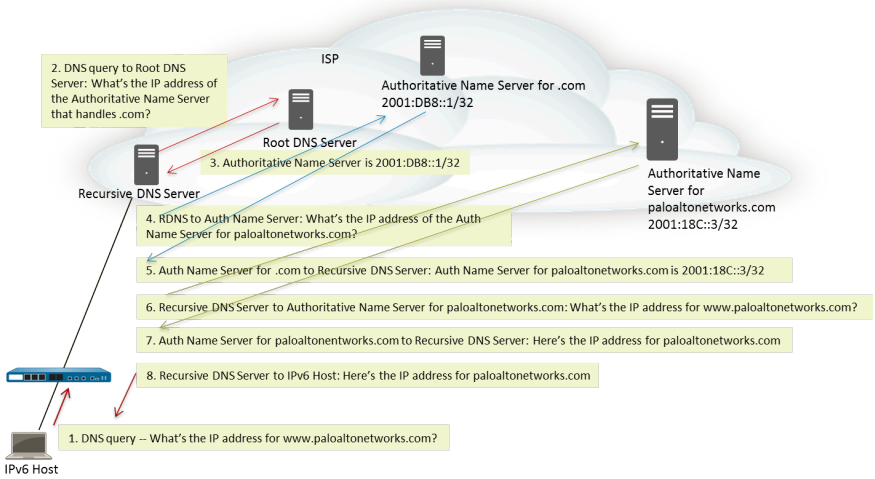
Se mejora la implementación del cortafuegos de la detección de vecinos (ND) de modo que pueda ofrecerle a los hosts IPv6 la opción de servidor DNS recursivo (RDNSS) y la opción de lista de búsqueda de DNS (DNSSL) según RFC 6106, Opciones de anuncios de enrutador IPv6 para la configuración del DNS. Cuando realiza la Configuración de interfaces de capa 3, configura estas opciones de DNS en el cortafuegos y el cortafuegos puede suministrar a los hosts IPv6; por lo tanto, no es necesario que un servidor DHCPv6 independiente para suministrar a los hosts. El cortafuegos envía anuncios de enrutador (RA) IPv6 con estas opciones a hosts IPv6 como parte de su configuración de DNS para suministrarlos completamente con el fin de alcanzar los servicios de internet. Por lo tanto, sus hosts IPv6 se configuran con las siguientes variables:

- Las direcciones de los servidores RDNS que pueden resolver consultas de DNS.
- Una lista de nombres de dominio (sufijos) que el cliente DNS agrega (una a la vez) a un nombre de dominio no calificado antes de introducir el nombre de dominio en una consulta DNS.

Los anuncios de enrutador IPv6 para la configuración del DNS son compatibles con los interfaces Ethernet, los subinterfaces, los interfaces Ethernet agregados y los interfaces VLAN de capa 3 en todas las plataformas PAN-OS.

La capacidad del cortafuegos de enviar RA IPv6 para la configuración del DNS le permite al cortafuegos realizar una función similar al DHCP y no se relaciona con el cortafuegos como proxy DNS, cliente DNS o servidor DNS.

Después de configurar el cortafuegos con las direcciones de los servidores RDNS, el cortafuegos suministra un host IPv6 (el cliente DNS) con esas direcciones. El host IPv6 utiliza una o más de estas direcciones para alcanzar un servidor RDNS. El DNS recursivo corresponde a una serie de solicitudes DNS de un servidor RDNS, como se muestra con tres pares de consultas y respuestas en la siguiente figura. Por ejemplo, cuando un usuario intenta acceder a www.paloaltonetworks.com, el explorador local detecta que esa dirección IP para ese nombre de dominio no se encuentra en su almacenamiento en caché ni en el sistema operativo del cliente. El sistema operativo del cliente inicia una consulta DNS para un servidor DNS recursivo perteneciente al ISP local.



Un anuncio de enrutador IPv6 puede incluir varias opciones de dirección de servidor DNS recursivo y cada opción posee una duración similar o diferente. Una opción única de dirección de servidor DNS recursivo puede incluir varias direcciones de servidor DNS recursivo siempre que las direcciones compartan la misma duración.

Una lista de búsqueda de DNS es una lista de los nombres de dominio (sufijos) que el cortafuegos anuncia a un cliente DNS. Por lo tanto, el cortafuego suministra al cliente DNS para que utilice los sufijos en sus consultas de DNS no calificadas. El cliente DNS agrega los sufijos, uno a uno, a un nombre de dominio no calificado antes de introducir el nombre en una consulta DNS, y utilizar, de ese modo, un nombre de dominio completo (FQDN) en la consulta DNS. Por ejemplo, si un usuario (del cliente DNS que se configura) intenta enviar una consulta DNS con el nombre "calidad" sin un sufijo, el enrutador agrega un punto y el primer sufijo DNS de la lista de búsqueda de DNS al nombre y transmite una consulta DNS. Si el primer sufijo DNS de la lista es "empresa.com", la consulta DNS resultante del enrutador se realizará con el FQDN "calidad.empresa.com".

Si la consulta DNS falla, el cliente agrega el segundo sufijo DNS de la lista al nombre no calificado y transmite una nueva consulta DNS. El cliente utiliza los sufijos DNS en orden hasta que una

búsqueda de DNS sea correcta (se omiten los sufijos restantes) o hasta que el enrutador haya intentado todos los sufijos de la lista.

Configure el cortafuegos con los sufijos que desea facilitar al enrutador de cliente DNS en una opción DNSSL de ND; el cliente DNS que recibe la lista de búsqueda de DNS utiliza los sufijos en sus consultas DNS no calificadas.

Para especificar los servidores RDNS y una lista de búsqueda de DNS, realice la Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6.

Configuración de los servidores RDNS y la lista de búsqueda de DNS para los anuncios de enrutadores IPv6

Realice esta tarea para llevar a cabo los Anuncios de enrutadores IPv6 para la configuración de DNS de hosts IPv6.

STEP 1 | Permita que el cortafuegos envíe anuncios de enrutadores IPv6 desde una interfaz.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que desea configurar.
3. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
4. En la pestaña **Router Advertisement (Anuncios de enrutadores)**, seleccione **Enable Router Advertisement (Habilitar anuncios de enrutadores)**.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Especifique las direcciones del servidor DNS recursivo y la lista de búsqueda de DNS que el cortafuegos anunciará en los anuncios de enrutadores de ND de esta interfaz.

Los servidores RDNS y la lista de búsqueda DNS son parte de la configuración DNS para el cliente DNS, de manera que el cliente pueda resolver las solicitudes DNS IPv6.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6** > **DNS Support (Soporte DNS)**.
4. Seleccione **Include DNS information in Router Advertisement (Incluir información DNS en el anuncio de enrutador)** para habilitar el cortafuegos para que envíe información DNS IPv6.
5. Para el **Server (Servidor)** DNS, seleccione **Add (Añadir)** para añadir la dirección IPv6 de un servidor DNS recursivo. Seleccione **Add (Añadir)** para añadir hasta ocho servidores DNS recursivos. El cortafuegos envía direcciones de servidor en un anuncio de enrutador ICMPv6 en orden descendente.
6. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el servidor RDNS específico para resolver nombres de dominio.
   - El intervalo de la **Lifetime (Duración)** es cualquier valor igual o entre el **Max Interval (Intervalo máximo)** (que configuró en la pestaña **Router Advertisement [Anuncio de enrutador]**) y dos veces ese **Max Interval (Intervalo máximo)**. Por ejemplo, si su intervalo máximo es de 600 segundos, el intervalo de duración es de 600 a 1200 segundos.

- La **Lifetime (Duración)** predeterminada es de 1200 segundos.

7. Para el sufijo DNS, seleccione **Add (Añadir)** un **DNS Suffix (Sufijo DNS)** (nombre de dominio de un máximo de 255 bytes). Seleccione **Add (Añadir)** para añadir hasta ocho sufijos DNS. El cortafuegos envía sufijos en un anuncio de enrutador ICMPv6 en orden descendente.
8. Especifique la **Lifetime (Duración)** en segundos, que es la extensión de tiempo máxima durante la que el cliente puede usar el sufijo. La duración posee el mismo intervalo y valor predeterminado que el **servidor**.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

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

Monitorización NDP

El protocolo de detección de vecinos (NDP) para la dirección IPv6 (RFC 4861) lleva a cabo funciones similares a las funciones de ARP para IPv4. El cortafuegos predeterminado ejecuta el NDP, que utiliza paquetes ICMPv6 para encontrar y rastrear las direcciones de capa de enlace y el estado de los vecinos en los enlaces conectados.

Habilitar supervisión NDP de modo que pueda visualizar las direcciones IPv6 de los dispositivos en la red local del enlace, sus direcciones MAC, el nombre de usuario asociado de User-ID (si el usuario de ese dispositivo utilizó un servicio de directorio para iniciar sesión), el estado de alcance de la dirección, y la última fecha y hora informada en la que el supervisor NDP recibió un anuncio de enrutador de esta dirección IPv6. El nombre de usuario depende del mejor caso; pueden existir varios dispositivos IPv6 en una red sin nombre de usuario, como las impresoras, los equipos de fax, los servidores, etc.

Si desea rastrear con rapidez un dispositivo y un usuario que violó una regla de seguridad, es útil que la dirección IPv6, la dirección MAC y el nombre de usuario se muestren en un lugar. Necesita la dirección MAC que corresponde a la dirección IPv6 para rastrear la dirección MAC de vuelta a un conmutador físico o punto de acceso.

No se garantiza que la supervisión de NDP descubra todos los dispositivos debido a que podría haber otros dispositivos de red entre el cortafuegos y el cliente que filtra mensajes de NDP o detección de direcciones duplicadas (DAD). El cortafuegos solo puede supervisar los dispositivos que encuentra en la interfaz.

La supervisión de NDP también supervisa los paquetes de detección de direcciones duplicadas (DAD) de clientes y vecinos. También puede supervisar los logs de ND IPv6 para facilitar la resolución de problemas.

La supervisión de NDP admite interfaces Ethernet, subinterfaces, interfaces Ethernet de agregación e interfaces VLAN en todos los modelos PAN-OS.

Habilitar supervisión NDP

Realice esta tarea para habilitar la supervisión NDP en una interfaz.

STEP 1 | Habilite la supervisión NDP.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. Seleccione la interfaz que está configurando.
3. Seleccione **IPv6**.
4. Seleccione **Address Resolution (Resolución de dirección)**.
5. Seleccione **Enable NDP Monitoring (Habilitar supervisión NDP)**.

   *Tras habilitar o deshabilitar la supervisión NDP, debe hacer clic en **Commit (Confirmar)** para confirmar el cambio antes de que la supervisión NDP se inicie o se detenga.*
6. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

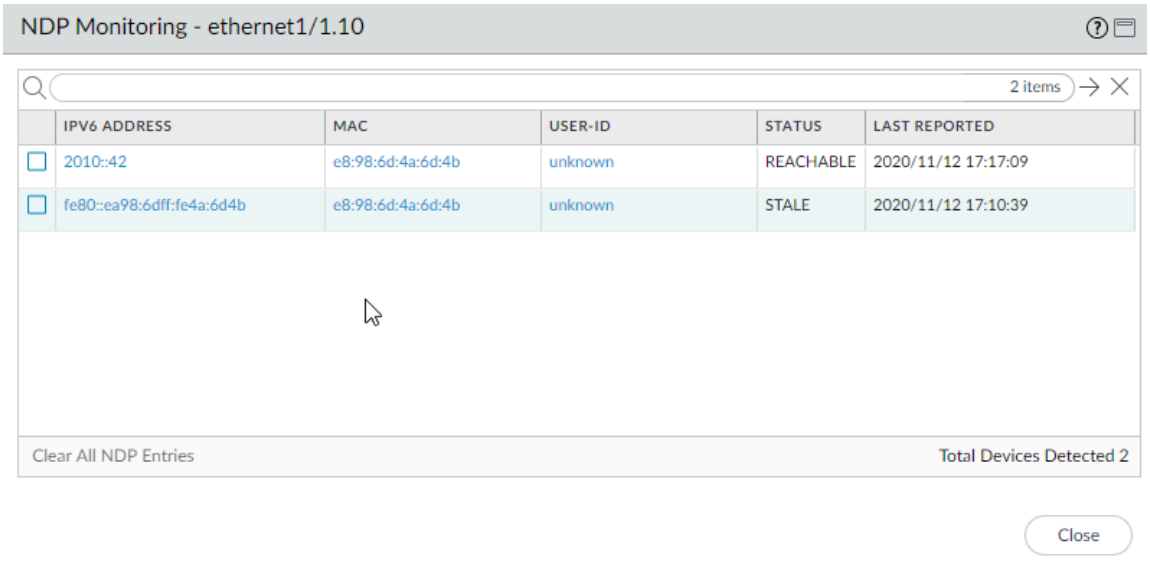
Haga clic en **Commit (Confirmar)**.

STEP 3 | Supervise paquetes NDP y DAD de clientes y vecinos.

1. Seleccione **Network (Red)** > **Interfaces** y **Ethernet** o **VLAN**.
2. En la interfaz donde habilitó la supervisión NDP, en la columna Features (Funciones), coloque el cursor sobre el icono de NDP Monitoring (Supervisión NDP) :

   El resumen de supervisión NDP de la interfaz muestra la lista de **prefijos** IPv6 que la interfaz enviará en el anuncio de enrutador (RA) si se encuentra habilitada esta opción (se trata de los prefijos IPv6 de la interfaz misma).

   Además, el resumen indica si las opciones DAD, anuncio de enrutador o asistencia de DNS están habilitadas; si las direcciones IP de los servidores DNS recursivos están configurados y los sufijos DNS configurados en la lista de búsqueda de DNS.
3. Haga clic en el icono de supervisión NDP para mostrar información detallada.



   Cada fila de la tabla detallada de supervisión NDP de la interfaz muestra la dirección IPv6 de un vecino que descubrió el cortafuegos, la dirección MAC correspondiente, la ID de usuario correspondiente (basada en el mejor caso), estado de alcance de la dirección,

y última fecha y hora informada en la que este supervisor NDP recibió un RA de esta dirección IP. Una ID de usuario no se mostrará en las impresoras u otros hosts no basados en un usuario. Si el estado de la dirección IP es antiguo, se desconoce si el vecino es alcanzable, según RFC 4861.

En la esquina inferior derecha, se encuentra el contador de **Total Devices Detected (Dispositivos totales detectados)** en la red local del enlace.

- Introduzca una dirección IPv6 en el campo de filtro para buscar la dirección que desea mostrar.
- Seleccione las casillas de verificación para mostrar o no mostrar las direcciones IPv6.
- Haga clic en los números, la flecha derecha o izquierda, o la barra de desplazamiento vertical para avanzar a través de las entradas.
- Haga clic en **Clear All NDP Entries (Borrar todas las entradas de NDP)** para borrar toda la tabla.

STEP 4 | Supervise los logs de ND para crear informes.

1. Seleccione **Monitor (Supervisar)** > **Logs** > **System (Sistema)**.
2. En la columna Type (Tipo), visualice los logs **ipv6nd** y las descripciones correspondientes.

   Por ejemplo, `inconsistent router advertisementreceived`(anuncio de enrutador incoherente recibido) indica que el cortafuegos recibió un RA diferente al RA que enviará.

Configuración de los grupos de interfaces de agregación

Un grupo de interfaz de agregación utiliza la agregación de enlaces IEEE 802.1AX para combinar varias interfaces de Ethernet en una sola interfaz virtual que conecta el cortafuegos a otro dispositivo de red o cortafuegos. Un grupo de agregación aumenta el ancho de banda entre peers al equilibrar la carga de tráfico en las interfaces combinadas. También proporciona redundancia; cuando una interfaz falla, las interfaces restantes continúan manteniendo el tráfico.

Por defecto, la detección de fallos de interfaz es automática solo en la capa física, entre peers conectados directamente. Sin embargo, si habilita el protocolo de control de adición de enlaces (Link Aggregation Control Protocol, LACP), la detección de fallos es automática en la capa física y de enlace de datos, independientemente de si los peers están conectados directamente. LACP también permite la conmutación por error automática a interfaces en espera si configura reservas activas. Todos los cortafuegos de Palo Alto Networks® admiten los grupos de agregación, excepto los modelos VM-Series. La herramienta de selección de productos indica la cantidad de grupos de agregación que admite cada cortafuegos. Cada grupo de agregación puede tener hasta ocho interfaces.

Los modelos de cortafuegos PAN-OS® admiten un máximo de 16.000 direcciones IP asignadas a interfaces de capa 3 físicas o virtuales; este máximo incluye direcciones IPv4 e IPv6.

QoS solo es compatible con los primeros ocho grupos de agregación.

Antes de configurar un grupo de agregación, debe configurar sus interfaces. Entre las interfaces asignadas a cualquier grupo de agregación particular, el soporte físico del hardware puede ser diferente (por ejemplo, puede mezclar fibra óptica y cobre), pero el ancho de banda y el tipo de interfaz deben ser los mismos. Las opciones de ancho de banda y tipo de interfaz son las siguientes:

- **Ancho de banda**: 1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps
- **Interface type**: HA3, Virtual Wire, capa 2 o capa 3.

Este procedimiento describe los pasos de configuración únicamente para el cortafuegos de Palo Alto Networks. También debe configurar el grupo de agregación en el dispositivo peer. Consulte la documentación de dicho dispositivo para obtener instrucciones.

STEP 1 | Configure los parámetros de grupo de interfaz generales.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y **Add Aggregate Group (Añadir grupo de agregación)**.
2. En el campo adyacente a **Interface Name (Nombre de interfaz)** de solo lectura, introduzca un número (1-8) para identificar el grupo de agregación.
3. Para el **Interface Type**, seleccione **HA**, **Virtual Wire**, **Layer2** o **Layer3**.
4. Configure los parámetros restantes para el **Interface Type** que seleccionó.

STEP 2 | Configure los ajustes de LACP.

Realice este paso únicamente si desea habilitar LACP para el grupo de agregación.

No puede habilitar LACP para interfaces de cable virtual.

1. Seleccione la pestaña **LACP** y luego **Enable LACP (Habilitar LACP)**.
2. Configure el **Mode** para las consultas de estado de LACP en **Passive** (el valor por defecto es que el cortafuegos solo responde) o **Active** (el cortafuegos consulta a dispositivos peer).

   Se recomienda configurar un peer LACP como activo y el otro como pasivo. LACP no puede funcionar si los dos peers son pasivos. El cortafuegos no puede detectar el modo de su dispositivo peer.
3. Configure el **Transmission Rate** para la consulta LACP e intercambios de respuesta en **Slow** (cada 30 segundos, el valor por defecto) o **Fast** (cada segundo). Base su selección en el nivel de procesamiento LACP que admite la red y con qué velocidad los peers LACP deben detectar y resolver fallos de interfaz.
4. Seleccione **Fast Failover** si desea habilitar la conmutación por error a una interfaz en espera en menos de un segundo. Por defecto, la opción está deshabilitada y el cortafuegos utiliza el estándar IEEE 802.1ax para el procesamiento de conmutación por error, que demora al menos tres segundos.

   *La práctica recomendada es usar **Fast Failover** en implementaciones en las que pueda perder datos críticos durante el intervalo de conmutación por error estándar.*
5. Introduzca el **máximo de puertos** (cantidad de interfaces) que están activas (de 1 a 8) en el grupo de agregación. Si el número de interfaces que asigna al grupo supera el **máximo de puertos**, el resto de las interfaces están en modo de espera. El cortafuegos usa la **LACP Port Priority (Prioridad de puerto LACP)** de cada interfaz que usted asigna (paso 3) para determinar qué interfaces están activas inicialmente y el orden en que se activan las interfaces en espera tras la conmutación por error. Si los peers de LACP no tienen valores de prioridad de puerto coincidentes, los valores del peer con el número de **prioridad del sistema** más bajo (el valor predeterminado es 32 768; el intervalo es de 1a 65 535), cancelará el otro peer.
6. (Opcional) Para los cortafuegos activos/pasivos únicamente, seleccione **Enable in HA Passive State** si desea habilitar la negociación previa de LACP para el cortafuegos pasivo. La negociación previa de LACP permite una conmutación por error más rápida al cortafuegos pasivo (para obtener detalles, consulte Negociación previa de LACP y LLDP para la HA activa/pasiva)

   *Si selecciona esta opción, no puede seleccionar **Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para HA activo-pasivo)**; la negociación previa requiere direcciones MAC de interfaz únicas en cada cortafuegos HA.*
7. (Opcional) Para los cortafuegos activos/pasivos únicamente, seleccione **Same System MAC Address for Active-Passive HA (Misma dirección MAC del sistema para HA activo-pasivo)** y especifique una sola **MAC Address (Dirección MAC)** para ambos cortafuegos HA. Esta opción minimiza la latencia de conmutación por error si los peers LACP están

virtualizados (aparecen en la red como un solo dispositivo). Por defecto, esta opción está deshabilitada: cada cortafuegos de un par en HA tiene una única dirección MAC.

Cuando los peers del LACP no se virtualizan, utilizar las direcciones MAC únicas minimiza la latencia de la conmutación por error.

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

STEP 4 | Asignación de interfaces al grupo de agregación

Realice los siguientes pasos para cada interfaz (1-8) que pertenecerá al grupo de agregación.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y haga clic en el nombre de la interfaz para editarla.
2. Cambie el **Tipo de interfaz** a **Ethernet de agregación**.
3. Seleccione el **Grupo de agregación** que acaba de definir.
4. Seleccione **Link Speed (Velocidad de enlace)**, **Link Duplex (Dúplex de enlace)** y **Link State (Estado de enlace)**.

   Se recomienda establecer la misma velocidad de enlace y valores duplicados para cada interfaz del grupo. Para los valores que no coinciden, el cortafuegos activa por defecto la velocidad más alta y dúplex completo.
5. (Opcional) Introduzca una **prioridad del puerto LACP** (el valor predeterminado es 32 768; el intervalo es de 1 a 65 535) si habilitó LACP para el grupo de agregación. Si el número de interfaces que asigna excede el valor de **Max Ports** del grupo, las prioridades de puerto determinan qué interfaces están activas o en espera. Se activarán las interfaces con los valores numéricos más bajos (prioridades más altas).
6. Haga clic en **OK (Aceptar)**.

STEP 5 | Si los cortafuegos tienen una configuración activa/activa y usted está agregando interfaces HA3, habilite el reenvío de paquetes para el grupo de agregación.

1. Seleccione **Device (Dispositivo)** > **High Availability (Alta disponibilidad)** > **Active/Active Config (Config. activa/activa)**, y edite la sección Packet Forwarding (Reenvío de paquetes).
2. Seleccione el grupo de agregación que configuró para **HA3 Interface** y haga clic en **OK**.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Verifique el estado del grupo de agregación.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**.
2. Compruebe que la columna Estado de enlace muestra un icono verde para el grupo de agregación, indicando que todas las interfaces miembro están funcionando. Si el icono es amarillo, al menos un miembro falla, pero no todos. Si el icono está en rojo, todos los miembros han fallado.
3. Si configuró LACP, compruebe que la columna Features muestre el icono de LACP habilitado para el grupo de agregación.

STEP 8 | (Solo en el caso de cortafuegos PA-7050 y PA-7080) Si tiene un grupo de interfaz de agregación que cuenta con interfaces ubicadas en diferentes tarjetas de línea, una práctica recomendada es habilitar el cortafuegos para que pueda manejar paquetes IP fragmentados

que recibe en diversas interfaces del grupo AE que se distribuyen en varias tarjetas. Para ello, utilice el siguiente comando operativo de la CLI con la palabra clave **hash.** (Las otras dos palabras clave también se muestran para mayor exhaustividad).

1. Acceda la CLI.
2. Utilice el siguiente comando operativo de la CLI: **set ae-frag redistribution-policy** <**self** | **fixed sXdpX** | **hash**>
   - **self**—(predeterminado) Esta palabra clave es para el comportamiento heredado; no permite que el cortafuegos maneje paquetes fragmentados que reciben las diversas interfaces de un grupo de interfaces AE.
   - **fixed s**<*slot-number*>**dp**<*dataplane-cpu-number*>: reemplace la variable *slot-number* y la *data-plane-cpu-number* por el número de plano de datos que manejará todos los fragmentos de IP que reciben todos los miembros de cada interfaz AE. La palabra clave **fixed** se utiliza, en esencia, para la solución de problemas y no debe usarse en producción.
   - **hash**: se utiliza para permitir que el cortafuegos maneje paquetes fragmentados que recibe en varias interfaces de un grupo de interfaces AE que se encuentran en más de una tarjeta de línea.

Configuración del reflector de Bonjour para la segmentación de red

Apple Bonjour (también conocida como red de configuración cero) permite la detección automática de dispositivos y servicios en una red local. Por ejemplo, Bonjour le permite conectarse a una impresora sin configurar manualmente su dirección IP. Para traducir nombres a direcciones en una red local, Bonjour usa DNS de multidifusión (mDNS, Multicast DNS). Bonjour utiliza un intervalo de multidifusión privado para su tráfico, que no permite el enrutamiento del tráfico. Esto evita el uso en un entorno que utilice la segmentación de red con fines administrativos o de seguridad (por ejemplo, cuando los servidores y los clientes se encuentren en subredes diferentes).

Para admitir Apple Bonjour en entornos de red en los que se utilice la segmentación para enrutar el tráfico, puede reenviar el tráfico IPv4 de Bonjour entre interfaces o subinterfaces de Ethernet Interfaces de capa 3 (L3) o de Ethernet de agregación (AE) que especifique. La opción de reflector de Bonjour le permite reenviar anuncios y consultas de Bonjour de multidifusión a interfaces o subinterfaces Ethernet de L3 y AE, lo que garantiza el acceso del usuario a los servicios y la detección del dispositivo independientemente de los valores de tiempo de vida (TTL, Time To Live) o las limitaciones de salto.

El reenvío de tráfico de Bonjour es compatible con PA-220, PA-400, PA-800 y PA-3200 Series.

Cuando habilite esta opción, el cortafuegos redirigirá el tráfico de Bonjour a las interfaces y subinterfaces de L3 y AE donde habilite esta opción. Debe habilitar esta opción en todas las interfaces compatibles en las que desee gestionar el tráfico de Bonjour; por ejemplo, si desea que una interfaz de L3 específica reenvíe el tráfico de Bonjour a una interfaz de AE, debe habilitar esta opción en ambas interfaces. Puede habilitar esta opción en hasta 16 interfaces.

Para evitar bucles, el cortafuegos modifica la dirección MAC de origen a la dirección MAC de la interfaz de salida del cortafuegos. Para ayudar a prevenir ataques de inundación, si el cortafuegos recibe más paquetes por segundo que el número especificado en la siguiente tabla, el cortafuegos descarta los paquetes para proteger el cortafuegos y la red.

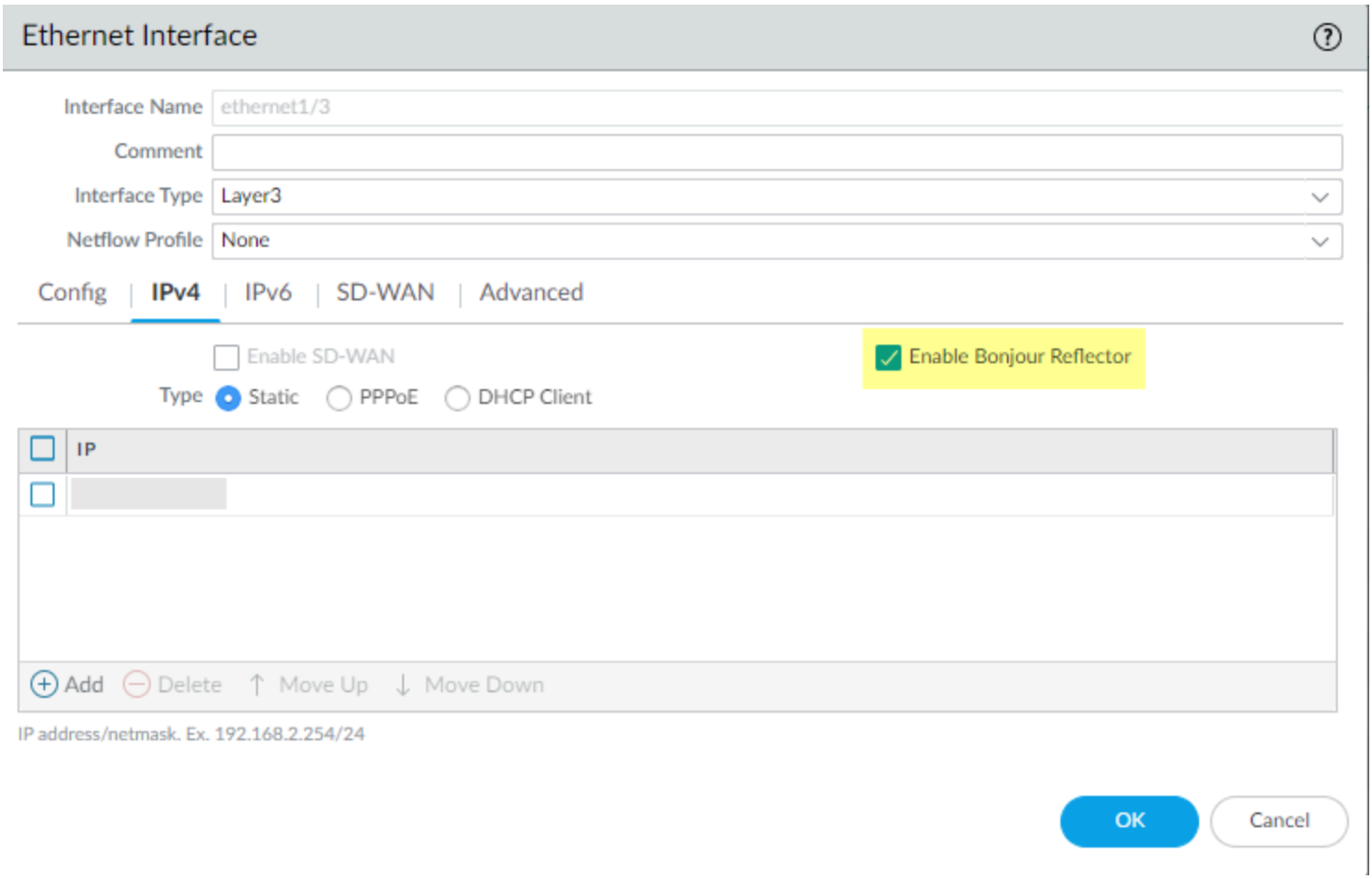
Límite de frecuencia de la	*serie (por segundo)*
PA-220	*100*
PA-400	*n/c*
PA-800	*200*
PA-3200	*500*

STEP 1 | Seleccone **Network (Red)** > **Interfaces**.

STEP 2 | Seleccione o **añada** una Ethernet o subinterfaz de L3 o interfaz de AE.

*Si añade una subinterfaz, debe usar una **etiqueta** distinta de 0.*

STEP 3 | Seleccione **IPv4** y, a continuación, seleccione la opción **Enable Bonjour Reflector (Habilitar reflector de Bonjour)**.



STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Repita los pasos del 1 al 4 para todas las interfaces y subinterfaces de L3 o AE a las que desee reenviar el tráfico de Bonjour.

Puede habilitar esta opción en hasta 16 interfaces o subinterfaces diferentes.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Confirme que la columna **Features (Funciones)** para la interfaz o interfaces donde habilita la opción de reflector de Bonjour muestre `Bonjour Reflector:yes` ( ).

STEP 8 | Utilice el comando de la CLI `show bonjour interface (mostrar interfaz de bonjour)` para mostrar todas las interfaces a las que el cortafuegos reenvía el tráfico de Bonjour y una lista de contadores. `rx` representa el número total de paquetes de Bonjour

que recibe la interfaz, **tx** representa el número total de paquetes de Bonjour que transmite la interfaz y **drop (descartar)** representa el número de paquetes que descarta la interfaz.

```
admin> show bonjour interface

name                    rx          tx          drop
-----------------------------------------------------------
ethernet1/4             1           1           0
ethernet1/7             0           0           0
ethernet1/7.10          0           0           0
ethernet1/7.20          4           4           0
ae15                    0           0           0
ae16                    0           0           0
ae16.30                 0           2           0
ae16.40                 0           0           0
```


Uso de los perfiles de gestión de interfaz para restringir el acceso

Un perfil de gestión de interfaz protege al cortafuegos contra el acceso no autorizado mediante la definición de los protocolos, servicios y direcciones IP que una interfaz de cortafuegos permite para el tráfico de gestión. Por ejemplo, puede impedir que los usuarios accedan a la interfaz web del cortafuegos en la interfaz Ethernet1/1, pero permitir que la interfaz reciba consultas SNMP de su sistema de supervisión de red. En este caso, usted habilitaría SNMP y deshabilitaría HTTP/HTTPS en un perfil de gestión de interfaz y asignaría el perfil a Ethernet1/1.

Puede asignar un perfil de gestión de interfaz a interfaces Ethernet capa 3 (incluidas las subinterfaces) y a interfaces lógicas (interfaces de grupo de agregación, VLAN, loopback y de túnel) Si no asigna un perfil de gestión de interfaz a una interfaz, esta denegará por defecto el acceso a todas las direcciones IP, protocolos y servicios.

La interfaz de gestión (MGT) no requiere un perfil de gestión de interfaz. Los protocolos, los servicios y las direcciones IP para la interfaz MGT los restringe cuando realiza la configuración inicial del cortafuegos. En caso de que la interfaz MGT deje de funcionar, permitir el acceso de gestión por otra interfaz le da la posibilidad de seguir gestionando el cortafuegos.

Si permite el acceso a la interfaz del cortafuegos con un perfil de gestión de interfaces, no habilite el acceso de gestión (HTTP, HTTPS, SSH ni Telnet) desde internet ni desde zonas no fiables que estén dentro de los límites de seguridad de su empresa. No habilite nunca el acceso por HTTP ni Telnet porque esos protocolos realizan transmisiones de texto sin cifrar. Respete las Prácticas recomendadas para proteger el acceso administrativo para garantizar que protege adecuadamente el acceso de gestión al cortafuegos.

STEP 1 | Configure el perfil de gestión de interfaz.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
2. Seleccione los protocolos que la interfaz permitirá para el tráfico de gestión: **Ping**, **Telnet**, **SSH**, **HTTP**, **HTTP OCSP**, **HTTPS** o **SNMP**.

   *No habilite **HTTP** ni **Telnet** porque esos protocolos realizan transmisiones de texto sin cifrar y, por lo tanto, no son seguros.*
3. Seleccione los servicios que la interfaz permitirá para el tráfico de gestión:
   - **Response Pages (Páginas de respuesta)**: utilícela para habilitar páginas de respuesta para lo siguiente:
     - **Portal cautivo**: para servir a las páginas de respuesta del portal cautivo, el cortafuegos deja los puertos abiertos en las interfaces de capa 3: 6081 para portal cautivo en modo transparente y 6082 para portal cautivo en modo de redirección. Para obtener información, consulte Política de autenticación y portal de autenticación.
     - **Anulación de administrador de URL:** para obtener información detallada, consulte Permiso de acceso con contraseña a ciertos sitios.

- **ID del usuario**: se utiliza para redistribuir datos y marcas de tiempo de autenticación.
- **User-ID Syslog Listener-SSL (SSL de escucha de Syslog de User-ID)** o **User-ID Syslog Listener-UDP (UDP de escucha de Syslog de User-ID)**: utilice esta opción para la Configuración de User-ID para supervisar los remitentes de Syslog para la asignación de usuarios en SSL o UDP.

4. (Opcional) Seleccione **Add (Añadir)** para añadir las direcciones IP permitidas que pueden acceder a la interfaz. Si no añade entradas a la lista, la interfaz no tendrá restricciones de direcciones IP.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Asigne el perfil de gestión de interfaz a una interfaz.

1. Seleccione **Network (Red)** > **Interfaces**, seleccione el tipo de interfaz (**Ethernet**, **VLAN**, **Loopback [Bucle invertido]** o **Tunnel [Túnel]**) y seleccione la interfaz.
2. Seleccione **Advanced (Avanzado)** > **Other info (Otra información)** y seleccione la interfaz **Management Profile (Perfil de gestión)** que acaba de añadir.
3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

Enrutadores virtuales

Obtenga información sobre cómo un enrutador virtual en el cortafuegos participa en el enrutamiento de capa 3 y configura un enrutador virtual.

> Descripción general del enrutador virtual
> Configuración de los enrutadores virtuales

Descripción general del enrutador virtual

El cortafuegos utiliza enrutadores virtuales para obtener rutas de capa 3 hacia otras subredes al definir de forma manual rutas estáticas o mediante la participación en uno o más protocolos de enrutamiento de capa 3 (rutas dinámicas). Las rutas que obtiene el cortafuegos mediante estos métodos completan la base de información de enrutamiento (routing information base, RIB) IP del cortafuegos. Cuando un paquete esté destinado a una subred diferente, el enrutador virtual obtendrá la mejor ruta de la RIB, la ubicará en la base de información de reenvío (FIB) y reenviará el paquete al siguiente enrutador de salto definido en la FIB. El cortafuegos utiliza la conmutación de Ethernet para llegar a otros dispositivos de la misma subred IP. (Una excepción para una mejor ruta que se dirige a la FIB se produce si utiliza ECMP, en cuyo caso todas las rutas a igual coste se encuentran en la FIB).

Las interfaces Ethernet, VLAN y del túnel definidas en el cortafuegos reciben y reenvían paquetes de capa 3. La zona de destino se deriva de la interfaz de salida basada en los criterios de reenvío y el cortafuegos consulta las reglas de la política para identificar las políticas de seguridad que se aplican a cada paquete. Además de enrutar a otros dispositivos de red, los enrutadores virtuales pueden enrutar a otros enrutadores virtuales en el mismo cortafuegos si se especifica un siguiente salto que señale a otro enrutador virtual.

Puede configurar interfaces de capa 3 en un enrutador virtual para participar con protocolos de enrutamiento dinámico (BGP, OSPF, OSPFv3 o RIP), así como añadir rutas estáticas. También puede crear varios enrutadores virtuales, cada uno de los cuales mantendrá un conjunto separado de rutas que no se comparten entre enrutadores virtuales, lo que le permitirá configurar diferentes comportamientos de enrutamiento para diferentes interfaces.

Puede configurar el enrutamiento dinámico de un enrutador virtual a otro al configurar una interfaz de bucle invertido en cada enrutador virtual, lo que crea una ruta estática entre las dos interfaces de bucle invertido y, a continuación, al configurar un protocolo de enrutamiento dinámico para que se interconecte entre estas dos interfaces.

Todas las interfaces de capa 3, de bucle invertido, de VLAN y de túnel definidas en el cortafuegos se deben asociar con un enrutador virtual. Si bien cada interfaz puede pertenecer a un único enrutador virtual, puede configurar varios protocolos de enrutamiento y rutas estáticas para un enrutador virtual. Más allá de las rutas estáticas y los protocolos de enrutamiento dinámico que se configuran para un enrutador virtual, es necesario contar con una configuración general.

Configuración de los enrutadores virtuales

Cree un enrutador virtual en el cortafuegos para que participe en el enrutamiento de capa 3.

STEP 1 | Obtenga la información necesaria de su administrador de red.

- Interfaces en el cortafuegos que desea para realizar el enrutamiento.
- Distancias administrativas para rutas estáticas, internas de OSFP, externas de OSPF, IBGP, EBGP y RIP.

STEP 2 | Cree un enrutador virtual y aplique interfaces a él.

El cortafuegos incluye un enrutador virtual denominado **default (predeterminado)**. Puede editar el enrutador virtual **default (predeterminado)** o añadir un nuevo enrutador virtual.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. Seleccione un enrutador virtual (**default [predeterminado]** o un enrutador virtual diferente) o haga clic en **Add (Añadir)** para añadir un nombre en **Name (Nombre)** para un nuevo enrutador virtual.
3. Seleccione **Router Settings (Configuración de enrutador)** > **General**.
4. En el cuadro **Interfaces**, haga clic en **Add (Añadir)** y seleccione una interfaz que ya esté definida.

   Repita este paso para todas las interfaces que desee añadir al enrutador virtual.
5. Haga clic en **OK (Aceptar)**.

STEP 3 | Establezca las distancias administrativas para las rutas estáticas y el enrutamiento dinámico.

Establezca las distancias administrativas para los tipos de rutas como sea necesario para su red. Cuando el enrutador virtual tiene dos o más rutas diferentes hacia el mismo destino, utiliza la distancia administrativa para seleccionar la mejor ruta de diferentes protocolos de enrutamiento y rutas estáticas, y prefiere una distancia menor.

- **Static (Estático)**: el intervalo es de 10 a 240; el valor predeterminado, 10.
- **OSPF Internal (OSPF interno)**: el intervalo es de 10 a 240; el valor predeterminado, 30.
- **OSPF External (OSPF externo)**: el intervalo es de 10 a 240; el valor predeterminado, 110.
- **IBGP**: el intervalo es de 10 a 240; el valor predeterminado, 200.
- **EBGP**: el intervalo es de 10 a 240; el valor predeterminado, 20.
- **RIP**: el intervalo es de 10 a 240; el valor predeterminado, 120.

Consulte ECMP si desea aprovechar varias rutas a igual coste para el reenvío.

STEP 4 | Confirme la configuración general del enrutador virtual.

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

STEP 5 | Configure las interfaces Ethernet, VLAN, de bucle invertido y de túnel como sea necesario.

Configuración de interfaces de capa 3.

Rutas de servicio

Obtenga información sobre cómo el cortafuegos usa rutas de servicio para enviar solicitudes a servicios externos y configurar rutas de servicio.

> Información general sobre las rutas de servicio
> Configuración de las rutas de servicio

Información general sobre las rutas de servicio

El cortafuegos utiliza la interfaz de gestión (MGT) de manera predeterminada para acceder a servicios externos, como los servidores DNS, los servidores de autenticación externa y los servicios de Palo Alto Networks® (como software, actualizaciones de URL, licencias y AutoFocus. Una alternativa al uso de la interfaz MGT es la configuración de un puerto de datos (una interfaz regular) para acceder a estos servicios. La ruta desde la interfaz al servicio en un servidor se conoce como ***ruta de servicio***. Los paquetes de servicio abandonan el cortafuegos en un puerto asignado al servicio externo y el servidor envía su respuesta a la interfaz de origen configurada y a la dirección IP de origen.

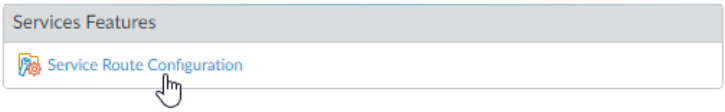
Puede Configuración de las rutas de servicio a nivel global para el cortafuegos o personalizar las rutas de servicio para un sistema virtual en un cortafuegos habilitado para varios sistemas virtuales a fin de que cuente con la flexibilidad para utilizar interfaces asociadas al sistema virtual. Cualquier sistema virtual que no tenga una ruta de servicio configurada para un servicio particular hereda una interfaz y dirección IP establecidas globalmente para ese servicio.

Configuración de las rutas de servicio

Mediante el siguiente procedimiento, puede configurar las rutas de servicio a fin de cambiar la interfaz que utiliza el cortafuegos para enviar solicitudes a los servicios externos.

STEP 1 | Personalice las rutas de servicio.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **Global** (omita la opción Global en un cortafuegos sin capacidad para varios sistemas virtuales), y en la sección Services Features (Funciones de servicio), haga clic en **Service Route Configuration (Configuración de ruta de servicio)**.



2. Seleccione **Customize (Personalizar)** y realice una de las siguientes tareas para crear una ruta de servicio:

   - Para un servicio predefinido:
     - Seleccione **IPv4** o **IPv6** y haga clic en el enlace del servicio cuya ruta de servicio desea personalizar.

       *Para utilizar la misma dirección de origen en varios servicios, seleccione la casilla de verificación de los servicios, haga clic en **Set Selected Routes (Establecer rutas seleccionadas)** y pase al siguiente paso.*

     - Para limitar la lista de direcciones de origen, seleccione una interfaz en **Source Interface (Interfaz de origen)** y, luego, una dirección de esa interfaz en **Source Address (Dirección de origen)** como ruta de servicio. También se puede hacer referencia a un objeto de dirección como una dirección de origen si ya está configurado en la interfaz seleccionada. Si selecciona **Any (Cualquiera)** en Source Interface (Interfaz de origen), están disponibles todas las direcciones IP de todas las interfaces en la lista Source Address (Dirección de origen) en la que debe seleccionar una dirección. Si selecciona **Use default (Utilizar predeterminado)**, el cortafuegos utilizará la interfaz de gestión para la ruta de servicio, a menos que la dirección IP de destino del paquete coincida con la dirección IP de destino configurada, en cuyo caso, la dirección IP de origen se establece como la **Source Address (Dirección de origen)** configurada para la dirección de **Destination (Destino)**. Si selecciona **MGT (Gestión)**, el cortafuegos utilizará la interfaz MGT (Gestión) en la ruta de servicio independientemente de la ruta de servicio de destino.

       La dirección de origen de la ruta de servicio no hereda los cambios de configuración de la interfaz a la que se hace referencia y viceversa. La modificación de una dirección IP de interfaz a una dirección IP u objeto de dirección diferente no actualizará una dirección de origen de ruta de servicio correspondiente. Esto puede provocar un error de confirmación y requerir que actualice la/s ruta/s de servicio a un valor de dirección de origen válido.

     - Haga clic en **OK (Aceptar)** para guardar la configuración.
     - Repita este paso si desea especificar las direcciones IPv4 e IPv6 de un servicio.

- Para una ruta de servicio de destino:
  - Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una dirección IP de **Destination (Destino)**. En este caso, si el paquete llega con una dirección IP de destino que coincide con esta dirección de **Destination (Destino)** configurada, la dirección IP de origen del paquete se establecerá como la **Source Address (Dirección de origen)** configurada en el siguiente paso.
  - Para limitar la lista de direcciones de origen, seleccione una interfaz en **Source Interface (Interfaz de origen)** y, luego, una dirección de esa interfaz en **Source Address (Dirección de origen)** como ruta de servicio. Si selecciona **Any (Cualquiera)** en Source Interface (Interfaz de origen), están disponibles todas las direcciones IP de todas las interfaces en la lista Source Address (Dirección de origen) en la que debe seleccionar una dirección. Si selecciona **MGT (Gestión)**, el cortafuegos utilizará la interfaz MGT (Gestión) en la ruta de servicio.
  - Haga clic en **OK (Aceptar)** para guardar la configuración.

3. Repita los pasos indicados anteriormente para cada ruta de servicio que desea personalizar.
4. Haga clic en **OK (Aceptar)** para guardar la configuración de la ruta de servicio.

STEP 2 | Seleccione **Confirmar**.

Rutas estáticas

Por lo general, las rutas estáticas se utilizan junto con protocolos de enrutamiento dinámico. Puede configurar una ruta estática para una ubicación que un protocolo de enrutamiento dinámico no puede alcanzar. Las rutas estáticas requieren una configuración manual en cada enrutador de la red, en lugar del cortafuegos que ingresa a las rutas dinámicas en sus tablas de rutas. A pesar de que las rutas estáticas requieren esa configuración en todos los enrutadores, es posible que se la recomiende para redes pequeñas en lugar de utilizarla para protocolo de enrutamiento.

> Descripción general de la ruta estática
> Eliminación de ruta estática basada en el control de ruta
> Configuración de una ruta estática
> Configuración del control de ruta para una ruta estática

Descripción general de la ruta estática

Si desea que el tráfico específico de la capa 3 tome una ruta determinada sin participar en los protocolos de enrutamiento IP, puede realizar el procedimiento Configuración de una ruta estática utilizando rutas IPv4 e IPv6.

Una ruta predeterminada es una ruta estática específica. Si no utiliza el enrutamiento dinámico para obtener una ruta predeterminada para su enrutador virtual, debe configurar una ruta estática predeterminada. Cuando el enrutador virtual posee un paquete entrante y no encuentra coincidencias para el destino del paquete en su tabla de rutas, el enrutador virtual envía el paquete a la ruta predeterminada. La ruta IPv4 predeterminada es 0.0.0.0/0; la ruta IPv6 predeterminada es ::/0. Puede configurar rutas predeterminadas para IPv4 y para IPv6.

Las rutas estáticas no cambian ni se ajustan a los cambios en los entornos de red, de modo que por lo general, el tráfico no se redirige si se produce una falla en la ruta hacia un extremo definido como estático. Sin embargo, cuenta con opciones para respaldar las rutas estáticas si se produce un problema:

- Puede configurar una ruta estática con un perfil de detección de reenvío bidireccional (bidirectional forwarding detection, BFD). Así, si falla la sesión de BFD entre el cortafuegos y el peer de BFD, el cortafuegos elimina la ruta estática fallida de las tablas de las bases de información de enrutamiento (routing information base, RIB) y de reenvío (forwarding information base, FIB) y utiliza una ruta alternativa de menor prioridad.
- Realice el procedimiento Configuración del control de ruta para una ruta estática para que el cortafuegos pueda utilizar una ruta alternativa.

De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 10. Cuando el cortafuegos tiene dos o más rutas hacia el mismo destino, utiliza la ruta con la menor distancia administrativa. Si se aumenta la distancia administrativa de una ruta estática a un valor mayor que el de una ruta dinámica, puede utilizar la ruta estática como una ruta de respaldo si la ruta dinámica no se encuentra disponible.

Cuando configura una ruta estática, puede especificar si el cortafuegos instala una ruta estática IPv4 en la tabla de rutas (RIB) de unidifusión o multidifusión, o en ambas tablas, o si no la instala. Por ejemplo, solo puede instalar una ruta estática IPv4 en la tabla de rutas de multidifusión debido a que solo desea que el tráfico multidifusión utilice esta ruta. Esta opción le proporciona más control sobre la ruta que toma el tráfico. Puede especificar si el cortafuegos instala una ruta estática IPv6 en la tabla de rutas de unidifusión o no.

Eliminación de ruta estática basada en el control de ruta

Cuando configura el control de red para una ruta estática, el cortafuegos utiliza el control de red para detectar cuando una ruta a uno o más destinos se ha caído. Así puede redirigir el tráfico por rutas alternativas. El cortafuegos utiliza el control de rutas para las rutas estáticas de manera similar al control de rutas para el reenvío HA o basado en políticas (policy-based forwarding, PBF), de la siguiente manera:

- El cortafuegos envía mensajes de ping ICMP (mensajes de heartbeat) a uno o más destinos controlados que usted determine que son robustos y que reflejan la disponibilidad de la ruta estática.
- Si los pings a cualquiera de los destinos, o a todos los destinos, fallan, el cortafuegos considera la ruta estática como inactiva también y la elimina de la base de información de enrutamiento (Routing Information Base, RIB) y la base de información de reenvío (Forwarding Information Base, FIB). La RIB es la tabla de rutas estáticas con las que el cortafuegos está configurado y las rutas dinámicas que detectó en los protocolos de enrutamiento. La FIB es la tabla de reenvío de rutas que el cortafuegos utiliza para el reenvío de paquetes. El cortafuegos selecciona una ruta estática alternativa hacia el mismo destino (según la ruta con la métrica más baja) desde la RIB y la coloca en la FIB.
- El cortafuegos continúa controlando la ruta que falló. Cuando la ruta se reactiva (según la condición de fallo **Any [Cualquiera]** o **All [Todos]**) y el control de ruta regresa al estado activo, se inicia el temporizador de tiempo de espera preferente. El control de ruta debe permanecer activo por la duración del temporizador de tiempo de espera; luego el cortafuegos considera la ruta estática como estable y la restablece en la RIB. El cortafuegos luego compara las métricas de las rutas hacia el mismo destino para decidir qué rutas corresponden a la FIB.

La supervisión de rutas es un mecanismo deseable para evitar el descarte de tráfico silenciosamente para los siguientes elementos:

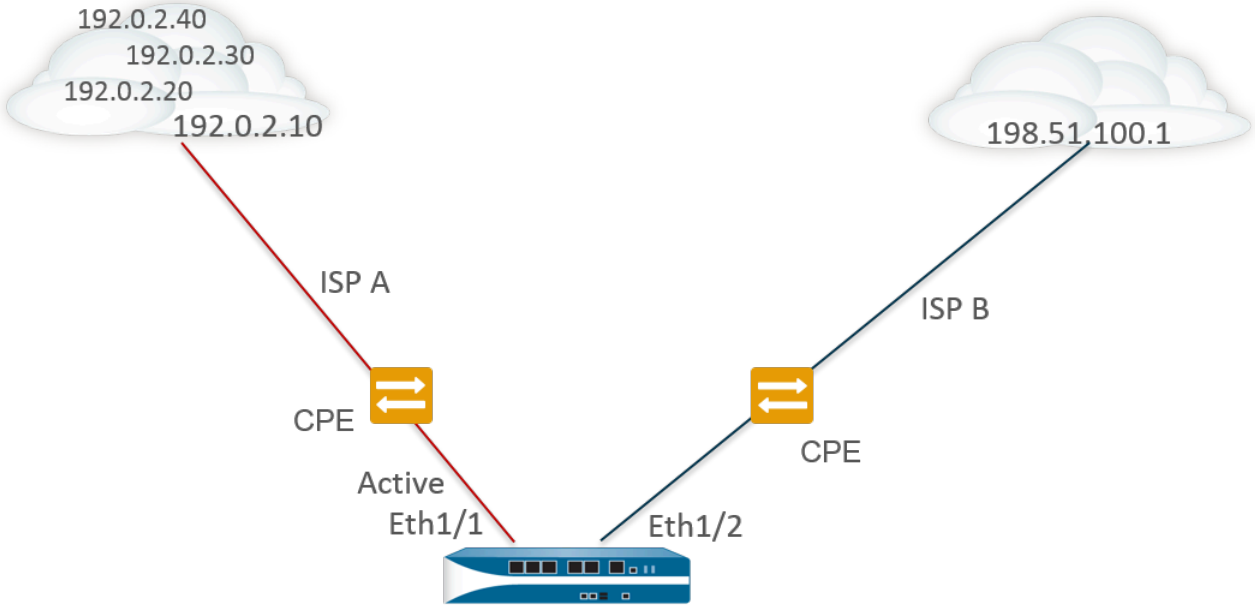
- Una ruta estática o predeterminada.
- Una ruta estática o predeterminada redistribuida a un protocolo de enrutamiento.
- Una ruta estática o predeterminada cuando un peer no admite BFD. (La práctica recomendada es no habilitar tanto BFD como el control de ruta en una misma interfaz).
- Una ruta estática o predeterminada en lugar de usar el control de ruta PBF, que no elimina una ruta estática que falló de la RIB, FIB o política de redistribución.

> ***El control de ruta no se aplica a las rutas estáticas configuradas entre enrutadores virtuales.***

En la siguiente figura, el cortafuegos está conectado a dos ISP para la redundancia de ruta a Internet. La ruta predeterminada principal 0.0.0.0 (métrica 10) utiliza el próximo salto 192.0.2.10; la ruta predeterminada secundaria 0.0.0.0 (métrica 50) utiliza el próximo salto 198.51.100.1. El equipo del cliente en las instalaciones (customer premises equipment, CPE) para ISP A mantiene el enlace físico principal activo, incluso después de que la conexión a Internet cae. Cuando el enlace está artificialmente activo, el cortafuegos no puede detectar que el enlace está inactivo y que debe reemplazar la ruta que falló por la ruta secundaria de la RIB.

Para evitar el descarte silenciosos del tráfico hacia un enlace erróneo, configure el control de ruta de 192.0.2.20, 192.0.2.30 y 192.0.2.40 y si todas las rutas (o algunas de las rutas) a estos destinos

fallan, el cortafuegos asume que la ruta al próximo salto 192.0.2.10 también está inactiva, elimina la ruta estática 0.0.0.0 (que utiliza el próximo salto 192.0.2.10) de su RIB y la reemplaza por la ruta secundaria al mismo destino 0.0.0.0 (que utiliza el próximo salto 198.51.100.1), que también accede a Internet.



Route Table

Destination	Next Hop	Metric	Interface	
0.0.0.0/0	192.0.2.10	10	ethernet1/1	X Pings to 192.0.2.20, 192.0.2.30, and 192.0.2.40 fail, so static route remove
0.0.0.0/0	198.51.100.1	50	ethernet1/2	

Cuando Configura una ruta estática, uno de los siguientes campos es el próximo salto hacia ese destino. El tipo de próximo salto que configure determinará la medida que tomará el cortafuegos durante el control de ruta, de la siguiente manera:

Si Next Hop Type (Tipo de próximo salto) en Static Route (Ruta estática) es:	Acción del cortafuegos para el ping ICMP
Dirección IP	El cortafuegos utiliza la dirección IP de origen y la interfaz de salida de la ruta estática como la dirección de origen e interfaz de salida en el ping ICMP. Utiliza la dirección IP de destino configurada del destino controlado como la dirección de destino del ping. Utiliza la dirección de próximo salto de la ruta como la dirección de próximo salto del ping.
Next VR (Siguiente VR)	El cortafuegos utiliza la dirección IP de origen de la ruta estática como la dirección de origen en el ping ICMP. La interfaz de salida se basa en el resultado de búsqueda del enrutador virtual de próximo salto. La dirección

Si Next Hop Type (Tipo de próximo salto) en Static Route (Ruta estática) es:	Acción del cortafuegos para el ping ICMP
	IP de destino configurada del destino controlado como es la dirección de destino del ping.
ninguno	El cortafuegos utiliza la dirección IP de destino del control de ruta como el próximo salto y envía el ping de ICMP a la interfaz especificada en la ruta estática.

Cuando el control de ruta para una ruta estática o predeterminada falla, el cortafuegos registra un evento crítico (ruta-control-fallo). Cuando la ruta estática o predeterminada se recupera, el cortafuegos registra otro evento crítico (ruta-contro-recuperación).

El cortafuegos sincroniza las configuraciones de control de ruta para una implementación HA activa/pasiva, pero el cortafuegos bloquea los paquetes de ping ICMP de salida en un peer HA pasivo, debido a que no procesa activamente el tráfico. El cortafuegos no sincroniza las configuraciones de control de ruta para las implementaciones HA activas/activas.

Configuración de una ruta estática

Realice la siguiente tarea para configurar las Rutas estáticas o una ruta predeterminada para un enrutador virtual en el cortafuegos.

STEP 1 | Configure una ruta estática.

1. Seleccione **Network (Red)** > **Virtual Router (Enrutador virtual)** y seleccione el enrutador virtual que desea configurar, como **default (predeterminado)**.
2. Seleccione la pestaña **Static Routes**.
3. Seleccione **IPv4** o **IPv6**, según el tipo de ruta estática que desee configurar.
4. **Add (Añada)** un **Name (Nombre)** para la ruta.
5. En **Destination (Destino)**, introduzca la ruta y la máscara de red (por ejemplo, 192.168.2.2/24 como dirección IPv4 o 2001:db8:123:1::1/64 como dirección IPv6). Si crea una ruta predeterminada, introduzca la ruta predeterminada (0.0.0.0/0 como dirección IPv4 o ::/0 como dirección IPv6). O bien, puede crear un objeto de dirección de tipo máscara de red IP.
6. (Opcional) En **Interface (Interfaz)**, especifique la interfaz saliente que utilizarán los paquetes para ir al próximo salto. Utilice este control más estricto en la interfaz que el cortafuegos utiliza en lugar de la interfaz en la tabla de rutas para el próximo salto de esta ruta.
7. En **Next Hop (Próximo salto)**, seleccione una de las siguientes opciones:
   - **IP Address (Dirección IP):** introduzca la dirección IP (por ejemplo, 192.168.56.1 o 2001:db8:49e:1::1) cuando desee enrutarla a un próximo salto específico. Debe **habilitar direcciones IPv6 en la interfaz** (cuando Configuración de interfaces de capa 3) para utilizar una dirección IPv6 de próximo salto. Si crea una ruta predeterminada, en **Next Hop (Próximo salto)**, debe seleccionar **IP Address (Dirección IP)** e introducir la dirección IP de su puerta de enlace de internet (por ejemplo, 192.168.56.1 o 2001:db8:49e:1::1). O bien, puede crear un objeto de dirección de tipo máscara de red IP. El objeto de dirección debe tener la máscara de red /32 para IPv4 o /128 para IPv6.
   - **Next VR (Próximo VR):** seleccione esta opción y seleccione un enrutador virtual si desea enrutarlo internamente a un enrutador virtual diferente en el cortafuegos.

- **FQDN**: introduzca un nombre de dominio completo (Fully Qualified Domain Name, FQDN), seleccione un objeto de dirección que utilice un FQDN o cree un objeto de dirección del tipo FQDN.

  Si utiliza un FQDN como siguiente salto de la ruta estática, se debe resolver en una dirección IP que pertenezca a la misma subred que la interfaz configurada para dicha ruta; de lo contrario, el cortafuegos rechaza la resolución y el FQDN se queda sin resolver.

  El cortafuegos solo emplea una dirección IP (de cada tipo de familia, esto es, IPv4 o IPv6) de la resolución de DNS del FQDN. Si se devuelven varias direcciones, el cortafuegos utiliza la dirección IP preferida que coincida con el tipo de familia de IP (IPv4 o IPv6) configurado para el siguiente salto. La dirección IP preferida es la primera dirección que devuelve el servidor DNS en su respuesta inicial. El cortafuegos la mantiene como preferida mientras siga apareciendo en las respuestas posteriores, aunque el orden sea distinto.

- **Discard (Descartar):** seleccione esta opción para descartar los paquetes que se dirigen a este destino.
- **None (Ninguno)**: seleccione esta opción si no existe el siguiente salto en la ruta. Por ejemplo, una conexión punto a punto no requiere un próximo salto debido a que solo existe una dirección de destino para los paquetes.

8. Introduzca una **Admin Distance (Distancia administrativa)** para que la ruta anule la distancia administrativa predeterminada establecida para las rutas estáticas en este enrutador virtual (intervalo de 10 a 240; valor predeterminado: 10).
9. Introduzca una **Metric (Métrica)** para la ruta (el intervalo es de 1 a 65 535).

STEP 2 | Seleccione la ubicación donde se instalará la ruta.

Seleccione la **Route Table (Tabla de rutas)** (RIB) en la que desea que el cortafuegos instale la ruta estática:

- **Unicast (Unidifusión):** instale la ruta en la tabla de rutas de unidifusión. Seleccione esta opción si desea que la ruta se utilice únicamente para el tráfico de rutas de unidifusión.
- **Multicast (Multidifusión):** instale la ruta en la tabla de rutas de multidifusión (disponible solo en el caso de las rutas IPv4). Seleccione esta opción si desea que la ruta se utilice únicamente para el tráfico de rutas de multidifusión.
- **Both (Ambas):** instale la ruta en la tabla de rutas de unidifusión y multidifusión (disponible solo en el caso de las rutas IPv4). Seleccione esta opción si desea que el tráfico de unidifusión o de multidifusión utilice esta ruta.
- **No Install (Sin instalación):** no instale la ruta en ninguna de las tablas de rutas.

STEP 3 | (Opcional) Si su modelo de cortafuegos admite BFD, puede aplicar un **perfil de BFD** a la ruta estática, de modo que si la ruta estática falla, el cortafuegos elimine la ruta de la RIB y la FIB, y utilice una ruta alternativa. El valor predeterminado es **None (Ninguna)**.

STEP 4 | Haga clic en **OK** dos veces.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Configuración del control de ruta para una ruta estática

Utilice el siguiente procedimiento para configurar la Eliminación de ruta estática basada en el control de ruta.

STEP 1 | Habilite el control de ruta para una ruta estática.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Static Routes (Rutas estáticas)**, **IPv4** o **IPv6**, y la ruta estática que desea controlar. Puede controlar hasta 128 rutas estáticas.
3. Seleccione **Path Monitoring (Control de ruta)** para habilitar el control para la ruta.

STEP 2 | Configure los destinos controlados para la ruta estática.

1. Seleccione **Add (Añadir)** para añadir un destino controlado por **Name (Nombre)**. Puede añadir hasta ocho destinos controlados por ruta estática.
2. Seleccione **Enable (Habilitar)** para controlar el destino.
3. Para **Source IP (IP de origen)**, seleccione la dirección IP que el cortafuegos utiliza en el ping ICMP para el destino controlado:
   - Si la interfaz tiene varias direcciones IP, seleccione una.
   - Si selecciona una interfaz, el cortafuegos utilizará la primera dirección IP asignada a la interfaz de forma predeterminada.
   - Si selecciona **DHCP (Use DHCP Client address) (DHCP (Usar la dirección del cliente DHCP))**, el cortafuegos utilizará la dirección que DHCP asignó a la interfaz. Para ver la dirección DHCP, seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet** y, en la fila de la interfaz Ethernet, haga clic en **Dynamic DHCP Client (Cliente DHCP dinámico)**. La dirección IP aparecerá en la ventana Estado de la interfaz IP dinámica.
4. Para **Destination IP (IP de destino)**, ingrese una dirección IP o un objeto de dirección para el cual el cortafuegos supervisará la ruta. El destino controlado y el destino de ruta estática deben usar la misma familia de direcciones (IPv4 o IPv6).

   La dirección IP de destino debe pertenecer a un endpoint confiable; no debería basar el control de ruta en un dispostivio que es inestable o no confiable.
5. (Opcional) Especifique el **Ping Interval (sec) (Intervalo de ping [s])** ICMP en segundos para determinar con qué frecuencia el cortafuegos supervisará la ruta (el intervalo es de 1 a 60 y el valor predeterminado es 3).
6. (Opcional) Especifique el **Ping Count (Recuento de pings)** ICMP de paquetes que no regresan del destino para que el cortafuegos considere la ruta estática como inactiva y la elimine de RIB y FIB (el intervalo es de 3 a 10; el valor predeterminado es 5).
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Determine si el control de ruta para la ruta estática se basa en uno o todos los destinos controlados, y configure el tiempo de retención preferente.

1. Seleccione una **Failure Condition (Condición de fallo)**, **Any (Cualquiera)** o **All (Todas)** de los destinos controlados para la ruta estática deben estar al alcance del ICMP para que el

cortafuegos elimine la ruta estática de RIB y FIB, y añada la ruta estática que contenga la siguiente métrica más baja al mismo destino en FIB.

*Seleccione **All (Todos)** para evitar la posibilidad de que un solo destino controlado designe un fallo de ruta cuando, por ejemplo, el destino esté simplemente fuera de línea para el mantenimiento.*

2. (Opcional) Especifique el **Preemptive Hold Time (min) (Tiempo de espera preferente [s])**, que es la cantidad de minutos que un monitor de ruta inactivo debe permanecer en estado activo para que el cortafuegos vuelva a instalar la ruta estática en RIB. El monitor de ruta evalúa todos sus destinos controlados para la ruta estática y aparece según la condición de fallo de **Any (Cualquiera)** o **All (Todos)**. Si el enlace se desactiva o fluctúa durante el tiempo de espera, cuando el enlace vuelve a estar activo, el monitor de ruta puede volver a activarse; el temporizador se reinicia cuando el monitor de ruta regresa al estado activo.

   Un **Preemptive Hold Time (Tiempo de espera preferente)** de cero hace que el cortafuegos vuelva a instalar la ruta en el RIB inmediatamente después de que el monitor de ruta se activa. El intervalo es de 0 a 1,440; el valor predeterminado es 2.
3. Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione Confirmar.

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

STEP 5 | Verifique el control de ruta en rutas estáticas.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual en el que está interesado, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. En la pestaña **Routing (Enrutamiento)**, seleccione **Static Route Monitoring (Control de ruta estática)**.
3. Para una ruta estática (Destino), visualice si el control de ruta está habilitado o inhabilitado. La columna Status (Estado) indica si la ruta está activa, inactiva o inhabilitada. Las marcas para la ruta estática son las siguientes: A: activa, S: estática; E: ECMP.
4. Seleccione **Refresh (Actualizar)** periódicamente para ver el estado más reciente del control de ruta (comprobación de estado).
5. Pase el ratón sobre el estado de una ruta para ver las direcciones IP controladas y los resultados de los pings enviados a los destinos controlados para esa ruta. Por ejemplo, 3/5 significa que un intervalo de ping de 3 segundos y un recuento de pings de 5 pings omitidos consecutivos (el cortafuegos no recibe ningún ping en los últimos 15 segundos) indica que el control de rutas detecta un fallo de enlace. Según la condición de fallo **Any (Cualquiera)** o **All (Todos)**, si el control de ruta está en modo de fallo y el cortafuegos recibe un ping después de 15 segundos, la ruta puede considerarse activa y se inicia el **Preemptive Hold Time (Tiempo de espera preferente)**.

   El estado indica los resultados del último ping controlado: correcto o fallido. El fallo indica que la serie de paquetes de ping (intervalo de pings multiplicado por el recuento de pings) no fue correcta. Un solo fallo de paquete de ping no refleja un estado de fallo de ping.

STEP 6 | Visualice el RIB y FIB para verificar que la ruta estática se haya eliminado.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual en el que está interesado, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. En la pestaña **Routing (Enrutamiento)**, seleccione **Route Table (Tabla de rutas)** (RIB) y luego la **Forwarding Table (Tabla de reenvío)** (FIB) para visualizar cada una, respectivamente.
3. Seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para visualizar la tabla de rutas correspondiente.
4. Para **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 and IPv6 (IPv4 e IPv6)**, **IPv4 Only (IPv4 únicamente)** o **IPv6 Only (IPv6 únicamente)**.
5. (Opcional) En el campo de filtros, ingrese la ruta que está buscando y seleccione la flecha o use la barra de desplazamiento para moverse por las páginas de rutas.
6. Determine si la ruta se eliminó o está presente.
7. Seleccione **Refresh (Actualizar)** periódicamente para ver el estado más reciente del control de ruta (comprobación de estado).

*Para visualizar los eventos registrados para el control de ruta, seleccione **Monitor (Supervisar)** > **Logs [Logs]** > **System (Sistema)**. Verifique la entrada para **path-monitor-failure (ruta-control-fallo)**, que indica el control de ruta para un destino de ruta estática fallido, de tal forma que la ruta se eliminó. Verifique la entrada para **path-monitor-recovery (ruta-control-recuperación)**, que indica el control de ruta para un destino de ruta estática recuperado, de tal forma que la ruta se restauró.*

RIP

Considere si RIP es un protocolo de enrutamiento apropiado para su red y, de ser así, configúrelo.

> Descripción general de RIP
> Configurar RIP

Descripción general de RIP

El protocolo de información de enrutamiento (RIP, Routing Information Protocol) es un protocolo de gateway interior (IGP, interior gateway protocol) diseñado para redes IP pequeñas. RIP se basa en el recuento de saltos para determinar las rutas; las mejores rutas tienen el menor número de saltos. RIP se basa en UDP y utiliza el puerto 520 para las actualizaciones de rutas. Al limitar las rutas a un máximo de 15 saltos, el protocolo ayuda a evitar el desarrollo de bucles de enrutamiento, pero también limita el tamaño de red admitido. Antes de configurar RIP, tenga en cuenta que, si se requieren más de 15 saltos, el tráfico no se enruta. RIP también puede tardar más en converger que OSPF y otros protocolos de enrutamiento.

El cortafuegos admite RIP v2.

Configurar RIP

Realice el siguiente procedimiento para configurar RIP:

STEP 1 | Configure los ajustes generales del enrutador virtual.

STEP 2 | Configure los ajustes de configuración general de RIP.

1. Seleccione un enrutador virtual (**Red** > **Enrutadores virtuales**) y, para el enrutador virtual, seleccione **RIP**.
2. Seleccione **Enable (Habilitar)** para habilitar el protocolo RIP.
3. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta predeterminada a través de RIP. Este es el ajuste predeterminado recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas predeterminadas mediante RIP.

STEP 3 | Configure interfaces para RIP.

1. En la sección de configuración de la interfaz de la pestaña **Interfaces**, seleccione una interfaz.
2. Seleccione una interfaz ya definida.
3. Seleccione **Enabled (Habilitado)**.
4. Seleccione **Advertise Default Route (Anunciar ruta predeterminada)** si desea anunciar una ruta predeterminada a los pares de RIP con el valor métrico especificado.
5. (Opcional) Seleccione un perfil en la lista **Auth Profile (Perfil de autenticación)**.
6. En la lista **Mode (Modo)**, seleccione normal (normal), passive (pasivo) o send-only (solo envío).
7. (Opcional) A fin de habilitar BFD para RIP a nivel global para el enrutador virtual, seleccione un perfil **BFD**.
8. Haga clic en **OK (Aceptar)**.

STEP 4 | Configure los temporizadores de RIP.

1. En la pestaña **Timers**, introduzca un valor para **Interval Seconds (sec)**. Mediante este ajuste, se define la duración de los siguientes intervalos del temporizador de RIP en segundos (el intervalo es de 1 a 60; el valor predeterminado es 1).
2. Especifique los **Intervalos de actualización** para definir el número de intervalos entre los anuncios de actualización de ruta (el intervalo es de 1 a 3600; el valor predeterminado es 30).
3. Especifique los **intervalos de vencimiento** para definir la cantidad de intervalos entre la última vez que se actualizó la ruta y su vencimiento (el intervalo es de 1 a 3600; el valor predeterminado es 120).
4. Especifique los **intervalos de eliminación** para definir el número de intervalos entre el momento en el que vence la ruta y su eliminación (el intervalo es de 1 a 3600; el valor predeterminado es 180).

STEP 5 | (Opcional) Configure perfiles de autenticación.

De manera predeterminada, el cortafuegos no utiliza autenticación de RIP para el intercambio entre vecinos de RIP. Opcionalmente, puede configurar una autenticación de RIP entre vecinos de RIP con una contraseña simple o la autenticación MD5. Se recomienda la autenticación MD5; es más segura que una contraseña simple.

Autenticación de contraseña simple de RIP

1. Seleccione **Auth Profiles (Perfiles de autenticación)** y haga clic en **Add (Añadir)** para añadir un nombre para el perfil de autenticación para autenticar los mensajes RIP.
2. Seleccione Contraseña simple como Tipo de contraseña.
3. Introduzca una contraseña simple y, a continuación, confírmela.

Autenticación MD5 de RIP

1. Seleccione **Auth Profiles (Perfiles de autenticación)** y haga clic en **Add (Añadir)** para añadir un nombre para el perfil de autenticación para autenticar los mensajes RIP.
2. Seleccione **MD5** como el **Password Type (Tipo de contraseña)**.
3. Haga clic en **Add (Añadir)** para añadir una o más entradas de contraseña, que incluyan las siguientes:
   - ID de clave (el intervalo es de 0 a 255)
   - Clave
4. (Opcional) Seleccione el estado **Preferred (Preferido)**.
5. Haga clic en **ACEPTAR** para especificar la clave que deberá utilizarse para autenticar el mensaje saliente.
6. Vuelva a hacer clic en **ACEPTAR** en el cuadro de diálogo Enrutador virtual - RIP - Perfil de autenticación.

STEP 6 | **Commit (Confirmar)** los cambios.

OSPF

Abrir primero la ruta libre más corta (OSPF) es un protocolo de gateway interior (IGP) que suele utilizarse la mayoría de las veces para gestionar de forma dinámica rutas de red en redes de empresas de gran tamaño. Determina las rutas de forma dinámica obteniendo la información de otros enrutadores y anunciando las rutas a otros enrutadores mediante anuncios de estado de enlaces (LSA, Link State Advertisements). La información recopilada de los LSA se utiliza para construir un mapa de topología de la red. Este mapa de topología se comparte entre los enrutadores de la red y se utiliza para cumplimentar la tabla de enrutamiento IP con rutas disponibles.

Los cambios en la topología de la red se detectan dinámicamente y se utilizan para generar un nuevo mapa de topología en cuestión de segundos. Se calcula un árbol con la ruta más corta de cada ruta. Se utilizan las medidas asociadas a cada interfaz de enrutamiento para calcular la mejor ruta. Pueden incluir distancia, rendimiento de red, disponibilidad de enlaces, etc. Además, estas medidas pueden configurarse de manera estática para dirigir el resultado del mapa de topología de OSPF.

La implementación de Palo Alto Networks® de OSPF admite los siguientes RFC en su totalidad:

- RFC 2328 (para IPv4)
- RFC 5340 (para IPv6)

Los siguientes temas ofrecen más información sobre el OSPF y los procedimientos para configurar OSPF en el cortafuegos:

- Conceptos de OSPF
- Configuración de OSPF
- Configuración de OSPFv3
- Configuración del reinicio correcto de OSPF
- Confirmación del funcionamiento de OSPF

Conceptos de OSPF

Los siguientes temas presentan los conceptos de OSPF que debe comprender para configurar el cortafuegos con el fin de que participe en una red OSPF:

- OSPFv3
- Vecinos OSPF
- Áreas OSPF
- Tipos de enrutadores OSPF

OSPFv3

OSPFv3 permite la compatibilidad con el protocolo de enrutamiento OSPF dentro de una red IPv6. Como tal, permite la compatibilidad con direcciones y prefijos IPv6. Conserva la mayor parte de la estructura y las funciones de OSPFv2 (para IPv4) con algunos cambios menores. A continuación se indican algunas de las adiciones y los cambios en OSPFv3:

- **Compatibilidad con varias instancias por enlace**: Con OSPFv3, puede ejecutar varias instancias del protocolo OSPF a través de un único enlace. Esto se consigue al asignar un número de ID de instancia de OSPFv3. Una interfaz que esté asignada a un ID de instancia descartará paquetes que contengan un ID diferente.
- **Procesamiento de protocolos por enlace**: OSPFv3 funciona según enlace en lugar de hacerlo según subred IP como en OSPFv2.
- **Cambios en las direcciones**: Las direcciones IPv6 no están presentes en paquetes OSPFv3, excepto en el caso de cargas de LSA en paquetes de actualización de estado de enlace. Los enrutadores vecinos se identifican mediante el ID de enrutador.
- **Cambios de autenticación**: OSPFv3 no incluye ninguna capacidad de autenticación. Para configurar OSPFv3 en un cortafuegos, es necesario un perfil de autenticación que especifique una carga de seguridad encapsulada (ESP) o un encabezado de autenticación (AH) de IPv6. El procedimiento de nueva asignación de claves especificado en el RFC 4552 no se admite en esta versión.
- **Compatibilidad con varias instancias por enlace**: Cada instancia se corresponde con un ID de instancia incluido en el encabezado de paquete OSPFv3.
- **Nuevos tipos de LSA**: OSPFv3 admite dos nuevos tipos de LSA: LSA de enlace y LSA de prefijo intraárea.

Todos los cambios adicionales se describen de manera detallada en el RFC 5340.

Vecinos OSPF

Dos enrutadores con OSPF conectados por una red común y en la misma área OSPF que forman una relación son vecinos OSPF. La conexión entre estos enrutadores puede ser a través de un dominio de difusión común o mediante una conexión de punto a punto. Esta conexión se realiza a través del intercambio de paquetes de saludo del protocolo OSPF. Estas relaciones de vecinos se utilizan para intercambiar actualizaciones de enrutamiento entre enrutadores.

Áreas OSPF

OSPF funciona en un único sistema autónomo (AS). No obstante, las redes de dentro de este AS único pueden dividirse en distintas áreas. De manera predeterminada, se crea el área 0. El área 0 puede funcionar por sí sola o actuar como la red troncal de OSPF para un mayor número de áreas. Cada área OSPF recibe un nombre que es un identificador de 32 bits, el cual, en la mayoría de los casos, se escribe en la misma notación decimal con puntos que una dirección IP4. Por ejemplo, el área 0 suele escribirse como 0.0.0.0.

La topología de un área se mantiene en su propia base de datos de estados de enlaces y se oculta de otras áreas, lo que reduce la cantidad de tráfico de enrutamiento que necesita OSPF. A continuación, la topología se comparte de manera resumida entre áreas mediante un enrutador de conexión.

Tipos de áreas OSPF	Description (Descripción)
Área troncal	El área troncal (Área 0) es el núcleo de una red OSPF. El resto de las áreas se conectan a ella y todo el tráfico entre las áreas debe atravesarla. Todo el enrutamiento entre las áreas se distribuye a través del área troncal. Si bien el resto de las áreas OSPF deben conectarse al área troncal, esta conexión no tiene que ser directa y puede realizarse a través de un enlace virtual.
Área OSPF normal	En un área OSPF normal no hay restricciones; el área puede aceptar todo tipo de rutas.
Área OSPF de código auxiliar	Un área de código auxiliar no recibe rutas de otros sistemas autónomos. El enrutamiento desde el área de código auxiliar se realiza a través de la ruta predeterminada hasta el área troncal.
Área de NSSA	El área de NSSA (Not So Stubby Area) es un tipo de área de código auxiliar que puede importar rutas externas con algunas excepciones limitadas.

Tipos de enrutadores OSPF

Dentro de un área OSPF, los enrutadores se dividen en las siguientes categorías.

- **Enrutador interno**: Enrutador que solamente tiene relaciones de vecino OSPF con los dispositivos de la misma área.
- **Enrutador de borde de área (ABR)**: un enrutador que tiene relaciones de vecino OSPF con los dispositivos de varias áreas OSPF. Los ABR recogen información de topología de sus áreas conectadas y la distribuyen al área troncal.
- **Enrutador de área troncal:** un enrutador de área troncal es un enrutador que ejecuta OSPF y cuenta con, al menos, una interfaz conectada al área troncal OSPF. Como los ABR siempre están conectados a la red troncal, siempre se clasifican como enrutadores troncales.
- **Enrutador de límite de sistema autónomo (ASBR)**: Enrutador que se conecta a más de un protocolo de enrutamiento e intercambia información de enrutamiento entre ellos.

Configuración de OSPF

OSPF determina las rutas de forma dinámica obteniendo la información de otros enrutadores y anunciando las rutas a otros enrutadores mediante anuncios de estado de enlaces (LSA). El enrutador mantiene la información sobre los enlaces entre él y el destino y puede realizar decisiones de enrutamiento con gran eficiencia. Se asigna un coste a cada interfaz de enrutador y las mejores rutas son aquellas con menor coste, después de sumar todas las interfaces de enrutador saliente detectadas y la interfaz que recibe los LSA.

Las técnicas jerárquicas se utilizan para limitar el número de rutas que se deben anunciar y los LSA asociados. Como OSPF procesa dinámicamente una cantidad considerable de información de enrutamiento, tiene mayores requisitos de procesador y memoria que RIP.

STEP 1 | Configure los ajustes generales del enrutador virtual.

STEP 2 | Habilite OSPF.

1. Seleccione la pestaña OSPF.
2. Seleccione **Enable** para habilitar el protocolo OSPF.
3. Introduzca el **Router ID (Identificador de enrutador)**.
4. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta predeterminada a través de OSPF. Este es el ajuste predeterminado recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas por defecto a través de OSPF.

STEP 3 | Configure el tipo de áreas para el protocolo OSPF.

1. En la pestaña **Areas (Áreas)**, seleccione **Add (Añadir)** para añadir un **Area ID (Identificador de área)** para el área, con formato ***x.x.x.x***. Es el identificador que cada vecino debe aceptar para formar parte de la misma área.
2. En la pestaña **Type (Tipo)**, seleccione una de las siguientes opciones de la lista **Type (Tipo)** del área:
   - **Normal**: no hay restricciones; el área puede aceptar todos los tipos de rutas.
   - **Stub (Código auxiliar)**: no hay salida desde el área. Para acceder a un destino fuera del área, es necesario atravesar el límite, que conecta con el resto de áreas. Si selecciona esta opción, configure lo siguiente:
     - **Aceptar resumen**: Los anuncios de estado de enlaces (LSA) se aceptan desde otras áreas. Si esta opción de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está deshabilitada, el área OSPF se comportará como un área totalmente de código auxiliar (TSA) y ABR no propagará ninguno de los LSA de resumen.
     - **Advertise Default Route (Anunciar ruta predeterminada)**: los LSA de ruta por defecto se incluirán en los anuncios al área de código auxiliar junto con un valor de medida configurado dentro del intervalo configurado 1-255.
   - **NSSA**: el cortafuegos solamente puede salir del área por rutas que no sean rutas de OSPF. Si selecciona NSSA, seleccione **Accept Summary (Aceptar resumen)** y **Advertise**

Default Route (Anunciar ruta predeterminada) como se describió para el **Stub (Código auxiliar)**. Si selecciona esta opción, configure lo siguiente:

- **Type (Tipo)**: Seleccione el tipo de ruta **Ext 1** o **Ext 2** para anunciar el LSA predeterminado.
- **Ext Ranges (Intervalos externos)**: seleccione **Add (Añadir)** para añadir intervalos de rutas externas que desee en **Advertise (Anunciar)** o para los que desee **Suppress (Suprimir)** el anuncio.

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

STEP 4 | Configure el intervalo de áreas para el protocolo OSPF.

1. En la pestaña **Range (Intervalo)**, haga clic en **Add (Añadir)** para añadir direcciones de destino LSA agrupadas en el área en subredes.
2. Seleccione **Anunciar** o **Suprimir** los anuncios de LSA que coincidan con la subred y haga clic en **ACEPTAR**. Repita esta acción para añadir intervalos adicionales.

STEP 5 | Configure las interfaces de áreas para el protocolo OSPF.

1. En la pestaña **Interface (Interfaz)**, haga clic en **Add (Añadir)** e ingrese la siguiente información para cada interfaz que se incluirá en el área:
   - **Interface (Interfaz)**: seleccione una interfaz.
   - **Enable (Habilitar)**: al seleccionar esta opción, la configuración de la interfaz OSPF surte efecto.
   - **Passive**: seleccione esta opción si no desea que la interfaz OSPF envíe o reciba paquetes OSPF. Aunque los paquetes OSPF no se envían ni reciben, si selecciona esta opción, la interfaz se incluirá en la base de datos de LSA.
   - **Link type**: seleccione **Broadcast** si desea poder acceder a todos los vecinos mediante la interfaz y poder detectarlos automáticamente por mensajes de saludo OSPF de multidifusión, como una interfaz Ethernet. Seleccione **p2p** (punto a punto) para descubrir al vecino automáticamente. Elija **p2mp** (punto a multipunto) cuando los vecinos deban definirse manualmente y seleccione **Add (Añadir)** para añadir las direcciones IP vecinas para todos los vecinos cercanos a través de esta interfaz.
   - **Metric**: introduzca una métrica OSPF para esta interfaz (el intervalo es 0-65.535; el valor por defecto es 10).
   - **Prioridad**: Introduzca una prioridad de OSPF para esta interfaz. Esta es la prioridad del enrutador para ser el enrutador designado (DR) o de reserva (BDR) según el protocolo OSPF (intervalo: 0-255; predeterminado: 1). Si el valor se configura como cero, el enrutador no se designará como DR ni BDR.
   - **Auth Profile**: seleccione un perfil de autenticación definido previamente.
   - **Timing (Sincronización)**: modifique los ajustes de sincronización si lo desea (no recomendado). Si desea obtener información detallada sobre estos ajustes, consulte la ayuda en línea.
2. Haga clic en **OK (Aceptar)**.

STEP 6 | Configure enlaces virtuales de áreas.

1. En la pestaña **Virtual Link (Enlace virtual)**, haga clic en **Add (Añadir)** e ingrese la siguiente información para cada enlace virtual que se incluirá en el área troncal:
   - **Name**: introduzca un nombre para el enlace virtual.
   - **Enable**: seleccione para habilitar el enlace virtual.
   - **Neighbor ID**: introduzca el ID del enrutador (vecino) del otro lado del enlace virtual.
   - **Transit Area**: introduzca el ID del área de tránsito que contiene físicamente al enlace virtual.
   - **Timing**: es recomendable que mantenga su configuración temporal por defecto.
   - **Auth Profile**: seleccione un perfil de autenticación definido previamente.
2. Haga clic en **OK (Aceptar)** para guardar los enlaces virtuales.
3. Haga clic en **OK (Aceptar)** para guardar el área.

STEP 7 | (Opcional) Configure perfiles de autenticación.

De manera predeterminada, el cortafuegos no utiliza autenticación de OSPF para el intercambio entre vecinos OSPF. Opcionalmente, puede configurar una autenticación de OSPF entre vecinos OSPF mediante una contraseña simple o mediante la autenticación MD5. Se recomienda la autenticación MD5; es más segura que una contraseña simple.

Autenticación de contraseña simple de OSPF

1. Seleccione la pestaña **Auth Profiles (Perfiles de autenticación)** y luego **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPF.
2. Seleccione Contraseña simple como Tipo de contraseña.
3. Introduzca una contraseña simple y, a continuación, confírmela.

Autenticación MD5 de OSPF

1. Seleccione la pestaña **Auth Profiles (Perfiles de autenticación)** y luego **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPF.
2. Seleccione **MD5** como el **Password Type (Tipo de contraseña)** y luego **Add (Añadir)** para añadir una o más entradas de contraseña, incluidas las siguientes:
   - ID de clave (intervalo: 0-255)
   - Clave
   - Seleccione la opción Preferido para especificar que la clave debe utilizarse para autenticar mensajes salientes.
3. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure las opciones avanzadas de OSPF.

1. En la pestaña **Advanced (Avanzado)**, seleccione **RFC 1583 Compatibility (Compatibilidad con RFC 1583)** para garantizar la compatibilidad con RFC 1583.
2. Especifique un valor para el temporizador **SPF Calculation Delay (sec) (Retardo de cálculo SPF [s])**, que le permite definir el retraso de tiempo (en segundos) entre la recepción de nueva información de topología y la ejecución de un cálculo SPF. Los valores menores permiten una reconvergencia OSPF más rápida. Los enrutadores que se emparejan

con el cortafuegos deben usar el mismo valor de retardo para optimizar los tiempos de convergencia.

3. Especifique un valor para el temporizador **LSA Interval (sec) (Intervalo LSA [s])**, que es el tiempo mínimo entre las transmisiones de dos instancias del mismo LSA (mismo enrutador, mismo tipo, mismo ID de LSA). Es un equivalente de MinLSInterval en RFC 2328. Los valores más bajos se pueden utilizar para reducir los tiempos de reconvergencia cuando se producen cambios en la tipología.
4. Haga clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios.

