Configuración de PBR basado en aplicaciones FTD para Umbrella SIG

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Overview

- Limitaciones

PBR basada en aplicaciones

Verificación

Introducción

Este documento describe cómo configurar el routing basado en políticas (PBR) basado en aplicaciones de Firewall Threat Defence (FTD) para Umbrella SIG.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al panel de Umbrella
- Acceso de administrador al FMC que ejecuta 7.1.0+ para implementar la configuración en el FTD versión 7.1.0+. PBR basado en aplicaciones solo es compatible con la versión 7.1.0 y posteriores
- (Preferido) Conocimientos sobre la configuración de FMC/FTD y Umbrella SIG
- (Opcional, pero muy recomendado): Umbrella Root Certificate instalado, es utilizado por SIG cuando el tráfico es proxy o bloqueado. Para obtener más información sobre la instalación del certificado raíz, consulte la documentación de Umbrella.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella Secure Internet Gateway (SIG).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

La información de este documento pretende cubrir los pasos de configuración sobre cómo implementar PBR basado en aplicaciones en el FTD al establecer un túnel SIG IPsec VTI a Umbrella, para que pueda excluir o incluir tráfico en una VPN basada en aplicaciones que utilizan PBR.

El ejemplo de configuración descrito en este artículo se centra en cómo excluir ciertas aplicaciones de la VPN IPsec mientras se envía todo lo demás a través de la VPN.

Puede encontrar información completa sobre PBR en FMC en la documentación de Cisco.

Limitaciones

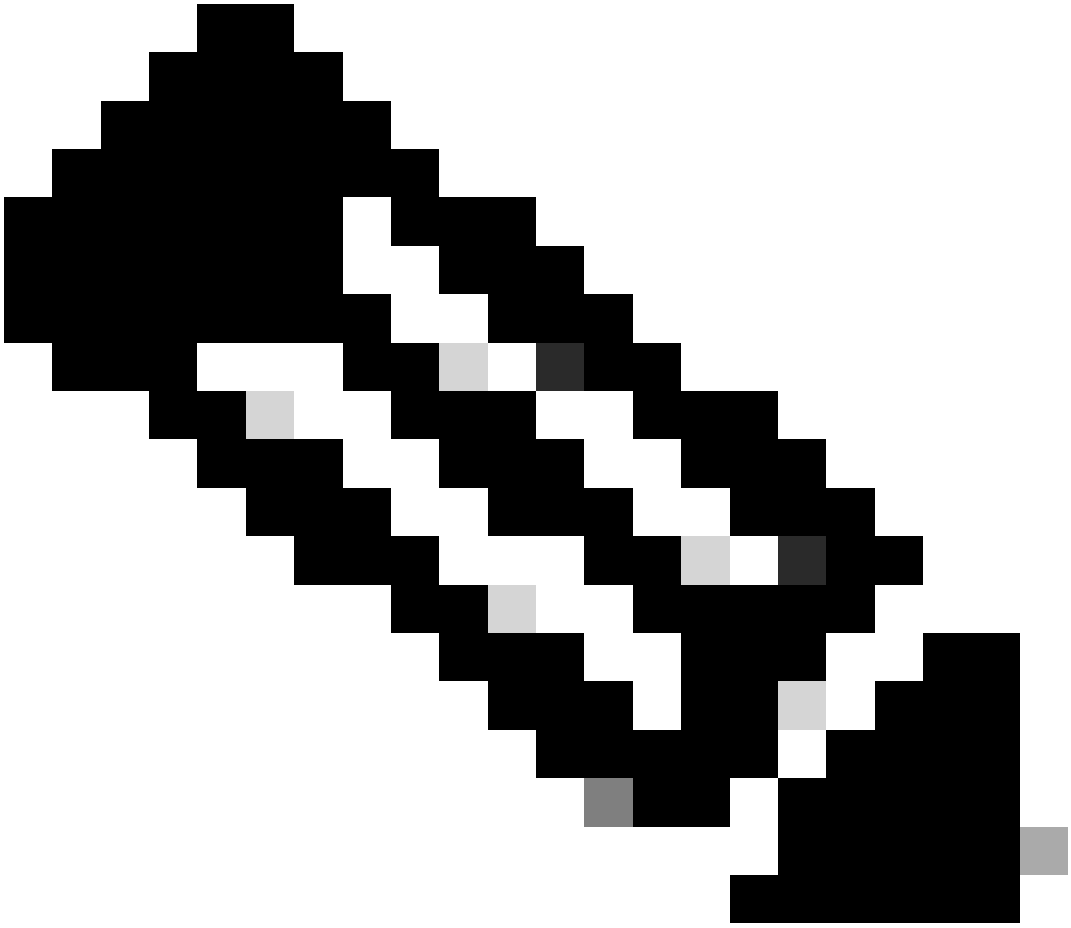
- No puede tener una aplicación y una dirección de destino definidas en una ACE.
- Al definir la ACL para los criterios de coincidencia de políticas, puede seleccionar varias aplicaciones de una lista de aplicaciones predefinidas para formar una entrada de control de acceso (ACE).
  Actualmente, no puede agregar ni modificar la lista de aplicaciones predefinidas.
- Para aquellas aplicaciones no incluidas en la lista de aplicaciones predefinidas en el FMC o cualquier comportamiento inesperado con una aplicación, se pueden utilizar IP en lugar de aplicaciones en el PBR.
- Para obtener una lista de las limitaciones completas, consulte la documentación del PBR.

