Configuración del objeto FQDN en la ACL extendida para PBR en FMC

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

Verificación

Problemas comunes

- PBR deja de funcionar después de una segunda implementación
- FQDN no resuelto

Introducción

Este documento describe el procedimiento para configurar un objeto FQDN en una lista de acceso ampliada (ACL) para su uso en el routing basado en políticas (PBR).

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- Centro de gestión de firewall seguro (FMC)
- Protección frente a amenazas de firewall (FTD)
- PBR

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Threat Defense para VMware versión 7.6.0
- Secure Firewall Management Center para VMware versión 7.6.0

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.

Antecedentes

Actualmente, el FTD no permite filtrar el tráfico no HTTP mediante objetos de nombre de dominio completo (FQDN), como se menciona en el ID de error de funcionamiento de Cisco CSCuz98322.

Esta funcionalidad es compatible con las plataformas ASA, sin embargo, solo las redes y las aplicaciones se pueden filtrar en FTD.

Puede agregar un objeto FQDN a una lista de acceso ampliada para configurar PBR mediante este método.

Configurar

Paso 1. Cree objetos FQDN según sea necesario.

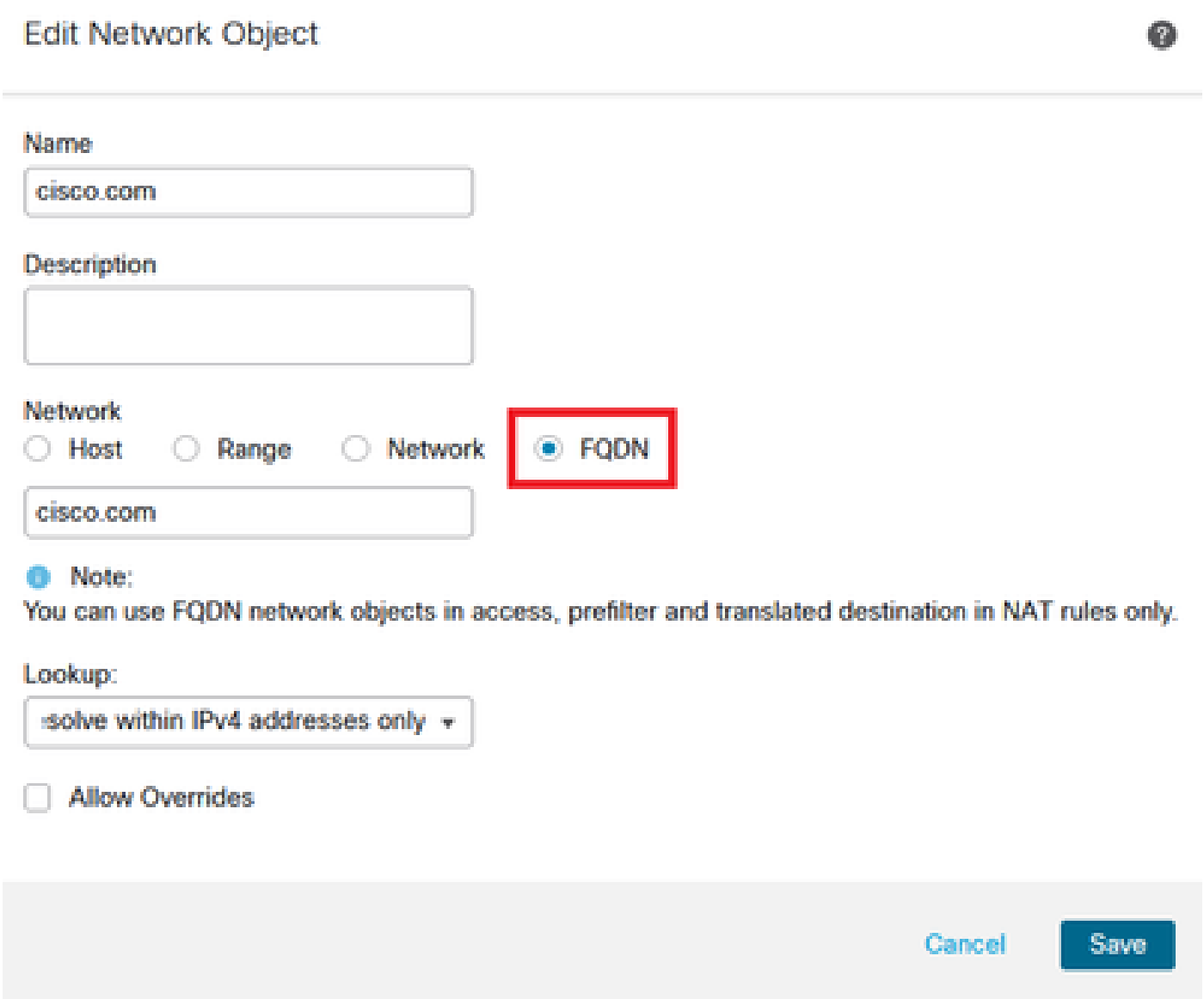

Imagen 1. Menú Objeto de red

Paso 2. Cree una lista de acceso ampliada en Objetos > Administración de objetos > Lista de

acceso > Ampliada.

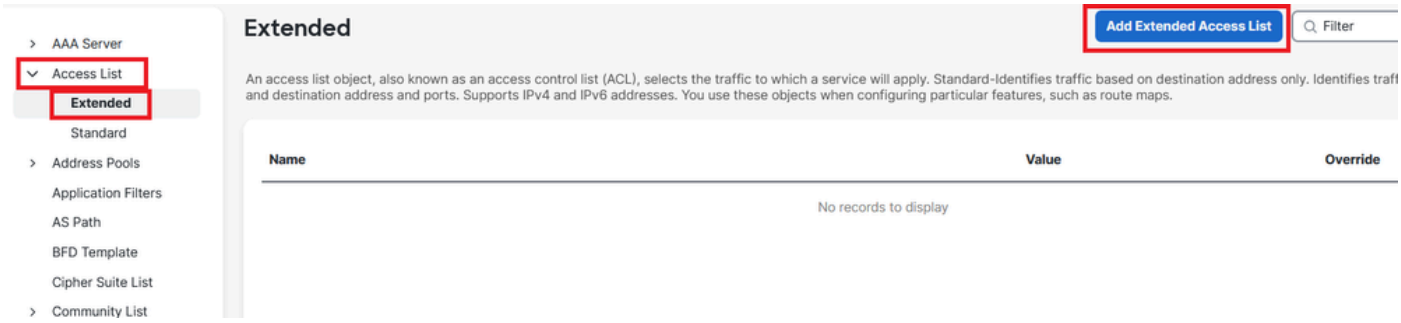

Imagen 2. Menú de lista de acceso ampliado

Al agregar una nueva regla, observe que no puede ver el objeto FQDN configurado al realizar una búsqueda en los objetos de red para seleccionar el origen y el destino.