Configuración de OSPFv3

OSPF admite IPv4 e IPv6. Debe OSPFv3 si está utilizando IPv6.

STEP 1 | Configure los ajustes generales del enrutador virtual.

STEP 2 | Configure los ajustes de configuración general de OSPFv3.

1. Seleccione la pestaña **OSPFv3**.
2. Seleccione **Enable** para habilitar el protocolo OSPF.
3. Introduzca el **Router ID (Identificador de enrutador)**.
4. Seleccione la casilla **Reject Default Route (Rechazar ruta predeterminada)** si no desea conocer ninguna ruta por defecto a través de OSPFv3. Este es el ajuste por defecto recomendado.

   Cancele la selección de **Reject Default Route (Rechazar ruta predeterminada)** si desea permitir la redistribución de rutas predeterminadas a través de OSPFv3.

STEP 3 | Configure el perfil de autenticación para el protocolo OSPFv3.

OSPFv3 no incluye ninguna capacidad de autenticación propia; se basa completamente en IPSec para proteger las comunicaciones entre vecinos.

Al configurar un perfil de autenticación, debe utilizar una carga de seguridad encapsulada (Encapsulating Security Payload, ESP) o un encabezado de autenticación (Authentication Header, AH) de IPv6.

Autenticación de ESP OSPFv3

1. En la pestaña **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPFv3.
2. Especifique un índice de política de seguridad (**SPI**) (valor hexadecimal en el intervalo de 00000000 a FFFFFFFF). Los dos extremos de la adyacencia OSPFv3 debe incluir valores SPI coincidentes.
3. Seleccione **ESP** como **Protocol (Protocolo)**.
4. Seleccione el valor adecuado en **Crypto Algorithm (Algoritmo criptográfico)**.

   Puede seleccionar **None (Ninguno)** o alguno de los siguientes algoritmos: SHA1, SHA256, SHA384, SHA512 o MD5.
5. Si se seleccionó un **Crypto Algorithm (Algoritmo criptográfico)** en lugar de no seleccionar ningún valor, ingrese un valor para **Key (Clave)** y, a continuación, confírmelo.

Autenticación de AH OSPFv3

1. En la pestaña **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un nombre para el perfil de autenticación, a fin de autenticar los mensajes OSPFv3.
2. Especifique un índice de política de seguridad (**SPI**). El SPI debe coincidir entre ambos extremos de la adyacencia de OSPFv3. El número del SPI debe ser un valor hexadecimal entre 00000000 y FFFFFFFF.
3. Seleccione **AH** como **Protocolo**.
4. Seleccione el valor adecuado en **Crypto Algorithm (Algoritmo criptográfico)**.

   Debe introducir uno de los siguientes algoritmos: SHA1, SHA256, SHA384, SHA512 o MD5.
5. Introduzca un valor para **Clave** y, a continuación, confírmelo.
6. Haga clic en **OK (Aceptar)**.
7. Vuelva a hacer clic en **OK (Aceptar)** en el cuadro de diálogo Enrutador virtual - OSPF - Perfil de autenticación.

STEP 4 | Configure Areas - Type (Áreas - Tipo) para el protocolo OSPFv3.

1. En la pestaña **Areas (Áreas)**, seleccione **Add (Añadir)** para añadir un **Area ID (Identificador de área)**. Es el identificador que cada vecino debe aceptar para formar parte de la misma área.
2. En la pestaña **General**, seleccione una de las siguientes opciones de la lista **Type (Tipo)** del área:
   - **Normal**: no hay restricciones; el área puede aceptar todos los tipos de rutas.
   - **Stub (Código auxiliar)**: no hay salida desde el área. Para acceder a un destino fuera del área, es necesario atravesar el límite, que conecta con el resto de áreas. Si selecciona esta opción, configure lo siguiente:
     - **Aceptar resumen**: Los anuncios de estado de enlaces (LSA) se aceptan desde otras áreas. Si esta opción de un área de código auxiliar de la interfaz de enrutador de borde de área (ABR) está deshabilitada, el área OSPF se comportará como un área totalmente de código auxiliar (TSA) y ABR no propagará ninguno de los LSA de resumen.
     - **Advertise Default Route (Anunciar ruta predeterminada)**: los LSA de ruta por defecto se incluirán en los anuncios al área de código auxiliar junto con un valor de medida configurado dentro del intervalo configurado 1-255.
   - **NSSA**: el cortafuegos solamente puede salir del área por rutas que no sean rutas de OSPF. Si está seleccionado, configure Aceptar resumen y Anunciar ruta predeterminada como se describe para Código auxiliar. Si selecciona esta opción, configure lo siguiente:
     - **Type (Tipo)**: Seleccione el tipo de ruta **Ext 1** o **Ext 2** para anunciar el LSA predeterminado.
     - **Ext Ranges (Intervalos extendidos)**: haga clic en **Add (Añadir)** para añadir intervalos de rutas externas para los que desee habilitar o suprimir los anuncios.

STEP 5 | Asocie un perfil de autenticación OSPFv3 a un área o una interfaz.

Para un área

1. En la pestaña **Areas (Áreas)**, seleccione un área existente de la tabla.
2. En la pestaña **General**, seleccione un perfil definido previamente con la opción **Authentication Profile (Perfil de autenticación)** de la lista **Authentication (Autenticación)**.
3. Haga clic en **OK (Aceptar)**.

Para una interfaz

1. En la pestaña **Areas (Áreas)**, seleccione un área existente de la tabla.
2. Seleccione la pestaña **Interface (Interfaz)** y haga clic en **Add (Añadir)** para añadir el perfil de autenticación que desea asociar a la interfaz de OSPF de la lista **Auth Profile (Perfil de autenticación)**.
3. Haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **OK (Aceptar)** para guardar la configuración del área.

STEP 7 | (Opcional) Configure reglas de exportación.

1. En la pestaña **Export Rules (Reglas de exportación)**, seleccione **Allow Redistribute Default Route (Permitir redistribución de ruta predeterminada)** para permitir la redistribución de rutas predeterminadas a través de OSPFv3.
2. Haga clic en **Add (Añadir)**.
3. Ingrese un nombre en **Name**: el valor debe ser una subred IPv6 válida o un nombre de perfil de redistribución válido.
4. Seleccione **New Path Type (Nuevo tipo de ruta)**, **Ext 1** o **Ext 2**.
5. Especifique una **New Tag (Nueva etiqueta)** para la ruta coincidente que tenga un valor de 32 bits en notación decimal con punto.
6. Asigne una **Metric (Métrica)** para la nueva regla (el intervalo es 1 a 16,777,215).
7. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure las opciones avanzadas de OSPFv3.

1. En la pestaña **Advanced (Avanzado)** seleccione la casilla de verificación **Disable Transit Routing for SPF Calculation (Deshabilitar el enrutamiento de tránsito para el cálculo de SPF)** si desea que el cortafuegos participe en la distribución de la topología de OSPF sin ser utilizado para reenviar tráfico de tránsito.
2. Especifique un valor para el temporizador **SPF Calculation Delay (sec) (Retardo de cálculo SPF [s])**, que le permite definir el retraso de tiempo (en segundos) entre la recepción de nueva información de topología y la ejecución de un cálculo SPF. Los valores menores permiten una reconvergencia OSPF más rápida. Los enrutadores que se emparejan con el cortafuegos deben usar el mismo valor de retardo para optimizar los tiempos de convergencia.
3. Especifique un valor para el temporizador **LSA Interval (sec) (Intervalo LSA [s])**, que es el tiempo mínimo (en segundos) entre las transmisiones de dos instancias del mismo LSA (mismo enrutador, mismo tipo, mismo ID de LSA). Es un equivalente de MinLSInterval en RFC 2328. Los valores más bajos se pueden utilizar para reducir los tiempos de reconvergencia cuando se producen cambios en la tipología.
4. (Opcional) Configuración del reinicio correcto de OSPF.
5. Haga clic en **OK (Aceptar)**.

STEP 9 | **Commit (Confirmar)** los cambios.

Configuración del reinicio correcto de OSPF

El reinicio correcto de OSPF dirige a los vecinos OSPF para que sigan utilizando rutas mediante un cortafuegos durante una breve transición cuando esté fuera de servicio. Este comportamiento aumenta la estabilidad de red reduciendo la frecuencia de reconfiguración de la tabla de enrutamiento y los flaps de ruta relacionados que pueden producirse durante breves tiempos de inactividad periódicos.

En el caso de un cortafuegos de Palo Alto Networks®, el reinicio correcto de OSPF implica las siguientes operaciones:

- **Cortafuegos como dispositivo de reinicio**: si el cortafuegos estará inactivo durante un breve periodo de tiempo o no estará disponible durante intervalos breves, enviará LSA de gracia a sus vecinos OSPF. Los vecinos deben configurarse para ejecutarse en modo auxiliar de reinicio correcto. En el modo auxiliar, los vecinos reciben los LSA de gracia que le informan de que el cortafuegos realizará un reinicio correcto en un periodo de tiempo especificado definido como el **Periodo de gracia**. Durante el periodo de gracia, el vecino sigue reenviando rutas a través del cortafuegos y enviando LSA que anuncian rutas a través del cortafuegos. Si el cortafuegos reanuda su funcionamiento antes de que venza el periodo de gracia, el reenvío de tráfico seguirá como antes sin ninguna interrupción de la red. Si el cortafuegos no reanuda su funcionamiento después de que venza el periodo de gracia, los vecinos saldrán del modo auxiliar y reanudarán el funcionamiento normal, lo que implicará la reconfiguración de la tabla de enrutamiento para eludir el cortafuegos.
- **Cortafuegos como auxiliar de reinicio correcto:** si es posible que los enrutadores vecinos estén inactivos durante breves períodos de tiempo, se puede configurar el cortafuegos para que funcione en el modo auxiliar de reinicio correcto, en cuyo caso, el cortafuego emplea un **Max Neighbor Restart Time (Tiempo de reinicio máximo de vecinos)**. Cuando el cortafuegos reciba los LSA de gracia de su vecino OSPF, seguirá enrutando tráfico hacia el vecino y anunciando rutas a través del vecino hasta que venza el periodo de gracia o hasta alcanzar el tiempo máximo de reinicio del mismo nivel. Si ninguno de los dos vence antes de que el vecino vuelva a estar en funcionamiento, el reenvío de tráfico continuará como antes sin ninguna interrupción de la red. Si ninguno de los dos periodos vence antes de que el vecino vuelva a estar en funcionamiento, el cortafuegos saldrá del modo auxiliar y reanudará el funcionamiento normal, lo que implicará la reconfiguración de la tabla de enrutamiento para eludir el vecino.

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que desea configurar.

STEP 2 | Seleccione **OSPF** > **Advanced (Avanzado)** o **OSPFv3** > **Advanced (Avanzado)**.

STEP 3 | Verifique que las siguientes casillas de verificación están seleccionadas (están habilitadas por defecto):

- **Habilitar reinicio correcto**
- **Habilitar modo auxiliar**
- **Habilitar comprobación de LSA estricta**

Las tres opciones deberían permanecer seleccionadas a menos que su topología requiera lo contrario.

STEP 4 | Configure un **Período de gracia** en segundos.

STEP 5 | Configure un **Max Neighbor Restart Time (Tiempo máx. de reinicio del mismo nivel)** en segundos.

Confirmación del funcionamiento de OSPF

Una vez se haya compilado una configuración de OSPF, podrá utilizar cualquiera de las operaciones siguientes para confirmar que OSPF está funcionando:

- Visualización de la tabla de enrutamiento
- Confirmación de adyacencias OSPF
- Confirmación de que se han establecido conexiones OSPF

Visualización de la tabla de enrutamiento

Al visualizar la tabla de enrutamiento, puede ver si se han establecido rutas OSPF. Se puede acceder a la tabla de enrutamiento desde la interfaz web o la CLI. Si está utilizando la CLI, utilice los siguientes comandos:

- **`show routing route`**
- **`show routing fib`**

Si utiliza la interfaz web para ver la tabla de enrutamiento, utilice el siguiente flujo de trabajo:

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la misma fila del enrutador virtual en el que está interesado, haga clic en el enlace **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 2 | Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de rutas)** y examine la columna **Flags (Marcas)** de la tabla de enrutamiento para determinar qué rutas ha obtenido OSPF.

Confirmación de adyacencias OSPF

Utilice el siguiente flujo de trabajo para confirmar que se establezcan las adyacencias OSPF:

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la misma fila del enrutador virtual en el que está interesado, haga clic en el enlace **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 2 | Seleccione **OSPF** > **Neighbor (Vecino)** y examine la columna **Status (Estado)** para determinar si se establecieron adyacencias OSPF.

Confirmación de que se han establecido conexiones OSPF

Visualice el log del sistema para confirmar que el cortafuegos haya establecido conexiones OSPF.

STEP 1 | Seleccione **Monitor (Supervisar)** > **System (Sistema)** y observe los mensajes para confirmar que se establecieron adyacencias OSPF.

STEP 2 | Seleccione **OSPF** > **Neighbor (Vecino)** y examine la columna **Status (Estado)** para determinar si se establecieron adyacencias OSPF (completas).

BGP

El protocolo de gateway de borde (BGP) es el principal protocolo de enrutamiento de Internet. BGP determina el alcance de la red en función de los prefijos IP que están disponibles en sistemas autónomos (AS), donde un sistema autónomo es un conjunto de prefijos IP que un proveedor de red ha designado para formar parte de una política de enrutamiento simple.

> Descripción general del BGP
> MP-BGP
> Configuración de BGP
> Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6
> Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4
> Confederaciones BGP

Descripción general del BGP

El BGP funciona entre sistemas autónomos (BGP externo o eBGP) o dentro de un AS (BGP interno o iBGP) para intercambiar información de enrutamiento y alcance con los emisores del BGP. El cortafuegos proporciona una implementación completa de BGP que incluye las siguientes funciones:

- Especificación de una instancia de enrutamiento BGP por enrutador virtual.
- Configuración de BGP por enrutador virtual, que incluye parámetros básicos como ID de ruta local y AS local, y opciones avanzadas como selección de ruta, reflector de ruta, confederaciones BGP, amortiguación de flap de ruta y reinicio correcto.
- Configuración de vecino y grupos de peers, que incluye direcciones de vecino y AS remotos, y opciones avanzadas como atributos y conexiones de vecino.
- Políticas de enrutamiento para controlar los procesos de importación, exportación y anuncios de rutas; filtrado basado en prefijos; y agregación de direcciones.
- Interacción IGP-BGP para introducir rutas en BGP utilizando perfiles de redistribución.
- Perfiles de autenticación que especifican la clave de autenticación MD5 para conexiones BGP. La autenticación permite prevenir fugas de rutas y ataques exitosos al DoS.
- El BGP multiprotocolo (MP-BGP), que permite a los peers de BGP transportar rutas de unidifusión IPv6 y rutas de multidifusión IPv4 en paquetes de actualización, y permite al cortafuegos y a un peer de BGP comunicarse entre sí mediante direcciones IPv6.
- BGP admite un máximo de 255 números AS en una lista de AS_PATH para un prefijo.

MP-BGP

BGP admite prefijos de unidifusión IPv4, pero una red BGP que utiliza rutas multidifusión IPv4 o prefijos de unidifusión IPv6 necesita BGP multiptotocolo (MP-BGP) a fin de intercambiar rutas de tipos de direcciones que no sean unidifusión IPv4. MP-BGP permite a los peers BGP que transporten rutas multidifusión IPv4 y rutas unidifusión IPv6 en paquetes de actualización, además de las rutas unidifusión IPv4 que los peers BGP pueden transportar sin habilitar MP-BGP.

De esta manera, MP-BGP proporciona conectividad IPv6 para sus redes BGP que utilizan IPv6 nativa o IPv4 e IPv6 de pila doble. Los proveedores de servicio pueden ofrecer servicio IPv6 a sus clientes y las empresas pueden usar servicio IPv6 de los proveedores de servicio. El cortafuegos y un peer BGP pueden comunicarse entre sí usando direcciones IPv6.

A fin de que BGP admita protocolos de capa de red múltiples (que no sea BGP para IPv4), extensiones multiprotocolo para BGP-4 (RFC 4760), utilice la información de disponibilidad de capa de red (Network Layer Reachability Information, NLRI) en un atributo NLRI alcanzable multiprotocolo que el cortafuegos envía y recibe en paquetes de actualización BGP. El atributo contiene información sobre el prefijo de destino, incluidos estos dos identificadores:

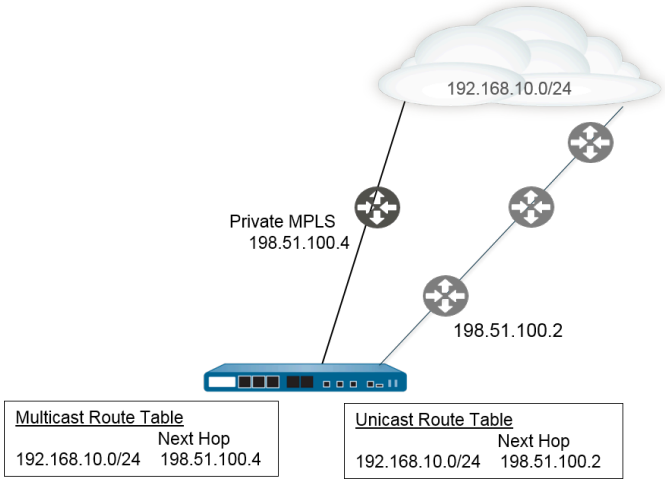
- El identificador de familia de direcciones (Address Family Identifier, AFI), según se define en IANA en Números de familia de direcciones, indica que el prefijo de destino es una dirección IPv4 o IPv6. (PAN-OS admite AFI IPv4 e IPv6).
- El identificador de familia de direcciones posterior (SAFI) en PAN-OS indica que el prefijo de destino es una dirección de unidifusión o multidifusión (si AI es IPv4) o que el prefijo de destino es una dirección de unidifusión (si el AFI es IPv6). PAN-OS no admite multidifusión IPv6.

Si usted habilita MP-BGP para la multidifusión IPV4 o si configura una ruta est´tica de multidifusión, el cortafuegos admite tablas de ruta de unidifusión y multidifusión separadas para las rutas estáticas. Es posible que desee separar el tráfico de unidifusión y multidifusión que va al mismo destino. El tráfico de multidifusión puede tomar una ruta diferente del tráfico de unidifusión ya que, por ejemplo, su tráfico de multidifusión es crítico, por lo que debe ser más eficiente, con menos saltos, o someterse a una menor latencia.

También puede ejercer más control sobre el funcionamiento de BGP al configurar BGP para que utilice rutas solo de la tabla de rutas de unidifusión o multidifusión (o ambas) cuando BGP importa o exporta rutas, envía anuncios condicionales o realiza la redistribución o agregación de rutas.

Usted puede decidir usar un RIB de multidifusión (tabla de rutas) al habilitar MP-BGP y seleccionar la familia de direcciones de IPv4 y la familia de direcciones posteriores de multidifusión, o al instalar una ruta estática IPv4 en la tabla de rutas de multidifusión. Después de aplicar cualquiera de los métodos para usar el RIB de multidifusión, el cortafuegos usa el RIB de multidifusión para todo el enrutamiento de multidifusión y envío de rutas inverso (RPF). Si prefiere usar el RIB de unidifusión para todo el enrutamiento (unidifusión y multidifusión) no debe habilitar el RIB de multidifusión por ninguno de los métodos.

En la siguiente figura, una ruta estática a 192.168.10.0/24 está instalada en la tabla de ruta de unidifusión, y el siguiente salto es 198.51.100.2. Sin embargo, el tráfico de multidifusión puede tomar una ruta diferente a una nube MPLS privada; la misma ruta estática está instalada en la tabla de rutas de multidifusión con un salto siguiente diferente (198.51.100.4), por lo que la ruta es diferente.



El uso de tablas de rutas de unidifusión y multidifusión separadas le brinda mayor flexibilidad y control cuando configura estas funciones BGP:

- Instale una ruta estática IPv4 en la tabla de rutas de unidifusión o multidifusión, o ambas, según se describió en el ejemplo anterior. (Puede instalar una ruta estática IPv6 en la tabla de ruta de unidifusión únicamente).
- Cree una regla de importación para que cualquier prefijo que coincida con los criterios se importen en la tabla de rutas de unidifusión o multidifusión, o ambas.
- Cree una regla de exportación para que cualquier prefijo que coincida con los criterios se exporten (envíen al peer) desde la tabla de rutas de unidifusión o multidifusión, o ambas.
- Configure un anuncio condicional con un filtro no existente, para que el cortafuegos busque la tabla de ruta de unidifusión o multidifusión (o ambas) para garantizar que la ruta no exista en la tabla y el cortafuegos anuncie una ruta diferente.
- Configure un anuncio condicional con un filtro de anuncio, de manera que el cortafuegos anuncie rutas que coincidan con los criterios de la tabla de rutas de unidifusión o multidifusión, o ambas.
- Redistribuya una ruta que aparezca en la tabla de rutas de unidifusión o multidifusión, o ambas.
- Configure la agregación de rutas con un filtro de anuncio, de manera que las rutas agregadas que deben anunciarse provengan de la tabla de rutas de unidifusión o multidifusión, o ambas.
- A la inversa, configure la agregación de rutas con un filtro de supresión, de manera que las rutas agregadas que deben suprimirse (no anunciarse) provengan de la tabla de rutas de unidifusión o multidifusión, o ambas.

Cuando configura un peer con MP_BGP utilizando una familia de direcciones de IPv6, puede usar direcciones IPv6 en los campos de prefijo de dirección y próximo salto de una regla de importación, regla de exportación, anuncio condicional (filtro de anuncio y filtro no existente), y regla de agregación (filtro de anuncio, filtro de supresión y atributo de ruta de agregación).

Configuración de BGP

Realice la siguiente tarea para configurar BGP.

STEP 1 | Configure los ajustes generales del enrutador virtual.

STEP 2 | Habilite BGP para el enrutador virtual, asigne una ID de enrutador y asigne el enrutador virtual a un AS.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP**.
3. **Habilite** BGP para este enrutador virtual.
4. Asigne un **Router ID (ID de enrutador)** a BGP para el enrutador virtual, que generalmente es una dirección IPv4, para garantizar que el ID de enrutador sea único.
5. Asigne el **AS Number**, el número AS al que pertenece el enrutador virtual, en función del ID del enrutador (el intervalo es de 1 a 4 294 967 295).
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Configure los ajustes de configuración general de BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **General**.
3. Seleccione **Reject Default Route (Rechazar ruta predeterminada)** para ignorar todas las rutas por defecto anunciadas por peers BGP.
4. Seleccione **Install Route (Instalar ruta)** para instalar rutas BGP en la tabla de enrutamiento global.
5. Seleccione **Aggregate MED (Agrupar MED)** para activar la agregación de rutas incluso si las rutas tienen valores diferentes valores de discriminador de salida múltiple (Multi-Exit Discriminator, MED).
6. Especifique la **Default Local Preference (Preferencia local predeterminada)** que se puede utilizar para determinar preferencias entre las diferentes rutas.
7. Seleccione el **AS Format (Formato AS)** para fines de interoperabilidad:
   - **2 bytes** (predeterminado)
   - **4 bytes**

   Las estadísticas de tiempo de ejecución muestran números AS de 4 bytes de BGP con una notación simple de acuerdo con RFC 5396**.**
8. Habilite o deshabilite cada uno de los siguientes ajustes de **Path Selection (Selección de rutas)**:
   - **Always Compare MED (Comparar siempre MED)**: habilite esta comparación para elegir rutas de vecinos en diferentes sistemas autónomos.
   - **Comparación determinista de MED**: Habilite esta comparación para elegir entre rutas anunciadas por peers IBGP (peers BGP en el mismo sistema autónomo).
9. Para los **Auth Profiles (Perfiles de autenticación)**, seleccione **Add (Añadir)** para añadir un perfil de autenticación:
   - **Profile Name**: introduzca un nombre para identificar el perfil.
   - **Secret/Confirm Secret (Secreto/Confirmar secreto)**: Introduzca y confirme la contraseña para comunicaciones de peer BGP. El secreto se utiliza como clave en una autenticación MD5.
10. Haga clic en **OK** dos veces.

STEP 4 | (Opcional) Configure los ajustes de BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Advanced (Avanzado)**.
3. Seleccione **ECMP Multiple AS Support (Compatibilidad AS múltiple de ECMP)** si configuró ECMP y desea ejecutar ECMP en varios sistemas BGP autónomos.
4. Seleccione **Enforce First AS for EBGP (Aplicar primero AS para EBGP)** (habilitado de forma predeterminada) para que el cortafuegos descarte un paquete de actualización

entrante de un peer de eBGP que no enumera el propio número AS del peer de eBGP como el primer número de AS en el atributo AS_PATH.

5. Seleccione **Graceful Restart (Reinicio correcto)** y configure los siguientes temporizadores:
   - **Stale Route Time (sec) (Tiempo de ruta obsoleto (s))**: especifica la cantidad de tiempo en segundos que una ruta puede permanecer en el estado obsoleto (el intervalo es de 1 a 3600; el valor predeterminado es 120).
   - **Local Restart Time (sec) (Hora de reinicio local (s))**: especifica la cantidad de tiempo en segundos que el dispositivo local tarda en reiniciar. Este valor se les comunica a los peers (el intervalo es de 1 a 3600; el valor predeterminado es 120).
   - **Max Peer Restart Time (sec) (Máx. de hora de reinicio del peer (s))**: especifica el tiempo máximo en segundos que el dispositivo local acepta como periodo de gracia para reiniciar los dispositivos peer (el intervalo es 1 de 3600; el valor predeterminado es 120).
6. Para **Reflector Cluster ID (ID de clúster reflector)**, especifique un identificador IPv4 para representar el clúster reflector.
7. Para **Confederation Member AS (AS de miembro de confederación)**, especifique el identificador de número de sistema autónomo (también se denomina número de sistema subautónomo), visible únicamente en la confederación BGP. Para obtener más información, consulte Confederaciones BGP.
8. Haga clic en **Add (Añadir)**para introducir la siguiente información para cada perfil de amortiguación que quiera configurar, seleccione **Enable (Habilitar)** y haga clic en **OK (Aceptar)**:
   - **Profile Name**: introduzca un nombre para identificar el perfil.
   - **Cutoff (Corte)**: especifique un umbral retirada de ruta por encima del que se suprime un anuncio de ruta (el intervalo es de 0,0 a 1000; el valor predeterminado es 1,25).
   - **Reuse (Reutilizar)**: especifique un umbral de retirada de ruta por debajo del cual una ruta suprimida se vuelve a utilizar (el intervalo es de 0,0 a 1000; el valor predeterminado es 5).
   - **Max Hold Time (sec) (Máx. de tiempo de espera (s))**: especifique el tiempo máximo en segundos durante el que una ruta se puede suprimir, independientemente de su inestabilidad (el intervalo es de 0 a 3600; el valor predeterminado es 900).
   - **Decay Half Life Reachable (sec) (Media vida de disminución alcanzable (s))**: especifique el tiempo en segundos después del cual la métrica de estabilidad de una ruta se divide entre dos si la ruta se considera alcanzable (el intervalo es de 0 a 3600; el valor predeterminado es 300).
   - **Decay Half Life Reachable (sec) (Media vida de disminución no alcanzable (s))**: especifique el tiempo después del cual la métrica de estabilidad de una ruta se divide entre dos si la ruta se considera inalcanzable (el intervalo es de 0 a 3600; el valor predeterminado es 300).
9. Haga clic en **OK** dos veces.

STEP 5 | Configure el grupo del peer BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y **Add (Añadir)** para añadir un **nombre** para el grupo de peers y **habilítelo**.
3. Seleccione **Aggregated Confed AS Path** para incluir una ruta a la AS de confederación agregada configurada.
4. Seleccione **Soft Reset with Stored Info (Restablecimiento parcial con información almacenada)** para ejecutar un restablecimiento parcial del cortafuegos después de actualizar los ajustes de peer.
5. Seleccione el **Type (Tipo)** de grupo de peers.
   - IBGP: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP confederado: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP confederado: Exportar siguiente salto: Seleccione **Original** o **Use self**.
   - EBGP: Importar siguiente salto: Seleccione **Original** o **Use self**; y **Export Next Hop (Exportar siguiente salto)**: Especifique **Resolve (Resolver)** o **Use self (Utilizar automático)**. Seleccione **Remove Private AS (Eliminar AS privado)** si desea forzar que BGP elimine números AS privados del atributo AS_PATH en las actualizaciones que el cortafuegos envía a un peer en otro AS.
6. Haga clic en **OK (Aceptar)**.

STEP 6 | Configure un peer BGP que pertenezca al grupo de peers y especifique su direccionamiento.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Para el peer, seleccione **Add (Añadir)** para añadir un peer por **Name (Nombre)**.
4. **Habilite** el peer.
5. Introduzca el **Peer AS** al cual pertenece el peer.
6. Seleccione **Addressing (Direccionamiento)**.
7. Para **Local Address (Dirección local)**, seleccione la **Interface (Interfaz)** para la cual está configurando BGP. Si la interfaz tiene más de una dirección **IP**, introduzca la dirección IP para que esa interfaz sea el peer BGP.
8. En **Peer Address (Dirección de peer)**, tiene dos opciones: seleccione **IP** e introduzca la dirección IP, seleccione un objeto de dirección o cree un objeto de dirección, o bien

seleccione **FQDN** e introduzca el nombre de dominio completo (fully qualified domain name, FQDN) o un objeto de dirección del tipo FQDN.

El cortafuegos solo emplea una dirección IP (de cada tipo de familia, esto es, IPv4 o IPv6) de la resolución de DNS del FQDN. Si se devuelven varias direcciones, el cortafuegos utiliza la dirección IP preferida que coincida con el tipo de familia de IP (IPv4 o IPv6) configurado para el peer de BGP. La dirección IP preferida es la primera dirección que devuelve el servidor DNS en su respuesta inicial. El cortafuegos la mantiene como preferida mientras siga apareciendo en las respuestas posteriores, aunque el orden sea distinto.

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

STEP 7 | Configure los ajustes de conexión para el peer BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Seleccione el **Peer** que configuró.
4. Seleccione las **Connection Options (Opciones de conexión)**.
5. Seleccione un **Auth Profile (Perfil de autenticación)** para el peer.
6. **Keep Alive Interval (sec) (Mantener el intervalo activo (s))**: el intervalo (en segundos) después del cual las rutas de un peer se suprimen según el parámetro de tiempo de espera (el intervalo es de 0 a 1200; el valor predeterminado es 30).
7. Configure **Multi Hop (Salto múltiple)**, el valor del tiempo de vida (Time-To-Live, TTL) en el encabezado IP (el intervalo es de 0 a 255; el valor predeterminado es 0). El valor predeterminado de 0 significa 1 para iBGP. El valor predeterminado de 0 significa 255 para iBGP.
8. Configure **Open Delay Time (sec) (Tiempo de retardo de apertura (s))**, el retardo, en segundos, entre un protocolo TCP y el envío del cortafuegos del primer mensaje de apertura de BGP para establecer una conexión BGP (el intervalo es de 0 a 240; el valor predeterminado es 0).
9. Configure el **Hold Time (sec) (Tiempo de espera (s))**, el período, en segundos, que puede transcurrir entre mensajes Keepalive o de actualización sucesivos de un peer antes de cerrar la conexión del peer (el intervalo es de 3 a 3600; el valor predeterminado es 90).
10. Configure **Idle Hold Time (sec) (Tiempo de espera inactivo [s])**, el período de espera (en segundos) antes de reintentar conectarse al peer (el intervalo es de 1 a 3600; el valor predeterminado es 15).
11. En **Min Route Advertisement Interval (sec) (Intervalo mínimo entre anuncios de rutas (s))**, establezca el número mínimo de segundos que debe transcurrir entre dos mensajes de actualización (Update) sucesivos que envíe el emisor de BGP (esto es, el cortafuegos) a

un peer de BGP para anunciar que se han establecido o retirado rutas; el intervalo es de 1 a 600 y el valor predeterminado es 30.

12. Para **Incoming Connections (Conexiones entrantes)**, introduzca un **Remote Port (Puerto remoto)** y seleccione **Allow (Permitir)** para permitir el tráfico entrante a este puerto.
13. Para **Outgoing Connections (Conexiones salientes)**, introduzca un **Local Port (Puerto local)** y seleccione **Allow (Permitir)** para permitir el tráfico saliente de este puerto.
14. Haga clic en **OK (Aceptar)**.

STEP 8 | Configure el peer BGP con los ajustes para el cliente reflector de ruta, tipo de emparejamiento, prefijos máximos y detección de reenvío bidireccional (BFD).

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **BGP** > **Peer Group (Grupo de peers)** y seleccione el grupo de peers que creó.
3. Seleccione el **Peer** que configuró.
4. Seleccione **Advanced (Avanzado)**.
5. En **Reflector Client (Cliente reflector)**, seleccione una de las opciones siguientes:
   - **non-client (no cliente)** (predeterminado): el peer no es un cliente reflector de ruta.
   - **client (cliente)**: el peer es un cliente reflector de ruta.
   - **meshed-client (cliente en malla)**
6. Para **Peering Type (Tipo de emparejamiento)**, seleccione una de las siguientes opciones:
   - **Bilateral**: los dos peers BGP establecen una conexión de peer.
   - **Unspecified (No especificado)**: (predeterminado).
7. Para los **Max Prefixes (Prefijos máximos)**, introduzca la cantidad máxima de prefijos IP admitidos (el intervalo es de 1 a 100 000) o seleccione **unlimited (ilimitado)**.
8. Para habilitar **BFD** para el peer (y por lo tanto, cancelar la configuración BFD por BGP, siempre que BFD no esté deshabilitado para BGP a nivel del enrutador virtual), seleccione una de las siguientes opciones:
   - **default (predeterminado)**: usa únicamente los ajustes BFD por defecto.
   - **Inherit-vr-global-setting (Heredar ajuste global para el enrutador virtual)** (valor predeterminado): el peer hereda el perfil BFD que usted seleccionó globalmente para BGP para el enrutador virtual.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

   *Seleccione **Disable BFD (Deshabilitar BFD)** para deshabilitar el peer de BGP.*
9. Haga clic en **OK (Aceptar)**.

STEP 9 | Configure reglas de importación y exportación.

Las reglas de importación y exportación se utilizan para importar y exportar rutas desde otros enrutadores y hacia otros enrutadores (por ejemplo, mediante la importación la ruta predeterminada desde su proveedor de servicios de Internet).

1. Seleccione **Import (Importar)** y **añada** un nombre en el campo **Rules (Reglas)**, y **habilite** la regla de importación.
2. Haga clic en **Add (Añadir)** y seleccione el **Peer Group (Grupo del peer)** desde el que se importarán las rutas.
3. Seleccione **Match (Coincidencia)** y defina las opciones utilizadas para filtrar la información de enrutamiento. También puede definir el valor de discriminador de salida múltiple (MED) y un valor de siguiente salto como enrutadores o subredes para el filtrado de rutas. La opción MED es una medida externa que permite que los vecinos sepan cuál es la ruta preferida de un AS. Se prefiere un valor más bajo antes que un valor más alto.
4. Seleccione **Action (Acción)** y defina la acción que debería producirse (permitir o denegar) basándose en las opciones de filtrado definidas en la pestaña **Coincidencia**. Si selecciona **Deny (Denegar)**, no tendrá que definir ninguna opción adicional. Si selecciona **Allow (Permitir)**, tendrá que definir otros atributos.
5. Seleccione **Export (Exportar)** y defina atributos de exportación, que son similares a los ajustes de **Importar**, pero que se utilizan para controlar la información de rutas que se exporta desde el cortafuegos a los vecinos.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Configure los anuncios condicionales, que le permiten controlar la ruta que se anunciará en caso de que no exista ninguna ruta diferente en la tabla de enrutamiento BGP local (LocRIB), indicando un fallo de emparejamiento o alcance.

Esta función es útil si desea intentar forzar rutas de un AS a otro, por ejemplo, si tiene enlaces a Internet a través de varios ISP y desea enrutar el tráfico a un único proveedor, en lugar de a los otros, salvo que se produzca una pérdida de conectividad con el proveedor preferido.

1. Seleccione **Conditional Adv (Anuncio condicional)** y **añada** un nombre de **política**.
2. **Habilite** el anuncio condicional.
3. En la sección **Used By (Utilizado por)**, **añada** los grupos de peers que utilizarán la política de anuncios condicionales.
4. Seleccione **Non Exist Filter (Filtro no existente)** y defina los prefijos de red de la ruta preferida. De esta forma, se especifica la ruta que desea anunciar, si está disponible en la tabla de ruta de BGP local. Si un prefijo se va a anunciar y coincide con un filtro no existente, el anuncio se suprimirá.
5. Seleccione **Advertise Filters (Anunciar filtros)** y defina los prefijos de la ruta de la tabla de enrutamiento Local-RIB que se debería anunciar en caso de que la ruta del filtro no existente no esté disponible en la tabla de enrutamiento local. Si un prefijo se va a anunciar y no coincide con un filtro no existente, el anuncio se producirá.
6. Haga clic en **OK (Aceptar)**.

STEP 11 | Configure opciones agregadas para resumir rutas en la configuración de BGP.

La agregación de rutas de BGP se utiliza para controlar el modo en que BGP agrega direcciones. Cada entrada de la tabla da como resultado la creación de una dirección de agregación. El

resultado será una entrada agregada en la tabla de enrutamiento cuando se obtiene al menos una ruta específica que coincide con la dirección especificada.

1. Seleccione **Aggregate (Agregación)** y **añada** un nombre para la dirección de agregación.
2. Especifique el **prefijo** de la red, que será el prefijo principal de los prefijos agregados.
3. Seleccione **Suppress Filters (Suprimir filtros)** y defina los atributos que harán que las rutas coincidentes se supriman.
4. Seleccione **Advertise Filters (Anunciar filtros)** y defina los atributos que harán que las rutas coincidentes se anuncien siempre a los peers.
5. Haga clic en **OK (Aceptar)**.

STEP 12 | Configure las reglas de redistribución.

Esta regla se utiliza para redistribuir las rutas de host y las rutas desconocidas que no se encuentran en la RIB local de los enrutadores de peers.

1. Seleccione **Redist Rules (Reglas de redistribución)** y **añada** una nueva regla de redistribución.
2. Especifique el **nombre** de una subred IP o seleccione un perfil de redistribución. Si es necesario, también puede configurar un perfil de redistribución nuevo.
3. Seleccione **Enable (Habilitar)** para habilitar la regla.
4. Especifique la **métrica** de ruta que se utilizará para la regla.
5. En la lista **Set Origin (Configurar origen)**, seleccione **incomplete (incompleto)**, **igp** o **egp**.
6. (Opcional) Establezca MED, la preferencia local, el límite de ruta AS y los valores de comunidad.
7. Haga clic en **OK (Aceptar)**.

STEP 13 | **Commit (Confirmar)** los cambios.

Configuración de un peer BGP con MP-BGP para unidifusión IPv4 o IPv6

Después de configurar BGP, configure un peer BGP con MP-BGP para unidifusión IPv4 o IPv6 por cualquiera de los siguientes motivos:

- Para que su peer BGP transporte rutas de unidifusión IPv6, configure MP-BGP con el tipo de familia de dirección **IPv6** y la familia de direccion posterior **Unicast**, de manera que el peer pueda enviar actualizaciones BGP que incluyan rutas de unidifusión IPv6. Los peer BGP (dirección local y dirección de peer) pueden ser las direcciones IPv4 o las direcciones IPv6.
- Para realizar el emparejamiento de BGP en direcciones IPv6 (**Local Address [Dirección local]** y **Peer Address [Dirección de peer]** utilizan direcciones IPv6).

La siguiente tarea muestra cómo habilitar un peer BGP con MP-BGP para poder transportar rutas de unidifusión IPv6, y así poder emparejarlo usando direcciones IPv6.

La tarea también muestra cómo ver las tablas de ruta unidifusión o multidifusión, y cómo ver la tabla de reenvío, la RIB local de BGP y salida RIB de BGP (rutas enviada a vecinos) para ver las rutas de la tabla de rutas de unidifusión o multidifusión, o una familia de direcciones específica (IPv4 o IPv6).

STEP 1 | Habilite la extensiones MP-BGP para un peer.

Configure lo siguiente para que un peer de BGP pueda transportar rutas unidifusión IPv4 o IPv6 en paquetes de actualización y el cortafuegos pueda usar direcciones IPv4 o IPv6 para comunicarse con su peer.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **BGP**.
3. Seleccione **Peer Group (Grupo de peers)** y seleccione un grupo de peers.
4. Seleccione un peer BGP (enrutador).
5. Seleccione **Addressing (Direccionamiento)**.
6. Seleccione **Enable MP-BGP Extensions (Habilitar las extensiones MP-BGP)** para el peer.
7. En **Address Family Type (Tipo de familia de direcciones)**, haga clic en **IPv4** o **IPv6**. Por ejemplo, seleccione IPv6.
8. En **Subsequent Address Family (Familia de direcciones posteriores)**, se selecciona **Unicast (Unidifusión)**. Si elige **IPv4** para la familia de direcciones, puede seleccionar también **Multicast (Multidifusión)**.
9. En **Local Address (Dirección local)**, seleccione una **Interface (Interfaz)** y, opcionalmente, seleccione una dirección **IP**; por ejemplo, 2001:DB8:55::/32
10. En **Peer Address (Dirección de peer)**, introduzca la dirección **IP**, utilizando la misma familia de direcciones (IPv4 o IPv6) como la dirección local; por ejemplo, 2001:DB8:58::/32.
11. Seleccione **Advanced (Avanzado)**.
12. (Opcional) **Enable Sender Side Loop Detection (Habilitar detección de bucle en el lado del remitente)**. Cuando habilita la detección de bucle en el lado del remitente, el cortafuegos comprobará el atributo AS_PATH de una ruta en su FIB antes de enviar la ruta

en una actualización, para asegurarse de que el número de AS del peer no esté en la lista AS_PATH. Si está, el cortafuegos lo elimina para evitar un bucle.

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

STEP 2 | (Opcional) Cree una ruta estática e instálela en la tabla de rutas de unidifusión, ya que desea que la ruta se utilice solo para fines de unidifusión.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **Static Routes (Rutas estáticas)**, seleccione **IPv4** o **IPv6**, y luego **Add (Añadir)** para añadir una ruta.
3. Introduzca un nombre en **Name (Nombre)** para la ruta estática.
4. Introduzca el prefijo y la máscara de red de **Destination (Destino)** IPv4 o IPv6, según si elige IPv4 o IPv6.
5. Seleccione la salida **Interface (Interfaz)**.
6. Seleccione **Next Hop (Próximo salto)** como **IPv6 Address (Dirección IPv6)** (o **IP Address [Dirección IP]** si elige IPv4) e introduzca la dirección del siguiente salto al cual desea dirigir el tráfico de unidifusión para esta ruta estática.
7. Ingrese una **Admin Distance (Distancia de administrador)**.
8. Ingrese una **Metric (Métrica)**.
9. Para la **Route Table (Tabla de ruta)**, seleccione **Unicast (Unidifusión)**.
10. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

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

STEP 4 | Visualice la tabla de ruta de unidifusión o multidifusión.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de enrutamiento)**.
4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

*La selección de **Multicast (Multidifusión)** con **IPv6 Only (IPv6 únicamente)** no es compatible.*

STEP 5 | Visualice la tabla de reenvío.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Forwarding Table (Tabla de desvío)**.
4. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

STEP 6 | Visualice las tablas RIB de BGP.

1. Visualice la RIB local de BGP, que muestra las rutas BGP que el cortafuegos utiliza para enrutar paquetes BGP.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
   2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
   3. Seleccione **BGP** > **Local RIB**.
   4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
   5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

   *La selección de **Multicast (Multidifusión)** con **IPv6 Only (IPv6 únicamente)** no es compatible.*
2. Visualice la tabla de salida RIB de BGP, que muestra las rutas que el cortafuegos envía a los vecinos BGP.
   1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
   2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
   3. Seleccione **BGP** > **RIB Out (Salida RIB)**.
   4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
   5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

   *La selección de **Multicast (Multidifusión)** con **IPv6 Only (IPv6 únicamente)** no es compatible.*

Configuración de un peer de BGP con MP-BGP para rutas de multidifusión IPv4

Tras la Configuración del BGP, configure un peer de BGP con MP-BGP para la ruta de multidifusión IPv4 si desea que su peer de BGP pueda aprender y pasar rutas de multidifusión IPv4 en las actualizaciones de BGP. Podrá separar el tráfico de rutas de unidifusión del de rutas de multidifusión, o emplear las funciones enumeradas en el MP-BGP para utilizar solo rutas de la tabla de rutas de unidifusión o de multidifusión, o rutas de ambas tablas.

Si desea admitir solo tráfico de rutas de multidifusión, debe utilizar un filtro para eliminar el tráfico de rutas de unidifusión.

El cortafuegos no es compatible con el ECMP de tráfico de rutas de multidifusión.

STEP 1 | Habilite las extensiones del MP-BGP para que un peer de BGP puede intercambiar rutas de multidifusión IPv4.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **BGP**.
3. Seleccione **Peer Group (Grupo de peers)**, seleccione un grupo de peers y un peer de BGP.
4. Seleccione **Addressing (Direccionamiento)**.
5. Seleccione **Enable MP-BGP Extensions (Habilitación de las extensiones del MP-BGP)**.
6. En el campo **Address Family Type (Tipo de familia de dirección)**, seleccione **IPv4**.
7. En el campo **Subsequent Address Family (Familia de la dirección siguiente)**, seleccione **Unicast (Unidifusión)** y **Multicast (Multidifusión)**.
8. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cree una ruta estática IPv4 e instálela en la tabla de rutas de multidifusión únicamente.

Estos pasos se realizan para dirigir el tráfico de rutas de multidifusión de un peer de BGP a un siguiente salto específico, como se muestra en la topología en el MP-BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual que está configurando.
2. Seleccione **Static Routes (Rutas estáticas)** > **IPv4** y **Add (Añadir)** para añadir un nombre en el campo **Name (Nombre)** para la ruta.
3. Introduzca el prefijo de **Destination (Destino)** IPv4 y la máscara de red.
4. Seleccione la salida **Interface (Interfaz)**.
5. Seleccione el **Next Hop (Siguiente salto)** como la **IP Address (Dirección IP)** e introduzca la dirección IP del siguiente salto al que desea dirigir el tráfico de rutas de multidifusión para esta ruta estática.
6. Ingrese una **Admin Distance (Distancia de administrador)**.
7. Ingrese una **Metric (Métrica)**.
8. En **Route Table (Tabla de rutas)**, seleccione **Multicast (Multidifusión)**.
9. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

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

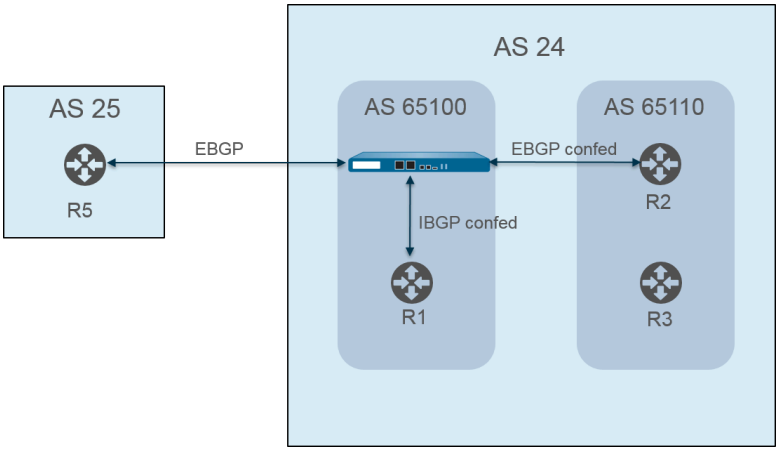
STEP 4 | Vea la tabla de rutas.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.
2. En la fila del enrutador virtual, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
3. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de enrutamiento)**.
4. Para la **Route Table (Tabla de rutas)**, seleccione **Unicast (Unidifusión)** o **Multicast (Multidifusión)** para mostrar solo esas rutas.
5. En **Display Address Family (Mostrar familia de direcciones)**, seleccione **IPv4 Only (IPv4 únicamente)**, **IPv6 Only (IPv6 únicamente)** o **IPv4 and IPv6 (IPv4 e IPv6)** para mostrar solo las rutas para esa familia de direcciones.

STEP 5 | Para ver la tabla de reenvío, la tabla de la RIB local del BGP o la tabla de salida de la RIB del BGP, consulte la Configuración de un peer de BGP con MP-BGP para rutas de unidifusión IPv4 o IPv6.

Confederaciones BGP

Las confederaciones BGP proporcionan una manera de dividir un sistema autónomo (autonomous system, AS) en dos o más sistemas subautónomos (sub-AS) para reducir la carga que provoca el requisito de malla completa de IBGP. Los cortafuegos (u otros dispositivos de enrutamiento) en un sistema subautónomo deben poseer una malla completa de iBGP con otros cortafuegos en el mismo sistema subautónomo. Es necesario el emparejamiento de BGP entre sistemas subautónomos para garantizar una conectividad completa en el sistema subautónomo principal. Los cortafuegos que se emparejan entre sí en un sistema subautónomo forman un emparejamiento de confederación IBGP. El cortafuegos en un sistema subautónomo que se empareja con un cortafuegos en un sistema subautónomo diferente forma un emparejamiento de confederación EBGP. Dos cortafuegos de diferentes sistemas autónomos que se conectan son peers de EBGP.

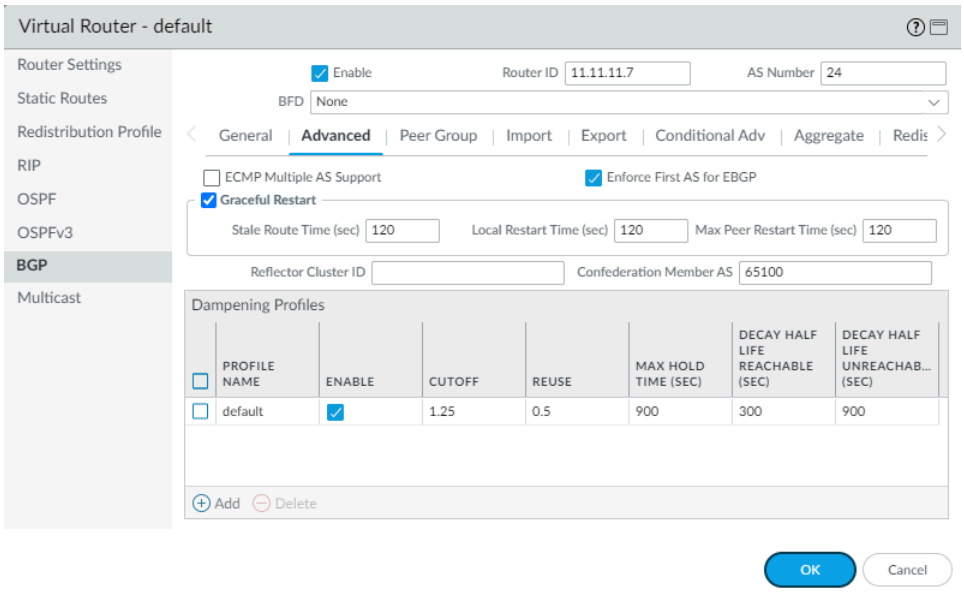


Los sistemas autónomos se identifican con un número de AS (asignado globalmente) público como AS 24 y AS 25 en la figura previa. En un entorno PAN-OS, asigne a cada sistema subautónomo un número de AS de miembro de la confederación único, que es un número privado que solo se ve dentro del sistema subautónomo. En esta figura, las confederaciones son AS 65100 y AS 65110. (RFC6996, reserva de sistema subautónomo [AS] para uso privado; indica que la IANA reserva los números del AS 64512 a 65534 para uso privado).

Las confederaciones de sistemas subautónomos parecen sistemas autónomos completos entre sí dentro del sistema subautónomo. Sin embargo, cuando el cortafuegos envía una ruta de AS a un peer de EBGP, únicamente el número público de AS aparece en la ruta de AS; no se incluyen números privados de sistema subautónomo (AS miembro de la confederación).

Se produce el emparejamiento de BGP entre el cortafuegos y R2; el cortafuegos en la figura posee los siguientes ajustes relevantes:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP confederado
- AS del peer: 65110



El enrutador 2 (R2) en AS 65110 se configura de la siguiente manera:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP confederado
- AS del peer: 65110

El emparejamiento de BGP también se produce entre el cortafuegos y R1. El cortafuegos posee la siguiente configuración adicional:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: IBGP confederado
- AS del peer: 65110

R1 se configura de la siguiente manera:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: IBGP confederado
- AS del peer: 65110

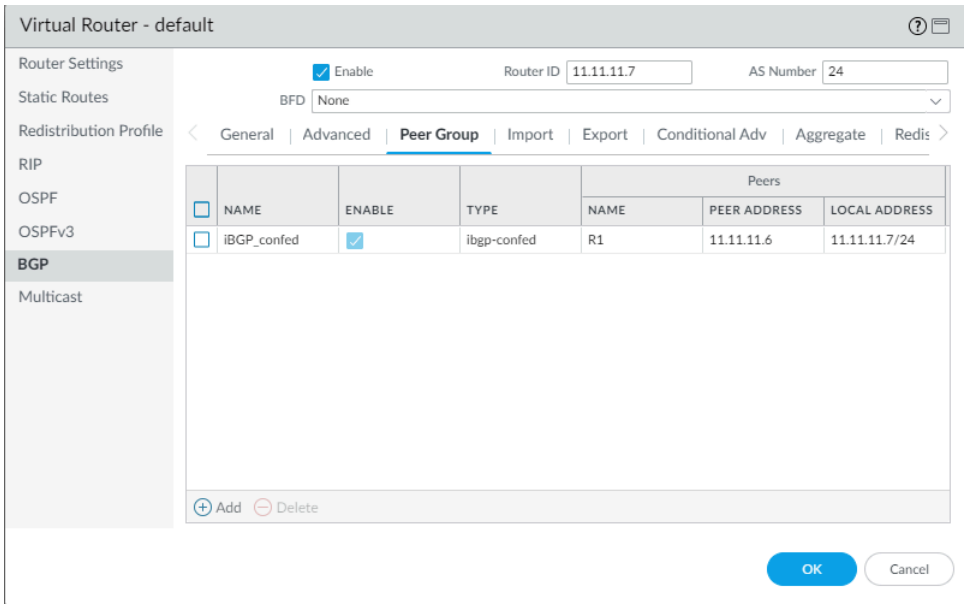
El emparejamiento de BGP se produce entre el cortafuegos y R5. El cortafuegos posee la siguiente configuración adicional:

- Número AS: 24
- AS de miembro de confederación: 65100
- Tipo del peer: EBGP
- AS del peer: 25

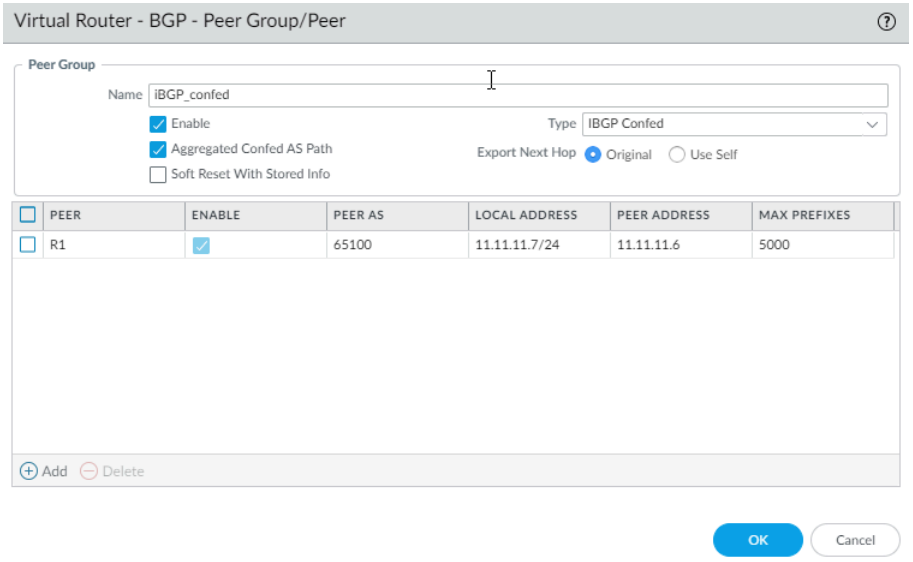
R5 se configura de la siguiente manera:

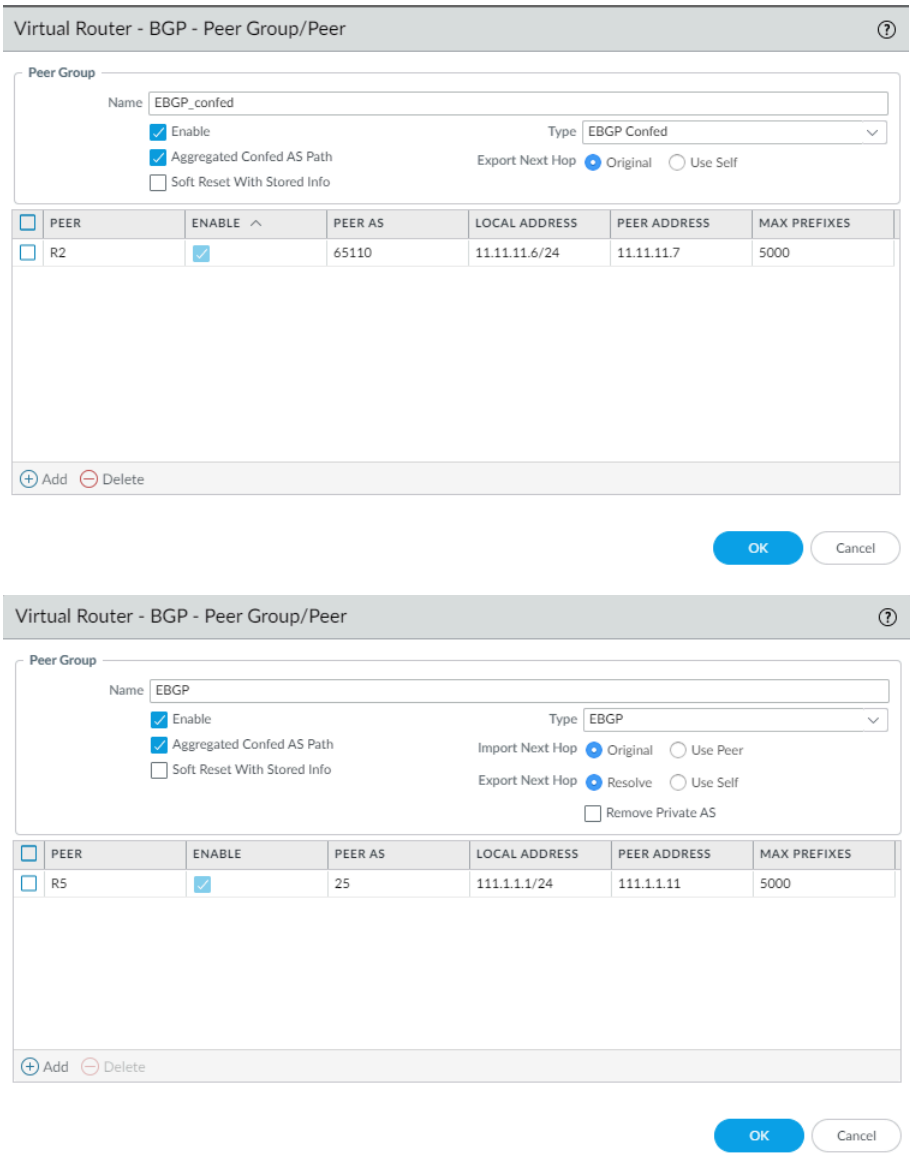
- AS—25
- Tipo del peer: EBGP
- AS del peer: 24

Después de que el cortafuegos se configure para emparejarse con R1, R2 y R5, sus peers se ven en la pestaña **Peer Group (Grupo de peers)**:

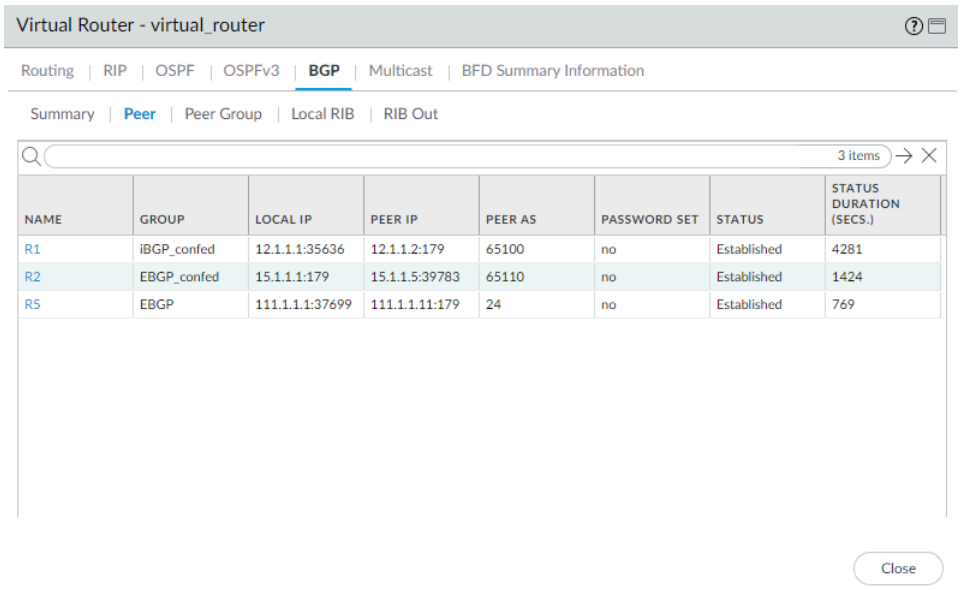


El cortafuegos muestra los peers R1, R2, and R5:

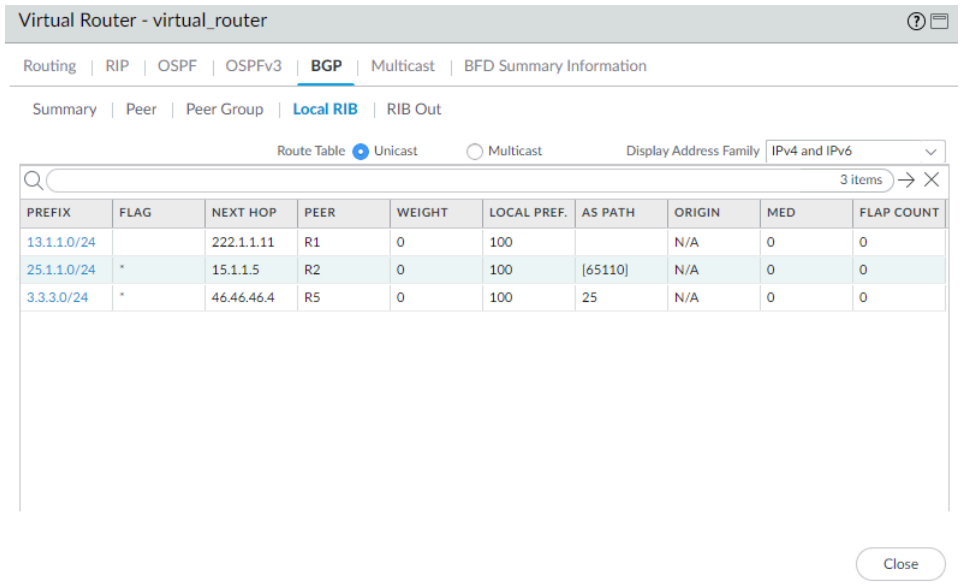




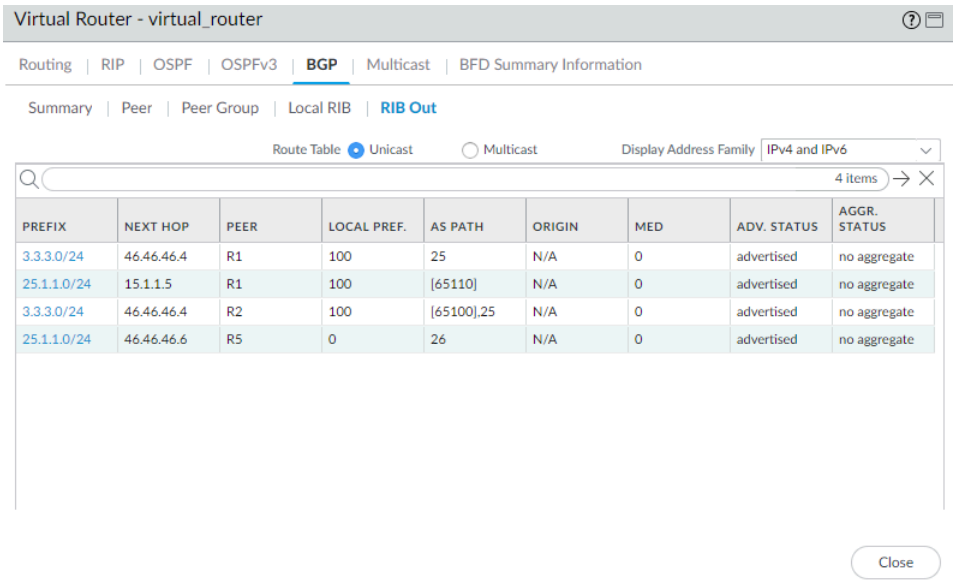
Para verificar que se establezcan las rutas desde el cortafuegos a los peers, en la pantalla del enrutador virtual, seleccione **More Runtime Stats (Más estadísticas de tiempo de ejecución)** y seleccione la pestaña **Peer**.



Seleccione la pestaña **Local RIB (RIB local)** para ver la información sobre las rutas almacenadas en la base de información de enrutamiento (Routing Information Base, RIB).



Luego, seleccione la pestaña **RIB Out (Salida RIB)**.



IP de multidifusión

La multidifusión de IP es un conjunto de protocolos que los dispositivos de red usan para enviar datagramas de IP de multidifusión a un grupo de receptores interesados mediante una trasmisión en lugar de una realizar una unidifusión del tráfico a varios receptores, lo que ahorra ancho de banda. La multidifusión de IP es adecuada para la comunicación desde una fuente (o varias) a muchos receptores, como la transmisión de audio o vídeo, IPTV, videoconferencias y distribución de otras comunicaciones, como noticias y datos financieros.

Una dirección de multidifusión identifica un grupo de receptores que desea recibir tráfico que se dirige a esa dirección. No debe utilizar las direcciones de multidifusión reservadas para casos especiales, como el rango de 224.0.0.0 a 224.0.0.255 o de 239.0.0.0 a 239.255.255.255. El tráfico de multidifusión usa UDP, que no vuelve a enviar los paquetes que faltan.

Los cortafuegos de Palo Alto Networks® admiten la multidifusión de IP y la Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) en una interfaz de capa 3 que configura para un enrutador virtual en el cortafuegos.

Para el enrutamiento de multidifusión, el tipo de interfaz de capa 3 puede ser Ethernet, Ethernet agregada (Aggregate Ethernet, AE), VLAN, bucle invertido o túnel. Los grupos de interfaces le permiten configurar más de una interfaz de cortafuegos a la vez con el mismo Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) y parámetros PIM, y con los mismos permisos de grupo (grupos de multidifusión que tienen permitido aceptar tráfico de cualquier fuente o de una única fuente específica). Una interfaz puede pertenecer a solo un grupo de interfaces.

El cortafuegos admite la multidifusión de IPv4, no admite la de IPv6. El cortafuegos no admite el Modo denso de PIM (PIM Dense Mode, PIM-DM), proxy IGMP, uniones estáticas de IGMP, RP de difusión limitada, GRE o configuraciones de multidifusión en un tipo de interfaz de cable virtual o capa 2. Sin embargo, una interfaz de cable virtual puede pasar paquetes de multidifusión. Además, una interfaz de capa 2 puede cambiar paquetes de multidifusión IPv4 de capa 3 entre diferentes VLAN y el cortafuegos volverá a etiquetar el ID de VLAN con el ID de VLAN de la interfaz de salida.

Debe habilitar la multidifusión para un enrutador virtual y habilitar PIM para una interfaz de entrada y salida para que las interfaces reciban o reenvíen paquetes de multidifusión. Además de PIM, también debe habilitar IGMP en las interfaces de salida que se orientan a los receptores. Debe configurar una regla de política de seguridad para permitir el tráfico de multidifusión de IP en una zona de destino de capa 3 predefinida con el nombre **multicast (multidifusión)** o a cualquier zona de destino cuando se configura como **any (cualquiera)**.

> IGMP
> PIM
> Configuración de IP de multidifusión
> Visualización de información de IP de multidifusión

IGMP

El Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) es un protocolo IPv4 que un receptor de multidifusión usa para comunicarse con una interfaz de un cortafuegos de Palo Alto Networks® y que el cortafuegos usa para registrar la pertenencia de los grupos de multidifusión. Cuando un host desea recibir tráfico de multidifusión, su implementación de IGMP envía un mensaje de informe de pertenencia de IGMP y el enrutador receptor envía un mensaje de unión de PIM a la dirección del grupo de multidifusión del grupo al cual el host desea unirse. Un enrutador habilitado para IGMP en la misma red física (como un segmento de Ethernet) usa PIM para comunicarse con otros enrutadores habilitados para PIM y determinar una ruta desde la fuente a los receptores interesados.

Habilite IGMP solo en interfaces que se orientan al receptor de multidifusión. Los receptores pueden estar a solo un salto de capa 3 de distancia del enrutador virtual. Los mensajes de IGMP son mensajes de capa 2 que tienen un valor TTL de uno y, por lo tanto, no pueden salir de la red LAN.

Cuando configure la multidifusión de IP, especifique si una interfaz usa IGMP Versión 1, IGMP Versión 2 o IGMP Versión 3. Puede aplicar la opción de alerta de enrutador de IP, RFC 2113, de modo que los paquetes entrantes de IGMP que use IGMPv2 o IGMPv3 tengan la opción de alerta de enrutador de IP.

De manera predeterminada, una interfaz acepta los informes de pertenencia de IGMP para todos los grupos de multidifusión. Puede configurar permisos del grupo de multidifusión para controlar los grupos en los que el enrutador virtual acepta informes de pertenencia de cualquier fuente (Multidifusión de cualquier fuente [Any-Source Multicast, ASM]), que en esencia es el Modo disperso de PIM (PIM Sparse Mode, PIM-SM). También puede especificar los grupos en los que el enrutador virtual acepta los informes de pertenencia de una fuente específica Multidifusión de fuente específica [Source-Specific Multicast, SSM] de PIM). Si especifica permisos para los grupos ASM o SSM, el enrutador virtual rechaza los informes de pertenencia de otros grupos. La interfaz debe usar IGMPv3 para pasar el tráfico de PIM-SSM.

Puede especificar la cantidad máxima de fuentes y el número máximo de grupos de multidifusión que IGMP puede procesar simultáneamente para una interfaz.

El enrutador virtual realiza la multidifusión de una consulta de IGMP en intervalos regulares a todos los receptores de un grupo de multidifusión. Un receptor responde a una consulta de IGMP con un informe de pertenencia de IGMP que confirma que el receptor todavía desea recibir tráfico de multidifusión de ese grupo. El enrutador virtual conserva una tabla de los grupos de multidifusión que tienen receptores; el enrutador virtual reenvía un paquete de multidifusión fuera de la interfaz al siguiente salto solo si todavía hay un receptor en ese árbol de distribución de multidifusión que esté unido al grupo. El enrutador virtual no registra exactamente qué receptores se unieron a un grupo. Solo un enrutador en una subred responde a las consultas de IGMP y es el solicitante de IGMP, el enrutador con la dirección IP más baja.

Puede configurar una interfaz con el intervalo de consulta de IGMP y la cantidad de tiempo permitido para que un receptor responda a una consulta (la opción Max Query Response Time [(Máx. de tiempo de respuesta de consulta]). Cuando un enrutador virtual recibe un mensaje de salida de IGMP de un receptor para abandonar un grupo, el enrutador virtual comprueba que la interfaz que recibió este mensaje no esté configurada con la opción Immediate Leave (Salida inmediata). Si no está la opción Immediate Leave (Salida inmediata), el enrutador virtual envía una consulta para determinar si todavía existen miembros del receptor en el grupo. La opción Last Member Query Interval (Último intervalo de consulta del miembro) especifica cuántos segundos se

proporcionan para que los receptores restantes de ese grupo respondan y confirmen que todavía desea el tráfico de multidifusión de ese grupo.

Una interfaz admite la variable de potencia de IGMP, que puede ajustar para que el cortafuegos ajuste las opciones Group Membership Interval (Intervalo de pertenencia del grupo), Other Querier Present Interval (Otro intervalo presente del solicitante), Startup Query Count (Recuento de consultas de inicio) y Last Member Query Count (Último recuento de consulta del miembro). Una variable de mayor potencia puede tener una subred que probablemente descarte paquetes.

Visualice la información de multidifusión de IP para ver las interfaces habilitadas para IGMP, la versión de IGMP, la dirección del solicitante, la configuración de potencia, los límites en la cantidad de fuentes y grupos de multidifusión, y si la interfaz está confirmada para la salida inmediata. También puede ver los grupos de multidifusión a los cuales pertenecen las interfaces y otra información de pertenencia de IGMP.

PIM

La multidifusión de IP usa el protocolo de enrutamiento de Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) entre enrutadores para determinar la ruta del árbol de distribución que los paquetes de multidifusión toman desde el origen hasta los receptores (miembros del grupo de multidifusión). Un cortafuegos de Palo Alto Networks® admite el Modo disperso de PIM (PIM-SM) (RFC 4601), la Multidifusión de cualquier origen (Any-Source Multicast, ASM) de PIM (a veces denominada como el Modo disperso de PIM) y la Multidifusión de origen específico (Source-Specific Multicast, SSM) de PIM. En PIM-SM, el origen no reenvía tráfico de multidifusión hasta que un receptor (usuario) que pertenece a un grupo de multidifusión solicita que el origen envíe el tráfico. Cuando un host desea recibir tráfico de multidifusión, su implementación de IGMP envía un mensaje de informe de pertenencia de IGMP y el enrutador receptor envía un mensaje de unión de PIM a la dirección del grupo de multidifusión del grupo al que desea unirse.

- En **ASM**, el receptor usa IGMP para solicitar tráfico de una dirección de grupo de multidifusión; cualquier origen podría haber originado ese tráfico. Por consecuencia, el receptor no conoce necesariamente a los emisores, y el receptor podría recibir tráfico de multidifusión en el que no tiene interés.
- En **SSM** (RFC 4607), el receptor usa IGMP para solicitar tráfico desde uno o más orígenes específicos hacia una dirección de grupo de multidifusión. El receptor conoce la dirección IP de los emisores y recibe solo el tráfico de multidifusión que desea. SSM requiere IGMPv3. Puede anular el espacio de direcciones SSM predeterminado, que es 232.0.0.0/8.

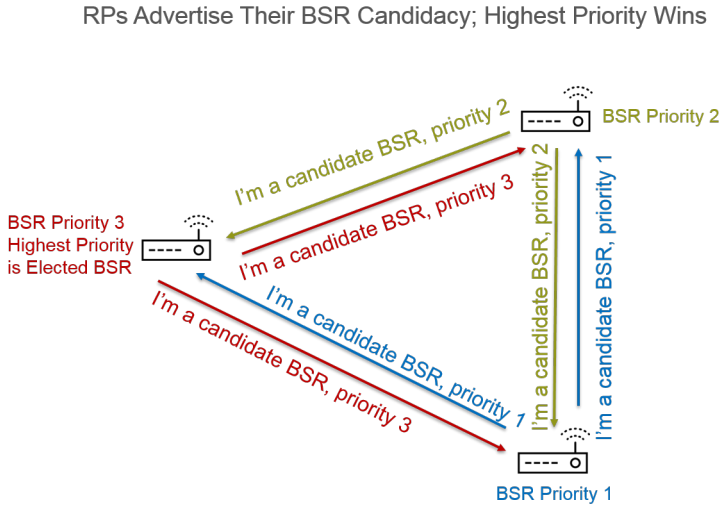
Cuando configura la multidifusión de IP en un cortafuegos de Palo Alto Networks, debe habilitar PIM para que una interfaz reenvíe el tráfico de multidifusión incluso en interfaces accesibles desde un receptor. Esto es diferente a IGMP, que habilita solo en interfaces accesibles desde un receptor.

ASM requiere un ***punto de encuentro*** (rendezvous point, RP), que es un enrutador localizado en la unión o raíz de un árbol de distribución compartida. El RP de un dominio de multidifusión sirve como un único punto al cual todos los miembros del grupo de multidifusión envían sus mensajes de unión. Este comportamiento reduce la probabilidad de un bucle de enrutamiento que, de lo contrario, ocurriría si los miembros del grupo enviaran sus mensajes de unión a varios enrutadores. (SSM no necesita un RP porque la multidifusión específica de origen usa un árbol con la ruta más corta y, por lo tanto, no necesita un RP).

En un entorno de ASM, existen dos maneras de que el enrutador virtual determine qué enrutador es el RP de un grupo de multidifusión:

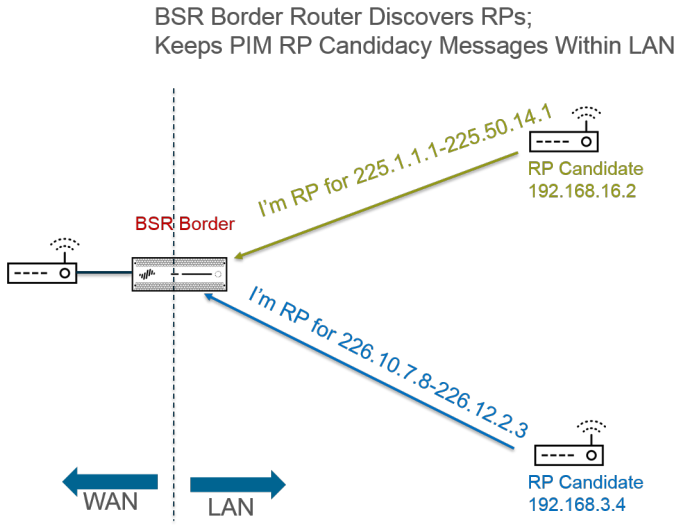
- **Asignación estática de RP a grupo:** configura el enrutador virtual en el cortafuegos para que actúe como RP de grupos de multidifusión. Puede configurar un RP local configurando una dirección RP estática o especificando que el RP local sea un RP candidato y el RP se elija dinámicamente (sobre la base del menor valor de prioridad). También puede configurar estáticamente uno o más RP externos para diferentes rangos de direcciones de grupo que no están cubiertos por el RP local, lo que ayuda a equilibrar la carga del tráfico de multidifusión para que un RP no se sobrecargue.

- **Enrutador de arranque (bootstrap router, BSR)**: (RFC 5059); define la función de un BSR. Primero, los candidatos para BSR anuncian su prioridad entre ellos y, luego, el candidato con la prioridad más alta es elegido BSR, como se muestra en la siguiente figura:



A continuación, el BSR descubre RP cuando los RP candidatos realizan la unidifusión periódica de un mensaje de BSR al BSR que contiene su dirección IP y el rango de grupo de multidifusión para el cual actuarán como RP. Puede configurar el enrutador virtual local para que sea un RP candidato, en este caso el enrutador virtual anuncia su candidatura de RP para grupos o un grupo de multidifusión específico. El BSR envía la información de RP a los demás RP del dominio de PIM.

Cuando configure PIM para una interfaz, puede seleccionar el borde de BSR cuando la interfaz en el cortafuegos esté en un límite empresarial que se sale de la red empresarial. La configuración de borde de BSR evita que el cortafuegos envíe los mensajes de BSR de la candidatura de RP fuera de la red LAN. En la siguiente ilustración, el borde de BSR está habilitado para la interfaz que está frente a la red LAN y esa interfaz tiene la prioridad más alta. Si el enrutador virtual tiene un RP estático y uno dinámico (obtenido del BSR), puede especificar si el RP estático debe anular el RP obtenido de un grupo cuando configure el RP estático local.



Para que el Modo disperso de PIM notifique al RP que tiene tráfico para enviar al árbol compartido, el RP debe conocer el origen. El host notifica al RP que está enviando tráfico a una dirección del grupo de multidifusión cuando el ***enrutador designado*** (designated router, DR) encapsula el primer paquete del host en un mensaje de registro de PIM y realiza la unidifusión del paquete al RP en su red local. El DR también reenvía mensajes de eliminación desde un receptor al RP. El RP mantiene la lista de direcciones IP de orígenes que se envían a un grupo de multidifusión y el RP puede reenviar paquetes de multidifusión desde los orígenes.

¿Por qué los enrutadores de un dominio de PIM necesitan un DR? Cuando el enrutador envía un mensaje de unión de PIM a un conmutador, dos enrutadores podrían recibirlo y reenviarlo al mismo RP, lo que provoca tráfico redundante y desperdicio de ancho de banda. Para evitar el tráfico innecesario, los enrutadores de PIM eligen un DR (el enrutador con la dirección IP más alta) y solo el DR reenvía el mensaje de unión al RP. De manera alternativa, puede asignar una prioridad de DR a un grupo de interfaces, que tiene precedencia sobre las comparaciones de direcciones IP. Como recordatorio, el DR reenvía (o realiza la unidifusión) mensajes de PIM; no realiza la multidifusión de paquetes de multidifusión de IP.

Puede especificar las direcciones IP de los vecinos de PIM (enrutadores) que el grupo de interfaces permitirá intercambiar con el enrutador virtual. De forma predeterminada, todos los enrutadores habilitados para PIM pueden ser vecinos de PIM, pero la opción para limitar vecinos proporciona un paso hacia la protección del enrutador virtual en su entorno de PIM.

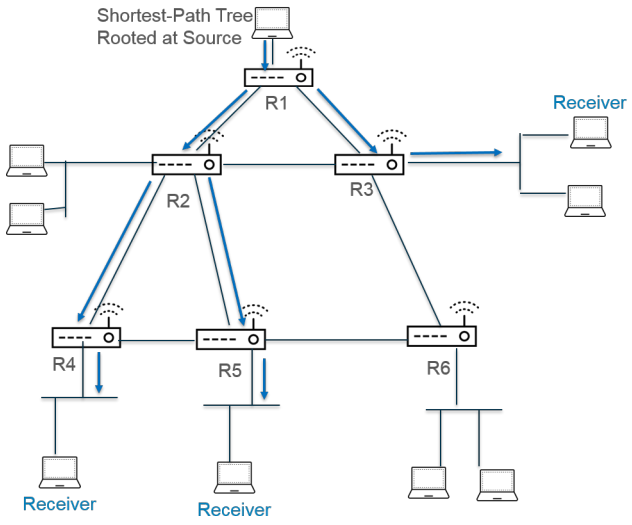
- Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido
- Mecanismo de imposición de PIM
- Reenvío de ruta inversa

Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido

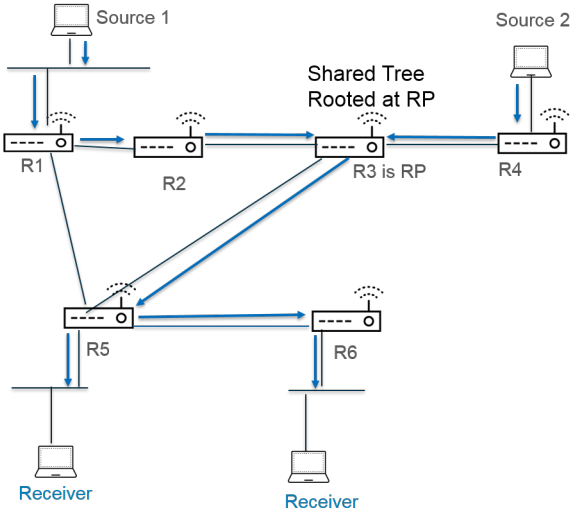
Después de que un receptor se una a un grupo de multidifusión, los enrutadores en la red de acceso múltiple crean las rutas necesarias para enviar datos a cada receptor del grupo. Cada datagrama de IP enviado a un grupo de multidifusión se distribuye (reenvía) a todos los miembros. Las rutas constituyen un tipo de árbol de distribución para un paquete de multidifusión. El objetivo de un árbol de distribución de multidifusión es que el enrutador duplique un paquete de multidifusión cuando este llegue a una divergencia de rutas y el enrutador debe enviarlo a varias rutas para llegar a todos los miembros del grupo, pero el árbol de distribución debe abstenerse de enviar paquetes por una ruta en la que no existen receptores interesados. El árbol de distribución es uno de los siguientes:

- Un **árbol fuente:** una ruta de una fuente de multidifusión (la raíz del árbol) a través de la red a los receptores en el grupo de multidifusión. El árbol fuente es la ruta más corta que un paquete de multidifusión puede tomar desde la fuente al receptor, por lo que también se le conoce como el **árbol con la ruta más corta (shortest-path tree, SPT)**. El emisor y receptor se anotan como un par del grupo multidifusión y fuente, abreviado a (S, G); por ejemplo, (192.168.1.1, 225.9.2.6).

La siguiente figura muestra tres árboles con la ruta más corta desde la fuente hasta los tres receptores.



- Un **árbol compartido:** una ruta con la raíz en el RP, no en la fuente de multidifusión. Al árbol compartido también se le conoce como árbol RP o RPT. Los enrutadores reenvían paquetes de multidifusión de varias fuentes al RP y el RP reenvía los paquetes al árbol compartido. Un árbol compartido se anota como (*,G) con un asterisco como la fuente porque todas las fuentes que pertenecen al grupo de multidifusión comparten el mismo árbol de distribución del RP. Un ejemplo de anotación de árbol compartido es (*, 226.3.1.5). La siguiente figura muestra un árbol compartido desde la raíz en el RP a los receptores.



La Multidifusión de fuente específica (Source-Specific Multicast, SSM) usa la distribución del árbol fuente. Cuando configura la multidifusión de IP para que use la Multidifusión de cualquier fuente (Any Source Multicast, ASM), puede especificar qué árbol de distribución usa el enrutador virtual en su cortafuegos de Palo Alto Networks® para entregar paquetes de multidifusión a un grupo mediante la configuración de un umbral de SPT para el grupo:

- De manera predeterminada, el enrutador virtual cambia el enrutamiento de multidifusión del árbol compartido a SPT cuando recibe el primer paquete de multidifusión para un grupo o prefijo (el **SPT Threshold [Umbral de SPT]** se configura en 0).

- Puede configurar que el enrutador virtual cambie a SPT cuando el número total de kilobits de los paquetes que llegan al grupo o prefijo de multidifusión especificado en cualquier interfaz durante cualquier período de tiempo alcance un número configurado.
- Puede configurar que el enrutador virtual nunca cambie a SPT para el grupo o prefijo (continúa usando el árbol compartido).

SPT requiere más memoria, por lo que debe elegir su configuración en función de su nivel de tráfico de multidifusión en el grupo. Si el enrutador virtual cambia a SPT, los paquetes llegarán desde la fuente (en lugar del RP) y el enrutador virtual envía un mensaje de eliminación al RP. La fuente envía paquetes de multidifusión subsiguientes para ese grupo por el árbol con la ruta más corta.

Mecanismo de imposición de PIM

Para evitar que los enrutadores de una red de acceso múltiple reenvíen el mismo tráfico de multidifusión al mismo salto siguiente (lo que provocaría tráfico redundante y un desperdicio de ancho de banda), PIM usa el mecanismo de imposición para elegir un solo reenviador de PIM para la red de acceso múltiple.

Si el enrutador virtual recibe un paquete multidifusión de una fuente en una interfaz que el enrutador virtual ya asocia como la interfaz de salida para el mismo par (S, G) identificado en el paquete, esto significa que es un paquete duplicado. Por tanto, el enrutador virtual envía un mensaje de imposición que contiene sus métricas a los demás enrutadores de la red de acceso múltiple. Luego, los enrutadores eligen un reenviador de PIM de esta manera:

1. El reenviador de PIM es el enrutador con la menor distancia administrativa a la fuente de multidifusión.
2. En el caso de un empate en la menor distancia administrativa, el reenviador de PIM es el enrutador con la mejor métrica de enrutamiento de unidifusión a la fuente.
3. En el caso de un empate en la mejor métrica, el reenviador de PIM es el enrutador con la dirección IP más alta.

Los enrutadores que se eligen como reenviador de PIM detendrán el reenvío de tráfico al grupo de multidifusión identificado en el par (S, G).

Cuando configure una multidifusión de IP, puede configurar el intervalo en cual el enrutador virtual envía mensajes de imposición de PIM a la interfaz (el intervalo de imposición). Cuando visualiza la información de la multidifusión de IP, la pestaña **PIM Interface (Interfaz de PIM)** muestra el intervalo de imposición de una interfaz.

Reenvío de ruta inversa

PIM usa el Reenvío de ruta inversa (reverse-path forwarding, RPF) para evitar bucles de enrutamiento de la multidifusión mediante el aprovechamiento de la tabla de enrutamiento de unidifusión en el enrutador virtual. Cuando el enrutador virtual recibe un paquete de multidifusión, busca la fuente en su tabla de enrutamiento de unidifusión para verificar si la interfaz de salida asociada con esa dirección IP de origen es la interfaz a la que llegó el paquete. Si las interfaces coinciden, el enrutador virtual duplica el paquete y lo reenvía desde las interfaces hacia los receptores de multidifusión del grupo. Si las interfaces no coinciden, el enrutador virtual descarta el paquete. La tabla de enrutamiento de unidifusión se basa en las rutas estáticas subyacentes o el protocolo de puerta de enlace interno (interior gateway protocol, IGP) que usa su red, como OSPF.

PIM también usa RPF para crear un árbol con la ruta más corta a una fuente, un salto de enrutador de PIM a la vez. El enrutador virtual tiene la dirección de la fuente de multidifusión, de modo que el enrutador virtual seleccione como su siguiente salto hacia la fuente el PIM vecino más próximo que el enrutador virtual usaría para reenviar paquetes de unidifusión a la fuente. El enrutador del siguiente salto realiza la misma acción.