PBR basada en aplicaciones

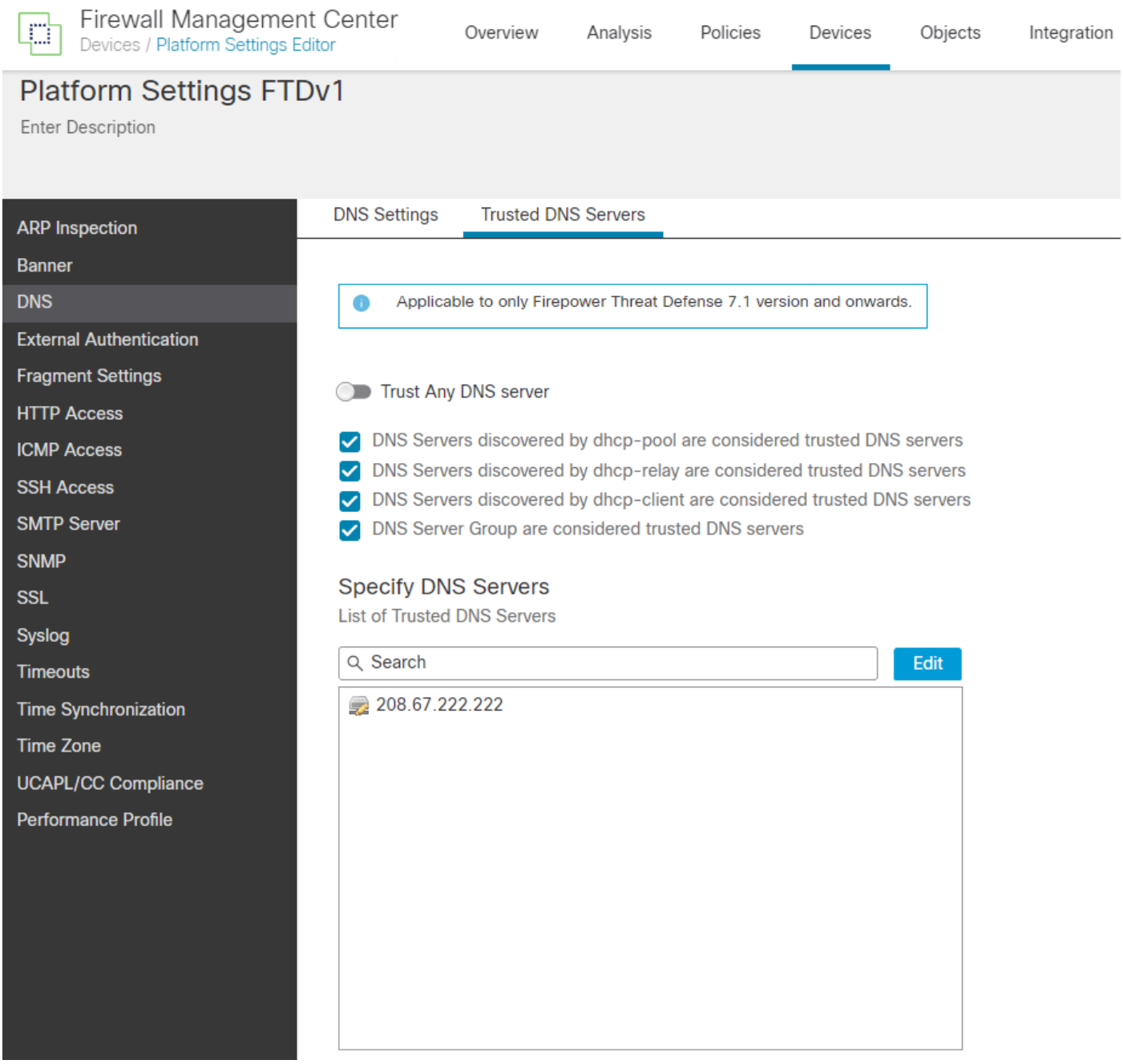
1. Comience configurando el túnel IPsec en el FMC, así como en el panel de Umbrella. Las instrucciones sobre cómo realizar esta configuración se pueden encontrar en la documentación de Umbrella.

2. Asegúrese de que el servidor DNS que utiliza el dispositivo del usuario final detrás del FTD aparezca como servidor DNS de confianza en Dispositivos > Configuración de la plataforma > DNS > Servidores DNS de confianza.

Si los dispositivos utilizan un servidor DNS que no aparece en la lista, la indagación de DNS puede fallar y, por lo tanto, el PBR basado en aplicaciones no puede funcionar. Opcionalmente (pero no se recomienda por motivos de seguridad), puede activar Trust Any DNS server para que sea necesario agregar los servidores DNS.



Nota: Si los VA se utilizan como resolvers DNS internos, deben agregarse como servidores DNS de confianza.