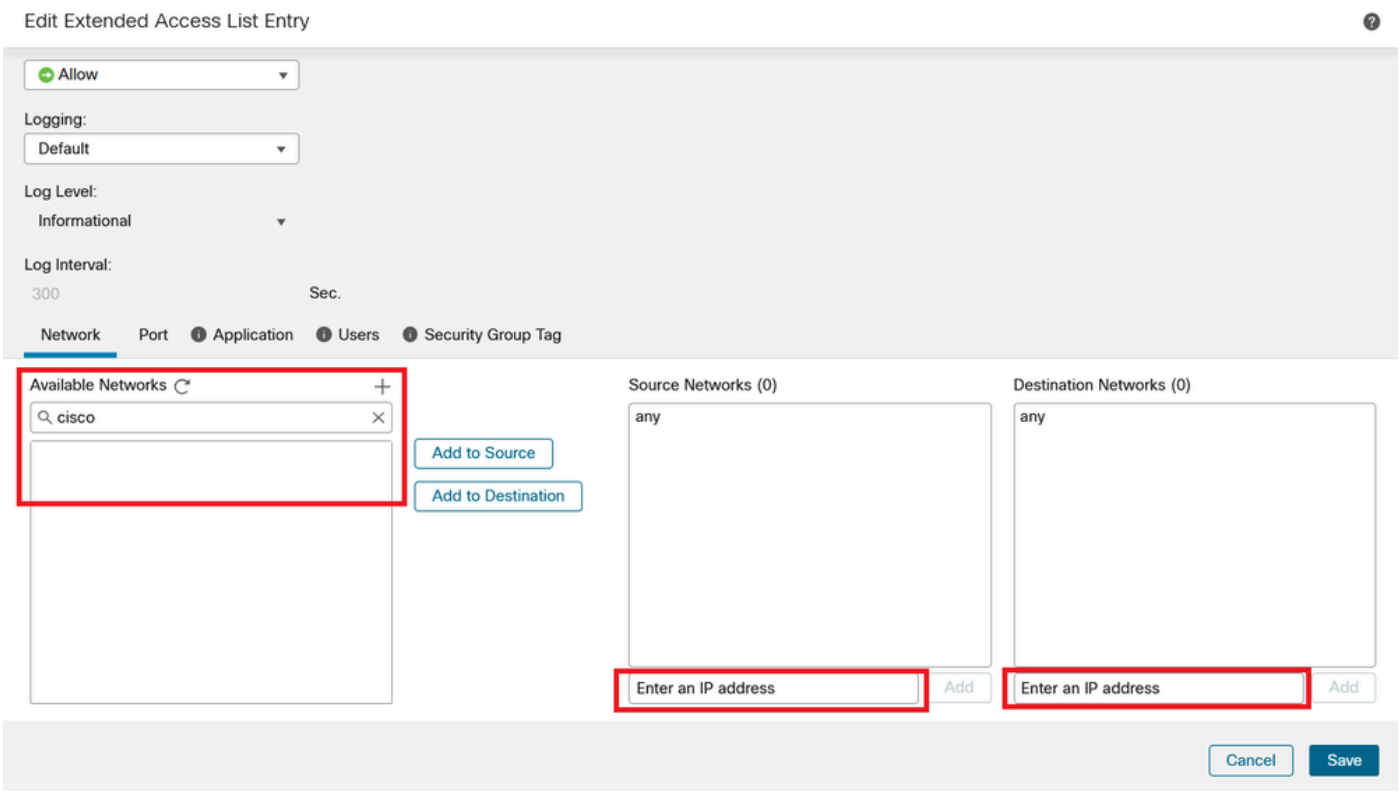

Imagen 3. Nuevo menú de reglas de lista de acceso ampliada

Paso 3. Cree una regla que no se pueda alcanzar para que la ACL extendida se cree y esté disponible para la configuración PBR.