Después de que el RPF se realice correctamente y el enrutador virtual tenga una entrada de ruta en su Base de información de enrutamiento multidifusión (multicast routing information base, mRIB), el enrutador virtual conserva las entradas del árbol basadas en la fuente (S,G) y las entradas de árbol compartido (*,G) en su base de información de reenvío de multidifusión (la tabla de reenvío de multidifusión [multicast forwarding table, mFIB]). Cada entrada incluye la dirección IP de origen, el grupo de multidifusión, la interfaz de entrada (interfaz de RPF) y la lista de interfaces de salida. Pueden existir varias interfaces de salida para una entrada porque el árbol con la ruta más corta puede bifurcarse en el enrutador, y el enrutador debe reenviar el paquete a varias interfaces para llegar a los receptores del grupo que están ubicados en diferentes rutas. Cuando el enrutador virtual usa mFIB para reenviar un paquete de multidifusión, coincide con una entrada (S,G) antes de intentar coincidir con una entrada (*,G).

Si anuncia prefijos de fuente de multidifusión en BGP (configuró MP-BGP con la familia de direcciones IPv4 y la familia de direcciones subsiguiente de multidifusión), el cortafuegos siempre realiza la comprobación de RPF en las rutas de BGP que el cortafuegos recibió conforme a la familia de direcciones subsiguiente de multidifusión.

Visualice la información de multidifusión de IP para verificar cómo ver las entradas mFIB y mRIB. Tenga en cuenta que la tabla de ruta de multidifusión (multicast route table, mRIB) es una tabla separada de la tabla de ruta de unidifusión (unicast route table, RIB)

Configuración de IP de multidifusión

Configure interfaces en un enrutador virtual de un cortafuegos de Palo Alto Networks® para recibir y reenviar paquetes de IP de multidifusión. Debe habilitar la multidifusión de IP para el enrutador virtual, configurar la Multidifusión independiente del protocolo (Protocol Independent Multicast, PIM) en las interfaces de entrada y salida, y configurar el Protocolo de administración de grupos de Internet (Internet Group Management Protocol, IGMP) en las interfaces que acceden los receptores.

STEP 1 | Habilite la multidifusión de IP para un enrutador virtual.

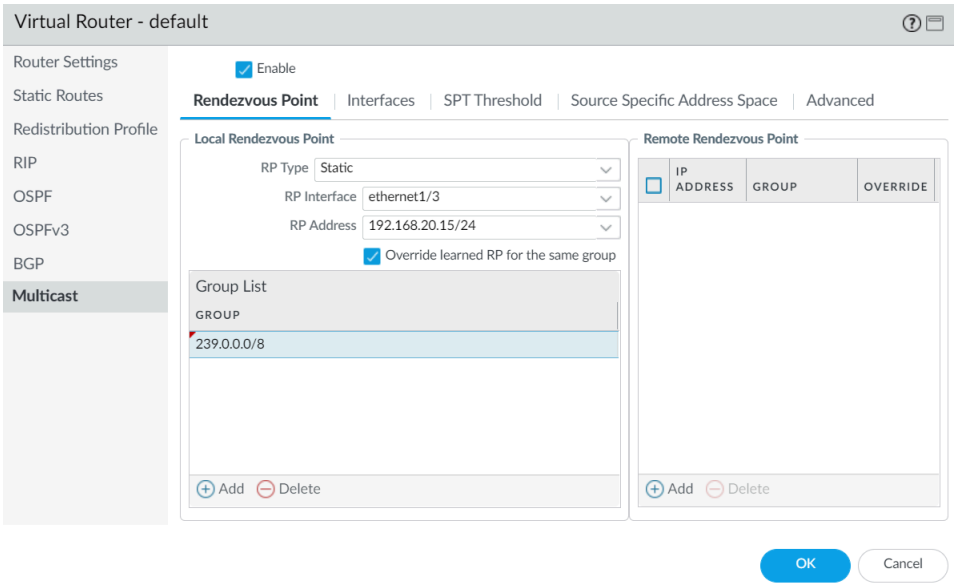
1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Multicast (Multidifusión)** y **Enable (Habilitar)** para habilitar la multidifusión de IP.

STEP 2 | (Únicamente en ASM) Si el dominio de multidifusión en el que el enrutador virtual está localizado usa Multidifusión de cualquier origen (Any-Source Multicast, ASM), identifique y configure los Puntos de encuentro (rendezvous points, RP) locales y remotos para los grupos de multidifusión.

1. Seleccione **Rendezvous Point (Punto de encuentro)**.

2. Seleccione un **RP Type (Tipo de RP)** local, que determine cómo se elige el RP (las opciones son **Static [Estático]**, **Candidate [Candidato]** o **None [Ninguno]**):

   - **Static (Estático)**: establece una asignación estática de un RP para grupos de multidifusión. Si configura un RP estático, se requiere que configure explícitamente el mismo RP en otros enrutadores de PIM en el dominio de PIM.
     - Seleccione **RP Interface (Interfaz de RP)**. Los tipos de interfaz válidos son Capa 3, cable virtual, bucle invertido, VLAN, Ethernet agregada (Aggregate Ethernet, AE) y túnel.
     - Seleccione **RP Address (Dirección de RP)**. La lista se llena con las direcciones IP de la interfaz de RP seleccionada.
     - Seleccione **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)** de modo que este RP estático sirva como RP en lugar del RP elegido para los grupos en la lista de grupos.
     - Seleccione **Add (Añadir)** para añadir uno o más **Groups (Grupos)** de multidifusión para que el RP actúe como RP.



   - **Candidate (Candidato)**: establece una asignación dinámica de un RP a grupos de multidifusión según la prioridad, de modo que cada enrutador en un dominio de PIM elija automáticamente el mismo RP.
     - Seleccione **RP Interface (Interfaz de RP)** del RP candidato. Los tipos de interfaz válidos son Capa 3, bucle invertido, VLAN, Ethernet agregada (Aggregate Ethernet, AE) y túnel.
     - Seleccione la **RP Address (Dirección de RP)** del RP candidato. La lista se llena con las direcciones IP de la interfaz de RP seleccionada.
     - (Opcional) Cambie la **Priority (Prioridad)** para el RP candidato. El cortafuegos compara la prioridad del RP candidato con la prioridad de otros RP candidatos para determinar cuál actúa como RP para los grupos especificados; el cortafuegos

selecciona el RP candidato con el valor de prioridad más bajo (el rango es de 0 a 255; el valor predeterminado es 192).

- (Opcional) Cambie el **Advertisement Interval (sec) (Intervalo de anuncios [segundos])** (el rango es de 1 a 26 214; el valor predeterminado es 60).
- Introduzca una **Group List (Lista de grupos)** de grupos de multidifusión que se comunique con el RP.

- **None (Ninguno)**: seleccione esta opción si este enrutador virtual no es un RP.

3. Seleccione **Add (Añadir)** para añadir un Punto de encuentro remoto e introduzca la **IP Address (Dirección IP)** de ese RP remoto (externo).
4. Seleccione **Add (Añadir)** para añadir las **Group Addresses (Direcciones del grupo)** de multidifusión para las cuales la dirección de RP remoto especificado actúa como RP.
5. Seleccione **Override learned RP for the same group (Cancelar RP obtenido para el mismo grupo)** de modo que el RP externo que configuró estáticamente sirva como RP en lugar de un RP que se obtenga (elija) de manera dinámica para los grupos en la lista de direcciones de grupos.
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Especifique un grupo de interfaces que comparta una configuración de multidifusión (IGMP, PIM y permisos de grupo).

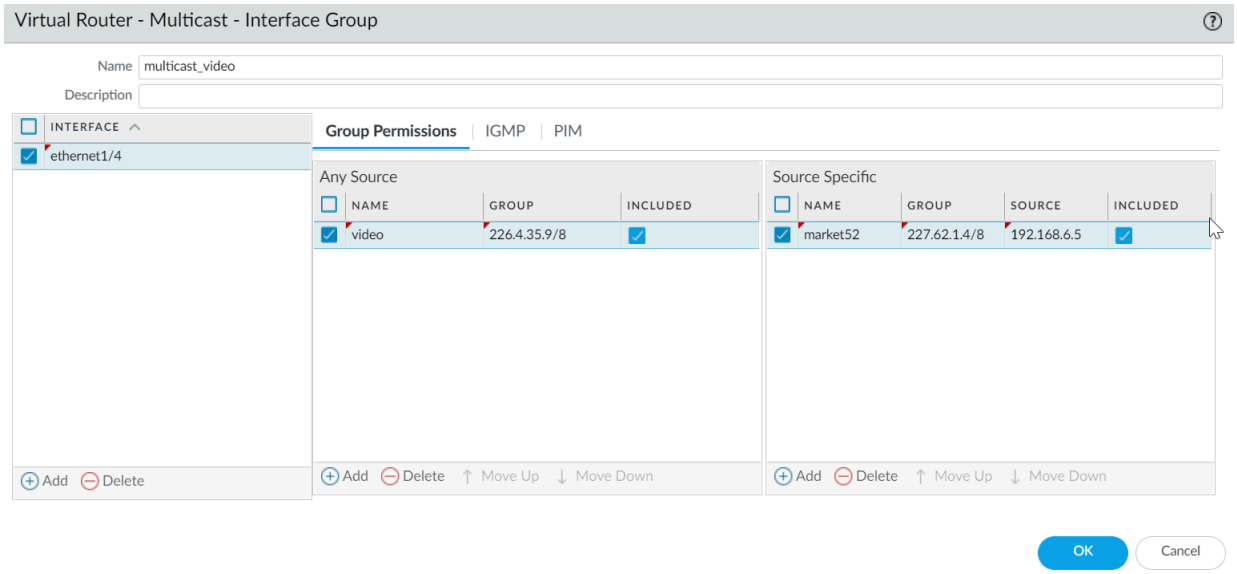
1. En la pestaña **Interfaces (Interfaces)**, seleccione **Add (Añadir)** para añadir un nombre en **Name (Name)** para el grupo de interfaces.
2. Introduzca una **Description (Descripción)**.
3. Seleccione **Add (Añadir)** para añadir una interfaz en **Interface (interfaz)** y seleccione una o más interfaces de Capa 3 que pertenezcan al grupo de interfaces.

STEP 4 | (Opcional) Configure permisos de grupo de multidifusión para el grupo de interfaces. De manera predeterminada, el grupo de interfaces acepta informes de pertenencia de IGMP y mensajes de unión de PIM de todos los grupos.

1. Seleccione **Group Permissions (Permisos del grupo)**.
2. Para configurar grupos de Multidifusión de cualquier origen (Any-Source Multicast, ASM) para este grupo de interfaces, en la ventana Any Source (Cualquier origen), seleccione **Add (Añadir)** para añadir un nombre en **Name (Nombre)** e identificar un grupo de multidifusión que acepte informes de pertenencia de IGMP y mensajes de unión de PIM de cualquier origen.
3. Introduzca una dirección de grupo o dirección de grupo de multidifusión en **Group (Grupo)** y el /prefijo que pueda recibir paquetes de multidifusión de cualquier origen en estas interfaces.
4. Seleccione **Included (Incluido)** para incluir la dirección del grupo de ASM en **Group (Grupo)** en el grupo de interfaces (predeterminado). Cancele la selección de **Included (Incluido)** para excluir con facilidad un grupo de ASM del grupo de interfaces, por ejemplo, durante una prueba.
5. Seleccione **Add (Añadir)** para añadir grupos de multidifusión adicionales en **Groups (Grupos)** (para el grupo de interfaces) que desean recibir paquetes de multidifusión de cualquier origen.

6. Para configurar los grupos de Multidifusión de origen específico (Source-Specific Multicast, SSM) en este grupo de interfaces, en la ventana Source Specific (Origen específico), seleccione **Add (Añadir)** para añadir un nombre en **Name (Nombre)** a fin de identificar el par de direcciones de origen y grupo de multidifusión. No utilice un nombre que use para la multidifusión de cualquier origen. (Debe usar IGMPv3 para configurar SSM).
7. Introduzca la dirección de grupo o una dirección de grupo de multidifusión en **Group (Grupo)** y el /prefijo del grupo que desea recibir paquetes de multidifusión del origen especificado solamente (y que puede recibir los paquetes en estas interfaces).

   *Un grupo de un origen específico para el cual especifica permisos es un grupo que el enrutador virtual debe tratar como específico del origen. Configure **Source Specific Address Space (Espacio de dirección de origen específico)** (Paso 9) que incluye los grupos específicos de origen para los cuales configuró el permiso.*
8. Introduzca la dirección IP de origen en **Source (Origen)** desde la cual este grupo de multidifusión puede recibir paquetes de multidifusión.
9. Seleccione **Included (Incluido)** para incluir el par de direcciones de origen y grupo SSM en el grupo de interfaces (predeterminado). Cancele la selección de **Included (Incluido)** para excluir con facilidad el par del grupo de interfaces, por ejemplo, durante una prueba.
10. Seleccione **Add (Añadir)** para añadir grupos de multidifusión adicionales en **Groups (Grupos)** (para el grupo de interfaces) que reciban paquetes de multidifusión de un único origen específico.



STEP 5 | Configure IGMP para el grupo de interfaces si una interfaz afronta receptores de multidifusión, que deben usar IGMP para unirse a un grupo.

1. En la pestaña **IGMP**, seleccione **Enable (Habilitar)** para habilitar IGMP (predeterminado).
2. Especifique los parámetros de IGMP para las interfaces del grupo de interfaces:
   - **IGMP Version (Versión de IGMP)**: **1**, **2** o **3** (predeterminada).
   - **Enforce Router-Alert IP Option (Aplicar opción de IP de enrutador-alerta)** (deshabilitada de forma predeterminada): seleccione esta opción si requiere paquetes de

IGMP que usen IGMPv2 o IGMPv3 para tener la opción de alerta de enrutador de IP, RFC 2113.

- **Robustness (Potencia)**: una variable que el cortafuegos usa para ajustar las opciones Group Membership Interval (Intervalo de pertenencia del grupo), Other Querier Present Interval (Otro intervalo presente del solicitante), Startup Query Count (Recuento de consultas de inicio) y Last Member Query Count (Último recuento de consulta del miembro) (el rango es de 1 a 7; el valor predeterminado es 2). Aumente el valor si la subred en la cual está ubicado este cortafuegos es propensa a perder paquetes.
- **Max Sources (Máx. de fuentes)**: la cantidad máxima de fuentes que IGMP puede procesar de manera simultánea para una interfaz (el rango es de 1 a 65 535; el valor predeterminado es **unlimited [ilimitado]**).
- **Max Groups (Máx. de grupos)**: la cantidad máxima de grupos que IGMP puede procesar de manera simultánea para una interfaz (el rango es de 1 a 65 535; el valor predeterminado es **unlimited [ilimitado]**).
- **Query Interval (Intervalo de consulta)**: la cantidad de segundos entre mensajes de consulta de pertenencia de IGMP que el enrutador virtual envía a un receptor para determinar si el receptor aún desea recibir los paquetes de multidifusión para un grupo (el rango es de 1 a 31 744; el valor predeterminado es 125).
- **Max Query Response Time (sec) (Máx. de tiempo de respuesta de consulta [segundos])**: la cantidad máxima de segundos permitidos para que un receptor responda a un mensaje de consulta de pertenencia de IGMP antes de que el enrutador virtual determine que el receptor ya no desea recibir paquetes de multidifusión para el grupo (el rango es de 0 a 3174,4; el valor predeterminado es 10).
- **Last Member Query Interval (sec) (Último intervalo de consulta del miembro [segundos])**: la cantidad de segundos permitidos para que un receptor responda a una consulta específica del grupo que el enrutador virtual envía después de que un receptor envía un mensaje para abandonar el grupo (el rango es de 0,1 a 3174,4; el valor predeterminado es 1).
- **Immediate Leave (Salida inmediata)** (deshabilitado de forma predeterminada): cuando existe solo un miembro en un grupo de multidifusión y el enrutador virtual recibe un mensaje de salida de IGMP para ese grupo, la configuración de Immediate Leave (Salida inmediata) provoca que el enrutador virtual elimine de inmediato ese grupo y la interfaz de salida de la Base de información del enrutador de multidifusión (multicast routing information base, mRIB) y la Base de información de reenvío de multidifusión, mFIB), en lugar de esperar que caduque el Último intervalo de consulta del miembro. La opción Immediate Leave (Salida inmediata) ahorra recursos de red. No puede seleccionar Immediate Leave (Salida inmediata) si el grupo de interfaces usa IGMPv1.

STEP 6 | Configure el Modo disperso de PIM (PIM Sparse Mode, PIM-SM) para el grupo de interfaces.

1. En la pestaña **PIM**, seleccione **Enable (Habilitar)** para habilitar PIM (habilitado de manera predeterminada).
2. Especifique los parámetros de PIM del grupo de interfaces:
   - **Assert Interval (Intervalo de imposición)**: la cantidad de segundos entre los mensajes de imposición de PIM que el enrutador virtual envía a otros enrutadores de PIM en la red de multiacceso cuando eligen un reenvío de PIM (el rango es de 0 a 65 534; el valor predeterminado es 177).

- **Hello Interval (Intervalo de saludo)**: la cantidad de segundos entre los mensajes de saludo de PIM que el enrutador virtual envía a sus vecinos de PIM de cada interfaz en el grupo de interfaces (el rango es de 0 a 18 000; el valor predeterminado es 30).
- **Join Prune Interval (Intervalo de unión/eliminación)**: la cantidad de segundos entre mensajes de unión de PIM (y entre mensajes de eliminación de PIM) que el enrutador virtual envía hacia un origen de multidifusión (el rango es de 0 a 18 000; el valor predeterminado es 60).
- **DR Priority (Prioridad de DR)**: la prioridad de Enrutador designado (Designated Router, DR) que controla qué enrutador de una red de multiacceso reenvía mensajes de unión y eliminación de PIM al RP (el rango es de 0 a 429 467 295; el valor predeterminado es 1). La prioridad de DR tiene precedencia sobre las comparaciones de direcciones IP para elegir el DR.
- **BSR Border (Borde de BSR)**: seleccione esta opción si las interfaces del grupo de interfaces se encuentran en un enrutador virtual que es el BSR localizado en el borde de una red LAN empresarial. Esto evitará que los mensajes del BSR de candidatura de RP salgan de la red LAN.

3. Seleccione **Add (Añadir)** para añadir uno o más **Permitted PIM Neighbors (Vecinos de PIM permitidos)** y especifique la **IP Address (Dirección IP)** de cada enrutador desde el cual el enrutador virtual acepta paquetes de multidifusión.

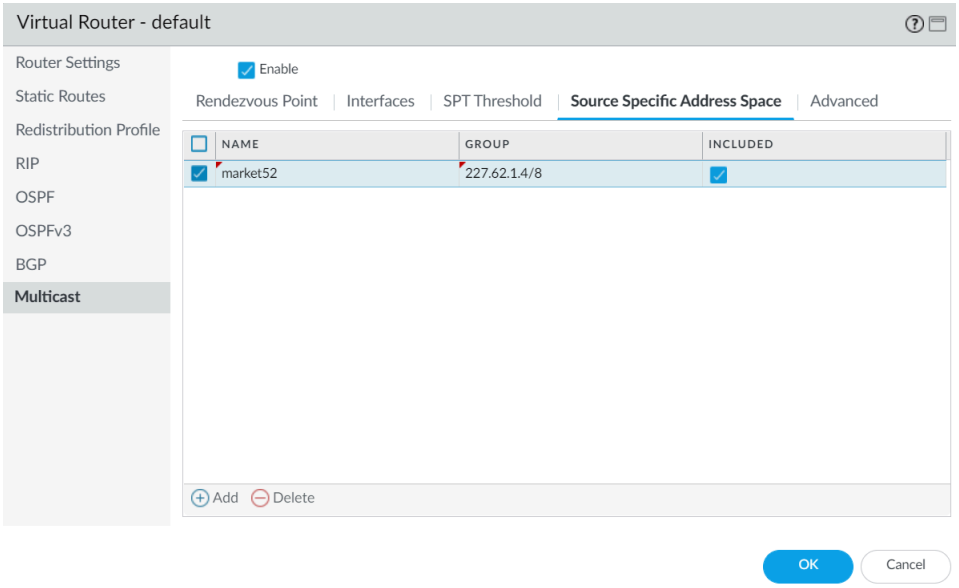
STEP 7 | Haga clic en **OK (Aceptar)** para guardar la configuración del grupo de interfaces.

STEP 8 | (Opcional) Cambie el umbral del Árbol con la ruta más corta (Shortest-Path Tree, SPT), como se describe en Árbol con la ruta más corta (Shortest-Path Tree, SPT) y árbol compartido.

1. Seleccione **SPT Threshold (Umbral de SPT)** y **Add (Añadir)** para añadir un **Multicast Group/Prefix (Prefijo/grupo de mulidifusión)**, el grupo de multidifusión o prefijo para el cual especifica el árbol de distribución.
2. Especifique el **Threshold (kb) (Umbral [kb])**: el punto en el que el enrutamiento al prefijo o grupo de multidifusión especificado cambia del árbol compartido (con origen desde el RP) a una distribución de SPT:
   - **0 (switch on first data packet) (0 [cambiar en el primer paquete de datos])** (predeterminado): el enrutador virtual cambia del árbol compartido al SPT para el grupo o prefijo cuando el enrutador virtual recibe el primer paquete de datos del grupo o prefijo.
   - **never (do not switch to spt) (Nunca [no cambia a spt])**: el enrutador virtual continúa usando el árbol compartido para reenviar paquetes al grupo o prefijo.
   - Introduzca el número total de kilobits de los paquetes de multidifusión que pueden llegar para el grupo de multidifusión o prefijo en cualquier interfaz y durante cualquier período de tiempo, en el que el enrutador virtual cambia a la distribución de SPT para ese prefijo o grupo de multidifusión.

STEP 9 | Identifique los grupos de multidifusión o grupos y prefijos que acepten paquetes de multidifusión solo desde una fuente específica.

1. Seleccione **Source Specific Address Space (Espacio de dirección de origen específico)** y **Add (Añadir)** para añadir un **Name (Nombre)** para el espacio.
2. Introduzca una dirección de grupo de multidifusión en **Group (Grupo)** con la longitud de prefijo para identificar el espacio de direcciones que recibe paquetes de multidifusión de una fuente específica. Si el enrutador virtual recibe un paquete de multidifusión para un grupo de SSM pero el grupo está cubierto por un **Source Specific Address Space (Espacio de dirección de origen específico)**, el enrutador virtual descarta el paquete.
3. Seleccione **Included (Incluido)** para incluir espacio de dirección de origen específico como un rango de direcciones del grupo de multidifusión desde el cual el enrutador virtual aceptará los paquetes de multidifusión que se originaron desde una fuente específica permitida. Cancele la selección de **Included (Incluido)** para excluir fácilmente un espacio de direcciones de grupo de la prueba.
4. Añada otros espacios de direcciones de origen específico para incluir todos estos grupos para los cuales especificó el permiso de grupo de SSM.



STEP 10 | (Opcional) Cambie la cantidad de tiempo que una ruta de multidifusión permanece en mRIB después de que finalice la sesión entre un grupo de multidifusión y una fuente.

1. Seleccione la pestaña **Advanced (Avanzado)**.
2. Especifique el **Multicast Route Age Out Time (sec) (Tiempo de vencimiento de ruta de multidifusión [segundos])** (el intervalo es de 210 a 7200; el valor predeterminado es 210).

STEP 11 | Haga clic en **OK (Aceptar)** para guardar la configuración de multidifusión.

STEP 12 | Cree una regla de política de seguridad para permitir el tráfico de multidifusión a la zona de destino.

1. Cree una regla de política de seguridad y en la pestaña **Destination (Destino)**, seleccione **multicast (Multidifusión)** o **any (Cualquiera)** para la **Destination Zone (Zona de destino)**. La zona **multicast (Multidifusión)** es una zona de Capa 3 predefinida que coincide con

todo el tráfico de multidifusión. La **Destination Address (Dirección de destino)** puede ser una dirección del grupo de multidifusión.

2. Configure el resto de la regla de política de seguridad.

STEP 13 | (Opcional) Habilite el almacenamiento en búfer de los paquetes de multidifusión antes de configurar una ruta.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Habilite el **Multicast Route Setup Buffering (Configuración del almacenamiento en búfer de la ruta de multidifusión)** (deshabilitado de forma predeterminada). El cortafuegos puede preservar los primeros paquetes desde un flujo de multidifusión si una entrada del grupo de multidifusión correspondiente todavía no existe en la tabla de reenvío de multidifusión (mFIB) El **Buffer Size (Tamaño del búfer)** controla cuántos paquetes almacena el cortafuegos en el búfer desde un flujo. Después de instalar la ruta en mFIB, el cortafuegos reenvía automáticamente los primeros paquetes almacenados en el búfer al receptor. (Solo debe habilitar la configuración de almacenamiento en el búfer de la ruta de multidifusión si los servidores de contenido están directamente conectados al cortafuegos y su aplicación de multidifusión no puede resistir que el primer paquete del flujo se omita).
3. (Opcional) Cambie el **Buffer Size (Tamaño del búfer)**. El tamaño del búfer es el número de paquetes por flujo de multidifusión que el cortafuegos puede almacenar en el búfer hasta que se configura la entrada de mFIB (el intervalo es de 1 a 2000; el valor predeterminado es 1000). El cortafuegos puede almacenar en el búfer un máximo de 5000 paquetes en total (para todos los flujos).
4. Haga clic en **OK (Aceptar)**.

STEP 14 | **Commit (Confirmar)** los cambios.

STEP 15 | Visualice la información de multidifusión de IP para ver las entradas de mRIB y mFIB, configuración de interfaz de IGMP, pertenencias de grupo de IGMP, modos de ASM SSM de PIM, asignaciones de grupo a los RP, direcciones de DR, configuración de PIM, vecinos de PIM y mucho más.

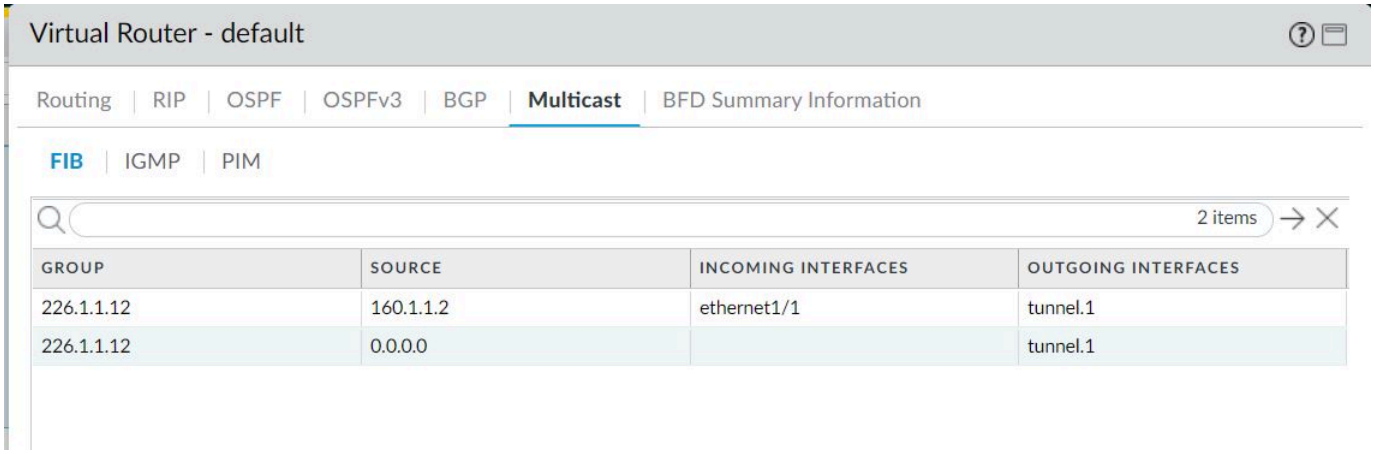
STEP 16 | Si configura una ruta estática para el tráfico de multidifusión, puede instalar la ruta solamente en la tabla de enrutamiento de multidifusión (no en la tabla de enrutamiento de unidifusión) de modo que la ruta se utilice solo para el tráfico de multidifusión.

STEP 17 | Si habilita la multidifusión de IP, no es necesario configurar BGP con MP-BGP para la multidifusión de IPv4 salvo que tenga una topología de multidifusión lógica separada de una topología de unidifusión lógica. Configure extensiones MP-BGP con la familia de direcciones IPv4 y la familia de direcciones subsiguientes de multidifusión solo cuando desee anunciar prefijos de origen de multidifusión en BGP bajo la familia de direcciones subsiguientes de multidifusión.

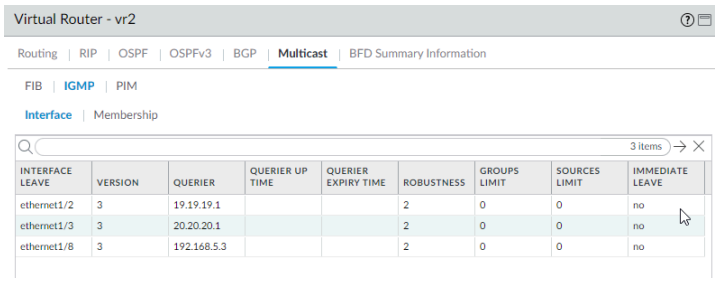
Visualización de información de IP de multidifusión

Luego de configurar el enrutamiento de la multidifusión de IP, visualice las rutas de multidifusión, las entradas de reenvío y la información sobre sus interfaces IGMP y PIM.

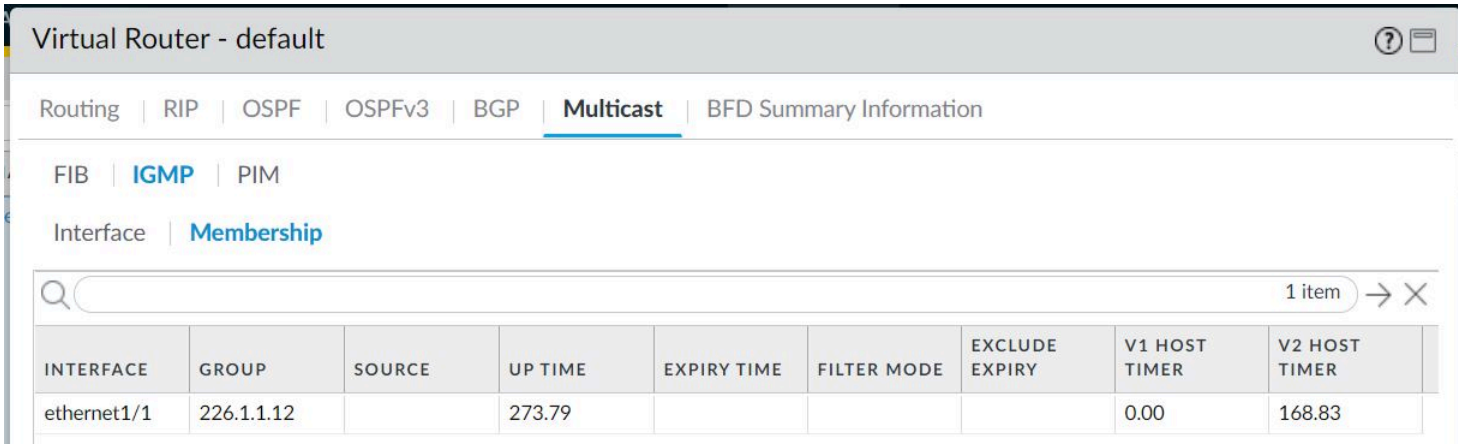
- Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y en la fila del enrutador virtual que configuró, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
  1. Seleccione **Routing (Enrutamiento)** > **Route Table (Tabla de rutas)** y luego el botón de opción **Multicast (Multidifusión)** para mostrar solo las rutas de multidifusión (grupo de multidifusión de IP de destino, el siguiente salto a ese grupo y la interfaz de salida). Esta información proviene de la mRIB.
  2. Seleccione **Multicast (Multidifusión)** > **FIB** para ver la información de la ruta de multidifusión de la mFIB: grupos de multidifusión a los que pertenece el enrutador virtual, la fuente correspondiente, las interfaces de entrada y las interfaces de salida hacia los receptores.



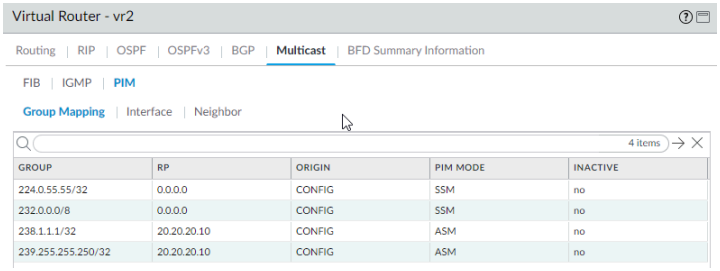
  3. Seleccione **Multicast (Multidifusión)** > **IGMP** > **Interface (Interfaz)** para ver las interfaces habilitadas para IGMP, la versión de IGMP asociada, la dirección IP del solicitante de IGMP, el tiempo en actividad y la fecha de validez del solicitante, la configuración de potencia, los límites en la cantidad de fuentes y grupos de multidifusión, y si la interfaz está configurada para la salida inmediata.



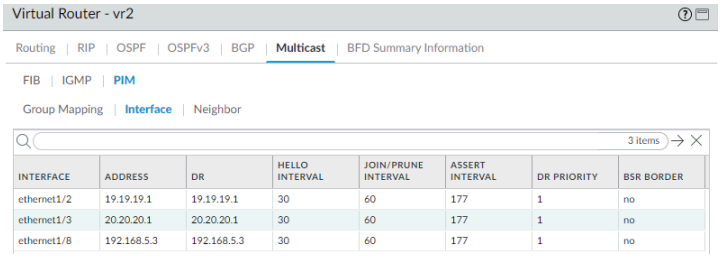
4. Seleccione **Multicast (Multidifusión)** > **IGMP** > **Membership (Pertenencia)** para ver las interfaces habilitadas para IGMP y los grupos de multidifusión a los cuales pertenecen, la fuente y otra información de IGMP.



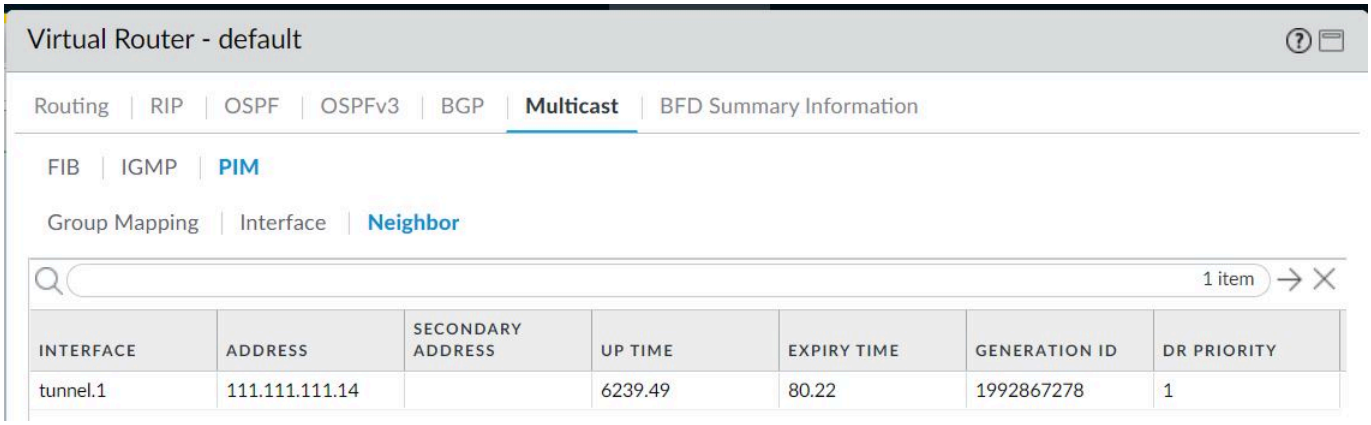
5. Seleccione **Multicast (Multidifusión)** > **PIM** > **Group Mapping (Asignación de grupos)** para ver los grupos de multidifusión asignados a un RP, el origen de la asignación de RP, el modo de PIM del grupo (ASM o SSM) y si el grupo está inactivo. Los grupos en modo SSM no usan un RP, de modo que la dirección de RP que se muestra es 0.0.0.0. El grupo SSM predeterminado es 232.0.0.0/8.



6. Seleccione **Multicast (Multidifusión)** > **PIM** > **Interface (Interfaz)** para ver la dirección IP del DR de una interfaz; la prioridad de DR; los intervalos de saludo, unión/eliminación e imposición; y si la interfaz es un enrutador de arranque (bootstrap router, BSR).



7. Seleccione **Multicast (Multidifusión)** > **PIM** > **Neighbor (Vecino)** para ver la información sobre enrutadores que son vecinos PIM del enrutador virtual.



Redistribución de ruta

Obtenga información y configure la redistribución de rutas para aumentar la accesibilidad del tráfico de red.

> Descripción general sobre la redistribución de rutas
> Configuración de la redistribución de rutas

Descripción general sobre la redistribución de rutas

La redistribución de rutas en el cortafuegos es el proceso de crear rutas que el cortafuegos obtuvo de un protocolo de enrutamiento (o una ruta estática o conectada) disponible para un protocolo de enrutamiento diferente, con lo cual se aumenta la accesibilidad del tráfico de red. Sin la redistribución de rutas, un enrutador o enrutador virtual anuncia y comparte rutas solo con otros enrutadores que se ejecutan en el mismo protocolo de enrutamiento. Puede redistribuir rutas BGP Ipv6 o IPv4, conectadas o estáticas en RIB OSPF y redistribuir rutas OSPFv3, conectadas o estáticas en RIB BGP.

Esto significa, por ejemplo, que puede crear redes específicas que una vez estuvieron disponibles solo mediante una configuración de ruta estática manual en enrutadores específicos para sistemas BGP autónomos o áreas OSPF. También puede anunciar rutas conectadas a nivel local, tal como rutas a una red de laboratorio privada, en sistemas BGP autónomos o en áreas OSPF.

Podría proporcionar a los usuarios de su red OSPFv3 interna acceso a BGP, para que puedan acceder a los dispositivos en Internet. En este caso, puede redistribuir las rutas BGP en el RIB OPSFv3.

Por el contrario, puede brindar a sus usuarios externos acceso a algunas partes de su red interna, de modo que puede poner sus redes OSPFv3 internas a disposición a través de BGP mediante la redistribución de las rutas OSPFv3 en el RIB de BGP.

Para Configuración de la redistribución de rutas, comience por crear un perfil de redistribución.

Configuración de la redistribución de rutas

Realice el siguiente procedimiento para configurar la redistribución de rutas.

STEP 1 | Cree un perfil de redistribución.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione un enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y, luego, **Add (Añadir)** para añadir un perfil.
3. Introduzca un **Name (Nombre)** para el perfil, que debe comenzar con un carácter alfanumérico y puede contener cero o más guiones bajos (_), guiones (-), puntos (.) o espacios (hasta 16 caracteres).
4. Introduzca una **Priority (Prioridad)** para el perfil en el intervalo de 1 a 255. El cortafuegos compara las rutas a los perfiles en orden y utiliza el perfil con la prioridad más alta (valor de prioridad más bajo) en primer lugar. Las reglas de prioridad más altas tienen preferencia sobre las reglas con prioridades más bajas.
5. Para **Redistribute (Redistribuir)**, seleccione una de las siguientes opciones:
   - **Redist (Redistribuir)**: seleccione esta opción para la redistribución de las rutas que coincidan con este filtro.
   - **No Redist (No redistribuir)**: seleccione las rutas de redistribución que coincidan con los perfiles de redistribución, excepto las rutas que coincidan con este filtro. Esta selección trata el perfil como una lista de bloqueo que especifica qué rutas no se deben seleccionar para la redistribución. Por ejemplo, si tiene varios perfiles de redistribución para BGP, puede crear un perfil **No Redist (No redistribuir)** para excluir varios prefijos y luego un perfil de redistribución general con una prioridad más baja (valor de prioridad más alto) posterior a aquel. Los dos perfiles se combinan y el perfil de prioridad más alta tiene preferencia. No puede tener solo perfiles **No Redist (No redistribuir)**; siempre necesita al menos un perfil **Redist (Redistribuir)** para redistribuir rutas.

6. En la pestaña **General Filter (Filtro general)**, para Source Type (Tipo de origen), seleccione uno o más tipos de rutas para redistribuir:
   - **bgp**: redistribuya rutas BGP que coincidan con el perfil.
   - **connect**: redistribuya rutas conectadas que coincidan con el perfil.
   - **ospf** (solo IPv4): redistribuya rutas OSPF que coincidan con el perfil.
   - **rip** (solo IPv4): redistribuya rutas RIP que coincidan con el perfil.
   - **ospfv3** (solo IPv6): redistribuya rutas OSPFv3 que coincidan con el perfil.
   - **static**: redistribuya rutas estáticas que coincidan con el perfil.
7. (Opcional) Para **Interface (Interfaz)**, seleccione **Add (Añadir)** y añada una o más interfaces de salida de las rutas asociadas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
8. (Opcional) Para **Destination (Destino)**, seleccione **Add (Añadir)** y añada uno o más destinos IPv4 o IPv6 de las rutas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
9. (Opcional) Para **Next Hop (Próximo salto)**, seleccione **Add (Añadir)** y añada una o más direcciones IPv4 o IPv6 de próximo salto de las rutas para que coincidan con la redistribución. Para eliminar una entrada, haga clic en **Delete (Eliminar)**.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional: cuando el filtrado general incluye ospf u ospfv3) Cree un filtro OSPF para especificar en detalle qué rutas OSPF u OSPFv3 redistribuir.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y seleccione el perfil que creó.
3. Seleccione **OSPF Filter (Filtro OSPF)**.
4. Para Path Type (Tipo de ruta), seleccione uno o más de los siguientes tipos de ruta OSPF para redistribuir: **ext-1**, **ext-2**, **inter-area**, or **intra-area**.
5. Para especificar un **Area (Área)** desde la cual redistribuir las rutas OSPF u OSPFv3, seleccione **Add (Añadir)** y añada un área en formato de dirección IP.
6. Para especificar una **Tag (Etiqueta)**, seleccione **Add (Añadir)** para añadir una etiqueta en formato de dirección IP.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional: cuando el filtrado general incluye bgp) Cree un filtro BGP para especificar en detalle qué rutas BGP redistribuir.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **Redistribution Profile (Perfil de redistribución)** e **IPv4** o **IPv6** y seleccione el perfil que creó.
3. Seleccione **BGP Filter (Filtro BGP)**.
4. Para **Community (Comunidad)**, seleccione **Add (Añadir)** para seleccionar de la lista de comunidades, tal como las comunidades reconocidas: **local-as**, **no-advertise**, **no-export**, or

nopeer. También puede introducir un valor de 32 bits en formato decimal o hexadecimal o formato AS:VAL en el que AS y VAL estén dentro del intervalo de 0 a 65 535. Introduzca un máximo de 10 entradas.

5. Para **Extended Community (Comunidad extendida)**, seleccione **Add (Añadir)** para añadir una comunidad extendida como un valor de 64 bits en formato hexadecimal o en formato TYPE:AS:VAL o TYPE:IP:VAL. TYPE es de 16 bits; AS o IP es de 16 bits; VAL es de 32 bits. Introduzca un máximo de cinco entradas.
6. Haga clic en **OK (Aceptar)**.

STEP 4 | Seleccione el protocolo en el cual está redistribuyendo las rutas, y establezca los atributos para esas rutas.

Esta tarea ilustra las rutas de redistribución en BGP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual.
2. Seleccione **BGP** > **Redist Rules (Reglas de redistribución)**.
3. Seleccione **Allow Redistribute Default Route (Permitir ruta predeterminada de redistribución)** para permitir que el cortafuegos redistribuya la ruta predeterminada.
4. Haga clic en **Add (Añadir)**.
5. Seleccione **Address Family Type (Tipo de familia de direcciones)**: **IPv4** o **IPv6** para especificar en qué tabla de rutas se colocarán las rutas redistribuidas.
6. En **Name (Nombre)**, seleccione el nombre del perfil de redistribución que creó, que selecciona las rutas para redistribuir.
7. Seleccione **Enable (Habilitar)** para habilitar la regla de redistribución.
8. (Opcional) Ingrese cualquiera de los siguientes valores, que el cortafuegos aplica a las rutas que se están redistribuyendo:
   - **Metric (Métrica)** en el intervalo de 1 a 65 535.
   - **Set Origin (Establecer origen)**; el origen de la ruta: **igp**, **egp**, or **incomplete**.
   - **Set MED (Configurar MED)**: valor MED en el intervalo de 0 a 4 294 967 295.
   - **Set Local Preference (Establecer preferencia local)**: valor de preferencia local en el intervalo de 0 a 4 294 967 295.
   - **Set AS Path Limit (Establecer límite de ruta AS)**: cantidad máxima de sistemas autónomos en AS_PATH en el intervalo de 1 a 255.
   - **Set Community (Establecer comunidad)**: seleccione o introduzca un valor de 32 bits en formato decimal o hexadecimal, o introduzca un valor en formato AS:VAL en el que AS y VAL estén dentro del intervalo de 0 a 65 525. Introduzca un máximo de 10 entradas.
   - **Set Extended Community (Establecer comunidad extendida)**: seleccione o introduzca una comunidad extendida como un valor de 64 bits en formato hexadecimal o en formato TYPE:AS:VAL o TYPE:IP:VAL. TYPE es de 16 bits; AS o IP es de 16 bits; VAL es de 32 bits. Introduzca un máximo de cinco entradas.
9. Haga clic en **OK (Aceptar)**.

STEP 5 | **Commit (Confirmar)** los cambios.

Túneles GRE

El protocolo de túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) es un protocolo de operador que encapsula un protocolo de carga. El paquete de GRE se encapsula en un protocolo de transporte (IPv4 o IPv6).

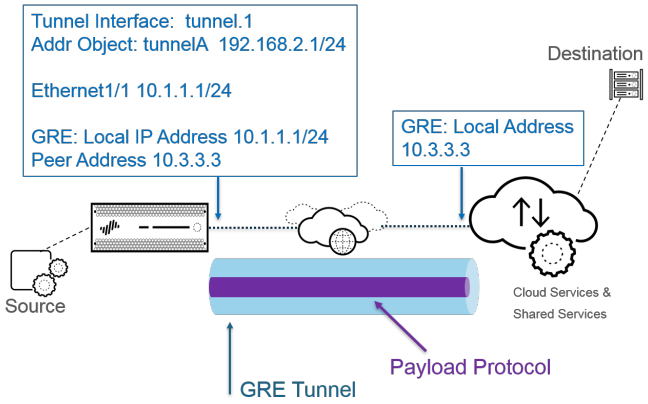
> Descripción general de los túneles de GRE
> Creación de túneles de GRE

Descripción general de los túneles de GRE

Un túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) se conecta a dos endpoints (un cortafuegos y otro dispositivo) con un enlace lógico punto a punto. El cortafuegos puede finalizarlos, y el usuario puede enrutar o reenviar paquetes a los túneles de GRE. Son tan fáciles de usar que se suelen elegir como protocolo de tunelización para ofrecer conectividad de punto a punto, sobre todo a los servicios en la nube o a las redes de socios.

Cree un túnel de GRE para que los paquetes destinados a cierta dirección IP sigan una ruta de punto a punto concreta, por ejemplo, a un proxy basado en la nube o a la red de un socio. Los paquetes atraviesan el túnel de GRE (por una red de tránsito como Internet) hasta servicio en la nube en su camino hacia la dirección de destino. De ese modo, el servicio en la nube puede aplicarles sus servicios o políticas.

En la figura siguiente se muestra un ejemplo de túnel de GRE que conecta el cortafuegos con un servicio en la nube a través de internet.



Para mejorar el rendimiento y para evitar fallos en puntos únicos, reparta las conexiones al cortafuegos entre varios túneles de GRE en vez de usar uno. Cada túnel de GRE necesita una interfaz de túnel.

Cuando el cortafuegos permite que un paquete pase (basándose en una coincidencia con la política) y el paquete sale a una interfaz de túnel de GRE, el cortafuegos añade encapsulación GRE, pero no genera ninguna sesión. El cortafuegos no realiza una búsqueda de las reglas de la política de seguridad para el tráfico encapsulado con GRE, por lo que no hacen falta en este caso. Ahora bien, cuando el cortafuegos recibe tráfico de GRE, genera una sesión y aplica todas las políticas al encabezado IP de GRE, además de al tráfico encapsulado. El cortafuegos trata el paquete de GRE recibido como cualquier otro paquete. Por lo tanto:

- Si el cortafuegos recibe el paquete de GRE en una interfaz que tiene la misma zona que la interfaz asociada al túnel de GRE (por ejemplo, tunnel.1 [túnel.1]), la zona de origen es la misma que la zona de destino. Como el tráfico se permite dentro de una zona concreta de manera predeterminada (tráfico intrazona), el tráfico de GRE de entrada también está permitido por defecto.
- No obstante, si configura una regla de la política de seguridad propia sobre intrazonas en la política de seguridad para denegar dicho tráfico, debe permitir de forma explícita el tráfico de GRE.

- De igual modo, si la zona de la interfaz asociada al túnel de GRE (por ejemplo, tunnel.1 [túnel.1]) es distinta de la zona de la interfaz de entrada, debe configurar una regla de la política de seguridad para permitir el tráfico de GRE.

Como el cortafuegos encapsula el paquete tunelizado en un paquete de GRE, los 24 bytes adicionales del encabezado de GRE tienen de forma automática un Tamaño de segmento máximo (MSS) más reducido en la unidad máxima de transmisión (Maximum Transmission Unit, MTU). Si no modifica el tamaño de ajuste del tamaño máximo de segmento (Maximum Segment Size, MSS) de IPv4 correspondiente a la interfaz, el cortafuegos reduce la MTU en 64 bytes (40 bytes del encabezado de IP más 24 bytes del encabezado de GRE) de forma predeterminada. Eso significa que, si la MTU predeterminada es de 1500 bytes, el MSS es de 1436 bytes (1500 - 40 - 24 = 1436). Si configura un tamaño de ajuste de MSS de 300 bytes, por ejemplo, el MSS es de solo 1,176 bytes (1500 - 300 - 24 = 1176).

El cortafuegos no admite el enrutamiento de un túnel de GRE o IPSec a un túnel de GRE, pero puede enrutar un túnel de GRE a un túnel de IPSec. Adicionalmente:

- Los túneles de GRE no admiten la calidad de servicio (quality of service, QoS).
- El cortafuegos no admite que una sola interfaz funcione a la vez como terminal de túneles de GRE y como agente de descifrado.
- La tunelización de GRE no admite la traducción de direcciones de red (network address translation, NAT) entre los terminales de los túneles de GRE.

Si necesita conectarse a la red de otro proveedor, le recomendamos que configure un túnel IPSec, no un túnel de GRE; solo debe usar un túnel de GRE si es el único mecanismo de túnel punto a punto que admite el proveedor. Además, si el endpoint remoto exige GRE por IPSec, puede habilitar esta opción en ***Add GRE Encapsulation (Añadir encapsulación GRE)****. Añada la encapsulación GRE si el terminal remoto exige que se encapsule el tráfico del túnel de GRE antes de que IPSec lo cifre. En algunas implementaciones, por ejemplo, es obligatorio encapsular el tráfico de multidifusión para que IPSec pueda cifrarlo. Si es un requisito de su entorno y si los túneles de GRE y de IPSec comparten la dirección IP, seleccione* ***Add GRE Encapsulation (Añadir encapsulación GRE)*** *cuando configure el túnel de IPSec.*

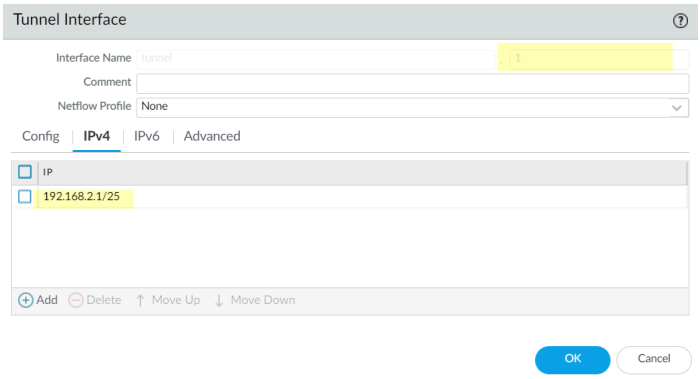
Si desea inspeccionar y controlar el tráfico que atraviesa el cortafuegos por un túnel de GRE, pero no tiene intención de finalizar este, no lo cree; en su lugar, realice el procedimiento Inspección del contenido del túnel para inspeccionar el tráfico de GRE. Aparte de tener esa finalidad, la inspección del contenido permite aplicar la política al tráfico de GRE que pasa a través del cortafuegos sin crear un enlace lógico punto a punto para dirigir el tráfico.

Creación de túneles de GRE

Cree un túnel de encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) para conectar dos endpoints con un enlace lógico punto a punto.

STEP 1 | Cree una interfaz de túnel.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)**.
2. **Añada** un túnel y especifique el **nombre de interfaz**seguido por un punto y un número (el intervalo es de 1 a 9999). Por ejemplo, **`tunnel.1`**.
3. En la pestaña **Config (Configuración)**, asigne la interfaz de túnel a un enrutador en **Virtual Router (Enrutador virtual)**.
4. Si el cortafuegos admite varios sistemas virtuales, asigne la interfaz de túnel a uno concreto en **Virtual System (Sistema virtual)**.
5. Asigne la interfaz de túnel a una zona segura en **Security Zone (Zona de seguridad)**.



6. Asigne una dirección IP a la interfaz de túnel. Es obligatorio asignarla si desea realizar el enrutamiento a este túnel o supervisar su terminal. Seleccione **IPv4** o **IPv6** o bien configure ambas opciones.

   Tanto esta dirección como la dirección correspondiente de la interfaz de túnel del peer deben estar en la misma subred, ya que es un enlace lógico de punto a punto.

   - (Solo IPv4) En la pestaña **IPv4**, haga clic en **Add (Añadir)** para agregar una dirección IPv4 o seleccionar un objeto de dirección o bien haga clic en **New Address (Nueva**

dirección), especifique el **tipo** de dirección e introdúzcala. Por ejemplo, especifique **192.168.2.1**.

- (Solo IPv6) En la pestaña **IPv6**, **habilite IPv6 en la interfaz**.
  1. En **Interface ID (ID de interfaz)**, seleccione **EUI-64 (default 64-bit Extended Unique Identifier) (EUI-64 [identificador único ampliado de 64 bits predeterminado])**.
  2. **Añada** una nueva **dirección**, seleccione un objeto de dirección IPv6 o haga clic en **New Address (Nueva dirección)** y especifique un **nombre** de dirección. **Habilite la dirección en la interfaz** y haga clic en **OK (Aceptar)**.
  3. Seleccione el **tipo** de dirección y especifique la dirección IPv6 o FQDN y haga clic en**OK (Aceptar)** para guardar la nueva dirección.
  4. Seleccione **Enable address on interface (Habilitar la dirección en la interfaz)** y haga clic en **OK (Aceptar)**.

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

STEP 2 | Cree un túnel de GRE para forzar que los paquetes atraviesen una ruta de punto a punto concreta.

1. Seleccione **Network (Red)** > **GRE Tunnels (Túneles de GRE)** y haga clic en **Add (Añadir)** para añadir un túnel según el valor de **Name (Nombre)**.
2. Seleccione la **interfaz** que se usará como en endpoint de túnel GRE (interfaz de túnel), que es una interfaz o subinterfaz Ethernet, una interfaz Ethernet de agregación (Aggregate Ethernet, AE), una interfaz de bucle invertido o una interfaz VLAN.
3. En **Local Address (Dirección local)**, seleccione la dirección que se debe introducir en **IP** y, luego, seleccione la dirección IP de la interfaz que acaba de seleccionar.
4. En **Peer Address (Dirección de peer)**, introduzca la dirección IP del terminal opuesto del túnel de GRE.
5. En **Tunnel Interface (Interfaz de túnel)**, seleccione la interfaz creada en el paso 1. Este valor identifica el túnel cuando actúa como interfaz de salida del enrutamiento.
6. Introduzca el **TTL** para el paquete IP encapsulado en el paquete GRE (el intervalo es de 1 a 255, el valor predeterminado es 64).
7. Marque **Copy ToS Header (Copiar encabezado de ToS)** para copiar el campo del tipo de servicio (type of service, ToS) del encabezado de la IP interna en el encabezado de la IP externa de los paquetes encapsulados a fin de conservar la información original del ToS.

Seleccione esta opción si la red utiliza la calidad de servicio (quality of service, QoS) y depende de los bits del ToS para aplicar las políticas de QoS.

STEP 3 | (Práctica recomendada) Habilite la función de conexión persistente en el túnel de GRE.

Si habilita la opción de conexión persistente, de manera predeterminada, toma tres paquetes keepalive no devueltos (reintentos) a intervalos de 10 segundos para que el túnel de GRE se desactive y toma cinco intervalos del temporizador de espera a intervalos de 10 segundos para que el túnel de GRE se reactive.

1. Haga clic en **Keep Alive (Conexión permanente)** para habilitar esta función en el túnel de GRE (no está activada de manera predeterminada).
2. (Opcional) En **Interval (sec) (Intervalo [s])**, configure los segundos que deben transcurrir entre los paquetes keepalive (conexión permanente) que envía el extremo local del túnel de GRE a su peer. Al multiplicar este intervalo por el valor de **Hold Timer (Temporizador de espera)**, se obtiene el tiempo durante el que el cortafuegos debe detectar paquetes keepalive (conexión permanente) correctos para que se vuelva a activar el túnel de GRE (el intervalo es de 1 a 50; el valor predeterminado es 10). Si configura un intervalo demasiado breve, pueden aparecer muchos paquetes keepalive (conexión permanente) innecesarios en el entorno, que exigen ancho de banda y procesamiento adicionales. Si configura un intervalo demasiado prolongado, se puede retrasar la conmutación por error porque no se identifican de inmediato las condiciones de error.
3. (Opcional) Introduzca el ajuste **Retry (Reintentar)**, que indica cuántos intervalos sin devolución de paquetes keepalive (conexión permanente) deben pasar para que el cortafuegos considere que el peer del túnel está inactivo (el intervalo es de 1 a 255; el valor predeterminado es 3). Si el túnel está inactivo, el cortafuegos elimina las rutas asociadas de la tabla de reenvío. Configure esta opción para evitar que se tomen medidas en túneles que no están desactivados.
4. (Opcional) En **Hold Timer (Temporizador de espera)**, configure cuántos intervalos con paquetes keepalive (conexión permanente) correctos deben pasar para que el cortafuegos restablezca la comunicación con el peer del túnel (el intervalo es de 1 a 64; el valor predeterminado es 5).

STEP 4 | Haga clic en **OK (Aceptar)**.

STEP 5 | Configure un protocolo de enrutamiento o una ruta estática para enrutar el tráfico al destino por medio del túnel de GRE. Por ejemplo, realice el procedimiento Configuración de una ruta estática para configurar la ruta a la red del servidor de destino y especifique la interfaz de

salida que funciona como endpoint local del túnel (tunnel.1). Configure como siguiente salto la dirección IP del extremo opuesto del túnel. Por ejemplo, 192.168.2.3.

STEP 6 | **Commit (Confirmar)** los cambios.

STEP 7 | Configure el extremo opuesto del túnel con su dirección IP pública, con las direcciones IP local y del peer (que se corresponden, respectivamente, con las direcciones IP del peer y local del túnel de GRE del cortafuegos) y con su protocolo de enrutamiento o ruta estática.

STEP 8 | Verifique que el cortafuegos se comunica con su peer por el túnel de GRE.

1. Acceso a la CLI.
2. > **ping source 192.168.2.1 host 192.168.2.3**

DHCP

En esta sección, se describen el protocolo de configuración de host dinámico (DHCP) y las tareas necesarias para configurar una interfaz en un cortafuegos de Palo Alto Networks® para actuar como servidor, cliente o agente de relé de DHCP. Al asignar esas funciones a distintas interfaces, el cortafuegos puede desempeñar múltiples funciones.

- Descripción general de DHCP
- Cortafuegos como servidor y cliente DHCP
- Mensajes DHCP
- Direccionamiento DHCP
- Opciones de DHCP
- Configure una interfaz como servidor DHCP
- Configure una interfaz como cliente DHCP
- Configuración de la interfaz de gestión como cliente DHCP
- Configure una interfaz como agente de relé DHCP
- Supervisión y resolución de problemas de DHCP

Descripción general de DHCP

DHCP es un protocolo estandarizado definido en RFC 2131, Protocolo de configuración de host dinámico. DHCP tiene dos objetivos principales: Proporcionar los parámetros de configuración de capa de enlace y TCP/IP y proporcionar direcciones de red con hosts configurados dinámicamente en la red TCP/IP.

DHCP usa un modelo cliente-servidor de comunicación. Este modelo consta de tres funciones que puede desempeñar el dispositivo: Cliente DHCP, servidor DHCP y agente de relé DHCP.

- Un dispositivo que funcione como cliente DHCP (host) puede solicitar una dirección IP y otros ajustes de configuración al servidor DHCP. Los usuarios de los dispositivos cliente ahorran el tiempo y esfuerzo de configuración, y no necesitan conocer el plan de direcciones de red y otros recursos y opciones que heredan del servidor DHCP.
- Un dispositivo que actúa como un servidor DHCP puede atender a los clientes. Si se usa alguno de esos tres mecanismos de Direccionamiento DHCP, el administrador de red ahorra tiempo y tiene la ventaja de reutilizar un número limitado de direcciones IP cuando un cliente ya no necesita una conectividad de red. El servidor puede ofrecer direcciones IP y muchas opciones DHCP a muchos clientes.
- Un dispositivo que actúa como un agente de relé DHCP transmite mensajes DHCP entre los clientes y los servidores DHCP.

DHCP usa el protocolo de datagramas de usuario (UDP), RFC 768, como su protocolo de transporte. Los mensajes DHCP que un cliente envía a un servidor se envían al puerto conocido 67 (UDP, protocolo de arranque y DHCP). Mensajes DHCP que un servidor envía a un cliente se envían al puerto 68.

Una interfaz de un cortafuegos de Palo Alto Networks® puede realizar la función de un servidor, un cliente o un agente de relé DHCP. La interfaz de un servidor o agente de relé DHCP debe ser una interfaz VLAN de capa 3, Ethernet agregado o Ethernet de capa 3. Puede configurar las interfaces del cortafuegos con la configuración adecuada para cualquier combinación de funciones. El comportamiento de cada función se resume en Cortafuegos como servidor y cliente DHCP.

El cortafuegos admite el servidor DHCPv4 y el relé DHCPv6.

Las implementaciones de Palo Alto Networks del servidor DHCP y el cliente DHCP solo admiten direcciones IPv4. Su implementación del relé DHCP admite IPv4 e IPv6. El cliente DHCP no es compatible en el modo HA activo/activo.

Cortafuegos como servidor y cliente DHCP

El cortafuegos puede funcionar como servidor DHCP y como cliente DHCP. El protocolo de configuración de host dinámico, Dynamic Host Configuration Protocol, RFC 2131, se ha diseñado para admitir direcciones IPv4 e IPv6. La implementación de Palo Alto Networks® del servidor DHCP solo admite direcciones IPv4.

El servidor DHCP funciona del siguiente modo:

- Cuando el servidor DHCP recibe un mensaje DHCPDISCOVER de un cliente, responde con un mensaje DHCPOFFER que contiene todas las opciones predefinidas y las opciones definidas por el usuario en el orden que aparecen en la configuración. El cliente selecciona las opciones que necesita y responde con un mensaje DHCPREQUEST.
- Cuando el servidor recibe un mensaje DHCPREQUEST de un cliente, el servidor responde con su mensaje DHCPACK, que contiene solo las opciones especificadas en la solicitud.

El cliente DHCP del cortafuegos funciona del siguiente modo:

- Cuando el cliente DHCP recibe una DHCPOFFER del servidor, el cliente automáticamente almacena en caché todas las opciones ofrecidas para futuros usos, independientemente de las opciones que enviara en su DHCPREQUEST.
- De manera predeterminada, y para ocupar menos memoria, el cliente almacena en caché solo el primer valor de cada código de opción si recibe varios valores para un código.
- No hay una longitud máxima para mensajes DHCP a menos que el cliente DHCP especifique un máximo en la opción 57 en sus mensajes DHCPDISCOVER o DHCPREQUEST.

Mensajes DHCP

DHCP usa ocho tipos de mensajes estándar, que se identifican mediante un número de tipo de opción en el mensaje DHCP. Por ejemplo, cuando un cliente quiere encontrar un servidor DHCP, difunde un mensaje DHCPDISCOVER en su subred física local. Si no hay ningún servidor DHCP en su subred y si DHCP auxiliar o un relé DHCP se configura adecuadamente, el mensaje se reenvía a los servidores DHCP en una subred física diferente. De lo contrario, el mensaje no avanzará más allá de la subred en la que se origina. Uno o más servidores DHCP responderán al mensaje DHCPOFFER que contienen una dirección de red disponible y otros parámetros de configuración.

Cuando el cliente necesita una dirección IP, envía un DHCPREQUEST a uno o más servidores. Por supuesto, si el cliente solicita una dirección IP, aún no tiene una, por lo que RFC 2131 requiere que el mensaje de difusión que envía el cliente tenga una dirección de origen de 0 en su encabezado IP.

Cuando un cliente solicita parámetros de configuración desde un servidor, puede recibir respuestas de más de un servidor. Cuando un cliente ha recibido su dirección IP, se dice que el cliente tiene al menos una dirección IP y posiblemente otros parámetros de configuración ***vinculados*** a ella. Los servidores DHCP gestionan esa vinculación de parámetros de configuración con los clientes.

La siguiente tabla enumera los mensajes de DHCP.

Mensaje DHCP	Description (Descripción)
DHCPDISCOVER	El cliente realiza una difusión para buscar los servidores DHCP disponibles.
DHCPOFFER	La respuesta del servidor al DHCPDISCOVER del cliente, ofreciendo parámetros de configuración.
DHCPREQUEST	Mensaje del cliente dirigido a uno o más servidores para hacer algo de lo siguiente: • Solicitar los parámetros a un servidor y rechazar implícitamente ofertas de otros servidores. • Confirmar que una dirección antes asignada es correcta, por ejemplo, un reinicio del sistema. • Extender la concesión de una dirección de red.
DHCPACK	El mensaje de reconocimiento del servidor al cliente, que contiene los parámetros de configuración, incluida una dirección de red confirmada.
DHCPNAK	Reconocimiento negativo del servidor al cliente, que indica que el cliente comprende que la dirección de red es incorrecta (por ejemplo, si el cliente se mueve a una subred nueva) o que la concesión del cliente ha vencido.

Mensaje DHCP	Description (Descripción)
DHCPDECLINE	Mensaje de cliente a servidor que indica que la dirección de red ya se está usando.
DHCPRELEASE	Mensaje de cliente a servidor que da al usuario la dirección de red y cancela el tiempo restante de la concesión.
DHCPINFORM	Mensaje de cliente a servidor que solicita únicamente los parámetros de configuración local; el cliente tiene una dirección de red configurada externamente.

Direccionamiento DHCP

- Métodos de asignación de direcciones DHCP
- Concesiones DHCP

Métodos de asignación de direcciones DHCP

El servidor DHCP asigna o envía una dirección IP a un cliente de tres formas:

- **Ubicación automática**: El servidor DHCP asigna una dirección IP permanente a un cliente desde sus **IP Pools (Grupos de IP)**. En el cortafuegos, una **Lease (Concesión)** que se especifique como **Unlimited (Ilimitada)** significa que la ubicación es permanente.
- **Ubicación dinámica**: El servidor DHCP asigna una dirección IP reutilizable desde **IP Pools (Grupos de IP)** de direcciones a un cliente para un periodo máximo de tiempo, conocido como *Concesión*. Este método de asignación de la dirección es útil cuando el cliente tiene un número limitado de direcciones IP; pueden asignarse a los clientes que necesitan solo un acceso temporal a la red. Consulte la sección DHCP Leases (Concesiones DHCP)
- **Asignación estática**: El administrador de red selecciona la dirección IP para asignarla al cliente y el servidor DHCP se la envía. La asignación DHCP estática es permanente; se realiza configurando un servidor DHCP y seleccionando una **Reserved Address (Dirección reservada)** para que corresponda con la **MAC Address (Dirección MAC)** del dispositivo cliente. La asignación DHCP continúa en su lugar aunque el cliente cierre sesión, reinicie, sufra un corte de alimentación, etc.

  La asignación estática de una dirección IP es útil, por ejemplo, si tiene una impresora en una LAN y no desea que su dirección IP siga cambiando porque se asocia con un nombre de impresora a través de DNS. Otro ejemplo es si el dispositivo cliente se usa para una función crucial y debe mantener la misma dirección IP aunque el dispositivo se apague, desconecte, reinicie o sufra un corte de alimentación, etc.

  Tenga lo siguiente en cuenta cuando configure una **Reserved Address (Dirección reservada)**:

  - Es una dirección de **IP Pools (Grupos de IP)**. Puede configurar múltiples direcciones reservadas.
  - Si no configura ninguna **Reserved Address (Dirección reservada)**, los clientes del servidor recibirán nuevas asignaciones de DHCP del grupo cuando sus concesiones venzan o si se reinician, etc. (a no ser que haya especificado que una **Lease (Concesión)** sea **Unlimited (Ilimitada)**).
  - Si asigna todas las direcciones de **IP Pools (Grupos IP)** como una **Reserved Address (Dirección reservada)**, no hay direcciones dinámicas libres para asignar al siguiente cliente DHCP que solicite una dirección.
  - Puede configurar una **Dirección reservada (Dirección reservada)** sin configurar una **Dirección MAC (Dirección MAC)**. En este caso, el servidor DHCP no asignará la **Reserved Address (Dirección reservada)** a ningún dispositivo. Puede reservar unas direcciones del grupo y asignarlas estáticamente a un fax e impresora, por ejemplo, sin usar DHCP.

Concesiones DHCP

Una concesión se define como la duración durante la que el servidor DHCP asigna a una dirección IP para un cliente. La concesión puede extenderse (renovarse) en las solicitudes posteriores. Si el cliente ya no necesita la dirección, puede liberarla en el servidor antes de que la concesión termine. El servidor es entonces libre de asignar esa dirección a un cliente distinto, si ya se le han agotado las direcciones sin asignar.

El periodo de concesión configurado para un servidor DHCP se aplica a todas las direcciones que un servidor DHCP único (interfaz) asigna dinámicamente a sus clientes. Es decir, todas las direcciones de interfaz asignadas dinámicamente tienen una duración **Ilimitada** o el mismo valor de **Tiempo de espera**. Un servidor DHCP diferente configurado en el cortafuegos puede tener un plazo de concesión distinto para sus clientes. Una **Reserved Address (Dirección reservada)** es una asignación de dirección estática y no está sometida a esas condiciones de concesión.

Según el estándar DHCP, RFC 2131, un cliente DHCP no espera a que la concesión venza, ya que se arriesga a que se le asigne una nueva dirección. En su lugar, cuando un cliente DHCP alcanza el punto medio de su periodo de concesión, intenta extenderla para conservar la misma dirección IP. Así, la duración de la concesión es como una ventana corredera.

Por lo general, si se ha asignado una dirección IP a un dispositivo, y este se saca de la red sin prolongar su concesión, el servidor DHCP dejará que esa concesión se agote. Como el cliente ha salido de la red y ya no necesita la dirección, se alcanza la duración de la concesión del servidor y la concesión pasa al estado “Expirado”.

El cortafuegos tiene un temporizador de espera que evita que la dirección IP expirada se reasigne inmediatamente. Este sistema reserva temporalmente la dirección para el dispositivo en caso de que vuelva a la red. Pero si el grupo de direcciones se queda sin direcciones, el servidor reubicará esta dirección expirada antes de que se termine el temporizador de espera. Las direcciones expiradas se borran automáticamente a medida que los sistemas necesitan más direcciones o cuando el temporizador de espera las libera.

En la CLI, use el comando operativo **`show dhcp server lease`** para ver la información de concesión de las direcciones IP asignadas. Si no desea esperar a que las concesiones vencidas se liberen automáticamente, puede utilizar el comando **`clear dhcp lease interface <interface> expired-only`** para borrar las concesiones vencidas y permitir que vuelvan a estar disponibles en el grupo. Puede utilizar el comando **`clear dhcp lease interface <interface> ip <ip_address>`** para liberar una dirección IP concreta. Puede utilizar el comando **`clear dhcp lease interface <interface> mac <mac_address>`** para liberar una dirección MAC concreta.

Opciones de DHCP

La historia del DHCP y sus opciones DHCP se remonta al protocolo de arranque (BOOTP). Un host usó BOOTP para configurarse dinámicamente durante su procedimiento de arranque. El host recibía una dirección IP y un archivo desde el que descargaba un programa de arranque desde un servidor, junto con la dirección del servidor y la dirección de la gateway de Internet.

En el BOOTP incluía un campo de información del proveedor, que contenía un número de campos etiquetados con distintos tipos de información como la máscara de subred, el tamaño del archivo BOOTP y muchos otros valores. RFC 1497 describe las extensiones de información de proveedor BOOTP. El DHCP sustituye a BOOTP; no se admite BOOTP en el cortafuegos.

Estas extensiones llegan a expandirse con el uso de los parámetros de configuración de host DHCP y DHCP, conocidos como opciones. Al igual que las extensiones de proveedor, las opciones de DHCP son elementos de datos etiquetados que proporcionan información a un cliente DHCP. La opciones se envían en un campo de longitud variable al final de un mensaje DHCP. Por ejemplo, el tipo de mensaje DHCP es la opción 53, y un valor de 1 indica un mensaje DHCPDISCOVER. Las opciones DHCP se definen en RFC 2132, Opciones DHCP y extensiones de proveedores de BOOTP.

Un cliente DHCP puede negociar con el servidor, limitándolo a enviar solo esas opciones que solicita el cliente.

- Opciones de DHCP predefinidas
- Múltiples valores para una opción de DHCP
- Opciones de DHCP 43, 55 y 60 y otras opciones personalizadas

Opciones de DHCP predefinidas

Los cortafuegos de Palo Alto Networks® admiten opciones de DHCP predefinidas y definidas por los usuarios en la implementación del servidor DHCP. Dichas opciones se configuran en el servidor DHCP y se envían a los clientes que envían una DHCPREQUEST al servidor. Se dice que los clientes ***heredan*** e implementan las opciones que están programados para aceptar.

El cortafuegos admite las siguientes opciones predefinidas en sus servidores DHCP, que se muestran en el orden en que aparecen en la pantalla de configuración del **servidor DHCP**:

Opción de DHCP	Nombre de opción de DHCP
51	Duración de la concesión
3	Gateway
1	Subred de grupo de IP (máscara)
6	Dirección de servidor del sistema de nombres de dominio (DNS:) (principal y secundaria)

Opción de DHCP	Nombre de opción de DHCP
44	Dirección de servidor del Servicio de nombres Internet de Windows (WINS) (primaria y secundaria)
41	Dirección de servidor del Servicio de información de la red (NIS) (primaria y secundaria)
42	Dirección de servidor del protocolo de tiempo de redes(NTP) (primaria y secundaria)
70	Dirección de servidor del Protocolo de oficina de correo Versión 3 (POP3)
69	Dirección de servidor del Protocolo simple de transferencia de correo (SMTP)
15	Sufijos DNS

Como se menciona, también puede configurar opciones específicas del proveedor y personalizadas, compatibles con una gran variedad de equipos de oficina, tales como teléfonos IP y dispositivos de infraestructura inalámbrica. Cada código de opción admite múltiples valores, que pueden ser direcciones IP o formato hexadecimal ASCII. Gracias a la compatibilidad con la opción de DCHP mejorada, las sucursales no necesitan comprar y gestionar sus propios servidores de DHCP para ofrecer opciones personalizadas y específicas de proveedores a los clientes de DHCP.

Múltiples valores para una opción de DHCP

Puede introducir varios valores de opciones para un **Option Code** con el mismo **Option Name**, pero todos los valores para un código particular y una combinación de nombre deben ser del mismo tipo (dirección IP, ASCII o hexadecimal). Si se hereda o introduce un tipo, y después se introduce un segundo tipo para la misma combinación de código y nombre, el segundo tipo sobrescribirá el primero.

Puede introducir un **Option Code** más de una vez usando un **Option Name** diferente. En este caso, el **Option Type** del Código de opción puede variar entre los múltiples nombres de opción. Por ejemplo, si la opción Coastal Server (código de opción 6) está configurada con el tipo de dirección IP, también se admite la opción Server XYZ (código de opción 6) con ASCII.

El cortafuegos envía múltiples valores para una opción (vinculados) a un cliente en orden descendente (de arriba abajo). Por lo tanto, al introducir múltiples valores para una opción, introduzca los valores en el orden de preferencia, o si no, mueva las opciones para establecer el orden que prefiera en la lista. El orden de las opciones en la configuración del cortafuegos determina el orden en que aparecen las opciones en los mensajes DHCPOFFER y DHCPACK.

Puede introducir un código de opción que ya existe como código de opción predefinida, y el código de opción personalizado sobrescribirá la opción de DHCP predefinida; el cortafuegos emitirá una advertencia.

Opciones de DHCP 43, 55 y 60 y otras opciones personalizadas

La siguiente tabla describe el comportamiento de las opciones para varias opciones descritas en RFC 2132.

Código de opción	Nombre de opción	Descripción/Comportamiento de la opción
43	Información específica del proveedor	Enviada desde el servidor al cliente. Información específica del proveedor que el servidor de DHCP ha configurado para ofrecerla al cliente. La información se envía al cliente solo si el servidor tiene un Identificador de clase de proveedor (VCI) en la tabla que coincide con el VCO en la DHCPREQUEST del cliente. Un paquete de opción 43 puede contener múltiples informaciones específicas del proveedor. También puede incluir extensiones de datos encapsuladas específicas del proveedor.
55	Lista de requisitos de parámetros	Enviado desde el cliente al servidor. Lista de parámetros de configuración (códigos de opción) que está solicitando un cliente DHCP, probablemente en el orden de preferencia del cliente. El servidor intenta responder con opciones en el mismo orden.
60	Identificador de clase de proveedor (VCI)	Enviado desde el cliente al servidor. Configuración y tipo de proveedor de un cliente DHCP. El cliente DHCP envía un código de opción 60 en una DHCPREQUEST al servidor de DHCP. Cuando el servidor recibe la opción 60, ve el VCI, busca el VCI correspondiente en su propia tabla y regresa con una opción 43 con el valor (que se corresponde con el VCI), por lo tanto, retransmitiendo información específica del proveedor al cliente correcto. Tanto el cliente como el servidor tienen conocimiento del VCI.

Puede enviar códigos específicos del proveedor personalizados que no están definidos en RFC 2132. Estos códigos de opción pueden estar dentro del intervalo 1-254 y tener una longitud fija o variable.

El servidor DHCP no valida las opciones de DHCP personalizadas; debe asegurarse de introducir los valores correctos para las opciones que cree.

Para tipos de opciones ASCII DHCP hexadecimal, el valor de opción puede ser de 255 octetos como máximo.

Configure una interfaz como servidor DHCP

Los requisitos previos de esta tarea son:

- Configure una interfaz Ethernet de capa 3 o VLAN de capa 3.
- Asigne la interfaz a un enrutador virtual y a una zona.
- Determine un grupo válido de direcciones IP de su plan de red que pueda designar para que su servidor DHCP las asigne a los clientes.
- Recopile los valores, identificadores de clase de proveedor y opciones de DHCP que tiene previsto configurar.

Estas son las funciones:

- Para ver modelos de cortafuegos distintos de PA-5200 Series y PA-7000 Series, consulte la Herramienta de selección de productos.
- En los cortafuegos PA-5220, puede configurar un máximo de 500 servidores DHCP y un máximo de 2048 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 1548 agentes de transmisión DHCP.
- En los cortafuegos PA-5250, PA-5260 y PA-7000 Series, puede configurar un máximo de 500 servidores DHCP y un máximo de 4096 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 3596 agentes de transmisión DHCP.

Realice la siguiente tarea para configurar una interfaz en el cortafuegos para que actúe como servidor DHCP.

STEP 1 | Seleccione una interfaz para que sea un servidor DHCP.

1. Seleccione **Network (Red)** > **DHCP** > **DHCP Server (Servidor DHCP)** y, luego, haga clic en **Add (Añadir)** para añadir o seleccionar el nombre de la interfaz en **Interface (Interfaz)**.
2. En **Mode (Modo)**, seleccione **enabled (habilitado)** o modo **auto (automático)**. El modo automático habilita el servidor y lo deshabilita si se detecta otro servidor DHCP en la red. El ajuste **disabled (deshabilitar)** desactiva el servidor.
3. (Opcional) Seleccione **Ping IP when allocating new IP (Hacer ping a la IP al asignar IP nuevas)** si desea que el servidor haga ping a la dirección IP antes de asignarla a su cliente.

   Si el ping recibe una respuesta, significará que ya hay un dispositivo diferente con esa dirección, por lo que no está disponible para su asignación. El servidor asigna la siguiente dirección desde el grupo. Este comportamiento es similar a Duplicar detección de dirección (DAD) para IPv6, RFC 4429*.*

   *Tras definir las opciones y volver a la pestaña del servidor DHCP, la columna **Probe IP** de la interfaz indicará si **Ping IP when allocating new IP** estaba seleccionada.*

STEP 2 | Configure las Opciones DHCP predefinidas que el servidor envía a sus clientes.

- En la sección Opciones, seleccione un tipo de **Concesión**.
- **Unlimited (Ilimitada)** provoca que el servidor seleccione dinámicamente direcciones IP desde los Grupos IP y los asigne de forma permanente a los clientes.
- **Timeout (Tiempo de espera)** determina cuánto durará esa concesión. Introduzca el número de **Días** y **Horas** y, opcionalmente, el número de **Minutos**.
- **Origen de herencia**: Deje **Ninguno** o seleccione una interfaz de cliente DHCP de origen o una interfaz de cliente PPPoE para propagar distintos ajustes de servidor en el servidor de DHCP. Si especifica un **Inheritance Source (Origen de herencia)**, seleccione una o varias opciones que desee como **inherited (heredadas)** desde este origen.

Especificar un origen de herencia permite al cortafuegos añadir rápidamente opciones de DHCP desde el servidor previo recibidas por el cliente DHCP. También mantiene actualizadas las opciones de cliente si el origen cambia una opción. Por ejemplo, si el origen sustituye a su servidor NTP (que se ha identificado como el servidor **NTP principal**), el cliente heredará automáticamente la nueva dirección como su nuevo servidor **NTP principal**.

Al heredar opciones de DHCP que contienen múltiples direcciones IP, el cortafuegos usa solo la primera dirección IP contenida en la opción para ocupar menos memoria caché. Si necesita múltiples direcciones IP para una única opción, configure las opciones DHCP directamente en el cortafuegos en lugar de configurar la herencia.

- **Check inheritance source status (Verificar estado del origen de herencia)**: si ha seleccionado **Inheritance Source (Origen de herencia)**, al hacer clic en este enlace se abrirá la ventana **Dynamic IP Interface Status (Estado de interfaz de IP dinámica)**, que muestra las opciones que se han heredado del cliente DHCP.
- **Gateway (Puerta de enlace)**: la dirección IP de la puerta de enlace de la red (una interfaz en el cortafuegos) que se usa para llegar a cualquier dispositivo que no esté en la misma LAN que este servidor DHCP.
- **Subnet Mask**: máscara de red con las direcciones del campo **IP Pools**.

En los siguientes campos, haga clic en la flecha hacia abajo y seleccione **None (Ninguno)** o **inherited (heredado)**, o introduzca una dirección IP de servidor remoto que su servidor DHCP enviará a los clientes para acceder a ese servicio. Si ha seleccionado **inherited (heredado)**,

el servidor DHCP hereda los valores desde el cliente DHCP de origen, especificado como **Inheritance Source (Origen de herencia)**.

- **Primary DNS (DNS primario)**, **Secondary DNS (DNS secundario)**: dirección IP de los servidores del sistema de nombres de dominio (DNS) preferidos y alternativos.
- **Primary WINS (WINS primario)**, **Secondary WINS (WINS secundario)**: dirección IP de los servidores Windows Internet Naming Service (WINS) preferidos y alternativos.
- **Primary NIS (NIS primario)**, **Secondary NIS (NIS secundario)**: introduzca la dirección IP de los servidores del Servicio de información de la red (NIS) preferidos y alternativos.
- **Primary NTP (NTP primario)**, **Secondary NTP (NTP secundario)**: dirección IP de los servidores del protocolo de tiempo de redes disponibles.
- **POP3 Server (Servidor POP3)**: dirección IP del servidor Post Office Protocol (POP3).
- **SMTP Server**: introduzca la dirección IP del servidor del protocolo simple de transferencia de correo (Simple Mail Transfer Protocol, SMTP).
- **DNS Suffix (Sufijo DNS)**: sufijo para que el cliente lo use localmente cuando se introduce un nombre de host sin cualificar que no puede resolverse.

STEP 3 | (Opcional) Configure una opción DHCP personalizada o específica del proveedor que el servidor DHCP enviará a los clientes.

1. En la sección opciones de DHCP personalizadas, haga clic en **Add (Añadir)** e introduzca un nombre descriptivo en **Name (Nombre)** para identificar la opción DHCP.
2. Introduzca el **Option Code (Código de opción)** que desea configurar para ofrezca el servidor (el intervalo es 1-254). (Consulte RFC 2132 para conocer códigos de opción).
3. Si el **Option Code** es **43**, aparecerá el campo **Vendor Class Identifier**. Introduzca un VCI, que es una cadena o valor hexadecimal (con prefijo 0x) usado como coincidencia frente a un valor procedente de la solicitud del cliente que contiene una opción 60. El servidor busca el VCI entrante en esta tabla, lo encuentra, y devuelve la opción 43 y el valor de opción correspondiente.
4. **Inherit from DHCP server inheritance source (Heredar del origen de herencia del servidor DHCP)**: seleccione esta opción si ha especificado un **Inheritance Source (Origen de herencia)** para las opciones predeterminadas del servidor DHCP y desea **heredar** también de este origen.
5. **Check inheritance source status (Verificar estado del origen de herencia)**: si ha seleccionado **Inheritance Source (Origen de herencia)**, al hacer clic en este enlace se abrirá la ventana **Dynamic IP Interface Status (Estado de interfaz de IP dinámica)**, que muestra las opciones que se han heredado del cliente DHCP.
6. Si no ha seleccionado la casilla de verificación **Inherit from DHCP server inheritance source**, seleccione un **Option Type**: **IP Address**, **ASCII** o **Hexadecimal**. Los valores hexadecimales deben empezar por el prefijo 0x.
7. Introduzca el **Option Value (Valor de opción)** que el servidor DHCP debe ofrecer para ese **Option Code (Código de opción)**. Puede introducir múltiples valores en líneas separadas.
8. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Añada otra opción DHCP personalizada o específica del proveedor.

1. Repita el paso anterior para introducir otra opción DHCP personalizada.
   - Puede introducir múltiples valores de opciones para un **Option Code** con el mismo **Option Name**, pero todos los valores para un **Option Code** deben ser del mismo tipo (**IP Address**, **ASCII** o **Hexadecimal**). Si se hereda o introduce un tipo y se introduce un segundo tipo para el mismo **Option Code** y **Option Name**, el segundo tipo sobrescribirá al primero.

     Al introducir múltiples valores para una opción, introduzca los valores en el orden de preferencia, o si no, mueva las opciones de DHCP personalizadas para establecer el orden que prefiera en la lista. Seleccione una opción y haga clic en **Move Up (Mover arriba)** o **Move Down (Mover abajo)**.
   - Puede introducir un **Option Code** más de una vez usando un **Option Name** diferente. En este caso, el **Option Type** del Código de opción puede variar entre los múltiples nombres de opción.
2. Haga clic en **OK (Aceptar)**.

STEP 5 | Identifique el grupo de direcciones IP de estado desde el que el servidor DHCP selecciona una dirección y la asigna a un cliente DHCP.

Si no es el administrador de su red, pídale a él un grupo válido de direcciones IP de su plan de red que puede designarse para que su servidor DHCP lo asigne.

1. En el campo **IP pools (Grupos IP)**, haga clic en **Add (Añadir)** e introduzca el intervalo de direcciones IP desde el cual este servidor asigna una dirección a un cliente. Introduzca una subred IP y una máscara de subred (por ejemplo, 192.168.1.0/24) o un intervalo de direcciones IP (por ejemplo, 192.168.1.10-192.168.1.20).
   - El grupo de IP o la **dirección reservada** son obligatorios para la asignación de dirección IP dinámica.
   - El grupo IP es opcional para la asignación de dirección IP, siempre y cuando las direcciones IP estáticas que asigne vayan a la subred que asiste la interfaz del cortafuegos.
2. (Opcional) Repita este paso para especificar otro grupo de direcciones IP.

STEP 6 | (Opcional) Especifique una dirección IP de los grupos IP que no se asignarán dinámicamente. Si especifica también una **Dirección MAC**, la **Dirección reservada** se asigna a ese dispositivo cuando el dispositivo solicita una dirección IP a través de DHCP.

Consulte la sección DHCP Addressing (Direccionamiento DHCP) *si desea una explicación de la asignación de una* ***Reserved Address (Dirección reservada).***

1. En el campo **Reserved Address (Dirección reservada)**, haga clic en **Add (Añadir)**.
2. Introduzca una dirección IP desde **Grupos IP** (formato *x.x.x.x*) que no desea que se asigne dinámicamente al servidor DHCP.
3. (Opcional) Especifique la **MAC Adress (Dirección MAC)** (formato *xx:xx:xx:xx:xx:xx*) del dispositivo al que desea asignar de forma permanente la dirección IP que acaba de especificar.
4. (Opcional) Repita los dos pasos anteriores para reservar otra dirección.