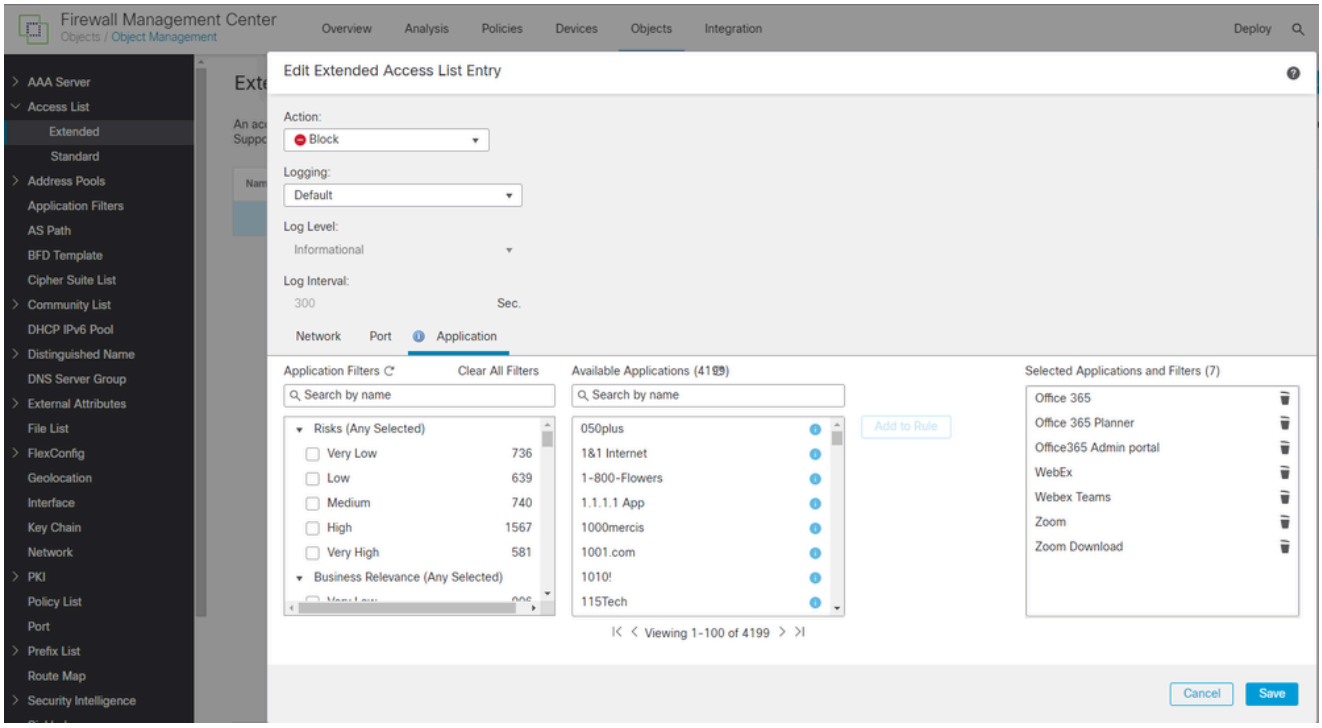
15669097907860

3. Cree una ACL extendida que pueda ser utilizada por el FTD para el proceso PBR para decidir si el tráfico se envía a Umbrella para SIG o si se excluye del IPSec y no se envía a Umbrella en absoluto.

- Una ACE de negación en la ACL significa que el tráfico se excluye de SIG.
- Una ACE de permiso en la ACL significa que el tráfico se envía a través del IPSec y puede aplicar una política SIG (CDFW, SWG, etc.).

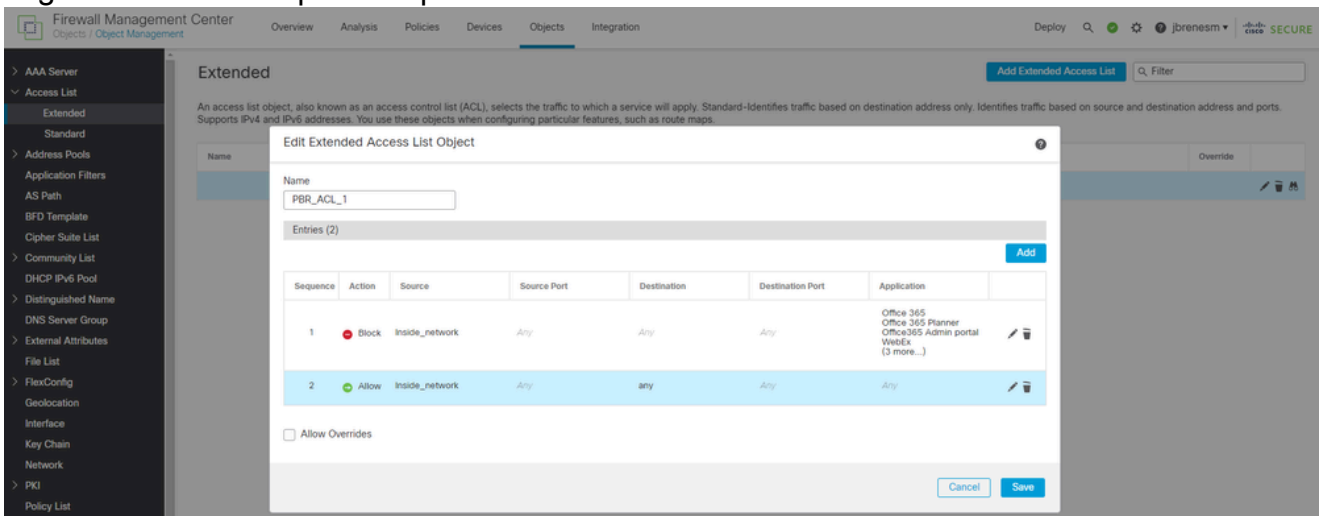
En este ejemplo se excluyen las aplicaciones "Office365", "Zoom" y "Cisco Webex" con una ACE de denegación. El resto del tráfico se envía a Umbrella para una inspección adicional.

1. Vaya a Object > Object Management > Access List > Extended.
2. Defina la red y los puertos de origen como lo haría normalmente y, a continuación, agregue las aplicaciones que participarán en el PBR.



15669947000852

La primera ACE puede "denegar" para las aplicaciones mencionadas anteriormente y la segunda ACE es un permiso para enviar el resto del tráfico a través de IPsec.