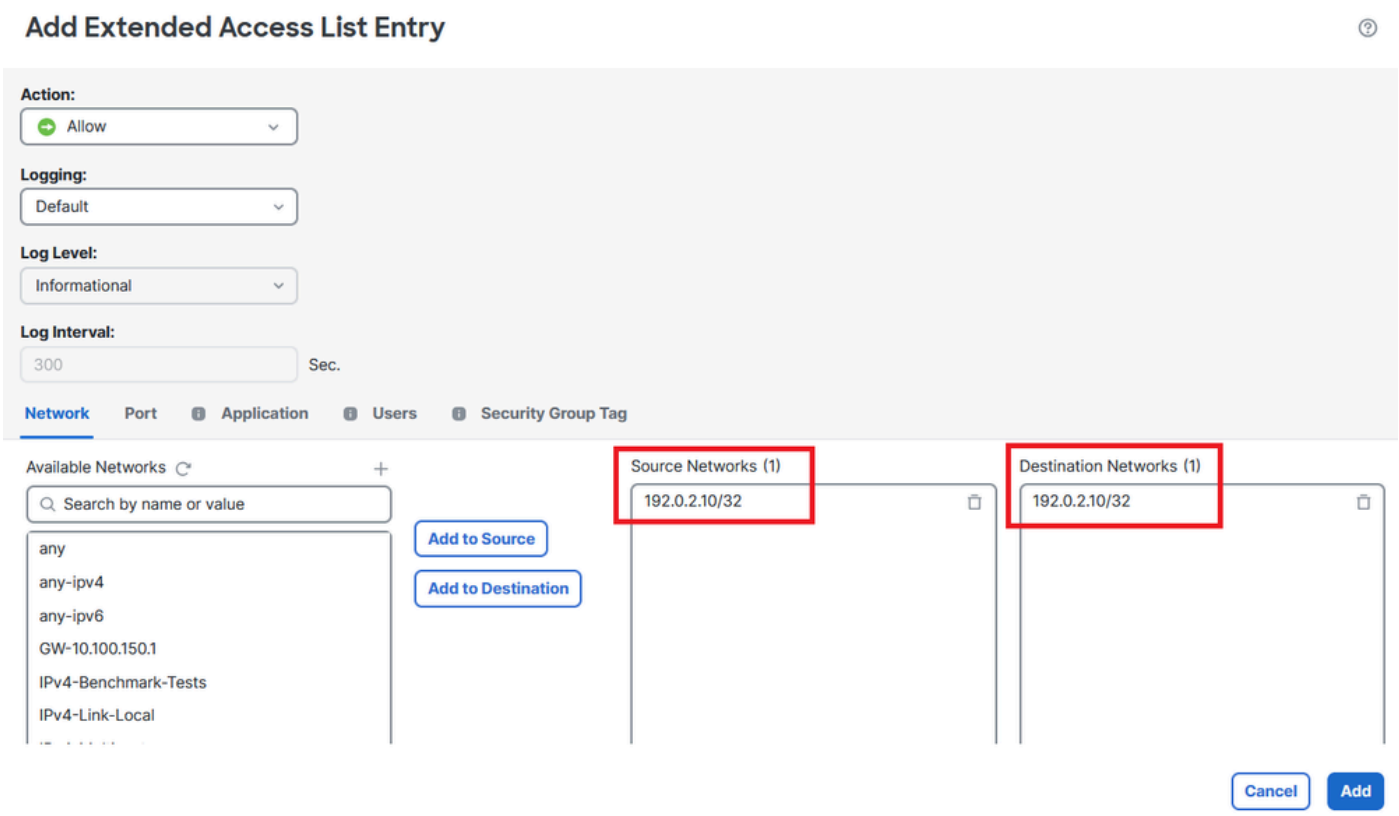

Imagen 4. Configuración de regla de lista de acceso que no se puede alcanzar

Paso 4. Debe crear una regla en la política de control de acceso (ACP) dirigida a su FTD con el objeto FQDN. El FMC implementa el objeto FQDN en el FTD para que pueda hacer referencia a él a través de un objeto FlexConfig.