STEP 7 | Confirme los cambios.

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

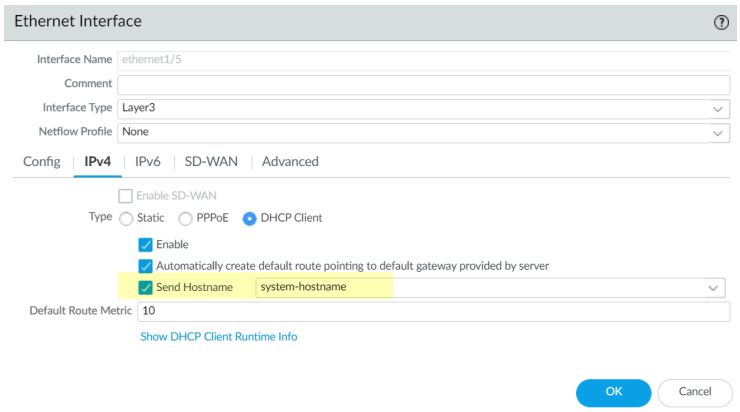
Configure una interfaz como cliente DHCP

Antes de configurar una interfaz de cortafuegos como cliente DHCP, tiene que haber configurado una interfaz de capa 3 (Ethernet, subinterfaz de Ethernet, VLAN, subinterfaz de VLAN, agregación o subinterfaz de agregación) y haberla asignado a una zona y a un enrutador virtual. Configure una interfaz como cliente DHCP si necesita usar DHCP para solicitar una dirección IPv4 para la interfaz.

También puede realizar la Configuración de la interfaz de gestión como cliente DHCP.

STEP 1 | Configure una interfaz como cliente DHCP.

1. Seleccone **Network (Red)** > **Interfaces**.
2. En las pestañas **Ethernet** o **VLAN**, **añada** una interfaz de capa 3 o seleccione una ya configurada que quiera que sea cliente DHCP.
3. Seleccione la pestaña **IPv4** y ,en **Type (Tipo)**, seleccione **DHCP Client (Cliente DHCP)**.
4. Seleccione **Enabled (Habilitado)**.
5. (Opcional) Habilite la opción para **crear una ruta predeterminada automáticamente que apunte a la puerta de enlace predeterminada proporcionada por el servidor** habilitada de forma predeterminada. Si activa esta opción, el cortafuegos creará una ruta estática a una puerta de enlace predeterminada que será útil cuando los clientes intenten acceder a muchos destinos que no necesitan mantener rutas en una tabla de enrutamiento en el cortafuegos.
6. (Opcional) Habilite la opción**Send Hostname (Enviar nombre de host)** para asignar un nombre de host a la interfaz del cliente DHCP y enviar dicho nombre (opción 12) a un servidor DHCP. Este lo registra en el servidor DNS, que puede gestionar automáticamente la resolución de nombres de host en direcciones IP dinámicas. Los hosts externos pueden identificar la interfaz por su nombre de host. El valor predeterminado es **system-hostname (nombre-host-sistema)**, que se corresponde con el nombre de host del cortafuegos definido en **Device (Dispositivo)** > **Setup (Configuración)** > **General Settings (Configuración general)**. Si lo prefiere, introduzca un nombre de host para la interfaz con 64 caracteres como máximo, que pueden incluir letras mayúsculas y minúsculas, números, puntos (.), guiones (-) y guiones bajos (_).



7. (Opcional) Introduzca una **Default Route Metric** (nivel de prioridad) para la ruta entre el cortafuegos y el servidor DHCP (el intervalo es de 1 a 65 535; el valor predeterminado

es 10). Un ruta con un número más bajo tiene una prioridad alta durante la selección de la ruta. Por ejemplo, una ruta con una métrica de 10 se usa antes que una ruta con una métrica de 100.

*La **métrica de ruta predeterminada** para la ruta entre el cortafuegos y el servidor DHCP es 10 de forma predeterminada. Si la ruta estática predeterminada 0.0.0.0/0 utiliza la interfaz DHCP como su interfaz de salida, la **métrica** predeterminada de esa ruta es también 10. Por lo tanto, hay dos rutas con una métrica de 10 y el cortafuegos puede elegir aleatoriamente una de las rutas una vez y la otra ruta en otro momento.*

*Suponga que habilita la opción para **crear automáticamente una ruta predeterminada que apunte a la puerta de enlace predeterminada proporcionada por el servidor**, selecciona un enrutador virtual, añade una ruta estática para la interfaz de capa 3, cambia la **métrica** (cuyo valor predeterminado es 10) a un valor superior a 10 (en este ejemplo, 100) y confirma los cambios. En la tabla de rutas, la métrica de la ruta no indicará 100. En su lugar, indicará el valor predeterminado de 10, como se esperaba, porque 10 tiene prioridad sobre el valor configurado de 100. Sin embargo, si cambia la **métrica** de la ruta estática a un valor inferior a 10 (como 6), se actualizará la ruta de la tabla de rutas para indicar la métrica configurada de 6.*

8. (Opcional) Habilite la opción **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)** para ver todos los ajustes que el cliente ha heredado del servidor DHCP.

STEP 2 | Confirme los cambios.

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

La interfaz Ethernet debe ahora indicar **Dynamic-DHCP Client (Cliente DHCP dinámico)** como **dirección IP** en la pestaña **Ethernet**.

STEP 3 | (Opcional) Vea qué interfaces del cortafuegos se han configurado como clientes DHCP.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y compruebe **IP Address (Dirección IP)** para verificar las interfaces que se indican como cliente DHCP.
2. Seleccione **Network (Red)** > **Interfaces** > **VLAN** y observe el campo **IP Address (Dirección IP)** para verificar las interfaces que se indican como cliente DHCP.

Configuración de la interfaz de gestión como cliente DHCP

La interfaz de gestión en el cortafuegos admite el cliente DHCP para IPv4 que permite que la interfaz de gestión reciba su dirección IPv4 de un servidor DHCP. La interfaz de gestión también admite la opción 12 y la opción 61 de DHCP, que permite que el cortafuegos envíe su nombre de host e identificador de cliente, respectivamente, a los servidores DHCP.

Por defecto, los cortafuegos de la serie VM implementados en AWS y Azure™ usan la interfaz de gestión como cliente DHCP para obtener su dirección IP, en lugar de una dirección IP estática, debido a que las implementaciones en la nube requieren la automatización que ofrece esta característica. DHCP en la interfaz de gestión está desactivada por defecto para el cortafuegos de la serie VM, excepto para el cortafuegos de la serie VM en AWS y Azure. Las interfaces de gestión en los modelos de WildFire y Panorama no admiten esta funcionalidad DHCP.

- *Para los modelos de cortafuegos basados en hardware (no la serie de VM), configure la interfaz de gestión con una dirección IP estática cuando fuera posible.*
- *Si el cortafuegos adquiere una dirección de interfaz de gestión a través de DHCP, asigne una reserva de dirección MAC en el servidor DHCP que se encarga de ese cortafuegos. La reserva garantiza que el cortafuegos conserve su dirección IP de gestión después de un reinicio. Si el servidor DHCP es un cortafuegos de Palo Alto Networks®, consulte el paso 6 de* Configuración de una interfaz como servidor DHCP *para reservar una dirección.*

Si configura la interfaz de gestión como un cliente DHCP, se aplican las siguientes restricciones:

- No puede usar la interfaz de gestión en una configuración HA para el enlace de control (copia de seguridad de HA1 o HA1), enlace de datos (copia de seguridad de HA2 o HA2 o la comunicación de reenvío de paquete (HA3).
- No puede seleccionar **MGT** como la interfaz de origen al personalizar las rutas de servicio (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Service Route Configuration [Configuración de ruta de servicio]** > **Customize [Personalizar]**). Sin embargo, puede seleccionar **Use default (Usar predeterminado)** para enrutar los paquetes a través de la interfaz de gestión.
- No puede usar la dirección IP dinámica de la interfaz de gestión para conectarse con un módulo de seguridad de hardware (Hardware Security Module, HSM). La dirección IP en el cortafuegos del cliente HSM debe ser una dirección IP estática debido a que HSM autentica el cortafuegos usando la dirección IP y las operaciones en HSM dejarían de funcionar si la dirección IP cambiara durante el tiempo de ejecución.

Un requisito previo para esta tarea es que la interfaz de gestión debe ser capaz de conectarse a un servidor DHCP.

STEP 1 | Configure la interfaz de gestión como cliente DHCP ara que pueda recibir su dirección IP (IPv4), máscara de red (IPv4) y puerta de enlace por defecto de un servidor DHCP.

O bien, también puede enviar el nombre de host e identificador de cliente de la interfaz de gestión al servidor DHCP si el sistema de orquestación que utiliza acepta esta información.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de interfaz de gestión.
2. Para **IP Type (Tipo de IP)**, seleccione **DHCP Client (Cliente DHCP)**.
3. (Opcional) Seleccione una de las opciones, o ambas, para que el cortafuegos envíe al servidor DHCP en los mensajes de detección o solicitud de DHCP:
   - **Send Hostname (Enviar nombre de host)**: envía el **Hostname (Nombre de host)** (como se definió en **Device [Dispositivo]** > **Setup [Configuración]** > **Management [Gestión]**) como parte de la opción 12 de DHCP.
   - **Send Client ID**: envía su identificador de cliente como parte de la opción 61 de DHCP. Un identificador de cliente identifica de manera única un cliente DHCP, y el servidor DHCP lo utiliza para indexar su base de datos de parámetro de configuración.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Configure el cortafuegos para que acepte el nombre de host y dominio del servidor DHCP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes generales.
2. Seleccione una opción o ambas:
   - **Accept DHCP server provided Hostname**: permite que el cortafuegos acepte el nombre de host del servidor DHCP (si es válido). Cuando está habilitada, el nombre de host del servidor DHCP sobrescribe cualquier Hostname (Nombre de host) existente especificado en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)**. No seleccione esta opción si desea configurar manualmente un nombre de host.
   - **Accept DHCP server provided Domain**: permite que el cortafuegos acepte el dominio del servidor DHCP. El dominio (sufijo DNS) del servidor DHCP sobrescribe cualquier **dominio** existente especificado en **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión).** No seleccione esta opción si desea configurar manualmente un dominio.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

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

STEP 4 | Visualice información del cliente DHCP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y Management Interface Settings (Ajustes de la interfaz de gestión).
2. Haga clic en **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)**.

STEP 5 | (Opcional) Renueve la DHCP lease (Concesión DHCP) con el servidor DHCP, independientemente del plazo de concesión.

Esta opción es práctica si está comprobando o resolviendo problemas de red.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes de interfaz de gestión.
2. Haga clic en **Show DHCP Client Runtime Info (Mostrar información de tiempo de ejecución de cliente DHCP)**.
3. Haga clic en **Renew**.

STEP 6 | (Opcional) Libere las siguientes opciones de DHCP provenientes del servidor DHCP:

- Dirección IP
- Máscara de red
- Gateway predeterminada
- Servidor DNS (primario y secundario)
- Servidor NTP (primario y secundario)
- Dominio (sufijo DNS)

Una liberación desbloquea la dirección IP, que desactiva la conexión de su red y hace que el cortafuegos no pueda gestionarse si no hay otra interfaz configurada para el acceso de gestión.

Use el comando operativo de CLI **`request dhcp client management-interface release`**.

Configure una interfaz como agente de relé DHCP

Para habilitar una interfaz de cortafuegos para que transmita mensajes DHCP entre clientes y servidores, debe configurar el cortafuegos como agente de transmisión DHCP. La interfaz puede reenviar mensajes a un máximo de ocho servidores DHCP IPv4 externos y ocho servidores DHCP IPv6 externos. Un mensaje de DHCPDISCOVER del cliente se envía a todos los servidores configurados, y el mensaje DHCPOFFER del primer servidor que responde se retransmite al cliente que originó la petición.

Estas son las funciones:

- Puede configurar un número total combinado de 500 servidores DHCP (IPv4) y agentes de retransmisión DHCP (IPv4 y IPv6) en todos los modelos de cortafuegos, excepto los cortafuegos PA-5200 Series y PA-7000 Series.
- En los cortafuegos PA-5220, puede configurar un máximo de 500 servidores DHCP y un máximo de 2048 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 1548 agentes de transmisión DHCP.
- En los cortafuegos PA-5250, PA-5260 y PA-7000 Series, puede configurar un máximo de 500 servidores DHCP y un máximo de 4096 agentes de retransmisión DHCP, menos el número de servidores DHCP configurados. Por ejemplo, si configura 500 servidores DHCP, puede configurar 3596 agentes de transmisión DHCP.

Antes de configurar un agente de retransmisión DHCP, asegúrese de que ha configurado una interfaz Ethernet de capa 3 o VLAN de capa 3, y de que la interfaz se ha asignado a una zona y un enrutador virtual.

STEP 1 | Seleccione Retransmisión DHCP.

Seleccione **Network (Red)** > **DHCP** > **DHCP Relay (Transmisión DHCP)**.

STEP 2 | Especifique la dirección IP del servidor DHCP con el que se comunicará el agente del relé DHCP.

1. En el campo **Interface (Interfaz)**, seleccione la interfaz que debe funcionar como agente de retransmisión DHCP.
2. Seleccione **IPv4** o **IPv6**, lo que indica el tipo de dirección del servidor DHCP que va a especificar.
3. Si seleccionó **IPv4**, en el campo **DHCP Server IP Address (Dirección IP del servidor DHCP)**, haga clic en **Add (Añadir)** e introduzca la dirección del servidor DHCP de origen y destino para la transmisión de mensajes DHCP.
4. Si seleccionó **IPv6**, en el campo **DHCP Server IPv6 Address (Dirección IPv6 del servidor DHCP)**, haga clic en **Add (Añadir)** e introduzca la dirección del servidor DHCP de origen y destino para la transmisión de mensajes DHCP. Si especifica una dirección ***multidifusión***, especifique también una **Interfaz** saliente.
5. (Opcional) Repita los tres pasos anteriores para introducir un máximo de ocho direcciones de servidor DHCP por cada familia de dirección IP.

STEP 3 | Confirme la configuración.

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

Supervisión y resolución de problemas de DHCP

Puede visualizar el estado de las concesiones de dirección dinámica que su servidor DHCP ha asignado o que se han asignado a su cliente DHCP al emitir comandos desde la CLI. También puede eliminar concesiones antes de que caduquen y se liberen automáticamente.

- Ver información de servidor DHCP principal
- Borrado de concesiones DHCP
- Ver información de cliente DHCP
- Recopilación de resultados de depuración sobre DHCP

Ver información de servidor DHCP principal

Realice esta tarea para ver las estadísticas del grupo DHCP, las direcciones IP que ha asignado el servidor DHCP, la dirección MAC correspondiente, el estado y la duración de la concesión, y la hora de inicio de la concesión. Si la dirección se ha configurado como **Reserved Address (Dirección reservada)**, la columna `state (estado)` indica `reserved (reservado)` y no se indican `duration (duración)` ni `lease_time (tiempo de concesión)`. Si la concesión se configuró como **Unlimited (Ilimitada)**, la columna `duration (duración)` se mostrará con un valor de `0`.

- Vea las estadísticas de grupo DHCP, la dirección IP que ha asignado el servidor DHCP, la dirección MAC, el estado y la duración de la concesión, y la hora de inicio de la concesión.

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip              mac                state      duration
 lease_time
192.168.3.11    f0:2f:af:42:70:cf  committed  0           Wed Jul
 2 08:10:56 2014
admin@PA-220>
```

- Vea las opciones que un servidor DHCP ha asignado a los clientes.

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit
 source
------------------------------------------------------------------------------
ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10
             ethernet1/3
admin@PA-220>
```


Borrado de concesiones DHCP

Cuenta con varias opciones para borrar las concesiones DHCP.

- Libere las concesiones DHCP vencidas de una interfaz (servidor), como ethernet1/2, antes de que el temporizador de espera las libere automáticamente. Estas direcciones volverán a estar disponibles en el grupo IP.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

- Libere una concesión de una dirección IP particular, por ejemplo, 192.168.3.1.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

- Libere una concesión de una dirección MAC particular, por ejemplo, f0:2c:ae:29:71:34.

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac
 f0:2c:ae:29:71:34
```

Ver información de cliente DHCP

Para visualizar el estado de las concesiones de dirección IP enviadas al cortafuegos cuando actúa como cliente DHCP, utilice cualquiera de estos comandos de la CLI.

- admin@PA-220>**show dhcp client state <*interface_name*>**
- admin@PA-220> **show dhcp client state all**

```
Interface       State        IP               Gateway
 Leased-until
--------------------------------------------------------------------------------
ethernet1/1     Bound        10.43.14.80      10.43.14.1
 70315
admin@PA-220>
```

Recopilación de resultados de depuración sobre DHCP

Para reunir los resultados de la depuración sobre DHCP, utilice uno de los siguientes comandos:

- admin@PA-220> **debug dhcpd**
- admin@PA-220> **debug management-server dhcpd**

DNS:

El sistema de nombres de dominio (Domain Name System, DNS) es un protocolo que traduce (resuelve) un nombre de dominio sencillo, como www.paloaltonetworks.com, en una dirección IP, de modo que los usuarios puedan acceder a ordenadores, sitios web, servicios u otros recursos en internet o en redes privadas.

- Descripción general del DNS
- Objeto proxy DNS
- Perfil de servidor DNS
- Implementaciones de DNS multiusuario
- Configuración de un objeto proxy DNS
- Configuración de un perfil de servidor DNS
- Caso de uso 1: el cortafuegos exige la resolución de DNS
- Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual.
- Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor
- Regla de proxy DNS y coincidencia FQDN

Descripción general del DNS

DNS realiza una función crucial en la habilitación del acceso de usuarios a los recursos de red, de modo que los usuarios no deban recordar las direcciones IP y los ordenadores individuales no deban almacenar un gran volumen de nombres de dominios asignados a las direcciones IP. DNS emplea un modelo de cliente/servidor; un servidor DNS resuelve una consulta de un cliente DNS buscando el dominio en su caché y, de ser necesario, enviando consultas a otros servidores hasta que puede responder al cliente con la dirección IP correspondiente.

La estructura de DNS de los nombres de dominio es jerárquica; el dominio de nivel superior (TLD) en un nombre de dominio puede ser un TLD genérico (gTLD): com, edu, gov, int, mil, net u org (gov y mil corresponden solo a Estados Unidos) o un código de país (ccTLD), como au (Australia) o us (Estados Unidos). Por lo general, los ccTLD se reservan para países y territorios independientes.

Un nombre de dominio completo (FQDN) incluye, como mínimo, un nombre de host, un dominio de segundo nivel y un TLD para especificar completamente la ubicación del host en la estructura del DNS. Por ejemplo, www.paloaltonetworks.com es un FQDN.

Siempre que un cortafuegos de Palo Alto Networks® utiliza un FQDN en la interfaz de usuario o la CLI, el cortafuegos debe resolver el FQDN que utiliza DNS. En función de dónde se origina la consulta del FQDN®, el cortafuegos determina qué configuración DNS se utilizará para resolver la consulta.

Los registros de DNS de los FQDN incluyen un valor de tiempo de vida (time-to-live, TTL). El cortafuegos actualiza de manera predeterminada cada uno de los FQDN que tiene almacenados en su caché en función del TTL que proporciona el servidor DNS, siempre que dicho valor sea igual o superior al tiempo mínimo de actualización de los FQDN que configure en el cortafuegos o, si no lo especifica, al ajuste predeterminado de 30 segundos. La actualización de los FQDN basada en el valor del TTL resulta de especial utilidad para proteger el acceso a los servicios de las plataformas en la nube, que suelen exigir una actualización frecuente para garantizar la alta disponibilidad. Por ejemplo, los entornos de nube con escalabilidad automática dependen de la resolución de los FQDN para ampliar o reducir los servicios de forma dinámica; en esos entornos donde el tiempo es un factor tan importante, es fundamental la rapidez en la resolución de los FQDN.

Si configura el tiempo mínimo de actualización de los FQDN, limita el valor mínimo de TTL que respeta el cortafuegos. Si sus direcciones IP no varían a menudo, defina un tiempo de actualización mayor para que el cortafuegos no actualice las entradas innecesariamente. El cortafuegos usa el valor que sea más alto: el TTL de DNS o el tiempo mínimo de actualización de los FQDN configurado.

Por ejemplo, dos FQDN tienen los siguientes valores de TTL. El tiempo mínimo de actualización de los FQDN los sustituye, ya que estos son más bajos, es decir, más breves.

	TTL	Tiempo mínimo de actualización de FQDN = 26	Tiempo real de actualización
FQDN A	20		26
FQDN B	30		30

El temporizador de actualización de un FQDN se pone en marcha cuando el cortafuegos recibe una respuesta de DNS del servidor DNS o del objeto de proxy DNS que resuelve el FQDN.

Además, puede configurar un tiempo de espera de obsolescencia, que determina cuánto tiempo debe seguir usando el cortafuegos las resoluciones de FQDN obsoletas (vencidas) si no se puede acceder al servidor DNS. Si termina el tiempo de espera de obsolescencia y aún no se puede acceder al servidor DNS, las entradas de FQDN obsoletas se quedan sin resolver, y el cortafuegos las elimina.

Las siguientes tareas del cortafuegos están relacionadas con el DNS:

- Configure su cortafuegos con, al menos, un servidor DNS para que resuelva los nombres de host. Configure los servidores DNS principal y secundario o un objeto de proxy DNS que especifique esos servidores como se explica en Caso de uso 1: el cortafuegos exige la resolución de DNS.
- Personalice cómo el cortafuegos gestiona la resolución de DNS iniciada por las reglas de la política de seguridad, la creación de informes y los servicios de gestión (como correo electrónico, Kerberos, SNMP, Syslog, etc.) de cada sistema virtual, como se muestra en Caso de uso 2: el usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, creación de informes y servicios dentro de su sistema virtual.
- Configure el cortafuegos para que actúe como un servidor DNS para un cliente, como se muestra en Caso de uso 3: el cortafuegos actúa como proxy DNS entre cliente y servidor.
- Configure un perfil antispyware para garantizar el Uso de consultas de DNS para identificar hosts infectados en la red.
- Realice la Habilitación de firmas de evasión y habilite las firmas de evasión para la prevención de amenazas.
- Realice la Configuración de una interfaz como servidor DHCP. Esto permite que el cortafuegos actúe como un servidor DHCP y envíe información de DNS a sus clientes DHCP, de modo que los clientes DHCP asignados puedan alcanzar los servidores DNS correspondientes.

Objeto proxy DNS

Cuando se configura como proxy DNS, el cortafuegos actúa como intermediario entre los clientes y servidores de DNS; actúa como un servidor DNS en sí mismo resolviendo consultas desde su caché de proxy DNS. Si no encuentra el nombre de dominio en la caché de proxy DNS, el cortafuegos busca una coincidencia del nombre de dominio entre las entradas en el objeto proxy DNS específico (en la interfaz en la que se recibe la consulta DNS). El cortafuegos reenvía la consulta a un servidor DNS en función de los resultados. Si no se encuentra una coincidencia, el cortafuegos utiliza los servidores DNS predeterminados.

Un objeto de proxy DNS es donde se configuran los ajustes que determinan el funcionamiento del cortafuegos como proxy DNS. Puede asignar un objeto de proxy DNS a un único sistema virtual o compartirlo entre todos los sistemas virtuales.

- Si el objeto de proxy DNS es para un sistema virtual, puede especificar un Perfil de servidor DNS, que especifica las direcciones de servidores de DNS principales y secundarias, junto con otra información. El perfil de servidor DNS simplifica la configuración.
- Si el objeto proxy de DNS es compartido, debe especificar al menos la dirección principal de un servidor DNS.

Al configurar múltiples usuarios (abonados del ISP) con servicios DNS, se debe definir el proxy DNS de cada usuario, lo que mantiene el servicio DNS separado de los servicios de otros usuarios.

En el objeto de proxy, se especifican las interfaces en las que el cortafuegos actúa como proxy DNS. El proxy DNS para la interfaz no usa la ruta de servicio; las respuestas a las solicitudes DNS se envían siempre a la interfaz asignada al enrutador virtual donde se recibió la solicitud de DNS.

Cuando realiza la Configuración de un objeto proxy DNS, puede introducir en el proxy DNS asignaciones estáticas de FQDN a dirección. Además, puede crear reglas de proxy DNS que controlen a qué servidor DNS se dirigen las consultas de nombres de dominio especificado (que coinciden con las reglas de proxy). Puede configurar un máximo de 256 objetos de proxy DNS en un cortafuegos. Debe habilitar la **caché** y **las respuestas de EDNS de la caché** (en **Network (Red)** > **DNS Proxy (Proxy DNS)** > **Advanced (Avanzado)**) si el objeto proxy DNS se asigna a **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **DNS** o **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** > **vsys** > **General** > **DNS Proxy (Proxy DNS)**. Además, si este objeto proxy DNS tiene configuradas **reglas de proxy DNS**, esas reglas también deben tener la caché habilitada (**Turn on caching of domains resolved by this mapping (Activar el almacenamiento en caché de dominios resueltos por esta asignación)**).

Cuando un cortafuegos recibe una consulta de FQDN (y el nombre del dominio no se encuentra en el caché de proxy DNS), el cortafuegos compara el nombre de dominio de la consulta de FQDN con los nombres de dominio en las reglas de proxy DNS del objeto de proxy DNS. Si especifica múltiples nombres de dominio en una regla de proxy DNS, una consulta que coincida con alguno de los nombres de dominio en la regla indicará que la consulta coincide con la regla. Regla de proxy DNS y coincidencia FQDN describe cómo el cortafuegos determina si un FQDN coincide con un nombre de dominio en una regla de proxy DNS. Una consulta de DNS que coincide con una regla se envía al servidor DNS principal configurado para el objeto de proxy que debe resolverse.

Perfil de servidor DNS

Para simplificar la configuración de un sistema virtual, un perfil de servidor DNS le permite especificar el sistema virtual que se está configurando, un origen de herencia o las direcciones IP principales y secundarias para los servidores de DNS, así como una interfaz y la dirección de origen (ruta de servicio) que se usará en los paquetes enviados al servidor DNS. La interfaz de origen determina el enrutador virtual, que tiene una tabla de enrutamiento. Se busca la dirección IP de destino en la tabla de rutas del enrutador virtual donde está asignada la interfaz de origen. Es posible que el resultado de la interfaz de salida de IP de destino difiera de la interfaz de origen. El paquete saldría de la interfaz de salida de IP de destino determinada por la búsqueda de la tabla de enrutamiento, pero la dirección IP de origen sería la dirección configurada. La dirección de origen se usa como la dirección de destino en la respuesta del servidor DNS.

El informe del sistema virtual y el perfil del servidor del sistema virtual envían sus consultas al servidor DNS especificado en el sistema virtual, de haberlo. (El servidor DNS utilizado se define en **Device [Dispositivo]** > **Virtual Systems [Sistemas virtuales]** > **General** > **DNS Proxy [Proxy DNS]**.) Si no hay ningún servidor DNS especificado para el sistema virtual, se consulta al servidor DNS especificado para el cortafuegos.

La Configuración de un perfil de servidor DNS se realiza solo para un sistema virtual; no sirve para la ubicación compartida global.

Implementaciones de DNS multiusuario

El cortafuegos determina cómo gestionar solicitudes DNS basadas en el origen de la solicitud. Un entorno donde un ISP tiene varios usuarios en un cortafuegos se conoce como multiusuario. Hay tres casos de uso para implementaciones de DNS multiusuario:

- **Resolución DNS de gestión global**: el cortafuegos necesita resolución DNS para sus propios fines; por ejemplo, la solicitud procede del plano de gestión para resolver un FQDN de un evento de gestión como en un servicio de actualización de software. El cortafuegos utiliza la ruta de servicio para llegar a un servidor DNS debido a que la solicitud DNS no proviene de un enrutador virtual específico.
- **Resolución FQDN de políticas e informes para un sistema virtual**: en el caso de las consultas DNS de una política de seguridad, un informe o un servicio, puede especificar un conjunto de servidores DNS específicos para el sistema virtual (usuario) o utilizar la opción predeterminada para los servidores DNS globales. Si su caso de uso requiere un conjunto diferente de servidores DNS por sistema virtual, debe configurar un objeto proxy DNS. La resolución es específica del sistema virtual al que se ha asignado el proxy DNS. Si no tiene servidores DNS específicos que puedan aplicarse a este sistema virtual, el cortafuegos utiliza la configuración de DNS global.
- **Resolución DNS en el plano de datos para un sistema virtual**: este método también se conoce como solicitud de red para resolución DNS. El sistema virtual del usuario se puede configurar de modo que los nombres de dominio especificados se resuelvan en el servidor DNS del usuario en su red. Este método es compatible con ***DNS dividido***, lo que significa que el usuario también puede usar sus propios servidores DNS del ISP para las consultas de DNS restantes no resueltas en su propio servidor. Las reglas de objeto proxy DNS controlan el DNS dividido; el dominio del usuario redirige las solicitudes DNS a sus servidores DNS, que están configurados con un perfil de servidor DNS. El perfil de servidor DNS tiene servidores DNS principales y secundarios designados, así como rutas de servicio DNS para IPv4 e IPv6, que anulan la configuración DNS predeterminada.

La siguiente tabla resume los tipos de resolución de DNS. La ubicación de enlace determina qué objeto de proxy DNS se usa para la resolución. Los casos de uso muestran, a modo de ejemplo, cómo un proveedor de servicios puede configurar los ajustes DNS con el fin de ofrecer servicios de DNS para resolver consultas de DNS requeridas en el cortafuegos y para los sistemas virtuales del usuario (abonado).

Tipo de resolución del	compartido: Lugar	compartido: Vsys específico
Resolución de DNS del cortafuegos: realizada por el plano de datos	Enlace: Global Ilustrado en el Caso de uso 1	n/c
Perfil de seguridad, informes y resolución de perfiles de servidor: realizado por el plano de gestión	Enlace: Global El mismo comportamiento que en caso de uso 1	Enlace: Vsys específico Ilustrado en el Caso de uso 2

Tipo de resolución del	compartido: Lugar	compartido: Vsys específico
Resolución de proxy DNS para hosts de clientes DNS conectados a la interfaz en el cortafuegos, que atraviesan el cortafuegos hacia un servidor DNS: realizado por el plano de datos.	Enlace: Interface (Interfaz) Ruta de servicio: Interfaz y dirección IP en las que se recibió la solicitud DNS. Ilustrado en el Caso de uso 3	

- Caso de uso 1: el cortafuegos exige la resolución de DNS
- Caso de uso 2: el usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, creación de informes y servicios dentro de su sistema virtual
- Caso de uso 3: el cortafuegos actúa como proxy DNS entre cliente y servidor

Configuración de un objeto proxy DNS

Si su cortafuegos va a funcionar como un proxy DNS, realice esta tarea para configurar un objeto proxy DNS. El objeto de proxy puede ser tanto compartido entre todos los sistemas virtuales como aplicado a un sistema virtual específico.

Cuando el cortafuegos está habilitado para funcionar como proxy DNS, las firmas de evasión que detectan solicitudes HTTP o TLS manipuladas pueden alertar en instancias en las que un cliente se conecta a un dominio que no sea el dominio especificado en la solicitud DNS original. Se recomienda habilitar las firmas de evasión *tras configurar el proxy DNS para que se active una alerta si se detectan solicitudes manipuladas.*

STEP 1 | Configure los ajustes básicos para un objeto de proxy DNS.

1. Seleccione **Network (Red)** > **DNS Proxy** y luego **Add (Añadir)** para añadir un nuevo objeto.
2. Verifique que **Enable** esté seleccionado.
3. Introduzca un nombre para el objeto en **Name**.
4. Para **Location (Ubicación)**, seleccione el sistema virtual al que se aplica el objeto. Si selecciona **Shared (Compartido)**, debe especificar al menos una dirección **Primary (Primaria)** de servidor DNS y, de manera opcional, una dirección **Secondary (Secundaria)**.
5. Si ha seleccionado un sistema virtual, para **Server Profile (Perfil de servidor)**, seleccione un perfil de servidor DNS o haga clic en **DNS Server Profile (Perfil de servidor DNS)** para configurar un nuevo perfil. Consulte Configuración de un perfil de servidor DNS.
6. Para Inheritance Source (Origen de herencia), seleccione un origen del cual heredar las configuraciones del servidor DNS predeterminadas. El valor predeterminado es **None (Ninguno)**.
7. Para **Interface**, haga clic en **Add** y especifique las interfaces a las que se aplica el objeto de proxy DNS.
   - Si usa el objeto de proxy DNS para realizar búsquedas de DNS, necesita una interfaz. El cortafuegos escuchará las solicitudes de DNS en esta interfaz, y después las transmitirá.
   - Si usa el objeto de proxy DNS para una ruta de servicio, la interfaz es opcional.

STEP 2 | (Opcional) Especifique reglas de proxy DNS

1. En la pestaña **DNS Proxy Rules (Reglas de proxy DNS)**, haga clic en **Add (Añadir)** e introduzca un nombre para la regla en **Name (Nombre)**.
2. Seleccione **Turn on caching of domains resolved by this mapping**, si desea que el cortafuegos almacene en caché los dominios resueltos.
3. En **Domain Name (Nombre de dominio)**, seleccione **Add (Añadir)** para añadir una o más entradas por fila, con las cuales el cortafuegos comparará las consultas FQDN. Si una consulta coincide con uno de los dominios de la regla, la consulta se envía a uno de los siguientes servidores para resolverse (según lo que configuró en el paso anterior):
   - El servidor DNS **Primary (Primario)** o **Secondary (Secundario)** especificado directamente para este objeto proxy.

- El servidor DNS **Primary (Primario)** o **Secondary (Secundario)** especificado directamente para este objeto proxy.

DNS Proxy Rule and FQDN Matching (Regla de proxy DNS y coincidencia FQDN) describe de qué manera el cortafuegos coteja los nombres de dominio en un FQDN con una regla proxy DNS. Si no se encuentra coincidencia, los servidores DNS predeterminados resuelven la consulta.

4. Realice una de las siguientes acciones, según lo que configure en **Location (Ubicación)**:
   - Si ha elegido un sistema virtual, seleccione aquí un **DNS Server profile (Perfil de servidor DNS)**.
   - Si ha elegido **Shared (Compartido)**, introduzca una dirección **Primary (Primaria)** y, opcionalmente, una dirección **Secondary (Secundaria)**.
5. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Indique las entradas estáticas FQDN a dirección en el proxy DNS. Las entradas DNS estáticas permiten al cortafuegos resolver el FQDN a una dirección IP sin enviar una consulta al servidor DNS.

1. En la pestaña **Static Entries (Entradas estáticas)**, haga clic en **Add (Añadir)** e introduzca un nombre en **Name (Nombre)**.
2. Introduzca el nombre de dominio completo (**FQDN**).
3. Para **Address (Dirección)**, haga clic en **Add (Añadir)** e introduzca la dirección IP a la que se debería asignar el FQDN.

   Puede proporcionar direcciones IP adicionales para una entrada. El cortafuegos proporcionará todas las direcciones IP en su respuesta DNS y el cliente elige qué dirección usar.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Habilite el almacenamiento en caché y configure otros ajustes avanzados para el proxy DNS.

1. En la pestaña **Advanced (Avanzada)**, seleccione **TCP Queries (Consultas TCP)** para habilitar las consultas DNS mediante TCP.
   - **Max Pending Requests**: introduzca el número máximo de solicitudes DNS TCP pendientes simultáneas que admitirá el cortafuegos (intervalo 64-256, por defecto: 64).
2. Para **UDP Queries Retries (Reintentos de consultas UDP)**, introduzca lo siguiente:
   - **Interval (Intervalo)**: el tiempo (en segundos) después del cual se enviará otra solicitud si no se ha recibido respuesta (el intervalo es de 1 a 30, el valor predeterminado es 2).
   - **Attempts (Intentos)**: el número máximo de intentos de consulta UDP (sin incluir el primer intento) después de los cuales se intentará el siguiente servidor DNS (el intervalo es de 1 a 5; el valor predeterminado es 30).
3. Seleccione **Cache (Caché)** para habilitar al cortafuegos para que almacene en caché las asignaciones de FQDN a dirección que detecte. Debe habilitar la **caché** (habilitada de forma predeterminada) si este objeto proxy DNS se utiliza para consultas que genera el cortafuegos (es decir, en **Device (Dispositivo)** > **Setup (Configuración)** > **Services**

(Servicios) > **DNS** o en **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** y seleccione un sistema virtual y **General** > **DNS Proxy (Proxy DNS)**.

- **Enable TTL (Habilitar TTL)**: limite el tiempo que el cortafuegos almacena en caché las entradas DNS del objeto proxy. De forma predeterminada, esta opción está deshabilitada.
  - Introduzca **Time to Live (sec) (Periodo de vida [s])**, la cantidad de segundos después de los cuales se eliminan todas las entradas de la memoria caché para el objeto proxy. Después de eliminar las entradas, las nuevas solicitudes de DNS deben volver a resolverse y almacenarse en caché. El intervalo es de 60-86.400. No hay TTL por defecto; las entradas permanecen hasta que el cortafuegos se queda sin memoria caché.
- **Cache EDNS Responses (Respuestas de EDNS de caché)**: debe habilitar esta configuración si se utiliza este objeto proxy DNS para consultas que genera el cortafuegos (es decir, en **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** > **DNS** o en **Device** > **Virtual Systems (Sistemas virtuales)** y selecciona un sistema virtual y **General** > **DNS Proxy (Proxy DNS)**.

STEP 5 | Confirme los cambios.

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

Configuración de un perfil de servidor DNS

Configure un perfil de servidor DNS, lo que simplifica la configuración de un sistema virtual. La dirección **Primary DNS (DNS primaria)** o **Secondary DNS (DNS secundaria)** se usa para crear la solicitud DNS que el sistema virtual envía al servidor DNS.

STEP 1 | Nombre el perfil de servidor DNS, seleccione el sistema virtual al que se aplica y especifica las direcciones de servidor DNS principal y secundaria.

1. Seleccione **Device (Dispositivo)** > **Server Profiles (Perfiles de servidor)** > **DNS** y **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil de servidor DNS.
2. Para **Location**, seleccione el sistema virtual al que se aplica el perfil.
3. En **Inheritance Source (Origen de herencia)**, seleccione **None (Ninguno)** si las direcciones del servidor DNS no se heredan. De lo contrario, especifique el servidor de DNS desde el que el perfil debería heredar la configuración. Si ha elegido un servidor DNS, haga clic en **Check inheritance source status** para ver esa información.
4. Especifique la dirección IP del servidor **Primary DNS** o déjelo como **inherited** si ha elegido un **Inheritance Source**.

   *Tenga en cuenta que si especifica un FQDN en lugar de una dirección IP, el DNS para ese FQDN se resuelve en **Device (Dispositivo) > Virtual Systems (Sistema virtual) > DNS Proxy (Proxy DNS).***
5. Especifique la dirección IP del servidor **Secondary DNS**, o déjelo como **inherited** si ha elegido un **Inheritance Source**.

STEP 2 | Configure la ruta de servicio que usa el cortafuegos automáticamente, basada en si el servidor DNS de destino tiene un tipo de familia de dirección IP IPv4 o IPv6.

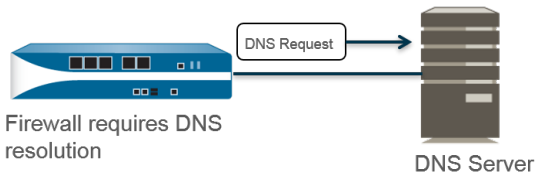
1. Haga clic en **Service Route IPv4** para habilitar la siguiente interfaz y la dirección IPv4 que se usará como ruta de servicio, si la dirección DNS de destino es una dirección IPv4.
2. Especifique la **Source Interface (Interfaz de origen)** para seleccionar la dirección IP de origen del servidor DNS que usará la ruta de servicio. El cortafuegos determina qué enrutador virtual se asigna a esa interfaz, y después realiza una búsqueda de rutas en la tabla de enrutamiento del enrutador virtual para llegar a la red de destino (en función de la dirección **Primary DNS**).
3. Especifique la **dirección de origen** IPv4 desde la que se originan los paquetes dirigidos al servidor de DNS.
4. Haga clic en **Service Route IPv6 (Ruta de servicio IPv6)** para habilitar la siguiente interfaz y la dirección IPv6 que se usará como ruta de servicio, si la dirección DNS de destino es una dirección IPv6.
5. Especifique la **Source Interface (Interfaz de origen)** para seleccionar la dirección IP de origen del servidor DNS que usará la ruta de servicio. El cortafuegos determina qué enrutador virtual se asigna a esa interfaz, y después realiza una búsqueda de rutas en la tabla de enrutamiento del enrutador virtual para llegar a la red de destino (en función de la dirección **Primary DNS**).
6. Especifique la **Source Address (Dirección de origen)** IPv6 desde la que se originan los paquetes dirigidos al servidor de DNS.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme la configuración.

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

Caso de uso 1: el cortafuegos exige la resolución de DNS

En este caso de uso, el cortafuegos es el cliente que solicita la resolución de DNS de los FQDN para las reglas de la política de seguridad, la creación de informes, los servicios de gestión (como correo electrónico, Kerberos, SNMP o syslog, entre otros) y los eventos de gestión (como servicios de actualización de software, actualizaciones dinámicas de software y WildFire). En los entornos dinámicos, los FQDN cambian con más frecuencia; por eso, una resolución de DNS precisa permite que el cortafuegos aplique las políticas con rigurosidad, preste servicios de gestión y elaboración de informes y maneje los eventos de gestión. Los servicios DNS globales y compartidos realizan la resolución DNS para las funciones del plano de gestión.



STEP 1 | Configure los servidores DNS principal y secundario que debe usar el cortafuegos para la resolución de DNS.

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

1. Edite los ajustes de los servicios (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Global** en los cortafuegos que admiten varios sistemas virtuales; **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** en los que no los admiten).
2. En la pestaña **Services (Servicios)**, en **DNS**, seleccione **Servers (Servidores)** e introduzca la dirección del **Primary DNS Server (Servidor DNS principal)** y la dirección del **Secondary DNS Server (Servidor DNS secundario)**.
3. Continúe al paso 3.

STEP 2 | De manera alternativa, puede configurar un objeto Proxy DNS si desea configurar funciones DNS avanzadas como DNS dividido, anulaciones de proxy DNS, reglas de proxy DNS, entradas estáticas o herencia DNS.

1. Edite los ajustes de los servicios (**Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** > **Global** en los cortafuegos que admiten varios sistemas virtuales; **Device [Dispositivo]** > **Setup [Configuración]** > **Services [Servicios]** en los que no los admiten).
2. En la pestaña **Services (Servicios)**, en **DNS**, seleccione **DNS Proxy Object (Objeto Proxy DNS)**.
3. En la lista **DNS Proxy (Proxy DNS)**, seleccione el proxy DNS que desea utilizar para configurar los servicios de DNS globales o bien seleccione **DNS Proxy (Proxy DNS)** para configurar un objeto de proxy DNS nuevo del modo siguiente:
   1. Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el objeto proxy DNS.
   2. En los cortafuegos que admiten varios sistemas virtuales, en **Location (Ubicación)**, seleccione **Shared (Compartido)** para los servicios proxy DNS globales en todo el cortafuegos.

      Los objetos proxy DNS compartidos no utilizan perfiles de servidor DNS porque no requieren una ruta de servicio específica que pertenezca a un sistema virtual del usuario.
   3. Introduzca la dirección IP del servidor DNS principal en **Primary (Principal)**. También puede introducir una dirección IP del servidor DNS **Secondary (Secundario)**.
4. Seleccione la pestaña **Advanced (Avanzado)**. Asegúrese de que la **caché** se habilite y se activen las **respuestas EDNS de la caché** (ambas habilitadas de forma predeterminada).
5. Haga clic en **OK (Aceptar)** para guardar el objeto proxy DNS.

STEP 3 | (Opcional) Configure el valor oportuno en **Minimum FQDN Refresh Time (sec) (Tiempo mínimo de actualización de FQDN [s])** para limitar la frecuencia con la que el cortafuegos actualiza las entradas de FQDN de la caché.

El cortafuegos actualiza de manera predeterminada cada uno de los FQDN que tiene almacenados en su caché en función del tiempo de vida (time-to-live, TTL) del FQDN incluido en un registro de DNS, siempre que dicho valor sea igual o superior a este tiempo mínimo de actualización de los FQDN o, si no lo configura, al ajuste predeterminado de 30 segundos. Si desea especificar un tiempo mínimo de actualización de los FQDN, introduzca el valor oportuno en segundos entre 0 y 14 400; el valor predeterminado es 30. El valor 0 significa que el cortafuegos actualiza los FQDN en función del valor de TTL que figura en los registros de DNS, ya que el cortafuegos no aplica ningún tiempo mínimo de actualización de los FQDN. El cortafuegos usa el valor que sea más alto: el TTL de DNS o el tiempo mínimo de actualización de los FQDN.

Si el TTL del FQDN de DNS es breve, pero las resoluciones de FQDN no cambian con tanta frecuencia y no hacen falta actualizaciones tan repetidas, debe configurar un tiempo mínimo de actualización de los FQDN para que no se produzcan más intentos de actualización de los FQDN de los necesarios.

STEP 4 | (Opcional) En **FQDN Stale Entry Timeout (min) (Tiempo de espera de entradas obsoletas de FQDN [min])**, especifique cuántos minutos debe seguir usando el cortafuegos las resoluciones

de FQDN obsoletas si no se puede acceder al servidor DNS; el intervalo admitido va de 0 a 10 080 y el valor predeterminado es 1440.

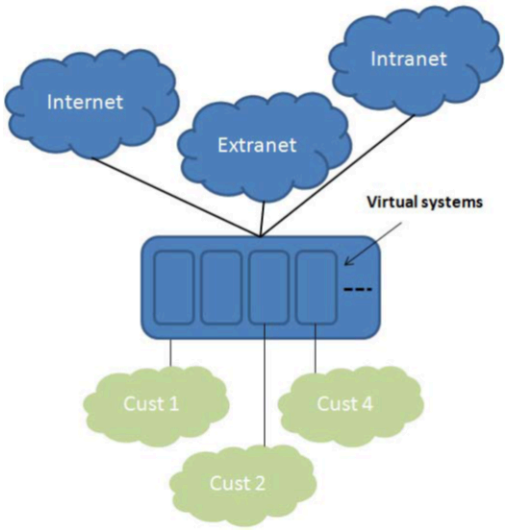
El valor 0 significa que el cortafuegos no sigue usando las entradas de FQDN obsoletas.

Asegúrese de que el tiempo de espera de las entradas de FQDN obsoletas sea lo suficientemente breve como para impedir el reenvío de tráfico incorrecto, que supone un riesgo para la seguridad, pero lo bastante prolongado para permitir la continuidad del tráfico sin causar interrupciones inesperadas en la red.

STEP 5 | Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

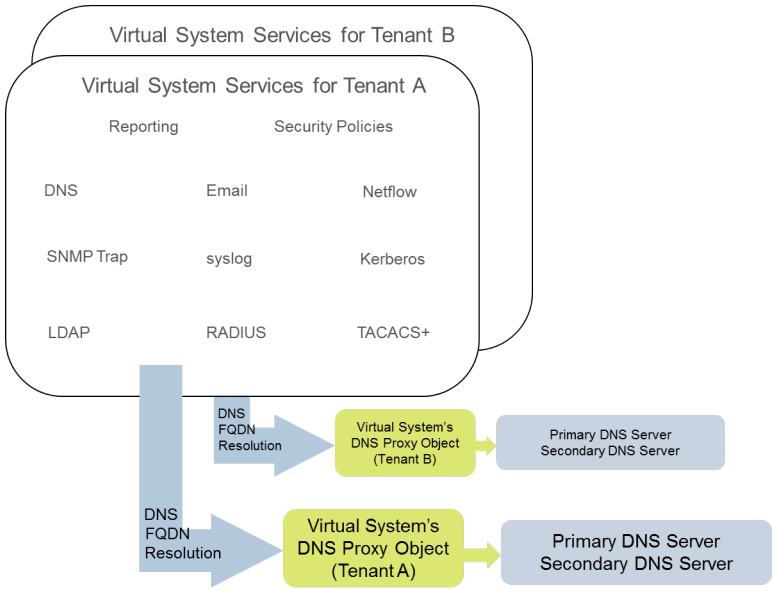
Caso de uso 2: El usuario del ISP usa proxy DNS para gestionar la resolución DNS para políticas de seguridad, informes y servicios dentro de su sistema virtual.

En este caso de uso, se definen varios usuarios (abonados del ISP) en el cortafuegos y a cada usuario se le asigna un sistema virtual (vsys) y un enrutador virtual diferentes para segmentar sus servicios y dominios administrativos. La siguiente figura ilustra varios sistemas virtuales dentro de un cortafuegos.



Cada usuario tiene sus propios perfiles de servidor para sus reglas de política de seguridad, informes y servicios de gestión (como correo electrónico, Kerberos, SNMP, syslog, etc.) definidos en sus propias redes.

Para las resoluciones DNS iniciadas por estos servicios, cada sistema virtual está configurado con su propio Objeto proxy DNS para permitir que cada usuario personalice la gestión de la resolución DNS dentro de su sistema virtual. Cualquier servicio con una **Location (Ubicación)** usará el objeto Proxy DNS configurado para el sistema virtual para determinar el servidor DNS principal (o secundario) para resolver FQDN, como se ilustra en la siguiente figura.



STEP 1 | Especifique el proxy DNS que se usará en cada sistema virtual.

1. Seleccione **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** y **Add (Añadir)** para añadir el **ID** del sistema virtual (el intervalo es de 1 a 255), y luego un nombre opcional en **Name (Nombre)**; en este ejemplo, Corp1 Corporation.
2. En la pestaña **General**, seleccione un **DNS Proxy (Proxy DNS)** o cree uno nuevo. En este ejemplo, se selecciona Corp1 DNS Proxy como el proxy para el sistema virtual de Corp1 Corporation.
3. En **Interfaces**, haga clic en **Add (Añadir)**. En este ejemplo, Ethernet 1/20 se dedica a este usuario.
4. En **Virtual Routers (Enrutadores virtuales)**, haga clic en **Add (Añadir)**. Se asigna al sistema virtual un enrutador virtual llamado Corp1 VR para separar las funciones de enrutamiento.
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Configure un proxy DNS y un perfil de servidor para permitir la resolución DNS para un sistema virtual.

1. Seleccione **Network (Red)** > **DNS Proxy** y haga clic en **Add (Añadir)**.
2. Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el proxy DNS.
3. En **Location (Ubicación)**, seleccione el sistema virtual del usuario, en este ejemplo, Corp1 Corporation (vsys6). (Puede elegir el recurso proxy DNS **Shared (Compartido)** en su lugar).
4. En **Server Profile (Perfil de servidor)**, seleccione o cree un perfil con el fin de personalizar servidores DNS para usar resoluciones DNS para esta política de seguridad de usuarios, informe y servicios de perfil de servidor.

   Si el perfil aún no está configurado, en el campo **Server Profile (Perfil de servidor)**, haga clic en **DNS Server Profile (Perfil de servidor DNS)** para Configuración de un perfil de servidor DNS.

   El perfil de servidor DNS identifica las direcciones IP del servidor DNS principal y secundario para usar las resoluciones de DNS de gestión para este sistema virtual.
5. También para este perfil de servidor, tiene la opción de configurar una **Service Route IPv4 (IPv4 de ruta de servicio)** o una **Service Route IPv6 (IPv6 de ruta de servicio)** para indicar al cortafuegos qué **Source Interface (Interfaz de origen)** usar en sus solicitudes DNS. Si esta interfaz tiene más de una dirección IP, configure también la **Source Address (Dirección de origen)**.
6. Seleccione la pestaña **Advanced (Avanzado)**. Asegúrese de que la **caché** se habilite y se activen las **respuestas EDNS de la caché** (ambas habilitadas de forma predeterminada). Esto es obligatorio si se utiliza el objeto proxy DNS en **Device (Dispositivo)** > **Virtual Systems (Sistemas virtuales)** > **vsys** > **General** > **DNS Proxy (Proxy DNS)**.
7. Haga clic en **OK (Aceptar)**.
8. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)**.

   *Se pueden configurar funciones avanzadas opcionales como DNS dividido usando **DNS Proxy Rules (Reglas de proxy DNS)**. Si es necesario, se puede usar un perfil de servidor DNS separado para redirigir las resoluciones DNS que coinciden con el **Domain Name (Nombre de dominio)** en una **DNS Proxy Rule (Regla de proxy DNS)** para otro conjunto de servidores DNS. El Caso de uso 3 ilustra el DNS dividido.*

   Si usa dos perfiles de servidor DNS separados en el mismo objeto Proxy DNS, uno para el proxy DNS y otro para la regla de proxy DNS, se produce lo siguiente:

   - Si se define una ruta de servicio en el perfil de servidor DNS usado por el proxy DNS, tiene prioridad y se usa.
   - Si se define una ruta de servicio en el perfil de servidor DNS usado en las reglas del proxy DNS, no se usa. Si la ruta de servicio difiere de la definida en el perfil de servidor

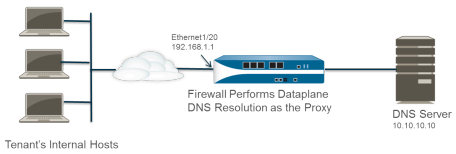
DNS usado en el proxy DNS, se muestra el siguiente mensaje de advertencia durante el proceso **Commit (Confirmar)**:

```
Warning: The DNS service route defined in the DNS proxy object
 is different from the DNS proxy rule’s service route. Using
 the DNS proxy object’s service route.
```

- Si no se define ninguna ruta de servicio en ningún perfil de servidor DNS, se usa la ruta de servicio global en caso necesario.

Caso de uso 3: El cortafuegos hace de proxy DNS entre cliente y servidor

En este caso de uso, el cortafuegos se encuentra entre el cliente DNS y el servidor DNS. Se configura un cortafuegos en el proxy DNS para que actúe como servidor DNS de los hosts que residen en la red del usuario conectada a la interfaz del cortafuegos. En dicho escenario, el cortafuegos realiza una resolución DNS en su plano de datos.



El escenario utiliza ***DNS dividido***, una configuración donde las reglas de proxy DNS se configuran para redirigir las solicitudes DNS a un conjunto de servidores DNS basados en una coincidencia de nombres de dominio. Si no hay coincidencia, el perfil del servidor determina los servidores DNS a los que se envía la solicitud; por eso, hay dos métodos de resolución de DNS dividido.

Para las resoluciones DNS de plano de datos, la dirección IP de origen desde el proxy DNS en PAN-OS al servidor DNS externo sería la dirección del proxy (la IP de destino de la solicitud original). No se usa ninguna ruta de servicio definida en el perfil de servidor DNS. Por ejemplo, si la consulta se realiza desde el host 172.16.1.1 al proxy DNS 192.168.1.1, la solicitud al servidor DNS (en 10.10.10.10) usaría un origen 192.168.1.1 y un destino 10.10.10.10.

STEP 1 | Seleccione **Network (Red)** > **DNS Proxy** y haga clic en **Add (Añadir)**.

STEP 2 | Haga clic en **Enable (Habilitar)** e introduzca un nombre en **Name (Nombre)** para el proxy DNS.

STEP 3 | En **Location (Ubicación)**, seleccione el sistema virtual del usuario, en este ejemplo, Corp1 Corporation (vsys6).

STEP 4 | En **Interface (Interfaz)**, seleccione la interfaz que recibirá las solicitudes DNS de los hosts del usuario, en este ejemplo, Ethernet 1/20.

STEP 5 | Seleccione o cree un **Server Profile (Perfil de servidor)** para personalizar servidores DNS para que resuelvan solicitudes DNS para este usuario.

STEP 6 | En la pestaña **DNS Proxy Rules (Reglas de proxy DNS)**, haga clic en **Add (Añadir)** e introduzca un nombre para la regla en **Name (Nombre)**.

STEP 7 | (Opcional) Seleccione **Turn on caching of domains resolved by this mapping (Activar el almacenamiento en caché de dominios resueltos por esta asignación)**.

STEP 8 | Haga clic en **Add (Añadir)** para añadir uno o más nombres de dominio en **Domain Name (Nombre de dominio)**, uno por fila. En Búsqueda de coincidencias de FQDN en la regla de proxy DNS, se describe cómo el cortafuegos encuentra coincidencias entre los FQDN y los nombres de dominio en una regla de proxy DNS.

STEP 9 | En **DNS Server profile (Perfil de servidor DNS)**, seleccione un perfil. El cortafuegos compara el nombre de dominio en la solicitud DNS con el nombre de dominio definido en **DNS Proxy Rules (Reglas de proxy DNS)**. Si hay coincidencia, se usa el **DNS Server profile (Perfil de servidor DNS)** definido en la regla para determinar el servidor DNS.

STEP 10 | En este ejemplo, si el dominio en la solicitud coincide con myweb.corp1.com, se usa el servidor DNS definido en perfil de servidor myweb DNS Server Profile. Si no hay coincidencia, se usa el servidor DNS definido en **Server profile (Perfil de servidor)** (perfil de servidor DNS Corp1).

STEP 11 | Haga clic en **OK** dos veces.

Regla de proxy DNS y coincidencia FQDN

Cuando configura el cortafuegos con un objeto proxy DNS que utiliza reglas de proxy DNS, el cortafuegos compara un FQDN de una consulta DNS con el nombre de dominio de una regla de proxy DNS. La comparación del cortafuegos funciona de la siguiente manera:

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
El cortafuegos primero divide en tokens los FQDN y los nombres de dominio de las reglas de proxy DNS. En un nombre de dominio, un token es una cadena delimitada por un punto (.).	**`*.boat.fish.com`** se compone de cuatro tokens tokens: **`[*][boat][fish][com]`**
El proceso de cotejo es una coincidencia de token exacta entre el FQDN y el nombre de dominio en la regla, las cadenas parciales no se cotejan.	Regla: **`fishing`** FQDN: **`fish`** — **no hay coincidencia**
Una excepción al requisito de coincidencia exacta es el uso del carácter comodín: un asterisco (*). El * coincide con uno o más tokens. Esto significa que una regla que consta únicamente de un carácter comodín (*) compara cualquier FQDN con uno o más tokens.	Regla: **`*.boat.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.blue.boat.com`** — coincidencia FQDN: **`boat.com`** — **no hay coincidencia**
	Regla: **`*`** FQDN: **`boat`** — coincidencia FQDN: **`boat.com`**: coincidencia FQDN: **`www.boat.com`** — coincidencia
Puede usar el * en cualquier posición: antes del token, entre tokens o al final de un token (pero no con otros caracteres, como un único token).	Regla: **`www.*.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.blue.boat.com`** — coincidencia
	Regla: **`www.*.com`** FQDN: **`www.boat.com`** — coincidencia FQDN: **`www.boat.fish.com`**: coincidencia
	Regla: **`www.boat*.com`**: **no válida**
Pueden aparecer varios caracteres comodines (*) en cualquier posición del	Regla: **`a.*.d.*.com`**

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
nombre de dominio: antes del token, entre tokens o al final del token. Cada * no consecutivo coincide con uno o más tokens.	FQDN: **a.b.d.e.com**: coincidencia FQDN: **a.b.c.d.e.f.com**: coincidencia FQDN: **a.d.d.e.f.com**: coincidencia (el primer * coincide con **d**; el segundo * coincide con **e** y **f**). FQDN: **a.d.e.f.com**: **no hay coincidencia** (el primer * coincide con **d**; las **d** posteriores de la regla no se cotejan).
Cuando se utilizan caracteres comodín en tokens consecutivos, el primer * coincide con uno o más tokens; el segundo * coincide con un token. Esto significa que una regla que consta únicamente de *.* compara cualquier FQDN con dos o más tokens.	Caracteres comodín consecutivos antes de los tokens: Regla: ***.*.boat.com** FQDN: **www.blue.boat.com** — coincidencia FQDN: **www.blue.sail.boat.com**: coincidencia
	Caracteres comodín consecutivos entre tokens: Regla: **www.*.*.boat.com** FQDN: **www.blue.sail.boat.com**: coincidencia FQDN: **www.big.blue.sail.boat.com**: coincidencia
	Caracteres comodín consecutivos al final de los tokens: Regla: **www.boat.*.*** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia
	Caracteres comodín consecutivos únicamente: Rule: *.* FQDN: **boat: no hay coincidencia** FQDN: **boat.com**: coincidencia FQDN: **www.boat.com** — coincidencia
Los caracteres comodín consecutivos y no consecutivos pueden aparecer en la misma regla.	Regla: **a.*.d.*.*.com**

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
	FQDN: **a.b.c.d.e.f.com**: coincidencia (el primer * coincide con **b** y **c**; el segundo * coincide con **e**; el tercer * coincide con **f**). FQDN: **a.b.c.d.e.com**: **no hay coincidencia** (el primer * coincide con **b** y **c**; el segundo * coincide con **e**; el tercer * no se coteja).
El comportamiento de coincidencia final implícita ofrece una taquigrafía adicional: Mientras el último token de la regla no sea un *, la comparación cotejará si todos los tokens de la regla coinciden con el FQDN, incluso si el FQDN posee tokens finales adicionales que la regla no tiene.	Regla: **www.boat.fish** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia FQDN: **www.boat.fish**: coincidencia
Esta regla finaliza con *, por lo que la regla de coincidencia final implícita no se aplica. El * actúa como se indica; coincide con uno o más tokens.	Regla: **www.boat.fish.*** FQDN: **www.boat.fish.com**: coincidencia FQDN: **www.boat.fish.ocean.com**: coincidencia FQDN: **www.boat.fish: no hay coincidencia** (este FQDN no posee un token para coincidir con el * en la regla).
En el caso en que un FQDN coincida con más de una regla, un algoritmo de separación selecciona la regla más específica (extensa); es decir, el algoritmo favorece la regla con más tokens y menos caracteres comodines (*).	Regla 1: ***.fish.com**: coincidencia Regla 2: ***.com**: coincidencia Regla 3: **boat.fish.com**: coincidencia y división FQDN: **boat.fish.com** El FQDN coincide con las tres reglas; el cortafuegos utiliza la regla 3 debido a que es la más específica.
	Regla 1: ***.fish.com: no hay coincidencia** Regla 2: ***.com**: coincidencia Regla 3: **boat.fish.com: no hay coincidencia** FQDN: **fish.com** El FQDN no coincide con la Regla 1 debido a que el * no tiene un token con el cual coincidir.
	Regla 1: ***.fish.com**: coincidencia y división Regla 2: ***.com**: coincidencia

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
	Regla 3: **boat.fish.com: no hay coincidencia** FQDN: **blue.boat.fish.com** El FQDN coincide con la Regla 1 y la Regla 2 (debido a que el * coincide con uno o más tokens). El cortafuegos utiliza la regla 1 debido a que es la más específica.
Al trabajar con caracteres comodín (*) y reglas de coincidencia final implícita, puede haber casos en los que el FQDN coincide con más de una regla y el algoritmo de separación pondera las reglas por igual. Para evitar ambigüedades, si las reglas con coincidencia final implícita o un carácter comodín (*) pueden superponerse, reemplace una regla de coincidencia final implícita al especificar el token final.	Reemplace lo siguiente: Regla: **www.boat** por lo siguiente: Regla: **www.boat.com**
Prácticas recomendadas para crear reglas de proxy DNS a fin de evitar ambigüedad y resultados inesperados	
Incluya un dominio de nivel superior en el nombre de dominio para que no se invoque una coincidencia final implícita, que podría hacer coincidir el FQDN con más de una regla.	**boat.com**
Si utiliza un carácter comodín (*), utilícelo únicamente como el token del extremo izquierdo. Esta práctica permite la comprensión común de los registros DNS con caracteres comodín y la naturaleza jerárquica del DNS.	***.boat.com**
No use más de un* en una regla.	
Use el * para establecer una regla de base asociada con un servidor DNS, y utilice reglas con más tokens para crear excepciones a la regla, la cual asocia con diferentes servidores.	Regla: ***.corporation.com**: servidor DNS A Regla: **www.corporation.com**: servidor DNS B Regla: ***.internal.corporation.com**: servidor DNS C

Comparación de FQDN con la regla de proxy DNS	Por ejemplo:
El algoritmo de división seleccionará la coincidencia más específica, en función de la cantidad de tokens coincidentes.	Regla: **`www.internal.corporation.com`**: servidor DNS D FQDN: **`mail.internal.corporation.com`**: coincide con el servidor DNS C FQDN: **`mail.corporation.com`**: coincide con el servidor DNS A

DDNS

Obtenga información sobre cómo el servicio DNS dinámico (DDNS) actualiza las asignaciones de nombres de dominio a direcciones IP para proporcionar direcciones IP precisas a los clientes DNS.

> Descripción general del DNS dinámico
> Configuración del DNS dinámico en las interfaces de cortafuegos

Descripción general del DNS dinámico

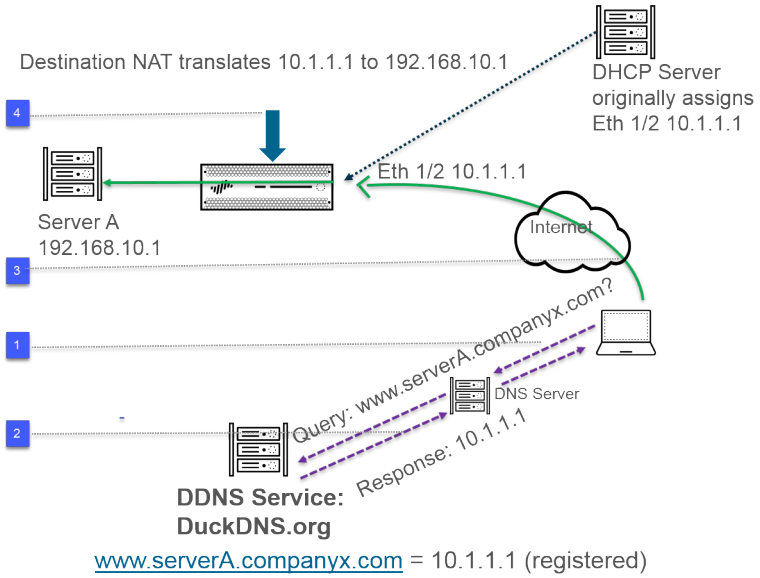
Si hay servicios alojados tras el cortafuegos y se emplean políticas de traducción de direcciones de red (network address translation, NAT) de destino para acceder al cortafuegos o si es preciso franquear el acceso remoto al cortafuegos, registre los cambios en las direcciones IPv4 (si la interfaz es un cliente DHCP que recibe una dirección dinámica o tiene una dirección estática) o las direcciones IPv6 (solo estáticas) de la interfaz con un proveedor de servicios de sistemas de nombres de dominio dinámicos (dynamic domain name system, DDNS). El servicio DDNS actualiza automáticamente las asignaciones de nombres de dominio a direcciones IP con el fin de proporcionar direcciones IP precisas a los clientes DNS para que puedan acceder al cortafuegos y a los servicios que protege. Este servicio se suele utilizar en las implementaciones de sucursales que alojan servicios. Si las interfaces de cortafuegos no admiten DDNS, hacen falta componentes externos para proporcionar direcciones IP precisas a los clientes.

Los cortafuegos admiten estos proveedores de servicios de DDNS: Duck DNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org y No-IP. Cada proveedor ofrece unos servicios distintos, por ejemplo, el número de direcciones IP que admite para cada nombre de host o la compatibilidad con direcciones IPv6. Palo Alto Networks® aprovecha las actualizaciones de contenido para añadir más proveedores de servicio DDNS y facilitar las actualizaciones de sus servicios.

En las configuraciones de alta disponibilidad (high availability, HA), compruebe que las versiones de contenido de los peers del cortafuegos de HA (activo/pasivo o activo/activo) estén sincronizadas, ya que el cortafuegos basa el mantenimiento de la configuración de DDNS en la versión de contenido vigente de Palo Alto Networks. Palo Alto Networks puede modificar o dejar de usar servicios de DDNS disponibles mediante versiones de contenido. Además, los proveedores de DDNS pueden alterar sus servicios. Si no coinciden las versiones de contenido de los peers de HA, pueden tener problemas para utilizar el servicio DDNS.

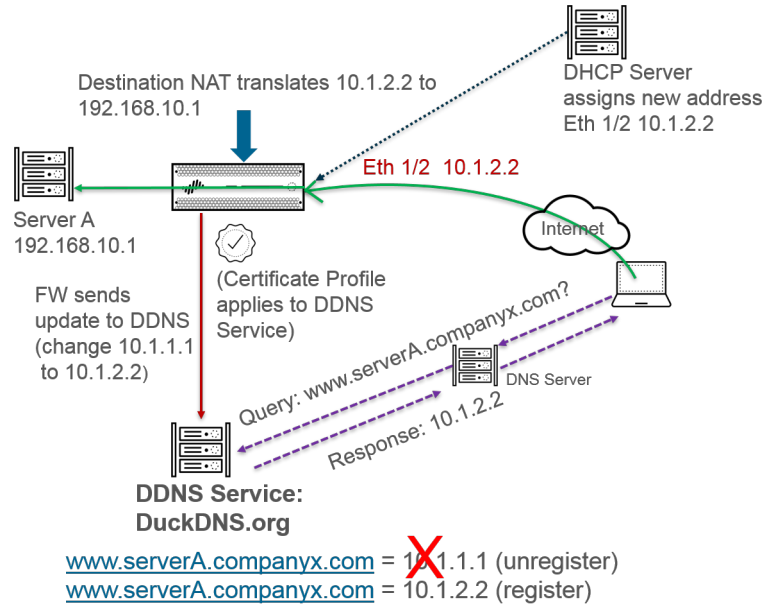
El cortafuegos no admite DDNS en las interfaces que actúan como punto de finalización del protocolo de punto a punto por Ethernet (point-to-point protocol over Ethernet, PPPoE).

En el ejemplo siguiente, el cortafuegos es un cliente DDNS de un proveedor de servicios de DDNS. Al principio, el servidor DHCP asigna la dirección IP 10.1.1.1 a la interfaz Ethernet 1/2. La política de NAT de destino traduce la dirección pública 10.1.1.1 a la auténtica dirección del servidor A (192.168.10.1), situado tras el cortafuegos.



1. Cuando el usuario se intenta poner en contacto con www.serverA.companyx.com, consulta la dirección IP en el servidor DNS local. En este ejemplo, www.serverA.companyx.com (configurado como CNAME en el registro de duckdns.org: serverA.companyx.duckdns.org) es un dominio que pertenece al proveedor de DDNS (Duck DNS). El servidor DNS comprueba el registro con el proveedor de DDNS para resolver la consulta.
2. El servidor DNS responde al usuario con 10.1.1.1, que es la dirección IP de www.serverA.companyx.com.
3. El paquete del usuario cuyo destino es 10.1.1.1 va a la interfaz del cortafuegos Ethernet 1/2.
4. En este ejemplo, el cortafuegos ejecuta la NAT de destino y traduce 10.1.1.1 a 192.168.10.1 antes de enviar el paquete al destino.

Algún tiempo después, DHCP asigna una dirección IP nueva a la interfaz del cortafuegos, lo cual provoca la siguiente actualización de DDNS:



1. El servidor DHCP asigna una dirección IP nueva (10.1.2.2) a Ethernet 1/2.
2. Cuando el cortafuegos recibe esta información, envía una actualización al servicio DDNS con la nueva dirección de www.serverA.companyx.com para que la registre. El cortafuegos también envía actualizaciones periódicas según los intervalos configurados. La actualizaciones de DDNS las envía por el puerto HTTPS 443.

La siguiente vez que el cliente consulta la dirección IP de www.serverA.companyx.com en el servidor DNS, que consulta el servicio DDNS, este envía la dirección actualizada (10.1.2.2). El usuario emplea esa dirección actualizada y logra acceder al servicio o a la aplicación que le interesa por medio de la interfaz del cortafuegos.

Si ha configurado el modo activo/pasivo de HA, el cortafuegos envía las actualizaciones de DDNS al servicio DDNS mientras convergen los estados de ambos cortafuegos. Cuando se alcanza la convergencia, se deshabilita DDNS en el cortafuegos pasivo. Por ejemplo, la primera vez que arrancan dos cortafuegos de HA, ambos envían actualizaciones de DDNS hasta que dilucidan si están en modo activo o pasivo. Mientras tanto, aparecen actualizaciones de DDNS en los logs del sistema. Cuando convergen los estados de HA y cada uno de los cortafuegos notifica a sus clientes si es activo o pasivo, el cortafuegos pasivo deja de enviar actualizaciones de DDNS. En el modo de HA con peers activo/activo, no se sincroniza la configuración de DDNS porque cada cortafuegos tiene la suya propia.

Configuración del DNS dinámico en las interfaces de cortafuegos

Antes de configurar sistemas de nombres de dominio dinámicos (dynamic domain name system, DDNS) en las interfaces de cortafuegos:

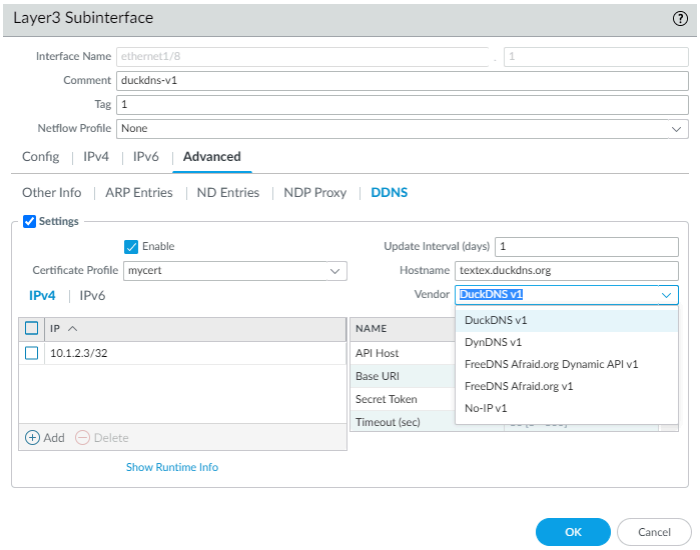
- Averigüe el nombre de host registrado en el proveedor de DDNS.
- Obtenga el certificado SSL público del servicio DDNS e impórtelo al cortafuegos.
- (Con FreeDNS Afraid.org v. 1 o FreeDNS Afraid.org Dynamic API v. 1) En el servidor DDNS, la pestaña de este servicio incluye la opción **Link updates of the same IP together? (Actualizar la misma IP a la vez).** Si la marca, el servicio DDNS actualiza el nombre de host en todos los registros de DNS que contengan la dirección IP antigua que ha cambiado, no solo en el registro de DNS de un nombre de host y una dirección IP únicos. Para evitarlo, quite la marca de la opción **Link updates of the same IP together? (Actualizar la misma IP a la vez)**. De ese modo, el servidor DDNS solo actualiza el registro de DNS que contiene el nombre de host concreto con la nueva dirección IP incluida en la actualización de DDNS.

STEP 1 | Configure DDNS.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz de capa 3, una subinterfaz o una interfaz Ethernet de agregación (AE) o bien seleccione **Network (Red)** > **Interfaces** > **VLAN** y seleccione una interfaz o una subinterfaz.
2. Seleccione **Advanced (Opciones avanzadas)** > **DDNS** y seleccione **Settings (Configuración)**.
3. Marque **Enable (Habilitar)** para habilitar DDNS. Debe habilitar inicialmente DDNS para configurarlo. Si la configuración de su DDNS no está terminada, guárdela sin habilitarla para no perder los cambios realizados hasta el momento.
4. En **Update Interval (days) (Intervalo entre actualizaciones [días])**, introduzca el número de días que debe transcurrir entre los envíos del cortafuegos al servicio DDNS para actualizar las direcciones IP asignadas a los FQDN; el valor predeterminado es 1 y el intervalo, de 1 a 30. Base este intervalo en la frecuencia con la que cambian las direcciones IP. Además de estas actualizaciones, el cortafuegos también envía otras a intervalos periódicos que, por ejemplo, garantizan que no se pierdan las relativas a cambios en las direcciones.
5. En **Hostname (Nombre de host)**, introduzca el nombre de host de la interfaz registrada en el servicio DDNS (por ejemplo, www.serverA.companyx.com o serverA).

   Cerciórese de que es el nombre de host registrado en el servicio DDNS. Debe introducir un FQDN como nombre de host. El cortafuegos no lo valida salvo para confirmar que la sintaxis solo utiliza los caracteres válidos que admite DNS para los nombres de dominio.
6. Seleccione **IPv4** y seleccione una dirección IPv4 o varias que estén asignadas a la interfaz o bien haga clic en **Add (Añadir)** para añadir la dirección IPv4 que desea asociar al nombre de host (por ejemplo, 10.1.1.1). Puede seleccionar tantas direcciones IPv4 como permita el servicio DDNS. Todas las direcciones IPv4 seleccionadas se registran en el servicio DDNS. Seleccione al menos una dirección IPv4 o IPv6.

7. Seleccione **IPv6** y seleccione una dirección IPv6 o varias que estén asignadas a la interfaz o bien haga clic en **Add (Añadir)** para añadir la dirección IPv6 que desea asociar al nombre de host. Puede seleccionar tantas direcciones IPv6 como permita el servicio DDNS. Todas las direcciones IPv6 seleccionadas se registran en el servicio DDNS. Seleccione al menos una dirección IPv4 o IPv6.
8. En **Certificate Profile (Perfil de certificados)**, seleccione o cree un perfil de certificados usando el certificado SSL importado del servicio DDNS para verificarlo cuando el cortafuegos se conecta por primera vez a dicho servicio para registrar alguna dirección IP y en cada actualización. Cuando el cortafuegos se conecta al servicio DDNS para enviar actualizaciones, este le otorga un certificado SSL firmado por la entidad de certificación (certificate authority, CA) con el que se puede autenticar en el servicio.
9. En **Vendor (Proveedor)**, seleccione el proveedor y el número de versión que utiliza para el servicio DDNS.



Palo Alto Networks® puede cambiar los proveedores de servicios de DDNS admitidos mediante una actualización de contenido.

En el campo Vendor (Proveedor), la selección DDNS de Palo Alto Network es un servicio DDNS reservado para funciones de Palo Alto Networks, como SD-WAN y ZTP, y no debe seleccionarse para esta tarea actual. Si selecciona por error DDNS de Palo Alto Networks cuando la función de soporte correspondiente no está habilitada, aparecerá un mensaje de error.

10. La opción seleccionada en Vendor (Proveedor) condiciona los valores que se muestran debajo en los campos **Name (Nombre)** y **Value (Valor)**. Algunos campos de valor son de solo lectura e indican los parámetros que utiliza el cortafuegos para conectarse al servicio DDNS. Configure los demás campos de valores, como la contraseña que proporciona el servicio DDNS y el tiempo de espera que aplica el cortafuegos si no recibe ninguna actualización del servicio DDNS.
11. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Si desea que el cortafuegos se comunique con el servicio DDNS con otra interfaz que no sea la de gestión, configure una ruta de servicio para DDNS; consulte Establecimiento de acceso a la red para servicios externos.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | Consulte la información de DDNS de la interfaz.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** o **Network (Red)** > **Interfaces** > **VLAN** y seleccione la interfaz que ha configurado. Las interfaces que tienen configurado DDNS muestran el icono  en el campo Features (Funciones).
2. Seleccione **Advanced (Opciones avanzadas)** > **DDNS** y marque **Settings (Configuración)**.
3. Haga clic en **Show Runtime Info (Mostrar información de tiempo de ejecución)** para ver los datos de DDNS de la interfaz, entre otros, el código generado con la última actualización de los FQDN o la fecha y la hora cuando el servicio DDNS la ha recibido.

NAT

Esta sección describe la traducción de direcciones de red (Network Address Translation, NAT) y cómo configurar el cortafuegos para NAT. El NAT le permite traducir la direcciones IPv4 privadas y no enrutables a una o más direcciones IPv4 globalmente enrutables, con lo cual se conservan las direcciones IP enrutables de la organización. El NAT le permite no tener que divulgar las direcciones IP reales de los hosts que deben acceder a direcciones públicas y gestionar el tráfico al realizar el reenvío de puertos. Puede usar NAT para resolver dificultades de diseño de la red y permitir que las redes con subredes IP idénticas se comuniquen entre sí. El cortafuegos admite NAT en capa 3 e interfaces de Virtual Wire.

La opción NAT64 traduce entre direcciones IPv4 e IPv6, por lo que ofrece conectividad entre las redes con esquemas de direcciones IP distintas y una ruta de migración hacia las direcciones IPv6. La traducción de prefijo de red IPv6 a IPv6 (NPTv6) traduce un prefijo IPv6 a otro prefijo IPv6. PAN-OS es compatible con todas estas funciones.

Cuando utilice direcciones IP privadas en sus redes internas, deberá utilizar NAT para traducir las direcciones privadas en direcciones públicas que puedan enrutarse a redes externas. En PAN-OS, usted crea reglas de políticas de NAT que indican al cortafuegos qué direcciones de paquetes y puertos necesitan traducción y cuáles son las direcciones y puertos traducidos.

- Reglas de políticas NAT
- NAT de origen y destino
- Casos de uso de NAT de destino con reescritura de DNS
- Capacidades de regla NAT
- Sobresuscripción de NAT de IP dinámica y puerto
- Estadísticas de memoria NAT de plano de datos
- Configuración de NAT
- Ejemplos de configuración de NAT

Reglas de políticas NAT

- Descripción general de la política de NAT
- Grupos de direcciones NAT identificados como objetos de direcciones
- ARP proxy para grupos de direcciones NAT

Descripción general de la política de NAT

Puede configurar una regla NAT que coincida con una zona de origen del paquete y una zona de destino, como mínimo. Además de las zonas, puede configurar criterios equivalentes basados en la interfaz de destino del paquete, la dirección de origen y destino y servicio. Puede configurar múltiples reglas NAT. El cortafuegos evalúa las reglas en orden descendente. Cuando un paquete compara los criterios de una única regla NAT, el paquete no está sujeto a reglas NAT adicionales. Por ello, su lista de reglas NAT debe estar en orden de más a menos específico, de modo que los paquetes estén sujetos a la regla más específica que haya creado para ellos.

Las reglas NAT estáticas no tienen prioridad sobre otras formas de NAT. Por lo tanto, para que la NAT estática funcione, las reglas NAT estática deben estar por encima del resto de reglas NAT en la lista del cortafuegos.

Las reglas NAT ofrecen traducción de direcciones, y son distintas de las reglas de políticas de seguridad, que permiten o deniegan paquetes. Es importante comprender la lógica del flujo del cortafuegos cuando aplica las reglas NAT y las reglas de política de seguridad, de modo que pueda determinar qué reglas necesita en función de las zonas que ha definido. Debe configurar reglas de política de seguridad para permitir el tráfico de NAT.

En la entrada, el cortafuegos examina el paquete y enruta la búsqueda para determinar la interfaz de salida y la zona. Entonces el cortafuegos determina si el paquete coincide con alguna de las reglas NAT que se han definido, basándose en la zona de origen o destino. A continuación, evalúa y aplica las políticas de seguridad que coincidan con el paquete basándose en las direcciones de origen y destino originales (anteriores a NAT), pero en las zonas posteriores a NAT. Por último, en la salida cuando una de las reglas NAT coincide, el cortafuegos traduce las direcciones y números de puerto de origen y de destino.

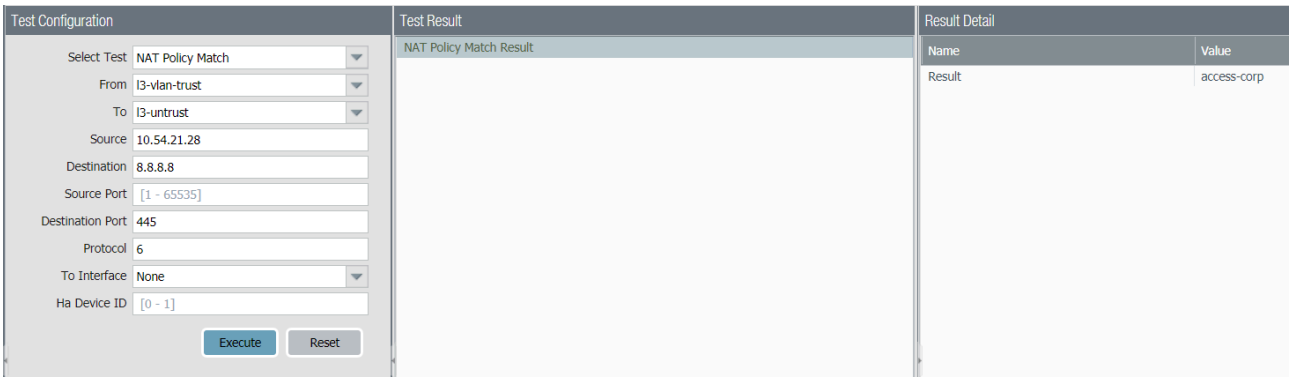
Tenga en cuenta que la traducción de la dirección IP y el puerto no se produce hasta que el paquete sale del cortafuegos. Las reglas y políticas de seguridad NAT se aplican a la dirección IP original (la dirección anterior a NAT). Una regla NAT se configura en función de la zona asociada con una dirección IP anterior a NAT.

Las políticas de seguridad difieren de las reglas NAT en que examinan las zonas anteriores a NAT para determinar si se permite o no el paquete. Como la naturaleza de NAT es modificar las direcciones IP de origen o destino, lo que puede provocar que se modifique la zona y la interfaz saliente del paquete, las políticas de seguridad se aplican en la zona posterior a NAT.

Una llamada SIP en ocasiones experimenta un audio unidireccional cuando atraviesa el cortafuegos, debido a que el administrador de llamadas envía un mensaje de SIP en reemplazo del teléfono para establecer la conexión. Cuando el mensaje del administrador de llamadas llega al cortafuegos, el SIP ALG debe colocar la dirección IP del teléfono a través de NAT. Si el administrador de llamadas y los teléfonos no están en la misma zona de seguridad, la búsqueda de NAT de la dirección IP del teléfono se realiza usando la zona del administrador de llamadas. La política de NAT debe tener esto en cuenta.

Las reglas no NAT están configuradas para permitir la exclusión de direcciones IP definidas en el intervalo de las reglas NAT definidas posteriormente en la política NAT. Para definir una política no NAT, especifique todos los criterios coincidentes y seleccione Sin traducción de origen en la columna de traducción de origen.

Si desea verificar las reglas de NAT procesadas, seleccione **Device (Dispositivo)** > **Troubleshooting (Solución de problemas)** y compruebe las coincidencias del tráfico con ellas. Por ejemplo:



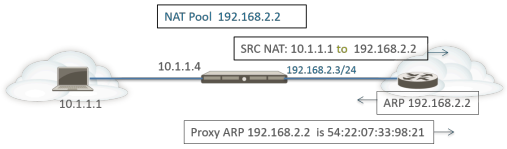
Grupos de direcciones NAT identificados como objetos de direcciones

Al configurar un grupo de direcciones NAT de **Dynamic IP** o **Dynamic IP and Port** en una regla de políticas NAT, lo habitual es configurar el grupo de direcciones traducidas con un objeto de dirección. Cada objeto de dirección puede ser una dirección IP de host, un intervalo de direcciones IP o una subred de IP.

Debido a que tanto las reglas NAT como las reglas de política de seguridad usan objetos de dirección, lo mejor es distinguirlas nombrando al objeto de dirección que se usa para NAT con un prefijo, como por ejemplo "nombre NAT".

ARP proxy para grupos de direcciones NAT

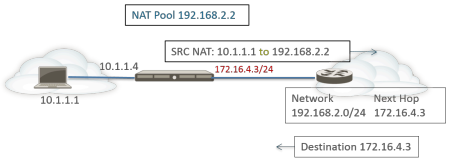
Los grupos de direcciones NAT no están vinculados a ninguna interfaz. La figura siguiente ilustra el comportamiento del cortafuegos cuando realiza ARP proxy para una dirección en un grupo de direcciones NAT.



El cortafuegos realiza NAT de origen para un cliente, traduciendo la dirección de origen 10.1.1.1 a la dirección en el grupo NAT, 192.168.2.2. El paquete traducido se envía a un enrutador.

Para el tráfico de retorno, el enrutador no sabe cómo llegar a 192.168.2.2 (porque la dirección IP solo es una dirección en el grupo de direcciones NAT), de modo que envía un paquete de solicitud de ARP al cortafuegos.

- Si el grupo de direcciones (192.168.2.2) está en la misma subred que la dirección IP de interfaz de entrada/salida (192.168.2.3/24), el cortafuegos puede enviar una respuesta de ARP proxy al enrutador, que indica la dirección MAC de capa 2 de la dirección IP, como muestra la figura anterior.
- Si el grupo de direcciones (192.168.2.2) no es una subred de una interfaz en el cortafuegos, el cortafuegos no enviará una respuesta ARP proxy al enrutador. Esto significa que el enrutador debe estar configurado con la ruta necesaria para saber a dónde enviar los paquetes destinados a 192.168.2.2, con el fin de garantizar que el tráfico de retorno se enruta de regreso al cortafuegos, como se muestra en la figura siguiente.



NAT de origen y destino

El cortafuegos admite tanto la traducción de puerto y/o dirección de origen como la traducción de puerto y/o dirección de destino.

- NAT de origen
- NAT de destino

NAT de origen

Los usuarios internos suelen usar el NAT de origen para acceder a Internet; la dirección de origen de traduce y se mantienen en privado. Hay tres tipos de NAT de origen:

- **IP y puerto dinámico (DIPP)**: Permite que múltiples hosts traduzcan sus direcciones IP de origen a la misma dirección IP pública con distintos números de puerto. La traducción dinámica es a la siguiente dirección disponible en el grupo de direcciones NAT, que configura como un grupo de **Dirección traducida** para dirección IP, intervalo de direcciones, subred o combinación de todas.

  Como alternativa al uso de la siguiente dirección en el grupo de direcciones NAT, el DIPP le permite especificar la dirección de la propia **interfaz**. La ventaja de especificar la interfaz de la regla NAT es que la regla NAT se actualizará automáticamente para utilizar cualquier dirección que adquiera la interfaz a continuación. DIPP también se conoce como NAT basada en interfaz o traducción de puertos de direcciones de red (NAPT).

  DIPP tiene una ratio predeterminada de sobresuscripción NAT, es decir, el número de ocasiones en las que el mismo par de dirección IP y puerto traducido se pueden usar de forma simultánea. Para obtener más información, consulte Sobresuscripción de NAT de IP dinámica y puerto y Modificación de la ratio de sobresuscripción para NAT DIPP.

  > ***(** Afecta solo a los cortafuegos PA-7000 Series que no usan tarjetas de gestión de conmutadores PA-7050-SMC-B o PA-7080-SMC-B de segunda generación**) Cuando use el protocolo de túnel punto a punto (Point-to-Point Tunnel Protocol, PPTP) con NAT DIPP, el cortafuegos se limitará a usar un par de puerto y dirección IP traducidos para una sola conexión; el cortafuegos no es compatible con NAT DIPP. La solución alternativa es actualizar el cortafuegos de PA-7000 Series a una tarjeta SMC-B de segunda generación.***

- **IP dinámica**: Permite una traducción dinámica 1 a 1 de una dirección IP de origen únicamente (sin número de puerto) a la siguiente traducción disponible en el grupo de direcciones NAT. El tamaño del grupo de NAT debe ser igual al número de hosts internos que requieren traducciones de red. Por defecto, si el grupo de direcciones de origen es mayor que el de direcciones NAT y en un momento dado se asignan todas las direcciones NAT, se descartan las nuevas conexiones que necesiten una traducción de la dirección. Para anular este comportamiento por defecto, use **Advanced (Dynamic IP/Port Fallback)** para habilitar el uso de direcciones DIPP cuando sea necesario. En cualquiera de los dos casos, a medida que las sesiones terminan y las direcciones en el grupo están disponibles, pueden asignarse para traducir nuevas conexiones.

  NAT de IP dinámica admite la opción de realizar una Reserva de direcciones NAT de IP dinámicas.

- **IP estática**: Permite la traducción estática 1 a 1 de una dirección IP de origen, pero deja el puerto de origen sin modificar. Una situación común en la que se traduce una IP estática es un servidor interno que debe estar disponible en Internet.

NAT de destino

La traducción de direcciones de red (network address translation, NAT) de destino se ejecuta en los paquetes entrantes cuando el cortafuegos traduce una dirección de destino a otra distinta; por ejemplo, traduce una dirección de destino pública a una privada. El NAT de destino también ofrece la opción para realizar reenvío o traducción de puertos.

El NAT de destino permite la traducción estática y dinámica:

- **Static IP (IP estática)**: puede configurar una traducción estática de uno a uno en varios formatos. Puede especificar que el paquete original tenga una dirección IP de destino única, un intervalo de direcciones IP o una máscara de red IP, siempre que el paquete traducido esté en el mismo formato y especifique la misma cantidad de direcciones IP. El cortafuegos traduce estáticamente una dirección de destino original a la misma dirección de destino traducida cada vez. Es decir, si hay más de una dirección de destino, el cortafuegos traduce la primera dirección de destino configurada para el paquete original a la primera dirección de destino configurada para el paquete traducido, y traduce la segunda dirección de destino original configurada a la segunda dirección de destino traducida configurada, y así sucesivamente, y siempre utiliza la misma traducción.

  Si utiliza la NAT de destino para traducir direcciones IPv4 estáticas, también puede recurrir a los servicios de DNS de un lado del cortafuegos para resolver los FQDN de clientes del otro lado. Cuando la respuesta de DNS que contiene la dirección IPv4 atraviesa el cortafuegos, el servidor DNS proporciona una dirección IP interna a un dispositivo externo, o al contrario. Desde PAN-OS 9.0.2 (y en las versiones 9.0 posteriores), puede configurar el cortafuegos para que reescriba la dirección IP de la respuesta de DNS (que coincide con la regla). De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino. El caso de uso de reescritura de DNS aplicable determina cómo se configura.
- **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])**: la NAT de destino permite traducir la dirección de destino original a un host o servidor de destino que tiene una dirección IP dinámica, es decir, un objeto de dirección que utiliza un FQDN, que puede devolver varias direcciones desde DNS. La IP dinámica con distribución de sesiones solo admite direcciones IPv4. La NAT de destino con una dirección IP dinámica resulta de especial utilidad en implementaciones en la nube que utilizan direcciones IP dinámicas.

  Si la dirección de destino traducida se resuelve en más de una dirección, el cortafuegos distribuye las sesiones de NAT entrantes entre todas a fin de mejorar el rendimiento. La distribución se basa en alguno de estos métodos: turnos (predeterminado), hash de IP de origen, módulo de IP, hash de IP o menos sesiones. Si el servidor DNS devuelve más de 32 direcciones IPv4 para un FQDN, el cortafuegos utiliza las 32 primeras del paquete.

  Si la dirección traducida es un objeto de dirección del tipo FQDN que solo se resuelve en direcciones IPv6, la regla de la política de NAT de destino considera que no se ha resuelto el FQDN.

  Utilizar la opción de **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])** le permite traducir varias direcciones IP de destino previas a la NAT ***M*** a varias direcciones IP de destino posteriores a la NAT ***N***. Una traducción de varios a varios implica que puede haber ***M*** x ***N*** traducciones de NAT de destino utilizando una regla de NAT.

Para el destino NAT, se recomienda lo siguiente:

- *Utilice la traducción de direcciones **IP estáticas** para las direcciones IP estáticas. De esa forma, el cortafuegos comprobará que el número de direcciones IP de destino originales sea igual al número de direcciones IP de destino traducidas y se asegurará de ello.*
- *Utilice la traducción de direcciones de **IP dinámicas (con distribución de sesiones)** solo para direcciones dinámicas basadas en FQDN (el cortafuegos no realiza una comprobación del número de direcciones IP).*

A continuación, se muestran ejemplos comunes de traducciones de NAT de destino que permite el cortafuegos:

Tipo de traducción	Dirección de destino del paquete original	Se asigna a la dirección de destino del paquete traducido	Notas
IP estática	192.168.1.1	2.2.2.2	El paquete original y el paquete traducido tienen una dirección de destino posible.
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	El paquete original y el paquete traducido tienen cuatro direcciones de destino posibles: 192.168.1.1 siempre se asigna a 2.2.2.1 192.168.1.2 siempre se asigna a 2.2.2.2 192.168.1.3 siempre se asigna a 2.2.2.3 192.168.1.4 siempre se asigna a 2.2.2.4
	192.168.1.1/30	2.2.2.1/30	El paquete original y el paquete traducido tienen cuatro direcciones de destino posibles: 192.168.1.1 siempre se asigna a 2.2.2.1 192.168.1.2 siempre se asigna a 2.2.2.2 192.168.1.3 siempre se asigna a 2.2.2.3

Tipo de traducción	Dirección de destino del paquete original	Se asigna a la dirección de destino del paquete traducido	Notas
			192.168.1.4 siempre se asigna a 2.2.2.4
IP dinámica (con distribución de sesiones)	192.168.1.1/30	domainname.com	El paquete original posee cuatro direcciones de destino y si, por ejemplo, el FQDN en la dirección de destino traducida dirige a cinco direcciones IP, existen 20 posibles traducciones de NAT de destino en una regla de NAT.

Un uso común de la NAT de destino es configurar varias reglas NAT que asignen una dirección de destino pública única a varias direcciones de host de destino privadas a servidores o servicios. En este caso, los números de puerto de destino se usan para identificar a los hosts de destino. Por ejemplo:

- **Reenvío de puertos**: Puede traducir una dirección de destino pública y un número de puerto a una dirección de destino privada, pero mantener el mismo número de puerto.
- **Traducción de puertos**: Puede traducir una dirección de destino pública y un número de puerto a una dirección de destino privada y un número de puerto distinto, con lo que el número de puerto real es privado. La traducción de puertos se configura introduciendo un **Translated Port (Puerto traducido)** en la pestaña **Translated Packet (Paquete traducido)** de la regla de política de NAT. Consulte NAT de destino con ejemplo de traducción de puerto.

Casos de uso de NAT de destino con reescritura de DNS

Cuando utiliza la traducción de direcciones de red (network address translation, NAT) de destino para ejecutar la traducción estática de direcciones IPv4 a otras del mismo tipo, es posible que también esté usando servicios de DNS de un lado del cortafuegos para resolver los FQDN de los clientes. Cuando la respuesta de DNS que contiene la dirección IP atraviesa el cortafuegos para dirigirse al cliente, el cortafuegos no realiza la NAT en esa dirección IP. Por eso, el servidor DNS proporciona una dirección IP interna a un dispositivo externo, o al contrario. En ese caso, el cliente DNS no logra conectar al servicio de destino.

Para evitar ese problema, puede configurar el cortafuegos para que reescriba la dirección IP de la respuesta de DNS (del registro A) basándose en la dirección IP traducida que haya configurado en la regla de la política de NAT. El cortafuegos ejecuta la NAT de la dirección IPv4 (es decir, la resolución del FQDN) incluida en la respuesta de DNS antes de reenviar esta al cliente. De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino. Basta una sola regla de la política de NAT para que el cortafuegos ejecute la NAT en los paquetes que coincidan con ella, así como en las direcciones IP incluidas en las respuestas de DNS que coincidan con la dirección de destino original o la dirección de destino traducida de la regla.

La reescritura de DNS se produce a nivel global; el cortafuegos asigna la dirección de destino en la pestaña Original Packet (Paquete original) a la dirección de destino en la pestaña Translated Packet (Paquete traducido). Todos los demás campos de la pestaña Original Packet (Paquete original) se ignoran. Cuando llega un paquete de respuesta de DNS, el cortafuegos verifica si la respuesta contiene algún registro A que coincida con una de las direcciones de destino asignadas según la dirección de la siguiente manera.

Debe especificar cómo el cortafuegos ejecuta NAT en la dirección IP en la respuesta de DNS relacionada con la regla de NAT: **reverse (inverso)** o **forward (directo)**:

- **reverse (inverso)**: si la respuesta de DNS coincide con la dirección de destino **traducida** en la regla, traduzca la respuesta de DNS mediante la traducción inversa que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP **1.1.1.10 a 192.168.1.10**, el cortafuegos reescribe una respuesta de DNS de **192.168.1.10 a 1.1.1.10**.
- **forward (directo)**: si el paquete es una respuesta de DNS que coincide con la dirección de destino **original** en la regla, traduzca la respuesta de DNS mediante la misma traducción que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP **1.1.1.10 a 192.168.1.10**, el cortafuegos reescribe una respuesta de DNS de **1.1.1.10 a 192.168.1.10**.

Si una regla de NAT está superpuesta y tiene deshabilitada la reescritura de DNS y una regla de NAT inferior incluida en la superposición sí la tiene habilitada, el cortafuegos reescribe la respuesta de DNS conforme a la regla de NAT inferior en sentido inverso o directo, según se especifique. Tiene prioridad la reescritura, así que se ignora el orden de las reglas de NAT.

Cuando configure la reescritura de DNS, tenga en cuenta estos casos de uso:

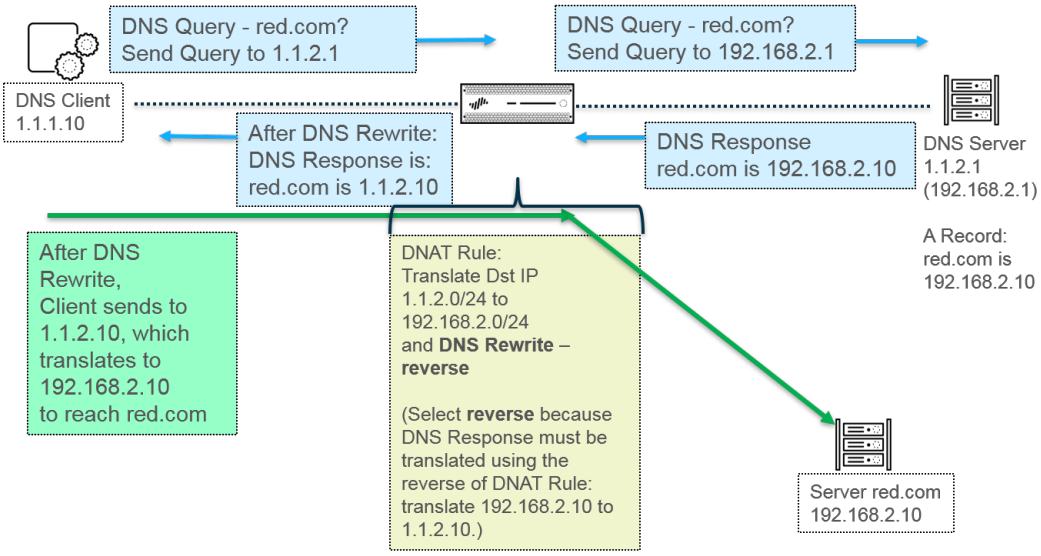
- Casos de uso de NAT de destino con reescritura inversa de DNS
- Casos de uso de NAT de destino con reescritura directa de DNS

Casos de uso de NAT de destino con reescritura inversa de DNS

En los siguientes casos de uso se ilustra la traducción de direcciones de red (network address translation, NAT) de destino con reescritura de DNS habilitada en sentido **inverso**. La única diferencia entre ambos estriba en si el cliente DNS, el servidor DNS y el servidor de destino están en el lado público o el interno del cortafuegos. La similitud en ambos es que el cliente DNS se encuentra en el lado del cortafuegos opuesto al del servidor de destino último. Si el cliente y ese servidor están en el mismo lado, consulte los casos 3 y 4 de Casos de uso de NAT de destino con reescritura directa de DNS.

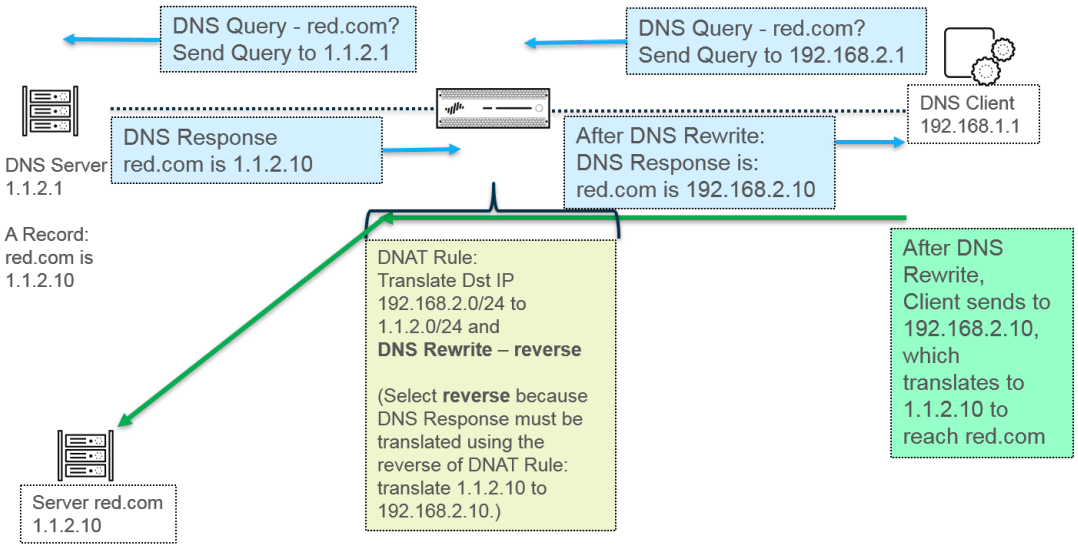
En este primer caso de uso, el cliente DNS está en el lado público del cortafuegos, en tanto que el servidor DNS y el servidor de destino último se encuentran en el lado interno. En este caso se necesita la reescritura de DNS en sentido inverso. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla de NAT para traducir la consulta (que se dirigía originalmente a la dirección pública 1.1.2.1) a la dirección interna 192.168.2.1. El servidor DNS responde que red.com tiene la dirección IP 192.168.2.10. Como la regla incluye **Enable DNS Rewrite - reverse (Habilitar reescritura de DNS: [Sentido] inverso)** y la respuesta de DNS 192.168.2.10 coincide con la dirección traducida de destino 192.168.2.0/24 de la regla, el cortafuegos traduce la respuesta de DNS con la traducción **inversa** que emplea la regla. La regla indica que se traduzca 1.1.2.0/24 a 192.168.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 192.168.2.10 a 1.1.2.10. El cliente DNS recibe la respuesta y realiza el envío a 1.1.2.10, que la regla traduce a 192.168.2.10 para acceder al servidor de red.com.

Resumen del caso de uso 1: el cliente DNS y el servidor de destino están en lados opuestos del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino traducida de la regla de NAT, es decir, convierte la respuesta de DNS usando la traducción **inversa** de dicha regla.



En este segundo caso de uso, el cliente DNS está en el lado interno del cortafuegos, en tanto que el servidor DNS y el servidor de destino último se encuentran en el lado público. En este caso se necesita la reescritura de DNS en sentido inverso. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla de NAT para traducir la consulta (que se dirigía originalmente a la dirección interna 192.168.2.1) a la dirección pública 1.1.2.1. El servidor DNS responde que red.com tiene la dirección IP 1.1.2.10. Como la regla incluye **Enable DNS Rewrite - reverse (Habilitar reescritura de DNS: [Sentido] inverso)** y la respuesta de DNS 1.1.2.10 coincide con la dirección traducida de destino 1.1.2.0/24 de la regla, el cortafuegos traduce la respuesta de DNS con la traducción **inversa** que emplea la regla. La regla indica que se traduzca 192.168.2.0/24 a 1.1.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 1.1.2.10 a 192.168.2.10. El cliente DNS recibe la respuesta y realiza el envío a 192.168.2.10, que la regla traduce a 1.1.2.10 para acceder al servidor de red.com.

El resumen del caso de uso 2 es idéntico al del caso 1: el cliente DNS y el servidor de destino están en lados opuestos del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino traducida de la regla de NAT, es decir, convierte la respuesta de DNS usando la traducción **inversa** de dicha regla.



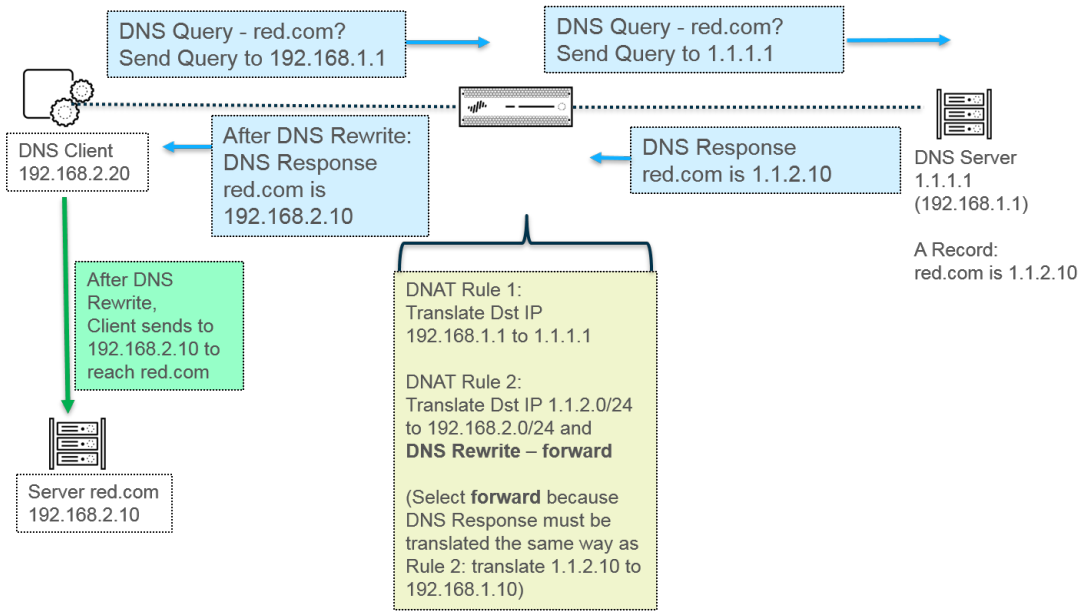
Para implementar la reescritura de DNS, realice el procedimiento Configuración de la NAT de destino con reescritura de DNS.

Casos de uso de NAT de destino con reescritura directa de DNS

En los siguientes casos de uso se ilustra la traducción de direcciones de red (network address translation, NAT) de destino con reescritura de DNS habilitada en sentido **directo**. La única diferencia entre ambos estriba en si el cliente DNS, el servidor DNS y el servidor de destino están en el lado público o el interno del cortafuegos. La similitud en ambos es que el cliente DNS se encuentra en el mismo lado del cortafuegos que el servidor de destino último. Si el cliente y ese servidor están en lados opuestos, consulte los casos 1 y 2 de Casos de uso de NAT de destino con reescritura inversa de DNS.

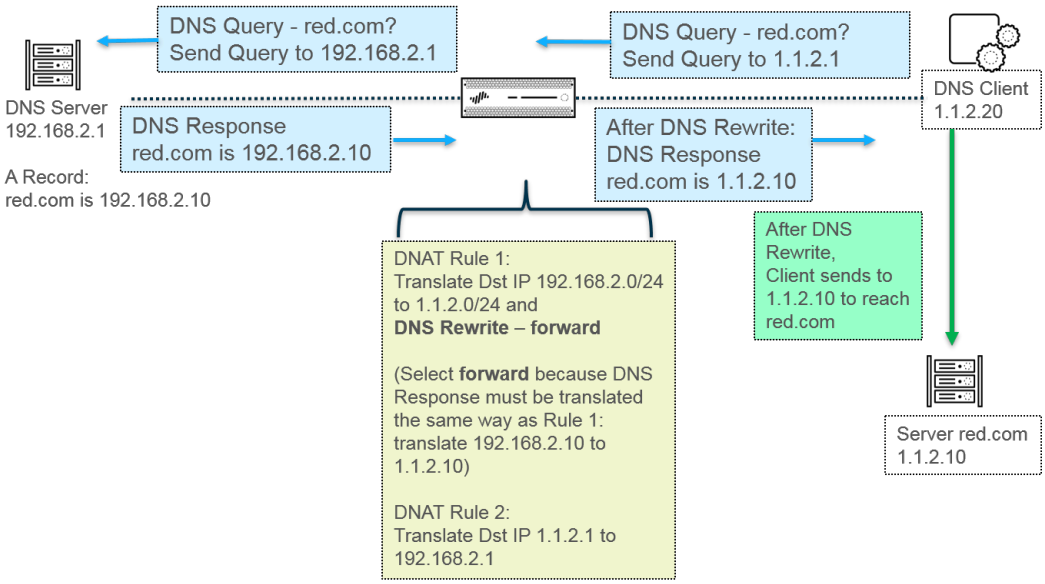
En este tercer caso de uso, el cliente DNS y el servidor de destino último están en el lado interno del cortafuegos, en tanto que el servidor DNS se encuentra en el lado público. En este caso se necesita la reescritura de DNS en sentido directo. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla 1 para traducir la consulta (que se dirigía originalmente a la dirección interna 192.168.1.1) a 1.1.1.1. El servidor DNS responde que red.com tiene la dirección IP 1.1.2.10. Como la regla 2 incluye **Enable DNS Rewrite - forward (Habilitar reescritura de DNS: [Sentido] directo)** y la respuesta de DNS 1.1.2.10 coincide con la dirección de destino original 1.1.2.0/24 de la regla 2, el cortafuegos traduce la respuesta de DNS con la **misma** traducción que emplea la regla. La regla 2 indica que se traduzca 1.1.2.0/24 a 192.168.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 1.1.2.10 a 192.168.2.10. El cliente DNS recibe la respuesta y realiza el envío a 192.168.2.10 para acceder al servidor de red.com.

Resumen del caso de uso 3: el cliente DNS y el servidor de destino están en el mismo lado del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino original de la regla de NAT, es decir, convierte la respuesta de DNS usando la misma traducción (**directa**) de dicha regla.



En este cuarto caso de uso, el cliente DNS y el servidor de destino último están en el lado público del cortafuegos, en tanto que el servidor DNS se encuentra en el lado interno. En este caso se necesita la reescritura de DNS en sentido directo. El cliente DNS consulta la dirección IP de red.com. El cortafuegos se basa en la regla 2 para traducir la consulta (que se dirigía originalmente al destino público 1.1.2.1) a 192.168.2.1. El servidor DNS responde que red.com tiene la dirección IP 192.168.2.10. Como la regla 1 incluye **Enable DNS Rewrite - forward (Habilitar reescritura de DNS: [Sentido] directo)** y la respuesta de DNS 192.168.2.10 coincide con la dirección de destino original 192.168.2.0/24 de la regla 1, el cortafuegos traduce la respuesta de DNS con la **misma** traducción que emplea la regla. La regla 1 indica que se traduzca 192.168.2.0/24 a 1.1.2.0/24, así que el cortafuegos reescribe la respuesta de DNS de 192.168.2.10 a 1.1.2.10. El cliente DNS recibe la respuesta y realiza el envío a 1.1.2.10 para acceder al servidor de red.com.

El resumen del caso de uso 4 es idéntico al del caso 3: el cliente DNS y el servidor de destino están en el mismo lado del cortafuegos. El servidor DNS proporciona una dirección que coincide con la dirección de destino original de la regla de NAT, es decir, convierte la respuesta de DNS usando la misma traducción (**directa**) de dicha regla.



Para implementar la reescritura de DNS, realice el procedimiento Configuración de la NAT de destino con reescritura de DNS.

Capacidades de regla NAT

La cantidad de reglas NAT permitidas se basan en el modelo del cortafuegos. Los límites de reglas individuales se definen para la NAT de IP dinámica (DIP) e IP dinámica y puerto (DIPP). La suma del número de reglas usadas para estos tipos de NAT no puede superar la capacidad total de reglas NAT. Para DIPP, el límite de reglas se basa en el ajuste de sobresuscripción (8, 4, 2 o 1) del cortafuegos y la suposición de una dirección IP traducida por regla. Para ver los límites de las reglas NAT y los límites de direcciones IP traducidas específicos de cada modelo, utilice la herramienta de Comparación de cortafuegos.

Considere lo siguiente cuando trabaje con reglas NAT:

- Si se queda sin recursos de grupo, no podrá crear más reglas NAT, aunque no se haya alcanzado el recuento máximo de reglas del modelo.
- Si consolida las reglas NAT, el logging e informes se consolidarán también. Las estadísticas se proporcionan por regla, no para todas las direcciones de la regla. Si necesita logging e informes granulares, no combine las reglas.

Sobresuscripción de NAT de IP dinámica y puerto

El NAT de IP dinámica y puerto (DIPP) le permite usar cada par de dirección IP y puerto traducidos varias veces (8, 4 o 2 veces) en sesiones simultáneas. Esta capacidad de reutilización de una dirección IP y puerto (conocida como sobresuscripción) ofrece escalabilidad a los clientes que tengan muy pocas direcciones IP públicas. El diseño se basa en el supuesto de que los hosts se conectan a distintos destinos, por lo que las sesiones pueden identificarse de forma única, con pocas posibilidades de colisiones. En efecto, la ratio de sobresuscripción multiplica el tamaño original del grupo de direcciones/puertos por 8, por 4 o por 2. Por ejemplo, el límite predeterminado de 64 000 sesiones simultáneas, si se multiplica por una ratio de sobresuscripción de 8, da lugar a 512 000 sesiones simultáneas.

Las tasas de sobresuscripción permitidas varían según el modelo. La tasa de sobresuscripción es global y se aplica al cortafuegos. Esta ratio de sobresuscripción se define por defecto y consume memoria, aunque tenga disponibles suficientes direcciones IP públicas para que la sobresuscripción sea innecesaria. Puede reducir la ratio del ajuste predeterminado a uno inferior, o incluso a 1 (que significa sin sobresuscripción). Al configurar una ratio reducida, está reduciendo el número de traducciones de dispositivo de origen posibles, pero aumentando la capacidad de reglas NAT DIP y DIPP. Para cambiar la ratio predeterminada, consulte Modificación de la ratio de sobresuscripción para NAT DIPP.

Si selecciona **Platform Default (Valor predeterminado de plataforma)**, se desactivará su configuración explícita de sobresuscripción y se aplicará el valor predeterminado para el modelo, tal y como se muestra en la siguiente tabla. El ajuste **Valor predeterminado de plataforma** le permite actualizar la licencia de software o cambiar a una menor.

La siguiente tabla muestra la tasa predeterminada (más alta) de sobresuscripción para cada modelo.

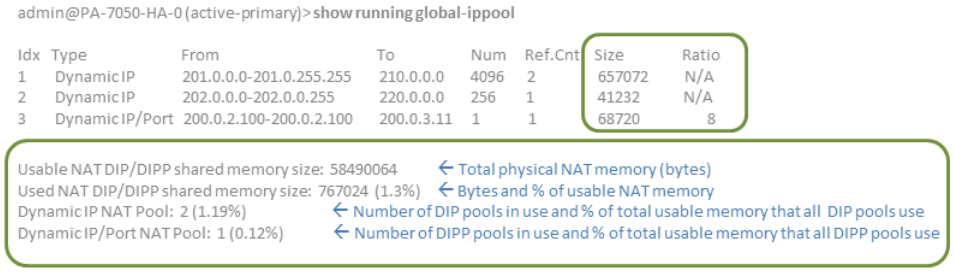
Modelo	Ratio de sobresuscripción predeterminada
PA-220	2
PA-820	2
PA-850	2
PA-3220	4
PA-3250	4
PA-3260	4
PA-5220	8
PA-5250	8
PA-5260	8
PA-5280	8

Modelo	Ratio de sobresuscripción predeterminada
PA-7050	8
PA-7080	8
VM-50	2
VM-100	2
VM-200	2
VM-300	2
VM-500	8
VM-700	8
VM-1000-HV	2

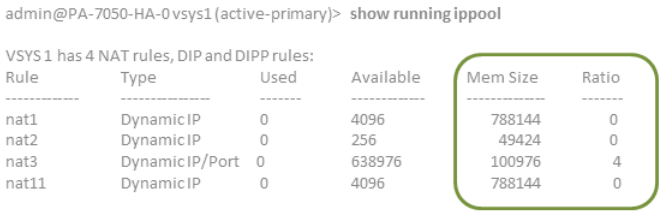
El cortafuegos admite un máximo de 256 direcciones IP traducidas por regla NAT y cada modelo admite una cantidad máxima de direcciones IP traducidas (para todas las reglas NAT combinadas). Si la sobresuscripción provoca que se supere el máximo de direcciones traducidas por regla (256), el cortafuegos reducirá automáticamente la tasa de sobresuscripción en un intento de que funcione la compilación. Sin embargo, si sus reglas NAT generan traducciones que superan el máximo de direcciones traducidas para el modelo, la confirmación fallará.

Estadísticas de memoria NAT de plano de datos

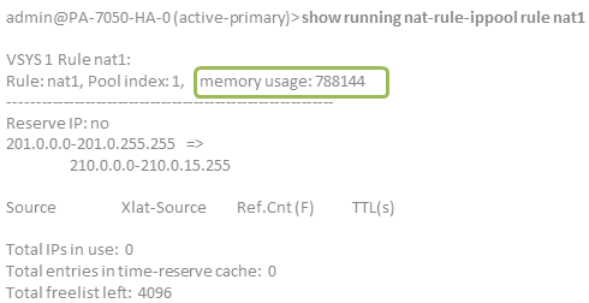
El comando **show running global-ippool** muestra estadísticas relacionadas con el consumo de memoria NAT de un grupo. La columna Tamaño muestra el número de bytes de memoria que está usando el grupo de recursos. La columna Tasa muestra la tasa de sobresuscripción (solo para grupos DIPP). Las líneas de grupos y estadísticas de memoria se explican en los siguientes resultados de muestras:



Para las estadísticas de grupo NAT de un sistema virtual, el comando **show running ippool** tiene comandos que indican el tamaño de memoria usado por la regla NAT y la tasa de sobresuscripción usada (para reglas DIPP). La siguiente es una muestra de resultados del comando.



Un campo del resultado del comando **show running nat-rule-ippool rule** muestra la memoria (bytes) usada por regla NAT. El siguiente es una ejemplo de resultados del comando con el uso de memoria de la regla rodeado.

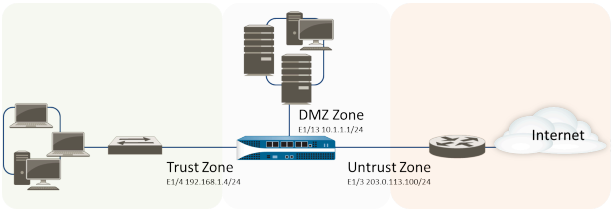


Configuración de NAT

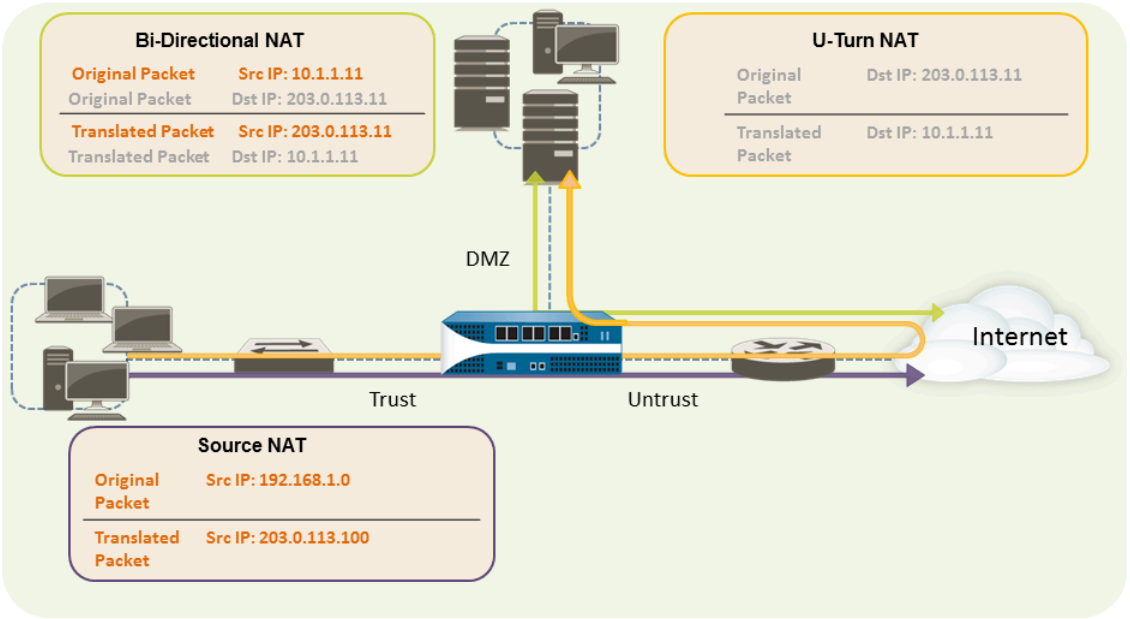
Realice las siguientes tareas para configurar varios aspectos del NAT. Además de los ejemplos siguientes, hay otros en la sección Ejemplos de configuración de NAT.

- Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen)
- Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino)
- Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática)
- Configuración de la NAT de destino con reescritura de DNS
- Configuración de NAT de destino utilizando direcciones IP dinámicas
- Modificación de la ratio de sobresuscripción para NAT DIPP
- Reserva de direcciones NAT de IP dinámicas
- Deshabilitación de NAT para un host o interfaz específico

Los primeros tres ejemplos de NAT en esta sección se basan en la siguiente topología:



En función de esta topología, se deben crear tres políticas de NAT de la siguiente manera:



- Para permitir que los clientes de la red interna accedan a recursos en Internet, las direcciones 192.168.1.0 internas deberán traducirse a direcciones enrutables públicamente. En este caso, configuraremos NAT de origen (el cuadro y la fecha púrpuras en la imagen anterior) utilizando la

dirección de interfaz de salida, 203.0.113.100, como la dirección de origen en todos los paquetes que salgan del cortafuegos desde la zona interna. Consulte Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen) para obtener las instrucciones.

- Para permitir que los clientes de la red interna accedan al servidor web público en la zona DMZ, debemos configurar una regla NAT que redirija el paquete desde la red externa, donde la búsqueda de tabla de enrutamiento original determinará que debe ir, basándose en la dirección de destino de 203.0.113.11 dentro del paquete, a la dirección real del servidor web de la red DMZ de 10.1.1.11. Para ello, deberá crear una regla NAT desde la zona fiable (donde se encuentra la dirección de origen del paquete) hasta la zona no fiable (donde se encuentra la dirección de destino) para traducir la dirección de destino a una dirección de la zona DMZ. Este tipo de NAT de destino se denomina ***NAT de ida y vuelta*** (el cuadro y la flecha amarillos en la imagen anterior). Consulte Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino) para obtener las instrucciones.
- Para permitir que el servidor web (que tiene tanto una dirección IP privada en la red DMZ como una dirección pública para que accedan usuarios externos) envíe y reciba solicitudes, el cortafuegos debe traducir los paquetes entrantes desde la dirección IP pública hacia la dirección IP privada y los paquetes salientes desde la dirección IP privada hacia la dirección IP pública. En el cortafuegos, puede lograr esto con una única política NAT de origen estática bidireccional (el cuadro y la flecha verdes de la imagen anterior). Consulte Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática).

Traducción de direcciones IP de clientes internos a su dirección IP pública (NAT DIPP de origen)

Cuando un cliente de su red interna envía una solicitud, la dirección de origen del paquete contiene la dirección IP del cliente de su red interna. Si utiliza intervalos de direcciones IP privadas, los paquetes del cliente no se podrán enrutar en Internet a menos que traduzca la dirección IP de origen de los paquetes que salen de la red a una dirección enrutable públicamente.

En el cortafuegos, puede realizar esta acción configurando una política NAT de origen que traduzca la dirección de origen (y opcionalmente el puerto) a una dirección pública. Un modo de hacerlo es traducir la dirección de origen de todos los paquetes a la interfaz de salida de su cortafuegos, como se muestra en el procedimiento siguiente.

STEP 1 | Cree un objeto de dirección para la dirección IP externa que tenga la intención de utilizar.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y **Add (Añadir)** para añadir un nombre en **Name (Nombre)** y una descripción opcional en **Description (Descripción)** para el objeto.
2. Seleccione **IP Netmask (Máscara de red de IP)** en **Type (Tipo)** y, a continuación, introduzca la dirección IP de la interfaz externa del cortafuegos (203.0.113.100 en este ejemplo).
3. Haga clic en **OK (Aceptar)**.

Aunque no tiene que utilizar objetos de dirección en sus políticas, es una práctica recomendada porque simplifica la administración al permitirle realizar actualizaciones en un lugar en vez de tener que actualizar cada política donde se hace referencia a la dirección.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la política.
3. (Opcional) Introduzca una etiqueta, que es una palabra clave o frase que le permite ordenar o filtrar políticas.
4. Para **NAT Type**, seleccione **ipv4** (opción por defecto).
5. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
6. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **Dynamic IP And Port (IP y puerto dinámicos)** en la lista **Translation Type (Tipo de traducción)** de la sección Source Address Translation (Traducción de dirección de origen).
7. Para **Address Type**, hay dos opciones. Puede seleccionar **Translated Address** y luego hacer clic en **Add**. Seleccione el objeto de dirección que acaba de crear.

   Un **Address Type (Tipo de dirección)** alternativo es una **Interface Address (Dirección de interfaz)** en la que la dirección traducida será la dirección IP de la interfaz. Para esta opción, debe seleccionar **Interface** y opcionalmente una **IP Address** si la interfaz tiene más de una dirección IP.
8. Haga clic en **OK (Aceptar)**.

STEP 3 | Confirme los cambios.

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

STEP 4 | (Opcional) Acceda a la CLI para verificar la traducción.

1. Use el comando **`show session all`** para ver la tabla de sesión, donde puede comprobar el puerto y la dirección IP y el puerto y dirección IP traducidos correspondientes.
2. Use *show session id <id_number>* para ver más detalles acerca de una sesión.
3. Si ha configurado una NAT de IP dinámica, use el comando **`show counter global filter aspect session severity drop | match nat`** para ver si falló alguna sesión debido a la asignación IP NAT. Si todas las direcciones en el grupo NAT de IP dinámica están asignadas cuando debería traducirse una conexión, el paquete será descartado.

Habilitación de clientes de la red interna para acceder a sus servidores públicos (NAT de ida y vuelta de destino)

Cuando un usuario de la red interna envíe una solicitud para acceder al servidor web corporativo en DMZ, el servidor DNS se resolverá en la dirección IP pública. Al procesar la solicitud, el cortafuegos utilizará el destino original del paquete (la dirección IP pública) y enrutará el paquete a la interfaz de salida para la zona no fiable. Para que el cortafuegos sepa que debe traducir la dirección IP pública del servidor web a una dirección de la red DMZ cuando reciba solicitudes de usuarios en la zona fiable, deberá crear una regla NAT de destino que permita al cortafuegos enviar la solicitud a la interfaz de salida para la zona DMZ de la manera siguiente.

STEP 1 | Cree un objeto de dirección para el servidor web.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)** para añadir un **Name (Nombre)** y una **Description (Descripción)** opcional para el objeto.
2. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e introduzca la dirección IP del servidor web, 203.0.113.11 en este ejemplo.

   Puede cambiar el tipo de objeto de dirección de **IP Netmask (Máscara de red IP)** a **FQDN** haciendo clic en **Resolve (Resolver)**, y cuando aparezca el FQDN, haga clic en **Use this FQDN (Utilizar este FQDN)**. De manera alternativa, para **Type (Tipo)**, seleccione **FQDN** e introduzca el FQDN que se utilizará para el objeto de dirección. Si introduce un FQDN y hace clic en **Resolve (Resolver)**, la dirección IP a la que dirige el FQDN aparece en el campo. Para cambiar el **Type (Tipo)** de objeto de dirección de un FQDN a una máscara de red IP utilizando esta dirección IP, haga clic en **Use this address (Utilizar esta dirección)** y el **Type (Tipo)** cambiará a **IP Netmask (Máscara de red IP)** con la dirección IP que aparece en el campo.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la regla NAT.
3. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
4. En la sección **Destination Address (Dirección de destino)**, haga clic en **Add (Añadir)** y seleccione el objeto de dirección que creó para su servidor web público.
5. En la pestaña **Translated Packet (Paquete traducido)**, para Destination Address Translation (Traducción de la dirección de destino), en **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)** e introduzca la dirección IP asignada a la interfaz del servidor web de la red DMZ, 10.1.1.11 en este ejemplo. Como alternativa, seleccione **Dynamic IP (with session distribution) (IP dinámica [con distribución de sesiones])** en **Translation Type (Tipo de traducción)** e introduzca en **Translated Address (Dirección traducida)** un objeto de dirección o un grupo de direcciones que utilicen una máscara de red de IP, un intervalo de IP o un FQDN; cualquiera de ellos puede devolver varias direcciones de DNS. Si la dirección de destino traducida se resuelve en más de una dirección, el cortafuegos distribuye las sesiones de NAT entrantes entre todas basándose en uno de los métodos que puede seleccionar: **Round Robin (Turnos)** (predeterminado), **Source IP Hash (Hash de IP de origen)**, **IP Modulo (Módulo de IP)**, **IP Hash (Hash de IP)** o **Least Sessions (Menos sesiones)**.
6. Haga clic en **OK (Aceptar)**.

STEP 3 | Haga clic en **Commit (Confirmar)**.

Habilitación de la traducción de direcciones bidireccional para sus servidores públicos (NAT de origen estática)

Cuando sus servidores públicos tengan direcciones IP privadas asignadas en el segmento de red en el que se encuentran físicamente, necesitará una regla NAT de origen para traducir la dirección de origen del servidor a la dirección externa en el momento de la salida. Puede crear una regla NAT estática para traducir la dirección de origen interna, 10.1.1.11, a la dirección del servidor web externa, 203.0.113.11 en nuestro ejemplo.

Sin embargo, un servidor orientado al público debe ser capaz de enviar y recibir paquetes. Necesita una política recíproca que traduzca la dirección pública (la dirección IP de destino en paquetes entrantes de usuarios de Internet) a la dirección privada para permitir que el cortafuegos enrute el paquete a su red DMZ. Puede realizar una regla NAT estática bidireccional como se describe en el procedimiento siguiente. La traducción bidireccional es una opción solo para NAT estática.

STEP 1 | Cree un objeto de dirección para la dirección IP interna del servidor web.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y **Add (Añadir)** para añadir un nombre en **Name (Nombre)** y una descripción opcional en **Description (Descripción)** para el objeto.
2. Seleccione **IP Netmask (Máscara de red de IP)** en la lista **Type (Tipo)** e introduzca la dirección IP del servidor web de la red DMZ (10.1.1.11 en este ejemplo).
3. Haga clic en **OK (Aceptar)**.

Si todavía no ha creado un objeto de dirección para la dirección pública de su servidor web, también debería crear ese objeto ahora.

STEP 2 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Nombre** para la regla NAT.
3. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la DMZ en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y, a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.
4. En la sección **Source Address (Dirección de origen)**, haga clic en **Add (Añadir)** y seleccione el objeto de dirección que creó para su dirección de servidor web interno.
5. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **Static IP (IP estática)** en la lista **Translation Type (Tipo de traducción)** de la sección **Source Address Translation (Traducción de dirección de origen)** y, a continuación, seleccione el objeto de dirección que ha creado para la dirección del servidor web externo en la lista **Translated Address (Dirección traducida)**.
6. En el campo **Bi-directional (Bidireccional)**, seleccione **Yes (Sí)**.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | Seleccione Confirmar.

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

Configuración de la NAT de destino con reescritura de DNS

Cuando configura una regla de la política de NAT de destino que ejecuta la traducción estática de las direcciones IPv4, también puede especificar que el cortafuegos reescriba las direcciones IPv4 de una respuesta de DNS en función de la dirección IP original o traducida que haya configurado para la regla. El cortafuegos ejecuta la NAT de la dirección IPv4 (es decir, la resolución del FQDN) incluida en la respuesta de DNS (que coincide con la regla) antes de reenviar esta al cliente. De ese modo, el cliente recibe la dirección adecuada para acceder al servicio de destino.

Consulte los casos de uso de reescritura de DNS para determinar si se debe realizar la reescritura **inversa** o **directa**.

*No puede habilitar la traducción de direcciones de origen de tipo **Bi-directional (Bidireccional)** en la misma regla de NAT en la que haya habilitado la reescritura de DNS.*

STEP 1 | Cree una regla de la política de NAT de destino en la que se especifique que el cortafuegos ejecute la traducción estática de las direcciones IPv4 que coincidan con ella y que, además, reescriba las direcciones IP de las respuestas de DNS cuando las direcciones IPv4 (del registro A) coincidan con la dirección de destino original o traducida de la regla de NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir una regla de la política de NAT.
2. (Opcional) En la pestaña **General**, introduzca un nombre descriptivo para la regla en **Name (Nombre)**.
3. Para **NAT Type (Tipo de NAT)**, seleccione **ipv4**.
4. En la pestaña **Original Packet (Paquete original)**, **añada** una **dirección de destino**.

   *También tendrá que seleccionar una zona de origen o **cualquier** zona de origen, pero la reescritura de DNS se produce a nivel global; solo coincide la dirección de destino en la pestaña Original Packet (Paquete original). La rescritura DNS ignora todos los demás campos de la pestaña Original Packet (Paquete original).*
5. En la sección Destination Address Translation (Traducción de dirección de destino) de la pestaña **Translated Packet (Paquete traducido)**, seleccione **Static IP (IP estática)** en **Translation Type (Tipo de traducción)**.
6. Seleccione una **dirección traducida** o especifique una nueva dirección.
7. Haga clic en **Enable DNS Rewrite (Habilitar reescritura de DNS)** y seleccione uno de estos valores en **Direction (Sentido)**:

   - Seleccione **reverse (inverso)**, que es el valor predeterminado, si la dirección IP de la respuesta de DNS exige la traducción opuesta que se especifica en la regla de NAT. Si la respuesta de DNS coincide con la dirección de destino **traducida** en la regla, traduzca la respuesta de DNS mediante la traducción inversa que utiliza la regla. Por ejemplo, si la regla traduce la dirección IP 1.1.1.10 a 192.168.1.10, el cortafuegos reescribe una respuesta de DNS de 192.168.1.10 a 1.1.1.10.
   - Seleccione **forward (directo)** si la dirección IP de la respuesta de DNS exige la misma traducción que se especifica en la regla de NAT. Si el paquete es una respuesta de DNS que coincide con la dirección de destino **original** en la regla, traduzca la respuesta de DNS mediante la misma traducción que utiliza la regla. Por ejemplo, si la regla traduce

la dirección IP 1.1.1.10 a 192.168.1.10, el cortafuegos reescribe una respuesta de DNS de 1.1.1.10 a 192.168.1.10.

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

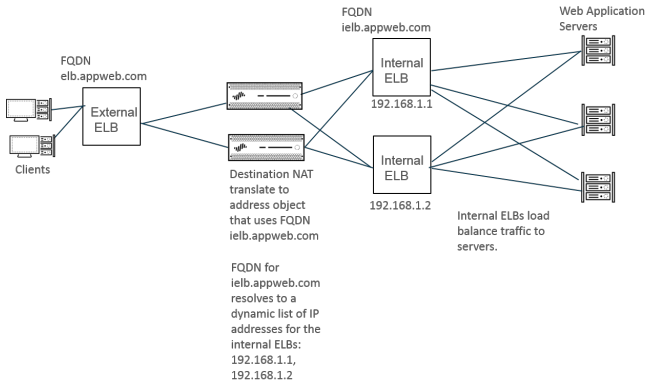
STEP 2 | **Commit (Confirmar)** los cambios.

Configuración de NAT de destino utilizando direcciones IP dinámicas

Utilice la NAT de destino para traducir la dirección de destino original a un host o servidor de destino que tiene una dirección IP dinámica y que utiliza un FQDN. Una NAT de destino con una dirección IP dinámica es especialmente útil en implementaciones en la nube que, por lo general, utilizan direcciones IP dinámicas. Cuando el host o el servidor en la nube posee nuevas direcciones IP (dinámico), no debe actualizar manualmente la regla de políticas de NAT realizando consultas continuamente al servidor DNS, ni debe utilizar un componente externo diferente para actualizar el servidor DNS con la asignación de FQDN a la dirección IP más reciente.

Al configurar el NAT de destino mediante direcciones IP dinámicas, debe usar solo un FQDN (no una máscara de red IP ni un intervalo de IP).

En el siguiente ejemplo de topología, los clientes desean comunicarse con los servidores que alojan aplicaciones web en la nube. Un equilibrador de carga elástico (Elastic Load Balancer, ELB) externo se conecta al cortafuegos, que se conecta a los ELB internos que se conectan a los servidores. Con el tiempo, Amazon Web Services (AWS), por ejemplo, añade (y elimina) direcciones IP del FQDN asignado a los ELB internos en función de la demanda de servicio. La flexibilidad utilizar un FQDN para la NAT del ELB interno ayuda a la política a dirigir a direcciones IP diferentes en momentos diferentes, lo que facilita la utilización de NAT de destino debido a que las actualizaciones son dinámicas.



STEP 1 | Cree un objeto de dirección utilizando el FQDN del servidor al que desea traducir la dirección.

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)** para añadir un objeto de dirección por **Name (Nombre)**, como **`post-NAT-Internal-ELB`**.
2. Seleccione **FQDN** como el **Type (Tipo)** e introduzca el FQDN. En este ejemplo, el FQDN es **`ielb.appweb.com`**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree la política NAT de destino.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir una regla de la política de NAT por **Name (Nombre)** en la pestaña **General**.
2. Seleccione **ipv4** en **NAT Type (Tipo de NAT)**.
3. En la pestaña **Original Packet (Paquete original)**, haga clic en **Add (Añadir)** para añadir la **Source Zone (Zona de origen)** y la **Destination Zone (Zona de destino)**.
4. En la pestaña **Translated Packet (Paquete traducido)**, en la sección Destination Address Translation (Traducción de la dirección de destino), seleccione la **Dynamic IP (with session distribution) (Dirección IP [con distribución de sesiones])** como el **Translation Type (Tipo de traducción)**.
5. En **Translated Address (Dirección traducida)**, seleccione el objeto de dirección que creó para el FQDN. En este ejemplo, el FQDN es **`post-NAT-Internal-ELB`**.
6. En **Session Distribution Method (Método de distribución de sesiones)**, seleccione una de estas opciones:
   - **Round Robin (Operación por turnos)**: (valor predeterminado) asigna nuevas sesiones a las direcciones IP de forma rotativa. Este método suele ser el adecuado, a menos que exista algún motivo para cambiarlo.
   - **Source IP Hash (Hash de IP de origen)**: asigna las sesiones nuevas en función del hash de la dirección IP de origen. Si tiene tráfico proveniente de una única dirección IP de origen, no seleccione Source IP Hash (Hash IP de origen); seleccione un método diferente.
   - **IP Modulo (Módulo IP)**: el cortafuegos considera la dirección IP de origen y destino del paquete entrante, realiza una operación XOR y una operación de módulo y el resultado determina a qué dirección IP el cortafuegos asignará las nuevas sesiones.
   - **IP Hash (Hash de IP)**: asigna las sesiones nuevas basándose en el hash de las direcciones IP de origen y de destino.
   - **Least Sessions (Menos sesiones)**: asigna las sesiones nuevas a la dirección IP que tiene menos sesiones simultáneas. Si tiene numerosas sesiones de corta duración, **Least Sessions (Últimas sesiones)** le proporcionará una distribución más equilibrada de las sesiones.

   El cortafuegos no elimina las entradas duplicadas de la lista de direcciones IP de destino antes de distribuir las sesiones entre varias, de modo que las distribuye entre las direcciones duplicadas igual que lo hace entre las únicas. Pueden aparecer direcciones duplicadas en el grupo de traducción si, por ejemplo, la dirección traducida es un grupo de direcciones de objetos de dirección, uno de los cuales es un FQDN que se resuelve en una dirección IP y otro, un intervalo que incluye esa misma dirección.
7. Haga clic en **OK (Aceptar)**.

STEP 3 | **Commit (Confirmar)** los cambios.

STEP 4 | (Opcional) Configure la frecuencia con la que el cortafuegos actualiza un FQDN. Consulte Caso de uso 1: el cortafuegos exige la resolución de DNS.

Modificación de la ratio de sobresuscripción para NAT DIPP

Si tiene suficientes direcciones IP públicas y no necesita usar una sobresuscripción de NAT DIPP, puede reducir la ratio de sobresuscripción, consiguiendo así que se permitan más reglas NAT de DIP y DIPP.

STEP 1 | Consulte la ratio de sobresuscripción NAT DIPP.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Session Settings (Configuración de sesión)**. Consulte el ajuste **Ratio de sobresuscripción NAT**.

STEP 2 | Defina la ratio de sobresuscripción NAT DIPP.

1. Modifique la sección Session Settings.
2. En la lista **NAT Oversubscription Rate (Ratio de sobresuscripción a NAT)**, seleccione **1x (1)**, **2x (2)**, **4x (4)** u **8x (8)**, en función de la proporción que le interese.

   *La configuración **Platform Default (Valor predeterminado de plataforma)** se aplica a la configuración de sobresuscripción predeterminada para el modelo. Si no desea ninguna sobresuscripción, seleccione **1x**.*
3. Haga clic en **ACEPTAR** y seleccione **Confirmar** el cambio.

Reserva de direcciones NAT de IP dinámicas

Puede reservar direcciones NAT IP dinámicas (durante un período configurable) para evitar que se asignen como direcciones traducidas a una dirección IP de origen diferente que necesita traducción. Cuando se configura, la reserva se aplica a todas las direcciones IP dinámicas traducidas en curso y a cualquier traducción nueva.

Tanto para traducciones en curso como para nuevas, cuando se traduce una dirección IP de origen a una dirección IP traducida disponible, ese emparejamiento se conserva incluso después de que hayan caducado todas las sesiones relacionadas con esa IP de origen específica. El temporizador de reservas para cada dirección IP de origen se inicia una vez que han caducado todas las sesiones que usen esa traducción de dirección IP de origen. La NAT de IP dinámica es una traducción de uno a uno; una dirección IP de origen se traduce a una dirección IP traducida que se elige dinámicamente entre aquellas direcciones disponibles en el grupo configurado. Por tanto, una dirección IP traducida que esté reservada no estará disponible para ninguna otra dirección IP de origen hasta que caduque la reserva al no haber iniciado una nueva sesión. El temporizador se reinicia cada vez que se inicia una nueva sesión para una asignación de IP de origen/IP traducida, tras un periodo sin sesiones activas.

De manera predeterminada, no hay ninguna dirección reservada. Puede reservar direcciones NAT de IP dinámicas para el cortafuegos o para un sistema virtual.

- Reserve direcciones NAT IP dinámicas para un cortafuegos.

  Introduzca los siguientes comandos:

```
admin@PA-3250# set setting nat reserve-ip yes
```

```
admin@PA-3250# set setting nat reserve-time <1-604800 secs>
```


- Reserve direcciones NAT IP dinámicas para un sistema virtual.

  Introduzca los siguientes comandos:

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
```

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800
 secs>
```

  Por ejemplo, supongamos que hay un grupo NAT de IP dinámicas de 30 direcciones y que hay 20 traducciones en curso cuando **nat reserve-time** se establece en 28800 segundos (8 horas). Estas 20 traducciones ahora están reservadas, de modo que cuando expire la última sesión (de cualquier aplicación) que use cada asignación de IP de origen /IP traducida, la dirección IP traducida estará reservada solo para aquella dirección IP de origen durante 8 horas en caso de que la dirección IP de origen necesite de nuevo una traducción. Asimismo, dado que las 10 direcciones traducidas restantes están asignadas, cada una está reservada para su dirección IP de origen, cada una con un temporizador que se inicia cuando expire la última sesión de esa dirección IP de origen.

  De este modo, cada dirección IP de origen puede traducirse repetidas veces en la misma dirección NAT del grupo; no se asignará la dirección IP traducida reservada del grupo a ningún otro host, incluso aunque no haya sesiones activas para esa dirección traducida.

  Supongamos que han caducado todas las sesiones de una asignación IP de origen/IP traducida y que se pone en marcha su temporizador de 8 horas. Si se inicia una nueva sesión, el temporizador se detiene y las sesiones continúan hasta su finalización, momento en el cual el temporizador de reservas se inicia de nuevo para reservar las direcciones traducidas.

  El temporizador de reservas permanece activo en el grupo NAT de IP dinámicas hasta que lo desactive al introducir el comando **set setting nat reserve-ip no** o al cambiar el valor de **nat reserve-time** por un valor diferente.

  Los comandos de la CLI para reservas no afectan a los grupos de IP y puertos dinámicos (DIPP) o NAT de IP estáticas.

Deshabilitación de NAT para un host o interfaz específico

Tanto las reglas NAT de origen como las NAT de destino se pueden configurar para deshabilitar la traducción de direcciones. Puede haber excepciones en las que no desee que se produzca el NAT para un host una subred o para el tráfico que sale de una interfaz específica. El siguiente procedimiento muestra cómo deshabilitar el NAT para un host.

STEP 1 | Cree la política NAT.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)** para añadir un nombre descriptivo en **Name (Nombre)** para la política.
2. En la pestaña **Original Packet (Paquete original)**, seleccione la zona que ha creado para la red interna en la sección **Source Zone (Zona de origen)** (haga clic en **Add [Añadir]** y,

a continuación, seleccione la zona) y la zona que ha creado para la red externa en la lista **Destination Zone (Zona de destino)**.

3. En **Dirección de origen**, haga clic en **Añadir** e introduzca la dirección del host. Haga clic en **OK (Aceptar)**.
4. En la pestaña **Translated Packet (Paquete traducido)**, seleccione **None (Ninguno)** en la lista **Translation Type (Tipo de traducción)** de la sección Source Address Translation (Traducción de dirección de origen).
5. Haga clic en **OK (Aceptar)**.

STEP 2 | Confirme los cambios.

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

Las reglas de NAT se procesan en orden descendente; ponga la política de excepción antes de otras políticas NAT para garantizar que se procesa antes de que se realice una traducción de dirección de los orígenes que quiere excluir.

Ejemplos de configuración de NAT

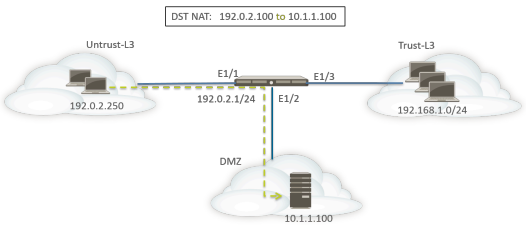
- Ejemplos de NAT de destino: asignación de uno a uno
- NAT de destino con ejemplo de traducción de puerto
- Ejemplo de NAT de destino: asignación de uno a uno
- Ejemplo de NAT de origen y destino
- Ejemplo de NAT de origen de Virtual Wire
- Ejemplo de NAT estática de Virtual Wire
- Ejemplo de NAT de destino de Virtual Wire

Ejemplos de NAT de destino: asignación de uno a uno

Los errores más frecuentes en la configuración de NAT y de reglas de seguridad se cometen en las referencias a los objetos de direcciones y zonas. Las direcciones usadas en las reglas NAT de destino se refieren siempre a la dirección IP original del paquete (es decir, la dirección pretraducida). La zona de destino de la regla NAT se determina después de la búsqueda de rutas de la dirección IP de destino en el paquete original (es decir, la dirección IP de destino pre-NAT).

Las direcciones en la política de seguridad también hacen referencia a las direcciones IP del paquete origina (es decir, la dirección pre-NAT). Sin embargo, la zona de destino es la zona donde está conectado físicamente el host de destino. Dicho de otro modo, la zona de destino en la regla de seguridad se determina tras la búsqueda de ruta de la dirección IP de destino post-NAT.

En el siguiente ejemplo de una asignación uno a uno de NAT de destino, los usuarios de la zona denominada Untrust-L3 acceden al servidor 10.1.1.100 en la zona denominada DMZ usando la dirección IP 192.0.2.100.



Antes de configurar las reglas NAT, tenga en cuenta la secuencia de eventos de esta situación.

- El host 192.0.2.250 envía una solicitud de ARP para la dirección 192.0.2.100 (la dirección pública del servidor de destino).
- El cortafuegos recibe el paquete de solicitud de ARP para el destino 192.0.2.100 en la interfaz Ethernet 1/1 y procesa la solicitud. El cortafuegos responde a la solicitud de ARP con su propia dirección MAC debido a la regla NAT de destino configurada.
- Se evalúan las reglas NAT para buscar coincidencias. Para traducir la dirección IP de destino, debe crearse una regla NAT de destino desde la zona Untrust-L3 a la zona Untrust-L3 para traducir la dirección IP de destino de 192.0.2.100 a 10.1.1.100.
- Tras determinar la dirección traducida, el cortafuegos realiza una búsqueda de ruta para el destino 10.1.1.100 con el fin de determinar la interfaz de salida. En este ejemplo, la interfaz de salida es Ethernet 1/2 en la zona DMZ.

- El cortafuegos realiza una búsqueda de políticas de seguridad para comprobar si se permite el tráfico desde la zona Untrust-L3 a DMZ.

  La dirección de la política coincide con la zona de entrada y la zona donde está ubicado físicamente el servidor.

  La política de seguridad hace referencia a la dirección IP en el paquete original, que tiene una dirección de destino de 192.0.2.100.

- El cortafuegos reenvía el paquete al servidor que está fuera de la interfaz de salida Ethernet1/2. La dirección de destino se cambia a 10.1.1.100 cuando el paquete abandona el cortafuegos.

Para este ejemplo, los objetos de dirección están configurados para servidor web-privado (10.1.1.100) y servidor web-público (192.0.2.100). La regla NAT configurada sería como esta:

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

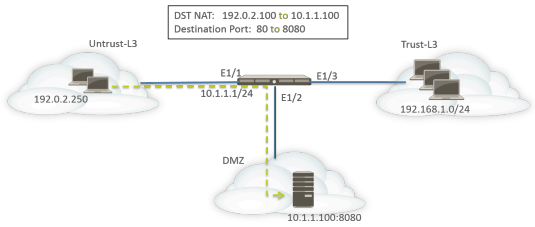
La dirección de las reglas NAT se basa en el resultado de la búsqueda de ruta.

La política de seguridad configurada para ofrecer acceso al servidor desde la zona untrust-l3 sería parecida a esta:

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

NAT de destino con ejemplo de traducción de puerto

En este ejemplo, el servidor web está configurado para escuchar el tráfico HTTP en el puerto 8080. Los clientes acceden al servidor web usando la dirección IP 192.0.2.100 y el puerto TCP 80. La regla NAT de destino está configurada para traducir tanto la dirección IP como el puerto a 10.1.1.100 y el puerto TCP 8080. Los objetos de dirección están configurados para servidor web-privado (10.1.1.100) y servidor web-público (192.0.2.100).



Deben configurarse en el cortafuegos las siguientes reglas de seguridad y NAT:

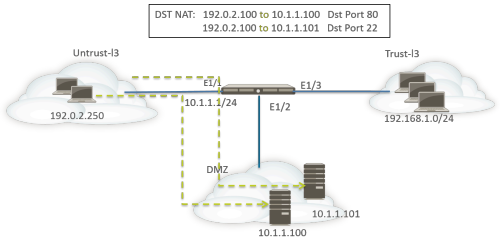
		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

Use el comando de la CLI **`show session all`** para verificar la traducción.

Ejemplo de NAT de destino: asignación de uno a uno

En este ejemplo, la dirección IP se asigna a dos hosts internos distintos. El cortafuegos usa la aplicación para identificar el host interno al que el cortafuegos reenvía el tráfico.



Todo el tráfico HTTP se envía al host 10.1.1.100 y el tráfico SSH se envía al servidor 10.1.1.101. Se requieren los siguientes tipos de perfil:

- Objeto de dirección para una dirección IP pretraducida del servidor
- Objeto de dirección para la dirección IP real del servidor SSH
- Objeto de dirección para la dirección IP real del servidor web

Se crean los objetos de dirección correspondientes:

- Servidores-públicos: 192.0.2.100
- Servidor-SSH: 10.1.1.101
- Servidor web-privado: 10.1.1.100

Las reglas NAT configuradas serían parecidas a esta:

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

Las reglas de seguridad serían parecidas a esta:

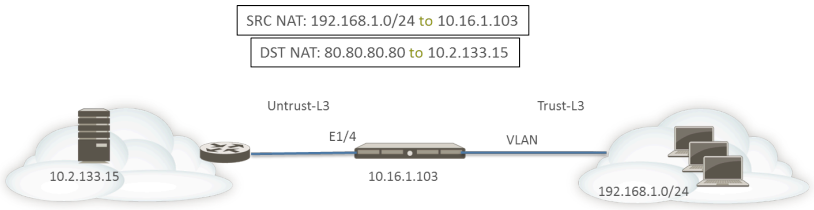
			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

Ejemplo de NAT de origen y destino

En este ejemplo, las reglas NAT traducen la dirección IP tanto de origen como de destino de paquetes entre los clientes y el servidor.

- NAT de origen: las direcciones de origen en los paquetes de los clientes en la zona Trust-L3 hacia el servidor en la zona Untrust-L3 se traducen desde las direcciones privadas de la red 192.168.1.0/24 a la dirección IP de la interfaz de salida en el cortafuegos (10.16.1.103). La traducción de puertos e IP dinámicas hace que los números de puerto también se traduzcan.

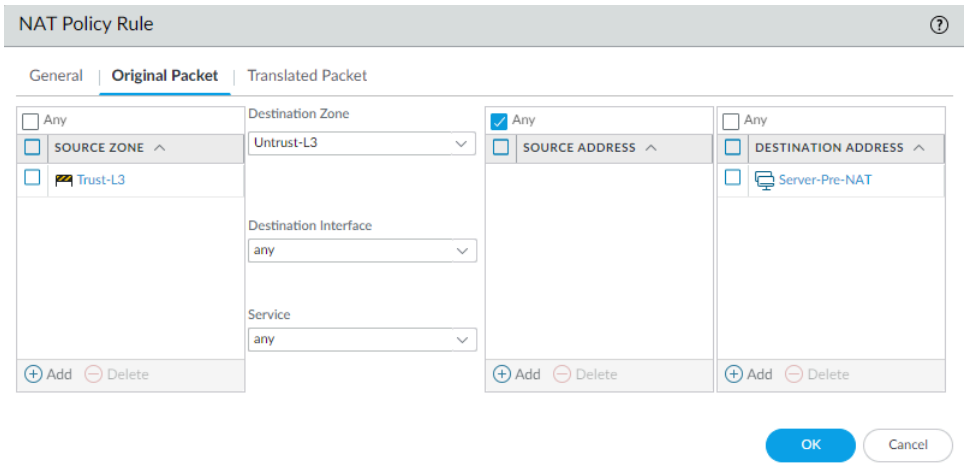
- NAT de destino: Las direcciones de destino en los paquetes procedentes de los clientes y dirigidos al servidor se traducen desde la dirección pública del servidor (80.80.80.80) a la dirección privada del servidor (10.2.133.15).

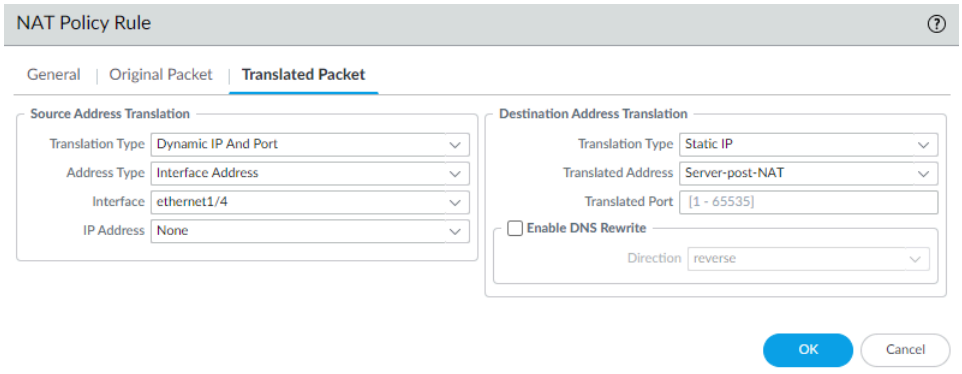


Se crean los siguientes objetos de dirección para la NAT de destino.

- Server-Pre-NAT: 80.80.80.80
- Server-post-NAT: 10.2.133.15

Las capturas de pantalla siguientes ilustran el modo de configurar las políticas NAT de origen y destino del ejemplo.





Para verificar las traducciones, use el comando de la CLI **`show session all filter destination 80.80.80.80`**. Una dirección de cliente 192.168.1.11 y su número de puerto se ha traducido a 10.16.1.103 y un número de puerto. La dirección de destino 80.80.80.80 se ha traducido a 10.2.133.15.

Ejemplo de NAT de origen de Virtual Wire

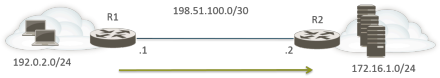
La implementación de cable virtual de un cortafuegos Palo Alto Networks® cuenta con la ventaja de ofrecer seguridad de forma transparente a los dispositivos de destino. Se puede configurar NAT para interfaces configuradas en un Virtual Wire. Están permitidos todos los tipos de NAT: NAT de origen (IP dinámica, IP y puerto dinámicos, estática) y NAT de destino.

Dado que las interfaces en un Virtual Wire no tienen una dirección IP asignada, no es posible traducir una dirección IP a una dirección IP de interfaz. Debe configurar un grupo de direcciones IP.

Si ejecuta NAT en interfaces de cable virtual, es recomendable que traduzca las direcciones de origen a una subred diferente de la subred con la que se comunican los dispositivos vecinos. El cortafuegos no utilizará ARP proxy para direcciones NAT. Debe configurarse un enrutamiento correcto en los enrutadores anteriores y posteriores para que los paquetes se traduzcan en el modo Virtual Wire. Los dispositivos vecinos solamente podrán resolver solicitudes ARP para direcciones IP que residan en la interfaz del dispositivo en el otro extremo del cable virtual. Consulte ARP proxy para grupos de direcciones NAT para acceder a más explicaciones sobre el ARP proxy.

En el siguiente ejemplo de NAT de origen, las políticas de seguridad (no se muestran) están configuradas desde la zona de cable virtual denominada vw-trust hasta la zona denominada vw-untrust.

En el topología siguiente, hay dos enrutadores configurados para ofrecer conectividad entre las subredes 192.0.2.0/24 y 172.16.1.0/24. El enlace entre los enrutadores está configurado en la subred 198.51.100.0/30. El enrutamiento estático está configurado en ambos enrutadores para establecer conexión entre las redes. Antes de implementar el cortafuegos en el entorno, la topología y la tabla de enrutamiento para cada enrutador son similares a esta:



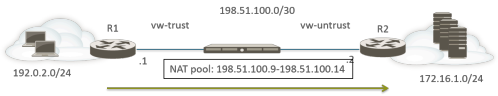
Ruta en R1:

IP Destino	siguiente salto
172.16.1.0/24	198.51.100.2

Ruta en R2:

IP Destino	siguiente salto
192.0.2.0/24	198.51.100.1

Ahora el cortafuegos está implementado en modo Virtual Wire entre los dos dispositivos de Capa 3. Se configura en el cortafuegos un grupo de direcciones IP de NAT con el intervalo 198.51.100.9 a 198.51.100.14. Todas las comunicaciones de clientes en la subred 192.0.2.0/24 que acceden a servidores en la red 172.16.1.0/24 llegarán a R2 con una dirección de origen traducida en el intervalo 198.51.100.9 a 198.51.100.14. La respuesta de los servidores se dirigirá a esas direcciones.



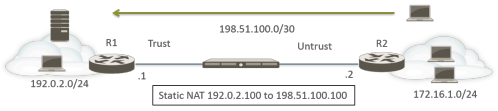
Para que la NAT de origen funcione, debe configurar el enrutamiento adecuado en R2, de modo que los paquetes dirigidos a otras direcciones no sean descartados. La siguiente tabla de enrutamiento muestra la tabla de enrutamiento modificada en R2; la ruta garantiza que el tráfico a los destinos 198.51.100.9 a 198.51.100.14 (es decir, hosts en la subred 198.51.100.8/29) se enviará de vuelta a R1 a través del cortafuegos.

Ruta en R2:

IP Destino	siguiente salto
198.51.100.8/29	198.51.100.1

Ejemplo de NAT estática de Virtual Wire

En este ejemplo, las políticas de seguridad están configuradas desde la zona Virtual Wire denominada Trust hasta la zona de Virtual Wire denominada Untrust. El host 192.0.2.100 se traduce estáticamente a la dirección 198.51.100.100. Con la opción **Bi-directional (Bidireccional)** habilitada, el cortafuegos genera una política NAT desde la zona Untrust hasta la zona Trust. Los clientes en la zona Untrust acceden al servidor usando la dirección IP 198.51.100.100, que el cortafuegos traduce a 198.0.2.100. Cualquier conexión iniciada por el servidor en 192.0.2.100 se traduce a la dirección IP de origen 198.51.100.100.



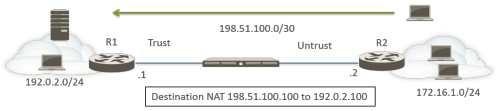
Ruta en R2:

IP Destino	siguiente salto
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

Ejemplo de NAT de destino de Virtual Wire

Los clientes de la zona Untrust acceden al servidor usando la dirección IP 198.51.100.100, que el cortafuegos traduce a 192.0.2.100. Tanto la NAT como las políticas de seguridad deben estar configuradas desde la zona Untrust hacia la zona Trust.



Ruta en R2:

IP Destino	siguiente salto
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

NPTv6

La traducción de prefijos de red IPv6 a IPv6 (NPTv6) realiza una traducción estática y sin estado de un prefijo IPv6 a otro prefijo IPv6 (los números de puerto no cambian). NPTv6 ofrece cuatro ventajas principales:

- Puede impedir problemas de enrutamiento asimétrico que hacen que las direcciones que no dependen del proveedor se anuncien a varios centros de datos.
- NPTv6 permite anunciar rutas más específicas, de modo que el tráfico de retorno llegue al mismo cortafuegos que lo transmitió.
- Las direcciones privadas y públicas son independientes; puede cambiar una sin que las otras se vean afectadas.
- Tiene la habilidad de traducir Direcciones locales exclusivas a direcciones enrutables globalmente.

Este tema se basa en conocimientos básicos de NAT. Debe estar familiarizado con los conceptos de NAT antes de configurar NPTv6.

- Resumen de NPTv6
- Funcionamiento de NPTv6
- Proxy NDP
- Ejemplo de NPTv6 y Proxy NDP
- Creación de una política NPTv6

Resumen de NPTv6

Esta sección describe la traducción de prefijos de red IPv6 a IPv6 (NPTv6) y el modo de configurarla. NPTv6 se define en RFC 6296. Palo Alto Networks® no implementa toda la funcionalidad definida en la RFC, pero la funcionalidad que ha implementado cumple la RFC.

NPTv6 realiza una traducción sin estado de un prefijo IPv6 a otro prefijo IPv6. No tiene estado, lo que implica que no guarda un registro de los puertos o sesiones de las direcciones traducidas. NPTv6 se diferencia de NAT66, que sí tiene estado. Palo Alto Networks admite la traducción de prefijos NPTv6 RFC 6296; no admite NAT66.

Con la limitación de direcciones en el espacio IPv4, la NAT se veía obligada a traducir direcciones IPv4 privadas no enrutables a una o más direcciones IPv4 enrutables a nivel global. Las organizaciones que usan el direccionamiento IPv6 no necesitan traducir las direcciones IPv6 a direcciones IPv6 gracias a la abundancia de direcciones IPv6. Sin embargo, hay Razones para usar NPTv6 con el fin de traducir prefijos de IPv6 en el cortafuegos.

Es importante comprender que NPTv6 no aporta seguridad. En general, la traducción de direcciones de red sin estado no brinda seguridad; solo aporta una función de traducción de direcciones. NPTv6 no oculta ni traduce números de puerto. Debe configurar las políticas de seguridad del cortafuegos correctamente en cada dirección para garantizar que el tráfico se controla del modo deseado.

NPTv6 traduce la parte del prefijo de una dirección IPv6 pero no la parte del host ni los números de puerto de la aplicación. La parte del host simplemente se copia, por lo que permanece igual en ambos lados del cortafuegos. La parte de host también permanece visible del encabezado del paquete.

NPTv6 es compatible con los siguientes modelos de cortafuegos (NPTv6 con búsqueda de hardware, pero los paquetes se transmiten a través de la CPU):

- Cortafuegos PA-7000 Series
- Cortafuegos PA-5200 Series
- Cortafuegos PA-3200 Series
- Firewall PA-800
- Cortafuegos PA-220

Los cortafuegos VM-Series admiten NPTv6, pero no tienen la capacidad de que el hardware realice una búsqueda de sesión.

- Direcciones locales exclusivas
- Razones para usar NPTv6

Direcciones locales exclusivas

RFC 4193, Direcciones IPv6 de unidifusión locales únicas, define direcciones locales únicas (ULA, Unique Local Address), que son direcciones IPv6 de unidifusión. Se pueden considerar equivalentes IPv6 de las direcciones IPv4 privadas identificadas en RFC 1918, Asignación de direcciones para Internet privadas, que no se pueden enrutar globalmente.

Una ULA es única a nivel internacional, pero no es de esperar que se pueda enrutar globalmente. Su uso está previsto para comunicaciones locales y para ser enrutable en un área limitada, como un sitio o entre un número pequeño de sitios. Palo Alto Networks® no recomienda asignar ULA, pero un cortafuegos configurado con NPTv6 traducirá los prefijos que se le envíen, incluidas las ULA.

Razones para usar NPTv6

Aunque no hay escasez de direcciones IPv6 enrutables globalmente, hay varias razones para traducir las direcciones IPv6. NPTv6:

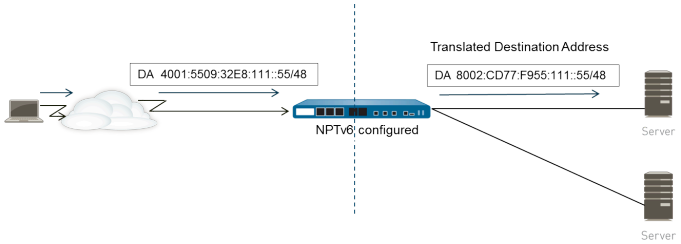
- **Evita el enrutamiento asimétrico**: se puede producir enrutamiento asimétrico si varios centros de datos anuncian en Internet global un espacio de dirección que no depende del proveedor (/48, por ejemplo). Al usar NPTv6, puede anunciar rutas más específicas desde cortafuegos regionales, y el tráfico de retorno llegará al mismo cortafuegos en el que se tradujo la dirección IP de origen.
- **Proporciona independencia de direcciones**: No es necesario que cambie los prefijos IPv6 usados dentro de su red local tras un cambio de los prefijos globales (realizado, por ejemplo, por el proveedor de servicios de Internet o como resultado de una fusión de organizaciones). Por el contrario, puede cambiar las direcciones interiores discrecionalmente sin interrumpir las direcciones usadas para acceder a los servicios en la red privada desde Internet. En cada caso, debe actualizar una regla NAT en lugar de reasignar las direcciones de red.
- **Traduce ULA para enrutamiento**: tiene Direcciones locales exclusivas asignadas dentro de su red privada, y puede hacer que el cortafuegos las traduzca a direcciones enrutables globalmente. Por lo tanto, puede disfrutar tanto de direccionamiento privado como de direcciones traducidas enrutables.
- **Reduce la exposición a prefijos IPv6**: Los prefijos IPv6 están menos expuestos que si no traduce los prefijos de red; sin embargo, NPTv6 no es una medida de seguridad. La parte del identificador de interfaz de cada dirección IPv6 no se traduce; permanece igual en cada lado del cortafuegos, y visible para cualquiera que pueda ver el encabezado del paquete. Asimismo, los prefijos no son seguros; pueden ser determinados por otros.

Funcionamiento de NPTv6

Cuando configura una política NPTv6, el cortafuegos de Palo Alto Networks® realiza una traducción de IPv6 uno a uno estática en ambas direcciones. La traducción está basada en el algoritmo descrito en RFC 6296.

En un caso de uso, el cortafuegos que realiza NPTv6 se encuentra entre una red interna y una externa (como Internet) que usa prefijos enrutables globalmente. Cuando los datagramas van en dirección de salida, el prefijo de origen interno se sustituye por un prefijo externo, lo que se conoce como traducción de origen.

En otro caso de uso, cuando los datagramas van en dirección de entrada, se sustituye el prefijo se sustituye por el prefijo interno, lo que se conoce como traducción de destino. La siguiente figura ilustra la traducción de destino y una característica de NPTv6: solo se traduce la parte del prefijo de una dirección IPv6. La parte del host de la traducción no se traduce y permanece en el mismo lado del cortafuegos. En la siguiente figura, el identificador del host es 111::55 a ambos lados del cortafuegos.



Es importante comprender que NPTv6 no aporta seguridad. Al planificar sus políticas NAT NPTv6, recuerde también configurar las políticas de seguridad en cada dirección.

Una regla de políticas NAT o NPTv6 no puede tener las dos direcciones (origen y destino) configuradas en Cualquiera.

En un entorno en el que quiera traducción de prefijos IPv6, se combinan tres funciones del cortafuegos: Políticas NAT NPTv6, políticas de seguridad y Proxy NDP.

El cortafuegos no traduce lo siguiente:

- Las direcciones que el cortafuegos tiene en su caché de Detección de vecinos (ND, Neighbor Discovery).
- La subred 0xFFFF (de acuerdo con RFC 6296, Apéndice B).
- Direcciones de multidifusión IP.
- Direcciones IPv6 con una longitud de prefijo de /31 o inferior.
- Direcciones locales de vínculo Si el cortafuegos está funcionando en el modo Virtual Wire, no hay direcciones IP que traducir, y el cortafuegos no traduce direcciones locales de vínculo.
- Direcciones de sesiones para TCP que autentican peers usando la opción de autenticación TCP (RFC 5925).

Al usar NPTv6, el rendimiento del tráfico de método rápido se ve afectado porque NPTv6 se realiza en el método lento.

NPTv6 funcionará con IPSec IPv6 solo si el cortafuegos se origina y termina en el túnel. El tráfico de tránsito IPSec fallaría porque la dirección IPv6 de origen o destino se modificaría. Una técnica NAT transversal que encapsulara el paquete permitiría a IPSec IPv6 trabajar con NPTv6.

- Asignación neutral de suma de comprobación
- Traducción bidireccional
- NPTv6 aplicada a un servicio específico

Asignación neutral de suma de comprobación

Las traducciones de asignaciones NPTv6 que realiza el cortafuegos son neutrales de suma de comprobación, lo que significa que "... dan como resultado encabezados IP que generarán la misma suma de comprobación de pseudoencabezado IPv6 cuando se calcule la suma de comprobación usando el algoritmo de suma de comprobación de Internet estándar [RFC 1071]." Consulte RFC 6296, Sección 2.6, para obtener más información acerca de la asignación neutral de suma de comprobación.

Si usa NPTv6 para realizar la NAT de destino, puede ofrecer la dirección de IPv6 interna y de la longitud de prefijo/prefijo externa de la interfaz del cortafuegos en la sintaxis del comando **`test nptv6`** de la CLI. La CLI responde con una dirección de IPv6 pública neutral de suma de comprobación que se usa en su configuración NPTv6 para alcanzar ese destino.

Traducción bidireccional

Con Creación de una política NPTv6, la opción **Bi-directional (Bidireccional)** en la pestaña **Translated Packet (Paquete traducido)** le ofrece una forma cómoda de hacer que el cortafuegos cree una NAT correspondiente o una traducción de NPTv6 en la dirección contraria a la traducción que ha configurado. Por defecto, la traducción **Bi- directional** está deshabilitada.

Si habilita la traducción bidireccional, es extremadamente importante asegurarse de tener establecidas políticas de seguridad para controlar el tráfico en ambas direcciones. Sin dichas políticas, la función Bi-directional permitirá la traducción automática de paquetes en ambas direcciones, algo que quizás no desee.

NPTv6 aplicada a un servicio específico

La implementación de Palo Alto Networks de NPTv6 ofrece la capacidad de filtrar paquetes para limitar qué paquetes están sujetos a traducción. Recuerde que NPTv6 no realiza traducción de puertos. No existe el concepto de traducción de IP y puertos dinámicos (DIPP) porque NPTv6 solo traduce prefijos IPv6. Sin embargo, puede especificar que solo se realice traducción NPTv6 de los paquetes de un cierto puerto de servicios. Para ello, realice la Creación de una política NPTv6 que especifique un **Service (Servicio)** en el paquete original.

Proxy NDP

El protocolo de detección de vecinos (NDP) para IPv6 realiza funciones similares a las que ofrece el protocolo de resolución de direcciones (ARP) para IPv4. RFC 4861 define la detección de vecinos para IP versión 6 (IPv6). Hosts, enrutadores y cortafuegos usan NDP para determinar las direcciones de capa de enlace de los vecinos en enlaces conectados, llevar un seguimiento de los vecinos con los que se puede contactar y actualizar las direcciones de capa de enlace de los vecinos que han cambiado. Los peers anuncian sus propias direcciones MAC y su dirección IPv6, y solicitan además direcciones de los peers.

NDP también es compatible con el concepto de ***proxy***, cuando un nodo tiene un dispositivo vecino que es capaz de reenviar paquetes en nombre del nodo. El dispositivo (cortafuegos) actúa como Proxy NDP.

Los cortafuegos de Palo Alto Networks® son compatibles con NDP y Proxy NDP en sus interfaces. Al configurar el cortafuegos para que actúe como un Proxy NDP para direcciones, este puede enviar anuncios de detección de vecinos (ND) y responder a solicitudes de ND de peers que están solicitando direcciones MAC de prefijos IPv6 asignados a dispositivos tras el cortafuegos. También puede configurar direcciones para las que el cortafuegos no responderá a solicitudes de proxy (direcciones negadas).

De hecho, NDP está habilitado de manera predeterminada, y necesita configurar Proxy NDP al configurar NPTv6 por estos motivos:

- NPTv6 no tiene estado, por lo que necesita un modo de indicar al cortafuegos que responda a paquetes de ND enviados a direcciones de Proxy NDP especificadas, y que no responda a direcciones Proxy NDP negadas.

  Se recomienda que niegue las direcciones de sus vecinos en la configuración de Proxy NDP, ya que Proxy NDP indica que el cortafuegos contactará con esas direcciones tras el cortafuegos, pero los vecinos no están tras el cortafuegos.

- NDP hace que el cortafuegos guarde las direcciones MAC y las direcciones IPv6 de los vecinos en su caché de ND. (Consulte la figura en Ejemplo de NPTv6 y Proxy NDP). El cortafuegos no realiza traducción NPTv6 de direcciones que encuentra en la caché de ND porque provocaría un conflicto. Si la parte del host de una dirección en la memoria caché coincide con la parte del host de la dirección de un vecino, y el prefijo en la caché se traduce al mismo prefijo que el del vecino (porque la interfaz de salida del cortafuegos pertenece a la misma subred del vecino), tendrá una dirección traducida exactamente igual que la dirección IPv6 legítima del vecino, lo que provoca un conflicto. (Si se intenta realizar una traducción NPTv6 en una dirección en la memoria caché de ND, un mensaje de syslog informativo registra el evento: `NPTv6 Translation Failed`).

Cuando una interfaz con proxy NDP habilitado recibe una solicitud de ND en la que le pide una dirección MAC para una dirección IPv6, se produce la secuencia siguiente:

- El cortafuegos busca en la memoria caché de ND para asegurarse de que no está ahí la dirección IPv6 de la solicitud. Si la dirección está ahí, el cortafuegos ignora la solicitud ND.
- Si la dirección IPv6 es 0, significa que el paquete es un paquete de detección de dirección duplicada, y el cortafuegos ignora la solicitud de ND.

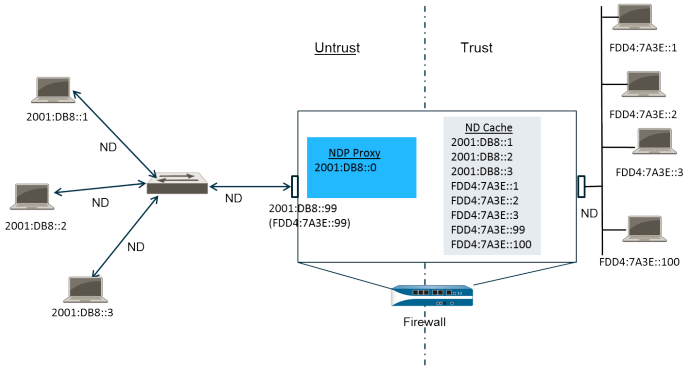
- El cortafuegos realiza una búsqueda de la coincidencia de prefijo más larga de las direcciones de Proxy NDP y encuentra la mejor coincidencia de la dirección en la solicitud. Si el campo Negar de la coincidencia está marcado (en la lista Proxy NDP), el cortafuegos descarta la solicitud de ND.
- Solo si la coincidencia de prefijo más larga busca coincidencias, y si la dirección coincidente no está negada, el Proxy NDP responderá a la solicitud de ND. El cortafuegos responde con un paquete ND, proporcionando su propia dirección MAC como dirección MAC del siguiente salto hacia el destino consultado.

Para una correcta compatibilidad con NDP, el cortafuegos no realiza Proxy NDP para lo siguiente:

- Detección de direcciones duplicadas (DAD)
- Direcciones en la caché de ND (dado que tales direcciones no pertenecen al cortafuegos; pertenecen a los vecinos detectados).

Ejemplo de NPTv6 y Proxy NDP

La siguiente figura ilustra cómo funcionan juntos NPTv6 y Proxy NDP.



- Caché de ND en el ejemplo de NPTv6
- Proxy ND en el ejemplo de NPTv6
- La traducción NPTv6 en el ejemplo de NPTv6
- Los vecinos en caché ND no se traducen

Caché de ND en el ejemplo de NPTv6

En el ejemplo anterior, varios peers conectan con el cortafuegos a través de un conmutador, y la ND se produce entre los peers y el conmutador, entre el conmutador y el cortafuegos y el cortafuegos y los dispositivos en el lado de confianza.

Cuando el cortafuegos detecta peers, guarda sus direcciones en su caché de ND. Los peers de confianza FDDA:7A3E::1, FDDA:7A3E::2 y FDDA:7A3E::3 se conectan al cortafuegos por el lado de confianza. FDDA:7A3E::99 es la dirección no traducida del propio cortafuegos; su dirección pública es 2001:DB8::99. Las direcciones de los peers en el lado no fiable se han detectado y aparecen en la caché de ND: 2001:DB8::1, 2001:DB8::2 y 2001:DB8::3.

Proxy ND en el ejemplo de NPTv6

En nuestro escenario, queremos que el cortafuegos actué como un Proxy NDP para los prefijos tras el cortafuegos. Cuando el cortafuegos es un Proxy NDP para un conjunto especificado de direcciones/intervalos/prefijos y ve una dirección de este intervalo en un anuncio o solicitud de ND, el cortafuegos responde siempre que no responda antes un dispositivo con esta dirección específica, la dirección no esté negada en la configuración de Proxy NDP y la dirección no esté en la caché ND. El cortafuegos realiza la traducción del prefijo (descrita más abajo) y envía el paquete al lado fiable, donde esa dirección puede estar asignada o no a un dispositivo.

En este ejemplo, la tabla de Proxy ND contiene la dirección de red 2001:DB8::0. Cuando la interfaz ve una ND para 2001:DB8::100, ningún otro dispositivo en el conmutador L2 reclama el paquete, de modo que el intervalo de proxy hace que el cortafuegos no reclame, y tras la traducción a FDD4:7A3E::100, el cortafuegos lo envía a la zona fiable.

La traducción NPTv6 en el ejemplo de NPTv6

En este ejemplo, el **Original Packet** está configurado con una **Source Address** de FDD4:7A3E::0 y un **Destination** de **Any**. El **Translated Packet** está configurado con la **Translated Address** de 2001:DB8::0.

Por lo tanto, los paquetes salientes con un origen FDD4:7A3E::0 se traducen a 2001:DB8::0. Los paquetes entrantes con un prefijo de destino en la red 2001:DB8::0 se traducen a FDD4:7A3E::0.

Los vecinos en caché ND no se traducen

En nuestro ejemplo, hay hosts tras el cortafuegos con identificadores de host :1, :2 y :3. Si los prefijos de aquellos hosts están traducidos a un prefijo que existe más allá del cortafuegos, y si esos dispositivos no tienen identificadores de host :1, :2 y :3 (ya que la parte del identificador de host de la dirección permanece inalterada), la dirección traducida resultante pertenecería al dispositivo existente, y se produciría un conflicto de dirección. Para evitar un conflicto con identificadores de host coincidentes, NPTv6 no traduce direcciones que encuentra en la caché de ND.

Creación de una política NPTv6

Realice esta tarea cuando desee configurar una política NPTv6 de NAT para traducir un prefijo IPv6 a otro prefijo IPv6. Los requisitos previos de esta tarea son:

- Habilite IPv6. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)**. Haga clic en **Edit** y seleccione **IPv6 Firewalling**.
- Configure una interfaz Ethernet de capa 3 con una dirección IPv6 válida y con IPv6 habilitado. Seleccione **Network (Red)** > **Interfaces** > **Ethernet**, seleccione una interfaz y en la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
- Cree políticas de seguridad de red, ya que NPTv6 no proporciona seguridad.
- Decida si quiere traducción de origen, de destino o ambas.
- Identifique las zonas a las que quiere aplicar la política NPTv6.
- Identifique sus prefijos IPv6 originales y traducidos.

STEP 1 | Cree una política NPTv6.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un nombre descriptivo en **Name (Nombre)** para la regla de política de NPTv6.
3. (Opcional) Introduzca una **Description (Descripción)** y **Tag (Etiqueta)**.
4. Para **NAT Type (Tipo de NAT)**, seleccione **NPTv6**.

STEP 2 | Especifique los criterios de coincidencia para los paquetes entrantes; los paquetes que coinciden en todos los criterios están sujetos a la traducción de NPTv6.

Las zonas son necesarias para ambos tipos de traducción.

1. En la pestaña **Original Packet (Paquete original)**, para **Source Zone (Zona de origen)**, deje **Any (Cualquiera)** o haga clic en **Add (Añadir)** para introducir la zona de origen a la que se aplica la política.
2. Introduzca la **Destination Zone (Zona de destino)** a la que se aplica la política.
3. (Opcional) Seleccione una **Destination Interface**.
4. (Opcional) Seleccione un **Service (Servicio)** para restringir los tipos de paquetes que se traducen.
5. Si está realizando una traducción de origen, introduzca una **Source Address (Dirección de origen)** o seleccione **Any (Cualquiera)**. Esta dirección puede ser un objeto de dirección. Se aplican las siguientes restricciones a la **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)**:
   - Los prefijos de **Source Address (Dirección de origen)** y **Destination Address (Dirección de destino)** para **Original Packet (Paquete original)** y **Translated Packet (Paquete traducido)** deben tener el formato xxxx:xxxx::/yy, aunque los ceros de inicio en el prefijo se pueden omitir.
   - La dirección IPv6 no puede tener definida una parte de identificador de interfaz (host).
   - El intervalo admitido de longitudes de prefijo es de /32 a /64.

- No es posible definir tanto la **Source Address** como la **Destination Address** en **Any**.

6. Si está realizando la traducción de origen, tiene la opción de introducir una **Destination Address**. Si está realizando una traducción de destino, la **Destination Address (Dirección de destino)** es obligatoria. La dirección de destino (se permite un objeto de dirección) debe ser una máscara de red, no solo una dirección IPv6 y no un intervalo. La extensión del prefijo debe ser un valor desde /32 hasta /64, inclusive. Por ejemplo, 2001:db8::/32.

STEP 3 | Especifique el paquete traducido.

1. En la pestaña **Translated Packet**, si desea realizar la traducción de origen, en la sección Source Address Translation, para el **Translation Type**, seleccione **Static IP**. Si no desea realizar traducción de origen, seleccione **None**.
2. Si ha elegido **Static IP**, se muestra el campo **Translated Address**. Introduzca el objeto de dirección o el prefijo IPv6 traducido. Consulte las restricciones enumeradas en el paso anterior.

   *Se recomienda configurar su **Translated Address** para que sea el prefijo de la dirección de interfaz no fiable de su cortafuegos. Por ejemplo, si su interfaz no fiable tiene la dirección 2001:1a:1b:1::99/64, configure su **Translated Address (Dirección traducida)** como 2001:1a:1b:1::0/64.*
3. (Opcional) Seleccione **Bi-directional (Bidireccional)** si desea que el cortafuegos cree una traducción NPTv6 correspondiente en la dirección opuesta de la traducción que configure.

   *Si habilita la traducción **Bi-directional**, es muy importante asegurarse de tener establecidas políticas de seguridad para controlar el tráfico en ambas direcciones. Sin dichas reglas de política, la traducción **Bi-directional** permitirá la traducción automática de paquetes en ambas direcciones, algo que quizás no desee.*
4. Si desea realizar una traducción de destino, seleccione **Destination Address Translation (Traducción de dirección de destino)**. En el campo **Translated Address (Dirección traducida)**, seleccione un objeto de dirección o introduzca la dirección de destino interna.
5. Haga clic en **OK (Aceptar)**.

STEP 4 | Configuración del NDP Proxy.

Al configurar el cortafuegos para que actúe como un Proxy NDP para direcciones, este puede enviar anuncios de detección de vecinos (ND) y responder a solicitudes de ND de peers que están solicitando direcciones MAC de prefijos IPv6 asignados a dispositivos tras el cortafuegos.

1. Seleccione **Network (Red)** > **Interfaces** > **Ethernet** y seleccione una interfaz.
2. En la pestaña **Advanced (Avanzado)** > **NDP Proxy**, seleccione **Enable NDP Proxy (Habilitar proxy NDP)** y haga clic en **Add (Añadir)**.
3. Introduzca las **IP Address(es)** para las que está habilitado Proxy NDP. Puede ser una dirección, un intervalo de direcciones o un prefijo y longitud de prefijo. El orden de las

direcciones IP es indiferente. Lo idóneo es que estas direcciones sean las mismas que las direcciones traducidas que ha configurado en una política NPTv6.

Si la dirección es una subred, el Proxy NDP responderá a todas las direcciones en la subred, de modo que deberá enumerar los vecinos en la subred con Negate (Negar) seleccionado, como se describe en el siguiente paso.

4. (Opcional) Introduzca una o más direcciones para las que no desea habilitar Proxy NDP, y seleccione **Negate (Negar)**. Por ejemplo, desde un intervalo de dirección IP o intervalo de prefijos configurado en el paso anterior, puede negar un subconjunto pequeño de direcciones. Se recomienda negar las direcciones de los vecinos del cortafuegos.

STEP 5 | Confirme la configuración.

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

NAT64

NAT64 proporciona una manera de pasar a IPv6 cuando sigue necesitando comunicarse con redes IPv4. Cuando debe comunicarse desde una red solo IPv6 a una red IPv4, utiliza NAT64 para traducir direcciones de origen y de destino desde IPv6 a IPv4 y viceversa. NAT64 permite que los clientes de IPv6 accedan a servidores IPv4; y que los clientes de IPv4 accedan a servidores IPv6. Debe comprender NAT antes de configurar NAT64.

> Descripción general de NAT64
> Dirección IPv6 integrada en la dirección IPv4
> Servidor DNS64
> Detección de MTU de ruta
> Comunicación de Pv6 iniciada
> Configuración de NAT64 para la comunicación iniciada por IPv6
> Configuración de NAT64 para la comunicación iniciada por IPv4
> Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto

Descripción general de NAT64

Puede configurar dos tipos de traducción NAT64 en un cortafuegos de Palo Alto Networks®; cada uno realiza una traducción bidireccional entre dos familias de direcciones IP:

- El cortafuegos admite NAT64 con estado para la Comunicación de Pv6 iniciada, que asigna varias direcciones IPv6 a una dirección IPv4, además de conservar las direcciones IPv4. (No admite NAT64 sin estado, que asigna una dirección IPv6 a una dirección IPv4, y, por lo tanto, no conserva las direcciones IPv4). Configuración de NAT64 para la comunicación iniciada por IPv6.
- El cortafuegos admite la comunicación de IPv4 iniciada con un enlace estático que asigna una dirección IPv4 y un número de puerto a una dirección IPv6. Configuración de NAT64 para la comunicación iniciada por IPv4. También admite la reescritura de puertos, lo que permite conservar incluso más direcciones IPv4 traduciendo una dirección IPv4 y un número de puerto a una dirección IPv6 con varios números de puerto. Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto.

Una dirección IPv4 puede utilizarse para NAT44 y NAT64; no reserva un grupo de direcciones IPv4 solo para NAT64.

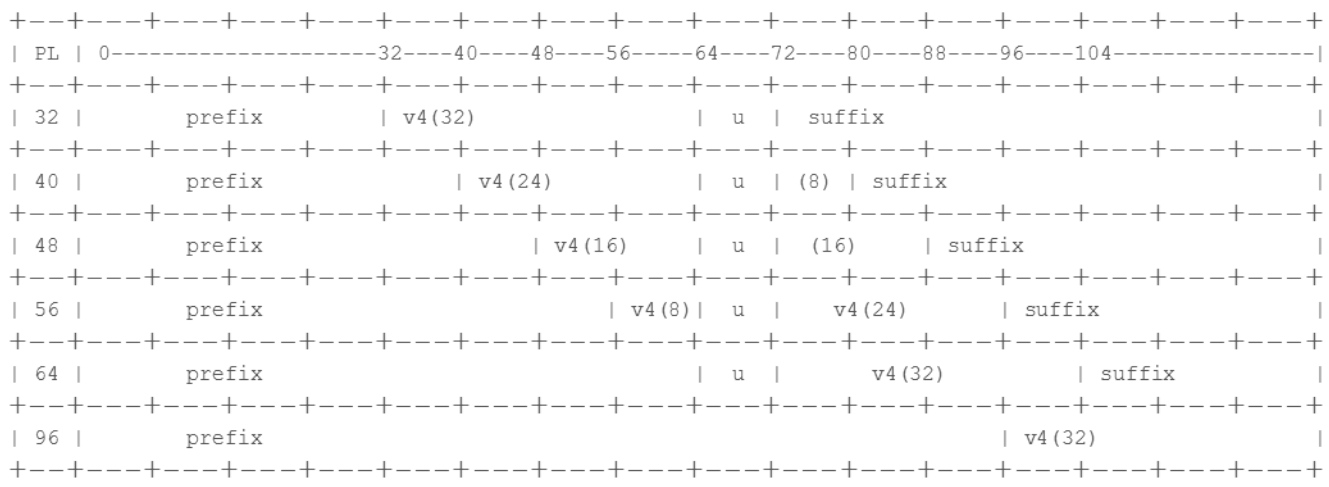
NAT64 opera en las interfaces, subinterfaces e interfaces de túnel de capa 3. Para utilizar NAT64 en el cortafuegos de Palo Alto Networks para la comunicación iniciada por IPv6, debe contar con un Servidor DNS64 externo o una solución para separar la función de consultas de DNS de la función NAT. El servidor DNS64 traduce entre su host IPv6 y un servidor DNS IPv4 codificando la dirección IPv4 que recibe de un servidor DNS público en una dirección IPv6 para el host IPv6.

Palo Alto Networks admite las siguientes funciones de NAT64:

- Redirección (Giro en U de NAT); además, NAT64 previene los ataques de bucle de redirección descartando todos los paquetes IPv6 entrantes que cuenten con un prefijo de origen 64::/n.
- Traducción de paquetes TCP/UDP/ICMP según RFC 6146 y el cortafuegos se esfuerza por traducir otros protocolos que no utilizan una puerta de enlace de nivel de aplicación (application-level gateway, ALG). Por ejemplo, el cortafuegos puede traducir un paquete GRE. Esta traducción tiene la misma limitación que NAT44: si no cuenta con una ALG para un protocolo que pueda utilizar un canal de control y datos separado, es posible que el cortafuegos no comprenda el flujo del tráfico de retorno.
- La traducción entre IPv4 y IPv6 del atributo de longitud de ICMP del campo de datagrama original, según RFC 4884.

Dirección IPv6 integrada en la dirección IPv4

NAT64 utiliza una dirección IPv6 integrada en la dirección IPv4 como se describe en RFC 6052, Direccionamiento de IPv6 para traductores de IPv4/IPv6. Una dirección IPv6 integrada en la dirección IPv4 es una dirección IPv6 con una dirección IPv4 decodificada en 32 bits. La longitud del prefijo (PL en la figura) de IPv6 determina donde se decodifica la dirección IPv4 en la dirección IPv6, de la siguiente manera:



El cortafuegos admite la traducción de subredes /32, /40, /48, /56, /64 y /96 utilizando estos prefijos. Un cortafuegos único admite múltiples prefijos; cada regla NAT64 utiliza un prefijo. El prefijo puede ser un prefijo conocido (64:FF9B::/96) o un prefijo específico de la red (NSP) que es único en la organización que controla el traductor de direcciones (el dispositivo DNS64). Por lo general, un NSP es una red dentro del prefijo IPv6 de la organización. Normalmente, el dispositivo DNS64 configura el campo u y el sufijo en cero; el cortafuegos ignora estos campos.

Servidor DNS64

Si desea utilizar DNS y realizar una traducción de NAT64 utilizando una Comunicación de Pv6 iniciada, debe utilizar un servidor DNS64 externo u otra solución DNS64 que se configure con el prefijo conocido o su NSP. Cuando un host IPv6 intenta acceder a un host ipV4 o un dominio en internet, el servidor DNS64 le solicita a un servidor DNS autorizado la dirección IPv4 asignada a ese nombre de host. El servidor DNS le envía un registro de dirección (registro A) al servidor DNS64 con la dirección IPv4 del nombre de host.

El servidor DNS64 convierte la dirección IPv4 en formato hexadecimal y la cifra en los octetos adecuados del prefijo IPv6 que su configuración le permite utilizar (el prefijo conocido o su NSP) en función de la longitud del prefijo, lo que produce una Dirección IPv6 integrada en la dirección IPv4. El servidor DNS64 envía un registro AAAA al host IPv6 que asigna la dirección IPv6 integrada en la dirección IPv4 al nombre de host IPv4.

Detección de MTU de ruta

IPv6 no fragmenta los paquetes, de modo que el cortafuegos utiliza dos métodos para reducir la necesidad de fragmentación de paquetes:

- Cuando el cortafuegos traduce paquetes IPv4 con un bit de no fragmentar (don't fragment, DF) en cero, esto indica que el remitente espera que el cortafuegos fragmente los paquetes que son demasiado grandes, pero que el cortafuegos no fragmenta paquetes para la red IPv6 (tras la traducción) debido a que IPv6 no fragmenta paquetes. En cambio, puede configurar el tamaño mínimo en el que el cortafuegos fragmentará los paquetes IPv4 antes de traducirlos. El valor **NAT64 IPv6 Minimum Network MTU (MTU de red mínima de IPv6 de NAT64e)** forma parte de la configuración, que cumple con RFC 6145, el algoritmo de traducción de IP/ICMP. Puede establecer la NAT64 IPv6 Minimum Network MTU (MTU de red mínima de IPv6 de NAT64) en su valor máximo (Device [Dispositivo]**Setup [Configuración]Session [Sesión]**), lo que provoca que el cortafuegos fragmente paquetes IPv4 en el tamaño mínimo de IPv6 antes de traducirlos a IPv6. (La **NAT64 IPv6 Minimum Network MTU [MTU de red mínima de IPv6 de NAT64]** no cambia la MTU de la interfaz).
- El otro método que utiliza el cortafuegos para reducir la fragmentación es la detección de MTU de ruta (Path MTU Discovery, PMTUD). En una comunicación de IPv4 iniciada, si un paquete IPv4 que se traducirá tiene un conjunto de bits de DF y la MTU de la interfaz de salida es más pequeña que el paquete, el cortafuegos utiliza la PMTUD para descartar el paquete y devolver un mensaje de ICMP "Destination Unreachable - fragmentation needed" (Destino inalcanzable: se requiere la fragmentación) al origen. El origen reduce la MTU de ruta para ese destino y reenvía el paquete hasta que las reducciones sucesivas en la MTU de ruta permiten la entrega del paquete.

Comunicación de Pv6 iniciada

La comunicación de IPv6 iniciada con el cortafuegos es similar a una NAT de origen en una topología IPv4. Realice la Configuración de NAT64 para la comunicación de IPv4 iniciada cuando su host IPv6 deba comunicarse con un servidor IPv4.

En la regla de la política NAT64, configure el origen original como dirección host IPv6 o como todos. Configure la dirección IPv6 de destino como prefijo conocido o el NSP que utiliza el servidor DNS64. (No configure la dirección IPv6 de destino completa en la regla).

Si debe utilizar un DNS, deberá utilizar un servidor DNS64 para convertir un resultado "A" DNS de IPv4 en un resultado "AAAA" fusionado con el prefijo NAT64. Si no utiliza un DNS, debe crear la dirección utilizando la dirección de destino IPv4 y el prefijo NAT64 configurado en el cortafuegos respetando las reglas RFC 6052.

En los entornos que utilizan un DNS, el siguiente ejemplo de topología ilustra la comunicación con el servidor DNS64. El servidor DNS64 debe configurarse de modo que se utilice el prefijo conocido 64:FF9B::/96 o el prefijo específico de la red, que debe cumplir con RFC 6052 (/32, /40,/48,/56,/64 o /96).

En el lado traducido del cortafuegos, el tipo de traducción debe ser IP dinámica y puerto para implementar NAT64 con estado. Configure la dirección de origen traducida para que sea la dirección IPv4 de la interfaz de salida en el cortafuegos. No configure el campo de traducción de destino; el cortafuegos traduce la dirección buscando la longitud del prefijo en la dirección original de destino de la regla y, luego, en función del prefijo, extrayendo la dirección IPv4 codificada de la dirección IPv6 de destino original en el paquete entrante.

Antes de que el cortafuegos observe la regla NAT64, el cortafuegos debe realizar una búsqueda de ruta para encontrar la zona de seguridad de destino de un paquete entrante. Debe garantizar que el prefijo NAT64 pueda alcanzarse mediante la asignación de zona de destino debido a que el cortafuegos no debe poder enrutar el prefijo NAT64. Probablemente, el cortafuegos asignaría el prefijo NAT64 a la ruta predeterminada o descartaría el prefijo NAT64 debido a que no existe una ruta para él. El cortafuegos no encontrará una zona de destino debido a que el prefijo NAT64 no se encuentra en la tabla de enrutamiento, asociado a la interfaz y la zona de salida.

Además, debe configurar una interfaz de túnel (sin punto de terminación). Aplique el prefijo NAT64 al túnel y aplique la zona adecuada para garantizar que el tráfico IPv6 con el prefijo NAT64 se asigna a la zona de destino correcta. El túnel también posee la ventaja de descartar el tráfico IPv6 con el prefijo NAT64 si el tráfico no coincide con la regla NAT64. El protocolo de enrutamiento configurado en el cortafuegos busca el prefijo IPv6 en su tabla de enrutamiento para buscar la zona de destino y busca en la regla NAT64.

La siguiente figura ilustra la función del servidor DNS64 en el proceso de resolución de nombres. En este ejemplo, el servidor DNS64 se configura de modo que se utilice el prefijo conocido 64:FF9B::/96.

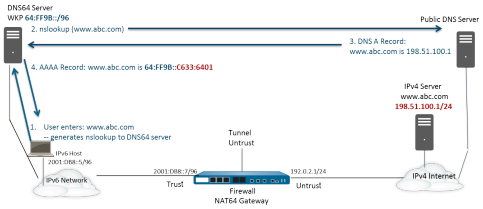
1. Un usuario en el host IPv6 ingresa a la URL www.abc.com, lo que genera una búsqueda en el servidor de nombres (nslookup) para el servidor DNS64.

2. El servidor DNS64 envía una nslookup de www.abc.com en el servidor DNS público y solicita su dirección IPv4.

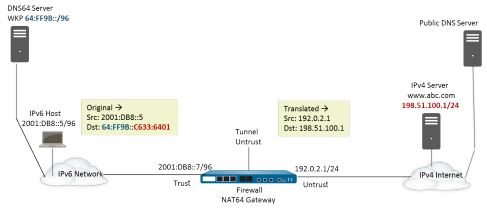
3. El servidor DNS devuelve un registro A que proporciona la dirección IPv4 al servidor DNS64.

4. El servidor DNS64 envía un registro AAAA al usuario IPv6, lo que convierte la dirección IPv4 decimal delimitada con puntos 198.51.100.1 en la dirección hexadecimal C633:6401 y la integra en su propio prefijo IPv6, 64:FF9B::/96. [198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] El resultado es la dirección IPv6 integrada en la dirección IPv4 64:FF9B::C633:6401.

Tenga en cuenta que en un prefijo /96, la dirección IPv4 se compone de los últimos cuatro octetos codificados en la dirección IPv6. Si el servidor DNS64 utiliza un prefijo /32, /40, /48, /56 o /64, la dirección IPv4 se codifica como se muestra en RFC 6052.



Tras la resolución de nombres transparente, el host IPv6 envía un paquete al cortafuegos con su dirección IPv6 de origen y su dirección IPv6 de destino 64:FF9B::C633:6401, como lo determina el servidor DNS64. El cortafuegos realiza la traducción de NAT64 en función de su regla NAT64.



Configuración de NAT64 para la comunicación iniciada por IPv6

Esta tarea de configuración y sus direcciones corresponden a las figuras de Comunicación iniciada por IPv6.

STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree un objeto de dirección para la dirección de destino IPv6 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, servidor nat64-IPv4.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese el prefijo IPv6 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96). Este es el prefijo conocido o su prefijo específico de red que está configurado en el servidor DNS64.

   Para este ejemplo, ingrese 64:FF9B::/96.

   El origen y el destino deben tener la misma máscara de red (extensión del prefijo).

   (Usted no introduce una dirección de destino completa porque, según la extensión del prefijo, el cortafuegos extrae la dirección IPv4 de la dirección IPv6 de destino original en el paquete entrante. En este ejemplo, el prefijo del paquete entrante está codificado con C633:6401 en hexadecimal, que es la dirección de destino IPv4 198.51.100.1).
4. Haga clic en **OK (Aceptar)**.

STEP 3 | (Opcional) Cree un objeto de dirección para la dirección de origen IPv6 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección del host IPv6; en este ejemplo, 2001:DB8::5/96.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | (Opcional) Cree un objeto de dirección para la dirección de origen IPv4 (traducida).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv4 de la interfaz de salida del cortafuegos; en este ejemplo, 192.0.2.1.
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv6_init.
3. (Opcional) Introduzca una **descripción**.
4. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 6 | Especifique la información de origen y destino original.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona fiable.
2. Seleccione la **Destination Zone (Zona de destino)**; en este ejemplo, la zona no fiable.
3. (Opcional) Seleccione una **Destination Interface (Interfaz de destino)** o la opción predeterminada (**any [cualquiera]**).
4. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección que creó para el host IPv6.
5. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** para añadir el objeto de dirección que creó para el destino IPv6; en este ejemplo, servidor nat64-IPv4.
6. (Opcional) Para **Service (Servicio)**, seleccione **any (cualquiera)**.

STEP 7 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, para **Translation Type (Tipo de traducción)**, seleccione **Dynamic IP and Port (IP dinámica y puerto)**.
2. Para **Address Type (Tipo de dirección)**, seleccione una de las siguientes opciones:
   - Seleccione **Translated Address (Dirección traducida)** y luego **Add (Añadir)** para añadir el objeto que creó para la dirección de origen IPv4.
   - Seleccione **Interface Address (Dirección de interfaz)**, en cuyo caso la dirección de origen traducida es la dirección IP y la máscara de red de la interfaz de salida del cortafuegos. Para esta opción, debe seleccionar **Interface (Interfaz)** y opcionalmente una **IP Address (Dirección IP)** si la interfaz tiene más de una dirección IP.
3. Deje **Destination Address Translation (Traducción de dirección de destino)** sin seleccionar. (El cortafuegos extrae la dirección IPv4 del prefijo IPv6 en el paquete entrante, según la extensión del prefijo especificada en el destino original de la regla NAT64).
4. Haga clic en **OK (Aceptar)** para guardar la regla de política de NAT64.

STEP 8 | Configure una interfaz de túnel para emular una interfaz de bucle invertido con una máscara de red que no sea 128.

1. Seleccione **Network (Red)** > **Interfaces** > **Tunnel (Túnel)** y haga clic en **Add (Añadir)** para añadir un túnel.
2. En **Interfaz Name (Nombre de interfaz)**, especifique un sufijo numérico, como .2.
3. En la pestaña **Config**, seleccione el **Virtual Router (Enrutador virtual)** donde configuró NAT64.
4. Para **Security Zone (Zona de seguridad)**, seleccione la zona de destino asociada con el destino de servidor IPv4 (zona fiable).
5. En la pestaña **IPv6**, seleccione **Enable IPv6 on the interface (Habilitar IPv6 en la interfaz)**.
6. Haga clic en **Add (Añadir)** y para **Address (Dirección)**, seleccione **New Address (Nueva dirección)**.
7. Introduzca en **Name (Nombre)** un nombre para el perfil.
8. (Opcional) Introduzca una **Description (Descripción)** para la dirección de túnel.
9. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese su prefijo IPv6 y la extensión del prefijo; en este ejemplo, 64:FF9B::/96.
10. Haga clic en **OK (Aceptar)**.
11. Seleccione **Enable address on interface (Habilitar la dirección en la interfaz)** y haga clic en **OK (Aceptar)**.
12. Haga clic en **OK (Aceptar)**.
13. Haga clic en **OK (Aceptar)** para guardar el túnel.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Trust (Fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **Untrust (No fiable)**.
5. Para **Application (Aplicación)**, seleccione **Any (Cualquiera)**.
6. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
7. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

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

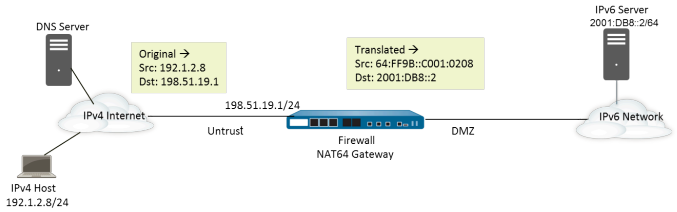
STEP 11 | Solucione los problemas o visualice una sesión NAT64.