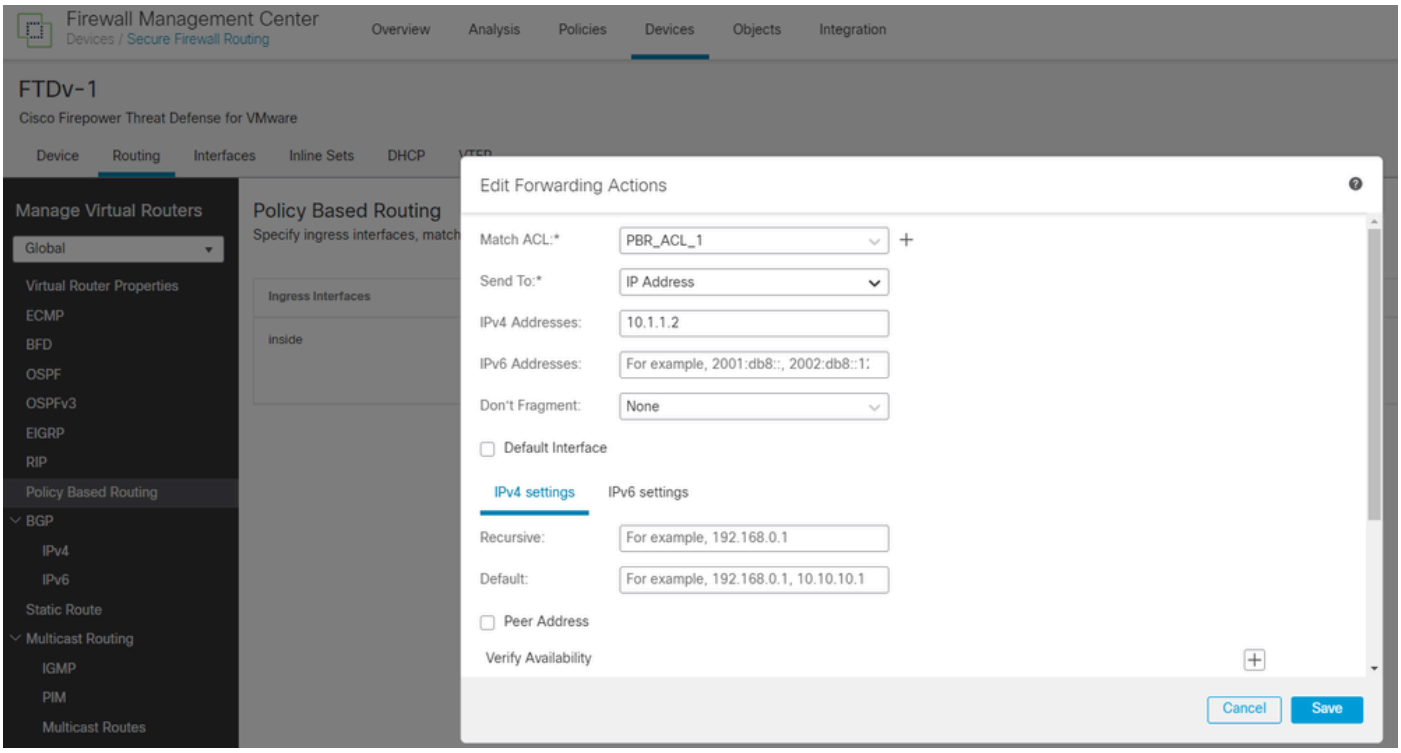


15670006987156

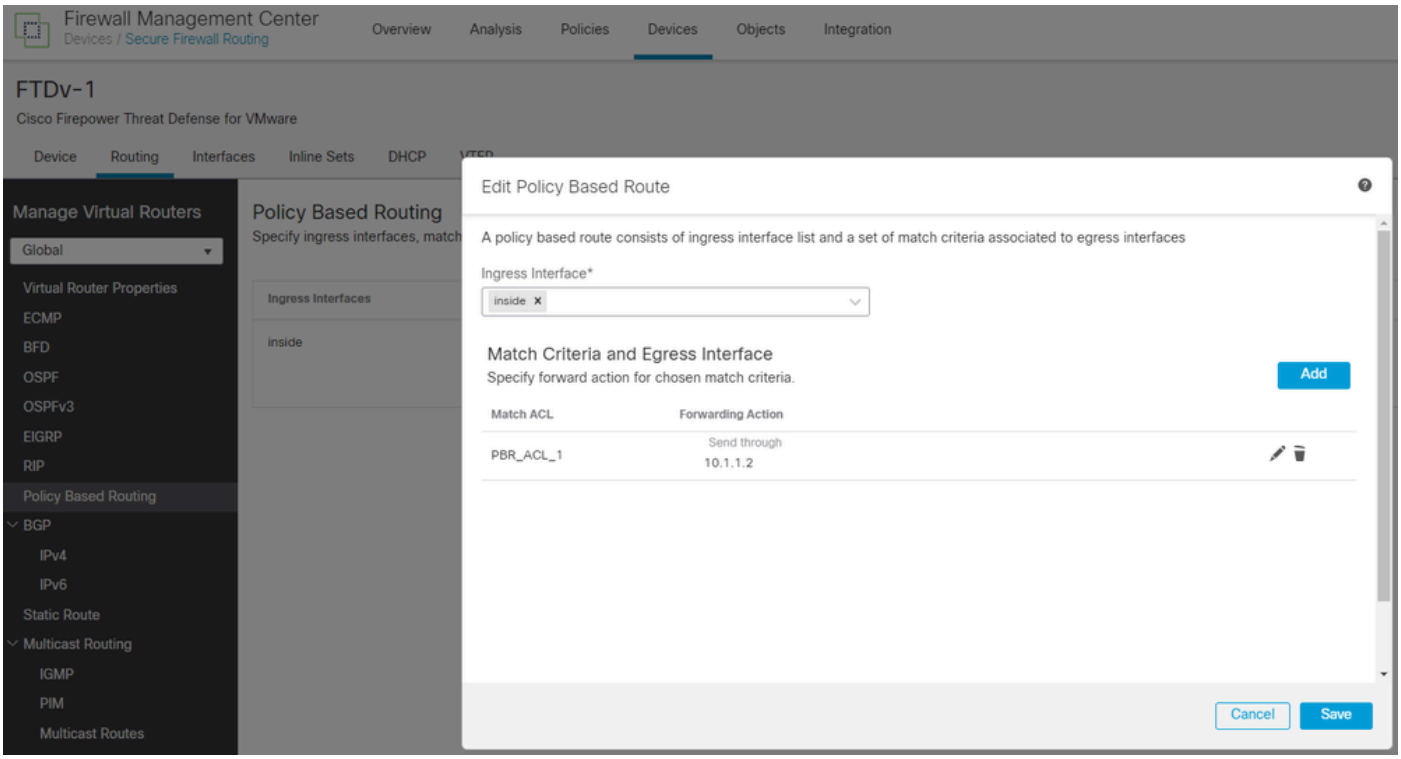
4. Cree el PBR en Devices > Device Management > [select the FTD Device] > Routing > Policy Based Routing.