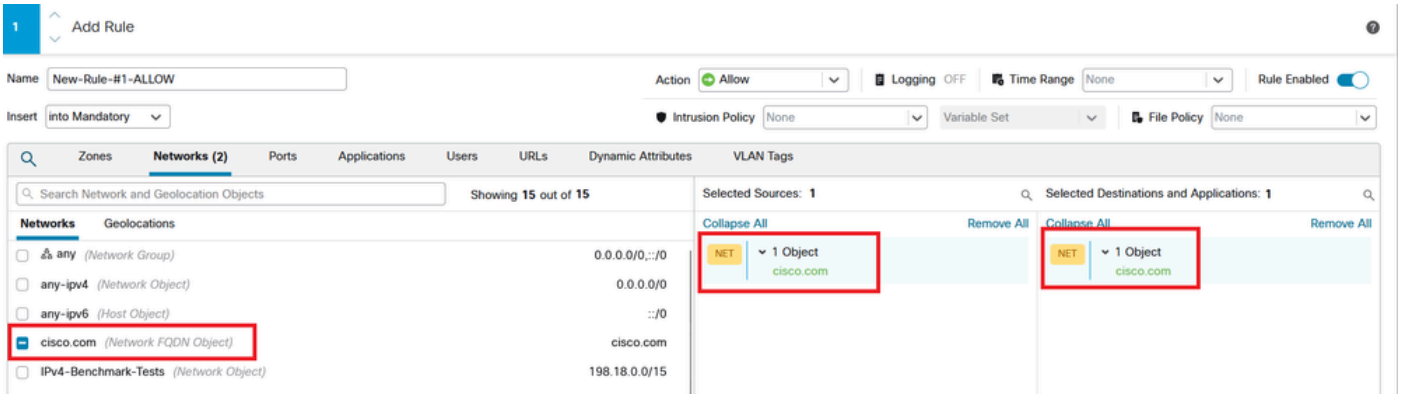

Imagen 5. Regla ACP con Objeto FQDN

Paso 5. Navegue hasta el FTD en Devices > Device Management y seleccione la pestaña Routing y navegue hasta la sección Policy Based Routing .

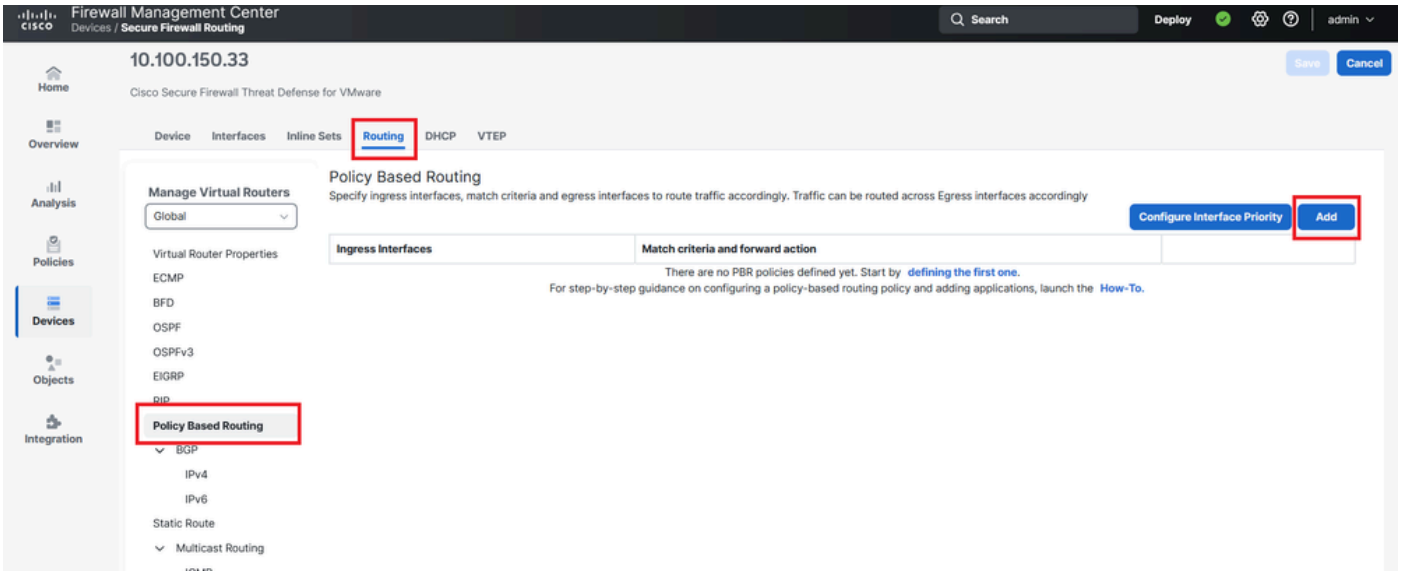

Imagen 6. Menú PBR

Paso 6. Configure el PBR en una interfaz usando la ACL configurada anteriormente e impleméntelo.