```
> show session id <session-id>
```


Configuración de NAT64 para la comunicación iniciada por IPv4

La comunicación de IPv4 iniciada con un servidor IPv6 es similar a una NAT de destino en una topología IPv4. La dirección IPv4 de destino se asigna a la dirección IPv6 de destino mediante una traducción de IP estática uno a uno (no una traducción de varios a uno).

El cortafuegos codifica la dirección IPv4 de origen en el prefijo conocido 64:FF9B::/96 como se define en RFC 6052. La dirección de destino traducida no es la dirección IPv6 real. Por lo general, el caso de uso de la comunicación de IPv4 iniciada se presenta cuando una organización proporciona acceso de la zona pública Untrust a un servidor IPv6 en la zona DMZ de la organización. Esta topología no utiliza un servidor DNS64.



STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cuando un paquete IPv4 posee su bit DF configurado en cero (y debido a que IPv6 no fragmenta los paquetes), asegúrese de que el paquete IPv6 traducido no supera la ruta MTU para la red IPv6 de destino.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. En **NAT64 IPv6 Minimum Network MTU (MTU de red mínima de IPv6 de NAT64)**, introduzca la cantidad mínima de bytes en la que el cortafuegos fragmentará los paquetes IPv4 para la traducción a IPv6 (rango: 1280 a 9216, valor predeterminado: 1280).

   Si no desea que el cortafuegos fragmente un paquete IPv4 antes de la traducción, configure el MTU en 9216. Si el paquete IPv6 traducido supera este valor, el cortafuegos descarta el paquete y emite un paquete ICMP que indica que el destino es inalcanzable y que se necesita fragmentación.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un objeto de dirección para la dirección de destino IPv4 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_ip4server.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red)** e ingrese la dirección IPv4 de la interfaz del cortafuegos en la zona no fiable. La dirección no debe usar una máscara de red o solo una máscara de red de /32. Este ejemplo utiliza 198.51.19.1/32.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Cree un objeto de dirección para la dirección de origen IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name (Nombre)**; por ejemplo, nat64_ip6source.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 NAT64 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96).

   Para este ejemplo, ingrese 64:FF9B::/96.

   (El cortafuegos codifica el prefijo con la dirección de origen IPv4 192.1.2.8, que es C001:0209 en hexadecimal).
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree un objeto de dirección para la dirección de destino IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_server_2.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 del servidor IPv6 (destino). La dirección no debe usar una máscara de red o solo una máscara de red de /128. Este ejemplo utiliza 2001:DB8::2/128.
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv4_init.
3. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 7 | Especifique la información de origen y destino original.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona no fiable.
2. Seleccione la **Destination Zone (Zona de destino)**, probablemente una zona fiable o DMZ.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección para el host IPv4.
4. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** el objeto de dirección para el destino IPv4; en este ejemplo, nat64_ip4server.
5. En **Service (Servicio)**, seleccione **any (cualquiera)**.

STEP 8 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)**.
2. Para **Translated Address (Dirección traducida)**, seleccione el objeto de dirección traducida que creó, nat64_ip6source.
3. En **Destination Address Translation (Traducción de dirección de destino)**, para **Translated Address (Dirección traducida)**, especifique una unica dirección IPv6 (el objeto de dirección; en este ejemplo, nat64_server_2 o la dirección IPv6 del servidor).
4. Haga clic en **OK (Aceptar)**.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona no fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Untrust (No fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **DMZ**.
5. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

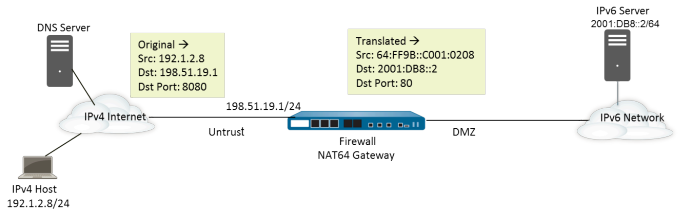
Haga clic en **Commit (Confirmar)**.

STEP 11 | Solucione los problemas o visualice una sesión NAT64.

```
> show session id <session-id>
```


Configuración de NAT64 para la comunicación iniciada por IPv4 con traducción de puerto

Esta tarea parte de la tarea de configuración de NAT64 para la comunicación iniciada por IPv4, pero la organización que controla la red IPv6 prefiere traducir el número de puerto de destino público a un número de puerto de destino interno y, por lo tanto, mantenerlo en privado para los usuarios del lado no fiable IPv4 del cortafuegos. En este ejemplo, el puerto 8080 se traduce en el puerto 80. Para hacer eso, en la regla de política NAT64, cree un nuevo servicio que especifique que el puerto de destino es 8080. Para el paquete traducido, el puerto traducido es 80.



STEP 1 | Habilite IPv6 para que opere en el cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Seleccione **Enable IPv6 Firewalling (Habilitar cortafuegos de IPv6)**.
3. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Cuando un paquete IPv4 posee su bit DF configurado en cero (y debido a que IPv6 no fragmenta los paquetes), asegúrese de que el paquete IPv6 traducido no supera la ruta MTU para la red IPv6 de destino.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.
2. Para **NAT64 IPv6 Minimum Network MTU (MTU de red mínima IPv6 NAT64)**, ingrese el número más bajo de bytes en los cuales el cortafuegos fragmentará los paquetes IPv4 para la traducción en IPv6 (el intervalo es 1280 a 9216; el valor predeterminado es 1280).

   Si no desea que el cortafuegos fragmente un paquete IPv4 antes de la traducción, configure el MTU en 9216. Si el paquete IPv6 traducido supera este valor, el cortafuegos descarta el paquete y emite un paquete ICMP que indica que el destino es inalcanzable y que se necesita fragmentación.
3. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un objeto de dirección para la dirección de destino IPv4 (previo a la traducción).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_ip4server.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red)** e ingrese la dirección IPv4 y máscara de red de la interfaz del cortafuegos en la zona no fiable. Este ejemplo utiliza 198.51.19.1/24.
4. Haga clic en **OK (Aceptar)**.

STEP 4 | Cree un objeto de dirección para la dirección de origen IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name (Nombre)**; por ejemplo, nat64_ip6source.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 NAT64 con una máscara de red que cumpla con RFC 6052 (/32, /40, /48, /56, /64 o /96).

   Para este ejemplo, ingrese 64:FF9B::/96.

   (El cortafuegos codifica el prefijo con la dirección de origen IPv4 192.1.2.8, que es C001:0209 en hexadecimal).
4. Haga clic en **OK (Aceptar)**.

STEP 5 | Cree un objeto de dirección para la dirección de destino IPv6 (traducido).

1. Seleccione **Objects (Objetos)** > **Addresses (Direcciones)** y haga clic en **Add (Añadir)**.
2. Introduzca un nombre para el objeto en **Name**; por ejemplo, nat64_server_2.
3. Para **Type (Tipo)**, seleccione **IP Netmask (Máscara de red IP)** e ingrese la dirección IPv6 del servidor IPv6 (destino). Este ejemplo utiliza 2001:DB8::2/64.

   El origen y el destino deben tener la misma máscara de red (extensión del prefijo).
4. Haga clic en **OK (Aceptar)**.

STEP 6 | Cree la regla NAT64.

1. Seleccione **Policies (Políticas)** > **NAT** y haga clic en **Add (Añadir)**.
2. En la pestaña **General**, introduzca un **Name (Nombre)** para la regla NAT64; por ejemplo, nat64_ipv4_init.
3. Para **NAT Type (Tipo de NAT)**, seleccione **nat64**.

STEP 7 | Especifique la información de origen y destino original, y cree un servicio para limitar la traducción a un solo número de puerto de ingreso.

1. Para **Original Packet (Paquete original)**, seleccione **Add (Añadir)** para añadir la **Source Zone (Zona de origen)**, posiblemente una zona no fiable.
2. Seleccione la **Destination Zone (Zona de destino)**, probablemente una zona fiable o DMZ.
3. Para **Service (Servicio)**, seleccione New **Service (Nuevo servicio)**.
4. Introduzca un nombre para el servicio en **Name**, tal como Port_8080.
5. Seleccione **TCP** como el **Protocol (Protocolo)**.
6. Para **Destination Port (Puerto de destino)**, ingrese 8080.
7. Haga clic en **OK (Aceptar)** para guardar el servicio.
8. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**o **Add (Añadir)** para añadir el objeto de dirección para el host IPv4.
9. Para **Destination Address (Dirección de destino)**, seleccione **Add (Añadir)** el objeto de dirección para el destino IPv4; en este ejemplo, nat64_ip4server.

STEP 8 | Especifique la información de paquete traducido.

1. Para el **Translated Packet (Paquete traducido)**, en **Source Address Translation (Traducción de dirección de origen)**, **Translation Type (Tipo de traducción)**, seleccione **Static IP (IP estática)**.
2. Para **Translated Address (Dirección traducida)**, seleccione el objeto de dirección traducida que creó, nat64_ip6source.
3. En **Destination Address Translation (Traducción de dirección de destino)**, para **Translated Address (Dirección traducida)**, especifique una unica dirección IPv6 (el objeto de dirección; en este ejemplo, nat64_server_2 o la dirección IPv6 del servidor).
4. Especifique el número de **Translated Port (Puerto traducido)** de destino privado al cual el cortafuegos traducirá el número de puerto de destino público; en este ejemplo, 80.
5. Haga clic en **OK (Aceptar)**.

STEP 9 | Cree una política de seguridad para permitir el tráfico NAT de la zona no fiable.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** de regla.
2. Seleccione **Source (Origen)** y luego **Add (Añadir)** para añadir una **Source Zone (Zona de origen)**; seleccione **Untrust (No fiable)**.
3. Para **Source Address (Dirección de origen)**, seleccione **Any (Cualquiera)**.
4. Seleccione **Destination (Destino)** y **Add (Añadir)** para añadir una **Destination Zone (Zona de destino)**; y seleccione **DMZ**.
5. Para **Actions (Acciones)**, seleccione **Allow (Permitir)**.
6. Haga clic en **OK (Aceptar)**.

STEP 10 | Confirme los cambios.

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

STEP 11 | Solucione los problemas o visualice una sesión NAT64.

```
> show session id <session-id>
```


ECMP

El procesamiento de trayectoria múltiple a igual coste (ECMP) es una función de red que permite al cortafuegos usar hasta cuatro rutas de igual coste hacia el mismo destino. Sin esta función, si hay múltiples rutas del mismo coste al mismo destino, el enrutador virtual selecciona una de estas rutas de la tabla de enrutamiento y la añade a su tabla de envío; no usará ninguna de las demás rutas a no ser que se interrumpa la ruta seleccionada.

La habilitación de la funcionalidad ECMP en un enrutador virtual permite que el cortafuegos tenga hasta cuatro rutas del mismo coste a un destino en esta tabla de reenvío, permitiendo que el cortafuegos:

- Equilibre la carga de los flujos (sesiones) al mismo destino en múltiples enlaces del mismo coste.
- Use de forma eficiente el ancho de banda disponible en enlaces hacia el mismo destino, en lugar de dejar algunos enlaces sin usar.
- Cambie dinámicamente el tráfico a otro miembro de ECMP hacia el mismo destino si falla un enlace, en lugar de tener que esperar a que el protocolo de enrutamiento o la tabla RIB seleccione una ruta alternativa. Esto puede ayudar a reducir el tiempo de inactividad cuando falla el enlace.

ECMP es compatible con todos los modelos de cortafuegos de Palo Alto Networks® y cuenta con compatibilidad con el reenvío mediante hardware los PA-7000 Series, PA-5200 y PA-3200. Los cortafuegos VM-Series admiten ECMP solo mediante software. El rendimiento se ve afectado para las sesiones que no se pueden descargar mediante hardware.

ECMP es compatible con Capa 3, subinterfaz de Capa 3, VLAN, túnel e interfaces de Ethernet de agregación.

ECMP se puede configurar para rutas estáticas y cualquiera de los protocolos de enrutamiento dinámico compatibles con el cortafuegos.

ECMP afecta a la capacidad de la tabla de enrutamiento porque la capacidad se basa en el número de rutas, de modo que una ruta ECMP con cuatro rutas consumirá cuatro entradas de la capacidad de la tabla de enrutamiento. La implementación de ECMP puede reducir ligeramente la capacidad de la tabla de enrutamiento porque se utiliza más memoria para usar etiquetas basadas en sesiones para asignar los flujos de tráfico a interfaces particulares.

El enrutamiento de enrutador a enrutador virtual mediante rutas estáticas no es compatible con ECMP.

Para obtener información sobre la selección de ruta ECMP cuando un peer HA falla, consulte ECMP en modo HA activo/activo.

Las siguientes secciones describen ECMP y cómo configurarlo.

- Algoritmos de equilibrio de carga de ECMP
- Configuración de ECMP en un enrutador virtual
- Habilitación de ECMP para varios sistemas BGP autónomos
- Verificación de ECMP

Algoritmos de equilibrio de carga de ECMP

Supongamos que la base de información de enrutamiento (RIB, Routing Information Base) del cortafuegos tiene múltiples trayectorias a igual coste a un único destino. El número máximo de rutas a igual coste es 2 de manera predeterminada. ECMP elige las dos mejores rutas de igual coste de la RIB para copiarlas a la base de información de reenvío (FIB, Forwarding Information Base). ECMP determina a continuación y basándose en el método de equilibrio de carga, cuál de las dos rutas en la FIB usará el cortafuegos para la designación durante esta sesión.

El equilibrio de carga de ECMP se realiza en este nivel de sesión, no en el nivel de paquete; el inicio de una nueva sesión se produce cuando el cortafuegos (ECMP) elige una ruta a igual coste. Las rutas a igual coste a un único destino se consideran miembros de la ruta de ECMP o miembros del grupo ECMP. ECMP determina cuál de las múltiples rutas a un destino en la FIB se utiliza para un flujo de ECMP, en función del algoritmo de equilibrio de carga que haya definido. Un enrutador virtual solo puede usar un algoritmo de equilibrio de carga.

Habilitar, deshabilitar o cambiar ECMP en un enrutador virtual existente provoca que el sistema reinicie el enrutador virtual, lo cual podría ocasionar que se cierren las sesiones existentes.

Cada uno de los cuatro algoritmos posibles hace hincapié en una prioridad diferente, tal y como se indica a continuación:

- **Los algoritmos basados en hash dan prioridad a la permanencia de la sesión**: los algoritmos **IP Modulo** e **IP Hash** usan hashes basados en la información del encabezado de paquete, como las direcciones de origen y destino. Dado que el encabezado de cada flujo en una sesión determinada contiene la misma información de origen y destino, estas opciones conceden prioridad a la ***pegajosidad*** de la sesión. Si elige el algoritmo **IP Hash**, el hash puede basarse en las direcciones de origen y destino o en la dirección de origen únicamente. Al usar un hash IP basado únicamente en la dirección de origen, todas las sesiones que pertenecen a la misma dirección IP tomarán siempre la misma ruta de las diversas rutas disponibles. Por lo tanto, la ruta se considera adhesiva y es más fácil detectar problemas en ella si fuera necesario. Puede definir opcionalmente un valor de **Hash Seed (Inicialización de hash)** para aleatorizar aún más el equilibrio de carga si tiene un gran número de sesiones hacia el mismo destino y no se están distribuyendo de manera uniforme entre los enlaces ECMP.
- **Los algoritmos equilibrados dan prioridad al equilibrio de carga**: el algoritmo **Balanced Round Robin (Operación por turnos equilibrada)** distribuye las sesiones entrantes equitativamente entre los enlaces, dando prioridad al equilibrio de carga sobre la permanencia de la sesión. (La operación por turnos indica una secuencia en la que se elige el elemento que hace más tiempo que no se escoge). Asimismo, si se añaden nuevas rutas o se eliminan de un grupo ECMP (por ejemplo, si una ruta del grupo deja de estar disponible), el enrutador virtual reequilibrará las sesiones en todos los enlaces del grupo. Además, si los flujos en una sesión tienen que conmutar rutas debido a una caída del servicio, cuando la ruta original asociada a la sesión vuelva a estar disponible, los flujos de la sesión se revertirán a la ruta original cuando el enrutador virtual reequilibre de nuevo la carga.
- **Weighted algorithm prioritizes link capacity and/or speed (El algoritmo ponderado prioriza la capacidad o velocidad de enlace)**: como una extensión del estándar del protocolo ECMP, la implementación de Palo Alto Networks® ofrece una opción de equilibrio de carga para **Weighted Round Robin** que tiene en cuenta las diferentes capacidades y velocidades de los enlaces en

las interfaces de salida del cortafuegos. Con esta opción, puede asignar **ponderaciones de ECMP** (el intervalo es de 1 a 255; el valor predeterminado es 100) a las interfaces basadas en el rendimiento de enlaces mediante factores como la capacidad, velocidad y latencia de los enlaces para garantizar que las cargas se equilibren con el fin de aprovechar por completo los enlaces disponibles.

Por ejemplo, imaginemos que el cortafuegos tiene enlaces redundantes a un ISP: Ethernet 1/1 (100 Mbps) y Ethernet 1/8 (200 Mbps). Aunque son rutas a igual coste, el enlace a través de Ethernet 1/8 ofrece un mayor ancho de banda y por lo tanto puede gestionar una mayor carga que el enlace Ethernet 1/1. Por lo tanto, para garantizar que la funcionalidad de equilibrio de carga tiene en cuenta la capacidad y velocidad de los enlaces, debe asignar a Ethernet 1/8 un peso de 200 y a Ethernet 1/1 un peso de 100. La relación de ponderación 2:1 hace que el enrutador virtual envíe el doble de sesiones a Ethernet 1/8 que a Ethernet 1/1. Sin embargo, dado que el protocolo ECMP se basa esencialmente en sesiones, al usar el algoritmo **Weighted Round Robin (Operación por turnos ponderada)**, el cortafuegos podrá equilibrar la carga a todos los enlaces de ECMP basándose solo en la mejor opción.

Tenga en cuenta que los pesos de ECMP se asignan a las interfaces para determinar el equilibrio de carga (para influir qué ruta ***a igual coste*** se elige), no para la selección de ruta (una elección de ruta entre rutas que podrían tener diferentes costes).

Asigne enlaces de menor velocidad o capacidad con un peso menor. Asigne enlaces de mayor velocidad o capacidad con un peso mayor. De este modo, el cortafuegos puede distribuir sesiones basándose en estas relaciones, en lugar de saturar un enlace de baja capacidad que es una de las rutas a igual coste.

Configuración de ECMP en un enrutador virtual

Utilice el siguiente procedimiento para habilitar ECMP en un enrutador virtual. Los requisitos previos son:

- Especifique las interfaces que pertenecen a un enrutador virtual (**Network [Red]** > **Virtual Routers [Enrutadores virtuales]** > **Router Settings [Configuración de enrutador]** > **General [General]**).
- Especifique el protocolo de enrutamiento de IP.

La habilitación, deshabilitación o cambio de ECMP para un enrutador virtual existente hace que el sistema reinicie el enrutador virtual, que puede causar la terminación de las sesiones.

STEP 1 | Habilitación de ECMP para un enrutador virtual.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual en el que se habilitará ECMP.
2. Seleccione **Router Settings (Configuración de enrutador)** > **ECMP** y seleccione **Enable (Habilitar)**.

STEP 2 | (Opcional) Habilite el retorno simétrico de paquetes del servidor al cliente.

Seleccione **Symmetric Return (Retorno simétrico)** para que los paquetes de retorno salgan de la misma interfaz a la que llegaron los paquetes de entrada asociados. Es decir, que el cortafuegos usará la interfaz de entrada a la que enviar los paquetes de retorno, en lugar de usar la interfaz ECMP. El ajuste de **Symmetric Return** anula el equilibrio de carga. Este comportamiento solo se produce con flujos de tráfico del servidor al cliente.

STEP 3 | Habilite **Strict Source Path (Ruta de origen estricta)** para asegurarse de que el tráfico IKE e IPSec que se origina en el cortafuegos salga de la interfaz física a la que pertenece la dirección IP de origen del túnel IPSec.

Cuando habilite ECMP, el tráfico IKE e IPSec que se origina en el cortafuegos de forma predeterminada, sale de una interfaz que determina un método de equilibrio de carga ECMP. También puede habilitar Strict Source Path (Ruta de origen estricta) para asegurarse de que el tráfico IKE e IPSec que se origina en el cortafuegos siempre salga de la interfaz física a la que pertenece la dirección IP de origen del túnel IPSec. Debe habilitar esta función cuando el cortafuegos tenga más de un ISP que proporcione rutas de igual coste al mismo destino. Los ISP suelen realizar una verificación de reenvío de ruta (RPF, Path Forwarding) inversa (o una verificación diferente para evitar la suplantación de direcciones IP) para confirmar que el tráfico está saliendo por la misma interfaz por la que llegó. Debido a que ECMP elegiría una interfaz de salida basada en el método ECMP configurado (en lugar de elegir la interfaz de origen como interfaz de salida), no sería el comportamiento esperado por el ISP y este podría bloquear el tráfico de retorno legítimo. En ese caso, habilite la ruta de origen estricta para que el cortafuegos use la interfaz de salida que es la interfaz a la que pertenece la dirección IP de origen del túnel IPSec, en la que se realiza la verificación RPF correctamente y donde el ISP permite el tráfico de retorno.

STEP 4 | Especifique el número máximo de rutas a igual coste (a una red de destino) que se pueden copiar desde la base de información de rutas (RIB) a la base de información de reenvío (FIB).

Para el valor máximo de rutas permitidas, en **Max Path (Ruta máxima)**, introduzca **2**, **3** o **4**. Default: 2.

STEP 5 | Seleccione el algoritmo de equilibrio de carga para el enrutador virtual. Para obtener más información sobre los métodos de equilibrio de carga y sus diferencias, consulte Algoritmos de equilibrio de carga ECMP .

En **Load Balance (Equilibrio de carga)**, seleccione una de las siguientes opciones en la lista **Method (Método)**:

- **IP Modulo** (predeterminado): usa un hash de las direcciones IP de origen y destino en el encabezado del paquete para determinar qué ruta ECMP se usará.
- **IP Hash**: existen dos métodos de hash IP que determinan qué ruta ECMP se usará (seleccione las opciones de hash en el paso 5):
  - Use un hash de la dirección de origen (disponible en PAN-OS 8.0.3 y versiones posteriores).
  - Utilice un hash de las direcciones IP de origen y destino (el método de hash IP predeterminado).
- **Balanced Round Robin (Operación por turnos equilibrada)**: usa operación por turnos entre rutas ECMP y reequilibra las rutas cuando cambia el número de rutas.
- **Weighted Round Robin**: usa operación por turnos y un peso relativo para seleccionar entre las rutas ECMP. Especifique los grados de ponderación en el paso 6 siguiente.

STEP 6 | (IP Hash únicamente) Configure las opciones de hash de IP.

Si ha seleccionado **IP Hash** como el **Method**:

1. Seleccione **Use Source Address Only (Usar dirección de origen únicamente)** (disponible en PAN-OS 8.0.3 y versiones posteriores) si desea asegurarse de que todas las sesiones que pertenecen a la misma dirección IP tomen siempre la misma ruta de las múltiples rutas disponibles. Esta opción de hash de IP proporcionan permanencia de la ruta y facilita la resolución de problemas. Si no selecciona esta opción o utiliza una versión anterior a PAN-OS 8.0.3, el hash de IP se basa en las direcciones IP de origen y destino (el método de hash de IP predeterminado).

   *Si selecciona **Use Source Address Only (Usar dirección de origen únicamente)**, no debe enviar la configuración de Panorama a los cortafuegos que ejecutan PAN-OS 8.0.2, 8.0.1 o 8.0.0.*

2. Seleccione **Use Source/Destination Ports** si desea usar los números de puerto de origen y destino en el cálculo de **IP Hash**.

   *La habilitación de esta opción junto con **Use Source Address Only (Usar la dirección de origen únicamente)** asignará aleatoriamente la selección de ruta incluso para las sesiones que pertenecen a la misma dirección IP de origen.*

3. Introduzca un valor **Hash Seed (Inicialización de hash)** (un valor entero con un máximo de nueve dígitos). Especifique un valor **Hash Seed** para aleatorizar aún más el equilibrio de

carga. Especificar un valor de inicialización de hash resulta útil si tiene un gran número de sesiones con la misma información de tupla.

STEP 7 | (Solo para Weighted Round Robin [Operación por turnos ponderada]) Defina un peso para cada interfaz en el grupo ECMP.

Si ha seleccionado **Weighted Round Robin** como **Method**, defina un peso para cada una de las interfaces que constituyen los puntos de salida para enrutar el tráfico a los mismos destinos (es decir, interfaces que forman parte de un grupo ECMP, como las interfaces que ofrecen enlaces redundantes a su ISP o interfaces a las aplicaciones empresariales fundamentales de su red corporativa).

A mayor peso, con mayor frecuencia se seleccionará la ruta a igual coste para una nueva sesión.

Aporte a los enlaces de mayor velocidad un peso más alto que a los enlaces más lentos, con el fin de que haya más tráfico ECMP que atraviese el enlace más rápido.

1. Para crear un grupo de ECMP, haga clic en **Add (Añadir)** y seleccione una interfaz en **Interface (Interfaz)**.
2. Seleccione **Add** para añadir las otras interfaces en el grupo ECMP.
3. Haga clic en **Weight (Peso)** y especifique el peso relativo de cada interfaz (el intervalo es 1-255; el valor por defecto es 100).

STEP 8 | Guarde la configuración.

1. Haga clic en **OK (Aceptar)**.
2. En el mensaje de cambio de configuración ECMP, haga clic en **Yes** para reiniciar el enrutador virtual. Al reiniciar el enrutador virtual, puede que se terminen las sesiones existentes.

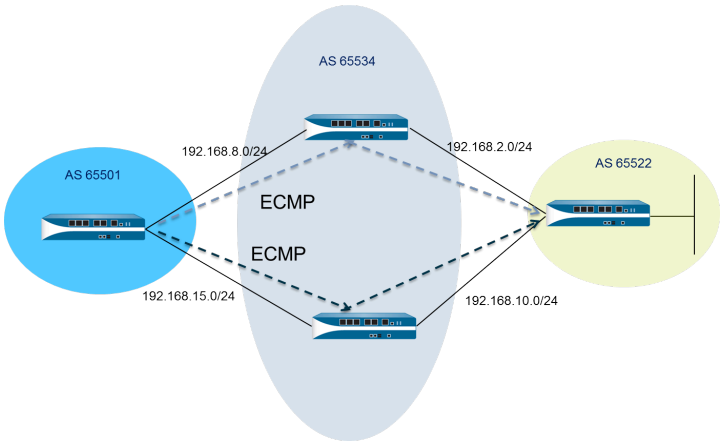
Este mensaje se muestra solo si está modificando un enrutador virtual con ECMP.

STEP 9 | Confirme los cambios.

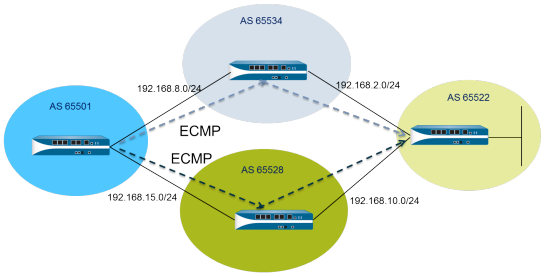
Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Habilitación de ECMP para varios sistemas BGP autónomos

Realice la siguiente tarea si ha configurado BGP y quiere habilitar ECMP en varios sistemas autónomos. Para esta tarea se da por hecho que ya ha configurado BGP. En la figura siguiente, dos rutas ECMP a un destino atraviesan dos cortafuegos que pertenecen a un único ISP en un único sistema BGP autónomo.



En la figura siguiente, dos rutas ECMP a un destino atraviesan dos cortafuegos que pertenecen a dos ISP diferentes en sistemas BGP autónomos distintos.



STEP 1 | Configurar ECMP.

Consulte Configuración de ECMP en un enrutador virtual.

STEP 2 | Para el enrutamiento de BGP, habilite ECMP en múltiples sistemas autónomos.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual en el que se habilitará ECMP para múltiples sistemas BGP autónomos.
2. Seleccione **BGP** > **Advanced (Avanzado)** y seleccione **ECMP Multiple AS Support (Soporte de AS de múltiple ECMP)**.

STEP 3 | Confirme los cambios.

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

Verificación de ECMP

Un enrutador virtual configurado para ECMP indica en la base de información de reenvío (FIB) qué rutas son ECMP. Una marca ECMP (E) para una ruta indica que está participando en ECMP para la interfaz de salida al siguiente salto para esa ruta. Para verificar el ECMP, utilice el siguiente procedimiento para observar la FIB y confirmar que algunas rutas son rutas múltiples a igual coste.

STEP 1 | Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**.

STEP 2 | En la fila del enrutador virtual en el que ha habilitado ECMP, haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.

STEP 3 | Seleccione **Routing (Enrutamiento)** > **Forwarding Table (Tabla de reenvío)** para ver la FIB.

En la tabla, observe que varias rutas al mismo destino (excepto una interfaz diferente) tienen la marca E. Un asterisco (*) indica la ruta preferida para el grupo ECMP.

LLDP

Los cortafuegos de Palo Alto Networks® son compatibles con el protocolo de detección de nivel de enlace (LLDP), que funciona en la capa de enlace para detectar dispositivos cercanos y sus capacidades. LLDP permite al cortafuegos y a otros dispositivos de la red intercambiar (enviar y recibir) unidades de datos LLDP (LLDPDU) con los vecinos. El dispositivo receptor almacena la información en un MIB, a la que puede acceder el protocolo simple de administración de redes (SNMP). LLDP facilita la solución de problemas, especialmente en el caso de implementaciones de virtual wire donde el cortafuegos suele pasar desapercibido en una topología de red.

- Descripción general de LLDP
- TLV compatibles con LLDP
- Mensajes de Syslog LLDP y capturas de SNMP
- Configuración de LLDP
- Visualización de estados y configuración de LLDP
- Borrado de estadísticas de LLDP

Descripción general de LLDP

El protocolo de detección de nivel de enlace (LLDP) opera en la capa 2 del modelo OSI mediante direcciones MAC. Una LLDPDU es una secuencia de elementos de tipo-longitud-valor (TLV) encapsulados en una trama Ethernet. El estándar IEEE 802.1AB define tres direcciones MAC para LLDPDU: 01-80-C2-00-00-0E, 01-80-C2-00-00-03 y 01-80-C2-00-00-00.

El cortafuegos de Palo Alto Networks® solo admite una dirección MAC para transmitir y recibir unidades de datos LLDP: 01-80-C2-00-00-0E. Al transmitir, el cortafuegos usa 01-80-C2-00-00-0E como la dirección MAC de destino. Al recibir, el cortafuegos procesa los datagramas con 01-80-C2-00-00-0E como dirección MAC de destino. Si el cortafuegos recibe cualquiera de las otras dos direcciones MAC para LLDPDU en sus interfaces, realiza la misma acción de reenvío que realizó antes de esta función, del siguiente modo:

- Si el tipo de interfaz es vwire, el cortafuegos reenvía el datagrama al otro puerto.
- Si el tipo de interfaz es L2, el cortafuegos proyecta el datagrama al resto de VLAN.
- Si el tipo de interfaz es L3, el cortafuegos descarta los datagramas.

No se admiten Panorama ni dispositivos de WildFire.

Los tipos de interfaz que admiten LLDP son TAP, alta disponibilidad (HA), reflejo de descifrado, subinterfaces virtuales wire/vlan/L3 e interfaces de tarjeta de procesamiento de logs (LPC) de PA-7000 Series.

Una trama Ethernet LLDP tiene el siguiente formato:

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Con la trama Ethernet LLDP, la estructura TLV tiene el siguiente formato:

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

TLV compatibles con LLDP

Las LLDPDU incluyen TLV obligatorios y opcionales. La siguiente tabla enumera los TLV obligatorios compatibles con el cortafuegos:

TLV obligatorios	Tipo de TLV	Description (Descripción)
TLV de ID de bastidor	1	Identifica el bastidor del cortafuegos. Cada cortafuegos debe tener exactamente un único ID de bastidor. El subtipo de ID del chasis es 4 (dirección MAC), y en los modelos de Palo Alto Networks® se utilizará la dirección MAC de Eth0 para garantizar la exclusividad.
TLV de ID de puerto	2	Identifica el puerto desde el que se envía la LLDPDU. Cada cortafuegos usa un ID de puerto para cada mensaje de LLDPDU transmitido. El subtipo de ID de puerto es 5 (nombre de interfaz) e identifica de manera exclusiva el puerto de transmisión. El cortafuegos usa ifname de la interfaz como el ID de puerto.
TLV de tiempo de vida (TTL)	3	Especifica cuánto tiempo (en segundos) se retiene la información de LLDPDU recibida del peer como válida en el cortafuegos local (el intervalo es 0-65.535). El valor es un múltiplo del multiplicador de tiempo de retención de LLDP. Cuando el valor de TTL es 0, la información asociada al dispositivo deja de ser válida y el cortafuegos elimina esa entrada de la MIB.
Fin de TLV de LLDPDU	0	Indica el fin de la TLV en la trama Ethernet de LLDP.

La siguiente tabla enumera los TLV opcionales compatibles con el cortafuegos de Palo Alto Networks:

TLV opcionales	Tipo de TLV	Finalidad y notas relacionadas con la implementación del cortafuegos
TLV de descripción del puerto	4	Describe el puerto del cortafuegos en formato alfanumérico. Se utiliza el objeto ifAlias.
TLV de nombre del sistema	5	Nombre configurado del cortafuegos en formato alfanumérico. Se utiliza el objeto sysName.
TLV de descripción del sistema	6	Describe el cortafuegos en formato alfanumérico. Se utiliza el objeto sysDescr.

TLV opcionales	Tipo de TLV	Finalidad y notas relacionadas con la implementación del cortafuegos
Capacidades del sistema	7	Describe el modo de implementación de la interfaz del siguiente modo: • Se anuncia una interfaz L3 con capacidad de enrutador (bit 6) y el “otro” bit (bit 1). • Se anuncia una interfaz L2 con capacidad de puente para MAC (bit 3) y el “otro” bit (bit 1). • Se anuncia una interfaz virtual wire con capacidad de repetidor (bit 2) y el “otro” bit (bit 1).
Dirección de gestión	8	Una o más direcciones IP usadas para la gestión del cortafuegos, del siguiente modo: • Dirección IP de la interfaz de gestión (MGT) • Dirección IPv4 o IPv6 de la interfaz • Dirección de bucle invertido • Dirección definida por el usuario en el campo de dirección de gestión Si no se indica una dirección IP de gestión, la predeterminada es la dirección MAC de la interfaz de transmisión. Se incluye el número de interfaz de la dirección de gestión especificada. También se incluye el OID de la interfaz de hardware con la dirección de gestión especificada (si se aplica). Si se ha especificado más de una dirección de gestión, se enviará en el orden especificado, empezando por el principio de la lista. Se admite un máximo de cuatro direcciones de gestión. Es un parámetro opcional que puede dejarse deshabilitado.

Mensajes de Syslog LLDP y capturas de SNMP

El cortafuegos almacena información de LLDP en las MIB, que puede supervisar un Gestor SNMP. Si desea que el cortafuegos envíe notificaciones de capturas de SNMP y mensajes de syslog acerca de eventos de LLDP, debe habilitar **SNMP Syslog Notification** en un perfil LLDP.

Conforme a RFC 5424, el protocolo de Syslog, y RFC 1157, Un protocolo simple de gestión de redes, LLDP envía mensajes de capturas de SNMP y syslog cuando hay un cambio en la MIB. Estos mensajes están limitados por frecuencia según el **Notification Interval**, un ajuste global de LLDP que se establece por defecto en 5 segundos y que se puede configurar.

Dado que los mensajes de captura de SNMP y syslog LLDP están limitados por frecuencia, es posible que parte de la información de LLDP proporcionada a esos procesos no coincida con las estadísticas de LLDP actuales cuando realice la Visualización de la información de estado del LLDP. Se trata del comportamiento normal y esperado.

Puede recibir un máximo de 5 MIB por interfaz (Ethernet o AE). Cada origen diferente tiene una MIB. Si se supera el límite, se lanza el mensaje de error `tooManyNeighbors`.

Configuración de LLDP

Para configurar el LLDP y crear un perfil de LLDP, debe ser superusuario o administrador del dispositivo (deviceadmin). Una interfaz de un cortafuegos admite un máximo de cinco peers LLDP.

STEP 1 | Habilite LLDP en el cortafuegos.

Seleccione **Network (Red)** > **LLDP** y edite la sección General de LLDP; seleccione **Enable (Habilitar)**.

STEP 2 | (Opcional) Cambie la configuración global de LLDP.

1. Para **Transmit Interval (sec) (Intervalo de transmisión [s])**, especifique el intervalo (en segundos) con el que se transmiten las LLDPDU. El intervalo es de 1 a 3600; el valor predeterminado es 30.
2. Para **Transmit Delay (sec) (Retardo de transmisión [s])**, especifique el tiempo de retraso (en segundos) entre las transmisiones de LLDP enviadas después de hacer un cambio en un elemento de TLV. Este intervalo impide la inundación del segmento con LLDPDU si muchos cambios de red aumentan el número de cambios LLDP o si la interfaz provoca flaps. El **Retraso de transmisión** debe ser inferior al **Intervalo de transmisión**. El intervalo es de 1 a 600; el valor predeterminado es 2.
3. Para **Hold Time Multiple (Múltiplo del tiempo de espera)**, especifique un valor que se multiplicará por el **Transmit Interval (Intervalo de transmisión)** para determinar el Tiempo de espera total de TTL. El rango es de 1 a 100; el valor predeterminado es 4. El tiempo de espera TTL máximo es 65 535 segundos, independientemente del valor de multiplicador.
4. En **Notification Interval (Intervalo de notificaciones)**, especifique el intervalo (en segundos) con el que se transmiten los Mensajes de Syslog LLDP y capturas de SNMP cuando se producen cambios en la MIB. El intervalo es de 1 a 3600; el valor predeterminado es 5.
5. Haga clic en **OK (Aceptar)**.

STEP 3 | Cree un perfil de LLDP.

Para obtener descripciones de los TLV opcionales, consulte TLV compatibles con LLDP.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **LLDP Profile (Perfil de LLDP)** y **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil de LLDP.
2. En **Mode**, seleccione **transmit-receive** (opción por defecto), **transmit-only** o **receive-only**.
3. Seleccione **SNMP Syslog Notification (Notificación Syslog SNMP)** para habilitar notificaciones de SNMP y mensajes de syslog. Si se habilita, se usa el **Notification Interval (Intervalo de notificación)**. El cortafuegos enviará ambos, una trampa SNMP y un evento de syslog, como está configurado en Device (Dispositivo) **Log Settings (Configuración**

de log) System (Sistema) SNMP Trap Profile (Perfil de trampa SNMP) y **Syslog Profile (Perfil de Syslog)**.

4. En Optional TLVs (TLV opcionales), seleccione los TLV que desea transmitir:
   - **Descripción de puerto**
   - **Nombre del sistema**
   - **Descripción del sistema**
   - **Capacidades del sistema**
5. (Opcional) Seleccione **Management Address** para añadir una o más direcciones de gestión y seleccione **Add** para añadir un nombre en **Name**.
6. Seleccione la **Interface** desde la cual obtener la dirección de gestión. Se requiere al menos una dirección de gestión si se ha activado el TLV **Management Address (Dirección de gestión)**. Si no se configura la dirección IP de gestión, el sistema usa la dirección MAC de la interfaz de transmisión como la dirección de gestión de TLV.
7. Seleccione **IPv4** o **IPv6** y, en el campo adyacente, seleccione una dirección IP en la lista de direcciones configuradas en la interfaz seleccionada o bien introduzca una.
8. Haga clic en **OK (Aceptar)**.
9. Se permiten hasta cuatro direcciones de gestión. Si ha especificado más de una **Management Address**, se enviarán en el orden especificado, empezando por la parte superior de la lista. Para cambiar el orden de las direcciones, seleccione una dirección y use los botones **Move Up** o **Move Down**.
10. Haga clic en **OK (Aceptar)**.

STEP 4 | Asigne un perfil de LLDP a una interfaz.

1. Seleccione **Network (Red)** > **Interfaces** y seleccione la interfaz a la que asignará un perfil de LLDP.
2. Seleccione **LLDP** > **Advanced (Avanzado)**.
3. Seleccione **Enable LLDP** para asignar un perfil de LLDP a la interfaz.
4. En **Profile (Perfil)**, seleccione el perfil que ha creado. Si selecciona **None (Ninguno)**, se habilita LLDP con funcionalidades básicas: envía los tres TLV obligatorios y habilita el modo **transmit-receive (transmisión-recepción)**.

   Si desea crear un nuevo perfil, haga clic en **LLDP Profile (Perfil de LLDP)** y siga las instrucciones de los pasos a continuación.
5. Haga clic en **OK (Aceptar)**.

STEP 5 | **Commit (Confirmar)** los cambios.

Visualización de estados y configuración de LLDP

Realice el siguiente procedimiento para ver los estados y la configuración de LLDP.

STEP 1 | Vea la configuración global de LLDP.

Seleccione **Network (Red)** > **LLDP**.

En la pantalla General de LLDP, la casilla de verificación **Enable (Habilitar)** indica si LLDP está o no habilitado.

- Si LLDP está habilitado, se muestran los ajustes globales configurados (Intervalo de transmisión, Retraso de transmisión, Múltiple tiempo de espera e Intervalo de notificaciones).
- Si LLDP no está habilitado, se muestran los valores predeterminados de los ajustes globales.

Para acceder a las descripciones de estos valores, consulte el segundo paso de la Configuración de LLDP.

STEP 2 | Vea la información de estado de LLDP.

1. Seleccione la pestaña **State (Estado)**.
2. (Opcional) Introduzca un filtro para restringir la información que se muestra.

Información de la interfaz:

- **Interface (Interfaz)**: nombre de las interfaces que tienen asignados perfiles LLDP.
- **LLDP**: estado de LLDP (habilitado o deshabilitado).
- **Mode (Modo)**: modo LLDP de la interfaz: Tx/Rx, Tx solo o Rx solo.
- **Profile (Perfil)**: nombre del perfil asignado a la interfaz.

Información de transmisión:

- **Total Transmitted (Total transmitido)**: recuento de las LLDPDU transmitidas fuera de la interfaz.
- **Dropped Transmit (Transmisión descartada)**: número de LLDPDU que no se han transmitido fuera de la interfaz por un error. Por ejemplo, un error de longitud cuando el sistema construye un LLDPDU para la transmisión.

Información recibida:

- **Total Received (Total recibido)**: número de tramas LLDP recibidas en la interfaz.
- **Dropped TLV (TLV descartada)**: número de las tramas LLDP descartadas en la recepción.
- **Errors (Errores)**: número de TLV que se recibieron en la interfaz y contenían errores. Entre los tipos de errores de TLV se incluyen: falta de uno o más TLV obligatorios, mal funcionamiento, información fuera de alcance o error de longitud.
- **Unrecognized (No reconocido)**: número de TLV recibidos en la interfaz que no reconoce el agente local de LLDP. Por ejemplo, el tipo TLV está en el intervalo de TLV reservado.
- **Aged Out (Caducado)**: número de elementos eliminados desde Receive MIB por una caducidad TTL adecuada.

STEP 3 | Ver resumen de información de LLDP para cada vecino visto en una interfaz.

1. Seleccione la pestaña **Peers**.
2. (Opcional) Si lo desea, puede incluir un filtro para restringir la información que se muestra.

   Local Interface: interfaz en el cortafuegos que detectó el dispositivo vecino.

   Remote Chassis ID: ID de bastidor del peer. Se usará la dirección MAC.

   Port ID: ID del puerto del peer.

   Name: nombre del peer.

   More info: ofrece la siguiente información del peer remoto, que se basa en TLV obligatorios y opcionales.

   - Tipo de bastidor: Dirección MAC.
   - Dirección MAC: La dirección MAC del peer.
   - Nombre del sistema: Nombre del peer.
   - Descripción del sistema: Descripción del peer.
   - Descripción de puerto: Descripción del puerto del peer.
   - Tipo de puerto: Nombre de interfaz.
   - ID de puerto: El cortafuegos usa el ifname de la interfaz.
   - Capacidades del sistema: Funcionalidades del sistema. O=Otro, P=Repetidor, B=Puente, W=LAN-Inalámbrico, R=Enrutador, T=Teléfono
   - Capacidades habilitadas: Funcionalidades habilitadas en el peer.
   - Dirección de gestión: Dirección de gestión del peer.

Borrado de estadísticas de LLDP

Puede borrar las estadísticas de LLDP para interfaces específicas.

Borre las estadísticas de LLDP para interfaces específicas.

1. Seleccione **Network (Red)** > **LLDP** > **Status (Estado)** y en la columna izquierda, seleccione una o más interfaces en las que desea borrar las estadísticas de LLDP.
2. Haga clic en **Clear LLDP Statistics (Borrar estadísticas de LLDP)** en la parte inferior de la pantalla.

BFD

El cortafuegos admite la detección de reenvío bidireccional (Bidirectional Forwarding Detection, BFD) (RFC 5880), un protocolo que reconoce un fallo en la ruta bidireccional entre dos peers de enrutamiento. La detección del fallo de BFD es extremadamente rápida, lo que brinda una conmutación por error más rápida que la alcanzada por la supervisión de enlaces o las comprobaciones de enrutamiento dinámico frecuentes, como los paquetes de bienvenida o heartbeats. Los centro de datos y redes de misión crítica que requieren alta disponibilidad y una conmutación por error sumamente rápida necesitan la detección de conmutación por error sumamente rápida que ofrece BFD.

> Descripción general de BFD
> Configuración de BFD
> Referencia: detalles de BFD

Descripción general de BFD

Al habilitar BFD, se establece una sesión desde un extremo (el cortafuegos) hacia su peer BFD en el extremo de un enlace que utiliza un protocolo de enlace de tres pasos. Los paquetes de control realizan el protocolo de enlace y negocian los parámetros configurados en el perfil BFD, incluidos los intervalos mínimos en los que los peers pueden enviar y recibir paquetes de control. Los paquetes de control BFD para IPv4 e IPv6 se transmiten por el puerto UDP 3784. Los paquetes de control BFD para compatibilidad con salto entre redes se transmiten por el puerto UDP 4784. Los paquetes de control BFD transmitidos por cualquiera de los puertos se encapsulan en los paquetes UDP.

Una vez que se establece la sesión BFD, la implementación de Palo Alto Networks® de BFD opera en modo asíncrono, lo que significa que ambos extremos se envían paquetes de control (que funcionan como paquetes de saludo) en el intervalo negociado. Si un peer no recibe un paquete de control dentro del período de detección (calculado como el intervalo de transmisión negociado multiplicado por un multiplicador de tiempo de detección), el peer considera la sesión como inactiva. (El cortafuegos no admite el modo de demanda, en el que los paquetes de control se envían únicamente si es necesario en lugar de periódicamente).

Cuando usted habilita BFD para una ruta estática y una sesión BFD entre el cortafuegos y el peer BFD falla, el cortafuegos elimina de las tablas RIB y FIB la ruta que falló, y permite que una ruta alternativa con una prioridad menor tome el control. Cuando usted habilita BFD para un protocolo de enrutamiento, BFD notifica al protocolo de enrutamiento que debe cambiar a una ruta alternativa al peer. Por lo tanto, el cortafuegos y peer BFD vuelven a converger en una nueva ruta.

Un perfil BFD le permite realizar la Configuración de BFD y aplicar estos ajustes a uno o más protocolos de enrutamiento o rutas estáticas en el cortafuegos. Si habilita BFD sin configurar un perfil, el cortafuegos usa su perfil BFD por defecto (con todos los ajustes por defecto). No puede cambiar el perfil BFD por defecto.

Cuando una interfaz ejecuta varios protocolos que usan diferentes perfiles BFD, BFD usa el perfil que tiene el **Desired Minimum Tx Interval** más bajo. Consulte BFD para protocolos de enrutamiento dinámico.

Los peers HA activos/pasivos sincronizan configuraciones y sesiones BFD; los peers HA activos/activos no.

BFD está estandarizado en RFC 5880. PAN-OS no admite todos los componentes de RFC 5880; consulte Componentes RFC no compatibles de BFD.

PAN-OS también es compatible con RFC 5881, www.rfc-editor.org/rfc/rfc5881.txt. En este caso, BFD realiza un seguimiento de un solo salto entre dos sistemas que usan IPv4 o IPv6, de manera que los dos sistemas se conectan directamente entre sí. BFD también realiza el seguimiento de varios saltos de peers conectados por BGP. PAN-OS sigue la encapsulación BFD como se describe en RFC 5883, www.rfc-editor.org/rfc/rfc5883.txt. Sin embargo, PAN-OS no admite la autenticación.

- Modelo, interfaz y soporte al cliente de BFD
- Componentes RFC no compatibles de BFD
- BFD para rutas estáticas
- BFD para protocolos de enrutamiento dinámico

Modelo, interfaz y soporte al cliente de BFD

Los siguientes modelos de cortafuegos no admiten BFD: cortafuegos PA-800 Series, PA-220 y VM-50. Los modelos que admiten una cantidad máxima de sesiones de BFD, como se enumera en la herramienta Selección de producto.

BFD se ejecuta en Ethernet física, Ethernet de agregación (Aggregated Ethernet, AE), VLAN e interfaces de túnel (VPN de sitio a sitio y LSVPN) y en subinterfaces de capa 3.

Los clientes BFD compatibles son los siguientes:

- Rutas estáticas (IPv4 e IPv6), que constan de un solo salto.
- OSPFv2 y OSPFv3 (los tipos de interfaz incluyen difusión, punto a punto y punto a multipunto).
- BGP IPv4 e IPv6 (IBGP, EBGP) consta de un solo salto o varios saltos.
- RIP (único salto).

Componentes RFC no compatibles de BFD

- Modo de demanda
- Autenticación
- El envío o la recepción de paquetes Echo; sin embargo, el cortafuegos pasará los paquetes Echo que lleguen en una interfaz de modo tap o por Virtual Wire. (Los paquetes Echo de BFD tienen la misma dirección IP para el origen y el destino).
- Secuencias de sondeo
- Control de congestión

BFD para rutas estáticas

Para usar BFD en una ruta estática, tanto el cortafuegos como el peer en el otro extremo de la ruta estática deben admitir las sesiones BFD. Una ruta estática puede tener un perfil BFD únicamente si el tipo **Next Hop (Próximo salto)** es **IP Address (Dirección IP)**.

Si una interfaz está configurada con más de una ruta estática a un peer (la sesión BFS tiene la misma dirección IP de origen y la misma dirección IP de destino), una sola sesión BFD maneja automáticamente las múltiples rutas estáticas. Este comportamiento reduce las sesiones BFD. Si las rutas estáticas tienen diferentes perfiles BDF, el perfil con el **Desired Minimum Tx Interval (Intervalo Tx mínimo deseado)** se activa.

En una implementación en la que desea configurar BFD para una ruta estática en una interfaz cliente DHCP o PPPE, debe realizar dos confirmaciones. La habilitación de BFD para una ruta estática requiere que el tipo **Next Hop (Próximo salto)** sea **IP Address (Dirección IP)**. Pero al momento de una confirmación de interfaz DHCP o PPPoE, la dirección IP de la interfaz y la dirección IP de siguiente salto (puerta de enlace por defecto) son desconocidas.

Primero debe habilitar un cliente DHCP o PPPoE para la interfaz, realizar una confirmación y esperar que el servidor DHCP o PPPoE envíen al cortafuegos la dirección IP del cliente y la dirección IP de la puerta de enlace por defecto. Luego puede configurar la ruta estática (usando la dirección de la puerta de enlace por defecto del cliente DHCP o PPPE como el siguiente salto), habilitar BFD y realizar una segunda confirmación.

BFD para protocolos de enrutamiento dinámico

Además de BFD para rutas estáticas, el cortafuegos admite BFD para los protocolos de enrutamiento BGP, OSPF y RIP.

La implementación de Palo Alto Networks® de BFD de varios saltos sigue la parte de encapsulación de RFC 5883, Detección de reenvío bidireccional (BFD) para rutas de varios saltos, pero no admite la autenticación. Una solución alternativa es configurar BFD en un túnel VPN para BGP. El túnel VPN puede brindar autenticación sin la duplicación de la autenticación de BFD.

Cuando habilita BFD para las interfaces de difusión OSPFv2 o OSPFv3, OSPF establece una sesión BFD únicamente con su enrutador designado (Designated Router, DR) y el enrutador designado de respaldo (Backup Designated Router, BDR). En las interfaces de punto a punto, OSPF establece una sesión BFD con el vecino directo. En las interfaces de punto a punto, OSPF establece una sesión BFD con cada peer.

El cortafuegos no admite BFD en un OSPF o enlace virtual OSPFv3.

Cada protocolo de enrutamiento puede tener sesiones BFD independientes en una interfaz. O bien, dos o más protocolos de enrutamiento (BGP, OSPf y RIP) pueden compartir una sesión de BFD común para una interfaz.

Cuando habilita BFD para múltiples protocolos en la misma interfaz, y la dirección IP de origen y la dirección IP de destino para los protocolos también son las mismas, los protocolos comparten una sola sesión BFD, con lo cual se reducen ambas cargas de trabajo del plano de datos (CPU) y carga de trabajo en la interfaz. Si configura diferentes perfiles BFD para estos protocolos, solo se usa un perfil BFD: el que tiene el **Desired Minimum Tx Interval** más bajo. Si los perfiles tienen el mismo **Desired Minimum Tx Interval (Intervalo Tx mínimo deseado)**, se activa el perfil utilizado por la primera sesión creada. En el caso de que una ruta estática y OSPF compartan la misma sesión, debido a que una sesión estática se crea inmediatamente después de una confirmación, si bien el OSPF espera hasta que haya una adyacencia activa, el perfil de la ruta estática tiene prevalencia.

El beneficio de usar una sola sesión de BFD en estos casos es que este comportamiento utiliza recursos de manera más eficiente. El cortafuegos puede utilizar los recursos guardados para admitir más sesiones de BFD en diferentes interfaces o admitir BFD para diferentes ares de dirección IP de origen y de destino.

IPv4 e IPv6 en la misma interfaz siempre crea diferentes sesiones BFD, incluso aunque usen el mismo perfil BFD.

Si implementa ambos BFD para el control de ruta HA y BGP, Palo Alto Networks le recomienda no implementar el BGP Graceful Restart (Reinicio correcto BGP). Cuando fallan la interfaz del peer de BFD y la supervisión de rutas, BFD puede eliminar las rutas afectadas de la tabla de enrutamiento y sincronizar este cambio en el cortafuegos de HA pasivo antes de que se produzca el reinicio correcto. Si decide implementar BFD para BGP, el reinicio correcto para BGP y el control de ruta HA, debe configurar BFD con un intervalo Tx mínimo deseado superior y un multiplicador de tiempo de detección superior a los valores predeterminados.

Configuración de BFD

Tras leer la Descripción general de BFD, que incluye información sobre los modelos de cortafuegos y las interfaces compatibles, realice los siguientes pasos antes de configurar BFD:

- Configure uno o más enrutadores virtuales.
- Configure una o más rutas estáticas si está aplicando BFD a rutas estáticas.
- Configure un protocolo de enrutamiento (BGP, OSPF, OSPFv3 o RIP) si está aplicando BFD a un protocolo de enrutamiento.

La eficacia de su implementación de BFD depende de diversos factores, tales como las cargas de tráfico, las condiciones de la red, qué tan agresiva es su configuración de BFD y qué tan ocupado está el plano de datos.

STEP 1 | Cree un perfil de BFD.

Si cambia un ajuste en un perfil de BFD que una sesión de BFD existente está utilizando y confirma el cambio, antes de que el cortafuegos elimine esa sesión BFD y vuelva a crearla con el nuevo ajuste, el cortafuegos envía un paquete BFD con el estado local configurado con el administrador inactivo. El dispositivo del peer puede o no alternar el protocolo de enrutamiento o ruta estática, según la implementación del peer de RFC 5882, Sección 3.2.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **BFD Profile (Perfil BFD)** y luego **Add (Añadir)** para añadir un **Name (Nombre)** para el perfil BFD. El nombre distingue entre mayúsculas y minúsculas y debe ser único en el cortafuegos. Utilice solamente letras, números, espacios, guiones y guiones bajos.
2. Seleccione el **Mode (Modo)** en el que BFD operará:
   - **Active**: BFD inicia el envío de los paquetes de control (por defecto). Al menos uno de los peers de BFD debe estar activo; ambos pueden estar activos.
   - **Passive**: BFD espera que el peer envíe los paquetes de control y responde según corresponda.

STEP 2 | Configure los intervalos de BFD.

1. Introduzca el **Desired Minimum Tx Interval (ms)**. Este es el intervalo mínimo, en milisegundos, con el cual usted desea que el protocolo BFD (denominad BFD) envíe paquetes de control BFD; con lo cual usted está negociando el intervalo de transmisión

con el peer. El mínimo en cortafuegos PA-7000 y PA-5200 Series es 50; el mínimo en cortafuegos VM-Series es 200. El máximo es 2.000; el valor por defecto es 1.000.

*Se recomienda configurar **Desired Minimum Tx Interval (Intervalo Tx mínimo deseado)** en 100 o más en los cortafuegos PA-7000 Series; un valor inferior a 100 puede causar fluctuaciones en la BFD.*

*Si tiene múltiples protocolos de enrutamiento que usan diferentes perfiles BFD en la misma interfaz, configure los perfiles BFD con el mismo valor de **Desired Minimum Tx Interval**.*

2. Introduzca el **Required Minimum Rx Interval (ms)**. Este es el intervalo mínimo, en milisegundos, en el cual BFD puede recibir paquetes de control BFD. El mínimo en cortafuegos PA-7000 y PA-5200 Series es 50; el mínimo en cortafuegos VM-Series es 200. El máximo es 2.000; el valor por defecto es 1.000.

   *Se recomienda configurar **Required Minimum Rx Interval (Intervalo Rx mínimo necesario)** en 100 o más en los cortafuegos PA-7000 Series; un valor inferior a 100 puede causar fluctuaciones en la BFD.*

STEP 3 | Configure el multiplicador de tiempo de detección BFD.

Introduzca el **Detection Time Multiplier**. El sistema local calcula el tiempo de detección como el **Detection Time Multiplier (Multiplicador de tiempo de detección)** recibido del sistema remoto, multiplicado por el intervalo de transmisión acordado del sistema remoto (el valor más alto de **Required Minimum Rx Interval [Intervalo Rx mínimo necesario]** y el último **Desired Minimum Tx Interval [Intervalo Tx mínimo deseado]** recibido). Si BFD no recibe un paquete de control BFD desde su peer antes de que se agote el tiempo de detección, se produjo un fallo. El intervalo va de 2 a 50 y el valor predeterminado es 3.

Por ejemplo, un intervalo de transmisión de 300 ms x 3 (multiplicador del tiempo de detección) = 900 ms de tiempo de detección.

Al configurar un perfil BFD, tenga en cuenta que el cortafuegos es un dispositivo basado en la sesión generalmente en el extremo de una red o centro de datos, y puede tener enlaces más lentos que un enrutador dedicado. Por lo tanto, el cortafuegos probablemente necesita un intervalo más prolongado y un multiplicador más alto de lo que permiten los ajustes más rápidos. Un tiempo de detección demasiado breve puede causar falsas detecciones de fallos cuando el problema es en realidad la congestión del tráfico.

STEP 4 | Configure el tiempo de retención de BFD.

Introduzca el **Hold Time (ms)**. Esta es la demora, en milisegundos, una vez que un enlace se activa antes de que BFD transmita los paquetes de control de BFD. **Hold Time (Tiempo de espera)** se aplica al modo activo de BFD únicamente. Si el BFD recibe paquetes de control BFD durante el **tiempo de espera**, los ignora. El intervalo es de 0-120000. El valor por defecto de 0, que significa que no se utiliza el **tiempo de espera** de transmisión; el BFD envía y recibe paquetes de control BFD de inmediato después de que establece el enlace.

STEP 5 | (Opcional: para una implementación de IPv4 de BGP únicamente) configure ajustes relacionados con el salto para el perfil BFD.

1. Seleccione **Multihop (Múltiples pasos)** para habilitar BFD en varios saltos de BGP.
2. Introduzca el **Minimum Rx TTL**. Este es el valor mínimo de período de vida (cantidad de saltos) que BFD aceptará (recibirá) en un paquete de control de BFD cuando BGP admite varios saltos de BFD. (El intervalo es 1-254; no hay valor por defecto).

   El cortafuegos descarta el paquete si recibe un TTL menor que el **Minimum Rx TTL (TTL Rx mínimo)** configurado. Por ejemplo, si el peer está a 5 saltos de distancia y el peer transmite un paquete BFD con un TTL de 100 al cortafuegos, y si el valor **Minimum Rx TTL (TTL Rx mínimo)** para el cortafuegos está configurado en 96 o más, el cortafuegos descarta el paquete.

STEP 6 | Guarde el perfil BFD.

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

STEP 7 | (Opcional) Habilite BFD para una ruta estática.

el cortafuegos y el peer en el otro extremo de la ruta estática deben admitir las sesiones BFD.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual donde esté configurada la ruta estática.
2. Seleccione la pestaña **Static Routes**.
3. Seleccione la pestaña **IPv4** o **IPv6**.
4. Seleccione la ruta estática donde desea aplicar el BFD.
5. Seleccione una **Interface** (incluso aunque esté usando una dirección DHCP). El ajuste de **Interface** no puede ser **None**.
6. Para **Next Hop**, seleccione **IP Address** e introduzca la dirección IP si aún no la especificó.
7. En **BFD Profile**, seleccione una de las opciones siguientes:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   *La selección de **None (Disable BFD) (Ninguno [deshabilitar BFD])** deshabilita BFD para la ruta estática.*
8. Haga clic en **OK (Aceptar)**.

Una columna BFD en la pestaña **IPv4** o **IPv6** indica el perfil BFD configurado para la ruta estática.

STEP 8 | (Opcional) Habilite BFD para todas las interfaces BGP o para un solo peer BGP.

Si habilita o deshabilita BFD de forma global, todas las interfaces que ejecutan BGP se desactivan y se vuelven a activar con la función BFD. Esto puede interrumpir todo el tráfico BGP. Cuando habilita BFD en la interfaz, el cortafuegos detendrá la conexión BGP al peer para programar BFD en la interfaz. El dispositivo del peer notará la caída de la conexión de BGP, lo cual podrá resultar en una nueva convergencia. Habilite BFD en las interfaces BGP durante un horario de menor demanda, cuando la nueva convergencia no afecte el tráfico de producción.

Si implementa ambos BFD para el control de ruta HA y BGP, Palo Alto Networks le recomienda no implementar el BGP Graceful Restart (Reinicio correcto BGP). Cuando la interfaz del peer de BFD falla y el control de ruta falla, BFD puede eliminar las rutas afectadas de la tabla de rutas y sincronizar este cambio con el cortafuegos HA pasivo antes de que el reinicio correcto surta efecto. Si decide implementar BFD para BGP, el reinicio correcto para BGP y el control de ruta HA, debe configurar BFD con un intervalo Tx mínimo deseado superior y un multiplicador de tiempo de detección superior a los valores predeterminados.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, y seleccione el enrutador virtual donde está configurado BGP.
2. Seleccione la pestaña **BGP**.
3. (Opcional) Para aplicar la BFD a todas las interfaces de BGP del enrutador virtual, seleccione una de las siguientes opciones en la lista **BFD** y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   *La selección de **None (Disable BFD) (Ninguno [Deshabilitar BFD])** deshabilita BFD para todas las interfaces BGP en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz BGP.*
4. (Opcional) Para habilitar BFD para una sola interfaz de peer BGP (con lo cual se cancela el ajuste de **BFD** para BGP, siempre y cuando no esté deshabilitado), realice las siguientes tareas:
   1. Seleccione la pestaña **Peer Group (Grupo de peers)**.
   2. Seleccione un grupo de peers.
   3. Seleccione un peer.
   4. En la lista **BFD**, seleccione una de las siguientes opciones:

      default (predeterminado): usa únicamente los ajustes por defecto.

      Inherit-vr-global-setting (valor por defecto): el peer BGP hereda el perfil BFD que usted seleccionó globalmente para BGP para el enrutador virtual.

      Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

      *La selección de **Disable BFD (Deshabilitar BFD)** deshabilita BFD para el peer BGP.*

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

Una columna BFD en BGP - Grupo de peers/Lista de peers indica el perfil BFD configurado para la interfaz.

STEP 9 | (Opcional) Habilite BFD para OSPF u OSPFv3 globalmente para una interfaz OSPF.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)** y seleccione el enrutador virtual donde OSPF u OSPFv3 están configurados.
2. Seleccione la pestaña **OSPF** u **OSPFv3**.
3. (Opcional) En la lista **BFD**, seleccione una de las siguientes opciones para habilitar la BFD en todas las interfaces de OSPF o de OSPF v. 3 y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   *La selección de **None (Disable BFD) (Ninguno [Deshabilitar BFD])** deshabilita BFD para todas las interfaces OSPF en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz OSPF.*
4. (Opcional) Para habilitar BFD para una sola interfaz de peer OSPF (con lo cual se cancela el ajuste de **BFD** para OSPF, siempre y cuando no esté deshabilitado), realice las siguientes tareas:
   1. Seleccione la pestaña **Areas** y seleccione un área.
   2. En la pestaña **Interface (Interfaz)**, seleccione una interfaz.
   3. En la lista **BFD**, seleccione una de las siguientes opciones para configurar la BFD en el peer de OSPF especificado:

      default (predeterminado): usa únicamente los ajustes por defecto.

      Inherit-vr-global-setting (valor por defecto): el peer OSPF hereda el ajuste de **BFD** para OSPF u OSPFv3 para el enrutador virtual.

      Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

      *La selección de **Disable BFD** deshabilita BFD para la interfaz OSPF u OSPFv3.*
   4. Haga clic en **OK (Aceptar)**.
5. Haga clic en **OK (Aceptar)**.

Una columna BFD en la pestaña de OSPF **Interface** indica el perfil BFD configurado para la interfaz.

STEP 10 | (Opcional) Habilite BFD para RIP globalmente o para una sola interfaz RIP.

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, y seleccione el enrutador virtual donde está configurado RIP.
2. Seleccione la pestaña RIP.
3. (Opcional) En la lista **BFD**, seleccione una de las siguientes opciones para habilitar la BFD en todas las interfaces de RIP del enrutador virtual y haga clic en **OK (Aceptar)**:
   - **default (predeterminado)**: usa únicamente los ajustes por defecto.
   - Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.
   - **New BFD Profile (Nuevo perfil BFD)**: le permite crear un perfil BFD.

   *La selección de **None (Disable BFD) (Ninguno [Deshabilitar BFD])** deshabilita BFD para todas las interfaces RIP en el enrutador virtual; usted no puede habilitar BFD para una sola interfaz RIP.*
4. (Opcional) Para habilitar BFD para una sola interfaz RIP (con lo cual se cancela el ajuste de **BFD** para RIP, siempre y cuando no esté deshabilitado), realice las siguientes tareas:
   1. Seleccione la pestaña **Interfaces** y seleccione una interfaz.
   2. En la lista **BFD**, seleccione una de las siguientes opciones:

      default: usa únicamente los ajustes por defecto.

      Inherit-vr-global-setting (heredar ajuste global para el enrutador virtual) (valor por defecto): la interfaz RIP hereda el perfil BFD que usted seleccionó globalmente para RIP para el enrutador virtual.

      Un perfil BFD que haya configurado. Consulte Creación de un perfil BFD.

      *La selección de **None (Disable BFD)** deshabilita BFD para la interfaz RIP.*
   3. Haga clic en **OK (Aceptar)**.
5. Haga clic en **OK (Aceptar)**.

La columna BFD en la pestaña **Interface** indica el perfil BFD configurado para la interfaz.

STEP 11 | Confirme la configuración.

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

STEP 12 | Visualización de resumen y detalles de BFD

1. Seleccione **Network (Red)** > **Virtual Routers (Enrutadores virtuales)**, busque el enrutador virtual de su interés y haga clic en **More Runtime Stats (Más estadísticas de tiempo de ejecución)**.
2. Seleccione la pestaña **BFD Summary Information (Información de resumen BFD)** para ver la información resumida, tal como el estado de BFD y las estadísticas del tiempo de ejecución.
3. (Opcional) Seleccione **details (detalles)** en la fila de la interfaz en la que está interesado para ver Referencia: detalles de BFD.

STEP 13 | Supervise los perfiles de BFD a los que hace referencia una configuración de enrutamiento; supervise las estadísticas de BFD, el estado y la condición.

Use los siguientes comandos operativos de CLI:

- show routing bfd active-profile [<name>]
- **show routing bfd details [interface**<*name*>**][local-ip**<*ip*>**][multihop] [peer-ip** <*ip*>**][session-id][virtual-router**<*name*>**]**
- show routing bfd drop-counters session-id <session-id>
- **show counter global | match bfd**

STEP 14 | (Opcional) Borre los contadores de transmisión, recepción y descarte de BFD.

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | (Opcional) Borre las sesiones de BFD para la depuración.