- Interfaz de entrada: La interfaz de donde proviene el tráfico local.
- ACL coincidente: ACL ampliada creada en el paso anterior, ACL "PBR_ACL_1".
- Enviar a: IP Address
- Direcciones IPv4: Next-hop cuando PBR encuentra una sentencia permit, por lo que el tráfico se rutea a la IP que agregue aquí. En este ejemplo, se trata de IPsec de Umbrella. Si la IP de su VPN VTI es 10.1.1.1, entonces la IP IPsec de Umbrella sería cualquier cosa

dentro de la misma red (10.1.1.2 por ejemplo).



15670209158036



15670247521556

5. Implemente los cambios en el CSP.

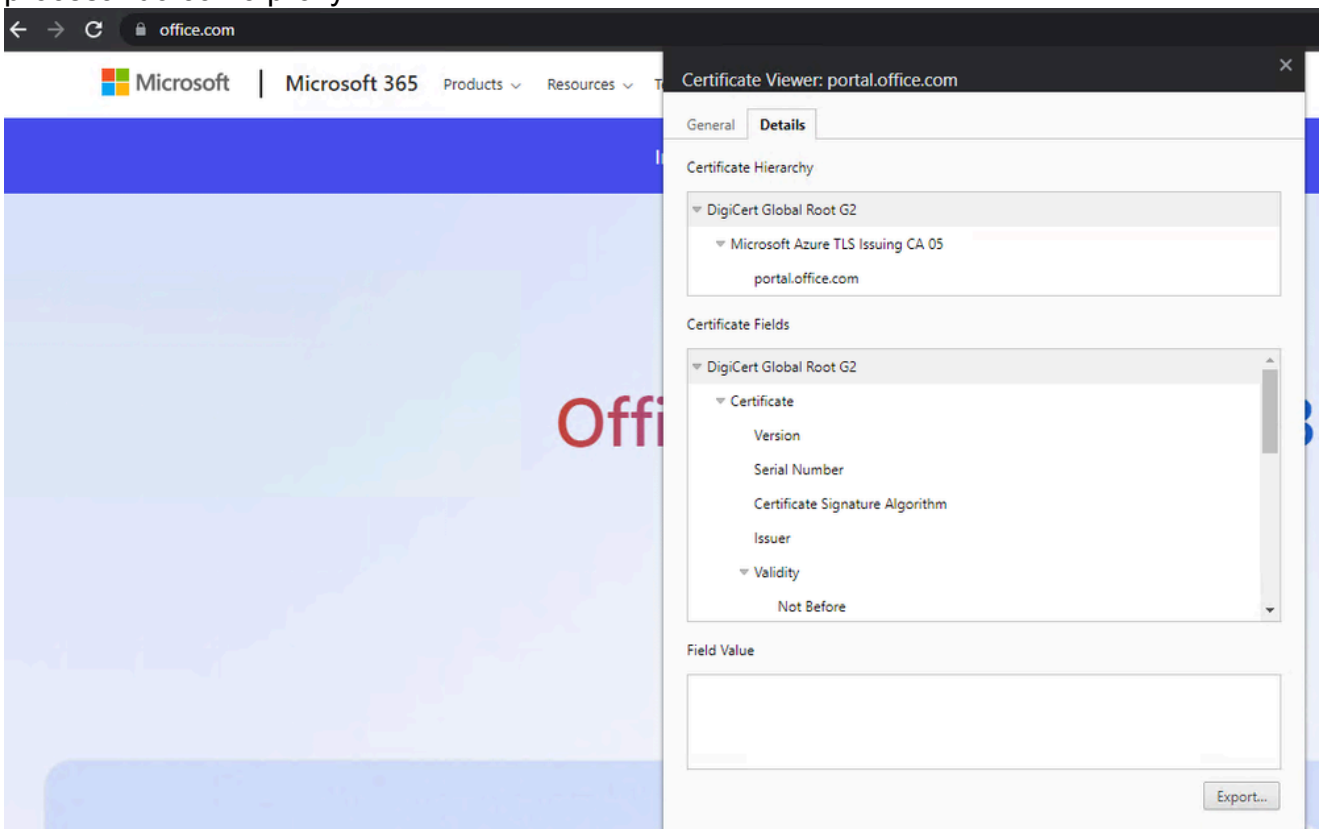
Verificación

En el equipo de prueba situado detrás del FTD, compruebe:

- El tráfico de la PC se envía realmente a Umbrella a través de IPsec.
  Vaya a: https://policy-debug.checkumbrella.com/

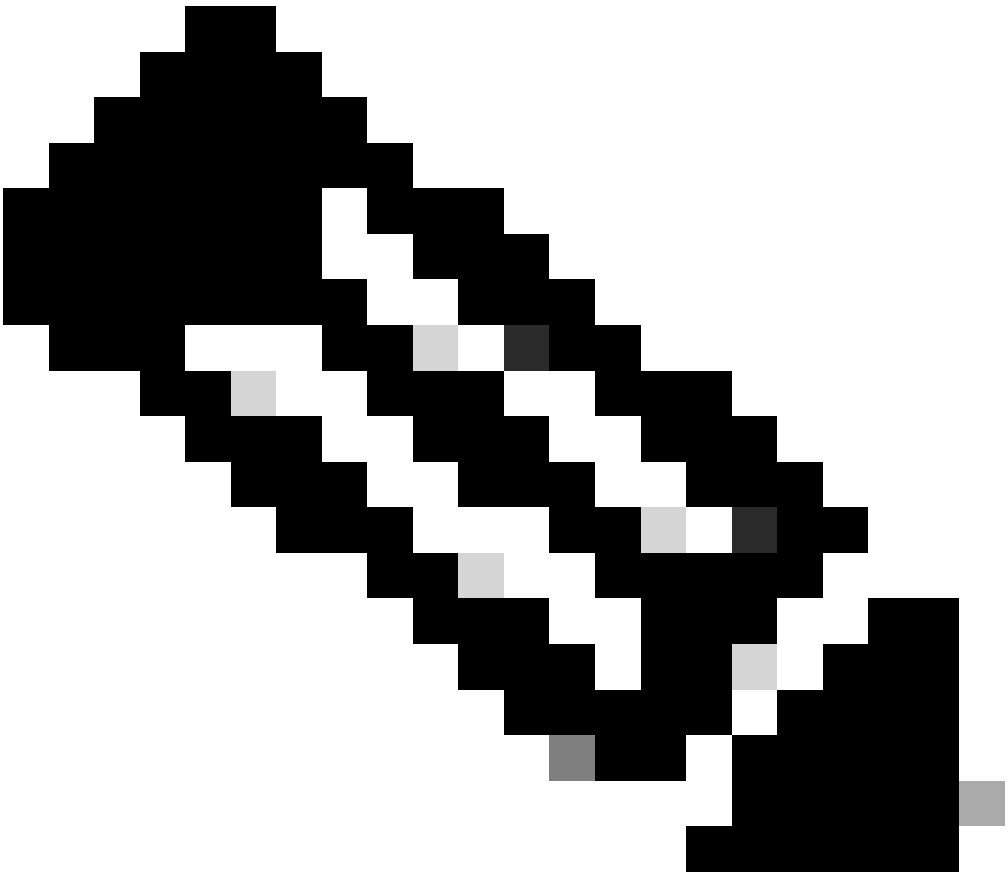
15670737148948

- Intente ir a cualquiera de los sitios excluidos en la configuración PBR/ACL y asegúrese de que la CA raíz de paraguas no esté presente, lo que significa que la conexión no se está procesando como proxy:

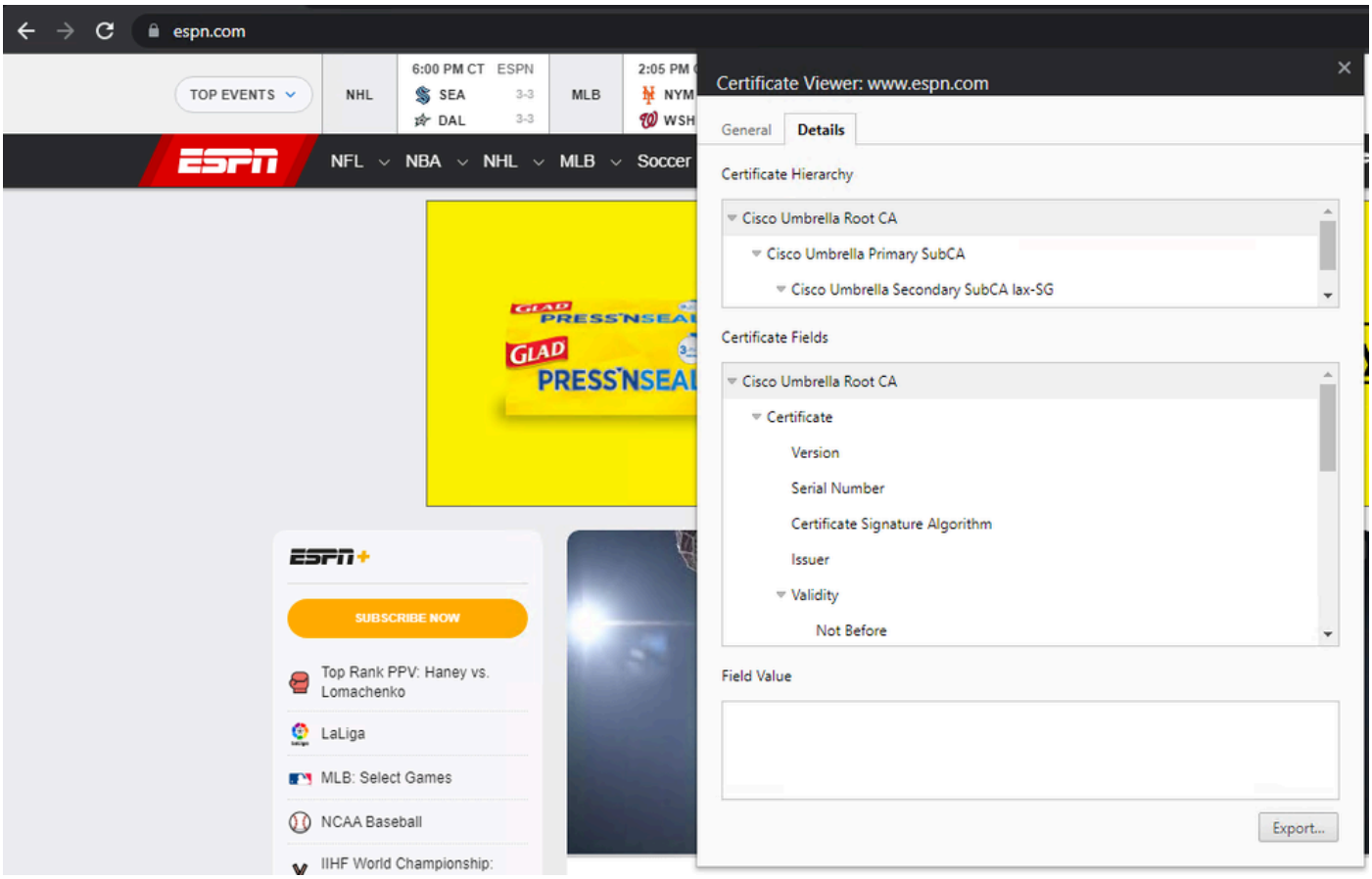


15670820980756

- Intente visitar cualquier otro sitio que no esté basado en las aplicaciones excluidas de PBR y asegúrese de que Umbrella esté realmente realizando proxy de la conexión:



Nota: Para evitar problemas con una página de advertencia en la que no se confía, asegúrese de que el certificado de CA raíz de Umbrella esté instalado.



- En la CLI del FTD, puede ejecutar algunos comandos para confirmar que la configuración se ha insertado y funciona correctamente:
  - `show run route-map` (verifica la configuración PBR):

```
ftd# sh run route-map
!
route-map FMC_GENERATED_PBR_1682004086289 permit 5
 match ip address PBR_ACL_1
 set ip next-hop 10.1.1.2

!
ftd#
```

15670322054036

  - `show run interface gigabitEthernet 0/1` (verifica que PBR se aplique a la interfaz adecuada)

```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (confirma los dominios agregados a la ACL para su exclusión)

```
ftd# sh run access-list PBR_ACL_1
access-list PBR_ACL_1 extended deny ip object Inside_network object-group-network-service FMC_NSG_17179869596
access-list PBR_ACL_1 extended permit ip object Inside_network any
ftd# sh object-group id FMC_NSG_17179869596
object-group network-service FMC_NSG_17179869596 (id=f1000001)
 network-service-member "Office 365" dynamic
  description Traffic generated by MS Office 365 applications and web services.
  app-id 2812
  domain nexus.officeapps.live.com (bid=-1815422039) ip (hitcnt=0)
  domain officehome.msocdn.com (bid=-1815266895) ip (hitcnt=0)
  domain scuofficehome.msocdn.com (bid=-1815215737) ip (hitcnt=0)
  domain eusofficehome.msocdn.com (bid=-1814954697) ip (hitcnt=0)
  domain seaofficehome.msocdn.com (bid=-1814948459) ip (hitcnt=0)
  domain msauth.net (bid=-1814770899) ip (hitcnt=0)
  domain msauthimages.net (bid=-1814643885) ip (hitcnt=0)
  domain msftauth.net (bid=-1814478573) ip (hitcnt=0)
  domain msftauthimages.net (bid=-1814363583) ip (hitcnt=0)
  domain officecdn.microsoft.com.edgesuite.net (bid=-1814169495) ip (hitcnt=0)
  domain staffhub.ms (bid=-1814084129) ip (hitcnt=0)
  domain mem.gfx.ms (bid=-1813977425) ip (hitcnt=0)
  domain assets.onestore.ms (bid=-1813901907) ip (hitcnt=0)
  domain o365weve.com (bid=-1813725851) ip (hitcnt=0)
  domain msappproxy.net (bid=-1813517013) ip (hitcnt=0)
  domain officeppe.com (bid=-1813427701) ip (hitcnt=0)
  domain Portal.Office.com (bid=-1813355559) ip (hitcnt=0)
  domain Home.Office.com (bid=-1813195231) ip (hitcnt=0)
  domain office365.com (bid=-1813005001) ip (hitcnt=0)
  domain office.com (bid=-1812953305) ip (hitcnt=0)
  domain office.net (bid=-1812729659) ip (hitcnt=0)
  domain microsoftonline.com (bid=-1812611427) ip (hitcnt=0)
  domain onmicrosoft.com (bid=-1812561405) ip (hitcnt=0)
  domain glbdns.microsoft.com (bid=-1812432381) ip (hitcnt=0)
  domain login.windows.net (bid=-1812242319) ip (hitcnt=0)
  domain login.microsoftonline.com (bid=-1812155687) ip (hitcnt=0)
  domain office365servicehealthcommunications.cloudapp.net (bid=-1812019313) ip (hitcnt=0)
  domain prod.msocdn.com (bid=-1811890529) ip (hitcnt=0)
  domain office.microsoft.com (bid=-1811800355) ip (hitcnt=0)
```

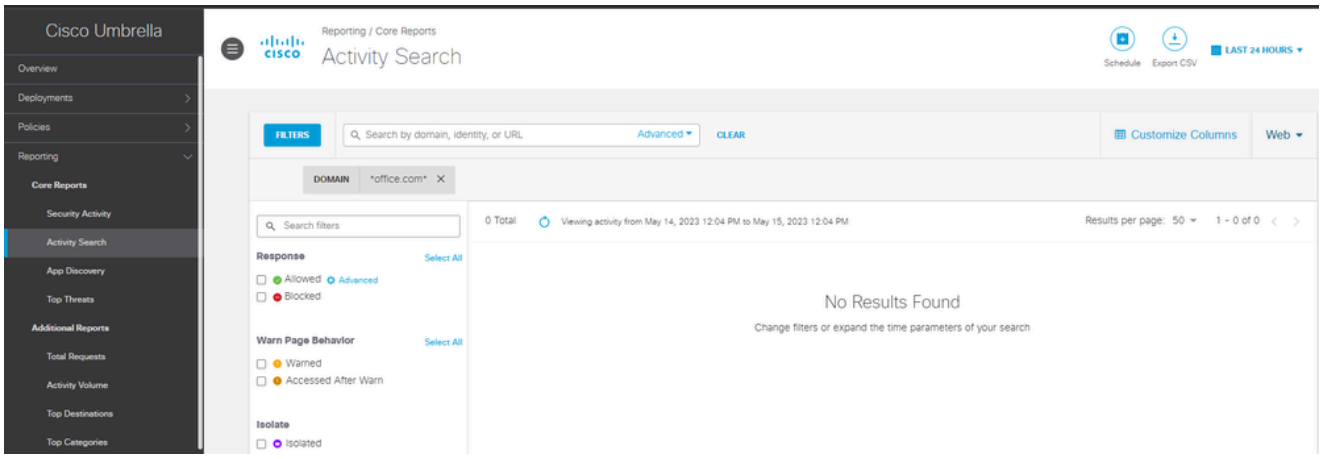
15670420887316