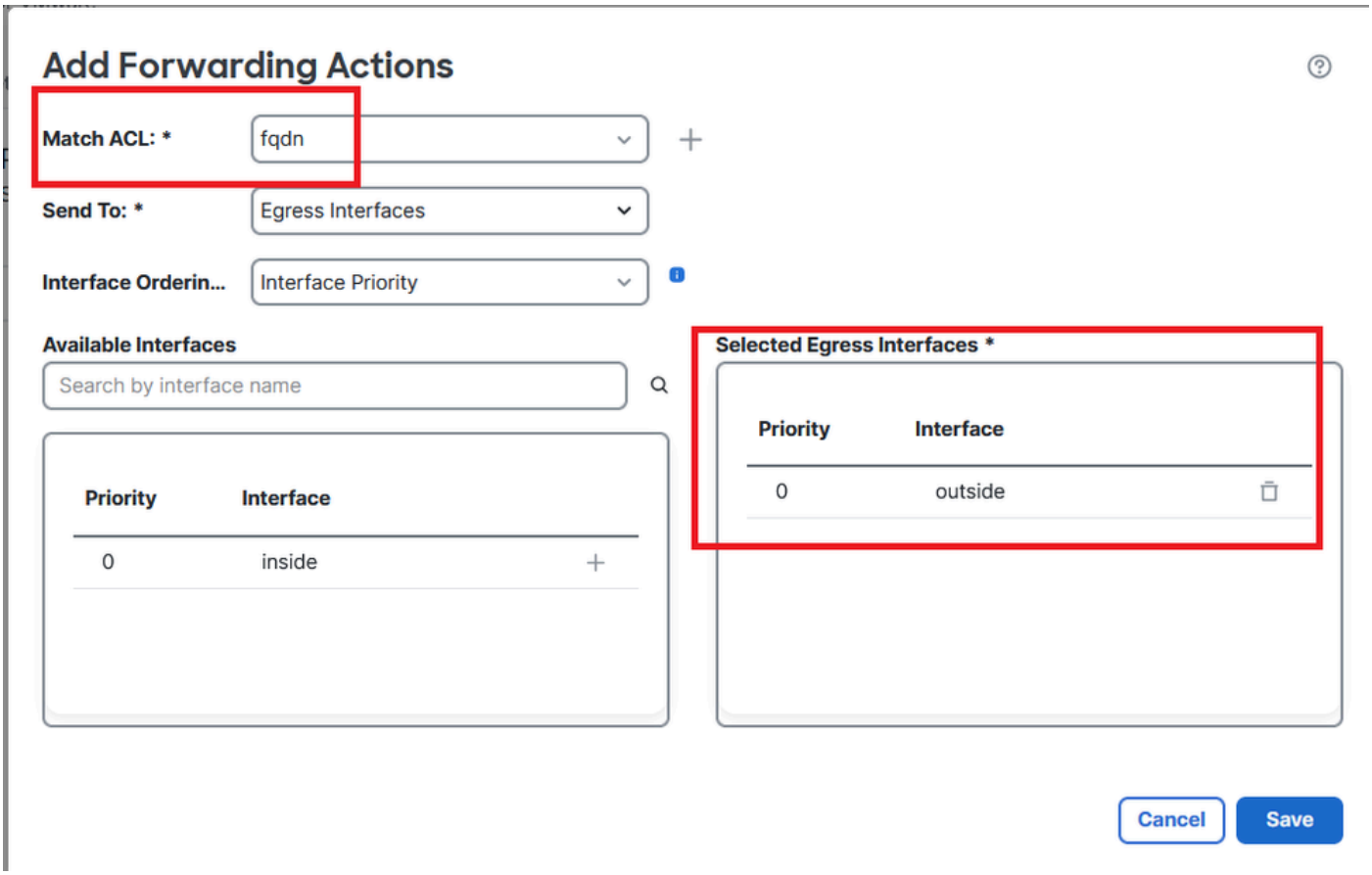

Imagen 7. Menú de selección de ACL e interfaz PBR

Paso 7. Navegue hasta Objetos > Administración de objetos > FlexConfig > Objeto y cree un nuevo objeto.