```
clear routing bfd session-state session-id all | <1-1024>
```


Referencia: Detalles de BFD

Para ver la siguiente información BFD de un enrutador virtual, puede consultar el paso Visualización de resumen y detalles de BFD.

Nombre	Valor (ejemplo)	Description (Descripción)
Session ID (ID de sesión)	1	Número de ID de la sesión BFD.
Interface (Interfaz)	ethernet1/12	Interfaz que seleccionó donde BFD se está ejecutando.
Protocolo	STATIC(IPV4) OSPF	Ruta estática (familia de dirección IP de ruta estática) y/o protocolo de enrutamiento dinámico que está ejecutando BFD en la interfaz.
Dirección IP local	10.55.55.2	Dirección IP de la interfaz.
Dirección IP vecina	10.55.55.1	Dirección IP del vecino de BFD.
Perfil BFD	valor por defecto *(Esta sesión BFD tiene varios perfiles BFD. El "intervalo de Tx deseado mínimo [ms]" más bajo se utiliza para seleccionar el perfil efectivo).	Nombre del perfil BFD aplicado a la interfaz. Debido a que la interfaz de muestra tiene una ruta estática y OSPF que ejecuta BFD con diferentes perfiles, el cortafuegos utiliza el perfil con el **intervalo de Tx deseado mínimo** más bajo. En este ejemplo, el perfil utilizado es el perfil por defecto.
Estado (local/remoto)	activo/activo	Estados de BFD de los peers de BFD locales y remotos. Los estados posibles son administrador inactivo, inactivo, inicializado y activo.
Tiempo de activación	2 h 36 m 21 s 419 ms	Período de tiempo que BFD estuvo activo (horas, minutos, segundos y milisegundos).
Discriminador (local/remoto)	1391591427/1	Discriminadores para peers BFD locales y remotos.
Modo	Activo	Modo en el que BFD está configurado en la interfaz: Activo o pasivo.
Modo de demanda	Disabled (Deshabilitado)	PAN-OS no admite el modo de demanda BFD, por lo cual siempre está en estado deshabilitado.

Nombre	Valor (ejemplo)	Description (Descripción)
Multihop	Disabled (Deshabilitado)	Pasos múltiples de BFD: Habilitado o deshabilitado.
Multihop TTL		TTL de múltiples pasos; el intervalo es 1-254. El campo está vacío si Multihop está deshabilitado.
Local Diag Code	0 (sin diagnóstico)	Los códigos de diagnóstico indican el motivo del último cambio de estado del sistema local: 0: sin diagnóstico 1: vencimiento del tiempo de detección de control 2: error de la función Echo 3: sesión de señalización de vecino inactiva 4: restablecimiento del plano de reenvío 5: ruta inactiva 6: ruta concatenada inactiva 7: función administrativa inactiva 8: ruta concatenada inversa inactiva
Last Received Remote Diag Code	0 (sin diagnóstico)	Último código de diagnóstico recibido del peer BFD.
Tiempo de espera de transmisión	0 ms	Tiempo de espera (en milisegundos) luego de que un enlace se activa antes de que BFD transmita los paquetes de control de BFD. Un tiempo de espera de 0 ms significa que se transmitirá inmediatamente. El intervalo es de 0-120.000 ms.
Received Min Rx Interval	1000 ms	Intervalo de Rx mínimo recibido del peer; el intervalo en el cual el peer BFD puede recibir paquetes de control. El valor máximo es de 2000 ms.
Negotiated Transmit Interval	1000 ms	El intervalo de transmisión (en milisegundos) que los peers de BFD han acordado para enviarse paquetes de control BFD mutuamente. El valor máximo es de 2000 ms.
Received Multiplier	3	Valor de multiplicador de tiempo de detección recibido del peer BFD. El tiempo de transmisión multiplicado por el multiplicador es igual al tiempo de detección. Si BFD no recibe un paquete de control BFD desde su peer antes de que se agote el tiempo

Nombre	Valor (ejemplo)	Description (Descripción)
		de detección, se produjo un fallo. El intervalo es de 2-50.
Detect Time (exceeded)	3000ms (0)	Tiempo de detección calculado (intervalo de transmisión negociado multiplicado por el multiplicador) y la cantidad de milisegundos que se excedió el tiempo de detección.
Tx Control Packets (last)	9383 (420 ms atrás)	Cantidad de paquetes de control BFD transmitidos (y tiempo desde que BFD transmitió el paquete de control más reciente).
Rx Control Packets (last)	9384 (407 ms atrás)	Cantidad de paquetes de control BFD recibidos (y tiempo desde que BFD recibió el paquete de control más reciente).
Agent Data Plane	Ranura 1 - DP 0	En los cortafuegos de la serie PA-7000, el CPU del plano de datos que se asignó para manejar los paquetes para esta sesión BFD.
Errores	0	Cantidad de errores de BFD.
Último paquete que causó el cambio de estado		
versión	1	Versión de BFD.
Poll Bit	0	Bit de sondeo de BFD; 0 indica que no está configurado.
Desired Min Tx Interval	1000 ms	Intervalo de transmisión mínimo deseado del último paquete que causó un cambio de estado.
Required Min Rx Interval	1000 ms	Intervalo de recepción mínimo necesario del último paquete que causó un cambio de estado.
Detect Multiplier	3	Multiplicador de detección del último paquete que causó un cambio de estado.
My Discriminator	1	Discriminador remoto. Un discriminador es un valor único distinto de cero que los peers utilizan para distinguir varias sesiones BFD entre sí.
Your Discriminator	1391591427	Discriminador local. Un discriminador es un valor único distinto de cero que los peers utilizan para distinguir varias sesiones BFD entre sí.

Nombre	Valor (ejemplo)	Description (Descripción)
Diagnostic Code	0 (sin diagnóstico)	Código de diagnóstico del último paquete que causó un cambio de estado.
Length	24	Extensión del paquete de control de BFD en bytes.
Demand Bit	0	PAN-OS no admite el modo de demanda BFD, por lo cual el bit de demanda siempre está configurado en 0 (deshabilitado).
Final Bit	0	PAN-OS no admite la secuencia de sondeo, por lo cual el bit final siempre está configurado en 0 (deshabilitado).
Multipoint Bit	0	Este bit está reservado para futuras extensiones de punto a multipunto para BFD. Debe ser cero en la transmisión y la recepción.
Control Plane Independent Bit	1	• Si está configurado en 1, la implementación BFD del sistema de transmisión no comparte el destino con su plano de control (es decir, BFD se implementa en el plano de reenvío y puede continuar funcionando a pesar de las alteraciones del plano de control). En PAN-OS, este bit siempre está configurado en 1. • Si está configurado en 0, la implementación de BFD del sistema de transmisión comparte el destino con su plano de control.
Authentication Present Bit	0	PAN-OS no admite la autenticación BFD, por lo cual el bit de presencia de autenticación siempre está configurado en 0.
Required Min Echo Rx Interval	0 ms	PAN-OS no admite la función Echo de BFD, por lo cual este valor siempre será 0 ms.

Configuración de sesión y tiempos de espera de sesión

Esta sección describe la configuración global que afecta a las sesiones TCP, UDP e ICMPv6, además de IPv6, NAT64, sobresuscripción NAT, tamaño de trama gigante, MTU, vencimiento acelerado y autenticación del portal cautivo. También hay un ajuste (Rematch Sessions [Reanalizar sesiones establecidas]) que le permite aplicar las políticas de seguridad recién configuradas a las sesiones que ya están en curso.

El primero de los siguientes temas ofrece breves resúmenes de la capa de transporte del modelo OSI, TCP, UDP e ICMP. Para obtener más información acerca de los protocolos, consulte sus RFC respectivos. El resto de temas describen la configuración y los tiempos de espera de sesión.

> Sesiones de capa de transporte
> TCP
> UDP
> ICMP
> Control de tipos y códigos específicos de ICMP o ICMPv6
> Configuración de los tiempos de espera de sesión
> Política de distribución de sesiones
> Configuración de los ajustes de sesión
> Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP

Sesiones de capa de transporte

Una sesión de red es un intercambio de mensajes que se produce entre dos o más dispositivos de comunicación, durante cierto periodo de tiempo. Cada sesión se establece, y luego se anula cuando termina. En las tres capas del modelo OSI tienen lugar distintos tipos de sesiones: la capa de transporte, la capa de sesión y la capa de aplicación.

La capa de transporte funciona en la capa 4 del modelo OSI y proporciona una entrega punto a punto, fiable o no fiable, y un control del flujo de los datos. Los protocolos de Internet que implementan sesiones en la capa de transporte incluyen el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP).

TCP

El protocolo de control de transmisión (TCP) (RFC 793) es uno de los protocolos principales del conjunto de protocolos de Internet (IP), y está tan extendido que a menudo se le hace referencia junto a IP como ***TCP/IP***. Se considera que el TCP es un protocolo de transporte fiable, ya que ofrece comprobación de errores mientras transmite y recibe segmentos, reconoce los segmentos recibidos y reorganiza los segmentos recibidos en un orden incorrecto. TCP también solicita y ofrece la retransmisión de segmentos que faltaban. TCP se basa en el estado y conexión, lo que significa que la conexión entre el remitente y el receptor se establece durante la duración de la sesión. TCP ofrece un control del flujo de paquetes para que pueda gestionar la gestión de las redes.

TCP realiza un protocolo de enlace durante la configuración de la sesión para iniciar y reconocer una sesión. Cuando se han transferido los datos, la sesión se cierra de manera ordenada: cada lado transmite un paquete FIN y lo reconoce con un paquete ACK. El protocolo de enlace que inicia la sesión TCP suele ser un protocolo de enlace en tres pasos (un intercambio de tres mensajes) entre el iniciador y el agente de escucha, o puede ser una variación, como un protocolo de enlace en cuatro o cinco pasos o abierto simultáneo. En Descarte de paquetes de protocolo de enlace dividido de TCP se explica el proceso de Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP.

Entre las aplicaciones que usan TCP como protocolo de transporte se incluyen el protocolo de transferencia de hipertexto (HTTP), protocolo HTTP seguro (HTTPS), protocolo de transferencia de archivos (FTP), protocolo simple de transferencia de correo (SMTP), Telnet, protocolo de oficina de correos versión 3 (POP3), protocolo de acceso a mensajes de Internet (IMAP) y shell seguro (SSH).

Los siguientes temas tienen información detallada sobre la implementación PAN-OS de TCP.

- Temporizadores de TCP semicerrado y de Tiempo de espera TCP
- Temporizador RST sin verificar
- Descarte de paquetes de protocolo de enlace dividido de TCP
- Tamaño de segmento máximo (MSS)

Puede configurar la protección contra ataques basada en paquetes y, por ende, descartar paquetes IP, TCP e IPv6 con características innecesarias o descartar opciones innecesarias de los paquetes antes de admitirlos en la zona. También puede configurar la protección contra inundaciones especificando la tasa de conexiones por segundo de UDP (que no coinciden con una sesión existente) que activan una alarma, provocan que el cortafuegos descarte paquetes SYN o utilice cookies de SYN de manera aleatoria, y causan que el cortafuegos descarte paquetes SYN que superan la tasa máxima.

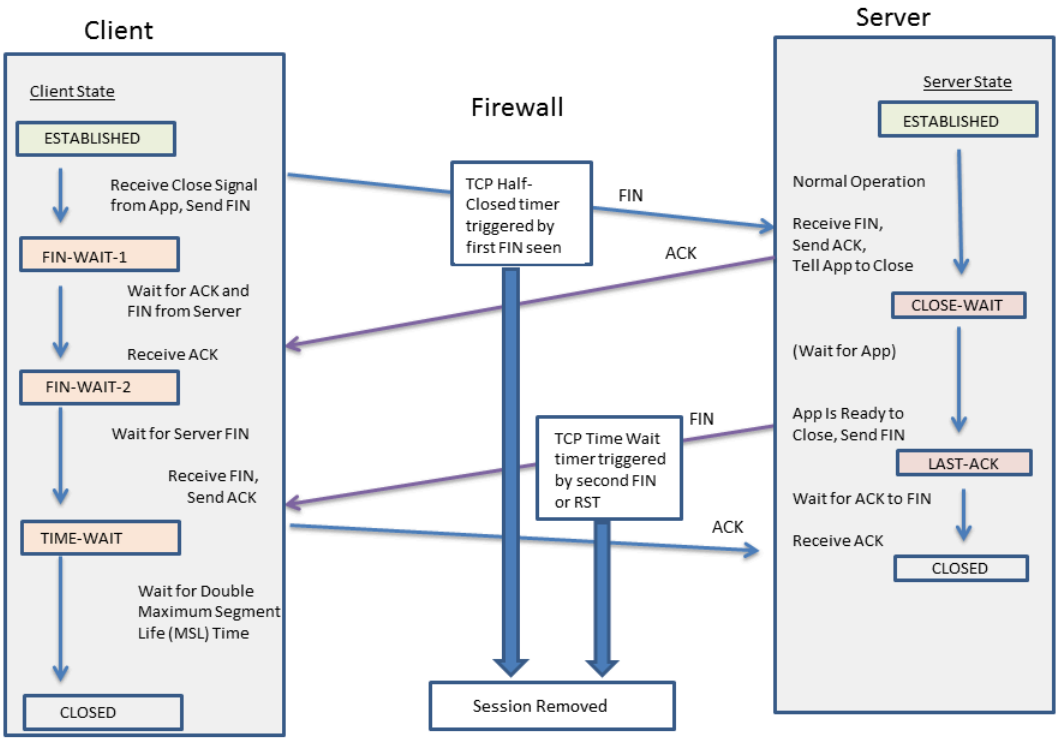
Temporizadores de TCP semicerrado y de Tiempo de espera TCP

El procedimiento de terminación de la conexión TCP usa un temporizador semicerrado TCP, que se activa con el primer FIN que detecta el cortafuegos para una sesión. El temporizador se denomina TCP semicerrado porque solo una parte de la conexión ha enviado un FIN. Un segundo temporizador, el de tiempo de espera TCP, se activa después de recibir el segundo FIN o RST.

Si en el cortafuegos solo se activara un temporizador con el primer FIN, un ajuste demasiado corto cerraría prematuramente las sesiones semicerradas. Por otro lado, un ajuste demasiado alto haría crecer demasiado la tabla de la sesión, y probablemente agotaría todas las sesiones. Dos temporizadores le permiten tener un temporizador TCP semicerrado relativamente largo y

un temporizador de tiempo de espera TCP corto, lo que hace vencer rápidamente las sesiones totalmente cerradas y controla el tamaño de la tabla de sesión.

La siguiente ilustración muestra el momento en que dos temporizadores del cortafuegos se activan durante el procedimiento de terminación de la conexión TCP.



El temporizador de tiempo de espera de TCP debe definirse con un valor inferior al temporizador semicerrado TCP por los siguientes motivos:

- Mientras más tiempo se permita tras ver el primer FIN, más tiempo tiene la otra parte de la conexión para cerrar por completo la sesión.
- El tiempo de espera más corto se debe a que no hay necesidad de que la sesión permanezca abierta durante mucho tiempo tras ver el segundo FIN o RST. Un tiempo de espera más breve libera los recursos antes, pero deja tiempo para que el cortafuegos vea la confirmación final y la posible retransmisión de otros datagramas.

Si configura un temporizador de tiempo de espera TCP con un valor más alto que el del TCP semicerrado, se aceptará la confirmación, pero en la práctica el temporizador de tiempo de espera TCP no superará el valor de TCP semicerrado.

Los temporizadores pueden definirse globalmente o por aplicación. Los ajustes globales se utilizan para todas las aplicaciones de forma predeterminada. Si configura las temporizadores de espera TCP en el nivel de aplicación, estos ajustes sustituirán a los ajustes globales.

Temporizador RST sin verificar

Si el cortafuegos recibe un paquete a RST que no puede comprobarse (porque tiene un número de secuencia inesperado con la ventana TCP o tiene una ruta asimétrica), el temporizador de RST sin verificar controla el vencimiento de la sesión. Cambia de forma predeterminada a 30 segundos, el intervalo es de 1-600 segundos. El temporizador RST sin verificar ofrece una medida de seguridad adicional, que se explica en el segundo párrafo que aparece a continuación.

Un paquete RST tendrá uno de las tres resultados posibles:

- El paquete RST queda fuera de la ventana TCP y se omite.
- El paquete RST queda dentro de la ventana TCP pero no tiene el número de secuencia esperado, por lo que queda sin verificar y está sujeto al ajuste de temporizador RST sin verificar. Este comportamiento evita los ataques de denegación de servicio (DoS), en los que se intenta interrumpir las sesiones existentes enviando paquetes RST aleatorios al cortafuegos.
- El paquete RST queda dentro de la ventana TCP y tiene el número de secuencia exacto esperado, por lo que queda sujeto al ajuste de temporizador de tiempo de espera RST.

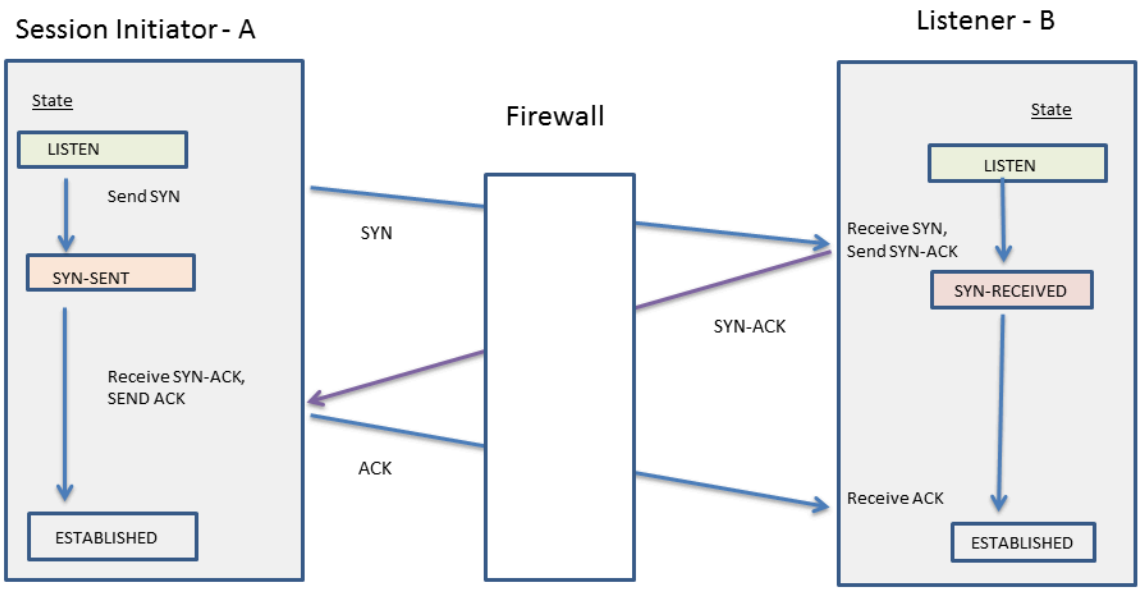
Descarte de paquetes de protocolo de enlace dividido de TCP

La opción **Split Handshake (Protocolo de enlace dividido)** en un perfil de protección de zona evitará que se establezca una sesión TCP si el procedimiento de establecimiento de sesión no utiliza el protocolo de enlace de tres pasos reconocido, sino una variación, como un protocolo de enlace dividido en cuatro o cinco pasos, o un procedimiento abierto simultáneo.

El cortafuegos de nueva generación de Palo Alto Networks® gestiona de forma correcta sesiones y todos los procesos de capa 7 para el protocolo de enlace dividido y el establecimiento de sesión abierta simultánea sin habilitar la opción de **Split Handshake (protocolo de enlace dividido)**. Sin embargo, la opción **Split Handshake (Protocolo de enlace dividido)** (que origina un descarte del protocolo de enlace dividido de TCP) pasa a estar disponible. Cuando se configura la opción de **Split Handshake (Protocolo de enlace dividido)** para un perfil de protección de zona y el perfil se aplica a una zona, las sesiones TCP para las interfaces de esa zona deben establecerse utilizando un protocolo de enlace estándar de tres direcciones; no se permiten las variaciones.

La opción **Split Handshake (Protocolo de enlace dividido)** está deshabilitada de manera predeterminada.

A continuación se ilustra el protocolo de enlace en tres pasos estándar usado para establecer una sesión TCP con un cortafuegos PAN-OS entre el iniciador (normalmente un cliente) y el agente de escucha (normalmente un servidor).



La opción **Split Handshake** está configurada para un perfil de Protección de zona que está asignado a una zona. Una interfaz que forme parte de la zona descarta cualquier paquete de sincronización (SYN) enviado desde el servidor, evitando así las siguientes variaciones de protocolos de enlace. La letra A en la figura representa al iniciador de la sesión y la B, al agente de escucha. Cada segmento numerado del protocolo de enlace tiene una flecha que indica la dirección del segmento desde el remitente hasta el destinatario, y cada segmento indica el ajuste de control de bits.

4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

Puede garantizar la Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP.

Tamaño de segmento máximo (MSS)

La unidad de transmisión máxima (maximum transmission unit, MTU) es un valor que indica la cantidad más grande de bytes que pueden transmitirse en un solo paquete TCP. La MTU incluye la extensión de los encabezados, por lo que la MTU menos la cantidad de bytes de los encabezados es igual al tamaño máximo del segmento (maximum segment size, MSS), que es la cantidad máxima de bytes de datos que pueden transmitirse en un solo paquete.

Un tamaño de ajuste de MSS configurable (se muestra a continuación) permite a su cortafuegos pasar el tráfico que tiene encabezados más extensos de lo que permite el ajuste por defecto. La encapsulación añade longitud a los encabezados, por lo que puede aumentar el tamaño de ajuste MSS para habilitar bytes, por ejemplo, para un encabezado MPLS o tráfico de túnel con una etiqueta VLAN.

Si el bit de no fragmentar (don't fragment, DF) se configura para un paquete, resulta especialmente útil tener un tamaño de ajuste de MSS mayor y un MSS menor, a fin de que los encabezados más extensos no generen una extensión de paquete que exceda la MTU permitida. Si se configuró el bit DF y se superó la MTU, los paquetes más grandes de descartarán.

Puede configurar el cortafuegos globalmente para fragmentar los paquetes IPv4 que excedan la MTU de la interfaz de salida, incluso cuando el bit de DF esté configurado en el paquete. Habilite esto para las interfaces físicas de capa 3 y las interfaces de túnel IPSec con el comando de la CLI ***debug dataplane set ip4-df-ignore yes****. Restaure el cortafuegos al comportamiento predeterminado mediante el comando de la CLI* ***debug dataplane set ipv4-df-ignore no****.*

El cortafuegos admite un tamaño de ajuste de MSS configurable para direcciones IPv4 e IPv6 en los siguientes tipos de interfaz de capa 3: Ethernet, subinterfaces, Ethernet de agregación (AE), VLAN y bucle invertido. El tamaño de ajuste de MSS de IPv6 se aplica únicamente si IPv6 está habilitada en la interfaz.

Si IPv4 e IPv6 están habilitadas en una interfaz y el tamaño de ajuste de MSS difiere entre los dos formatos de dirección IP, se usa el valor de MSS correspondiente al tipo de IP para el tráfico TCP.

Para las direcciones IPv4 e IPv6, el cortafuegos permite extensiones de encabezado TCP mayores de lo previsto. En el caso en que un paquete TCP tiene un encabezado más extenso de lo previsto, el cortafuegos elige para el tamaño de ajuste de MSS el mayor de los siguientes dos valores:

- El tamaño de ajuste de MSS configurado.
- La suma de la extensión del encabezado TCP (20) + la extensión de los encabezados IP en TCP SYN.

Este comportamiento significa que el cortafuegos cancela el tamaño de ajuste de MSS configurado si es necesario. Por ejemplo, si configura un tamaño de ajuste de MSS de 42, se prevé que el MSS sea igual a 1458 (el tamaño de MTU por defecto menos el tamaño de ajuste [1500 - 42]). Sin embargo, el paquete TCP tiene 4 bytes adicionales de opciones IP en el encabezado, por lo que el tamaño de ajuste (20+20+4) es igual a 44 que es mayor que el tamaño de ajuste de MSS configurado de 42. El MSS resultante es 1500-44=1456 bytes, menor de lo esperado.

Para configurar el tamaño de ajuste de MSS, consulte Configuración de los ajustes de sesión.

UDP

El protocolo de datagramas de usuario (UDP) (RFC 768) es otro de los principales protocolos del conjunto IP, y ofrece una alternativa al TCP. El UDP es independiente del estado y la conexión en el sentido de que no hay un protocolo para establecer sesión ni ninguna conexión entre el remitente y el receptor; los paquetes pueden tomar distintas rutas para llegar a un único destino. UDP no se considera un protocolo fiable porque no ofrece reconocimientos, comprobación de errores, retransmisión ni reorganización de datagramas. Al no tener la carga de trabajo necesaria para ofrecer estas funciones, UDP tiene una latencia reducida y es más rápido que TCP. UDP es conocido como el protocolo de menor esfuerzo, sin ningún mecanismo o forma de garantizar que los datos llegarán a su destino.

Un datagrama UDP se encapsula en un paquete IP. Aunque UDP usa una suma de comprobación para saber la integridad de los datos, no realizará ninguna comprobación de errores a nivel de la interfaz de red. Se asume que la comprobación de errores no es necesaria o que la realiza la aplicación en lugar del propio UDP. UDP no tiene ningún mecanismo para gestionar el control de flujo de paquetes.

UDP a menudo se usa con aplicaciones que requieren velocidades más altas y una entrega en tiempo real sensible al tiempo, como voz sobre IP (VoIP), transmisión de audio y vídeo y los juegos en línea. UDP se basa en las transacciones, por lo que también se usa para aplicaciones que responden a pequeñas consultas de muchos clientes, como el sistema de nombres de dominio (DNS) y el protocolo trivial de transferencia de archivos (TFTP).

Puede utilizar los perfiles de protección de zona del cortafuegos para configurar la protección contra inundaciones y, por ende, especificar la tasa de conexiones de UDP por segundo (que no coinciden con una sesión existente) que activan una alarma, provocan que el cortafuegos descarte paquetes UDP de manera aleatoria y causan que el cortafuegos descarte paquetes UDP que superan la tasa máxima. (A pesar de que el UDP es un protocolo sin conexión, el cortafuegos rastrea los datagramas UDP en los paquetes IP en función de las sesiones; por lo tanto, si el paquete UDP no coincide con una sesión existente, se considera una nueva sesión y se cuenta como una conexión en los umbrales).

ICMP

El protocolo de mensajes de control de Internet (ICMP) (RFC 792) es otro de los protocolos principales del conjunto de protocolos de Internet (IP), y opera en la capa de red del modelo OSI. El ICMP se usa para diagnóstico y control; para enviar mensajes de error sobre operaciones de IP o mensajes sobre servicios solicitados o el alcance de un host o enrutador. Hay utilidades de red como traceroute y ping que se implementan mediante varios mensajes ICMP.

ICMP es un protocolo sin conexión que no abre ni mantiene sesiones reales. Sin embargo, los mensajes ICMP entre dos dispositivos pueden considerarse una sesión.

Los cortafuegos de Palo Alto Networks® admiten ICMPv4 e ICMPv6. Puede controlar los paquetes ICMPv4 e ICMPv6 de varias maneras:

- Cree Reglas de la política de seguridad basadas en paquetes ICMP e ICMPv6 y seleccione la aplicación **icmp** o **ipv6-icmp** en la regla.
- Controle la Límite de tasa ICMPv6 cuando realice la Configuración de los ajustes de sesión.
- Configure la protección contra inundaciones al especificar la tasa de conexiones por segundo de ICMP o ICMPv6 (que no coincidan con una sesión existente) que activan una alarma. Active el cortafuegos para que descarte paquetes ICMP o ICMPv6 de manera aleatoria y provoque que descarte paquetes ICMP o ICMPv6 que superen la tasa máxima.
- Configure la protección contra ataques basada en paquetes:
  - En el caso del ICMP, puede descartar determinados tipos de paquetes o suprimir el envío de determinados paquetes.
  - En el caso de los paquetes ICMPv6 (tipos 1, 2, 3, 4 y 137), puede especificar que el cortafuegos utilice la clave de la sesión de ICMP para encontrar una coincidencia con la regla de la política de seguridad, lo que determina si se permite o no el paquete ICMPv6. (El cortafuegos utiliza la regla de la política de seguridad y anula el comportamiento predeterminado de utilizar el paquete integrado para determinar una coincidencia con la sesión). Cuando el cortafuegos descarta paquetes ICMPv6 que coinciden con una regla de la política de seguridad, el cortafuegos registra los detalles en los logs de tráfico.

Reglas de la política de seguridad basadas en paquetes ICMP e ICMPv6

El cortafuegos reenvía paquetes ICMP o ICMPv6 solo si una regla de la política de seguridad permite la sesión (como en el caso de otros tipos de paquetes). El cortafuegos determina una coincidencia con la sesión de dos maneras, en función de si el paquete es un paquete de error o un paquete de redirección ICMP o ICMPv6 en lugar de un paquete de información ICMP o ICMPv6:

- **ICMP tipos 3, 5, 11 y 12, e ICMPv6 tipos 1, 2, 3, 4 y 137**: de manera predeterminada, el cortafuegos busca los bytes de información del paquete IP integrado del datagrama que causó el error (el paquete de invocación). Si el paquete integrado coincide con una sesión existente, el cortafuegos reenvía o descarta el paquete ICMP o ICMPv6 según la acción definida en la regla de la política de seguridad que coincide con esa sesión. (Puede utilizar la protección contra ataques basada en paquetes a fin de cancelar este comportamiento predeterminado para los tipos ICMPv6).

- **Tipos de paquetes ICMP o ICMPv6 restantes:** el cortafuegos trata el paquete ICMP o ICMPv6 como si perteneciera a una nueva sesión. Si una regla de la política de seguridad coincide con el paquete (y el cortafuegos lo reconoce como una sesión **icmp** o **ipv6-icmp**), el cortafuegos reenvía o descarta el paquete en función de la acción de la regla de la política de seguridad. Los contadores de la política de seguridad y los logs de tráfico reflejan las acciones.

  Si ninguna regla de la política de seguridad coincide con el paquete, el cortafuegos aplica sus reglas predeterminadas de la política de seguridad, lo que permite tráfico intrazona y bloquea tráfico intrazona (la creación de logs está deshabilitada de manera predeterminada para estas reglas).

  A pesar de que puede anular las reglas predeterminadas para habilitar la creación de logs o cambiar la acción predeterminada, no recomendamos que modifique el comportamiento predeterminado para un caso específico dado que impactará en todo el tráfico que esas reglas predeterminadas afectan. En cambio, cree reglas de la política de seguridad para controlar y registrar paquetes ICMP o ICMPv6 explícitamente.

  Existen dos maneras de crear reglas explícitas de la política de seguridad para manejar paquetes ICMP o ICMPv6 que no son paquetes de error o redirigidos:

  - **Cree una regla de la política de seguridad para permitir (o denegar) todos los paquetes ICMP o ICMPv6:** en esta regla de la política de seguridad, especifique el **icmp** o **ipv6-icmp** de la aplicación; el cortafuegos permite (o deniega) todos los paquetes IP que coincidan con el número de protocolo ICMP (1) o el número de protocolos ICMPv6 (58), respectivamente, mediante el cortafuegos.
  - **Cree una aplicación personalizada y una regla de la política de seguridad para permitir (o denegar) paquetes desde o hacia esa aplicación:** este enfoque más detallado le permite Control de tipos y códigos específicos de ICMP o ICMPv6.

Límite de tasa ICMPv6

La limitación de tasa ICMPv6 es un mecanismo de limitación que evita las inundaciones y los intentos de DDoS. La implementación utiliza una tasa de paquetes de error y un depósito de tokens, que colaboran para permitir la limitación y garantizar que los paquetes de ICMP no inundan los segmentos de red protegidos por el cortafuegos.

Primero, la **tasa de paquetes de errores ICMPv6 globales (por segundo)** controla la tasa a la cual se permite pasar los paquetes de errores ICMP por el cortafuegos; el valor predeterminado es de 100 paquetes por segundo, el rango es de 10 a 65535 paquetes por segundo. Si el cortafuegos alcanza la tasa de paquetes de error de ICMPv6, el depósito de tokens se utiliza para activar la limitación, del siguiente modo.

El concepto de depósito de tokens lógico controla la velocidad a la que se pueden transmitir los mensajes ICMP. La cantidad de tokens en el depósito puede configurarse, y cada token representa un mensaje ICMPv6 que puede enviarse. El recuento de tokens se reduce cada vez que se envía un mensaje ICMPv6; cuando el depósito llega a cero tokens, ya no es posible enviar más mensajes ICMPv6 hasta que se añada otro token al depósito. El tamaño predeterminado del depósito de tokens es de 100 tokens (paquetes), y el intervalo es de 10 a 65535 tokens.

Para cambiar el tamaño predeterminado de tokens o la tasa de paquetes de errores, consulte la sección Configuración de los ajustes de sesión.

Control de tipos y códigos específicos de ICMP o ICMPv6

Utilice esta tarea para crear una aplicación ICMP o ICMPv6 personalizada y crear una regla en la política de seguridad que permita o deniegue la aplicación.

STEP 1 | Cree una aplicación personalizada para tipos y códigos de mensajes ICMP o ICMPv6.

1. Seleccione **Object (Objeto)** > **Applications (Aplicaciones)** y **Add (Añadir)** para añadir una aplicación personalizada.
2. En la pestaña **Configuration (Configuración)**, introduzca un nombre en **Name (Nombre)** para la aplicación personalizada y una descripción en **Description (Descripción)**. Por ejemplo, introduzca el nombre ping6.
3. En **Category (Categoría)**, seleccione **networking (redes)**.
4. En **Subcategory (Subcategoría)**, seleccione **ip-protocol (Protocolo IP)**.
5. En **Technology (Tecnología)**, seleccione **network-protocol (Protocolo de red)**.
6. Haga clic en **OK (Aceptar)**.
7. En la pestaña **Advanced (Avanzado)**, seleccione **ICMP Type (Tipo ICMP)** o **ICMPv6 Type (Tipo ICMPv6)**.
8. En **Type (Tipo)**, introduzca un número (rango: 0 a 255) que designe el tipo de mensaje ICMP o ICMPv6 que desea permitir o denegar. Por ejemplo, 128 corresponde al mensaje Echo Request (Solicitud de Echo) (ping).
9. Si el campo Type (Tipo) incluye los códigos, introduzca el número de **Code (Código)** (rango: 0 a 255) que aplique al valor de **Type (Tipo)** que desea permitir o denegar. Algunos valores de **Type (Tipo)** tienen solo un código 0.
10. Haga clic en **OK (Aceptar)**.

STEP 2 | Cree una regla en la política de seguridad que permita o deniegue la aplicación personalizada que creó.

Creación de una regla de política de seguridad. En la pestaña **Application (Aplicación)**, especifique el nombre de la aplicación personalizada que acaba de crear.

STEP 3 | Confirme los cambios.

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

Configuración de los tiempos de espera de sesión

El tiempo de espera de una sesión define la duración para la que PAN-OS mantiene una sesión en el cortafuegos después de la inactividad en esa sesión. De forma predeterminada, cuando la sesión agota su tiempo de espera para el protocolo, PAN-OS cierra la sesión. Puede definir un número de tiempos de espera para sesiones TCP, UDP e ICMP por separado. El tiempo de espera predeterminado se aplica a cualquier otro tipo de sesión. Estos tiempos de espera son globales, lo que significa que se aplican a todas la sesiones de ese tipo en el cortafuegos.

También puede configurar un ajuste global de tiempo de espera de caché de ARP, que controla el tiempo durante el cual el cortafuegos conserva las entradas de ARP (asignaciones de direcciones IP a direcciones de hardware) en su caché.

Además de los ajustes globales, puede definir los tiempos de espera para cada aplicación en la pestaña **Objects (Objetos)** > **Applications (Aplicaciones)**. El cortafuegos aplica los tiempos de espera de la aplicación a una aplicación que esté en estado establecido. Cuando se configuran, los tiempos de espera para una aplicación anulan los tiempos de espera globales de la sesión TCP o UDP.

Si cambia los temporizadores de TCP o UDP en el nivel de la aplicación, estos temporizadores para las aplicaciones predefinidas y las aplicaciones personalizadas compartidas se implementarán en todos los sistemas virtuales. Si desea que el temporizador de una aplicación sea diferente del temporizador de un sistema virtual, debe crear una aplicación personalizada, asignarle temporizadores únicos y asignar la aplicación personalizada a un sistema virtual único.

Realice la siguiente tarea si desea cambiar los valores predeterminados de los ajustes de tiempos de espera de sesión globales para TCP, UDP, ICMP, autenticación del portal cautivo u otros tipos de sesiones. Todos los valores se indican en segundos.

Los valores predeterminados son valores óptimos. Sin embargo, puede modificarlos según las necesidades de su red. Si configura un valor demasiado bajo, puede hacer que se detecten retrasos mínimos en la red, lo que podría producir errores a la hora de establecer conexiones con el cortafuegos. Si configura un valor demasiado alto, entonces podría retrasarse la detección de errores.

STEP 1 | Acceda a los tiempos de espera de la sesión.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique los tiempos de espera de la sesión.

STEP 2 | (Opcional) Cambie los tiempos de espera mixtos.

- **Predeterminado**: tiempo máximo que una sesión que no es TCP/UDP ni ICMP puede estar abierta sin una respuesta (el intervalo es de 1 a 15 999 999; el valor predeterminado es 30).
- **Descartar valor predeterminado**: tiempo máximo que una sesión no TCP/UDP permanece abierta cuando PAN-OS rechaza una sesión debido a las políticas de seguridad configuradas en el cortafuegos (el intervalo es de 1 a 15 999 999; el valor predeterminado es 60).
- **Análisis**: tiempo máximo de espera en el que una sesión seguirá abierta después de considerarse inactiva; se considera que una aplicación está inactiva cuando supera el

umbral de generación de aplicaciones que tiene definido (el intervalo es de 5 a 30; el valor predeterminado es 10).

- **Portal de autenticación**: Tiempo de espera de la sesión de autenticación para el formulario web del portal cautivo. Para acceder al contenido solicitado, el usuario debe introducir las credenciales de autenticación en este formato y autenticarse correctamente (el intervalo es de 1 a 15 999 999; el valor predeterminado es 30).
- Para definir otros tiempos de espera del portal de autenticación, como el temporizador de inactividad y el tiempo que debe transcurrir para volver a autenticar al usuario, seleccione **Device (Dispositivo)** > **User Identification (Identificador de usuario)** > **Authentication Portal Settings (Configuración del portal de autenticación)**. Consulte Configuración del portal de autenticación.

STEP 3 | (Opcional) Cambio de los tiempos de espera TCP.

- **Descartar TCP**: La longitud máxima de tiempo que una sesión TCP permanece abierta cuando se deniega una sesión debido a las políticas de seguridad configuradas en el cortafuegos. El intervalo es de 1 a 15,999,999; el valor predeterminado es 90.
- **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 de 1 a 15 999 999; el valor predeterminado es 3600.
- **Protocolo de enlace TCP**: Tiempo máximo entre la recepción de SYN-ACK y la siguiente ACK para establecer completamente la sesión. El intervalo es de 1 a 60; el valor predeterminado es 10.
- **Inicialización de TCP**: Tiempo máximo permitido entre la recepción de SYN y SYN-ACK antes de iniciar el temporizador del protocolo de enlace TCP. El rango es de 1 a 60; el valor predeterminado es 5.
- **TCP Half Closed (TCP semicerrado)**: Tiempo máximo entre la recepción del primer FIN y la recepción del segundo FIN o RST. El intervalo es de 1 a 604,800; el valor predeterminado es 120.
- **Tiempo de espera TCP**: Tiempo máximo después de recibir el segundo FIN o RST. El intervalo es de 1 a 600; el valor predeterminado es 15.
- **RST sin verificar**: Tiempo máximo después de recibir un RST que no se puede verificar (el RST está dentro de la ventana TCP pero tiene un número de secuencia inesperado o el RST procede de una ruta asimétrica). El intervalo es de 1 a 600; el valor predeterminado es 30.
- Consulte también el tiempo de espera de **Scan (Exploración)** en la sección (Opcional) Cambio de diversos tiempos de espera.

STEP 4 | (Opcional) Cambio de los tiempos de espera UDP.

- **Descartar UDP**: La longitud máxima de tiempo que una sesión UDP permanece abierta cuando se deniega una sesión debido a las políticas de seguridad configuradas en el cortafuegos. El intervalo es de 1 a 15,999,999; el valor predeterminado es 60.
- **UDP**: Tiempo máximo que una sesión UDP permanece abierta sin una respuesta de UDP. El intervalo es de 1 a 15,999,999; el valor predeterminado es 30.
- Consulte también el tiempo de espera de **Scan (Exploración)** en la sección (Opcional) Cambio de diversos tiempos de espera.

STEP 5 | (Opcional) Cambio de los tiempos de espera ICMP.

- **ICMP**: Tiempo máximo que una sesión ICMP puede permanecer abierta sin una respuesta de ICMP. El intervalo es de 1 a 15,999,999; el valor predeterminado es 6.
- Consulte también el tiempo de espera de **Discard Default (Descartar valor predeterminado)** y **Scan (Explorar)** en la sección (Opcional) Cambio de tiempos de espera mixtos.

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

STEP 7 | (Opcional) Cambie el tiempo de espera de caché de ARP.

1. Acceda a la CLI y especifique durante cuántos segundos el cortafuegos mantiene las entradas de ARP en el caché. Use el comando operativo **`set system setting arp-cache-timeout`** <*value*>, en el que el rango es de 60 a 65 535; el valor predeterminado es de 1800.

   Si disminuye el tiempo de espera y las entradas existentes en el caché poseen un TTL mayor que el nuevo valor de tiempo de espera, el cortafuegos elimina estas entradas y actualiza el caché de ARP. Si aumenta el tiempo de espera y las entradas existentes poseen un TTL mayor que el nuevo valor de tiempo de espera, estas vencen según el TTL y el cortafuegos almacena en caché las entradas nuevas con un valor de tiempo de espera mayor.
2. Vea la configuración de tiempo de espera de la caché de ARP con el comando operativo de la CLI **`show system setting arp-cache-timeout`**.

Configuración de los ajustes de sesión

En este tema se describen varios ajustes de las sesiones distintos de los valores de tiempo de espera. Realice esas tareas si necesita cambiar los ajustes por defecto.

STEP 1 | Cambie los ajustes de sesión.

Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** y modifique la configuración de la sesión.

STEP 2 | Especifique si aplicará las reglas de política de seguridad recientemente configuradas a las sesiones que están en curso.

Seleccione **Rematch all sessions on config policy change (Volver a cotejar todas las sesiones tras el cambio a la política configurada)** para aplicar las reglas de política de seguridad recientemente configurada a las sesiones que están en curso. Esta capacidad está habilitada de manera predeterminada. Si desmarca esta casilla de verificación, los cambios de la regla de política que realice se aplicarán únicamente a las sesiones iniciadas después de que confirmó el cambio de la política.

Por ejemplo, si se ha iniciado una sesión de Telnet mientras estaba configurada una política que permitía Telnet y usted posteriormente compiló un cambio de política para denegar Telnet, el cortafuegos aplica la política modificada a la sesión actual y la bloquea.

STEP 3 | Configure los ajustes de IPv6.

- **ICMPv6 Token Bucket Size (Tamaño de depósito de testigo de ICMPv6)**: predeterminado 100 tokens. Consulte la sección Límite de tasa de ICMPv6.
- **Tasa de paquetes (por segundo) de errores de ICMPv6** : Valor predeterminado: 100. Consulte la sección Límite de tasa de ICMPv6.
- **Enable IPv6 Firewalling (Habilitar cortafuegos IPv6)**: permite funciones de cortafuegos para IPv6. Todas las configuraciones basadas en IPv6 se ignorarán si IPv6 no se habilita. Incluso si IPv6 está activado para una interfaz, el ajuste **Cortafuegos IPv6** también debe estar activado para que IPv6 funcione.

STEP 4 | Habilite las tramas gigantes y establezca la MTU.

1. Seleccione **Enable Jumbo Frame (Habilitar tramas gigantes)** para habilitar la compatibilidad con tramas gigantes en interfaces de Ethernet. Las tramas gigantes tienen una unidad de transmisión máxima (MTU) de 9.216 bytes y están disponibles en determinados modelos.

2. Configure la **Global MTU**, dependiendo de si habilitó o no tramas gigantes:
   - Si no habilitó las tramas gigantes, la **MTU global** vuelve al valor por defecto de 1.500 bytes; el intervalo es de 576 a 1.500 bytes.
   - Si habilitó tramas gigantes, la **Global MTU** vuelve al valor por defecto de 9.192 bytes; el intervalo es de 9192 a 9.216 bytes.

   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.

   *Si importa (**Device [Dispositivo] > Setup [Configuración] > Operations [Operaciones] > Import [Importación]**), carga una configuración con Jumbo Frame habilitado y, a continuación, compila un cortafuegos que aún no tiene Jumbo Frame habilitado, la opción de ajuste **Habilitar Jumbo Frame** no se compila con la configuración. Primero debe **habilitar Jumbo Frame**, reiniciar y, a continuación, importar, cargar y compilar la configuración.*

STEP 5 | Establezca los ajustes detallados de la sesión NAT.

- **Tamaño mínimo de MTU para NAT64 en IPv6**: Introduzca la MTU global para el tráfico IPv6 traducido. El valor predeterminado de 1.280 bytes se basa en la MTU mínima estándar para el tráfico IPv6.
- **NAT Oversubscription Rate (Ratio de sobresuscripción NAT)**: si NAT se configura como traducción de IP dinámica y puerto (DIPP), es posible configurar una ratio de sobresuscripción para multiplicar el número de veces que se puede usar simultáneamente el mismo par de puertos y direcciones IP traducidas. El ratio es de 1, 2, 4 u 8. El ajuste predeterminado se basa en el modelo del cortafuegos.
- Una ratio de 1 significa que no existe ninguna sobresuscripción; cada par de dirección IP y puerto traducido se puede utilizar solo una vez en cada ocasión.
- Si el ajuste es **Platform Default (Valor predeterminado de plataforma)**, la configuración del usuario de la tasa está inhabilitada y se aplica la tasa de sobresuscripción predeterminada para el modelo.

La reducción de la ratio de sobresuscripción disminuye el número de traducciones de dispositivo de origen, pero proporciona más capacidades de regla de NAT.

STEP 6 | Establezca los ajustes detallados del vencimiento acelerado.

Seleccione **Accelerated Aging (Vencimiento acelerado)** para habilitar el vencimiento más rápido de las sesiones inactivas. También puede cambiar el umbral (%) y el factor de escala:

- **Accelerated Aging Threshold (Umbral de vencimiento acelerado)**: porcentaje de la tabla de sesión que se llena cuando comienza el vencimiento acelerado. El valor predeterminado es del 80%. Cuando la tabla de sesión alcanza este umbral (% lleno), PAN-OS aplica el factor de escala de vencimiento acelerado a los cálculos de vencimiento de todas las sesiones.
- **Accelerated Aging Scaling Factor (Factor de escala de vencimiento acelerado)**: factor de escala usado en los cálculos de vencimiento acelerado. El factor de escala predeterminado es 2, lo que significa que el vencimiento acelerado se produce a una velocidad dos veces más alta que el tiempo de espera de inactividad configurado. El tiempo de espera de inactividad configurado dividido entre 2 tiene como resultado un tiempo de espera más rápido (la mitad). Para calcular el vencimiento acelerado de la sesión, PAN-OS divide el tiempo de inactividad configurado (para ese tipo de sesión) entre el factor de escala para determinar un tiempo de espera más corto.

Por ejemplo, si se utiliza el factor de escala de 10, una sesión que por lo general vencería después de 3600 segundos lo hará 10 veces más rápido (en 1/10 del tiempo), es decir, 360 segundos.

STEP 7 | Habilite la protección de búfer de paquetes.

1. Seleccione **Packet Buffer Protection (Protección de búfer de paquetes)** para habilitar el cortafuegos para que tome medidas contra las sesiones que pueden inundar el búfer de paquetes y hacer que el tráfico no legítimo sea descartado; se habilita de forma predeterminada.
2. Si usted habilita la protección de búfer de paquetes, puede ajustar los umbrales y temporizadores que indican de qué manera el cortafuegos responde al uso indebido del búfer de paquetes.
   - **Alert (%) (Alerta)**: Cuando la utilización del búfer de paquetes supera este umbral, el cortafuegos crea un evento de logs. El umbral se configura en el 50 % de manera predeterminada y el intervalo es del 0 % al 99 %. Si el valor se configura en 0 %, el cortafuegos no crea un evento de log.
   - **Activate (%) (Activar)**: Cuando la utilización de un búfer de paquetes supera este umbral, el cortafuegos aplica el descarte aleatorio temprano (random early drop, RED) a las sesiones negativas. El umbral se configura en el 80 % de manera predeterminada y el intervalo es del 0 % al 99 %. Si el valor se configura en 0 %, el cortafuegos no aplica el RED.

     Los eventos de alerta se registran en el log del sistema. Los eventos para el tráfico descartado, las sesiones descartadas y la dirección IP bloqueada se registran en el log de amenazas.

   - **Block Hold Time (sec) (Tiempo de espera de bloqueo [s])**: el tiempo que se permite continuar a la sesión mitigada con RED antes de que se descarte. Por defecto, el tiempo de espera del bloqueo es de 60 segundos. El intervalo es de 0 a 65.535. Si el valor se configura en 0, el cortafuegos no descarta las sesiones en función de la protección de búfer de paquetes.

- **Block Duration (sec) (Duración del bloqueo [s])**: Este ajuste define por cuánto tiempo se descarta una sesión o se bloquea una dirección IP. El valor predeterminado es 3600 segundos con un intervalo de 0 segundos a 15 999 999 segundos. Si este valor se configura en 0, el cortafuegos no descarta las sesiones ni bloquea las direcciones IP en función de la protección de búfer de paquetes.

STEP 8 | Habilite el almacenamiento en búfer de los paquetes de configuración de ruta de multidifusión.

1. Seleccione **Multicast Route Setup Buffering**para habilitar al cortafuegos para preservar el primer paquete en una sesión de multidifusión cuando la ruta multidifusión o la entrada de la base de información de reenvío (forwarding information base, FIB) todavía no existe para el grupo de multidifusión correspondiente. De manera predeterminada, el cortafuegos no almacena en búfer el primer paquete multicast en una sesión nueva, en cambio, usa el primer paquete para configurar la ruta multicast. Este es un funcionamiento esperado para el tráfico multicast. Solo debe habilitar la configuración de buffering de ruta multicast si los servidores de contenido están directamente conectados con el cortafuegos y su aplicación personalizada no puede resistir que el primer paquete de la sesión se omita. Esta opción está deshabilitada de manera predeterminada.
2. Si habilita el almacenamiento en búfer, también puede ajustar el **Buffer Size (Tamaño de búfer)**, que especifica el tamaño del búfer según el flujo. El cortafuegos puede almacenar en búfer un máximo de 5000 paquetes.

> *También puede ajustar la duración, en segundos, durante la cual una ruta de multidifusión permanece en la tabla de enrutamiento en el cortafuegos después de que la sesión finaliza al configurar los ajustes de multidifusión en el enrutador virtual que maneja su enrutador virtual (configure **Multicast Route Age Out Time [sec] [Tiempo de vencimiento de ruta de multidifusión [s]]** en la pestaña **Multicast [Multidifusión] > Advanced [Avanzado]** en la configuración de enrutador virtual).*

STEP 9 | Guarde los ajustes de sesión.

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

STEP 10 | Configure los ajustes detallados de Maximum Segment Size (MSS) (Tamaño máximo del segmento) para una interfaz de capa 3.

1. Seleccione **Network (Red)** > **Interfaces**, seleccione **Ethernet**, **VLAN** o **Loopback (Bucle invertido)**, y seleccione la interfaz de capa 3.
2. Seleccione **Advanced (Avanzado)** > **Other Info (Otra información)**.
3. Seleccione **Adjust TCP MSS (Ajustar tamaño máximo del segmento de TCP)** e introduzca un valor para una de las dos opciones siguientes, o ambas:
   - **IPv4 MSS Adjustment Size (Tamaño de ajuste de MSS de IPv4)**: el intervalo va de 40 a 300 bytes y el valor predeterminado es 40 bytes.
   - **IPv6 MSS Adjustment Size (Tamaño de ajuste de MSS de IPv6)**: el intervalo va de 60 a 300 bytes y el valor predeterminado es 60 bytes.
4. Haga clic en **OK (Aceptar)**.

STEP 11 | Confirme los cambios.

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

STEP 12 | Reinicie el cortafuegos después de cambiar la configuración de tramas gigantes.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Operations (Operaciones)**.
2. Haga clic en **Reboot Device (Reiniciar dispositivo)**.

Política de distribución de sesiones

Las políticas de distribución de sesiones definen cómo los cortafuegos serie PA-5200 y PA-7000 distribuyen el procesamiento de seguridad (App-ID, Content-ID, filtrado de URL, cifrado SSL e IPSec) entre los procesadores de plano de datos (DP) en el cortafuegos. Cada política se diseña específicamente para un tipo determinado de entorno de red y configuración de cortafuegos para garantizar que el cortafuegos distribuya sesiones con máxima eficacia. Por ejemplo, la política de distribución de sesiones de hash es la mejor opción en los entornos que utilizan NAT de origen a gran escala.

La cantidad de DP en un cortafuegos varía según el modelo del cortafuegos:

Modelo de cortafuegos	Procesadores de planos de datos
PA-7000 Series	Depende de la cantidad de tarjetas de procesamiento de red (Network Processing Card, NPC). Cada NPC tiene varios procesadores de plano de datos (DP) y puede instalar varios NPC en el cortafuegos.
Cortafuegos PA-5220	1 ***El cortafuegos PA-5220 solo tiene un DP, de modo que las políticas de distribución de sesiones no causan efecto. Conserve la política establecida en el modo predeterminado (round-robin).***
Cortafuegos PA-5250	2
Cortafuegos PA-5260 y PA-5280	3
Firewall PA-5450	Depende del número de tarjetas de procesamiento de datos (DPD) instaladas.

Los siguientes temas proporcionan información sobre las políticas de distribución de sesiones disponibles, cómo cambiar una política activa y cómo ver las estadísticas de distribución de sesiones.

- Descripciones de las políticas de distribución de sesiones
- Cambio de la política de distribución de sesiones y visualización de las estadísticas

Descripciones de las políticas de distribución de sesiones

La siguiente tabla proporciona información sobre las Políticas de distribución de sesiones para ayudarle a decidir cuál es la política que se adapta mejor a su entorno y su configuración de cortafuegos.

Política de distribución de sesiones	Description (Descripción)
Fixed	Le permite especificar el procesador de plano de datos (DP) que utilizará el cortafuegos para el procesamiento de seguridad. Utilice esta política para la depuración.
Hash	El cortafuegos distribuye las sesiones basándose en un hash de la dirección de origen o destino. La distribución basada en hash mejora la eficiencia de la gestión de recursos de direcciones NAT y reduce la latencia de la configuración de sesiones NAT evitando posibles conflictos de puertos o direcciones IP. Utilice esta política en entornos que utilizan NAT de origen a gran escala con traducción de IP dinámicas, traducción de puertos e IP dinámicas o ambas. Cuando utilice la traducción de IP dinámicas, seleccione la opción de dirección de **origen**. Cuando utilice la traducción de puertos e IP dinámicas, seleccione la opción de dirección de **destino**.
Ingres-slot (predeterminado en cortafuegos serie PA-7000)	(Solo cortafuegos serie PA-7000) Las sesiones nuevas se asignan a un DP en la misma NPC a la que llegó el primer paquete de la sesión. La selección de DP se basa en el algoritmo session-load, pero, en este caso, las sesiones se limitan a los DP en la NPC de ingreso. Según el tráfico y la topología de red, esta política generalmente reduce las posibilidades que necesitará el tráfico para atravesar la matriz de conmutación. Utilice esta política para reducir la latencia si la NPC de ingreso y la NPC de salida se encuentran en la misma NPC. Si el cortafuegos cuenta con una combinación de NPC (por ejemplo, PA-7000 20G y PA-7000 20GXM), esta política puede aislar la capacidad aumentada a la NPC correspondiente y ayudar a aislar el impacto de los fallos de la NPC.
Random	De manera aleatoria, el cortafuegos selecciona un DP para el procesamiento de sesiones.
Round-robin (predeterminado en cortafuegos serie PA-5200)	El cortafuegos selecciona el procesador del plano de datos en función de un algoritmo round-robin entre planos de datos activos de modo que la entrada, la salida y las funciones de procesamiento de seguridad se compartan entre todos los planos de datos.

Política de distribución de sesiones	Description (Descripción)
	Utilice esta política en entornos de baja a media exigencia donde alcanzará un algoritmo de equilibrio de carga simple y predecible. En entornos de alta exigencia, recomendamos que utilice el algoritmo session-load.
Session-load	Esta política es similar a la política round-robin, pero utiliza un algoritmo basado en el peso para determinar cómo distribuir sesiones para lograr un equilibrio entre los DP. Debido a la variedad en la duración de una sesión, es probable que el DP no experimente siempre una carga uniforme. Por ejemplo, si el cortafuegos tiene tres DP y DP0 se encuentra al 25 % de la capacidad; DP1, al 25 % de la capacidad; y DP2, al 50 % de capacidad, se preferirá que la asignación de la nueva sesión se incline por la DP con menor capacidad. Esto permite mejorar el equilibrio de carga con el tiempo. Utilice esta política en entornos donde las sesiones se distribuyen a través de varias ranuras NPC, tales como un grupo de interfaces agregadas de varias ranuras o en entornos con reenvío asimétrico. También puede utilizar esta política o la política ingress-slot si el cortafuegos tiene una combinación de NPC con diferentes capacidades para las sesiones (como una combinación de NPC PA-7000 20G y PA-7000 20GXM).
Hash simétrico	(Cortafuegos serie PA-5200 y PA-7000 que ejecutan PAN-OS 8.0 o posterior) El cortafuegos selecciona el DP con un hash de direcciones IP de origen y de destino ordenadas. Esta política ofrece los mismos resultados para el tráfico server-to-client (s2c) y client-to-server (c2s) (suponiendo que el cortafuegos no utiliza NAT). Utilice esta política en implementaciones de IPSec o GTP de alta exigencia. Con estos protocolos, cada dirección se trata como un flujo unidireccional donde las tuplas de flujo no se pueden dividir. Esta política mejora el rendimiento y reduce la latencia garantizando que ambas direcciones se asignen al mismo DP, lo que elimina la necesidad de una comunicación entre DP.

Cambio de la política de distribución de sesiones y visualización de las estadísticas

La siguiente tabla describe cómo ver y cambiar las Políticas de distribución de sesiones activas y describe cómo ver las estadísticas de las sesiones de cada procesador del plano de datos (DP) en el cortafuegos.

Tarea	Comando

Mostrar la política activa de distribución de sesiones.	Utilice el comando **show session distribution policy** para ver la política activa de distribución de sesiones.
	El siguiente resultado muestra un cortafuegos PA-7080 con cuatro NPC instaladas en las ranuras 2, 10, 11 y 12 con la política de distribución ingress-slot habilitada:
	`> show session distribution policy`
	`Ownership Distribution Policy: ingress-slot`
	`Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12]`

Cambiar la política activa de distribución de sesiones.	Utilice el comando **set session distribution-policy *<policy>*** para cambiar la política activa de distribución de sesiones. Por ejemplo, para seleccionar la política session-load, introduzca el siguiente comando: `> set session distribution-policy session-load`

Ver estadísticas de distribución de sesiones.	Utilice el comando **show session distribution statistics** para ver los procesadores del plano de datos (DP) en el cortafuegos y la cantidad de sesiones en cada DP activo.
	El siguiente resultado es de un cortafuegos PA-7080:
	`> show session distribution statistics`
	`DP  Active  Dispatched Dispatched/sec`
	`----------------------------------------`
	`s1dp0  78698  7829818  1473`
	`s1dp1  78775  7831384  1535`
	`s3dp0  7796  736639  1488`
	`s3dp1  7707  737026  1442`
	La **columna Active DP (DP activos)** enumera cada plano de datos en las NPC instaladas. Los primeros dos caracteres indican el

Tarea	Comando
	número de ranura y los últimos tres caracteres indican el número de plano de datos. Por ejemplo, s1dp0 indica que el plano de datos es 0 en la NPC instalada en la ranura 1 y s1dp1 indica que el plano de datos es 1 en la NPC instalada en la ranura 1. La columna **`Dispatched (Enviados)`** muestra el número total de sesiones que ha procesado el plano de datos desde la última vez que se reinició el cortafuegos. La columna **`Dispatched/sec (Enviados/s)`** indica la tasa de envío. Si se suman los números en la columna **`Dispatched (Enviados)`**, el total equivale al número de sesiones activas en el cortafuegos. También podrá ver el número total de sesiones activas al ver el resultado del comando de la CLI **`show session info`**. *El resultado del cortafuegos serie PA-5200 será similar, excepto porque el número de los DP depende del modelo y que solo hay una ranura de NPC (s1).*

Prohibición del establecimiento de sesión de protocolo de enlace dividido de TCP

Puede configurar un descarte del protocolo de enlace dividido de TCP en un perfil de protección de zona para evitar que se establezcan sesiones de TCP a menos que se utilice el protocolo de enlace en tres pasos estándar. Esta tarea supone que usted asigne una zona de seguridad para la interfaz en la que desea evitar que los protocolos de enlace divididos de TCP establezcan una sesión.

STEP 1 | Configure un perfil de Zona de protección para impedir que las sesiones de TCP establezcan una sesión si no es mediante un protocolo de enlace en tres pasos.

1. Seleccione **Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y haga clic en **Add (Añadir)** para añadir un nuevo perfil (o seleccione un perfil existente).
2. Si está creando un nuevo perfil, introduzca un nombre en **Name** para el perfil y una descripción opcional en **Description**.
3. Seleccione **Packet Based Attack Protection (Protección contra ataques basados en paquetes)** > **TCP Drop (Descarte de TCP)** y seleccione **Split Handshake (Protocolo de enlace dividido)**.
4. Haga clic en **OK (Aceptar)**.

STEP 2 | Aplique el perfil a una o más zonas de seguridad.

1. Seleccione **Network (Red)** > **Zones (Zonas)** y seleccione la zona a la que desea asignar el perfil de protección de zona.
2. En la lista **Zone Protection Profile (Perfil de protección de zona)** de la ventana Zone (Zona), seleccione el perfil configurado en el paso anterior.

   O bien, puede iniciar la creación de un nuevo perfil al hacer clic en **Zone Protection Profile**, en cuyo caso debe continuar según corresponda.
3. Haga clic en **OK (Aceptar)**.
4. (Opcional) Repita los pasos del 1 al 3 para aplicar el perfil a zonas adicionales.

STEP 3 | Confirme los cambios.

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

Inspección del contenido del túnel

El cortafuegos puede inspeccionar el contenido del tráfico de los protocolos de túneles de texto sin cifrar sin tener que finalizar los túneles:

- Encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) (RFC 2784)
- Tráfico IPSec no cifrado (NULL Encryption Algorithm for IPSec [Algoritmo de cifrado nulo para IPSec] [RFC 2410] y modo de transporte AH IPSec)
- Protocolo de túnel del servicio general de paquetes vía radio para datos de usuario (general packet radio service [GPRS] tunneling protocol for user data, GTP-U)
- Red de área local ampliable virtual (virtual extensible local area network, VXLAN) (RFC 7348)

La inspección de contenido de túnel es para los túneles de texto normal, no para túneles de VPN o LSVPN, que transportan tráfico cifrado.

Puede utilizar la inspección del contenido del túnel para aplicar las políticas de seguridad, las políticas de protección contra DoS y las políticas de QoS en el tráfico en estos tipos de túneles y en el tráfico anidado dentro de otro túnel de texto normal (por ejemplo, un túnel IPSec con cifrado nulo dentro de un túnel GRE). Puede consultar los logs de inspección del túnel y la actividad del túnel en el ACC para verificar que el tráfico de túnel cumple con sus políticas corporativas de seguridad y uso.

Todos los modelos de cortafuegos admiten la inspección del contenido de los túneles con los protocolos GRE, IPSec sin cifrar y VXLAN. Solo admiten la inspección del contenido de los túneles con GTP-U los cortafuegos que admiten la seguridad de GTP. Consulte las versiones de PAN-OS por modelos que admiten la seguridad de GTP y SCTP en la matriz de compatibilidad.

De forma predeterminada, los cortafuegos compatibles realizan la aceleración de túneles para mejorar el rendimiento y la producción del tráfico que pasa por túneles GRE, VXLAN y GTP-U. La aceleración del túnel proporciona descarga de hardware para reducir el tiempo que se tarda en realizar búsquedas de flujo y permite que el tráfico del túnel se distribuya de manera más eficiente en función del tráfico interno. Sin embargo, puede Deshabilitación de aceleración de túneles para solucionar el problema.

- Descripción general de la inspección del contenido del túnel
- Configuración de la inspección del contenido del túnel
- Visualización de actividad de túneles inspeccionados
- Visualización de información del túnel en logs
- Creación de un informe personalizado basado en el tráfico de túnel etiquetado
- Deshabilitación de aceleración de túneles

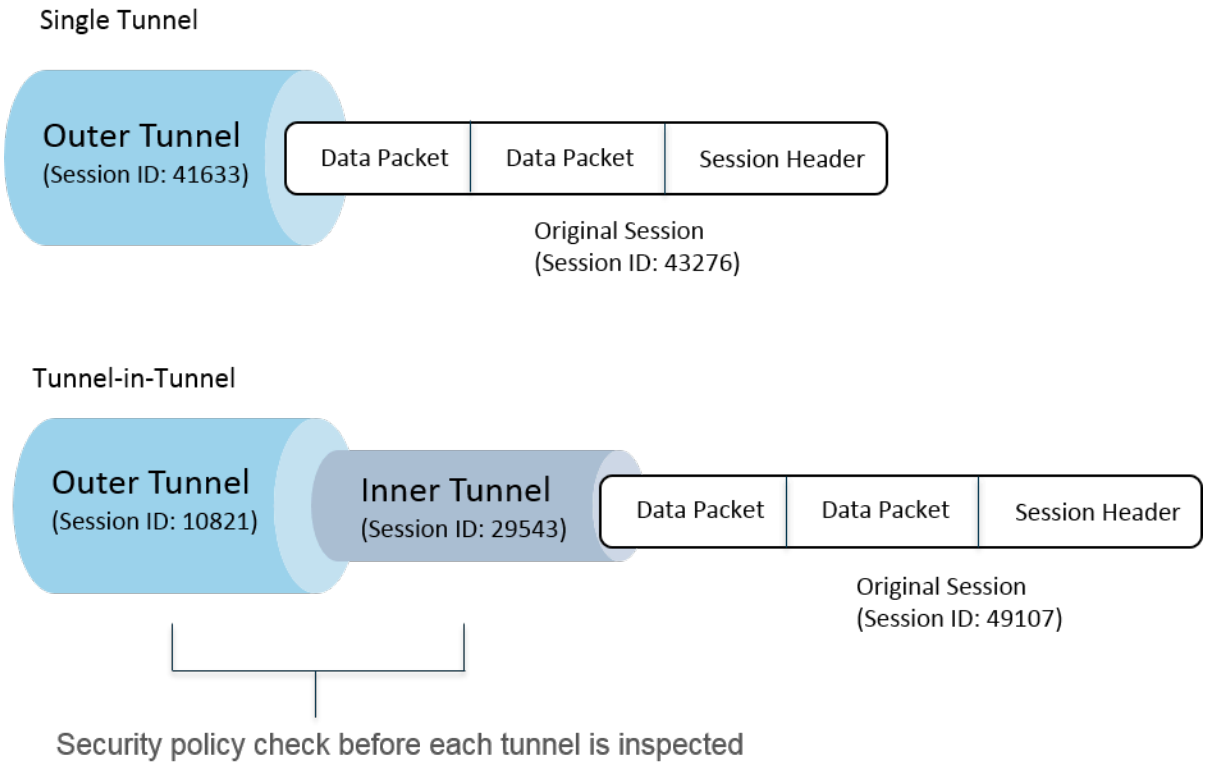
Descripción general de la inspección del contenido del túnel

Su cortafuegos puede inspeccionar el contenido del túnel en cualquier parte de la red donde no tenga la oportunidad de finalizar el túnel en primer lugar. Siempre que el cortafuegos esté en la ruta de un túnel de GRE, IPSec sin cifrar, GTP-U o VXLAN, puede inspeccionar el contenido del túnel.

- Los clientes empresariales que deseen usar la inspección del contenido de los túneles pueden tener parte o la totalidad del tráfico en el cortafuegos tunelizado por medio de GRE, VXLAN o IPSec sin cifrar. Por motivos de seguridad, QoS y presentación de informes, debe inspeccionar el tráfico dentro del túnel.
- Los clientes de proveedores de servicio usan GTP-U para tunelizar el tráfico de datos desde dispositivos móviles. Debe inspeccionar el contenido interno sin finalizar el protocolo de túnel y debe registrar los datos de usuario desde sus usuarios.

El cortafuegos admite la inspección del contenido de los túneles en interfaces de Ethernet, subinterfaces, interfaces de Ethernet agregada (aggregate Ethernet, AE), interfaces de VLAN e interfaces de túneles de VPN y LSVPN. (El túnel de texto no cifrado que el cortafuegos inspecciona puede estar dentro de un túnel VPN o LSVPN que finalice en el cortafuegos; por lo tanto, una interfaz de túnel VPN o LSVPN. En otras palabras, cuando el cortafuegos es un endpoint VPN o LSVPN, el cortafuegos puede inspeccionar el tráfico de cualquier protocolo de túnel no cifrado que la inspección del contenido de túnel admita).

La inspección del contenido de túnel se admite en las implementaciones de capa 3, capa 2, cable virtual y tap. La inspección del contenido de túnel funciona en puertas de enlace compartidas y en comunicaciones de sistema virtual a sistema virtual.



La figura anterior ilustra los dos niveles de inspección de túnel que el cortafuegos pueda realizar. Cuando un cortafuegos configurado con las reglas de política de inspección de túnel recibe un paquete:

- El cortafuegos primero realiza una comprobación de política de seguridad para determinar si el protocolo de túnel (aplicación) en el paquete está permitido o denegado. (Los paquetes IPv4 e IPv6 son protocolos compatibles dentro del túnel).
- Si la política de seguridad permite el paquete, el cortafuegos compara el paquete con una regla de política de inspección de túnel basada en la zona de origen, la dirección de origen, el usuario de origen, la zona de destino y la dirección de destino. La regla de política de inspección de túnel determina los protocolos de túnel que el cortafuegos inspecciona, el nivel máximo de encapsulación permitida (un solo túnel o un túnel dentro de un túnel), si permitir paquetes que contengan un protocolo de túnel que no aprueba la inspección de encabezado estricto según RFC 2780, y si permitir paquetes que contengan protocolos desconocidos.
- Si el paquete supera los criterios de coincidencia de la regla de la política de inspección de túnel, el cortafuegos inspecciona el contenido interno, que está sujeto a su política de seguridad (obligatoria) y las políticas opcionales que pueda especificar. (Los tipos de política admitidos para la sesión original se enumeran en la tabla siguiente).
- Si, por el contrario, el cortafuegos encuentra otro túnel, el cortafuegos recursivamente analiza el paquete para el segundo encabezado y ahora está al nivel dos de encapsulación, de manera que la segunda regla de política de inspección de túnel, que coincide con una zona de túnel, debe permitir un nivel un máximo de inspección de túnel de dos niveles para que el cortafuegos continúe procesando el paquete.
  - Si su regla permite dos niveles de inspección, el cortafuegos realiza una comprobación de política de seguridad en este túnel interno y luego la comprobación de política de inspección de túnel. El protocolo de túnel que usted utiliza en un túnel interno puede ser diferente al protocolo de túnel que utiliza en el túnel externo.
  - Si su regla no permite dos niveles de inspección, el cortafuegos basa su acción según si usted lo configuró para que descarte paquetes que tienen más niveles de encapsulación que el nivel de inspección de túnel máximo que usted configuró.

De manera predeterminada, el contenido encapsulado en un túnel pertenece a la misma zona de seguridad que el túnel, y está sujeto a las reglas de política de seguridad que protegen esa zona. Sin embargo, puede configurar una ***zona de túnel***, que le da flexibilidad para configurar las reglas de política de seguridad para el contenido interno que difiere de las reglas de política de seguridad para el túnel. Si utiliza una política de inspección de túnel diferente para la zona de túnel, siempre debe tener un nivel de inspección de túnel máximo de dos niveles, debido a que, por definición, el cortafuegos busca el segundo nivel de encapsulación.

El cortafuegos no admite una regla de política de inspección de túnel que compare el tráfico de un túnel que finalice en el cortafuegos, el cortafuegos descarta los paquetes que coinciden con la sesión de túnel interno. Por ejemplo, cuando un túnel IPSec finaliza en el cortafuegos, no cree una regla de política de inspección de túnel que coincida con el túnel que usted finaliza. El cortafuegos ya inspecciona el tráfico del túnel interno, por lo que no hace falta ninguna regla de la política de inspección de túneles.

Si bien la inspección de contenido de túnel funciona en puertas de enlace compartidas en comunicaciones de sistema virtual a sistema virtual, no puede asignar zonas de túnel a puertas de enlace compartidas o comunicaciones de sistema virtual a sistema virtual; estas están sujetas a las mismas reglas de política de seguridad que las zonas a las cuales pertenecen.

Tanto las sesiones del túnel interno como las del túnel externo cuentan para la capacidad máxima de sesiones del modelo de cortafuegos.

La siguiente tabla indica con una marca de verificación qué tipos de política puede aplicar a una sesión de túnel externa, una sesión de túnel interna y la sesión original interna:

Tipo de política	Sesión de túnel externa	Sesión de túnel interna	Sesión original interna
Cancelación de aplicación	✓ Solo en VXLAN	–	✓
Protección DoS	✓	✓	✓
NAT	✓	–	–
Reenvío basado en políticas (PBF) y retorno simétrico	✓	–	–
QoS	–	–	✓
Seguridad (obligatorio)	✓	✓	✓
User-ID	✓	✓	✓
Protección de zona	✓	✓	✓

VXLAN es diferente de otros protocolos. El cortafuegos puede usar cualquiera de los dos conjuntos diferentes de claves de sesiones para crear sesiones de VXLAN en el túnel externo.

- VXLAN UDP Session (Sesión de UDP de VXLAN): la clave es una tupla de seis elementos (zona, IP de origen, IP de destino, protocolo, puerto de origen y puerto de destino) que crea una sesión de UDP de VXLAN.
- VNI Session (Sesión de VNI): la clave es una tupla de cinco elementos que incorpora el ID del túnel (identificador de red VXLAN [VXLAN network identifier, VNI]) y utiliza la zona, la IP de origen, la IP de destino, el protocolo y el ID del túnel para crear una sesión de VNI.

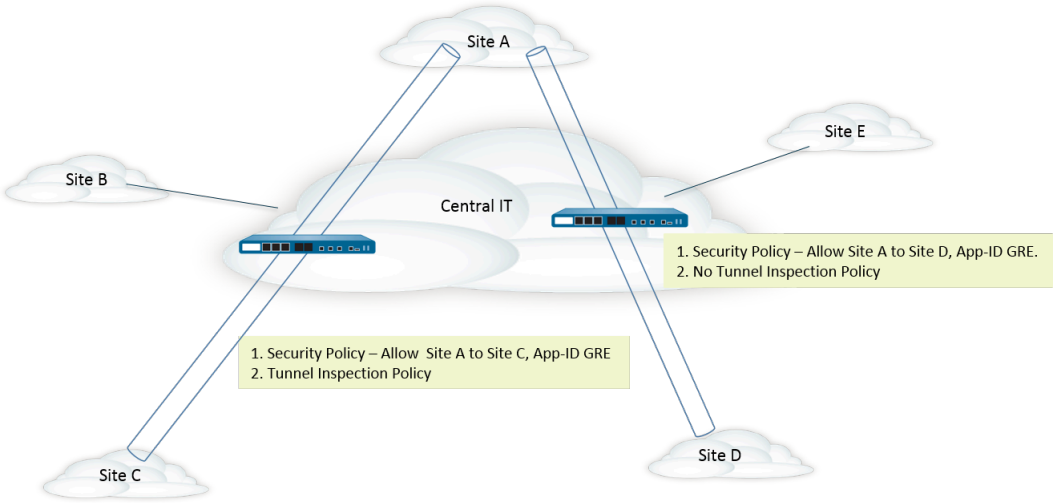
Puede Visualizar la actividad de túnel inspeccionado en el ACC o Visualizar la información de túnel en logs. Para facilitar una visualización rápida, configure una etiqueta de supervisión para poder supervisar la actividad del túnel y filtrar los resultados de log según esa etiqueta.

La actividad de túnel ACC proporciona datos en diferentes vistas. Para el uso de ID de túnel, etiqueta de supervisión de túnel y uso de aplicación de túnel, los datos de **bytes**, **sessions (sesiones)**, **threats (amenazas)**, **content (contenido)** y **URL** provienen de la base de datos de resumen de tráfico. Para el usuario del túnel, la IP de origen tunelizada y la actividad de IP de destino tunelizada, los datos de **bytes** y **sessions (sesiones)** provienen de la base de datos de resumen de tráfico, los datos de **threats (amenazas)** provienen del resumen de amenazas, los datos de **URL** provienen del resumen de URL y los datos de **contents (contenido)** provienen de la base de datos Data (Datos), que es un subconjunto de los logs de amenazas.

Si usted habilita NetFlow en la interfaz, NetFlow capturará las estadísticas del túnel externo únicamente, para evitar el recuento doble (recuento de bytes en los flujos interno y externo).

Para obtener información sobre la regla de política de inspección de túnel y las prestaciones de zona de túnel para su modelo de cortafuegos, consulte la Herramienta de selección de producto.

La siguiente figura ilustra una corporación que incluye varias divisiones y utiliza diferentes políticas de seguridad y una política de inspección de túnel. Un equipo de TI central se encarga de la conectividad entre las regiones. Un túnel conecta la ubicación A con la ubicación C; otro túnel conecta la ubicación A con la ubicación D. TI Central coloca un cortafuegos en la ruta de cada túnel; el cortafuegos en el túnel entre las ubicaciones A y C realiza la inspección de túnel; el cortafuegos en el túnel entre las ubicaciones A y D no posee una política de inspección de túnel debido a que el tráfico es muy delicado.



Configuración de la inspección del contenido del túnel

Realice esta tarea para configurar la inspección del contenido del túnel para un protocolo de túnel que usted permita en un túnel.

STEP 1 | Cree una regla de política de seguridad para permitir los paquetes que utilizan una aplicación específica (como la aplicación GRE) en el túnel desde la zona de origen a la zona de destino.

Creación de una regla de política de seguridad

El cortafuegos puede crear logs de inspección de túnel al inicio, al final de la sesión o en ambos momentos. Cuando especifique ***Actions (Acciones)*** *para la regla de política de seguridad, seleccione* ***Log at Session Start (Registrarse al inicio de la sesión)*** *para las sesiones de túnel de larga duración, como las sesiones GRE.*

STEP 2 | Cree una regla de política de inspección de túnel.

1. Seleccione **Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y luego **Add (Añadir)** para añadir una regla de políticas.
2. En la pestaña **General**, introduzca en **Name (Nombre)** un nombre para la regla de la política de inspección de túneles; debe empezar por un carácter alfanumérico y puede incluir caracteres alfanuméricos, guiones bajos, guiones, puntos y espacios.
3. Opcional) Introduzca una **descripción**.
4. Opcional) Especifique una **Tag (Etiqueta)** que identifique los paquetes que están sujetos a la regla de política de inspección de túnel, para fines de informes y registro.

STEP 3 | Especifique los criterios que determinan el origen de los paquetes a los cuales se aplica la regla de política de inspección de túneles.

1. Seleccione la pestaña **Source (Origen)**.
2. Seleccione **Add (Añadir)** para añadir una **Source Zone (Zona de origen)** en la lista de zonas (el valor predeterminado es **Any [Cualquiera]**).
3. Opcional) Seleccione **Add (Añadir)** para añadir una **Source Address (Dirección de origen)**. Puede introducir una dirección IPv4 o IPv6, un grupo de direcciones o un objeto de dirección de región geográfica **Any [Cualquiera]**).
4. Opcional) Seleccione **Negate (Negar)** para seleccionar cualquier dirección excepto las que especifica.
5. Opcional) Haga clic en **Add (Añadir)** para añadir un **Source User (Usuario de origen)** (el valor predeterminado es **any [cualquiera]**). **Known-user (Usuario conocido)** es un usuario que se ha autenticado; un usuario **Unknown (Desconocido)**, no se ha autenticado.

STEP 4 | Especifique los criterios que determinan el destino de los paquetes a los cuales se aplica la regla de política de inspección de túneles.

1. Seleccione la pestaña**Destination (Destino)**.
2. Seleccione**Add (Añadir)** para añadir una**Destination Zone (Zona de destino)** de la lista de zonas (el valor predeterminado es**Any [Cualquiera]**).
3. Opcional) Seleccione**Add (Añadir)** para añadir una**Destination Address (Dirección de destino)**. Puede introducir una dirección IPv4 o IPv6, un grupo de direcciones o un objeto de dirección de región geográfica (el valor predeterminado es**Any [Cualquiera]**).

   También puede configurar una nueva dirección o grupo de direcciones.
4. Opcional) Seleccione**Negate (Negar)** para seleccionar cualquier dirección excepto las que especifica.

STEP 5 | Especifique los protocolos de túnel que el cortafuegos inspeccionará para esta regla.

1. Seleccione la pestaña**Inspection (Inspección)**.
2. **Add (Añadir)** uno o más**Protocols (Protocolos)** de túnel que desea que el cortafuegos inspeccione:
   - **GRE**: el cortafuegos inspecciona los paquetes que utilizan encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) en el túnel.
   - **GTP-U**: el cortafuegos inspecciona los paquetes que utilizan el protocolo de túnel General Packet Radio Service (GPRS) para datos de usuario (GTP-U) en el túnel.
   - **Non-encrypted IPSec (IPSec sin cifrar)**: el cortafuegos inspecciona los paquetes que utilizan IPSec sin cifrar (IPSec con cifrado nulo o IPSec con encabezado de autenticación [authentication header, AH] en modo de transporte) en el túnel.
   - **VXLAN**: el cortafuegos inspecciona los paquetes que utilizan el protocolo de tunelización de red de área local ampliable virtual (virtual extensible local area network, VXLAN) en el túnel.

STEP 6 | Especifique cuántos niveles de encapsulación inspeccionará el cortafuegos y las condiciones en las que el cortafuegos descartará un paquete.

1. Seleccione**Inspect Options (Opciones de inspección)**.
2. Seleccione los**Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)** que el cortafuegos inspeccionará:
   - **One Level (Un nivel)** (predeterminado): el cortafuegos inspecciona el contenido que está en túnel externo únicamente.

     Con VXLAN, el cortafuegos inspecciona la carga útil de VXLAN para buscar el contenido o las aplicaciones encapsulados dentro del túnel. Debe seleccionar**One Level (Un nivel)** porque la inspección de VXLAN solo se realiza en el túnel externo.
   - **Two Levels (Tunnel In Tunnel) (Dos niveles [túnel en túnel)**: el cortafuegs inspecciona el contenido que está en el túnel externo y el contenido que está en el túnel interno.
3. Para especificar si el cortafuegos descarta los paquetes en determinadas circunstancias, seleccione una de estas opciones, todas o ninguna de ellas:
   - **Drop packet if over maximum tunnel inspection level (Descartar paquete si se supera el nivel máximo de inspección de túnel)**: el cortafuegos descartará el paquete que

contenga más niveles de encapsulación de los que están configurados para**Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)**.

- **Drop packet if tunnel protocol fails strict header check (Descartar paquete si el protocolo del túnel falla en la comprobación estricta de encabezado)**: el cortafuegos descarta un paquete que contiene un protocolo de túnel que utiliza un encabezado que no cumple con el RFC para el protocolo. Los encabezados no compatibles pueden indicar paquetes sospechosos. Esta opción hace que el cortafuegos verifique los encabezados GRE contra RFC 2890.

  *Si su cortafuegos tuneliza GRE con un dispositivo que implementa una versión de GRE anterior a*RFC 2890*, no debe habilitar la opción de**Drop packet if tunnel protocol fails strict header check (Descartar paquete si el protocolo de túnel falla en la comprobación estricta de encabezado).***

- **Drop packet if unknown protocol inside tunnel (Descartar paquete si hay un protocolo desconocido dentro del túnel)**: el cortafuegos descartará el paquete que contenga un protocolo dentro del túnel que el cortafuegos no pueda identificar.

  Por ejemplo, si esta opción está seleccionada, el cortafuegos descartará los paquetes IPSec cifrados que coincidan con la regla de política de inspección de túnel debido a que el cortafuegos no podrá leerlos. Por lo tanto, puede permitir los paquetes IPSec y el cortafuegos permitirá solo los paquetes AH IPsec e IPSec con cifrado Null.

- **Return scanned VXLAN tunnel to source (Devolver el túnel de VXLAN analizado al origen)**: cuando el tráfico se redirige al cortafuegos, VXLAN encapsula el paquete. La redirección del tráfico es una práctica habitual en los entornos de nube pública. Marque**Return scanned VXLAN tunnel to source (Devolver el túnel de VXLAN analizado al origen)** para restituir el paquete encapsulado al terminal del túnel de VXLAN (VXLAN tunnel endpoint, VTEP) de origen. Esta opción solo se admite en la capa 3, la subinterfaz de capa 3, la interfaz agregada de capa 3 y VLAN.

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

STEP 7 | Gestione las reglas de política de inspección de túnel.

Utilice lo siguiente para gestionar las reglas de política de inspección de túnel:

- (Campo de filtro): muestra solo las reglas de política de túnel nombradas en el campo de filtro.
- **Delete (Eliminar)**: elimina las reglas de política de túnel seleccionadas.
- **Clone (Clonar)**: una alternativa al botón**Add (Añadir)**, que duplica la regla seleccionada con un nuevo nombre, que luego puede modificar.
- **Enable (Habilitar)**: habilita las reglas de política de túnel seleccionadas.
- **Disable (Deshabilitar)**: deshabilita las reglas de política de túnel seleccionadas.
- **Move (Mover)**: desplaza las reglas de política de túnel seleccionadas hacia arriba o hacia abajo en la lista; los paquetes son evaluados según las reglas en orden descendente.