```
ftd# sh object-group id FMC_NSG_17179869596 | i office.com
  domain office.com (bid=-1812953305) ip (hitcnt=8)
  domain tasks.office.com (bid=-1674300035) ip (hitcnt=0)
  domain controls.office.com (bid=-1674092701) ip (hitcnt=0)
  domain clientlog.portal.office.com (bid=-1673794351) ip (hitcnt=0)
  domain portal.office.com (bid=88903411) ip (hitcnt=0)
ftd#
```

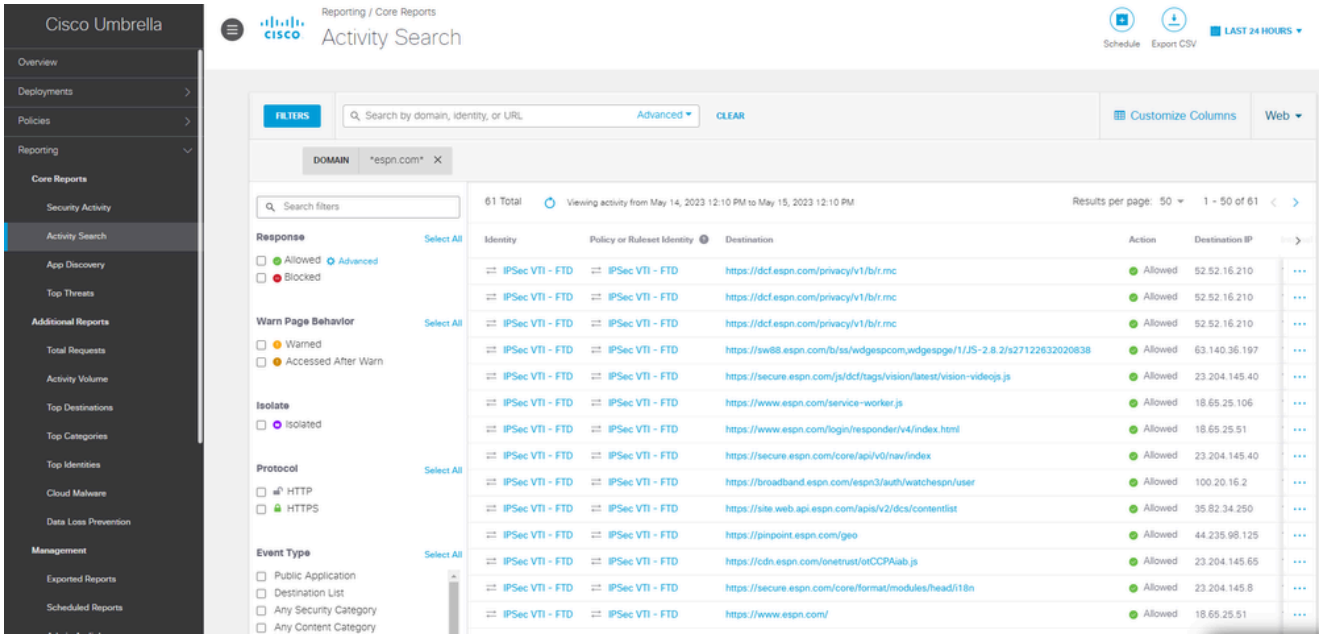
15670635784852

- `packet-tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed` (verifica que la interfaz externa se utiliza como salida y no la VTI one)

- En Umbrella Dashboard, en búsqueda de actividad, puede ver que el tráfico web que va a office.com nunca se envió a Umbrella, mientras que el tráfico que va a espn.com sí se envió.



15671098042516



15671302832788

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).