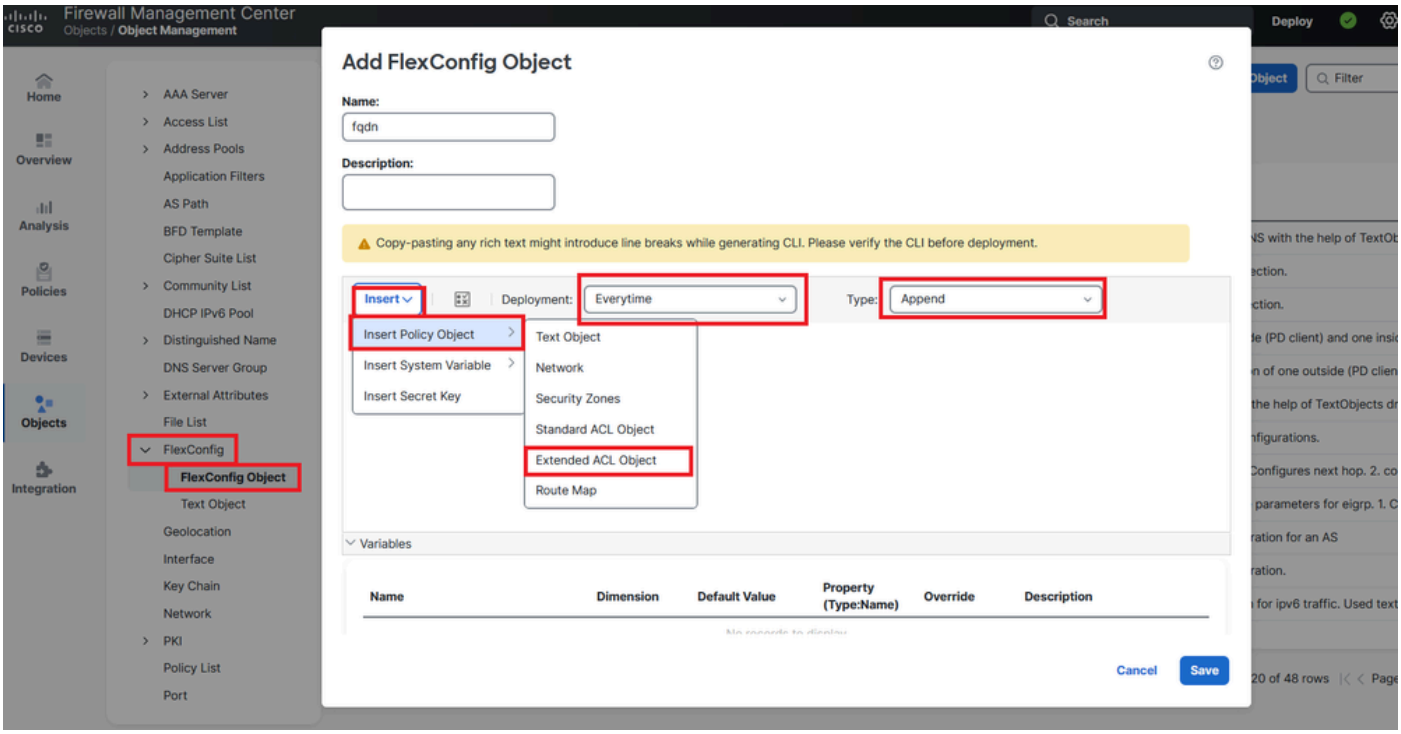

Imagen 8. Menú de configuración de objetos FlexConfig

Paso 8. Seleccione Insert > Extended ACL Object, asigne un nombre a la variable y seleccione la ACL extendida que creó anteriormente. La variable se agrega con el nombre que ha utilizado.