- **Highlight Unused Rules (Destacar reglas no utilizadas)**: resalta las reglas de política de túnel que no coinciden con ningún paquete desde la última vez que el cortafuegos se ha reiniciado.

STEP 8 | Opcional) Cree una zona de origen de túnel y una zona de destino de túnel para el contenido de túnel y configure una regla de política de seguridad para cada zona.

La práctica recomendada es crear zonas de túnel para su tráfico de túnel. Por lo tanto, el cortafuegos crea sesiones separadas para los paquetes tunelizados y no tunelizados que tienen la misma tupla de cinco (dirección IP y puerto de origen, dirección IP y puerto de destino, y protocolo).

La asignación de zonas de túnel al tráfico de túnel en un cortafuegos de la serie PA-5200 hace que el cortafuegos realice la inspección de túnel en el software; la inspección de túnel no se descarga en el hardware.

1. Si desea que el contenido del túnel esté sujeto a diferentes reglas de la política de seguridad de las reglas de política de seguridad para la zona del túnel externo (configurado anteriormente), seleccione**Network (Red)** > **Zones (Zonas)** y**Add (Añadir)** para añadir un**Name (Nombre)** para Tunnel Source Zone (Zona de origen del túnel).
2. Para**Location (Ubicación)**, seleccione el sistema virtual.
3. En**Tipo**, seleccione**Tunnel (Túnel)**.
4. Haga clic en**OK (Aceptar)**.
5. Repita estos pasos secundarios para crear la zona de destino de túnel.
6. Configure una regla de política de seguridad para la zona de origen del túnel.

   *Debido a que quizás no conozca al originador del tráfico de túnel o la dirección del flujo del tráfico y no desea prohibir accidentalmente el tráfico para una aplicación a través del túnel, especifique ambas zonas de túnel como la**Source Zone (Zona de origen)** y ambas zonas de túnel como la**Destination Zone (Zona de destino)** en su regla de política de seguridad, o seleccione**Any (Cuaquiera)** para las zonas de origen y destino; y luego especifique las**Applications (Aplicaciones)**.*
7. Configure una regla de política de seguridad para la zona de destino del túnel. El consejo en el paso anterior para configurar una regla de política de seguridad para la zona de origen del túnel se aplica también a la zona de destino del túnel.

STEP 9 | Opcional) Especifique la zona de origen de túnel y la zona de destino de túnel para el contenido interno.

1. Especifique la zona de origen del túnel y la zona de destino del túnel (que acaba de añadir) como las zonas para el contenido interno. Seleccione**Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y en la pestaña**General**, seleccione el**Name (Nombre)** de la regla de política de inspección que ha creado.
2. Seleccione**Inspection (Inspección)**.
3. Seleccione**Security Options (Opciones de seguridad)**.
4. Seleccione**Enable Security Options (Habilitar opciones de seguridad)** (deshabilitado de manera predeterminada) para hacer que el origen del contenido interno pertenezca a la**Tunnel Source Zone (Zona de origen del túnel)** que especifique y que el destino de

contenido interno pertenezca a la**Tunnel Destination Zone (Zona de destino del túnel)** que especifique.

Si no elige**Enable Security Options (Habilitar opciones de seguridad)**, el origen del contenido interno pertenecerá a la misma zona de origen que el origen del túnel externo y el destino de contenido interno pertenecerá a la misma zona de destino que el destino del túnel externo, y por lo tanto estarán sujetos a las mismas reglas de política de seguridad que se aplican a esas zonas externas.

5. En**Tunnel Source Zone (Zona de origen del túnel)**, seleccione la zona de túnel correspondiente que creó en el paso anterior, de modo que las políticas asociadas con esa zona se apliquen a la zona de origen del túnel. De lo contrario, de manera predeterminada, el contenido interno utilizará la misma zona de origen que se utiliza en el túnel externo y las políticas de la zona de origen del túnel externo también aplican a la zona de origen de contenido interno.
6. En**Tunnel Destination Zone (Zona de destino del túnel)**, seleccione la zona de túnel correspondiente que creó en el paso anterior, de modo que las políticas asociadas con esa zona se apliquen a la zona de destino del túnel. De lo contrario, de manera predeterminada, el contenido interno utilizará la misma zona de destino que se utiliza en el túnel externo y las políticas de la zona de destino del túnel externo también aplican a la zona de destino de contenido interno.

   *Si configura los valores de**Tunnel Source Zone (Zona de origen de túnel)** y**Tunnel Destination Zone (Zona de destino de túnel)** en la regla de la política de inspección de túneles, debe configurar zonas concretas en los campos**Source Zone (Zona de origen)** (paso3) y**Destination Zone (Zona de destino)** (paso4) de los criterios de coincidencia de dicha regla; no puede especificar**Any (Cualquiera)** en**Source Zone (Zona de origen)** ni en**Destination Zone (Zona de destino)**. De este modo, se asegura de que el sentido de la reasignación de zonas se corresponde correctamente con las zonas principales.*

   En los cortafuegos PA-5200 Series y PA-7080, si utiliza la capa subyacente de multidifusión e inspecciona VXLAN, la sesión interna se duplica en varios planos de datos y se pueden producir condiciones de carrera. Para evitar que se descarten algunos paquetes, son imprescindibles los siguientes requisitos:

   - *Configure una regla distinta de inspección del contenido de los túneles que busque coincidencias en los paquetes de VXLAN externos que se dirigen a cada uno de los VTEP.*
   - *En esa regla independiente, asigne una zona de túnel distinta. De esa forma, la sesión interna es diferente para cada terminal y no se producen condiciones de carrera, ni se descartan paquetes.*
7. Haga clic en**OK (Aceptar)**.

STEP 10 | Establezca opciones de supervisión para el tráfico que coincida con una regla de la política de inspección de túnel.

1. Seleccione**Policies (Políticas)** > **Tunnel Inspection (Inspección de túnel)** y seleccione el nombre de la regla de política de inspección de túnel que ha creado.
2. Seleccione**Inspection (Inspección)** > **Monitor Options (Opciones de supervisión)**.
3. Introduzca un**Monitor Name (Nombre de supervisor)** para agrupar el tráfico similar para fines de registro y elaboración de informes.
4. Introduzca una**Monitor Tag (number) (Etiqueta de supervisión [número])** para agrupar tráfico similar para fines de registro y elaboración de informes (el intervalo es de 1 a 16 777 215). El número de etiqueta se define globalmente.

   Este campo no se aplica al protocolo VXLAN. Los logs de VXLAN usan automáticamente el identificador de red VXLAN (VXLAN network identifier, VNI) del encabezado de VXLAN.

   Si marca el tráfico de túnel, posteriormente puede filtrar la etiqueta de supervisión en el log de inspección de túnel y usar el ACC para ver la actividad del túnel basada en la etiqueta de supervisión.
5. **Anule la configuración de logs de las reglas de seguridad** para permitir las opciones de generación y reenvío de logs para las sesiones que cumplen con la regla de la política de inspección de túnel seleccionada. Si no selecciona esta configuración, la generación y el reenvío de logs de túnel se definen con la configuración de logs de la regla de la política de seguridad que se aplica al tráfico del túnel. Puede anular los ajustes de reenvío de logs en las reglas de la política de seguridad que controlan los logs de tráfico configurando los ajustes de logs de inspección de túnel de modo que los logs de túnel y los logs de tráfico se almacenen por separado. Los logs de inspección de túneles almacenan las sesiones del túnel externo (GRE, IPSec sin cifrar, VXLAN o GTP-U) y los logs de tráfico, los flujos del tráfico interno.
6. Seleccione**Log at Session Start (Log al inicio de la sesión)** para crear logs de tráfico al inicio de la sesión.

   La práctica recomendada para los logs de túnel es crear logs al inicio de la sesión y al final de la sesión debido a que los túneles pueden ser duraderos. Por ejemplo, los túneles de GRE pueden activarse cuando el enrutador se reinicia y no finalizar hasta que el enrutador se reinicie. Si no crea logs al inicio de la sesión, nunca verá si existe un túnel de GRE activo en el ACC.
7. Seleccione**Log at Session End (Log al final de la sesión)** para crear logs de tráfico al final de la sesión.
8. Seleccione un perfil de**Log Forwarding (Reenvío de logs)** que determine dónde reenvía el cortafuegos los logs de túnel de las sesiones que cumplen con la regla de inspección de túnel. De manera alternativa, puede crear un nuevo perfil de reenvío de logs si realiza laConfiguración de reenvío de logs.
9. Haga clic en**OK (Aceptar)**.

STEP 11 | Opcional, solo en VXLAN)**Configure un VNI**. Todas las interfaces de red VXLAN se inspeccionan de manera predeterminada. Si configura VNI, la política solo inspecciona los configurados.

VXLAN es el único protocolo que utiliza la pestaña Tunnel ID (ID de túnel) para especificar el VNI.

1. Seleccione la pestaña**Tunnel ID (ID de túnel)** y haga clic en**Add (Añadir)**.
2. Asigne un nombre en**Name (Nombre)**. El nombre es un factor para mayor comodidad, no para la creación de logs, la supervisión o la creación de informes.
3. En el campo**VXLAN ID (VNI) (ID de VXLAN [VNI])**, introduzca un VNI único, una lista de VNI separados por comas, un intervalo de VNI separados por guiones o una combinación de estas opciones. Por ejemplo, puede especificar lo siguiente:

   1677002,1677003,1677011-1677038,1024

STEP 12 | Opcional) Si habilitó**Rematch Sessions (Volver a cotejar sesiones) Device [Dispositivo] > Setup [Configuración] > Session [Sesión]**), asegúrese de que el cortafuegos no descarte las sesiones existentes cuando cree o revise una política de inspección de túnel deshabilitando**Reject Non-SYN TCP (Rechazar TCP no sincronizados)** para las zonas que controlen sus políticas de seguridad de túnel.

El cortafuegos muestra la siguiente advertencia cuando usted:

- Cree una regla de política de inspección de túnel.
- Edite una regla de política de inspección de túnel añadiendo un**Protocol (Protocolo)** o aumentando los**Maximum Tunnel Inspection Levels (Niveles máximos de inspección de túnel)** de**One Level (Un nivel)** a**Two Levels (Dos niveles)**.
- Seleccione**Enable Security Options (Habilitar las opciones de seguridad)** en la pestaña**Security Options (Opciones de seguridad)** al añadir nuevas zonas o cambiar una zona por otra.

*Advertencia: La habilitación de políticas de inspección de túnel en las sesiones de túnel existentes harán que las sesiones TCP existentes dentro del túnel sean tratadas como flujos non-syn-tcp. Para garantizar que las sesiones existentes no se descarten cuando la política de inspección de túnel esté habilitada, configure el ajuste**Reject Non-SYN TCP (Rechazar TCP Non-SYN)** para las zonas en**no**, usando un perfil de protección de zona y aplíquelo a las zonas que controlan las políticas de seguridad del túnel. Una vez que las sesiones existentes han sido reconocidas por el cortafuegos, puede volver a habilitar el ajuste**Reject Non-SYN TCP (Rechazar TCP Non-SYN)** al configurarlo en**yes (sí)** o**global**.*

1. Seleccione**Network (Red) > Network Profiles (Perfiles de red) > Zone Protection (Protección de zona)** y**Add (Añadir)** para añadir un perfil.
2. Introduzca un**Name (Nombre)** para el perfil.
3. Seleccione**Packet Based Attack Protection (Protección contra ataques basados en paquetes) > TCP Drop (Descarte de TCP)**.
4. Para**Reject Non-SYN TCP (Rechazar TCP Non-SYN)**, seleccione**no**.
5. Haga clic en**OK (Aceptar)**.

6. Seleccione**Network (Red)** > **Zones (Zonas)** y seleccione la zona que controla las reglas de la política de seguridad de túnel.
7. En**Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil de protección de zona que acaba de crear.
8. Haga clic en**OK (Aceptar)**.
9. Repita los pasos 12f, 12g y 12h anteriores para aplicar el perfil de protección de zonas a las demás zonas que controlan las reglas de la política de seguridad de los túneles.
10. Una vez que las sesiones existentes han sido reconocidas por el cortafuegos, puede volver a habilitar el ajuste**Reject Non-SYN TCP (Rechazar TCP Non-SYN)** al configurarlo en**yes (sí)** o**global**.

STEP 13 | Opcional) Limite la fragmentación del tráfico en un túnel.

1. Seleccione**Network (Red)** > **Network Profiles (Perfiles de red)** > **Zone Protection (Protección de zona)** y**Add (Añadir)** para añadir un perfil por**Name (Nombre)**.
2. Introduzca una**Description (Descripción)**.
3. Seleccione una**Packet Based Attack Protection (Protección contra ataques basados en paquetes)** > **IP Drop (Descarte de IP)** > **Fragmented traffic (Tráfico de fragmentación)**.
4. Haga clic en**OK (Aceptar)**.
5. Seleccione**Network (Red)** > **Zones (Zonas)** y seleccione la zona de túnel en la que desea limitar la fragmentación.
6. Para**Zone Protection Profile (Perfil de protección de zona)**, seleccione el perfil que acaba de crear para aplicar el perfil de protección de zona a la zona de túnel.
7. Haga clic en**OK (Aceptar)**.

STEP 14 | **Commit (Confirmar)** los cambios.

Visualización de actividad de túneles inspeccionados

Realice la siguiente tarea para ver la actividad de los túneles inspeccionados.

STEP 1 | Seleccione **ACC** y seleccione un **Virtual System (Sistema virtual)** o **All (Todos)** los sistemas virtuales.

STEP 2 | Seleccione Tunnel Activity (Actividad del túnel).

STEP 3 | Seleccione un Time period (Período) para ver, como Last 24 Hrs (Últimas 24 horas) o Last 30 Days (Últimos 30 días).

STEP 4 | En Global Filters (Filtros globales), haga clic en los botones + o - para utilizar los filtros de ACC en la actividad del túnel.

STEP 5 | Vea la actividad del túnel inspeccionado; puede mostrar u ordenar los datos en cada ventana por **bytes**, **sessions (sesiones)**, **threats (amenazas)**, **content (contenido)** o **URLs**. Cada ventana muestra un aspecto diferente de los datos del túnel en un gráfico o una tabla:

- **Tunnel ID Usage (Uso de ID de túnel):** cada protocolo de túnel enumera los ID de túnel de los túneles que utilizan este protocolo. Las tablas brindan la cantidad total de bytes, las sesiones, las amenazas, el contenido y las URL del protocolo. Coloque el cursor sobre el ID de túnel para obtener un desglose de cada ID de túnel.
- **Tunnel Monitor Tag (Etiqueta de supervisión de túnel):** cada protocolo de túnel enumera las etiquetas de supervisión de túnel de los túneles que utilizan esta etiqueta. Las tablas brindan la cantidad total de bytes, las sesiones, las amenazas, el contenido y las URL de la etiqueta y el protocolo. Coloque el cursor sobre la etiqueta de supervisión de túnel para obtener un desglose de cada etiqueta.
- **Tunneled Application Usage (Uso de aplicaciones de transmisión mediante túneles):** las categorías de aplicaciones muestran mediante gráficos los tipos de aplicaciones agrupados por medios, interés general, colaboración y redes, y códigos de color según su riesgo. Las tablas de las aplicaciones también incluyen un recuento de los usuarios por aplicación.
- **Tunneled User Activity (Actividad de usuarios de transmisión mediante túneles):** muestra un gráfico de los bytes enviados y recibidos, por ejemplo, en un eje x de fecha y hora. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto. La tabla de usuario de origen y de usuario de destino brinda datos por usuario.
- **Tunneled Source IP Activity (Actividad IP de origen de transmisión mediante túneles):**muestra gráficos y tablas de bytes, sesiones, y amenazas, por ejemplo, de un atacante en una dirección IP. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto.
- **Tunneled Destination IP Activity (Actividad IP de destino de transmisión mediante túneles):** muestra gráficos y tablas basadas en las direcciones IP de destino. Vea las amenazas de cada víctima en una dirección IP, por ejemplo. Coloque el cursor sobre un punto del gráfico para ver los datos de ese punto.

Visualización de información del túnel en logs

Puede ver logs de inspección del túnel o ver información de inspección del túnel en otros tipos de logs.

Protocolos GRE, IPSec sin cifrar y GTP-U

- Cuando se produce una coincidencia con la regla de tráfico de inspección del contenido de los túneles (tunnel content inspection, TCI), los protocolos de encapsulación de enrutamiento genérico (generic routing encapsulation, GRE), de seguridad del protocolo de internet (internet protocol security, IPSec) y de túnel del servicio general de paquetes vía radio para datos de usuario (general packet radio service [GPRS] tunneling protocol for user data, GTP-U) se registran en el log de inspección de túneles con el tipo log Tunnel (Túnel) y el protocolo coincidente, así como el nombre y la etiqueta (número) de supervisión configurados.
- Si no hay ninguna coincidencia con la regla de TCI, todos los protocolos se registran en los logs de tráfico.

Protocolo VXLAN

- Cuando se produce una coincidencia con la regla de TCI, el protocolo VXLAN se registra en el log de inspección de túneles con el tipo log Tunnel (VXLAN) (Túnel [VXLAN]), el nombre de supervisión configurado y el ID del túnel (identificador de red VXLAN [VXLAN network identifier, VNI]).

  En el log de tráfico de la sesión interna, la marca Tunnel Inspected (Túnel inspeccionado) indica una sesión de VNI. La sesión principal es la sesión que estaba activa cuando se creó la sesión interna, por lo que es posible que el ID no coincida con el ID de la sesión actual.
- Si no hay ninguna coincidencia con la regla de TCI, las sesiones de VNI se registran en los logs de tráfico con el protocolo de datagramas de usuario (user datagram protocol, UDP), el puerto de origen 0 y el puerto de destino 4789 (predeterminado).

- Ver logs de inspección del túnel.
  1. Seleccione **Monitor (Supervisión)** > **Logs** > **Tunnel Inspection (Inspección de túneles)** y consulte los datos del log para identificar en **Applications (Aplicaciones)** las aplicaciones de túneles que se utilizan en el tráfico y los posibles problemas, como recuentos elevados de paquetes que no superan la comprobación estricta de encabezados.
  2. Haga clic en el icono de vista detallada () para obtener información detallada sobre el log.

- Visualice otros logs para obtener información sobre la inspección del túnel.
  1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
  2. Seleccione **Traffic (Tráfico)**, **Threat (Amenaza)**, **URL Filtering (Filtrado de URL)**, **WildFire Submissions (Envíos de WildFire)**, **Data Filtering (Filtrado de datos)** o **Unified (Unificado)**.
  3. Haga clic en el icono de vista detallada () en una entrada del log.
  4. En la ventana Flags (Marcas), consulte si se ha seleccionado la marca **Tunnel Inspected (Túnel inspeccionado)**. Una marca Tunnel Inspected (Túnel inspeccionado) indica que el cortafuegos utilizó una regla de la política Tunnel Inspection (Inspección del túnel) para inspeccionar el contenido interno o túnel interno. La información de Parent Session (Sesión

principal) corresponde a un túnel exterior (en relación a un túnel interior) o un túnel interno (en relación al contenido interno).

En los logs **Traffic (Tráfico)**, **Threat (Amenaza)**, **URL Filtering (Filtrado de URL)**, **WildFire Submissions (Envíos de WildFire)**, **Data Filtering (Filtrado de datos)**, solo la información principal directa aparece en la vista detallada del log de sesión interna, no la información del log del túnel. Si configuró dos niveles de inspección de túnel, puede seleccionar la sesión principal de la información principal directa para ver el segundo log principal. (Debe supervisar el log **Tunnel Inspection [Inspección de túnel]** como se muestra en el paso anterior para ver la información de log de túnel).

5. Mientras consulta el log de una sesión interna en la que se inspeccionan los túneles, haga clic en el enlace **View Parent Session (Ver sesión principal)** de la sección General para ver la información sobre la sesión externa.

Creación de un informe personalizado basado en el tráfico de túnel etiquetado

Puede crear un informe para recoger información en función de la etiqueta que aplicó al tráfico de túnel.

STEP 1 | Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** y haga clic en **Add (Añadir)**.

STEP 2 | En Database (Base de datos), seleccione el log de Tráfico, Amenaza, URL, Filtrado de datos o envíos de WildFire.

STEP 3 | En Available Columns (Columnas disponibles), seleccione Flags (Marcas) y Monitor Tag (Etiqueta de supervisión), además de otros datos que desee incluir en el informe.

También puede generar informes personalizados.

Deshabilitación de aceleración de túneles

De forma predeterminada, los cortafuegos compatibles realizan la aceleración de túneles para mejorar el rendimiento y la producción del tráfico que pasa por túneles GRE, VXLAN y GTP-U. La aceleración del túnel proporciona descarga de hardware para reducir el tiempo que se tarda en realizar búsquedas de flujo y permite que el tráfico del túnel se distribuya de manera más eficiente en función del tráfico interno.

La aceleración del túnel GRE y VXLAN es compatible con los cortafuegos PA-3200 Series y los cortafuegos PA-7000 Series con PA-7000-100G-NPC-A y PA-7050-SMC-B o PA-7080-SMC-B. Puede deshabilitar la aceleración del túnel para solucionar problemas. Cuando deshabilite la aceleración del túnel, lo hará para los túneles GRE, VXLAN y GTP-U simultáneamente.

STEP 1 | Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** y modifique los ajustes generales.

STEP 2 | Anule la selección de **Tunnel Acceleration (Aceleración de túnel)** para desactivarla.

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

STEP 4 | Seleccione **Confirmar**.

STEP 5 | Reinicie el cortafuegos.

STEP 6 | (Opcional) Verifique el estado de la aceleración del túnel.

1. Acceda la CLI.
2. **`> show tunnel-acceleration`**

   La salida del sistema puede tener estos estados **`Enabled (Habilitado)`** o **`Disabled (Deshabilitado)`**. Estado adicional y motivo de GTP-U únicamente:

   - **`Disabled (Deshabilitado)`**: la aceleración del túnel GTP-U no es compatible con el modelo de cortafuegos o la seguridad GTP está deshabilitada.
   - **`Error (TCI with GTP-U configured unexpectedly) (Error [TCI con GTP-U configurado inesperadamente])`**: el TCI con el protocolo GTP-U se configura cuando Tunnel Acceleration (Aceleración de túnel) se habilita.
   - **`Enabled (Habilitada)`**: Tunnel Accelaration (Aceleración de túnel) está habilitada; GTP-U Tunnel Acceleration (Aceleración de túnel GTP-U) no se está ejecutando todavía. La seguridad de GTP está habilitada, pero aún no se reinicia.
   - **`Installed (Instalado)`**: se está ejecutando la aceleración del túnel GTP-U.

Agente de paquetes de red

El agente de paquetes de red filtra y reenvía el tráfico de la red a una cadena de seguridad externa de uno o más dispositivos de seguridad de terceros. El agente de paquetes de red reemplaza la función del agente de descifrado incorporada en PAN-OS 8.1 y amplía sus capacidades para incluir el reenvío de tráfico TLS no descifrado y tráfico no TLS (texto no cifrado), así como tráfico TLS descifrado. La capacidad para manejar todo tipo de tráfico es especialmente valiosa en entornos de muy alta seguridad, como instituciones financieras y gubernamentales.

El agente de descifrado es compatible con los dispositivos PA-7000 Series, PA-5400 Series, PA-5200 Series, PA-3200 Series y los modelos VM-300 y VM-700. Este requiere que se habilite el descifrado de proxy SSL de reenvío, en el cual el cortafuegos se establece como un agente externo fiable (o man-in-the-middle) para el tráfico de sesiones.

Las interfaces de los cortafuegos no pueden actuar como agente de descifrado y como terminal de túneles de GRE.

> Descripción general del agente de paquetes de red
> Cómo funciona el agente de paquetes de red
> Preparación para implementar el agente de paquetes de red
> Configuración de las cadenas de seguridad de puente transparente
> Configuración de cadenas de seguridad de capa 3 enrutadas
> Compatibilidad con HA del agente de paquetes de red
> Cambios en la interfaz de usuario para agente de paquetes de red
> Limitaciones del agente de paquetes de red
> Solución de problemas del agente de paquetes de red

Descripción general del agente de paquetes de red

Si utiliza uno o más dispositivos de seguridad de terceros (una cadena de seguridad) como parte de su conjunto de seguridad general, puede utilizar el agente de paquetes de red para filtrar y reenviar el tráfico de red a esos dispositivos de seguridad. El agente de paquetes de red reemplaza la función del agente de descifrado incorporada en PAN-OS 8.1.

Al igual que el agente de descifrado, el agente de paquetes de red proporciona capacidades de descifrado y administración de la cadena de seguridad. Así se simplifica su red al eliminar las complicaciones que implican admitir dispositivos dedicados para esas funciones y se reducen los costos operativos y de capital. Además. al igual que el agente de descifrado, el agente de paquetes de red proporciona comprobaciones de estado para garantizar que la ruta a la cadena de seguridad esté en buen estado y opciones para manejar el tráfico si una cadena se avería.

El agente de paquetes de red amplía las capacidades de reenvío de la cadena de seguridad del cortafuegos para que pueda filtrar y reenviar no solo el tráfico TLS descifrado, sino también el tráfico TLS no descifrado y no TLS (texto no cifrado) a una o más cadenas de seguridad basadas en aplicaciones, usuarios, dispositivos, direcciones IP y zonas. Estas características son especialmente valiosas en entornos de muy alta seguridad, como instituciones financieras y gubernamentales.

Cambio a versiones superiores e inferiores:

- Al cambiar a la versión superior PAN-OS 10.1 en cortafuegos que tienen una licencia del agente de descifrado, tenga en cuenta lo siguiente:
  - El nombre de la licencia cambia de forma automática al agente de paquetes de red después de reiniciar el cortafuegos.

    Debe reiniciar el cortafuegos para que la licencia surta efecto y actualizar la interfaz de usuario, más allá de si el cortafuegos es independiente, forma parte de un par de HA o si envía licencias del agente de paquetes de red a cortafuegos desde Panorama.
  - PAN-OS traduce cualquier perfil de reenvío del agente de descifrado existente (**Profiles [Perfiles]** > **Decryption [Descifrado]** > **Forwarding Profile [Perfil de reenvío]**) en perfiles del agente de paquetes.
  - PAN-OS traduce toda política de descifrado existente para reenviar tráfico a cadenas de seguridad en reglas del agente de paquetes de red.
  - PAN-OS quita el perfil del agente de descifrado de la interfaz de usuario y lo reemplaza por el perfil del agente de paquetes (**Profiles [Perfiles]** > **Packet Broker [Agente de paquetes]**) y agrega la política del agente de paquetes de red (**Policies [Políticas]** > **Network Packet Broker [Agente de paquetes de red]**).

- Cuando cambie a la versión inferior PAN-OS 10.0 desde PAN-OS 10.1, tenga en cuenta lo siguiente:
  - PAN-OS traduce todo perfil del agente de paquetes existente en perfiles de reenvío del agente de descifrado.
  - PAN-OS quita la base de reglas del agente de paquetes de red e imprime un mensaje de advertencia. Debe volver a configurar las reglas de política de descifrado como reglas de política de descifrado para el reenvío de descifrado.
  - El nombre de la licencia sigue siendo Network Packet Broker (Agente de paquetes de red); el nombre de la licencia cambia de Decryption Broker (Agente de descifrado) a Network Packet Broker (Agente de paquetes de red) en todas las versiones de PAN-OS después de un reinicio y no afecta al funcionamiento del agente de descifrado). Sin embargo, la funcionalidad es la funcionalidad del agente de descifrado, no la del agente de paquetes de red.
  - PAN-OS quita el perfil del agente de paquetes de red de la interfaz de usuario y lo reemplaza por el perfil de reenvío de descifrado. También quita la política del agente de paquetes de red de la interfaz de usuario (no hay reemplazo; se utilizan reglas de políticas de descifrado para reenviar solo el tráfico de proxy de reenvío descifrado para cadenas de seguridad).

Requisitos para utilizar el agente de paquetes de red:

- Debe instalar una licencia gratuita del agente de paquetes en el cortafuegos. Sin la licencia gratuita, no puede acceder a la política ni al perfil del agente de paquetes en la interfaz.
- El cortafuegos debe tener, al menos, dos interfaces Ethernet de capa 3 disponibles para usar como un par dedicado de interfaces de reenvío de agentes de paquetes.
  - Puede configurar varios pares de interfaces de reenvío dedicadas del agente de paquetes de red para conectarse a diferentes cadenas de seguridad.
  - Para cada cadena de seguridad, el par de interfaces dedicadas del agente de paquetes de red debe estar en la misma zona de seguridad.
  - El par de interfaces dedicadas se conectan al primer y último dispositivo de una cadena de seguridad.

  El agente de paquetes de red admite cadenas de seguridad de capa 3 enrutadas y cadenas de seguridad de capa 1 de puente transparente. Para las cadenas de capa 3 enrutadas, un par de interfaces de reenvío de agentes de paquetes puede conectarse a varias cadenas de seguridad de capa 3 mediante un conmutador, enrutador u otro dispositivo configurado de forma correcta para realizar el enrutamiento de capa 3 requerido entre el cortafuegos y las cadenas de seguridad.
- Las interfaces de reenvío dedicadas del agente de paquetes de red no pueden utilizar protocolos de enrutamiento dinámico.
- Ninguno de los dispositivos de la cadena de seguridad puede modificar la dirección IP de origen o destino, el puerto de origen o destino ni el protocolo de la sesión original porque el cortafuegos no podría hacer coincidir la sesión modificada con la sesión original y, por lo tanto, eliminaría el tráfico.

El agente de paquetes de red admite lo siguiente:

- Tráfico TLS descifrado, TLS no descifrado y no TLS.
- Proxy SSL de reenvío, inspección de SSL entrante y tráfico SSH cifrado.

- Cadenas de seguridad de capa 3 enrutadas.
- Cadenas de seguridad de capa 1 de puente transparente.

  Puede configurar ambas cadenas de seguridad de capa 3 y capa 1 de puente transparente enrutadas en el mismo cortafuegos, pero debe utilizar diferentes pares de interfaces de reenvío para cada tipo.

- Flujo de tráfico unidireccional a través de la cadena: todo el tráfico a la cadena sale del cortafuegos mediante una interfaz dedicada y regresa a este a través de otra interfaz dedicada, por lo que todo el tráfico fluye en la misma dirección a través del par de interfaces dedicadas del agente de paquetes de red.

  Ambas interfaces de reenvío de cortafuegos deben estar en la misma zona.

- Flujo de tráfico bidireccional a través de la cadena de seguridad:
  - El tráfico de cliente a servidor (c2s) sale del cortafuegos mediante una interfaz de agente de cortafuegos dedicada y regresa a este a través de otra interfaz de agente de cortafuegos dedicada.
  - El tráfico de servidor a cliente (s2c) utiliza las mismas dos interfaces de agente de cortafuegos dedicadas que el tráfico c2s, pero el tráfico fluye en la dirección opuesta a través de la cadena de seguridad. La interfaz del agente de cortafuegos en la que el tráfico s2c va a la cadena es la misma interfaz en la que el tráfico c2s regresa de la cadena al cortafuegos. La interfaz del agente de cortafuegos en la que el tráfico s2c regresa al cortafuegos es la misma interfaz de la que el tráfico c2s sale hacia la cadena.

  Ambas interfaces de reenvío de cortafuegos deben estar en la misma zona.

El agente de paquetes de red no admite el tráfico SSH de multidifusión, difusión o descifrado.

Cómo funciona el agente de paquetes de red

El flujo de trabajo de alto nivel para conectar el cortafuegos a una cadena de dispositivos de seguridad de terceros es el siguiente:

1. Identifique el tráfico TLS no descifrado, TLS descifrado y no TLS (TCP y UDP) para reenviar.
2. Identifique la topología de la cadena de seguridad. Determine si los dispositivos de cada cadena de seguridad reenvían el tráfico de forma transparente (mediante puente) o si los dispositivos enrutan el tráfico según la información de la capa 3. El uso de múltiples cadenas de seguridad ayuda a equilibrar la carga del tráfico. Además, determine si desea omitir la cadena de seguridad (el tráfico pasa por el procesamiento normal en el cortafuegos y se reenvía o bloquea en consecuencia) o bloquear el tráfico si una cadena de seguridad falla en una verificación de estado.
3. Instale la licencia gratuita del agente de paquetes de red en los cortafuegos que reenviarán el tráfico a las cadenas de seguridad.
4. Identifique uno o más pares de interfaces de cortafuegos para reenviar el tráfico a una o más cadenas de seguridad y habilite el agente de paquetes de red en esas interfaces.
5. Configure, al menos, un perfil del agente de paquetes.
6. Configure, al menos, una política del agente de paquetes de red.

Para utilizar una cadena de dispositivos de seguridad de terceros para inspeccionar el tráfico, configure tres objetos en el cortafuegos:

- **Interfaces**: uno o más pares de interfaces de cortafuegos Ethernet de capa 3 para reenviar el tráfico desde el cortafuegos a la cadena de seguridad y recibir el tráfico procesado desde la cadena de seguridad. Configure los pares de interfaces del agente de paquetes de red antes de configurar perfiles y reglas de políticas porque necesita especificar los pares de interfaces en los perfiles.
- **Perfiles del agente de paquetes**: los perfiles controlan cómo reenviar el tráfico que define en una política a una cadena de seguridad. Cada regla de políticas del agente de paquetes de red tiene un perfil del agente de paquetes asociado. Los perfiles definen si la cadena de seguridad es una cadena de capa 3 enrutada o una cadena de puente transparente de capa 1, la dirección del tráfico a través de la cadena (unidireccional o bidireccional), las interfaces de cortafuegos dedicadas del agente de paquetes de red y cómo supervisar el estado de la conexión entre el cortafuegos y la cadena de seguridad. En el caso de varias cadenas de seguridad de capa 3 enrutadas, puede especificar el primer y el último dispositivo de cada cadena y un método de distribución de sesión (equilibrio de carga) para el tráfico asociado.
- **Reglas de políticas del agente de paquetes de red**: las reglas de políticas definen el tráfico de la aplicación para reenviar a cada cadena de seguridad o equilibrar la carga de varias cadenas enrutadas (capa 3). Las reglas de políticas definen el origen y el destino, los usuarios, las aplicaciones y los servicios del tráfico para reenviarlo a una cadena de seguridad. Las reglas de políticas también definen el tipo de tráfico para reenviar a una cadena de seguridad: puede seleccionar tráfico TLS descifrado, tráfico TLS no descifrado, tráfico no TLS o cualquier combinación de tipos de tráfico. También debe agregar un perfil del agente de paquetes en cada regla de políticas para especificar la cadena de seguridad a la que reenviar el tráfico (y todas las demás características del perfil).

  Utilice Policy Optimizer (Optimizador de políticas) para revisar y ajustar las reglas de políticas del agente de paquetes de red.

Para hacer coincidir el tráfico de aplicaciones con las reglas de políticas del agente de paquetes de red, este busca aplicaciones en la caché de ID de aplicación del cortafuegos. Si la aplicación no está en la caché de ID de la aplicación, el cortafuegos omite la cadena de seguridad y aplica al tráfico toda inspección de amenazas que esté configurada en la regla de permiso de la política de seguridad. Si la aplicación está en la caché de ID de la aplicación, el cortafuegos reenvía el tráfico a la cadena de seguridad de la manera que especifica la regla de políticas del agente de paquetes de red y su perfil asociado.

Para el tráfico TLS no descifrado y no TLS, el cortafuegos instala la aplicación en la caché de ID de la aplicación en la primera sesión, por lo que el cortafuegos trata al tráfico como se especifica en la política y el perfil del agente de paquetes de red.

Para el tráfico TLS descifrado, en la ***primera sesión*** de una aplicación, el agente de paquetes de red no sabe que la sesión se está descifrando y ve "ssl" como la aplicación. La aplicación específica subyacente aún no se conoce ni está instalada en la caché de ID de aplicación, por lo que la búsqueda del agente falla y el tráfico omite la cadena de seguridad. El tráfico aún está sujeto a ninguna inspección de amenazas configurada en la regla de permiso de la política de seguridad. Cuando el cortafuegos descifra el tráfico, aprende la aplicación específica y la instala en la caché de ID de la aplicación. Para la segunda y las siguientes sesiones descifradas de la misma aplicación, las búsquedas del agente de paquetes de red tienen éxito porque la aplicación específica ahora está en la caché de ID de aplicación, y el cortafuegos reenvía el tráfico a la cadena de seguridad como se esperaba.

Preparación para implementar el agente de paquetes de red

Realice las siguientes acciones para prepararse a fin de implementar el agente de paquetes de red:

1. Obtenga y active la licencia gratuita del agente de paquetes de red.
   1. Inicie sesión en el portal de atención al cliente.
   2. Seleccione **Assets (Activos)** > **Devices (Dispositivos)** en el panel de navegación de la izquierda.
   3. Encuentre el dispositivo en el que desea habilitar el agente de descifrado o el reflejo de puerto de descifrado, y seleccione **Actions (Acciones)** (el icono del lápiz).
   4. En Activate Licenses (Activar licencias), seleccione **Activate Feature License (Activar licencia de una función)**.
   5. Seleccione la licencia gratuita del **agente de paquetes de red**.
   6. Haga clic en **Agree and Submit (Aceptar y enviar)**.
2. Instale la licencia en el cortafuegos.
   1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)**.
   2. Haga clic en **Retrieve license keys from the license server (Recuperar claves de licencia del servidor de licencias)**.
   3. Compruebe que en la página **Device (Dispositivo)** > **Licenses (Licencias)** figure que la licencia del **agente de paquetes de red** ya está activa en el cortafuegos.
   4. Reinicie el cortafuegos (**Device [Dispositivo]** > **Setup [Configuración]** > **Operations [Operaciones]**). El agente de paquetes de red no está disponible para la configuración hasta que se reinicie el cortafuegos.

Puede enviar la licencia del agente de paquetes de red desde Panorama hasta los cortafuegos administrados. Debe reiniciar los cortafuegos para que la licencia surta efecto y actualizar la interfaz de usuario.

3. Habilite la caché de ID de aplicación para el agente de paquetes de red.
   1. La caché de ID de aplicación está inhabilitada por configuración predeterminada. Habilítela mediante el comando de la CLI del modo de configuración:

      ```
      admin@PA-3260# set deviceconfig setting application cache yes
      ```

   2. Habilite el cortafuegos para que use la caché de ID de aplicación a fin de identificar aplicaciones:

      ```
      admin@PA-3260# set deviceconfig setting application use-cache-
      for-identification yes
      ```

   Compruebe que en la configuración figure que la **caché de la aplicación** está establecida en **yes (sí)** y **Usar caché para id de aplicación** esté establecido en **sí (sí)**:

   ```
   admin@PA-3260> show running application setting
   Application setting:
   Application cache              : yes
   Supernode                      : yes
   Heuristics                     : yes
   Cache Threshold                : 1
   Bypass when exceeds queue limit: no
   Traceroute appid               : yes
   Traceroute TTL threshold       : 30
   Use cache for appid            : yes
   Use simple appsigs for ident   : yes
   Use AppID cache on SSL/SNI     : no
   Unknown capture                : on
   Max. unknown sessions          : 5000
   Current unknown sessions       : 33
   Application capture            : off
   ```

   ```
   Current APPID Signature
      Memory Usage                : 16768  KB (Actual 16461  KB)
         TCP 1 C2S                : regex 11898  states
         TCP 1 S2C                : regex 4549   states
         UDP 1 C2S                : regex 4263   states
         UDP 1 S2C                : regex 1605   states
   ```

4. Identifique el tráfico que desea reenviar a una o varias cadenas de seguridad.
5. Identifique la topología de cada cadena de seguridad y determine si desea utilizar el reenvío de puente transparente de capa 1 o el reenvío de capa 3 enrutado, que determina qué tipo de cadena de seguridad configura en el cortafuegos. Las consideraciones incluyen:
   - Ya sea que desee equilibrar la carga del tráfico a través de varias cadenas (use una cadena de seguridad de capa 3 enrutada para distribuir sesiones a través de varias cadenas mediante un enrutador, conmutador u otro dispositivo de enrutamiento), use una sola cadena o diferentes cadenas de seguridad para distintos tipos de tráfico. Para varias cadenas de puente transparente de capa 1, necesita un par de interfaces de cortafuegos dedicadas para cada cadena de seguridad porque la conexión de capa 1 no se enruta.

- Ya sea para utilizar el flujo de tráfico unidireccional o bidireccional a través de la cadena de seguridad.

6. Decida qué pares de interfaces de cortafuegos utilizar como interfaces de reenvío dedicadas del agente de paquetes de red.
   - Para las cadenas de puente transparente de capa 1, necesita un par de interfaces de cortafuegos dedicadas para cada cadena de seguridad de capa 1. Puede configurar reglas de directiva para enviar tráfico específico a diferentes cadenas de seguridad.
   - Para las cadenas de capa 3 enrutadas, un par dedicado de interfaces de cortafuegos puede equilibrar la carga del tráfico entre varias cadenas de seguridad de capa 3 a través de un conmutador, enrutador u otro dispositivo con capacidad de enrutamiento.
   - Para las cadenas de capa 3 enrutadas, puede utilizar varios pares de interfaces de cortafuegos dedicadas para enviar tráfico específico a diferentes cadenas de seguridad mediante distintas reglas de políticas.

Configuración de las cadenas de seguridad de puente transparente

Una cadena de seguridad de puente transparente de capa 1 reenvía el tráfico desde una interfaz de cortafuegos a través de una serie de dispositivos de inspección de datos y seguridad de procesamiento y, luego, regresa a través de una interfaz de cortafuegos diferente sin la necesidad de enrutar el tráfico.

Antes de configurar una cadena de seguridad de puente transparente de capa 1, realice los pasos para Preparación para implementar el agente de paquetes de red y asegúrese de que las conexiones físicas entre el cortafuegos y los dispositivos de la cadena de seguridad sean correctas.

Para distribuir sesiones a través de varias cadenas de seguridad de puente transparente, cree una cadena de seguridad de puente transparente de capa 1 en el cortafuegos para cada una de las cadenas de seguridad que desee utilizar para equilibrar la carga del tráfico. Cada cadena de seguridad de puente transparente en el cortafuegos requiere dos interfaces Ethernet de capa 3 dedicadas. Compruebe si tiene suficientes interfaces Ethernet libres para la topología que desea configurar.

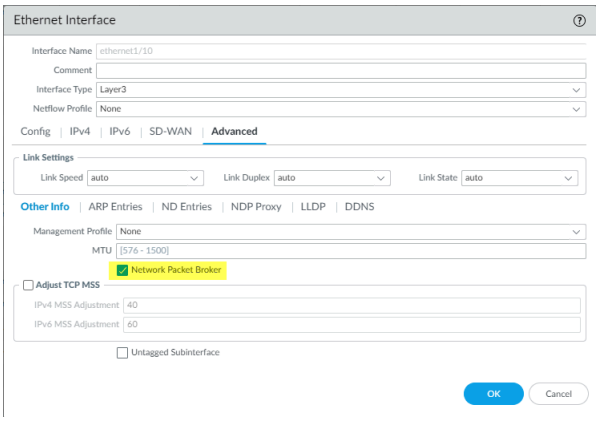
Las cadenas de seguridad de puente transparente de capa 1 no pueden conmutar por error a otra cadena de seguridad porque no se enrutan.

STEP 1 | Habilite dos interfaces Ethernet de capa 3 como interfaces de reenvío del agente de paquetes de red.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**.
2. Seleccione una interfaz Ethernet sin utilizar para usarla como una de las dos interfaces de reenvío del agente de paquetes de red.
3. Establezca el **Tipo de interfaz** en **Capa 3**.
4. En la pestaña **Configuración,** seleccione una zona a la que asignar la interfaz.

   Debe configurar ambas interfaces de cadena de seguridad en la misma zona.

5. En la pestaña **Configuración,** como práctica recomendada, use o cree un enrutador virtual dedicado para asignar la interfaz. El uso de un enrutador virtual dedicado garantiza que el tráfico de la interfaz del agente de paquetes de red permanezca separado del resto del tráfico.
6. Seleccione **Advanced (Avanzado)** y, a continuación, **Network Packet Broker (Agente de paquetes de red)** para habilitar la interfaz.



7. Haga clic en **OK (Aceptar)** para guardar la configuración de interfaz.
8. Repita este procedimiento en otra interfaz Ethernet sin utilizar para configurar la otra interfaz de reenvío del agente de paquetes de red.

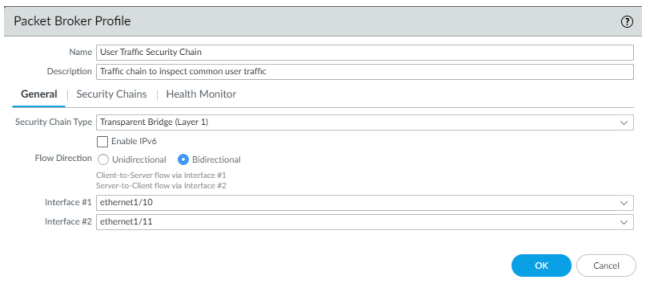
STEP 2 | Configure un perfil del agente de paquetes para controlar cómo se reenvía el tráfico a la cadena de seguridad de puente transparente de capa 1.

1. Seleccione **Objects (Objetos)** > **Packet Broker Profile (Perfil del agente de paquetes)** y **agregue** un nuevo perfil o modifique uno existente.
2. Asigne al perfil un **nombre** y una **descripción** para que pueda identificar con facilidad su propósito.
3. En la pestaña **General**, haga lo siguiente:
   - Seleccione **Transparent Bridge (Layer 1) Puente transparente (capa 1)** como el **tipo de cadena de seguridad**.
   - **Habilite IPv6** si el tráfico es IPv6.
   - Seleccione la **dirección de flujo**.

     La topología de red determina si se deben utilizar flujos unidireccionales o bidireccionales. El rendimiento es casi el mismo si utiliza cualquiera de los métodos.

     Para utilizar una interfaz de cortafuegos a fin de reenviar los flujos de sesión c2s y s2c a la cadena de seguridad y utilizar la otra interfaz de cortafuegos para recibir ambos flujos de sesión desde la cadena de seguridad, seleccione **Unidirectional (Unidireccional)**.

     A fin de usar la **Interface #1 (Interfaz nro. 1)** para reenviar el flujo c2s a la cadena de seguridad y recibir el flujo s2c de la cadena de seguridad, y usar la **Interface #2 (Interface nro.2)** para reenviar el flujo s2c a la cadena de seguridad y recibir el flujo c2s de la cadena de seguridad, seleccione **Bidirectional (Bidireccional)**.
   - Especifique el par de interfaz de reenvío del agente de paquetes de red en la **Interface #1 (Interfaz nro. 1)** y la **Interface #2 (Interfaz nro.2)**. Ambas interfaces ya deben estar habilitadas para que el agente de paquetes de red (consulte Preparación para implementar el agente de paquetes de red) esté disponible para su uso. Preste atención a la direccionalidad del flujo cuando configure qué interfaz es la **Interface #1 (Interfaz nro. 1)** y cuál la **Interface #2 (Interfaz nro.2)**.



4. La pestaña **Security Chains (Cadenas de seguridad** no se utiliza para puentes transparentes.
5. En la pestaña **Health Monitor (Supervisión de estado)**, haga lo siguiente:
   - Seleccione el tipo o los tipos de supervisión de estado que desea realizar para poder controlar lo que sucede si la cadena de seguridad experimenta un error. Puede seleccionar

una, dos o todas las opciones: **Path Monitoring (Supervisión de rutas)**, **HTTP Monitoring (Supervisión de HTTP)** o **HTTP Monitoring Latency (Latencia de supervisión de HTTP)**.

Path Monitoring (Supervisión de rutas): comprueba la conectividad del dispositivo mediante pings.

HTTP Monitoring (Supervisión de HTTP): comprueba la disponibilidad y el tiempo de respuesta del dispositivos.

HTTP Monitoring Latency (Latencia de supervisión de HTTP): comprueba la velocidad y la eficiencia de procesamiento del dispositivo. Al seleccionar esta opción, también se habilita de forma automática **HTTP Monitoring (Supervisión de HTTP)**.

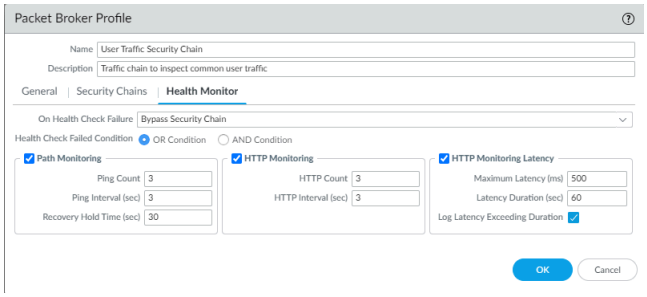
- Al habilitar uno o más tipos de supervisión de estado, se activan las opciones **Error al comprobar el estado**, que determinan cómo el cortafuegos gestiona el tráfico de la cadena de seguridad si se produce un error de estado de la cadena de seguridad. Las opciones son **Bypass Security Chain (Omitir cadena de seguridad)** y **Block Session (Bloquear sesión)**.

  Bypass Security Chain (Omitir cadena de seguridad): el cortafuegos reenvía el tráfico a su destino en lugar de a la cadena de seguridad y aplica los perfiles y las protecciones de seguridad configurados al tráfico.

  Block Session (Bloquear sesión): el cortafuegos bloquea la sesión.

  El método que seleccione depende de cómo desee tratar el tráfico si no puede ejecutarlo a través de la cadena de seguridad.

- Si selecciona más de una opción de comprobación de estado, seleccione si desea que el cortafuegos considere que la comprobación de estado ha fallado (**Condición de comprobación de estado fallida**) si alguna de las opciones de supervisión registra una condición fallida (**O condición**) o solo si todas las opciones de supervisión seleccionadas registran una condición fallida (**Y condición**). Por ejemplo, si habilita las tres opciones de comprobación de estado y una de las opciones registra una condición fallida, si ha seleccionado **O condición**, el cortafuegos considera que la conexión de la cadena de seguridad ha fallado y ejecuta la acción especificada en **Error al comprobar el estado**. Si seleccionó **Y condición**, el cortafuegos seguirá considerando que la conexión está en buen estado porque dos de las métricas de estado siguen siendo correctas.

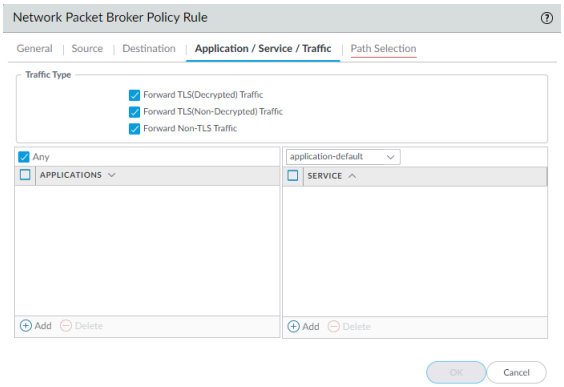


6. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Configure una política de agente de paquetes para definir el tráfico que se reenvía a la cadena de seguridad de puente transparente de capa 1.

1. Seleccione **Policies (Políticas)** > **Network Packet Broker (Agente de paquetes de red)** y **agregue** una nueva regla de políticas o modifique una existente.
2. En la pestaña **General (General)**, asigne a la regla de políticas un **Nombre** y una **Descripción** para que pueda identificar con facilidad su propósito, agregar un **comentario de auditoría** y aplicar etiquetas si las utiliza.
3. En la pestaña **Source (Origen)**, identifique las zonas de origen, las direcciones IP, los usuarios y los dispositivos del tráfico que desea que la regla reenvíe a la cadena de seguridad.
4. En la pestaña **Destination (Destino)**, identifique las zonas de destino, las direcciones IP y los dispositivos del tráfico que desea que la regla reenvíe a la cadena de seguridad.
5. En la pestaña **Application/Service/Traffic (Aplicación/Servicio/Tráfico)**, identifique las aplicaciones y los servicios que desea que la regla reenvíe a la cadena de seguridad. A menos que la regla controle las aplicaciones que espera que usen puertos no estándar, como las aplicaciones personalizadas internas, la práctica recomendada es establecer el **servicio** en **valor predeterminado de la aplicación** para que se bloqueen las aplicaciones que muestran un comportamiento evasivo mediante el uso de puertos no estándar.

   En **Traffic Type (Tipo de tráfico)**, seleccione todos los tipos de tráfico que desea que la regla reenvíe a la cadena de seguridad. **Forward TLS(Decrypted) Traffic (Reenviar tráfico TLS [descifrado])** es la selección predeterminada. Puede seleccionar cualquier combinación de **Forward TLS(Decrypted) Traffic (Reenviar tráfico TLS [descifrado])**, **Forward TLS (Non-Decrypted) (Reenviar TLS [No descifrado])**, y **Forward Non-TLS Traffic (Reenviar tráfico no TLS)** para reenviar a la cadena de seguridad.



6. En la pestaña **Path Selection (Selección de ruta)**, seleccione el perfil del agente de paquetes que creó en el Paso 2 o cree un nuevo perfil para controlar cómo enviar el tráfico que controla la regla de políticas a la cadena de seguridad.

STEP 4 | Repita el procedimiento del paso 1 al paso 3 para crear más cadenas de seguridad de puente transparente de capa 1.

Para cada cadena de seguridad de puente transparente de capa 1, haga lo siguiente:

- Las dos interfaces Ethernet utilizadas como interfaces de reenvío del agente de paquetes de red deben estar dedicadas a cada cadena de seguridad. Las interfaces Ethernet utilizadas

para una cadena de seguridad de puente transparente no se pueden utilizar para ningún otro propósito ni pueden transportar ningún otro tráfico.

- Cada par de interfaces de reenvío del agente de paquetes de red se conecta a una cadena de seguridad de puente transparente de capa 1.

Puede equilibrar la carga del tráfico mediante la creación de reglas de políticas del agente de paquetes de red que dividan el tráfico de manera relativamente equitativa entre las cadenas de seguridad de puente transparente. También puede usar reglas de políticas para dirigir tráfico y tipos de tráfico específicos a través de cadenas de seguridad específicas.

*Las cadenas de seguridad de puente transparente de capa 1 no pueden conmutar por error a otra cadena de seguridad porque no se enrutan. Utilice la pestaña **Health Monitor (Supervisión del estado)** del perfil del agente de paquetes para configurar cómo controlar el tráfico si se produce un error en una cadena de seguridad de puente transparente.*

Configuración de cadenas de seguridad de capa 3 enrutadas

Una cadena de seguridad de capa 3 enrutada reenvía el tráfico a una serie de dispositivos de inspección de datos y seguridad de procesamiento y, luego, de vuelta al cortafuegos mediante dos interfaces de reenvío dedicadas en el cortafuegos.

Antes de configurar una cadena de seguridad de capa 3 enrutada, realice los pasos para Preparación para implementar el agente de paquetes de red y asegúrese de que las conexiones físicas entre el cortafuegos y los dispositivos de la cadena de seguridad sean correctas. Compruebe que tenga suficientes interfaces Ethernet libres en el cortafuegos para la topología que desea configurar.

Cada cadena de seguridad de capa 3 enrutada que configure en el cortafuegos requiere dos interfaces Ethernet de capa 3 dedicadas, que pueden conectarse a una cadena de seguridad de capa 3 o distribuir sesiones (equilibrio de carga) en hasta 64 cadenas de seguridad de capa 3 con un enrutador, conmutador o dispositivo similar configurado de forma correcta entre el cortafuegos y las cadenas de seguridad.

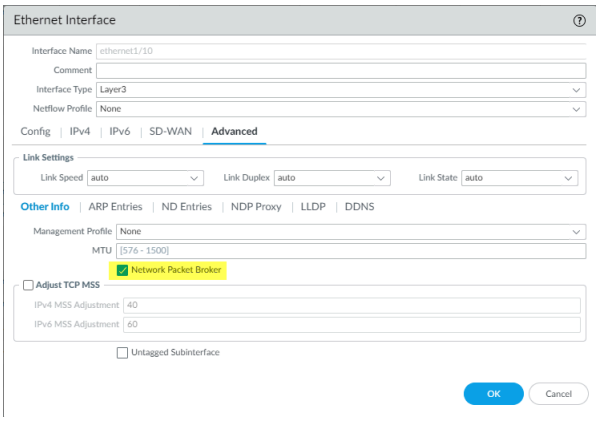
El agente de paquetes de red no puede reenviar el tráfico IPv6 en una cadena de seguridad de capa 3 enrutada. Para reenviar el tráfico IPv6, utilice una cadena de seguridad de puente transparente (capa 1).

STEP 1 | Habilite dos interfaces Ethernet de capa 3 como interfaces de reenvío del agente de paquetes de red.

1. Seleccione **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet**.
2. Seleccione una interfaz Ethernet sin utilizar para usarla como una de las dos interfaces de reenvío del agente de paquetes de red.
3. Establezca el **Tipo de interfaz** en **Capa 3**.
4. En la pestaña **Configuración,** seleccione una zona a la que asignar la interfaz.

   Debe configurar ambas interfaces de cadena de seguridad en la misma zona.

5. En la pestaña **Configuración,** como práctica recomendada, use o cree un enrutador virtual dedicado para asignar la interfaz. El uso de un enrutador virtual dedicado garantiza que el tráfico de la interfaz del agente de paquetes de red permanezca separado del resto del tráfico.
6. Seleccione **Advanced (Avanzado)** y, a continuación, **Network Packet Broker (Agente de paquetes de red)** para habilitar la interfaz.



7. Haga clic en **OK (Aceptar)** para guardar la configuración de interfaz.
8. Repita este procedimiento en otra interfaz Ethernet sin utilizar para configurar la otra interfaz de reenvío del agente de paquetes de red.

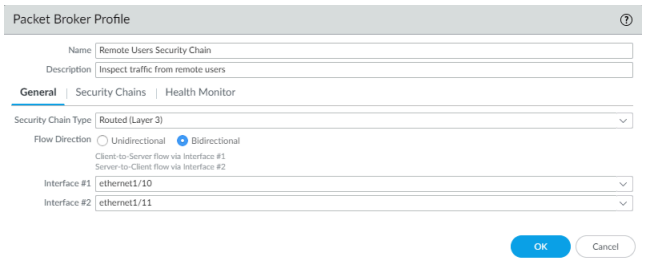
STEP 2 | Configure un perfil de agente de paquetes para controlar cómo reenviar el tráfico a la cadena de seguridad de capa 3 enrutada.

1. Seleccione **Objects (Objetos)** > **Packet Broker Profile (Perfil del agente de paquetes)** y **agregue** un nuevo perfil o modifique uno existente.
2. Asigne al perfil un **nombre** y una **descripción** para que pueda identificar con facilidad su propósito.
3. En la pestaña **General**, haga lo siguiente:
   - Seleccione **Routed (Layer 3) Enrutado (Capa 3)** como **tipo de cadena de seguridad**.
   - Seleccione la **dirección de flujo**.

     La topología de red determina si se deben utilizar flujos unidireccionales o bidireccionales. El rendimiento es casi el mismo si utiliza cualquiera de los métodos.

     Para utilizar una interfaz de cortafuegos a fin de reenviar los flujos de sesión c2s y s2c a la cadena de seguridad y utilizar la otra interfaz de cortafuegos para recibir ambos flujos de sesión desde la cadena de seguridad, seleccione **Unidirectional (Unidireccional)**.

     A fin de usar la **Interface #1 (Interfaz nro. 1)** para reenviar el flujo c2s a la cadena de seguridad y recibir el flujo s2c de la cadena de seguridad, y usar la **Interface #2 (Interface nro.2)** para reenviar el flujo s2c a la cadena de seguridad y recibir el flujo c2s de la cadena de seguridad, seleccione **Bidirectional (Bidireccional)**.
   - Especifique el par de interfaz de reenvío del agente de paquetes de red en la **Interface #1 (Interfaz nro. 1)** y la **Interface #2 (Interfaz nro.2)**. Ambas interfaces ya deben estar habilitadas para que el agente de paquetes de red (consulte el Paso 1) esté disponible para su uso. Preste atención a la direccionalidad del flujo cuando configure qué interfaz es la **Interface #1 (Interfaz nro. 1)** y cuál la **Interface #2 (Interfaz nro.2)**.

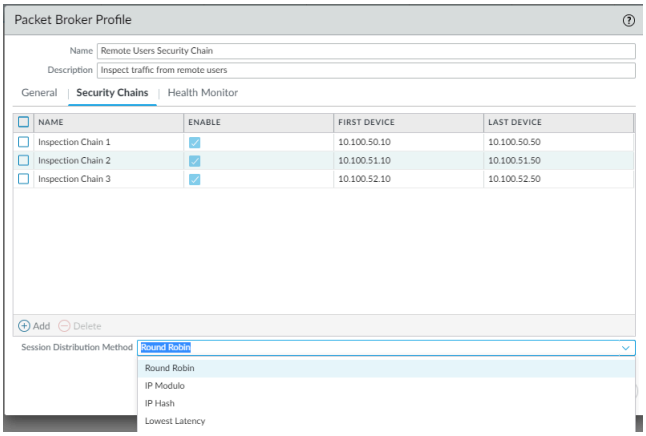


La distribución de sesiones (equilibrio de carga) solo aplica a las sesiones nuevas. El cortafuegos no reequilibra el tráfico en medio de una sesión. El cortafuegos solo distribuye sesiones a cadenas de seguridad cuyo estado es "arriba" (activo, saludable).

4. En la pestaña **Security Chains (Cadenas de seguridad)**, **agregue** las direcciones IP del primer y el último dispositivo de cada cadena de seguridad de capa 3 enrutada a la que desee conectarse. Debe especificar, al menos, una cadena de seguridad; de lo contrario, el cortafuegos no podrá enrutar el tráfico a una cadena ni podrá guardar el perfil.

   Si especifica varias cadenas de seguridad de capa 3 enrutadas, también deberá colocar un enrutador, conmutador o dispositivo similar configurado de forma correcta entre el cortafuegos y las cadenas de seguridad para realizar el enrutamiento adecuado. Además,

especifique el **método de distribución de sesiones** para equilibrar la carga del tráfico entre las cadenas de seguridad.



5. En la pestaña **Health Monitor (Supervisión de estado)**, haga lo siguiente:

   - Seleccione el tipo o los tipos de supervisión de estado que desea realizar para poder controlar lo que sucede si la cadena de seguridad experimenta un error.

     Puede seleccionar una, dos o todas las opciones: **Path Monitoring (Supervisión de rutas)**, **HTTP Monitoring (Supervisión de HTTP)** o **HTTP Monitoring Latency (Latencia de supervisión de HTTP)**.

     Path Monitoring (Supervisión de rutas): comprueba la conectividad del dispositivo mediante pings.

     HTTP Monitoring (Supervisión de HTTP): comprueba la disponibilidad y el tiempo de respuesta del dispositivos.

     HTTP Monitoring Latency (Latencia de supervisión de HTTP): comprueba la velocidad y la eficiencia de procesamiento del dispositivo. Al seleccionar esta opción, también se habilita de forma automática **HTTP Monitoring (Supervisión de HTTP)**.

   - Al habilitar uno o más tipos de supervisión de estado, se activan las opciones **Error al comprobar el estado**, que determinan cómo el cortafuegos gestiona el tráfico de la cadena de seguridad si se produce un error de estado de la cadena de seguridad.

     Si configura varias cadenas de seguridad en un conjunto de interfaces de agente de paquetes de red de capa 3 enrutadas, en un error de la cadena de seguridad, el tráfico conmuta por error a las cadenas de seguridad en buen estado restantes. Si no hay ninguna cadena de seguridad disponible para controlar el tráfico de conmutación por error, el

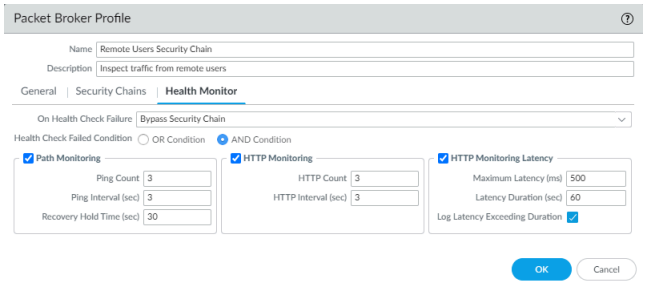
cortafuegos realiza la acción configurada **Error al comprobar el estado**. Las opciones son **Bypass Security Chain (Omitir cadena de seguridad)** y **Block Session (Bloquear sesión)**.

Bypass Security Chain (Omitir cadena de seguridad): el cortafuegos reenvía el tráfico a su destino en lugar de a la cadena de seguridad y aplica los perfiles y las protecciones de seguridad configurados al tráfico.

Block Session (Bloquear sesión): el cortafuegos bloquea la sesión.

El método que seleccione depende de cómo desee tratar el tráfico si no puede ejecutarlo a través de la cadena de seguridad.

- Si selecciona más de una opción de comprobación de estado, seleccione si desea que el cortafuegos considere que la comprobación de estado ha fallado (**Condición de comprobación de estado fallida**) si alguna de las opciones de supervisión registra una condición fallida (**O condición**) o solo si todas las opciones de supervisión seleccionadas registran una condición fallida (**Y condición**). Por ejemplo, si habilita las tres opciones de comprobación de estado y una de las opciones registra una condición fallida, si ha seleccionado **O condición**, el cortafuegos considera que la conexión de la cadena de seguridad ha fallado y ejecuta la acción especificada en **Error al comprobar el estado**. Si seleccionó **Y condición**, el cortafuegos seguirá considerando que la conexión está en buen estado porque dos de las métricas de estado siguen siendo correctas.



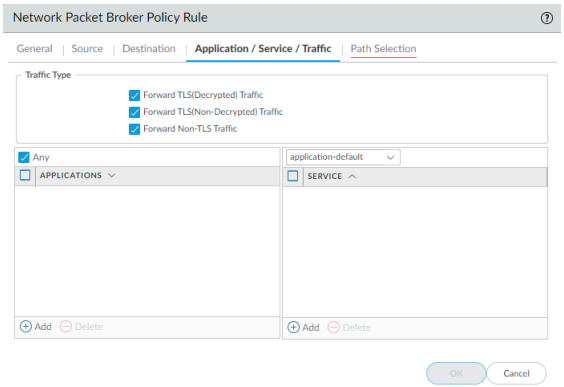
6. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Configure una política de agente de paquetes para definir el tráfico que se reenvía a la cadena de seguridad de capa 3 enrutada.

1. Seleccione **Policies (Políticas)** > **Network Packet Broker (Agente de paquetes de red)** y **agregue** una nueva regla de políticas o modifique una existente.
2. En la pestaña **General (General)**, asigne a la regla de políticas un **Nombre** y una **Descripción** para que pueda identificar con facilidad su propósito, agregar un **comentario de auditoría** y aplicar etiquetas si las utiliza.
3. En la pestaña **Source (Origen)**, identifique las zonas de origen, las direcciones IP, los usuarios y los dispositivos del tráfico que desea que la regla reenvíe a la cadena de seguridad.
4. En la pestaña **Destination (Destino)**, identifique las zonas de destino, las direcciones IP y los dispositivos del tráfico que desea que la regla reenvíe a la cadena de seguridad.
5. En la pestaña **Application/Service/Traffic (Aplicación/Servicio/Tráfico)**, identifique las aplicaciones y los servicios que desea que la regla reenvíe a la cadena de seguridad. A menos que la regla controle las aplicaciones que espera que usen puertos no estándar, como las aplicaciones personalizadas internas, la práctica recomendada es establecer el **servicio** en

valor predeterminado de la aplicación para que se bloqueen las aplicaciones que muestran un comportamiento evasivo mediante el uso de puertos no estándar.

En **Traffic Type (Tipo de tráfico)**, seleccione todos los tipos de tráfico que desea que la regla reenvíe a la cadena de seguridad. **Forward TLS(Decrypted) Traffic (Reenviar tráfico TLS [descifrado])** es la selección predeterminada. Puede seleccionar cualquier combinación de **Forward TLS(Decrypted) Traffic (Reenviar tráfico TLS [descifrado])**, **Forward TLS (Non-Decrypted) (Reenviar TLS [No descifrado])**, y **Forward Non-TLS Traffic (Reenviar tráfico no TLS)** para reenviar a la cadena de seguridad.



6. En la pestaña **Path Selection (Selección de ruta)**, seleccione el perfil del agente de paquetes que creó en el Paso 2 o cree un nuevo perfil para controlar cómo enviar el tráfico que controla la regla de políticas a la cadena de seguridad.

STEP 4 | Si desea crear cadenas de seguridad de capa 3 enrutadas separadas en las que se utilicen diferentes pares dedicados de interfaces de cortafuegos, repita el procedimiento del Paso 1 al Paso 3 a fin de crear más cadenas de seguridad del agente de paquetes de red. Las dos interfaces Ethernet de capa 3 utilizadas como interfaces de reenvío del agente de paquetes de red deben estar dedicadas a la cadena de seguridad y no se pueden utilizar para ningún otro propósito ni transportar ningún otro tráfico.

Compatibilidad con HA del agente de paquetes de red

Además de la supervisión del estado de la ruta de acceso y la latencia disponible en el perfil del agente de paquetes para protegerse de fallos de la cadena de seguridad, también puede configurar la alta disponibilidad (HA) en cortafuegos que tienen interfaces de reenvío del agente de paquetes de red para protegerse contra fallos del cortafuegos. La configuración de la supervisión de rutas y la HA brinda protección contra fallos de la cadena de seguridad y del cortafuegos.

El agente de paquetes de red admite pares de HA activo/pasivo. Los pares de HA activo/activo no se admiten porque las interfaces de reenvío del agente dedicadas deben especificarse en el perfil del agente de paquetes.

Después de una conmutación por error, el tráfico SSL descifrado se restablece porque el estado SSL no se sincroniza entre los nodos de HA. El tráfico de texto no cifrado se reanuda si la sesión se sincroniza de forma correcta y la secuencia TCP se vuelve a aprender como se debe.

Cambios en la interfaz de usuario para agente de paquetes de red

El agente de paquetes de red reemplaza la función del agente de descifrado incorporada en PAN-OS 8.1 y amplía sus capacidades a fin de incluir el reenvío de tráfico TLS y no TLS no descifrado, así como el tráfico TLS descifrado a una cadena de seguridad. Para admitir el agente de paquetes de red, la interfaz de usuario de PAN-OS 10.1 cuenta con los siguientes cambios:

- Una nueva política (**Policies [Políticas])** > **Network Packet Broker [Agente de paquetes de red]**) le permite configurar el tráfico específico para reenviar a la cadena de seguridad y adjuntar un perfil del agente de paquetes para controlar cómo se reenvía el tráfico especificado a la cadena de seguridad.

  El agente de descifrado utilizó las reglas de política de descifrado para reenviar solo el tráfico TLS descifrado a la cadena de seguridad. Las nuevas reglas de política del agente de paquetes de red le permiten seleccionar no solo el tráfico TLS descifrado, sino también el tráfico TLS cifrado y el tráfico no TLS.

- Un nuevo perfil **(Objects [Objetos]** > **Packet Broker Profile [Perfil del agente de paquetes]**reemplaza al **Objects (Objetos)** > **Decryption (Descifrado)** > **Decryption Broker Profile (Perfil del agente de descifrado)** y le permite configurar con exactitud cómo se reenvía el tráfico a la cadena de seguridad y se supervisa la ruta de acceso y el estado de la latencia. En la pestaña **General (General)**, los nombres de los campos en los que introduce el par dedicado de interfaz de reenvío del agente de paquetes de red del cortafuegos cambiaron de "Interfaz principal" e "Interfaz secundaria" a **Interface #1 (Interfaz nro. 1)** e **Interface #2 (Interface nro. 2)**, respectivamente.
- Cuando selecciona **Policies (Políticas)** > **Network Packet Broker (Agente de paquetes de red)**, puede seleccionar cualquiera de las opciones de Rule Usage (Uso de las reglas) en **Policy Optimizer (Optimizador de políticas)** para ver la información de uso de las políticas del agente de paquetes de red. Las estadísticas de **Rule Usage (Uso de red)** son útiles para evaluar si necesita mantener las reglas del agente de políticas de red sin utilizar o si puede eliminarlas y ajustar la base de reglas para reducir la superficie de ataque.
- Debido a que el agente de paquetes de red reemplazó al agente de descifrado, la política de descifrado ya no controla el tráfico de intermediación que se dirige a una cadena de seguridad. Por ese motivo, en la pestaña **Options (Opciones)**, la opción **Decrypt and Forward (Descifrar y reenviar)** ya no es una **acción** que la política puede realizar, y el campo **Forwarding Profile (Perfil de reenvío)** también se eliminó porque ahora solo los perfiles de descifrado son válidos en las políticas de descifrado.
- En **Network (Red)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, cuando establece el **Interface Type (Tipo de interfaz)** en Capa 3 y, a continuación, selecciona la pestaña **Advanced (Avanzado)**, el nombre de la casilla de verificación para habilitar la interfaz como interfaz de reenvío para el agente de paquetes de red cambió de "Decrypt Forward" (Descifrar reenvío) a **Network Packet Broker (Agente de paquetes de red)**.

- En **Device (Dispositivo)** > **Admin Roles (Funciones de administración)**, en la pestaña **Web UI (IU web)**, figuran dos cambios:
  - En **Policies (Políticas)**, ahora puede configurar los permisos de función de administración del **Network Packet Broker (Agente de paquetes de red)**.
  - En **Objects (Objetos)**, la opción **Decryption** > **Forwarding Profile (Perfil de reenvío de descifrado)** ya no está presente y se reemplaza por la opción **Packet Broker Profile (Perfil del agente de paquetes)** para los permisos de función de administración.
- En los cortafuegos, en **Monitor (Supervisar)** > **Manage Custom Reports (Administrar informes personalizados)**, cuando seleccione **Traffic Log (Log de tráfico)** de los logs detallados como la **Database (Base de datos)**, en la lista **Available Columns (Columnas disponibles)**, ahora puede seleccionar **Forwarded to Securty Chain (Reenviado a cadena de seguridad)**.

  En Panorama, para **Monitor (Supervisar)** > **Manage Custom Reports (Administrar informes personalizados)**, cuando seleccione **Panorama Traffic Log (Log de tráfico de Panorama)** de los logs detallados como la **Database (Base de datos)**, en la lista **Available Columns (Columnas disponibles)**, ahora puede seleccionar **Forwarded to Security Chain (Reenviado a la cadena de seguridad)**.
- En el log de tráfico, la columna "Decrypt Forward" (Descifrar reenvío) pasa a llamarse **Forwarded to Security Chain (Reenviado a cadena de seguridad)**. En la vista detallada del log de tráfico, en la sección **Flags (Indicadores)**, la casilla de verificación "Decrypt Forward" (Descifrar reenvío) pasa a llamarse **Forwarded to Security Chain (Reenviado a cadena de seguridad)**.
- La licencia gratuita para la función pasa de llamarse "Decryption Broker" (Agente descifrado) a **Packet Broker (Agente de paquetes)**. Si tiene la licencia gratuita del agente de descifrado en el cortafuegos, el nombre cambia de forma automática cuando cambia a la versión superior PAN-OS 10.1. El cambio solo afecta al nombre y no tiene ningún efecto en la función.

Limitaciones del agente de paquetes de red

La mayoría de las plataformas de Palo Alto Networks son compatibles con el agente de paquetes de red, pero algunas no lo son y unas pocas tienen ciertos límites:

- El soporte no está disponible en Prisma Access ni en NSX.
- AWS, Azure y GCP solo admiten cadenas de seguridad de capa 3 enrutadas.

El agente de paquetes de red tiene algunas limitaciones en Panorama para cortafuegos administrados y algunas limitaciones de uso. En Panorama, realice lo siguiente:

- Si envía licencias del agente de paquetes de red a cortafuegos administrados, debe reiniciar los cortafuegos para las licencias y los elementos de la interfaz de usuario asociados que se instalarán.
- No puede crear un perfil de agente de paquetes en un contexto **compartido** porque configura interfaces específicas en el perfil del agente de paquetes.
- Diferentes grupos de dispositivos no pueden compartir los mismos perfiles del agente de paquetes.
- Panorama no puede enviar una configuración del agente de paquetes de red (reglas y perfiles de políticas del agente de paquetes de red) a un grupo de dispositivos que contiene cortafuegos que ejecutan una versión de PAN-OS anterior a la 10.1.

  Si desea utilizar el agente de paquetes de red en un grupo de dispositivos que contiene cortafuegos en varias versiones de PAN-OS y algunos de esos cortafuegos ejecutan una versión de PAN-OS anterior a la 10.1, debe actualizar los cortafuegos anteriores a la 10.1 a PAN-OS. 10.1 o eliminar los cortafuegos anteriores a 10.1 del grupo de dispositivos antes de enviar la configuración del agente de paquetes de red.

  Puede utilizar Panorama para enviar un perfil de agente de paquetes adjunto a una regla de políticas de descifrado a cortafuegos anteriores a la 10.1 que tengan instaladas licencias del agente de descifrado. La acción para la regla (pestaña Options [Opciones]) debe ser Decrypt and Forward (Descifrar y reenviar) y debe adjuntar el perfil del agente de paquetes a la regla (configuración del Decryption Profile [Perfil de descifrado] en la pestaña Options [Opciones]). Los cortafuegos anteriores a la versión 10.1 utilizan el perfil del agente de paquetes como perfil de reenvío de descifrado para el agente de descifrado. La regla de políticas de descifrado determina el tráfico que el cortafuegos aplica el perfil.

  El tráfico que controla la regla de políticas de descifrado debe ser tráfico SSL descifrado (el agente de descifrado no admite tráfico SSL cifrado ni tráfico de texto no cifrado).
- Cuando actualiza de PAN-OS 10.0 a PAN-OS 10.1, solo las reglas de política de descifrado locales que se utilizan para el agente de descifrado se migran a las reglas del agente de paquetes de red. Las reglas de políticas del agente de descifrado que se enviaron desde Panorama hasta los cortafuegos se migran de forma automática en Panorama, pero no en el cortafuegos. Las reglas de políticas del agente de descifrado configuradas a nivel local en un cortafuegos se migran a las reglas del agente de paquetes de red solo en ese cortafuegos. En el caso de las reglas configuradas en Panorama, Panorama debe realizar otro envío de compilación al cortafuegos para sincronizar las reglas del agente de descifrado que se migraron a las reglas del agente de paquetes de red en Panorama.

- Cuando cambia de PAN-OS 10.1 a PAN-OS 10.0, las reglas del agente de paquetes de red se eliminan de forma automática.

El agente de paquetes de red también tiene algunas limitaciones de uso:

- Si el cortafuegos del agente de paquetes de red también realiza la traducción de la dirección de red de origen (SNAT), y el tráfico es de texto no cifrado, el cortafuegos realiza la NAT en el tráfico y lo reenvía a la cadena de seguridad. Los dispositivos de la cadena de seguridad solo ven las direcciones NAT, no las direcciones de origen originales:

  1. El cortafuegos realiza la NAT en el tráfico del cliente.
  2. El cortafuegos reenvía el tráfico a la cadena de seguridad y todo enrutamiento debe basarse en la dirección NAT.
  3. Debido a que la dirección de origen en el paquete ahora es la dirección NAT, los dispositivos de la cadena de seguridad solo ven la dirección NAT. No ven la dirección de origen del cliente real.
  4. Cuando la cadena de seguridad devuelve el tráfico al cortafuegos, el resultado es que el cortafuegos no sabe quién es el usuario.

  Puede averiguar quién era el usuario de origen de una sesión al comprobar los logs de tráfico de esa sesión y al correlacionar el paquete con esos logs. Los log de tráfico incluyen tanto la dirección de origen original, a partir de la cual puede determinar el usuario de origen, como la dirección SNAT.

  Puede evitar esta situación al realizar la NAT en un dispositivo que no sea el cortafuegos.

- No se admiten el tráfico de difusión, multidifusión y SSH descifrado.
- La autenticación de cliente no es compatible con la inspección de SSL entrante cuando se utilizan certificados RSA.
- En el modo puente transparente de capa 1, si falla una cadena de seguridad, no hay conmutación por error porque cuando se usan conexiones de puente transparente, y cada par de interfaces de cortafuegos dedicadas del agente de paquetes de red se conecta a una sola cadena de seguridad. (No puede enrutar el tráfico de la capa 1, solo puede reenviarlo al siguiente dispositivo conectado).
- Puede reenviar tráfico IPv6 solo en el modo puente transparente de capa 1. No puede reenviar el tráfico IPv6 en el modo enrutado (capa 3).
- No puede utilizar interfaces de bucle invertido o de túnel como interfaces del agente de paquetes de red.
- Las interfaces de Network Packet Broker no pueden utilizar protocolos de enrutamiento dinámico.
- Ambas interfaces deben estar en la misma zona.
- Los dispositivos de una cadena de seguridad no pueden modificar la dirección IP de origen, la dirección IP de destino, el puerto de origen, el puerto de destino ni el protocolo de la sesión original porque el cortafuegos no podría hacer coincidir la sesión modificada con la sesión original y, por lo tanto, eliminaría el tráfico.
- La alta disponibilidad para el agente de paquetes de red solo es compatible con los pares de cortafuegos de HA activos/pasivos. La alta disponibilidad para el agente de paquetes de red no es compatible con los pares de cortafuegos activos/activos.

- La alta disponibilidad no es compatible con el tráfico SSL. Las sesiones SSL se restablecen en las conmutaciones por error.
- Cuando actualiza de PAN-OS 10.0 a PAN-OS 10.1, las reglas de políticas de descifrado locales que se utilizan para el agente de descifrado se migran a las reglas del agente de paquetes de red.
- Cuando cambia de PAN-OS 10.1 a PAN-OS 10.0, las reglas del agente de paquetes de red se eliminan de forma automática.

Solución de problemas del agente de paquetes de red

Si tiene problemas para configurar al agente de paquetes de red, compruebe los siguientes elementos:

- Configuración del cortafuegos:
  - Compruebe la ruta del siguiente salto en los pares de interfaz de reenvío para asegurarse de que especifique la interfaz del dispositivo correcta.
  - Las direcciones IP de los dispositivos de la cadena y las interfaces de cortafuegos, y asegúrese de que se introduzcan de forma correcta en el perfil del agente de paquetes.
  - Si HA está habilitado, compruebe que las interfaces correctas estén especificadas en el perfil.
  - Compruebe la dirección del flujo del tráfico a través de la cadena.
  - Asegúrese de que en el perfil se indique el tipo de cadena de seguridad adecuado.
- Para la configuración de la cadena de seguridad; compruebe lo siguiente:
  - Direcciones IP, direcciones de siguiente salto y puertas de enlace predeterminadas para cada dispositivo de la cadena de seguridad.
  - La configuración de cualquier dispositivo entre el cortafuegos y la cadena de seguridad (enrutadores, conmutadores, etc.) para la configuración incorrecta del direccionamiento IP, el siguiente salto y la puerta de enlace predeterminada.
  - La ruta entre el firewall y la cadena.
- Compruebe los log de tráfico del cortafuegos para validar que ve el indicador "Forwarded" (Reenviado) establecido como se esperaba para el tráfico intermediado.
- Los comandos de la CLI útiles incluyen:
  - `show rulebase network-packet-broker`
  - `show running network-packet-broker status`
  - `show running network-packet-broker statistics`
  - `show running application-cache all`
  - `show running application setting`: confirme que la caché del ID de aplicación esté habilitada y que se use para el ID de aplicación, compruebe la configuración del umbral de caché, etc.