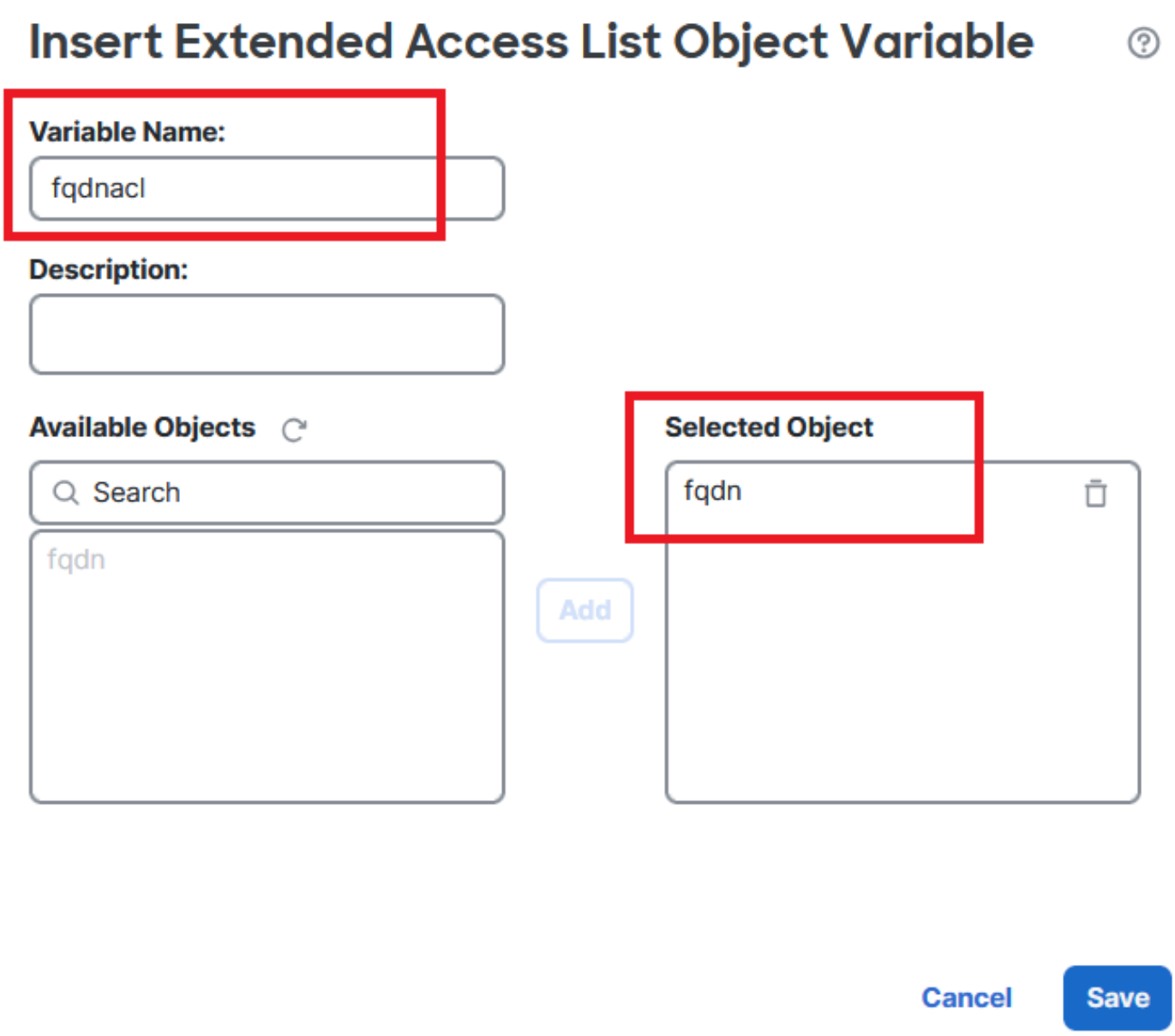

Imagen 9. Creación de variables para el objeto FlexConfig

Paso 9. Introduzca esta línea para cada objeto FQDN que desee agregar a su ACL.

<#root>

```
access-li $
```

```
extended permit ip any object
```

Paso 10. Guarde el objeto FlexConfig como Everytime > Append.

Paso 11.Vaya al menú Política de FlexConfig en Dispositivos > FlexConfig.

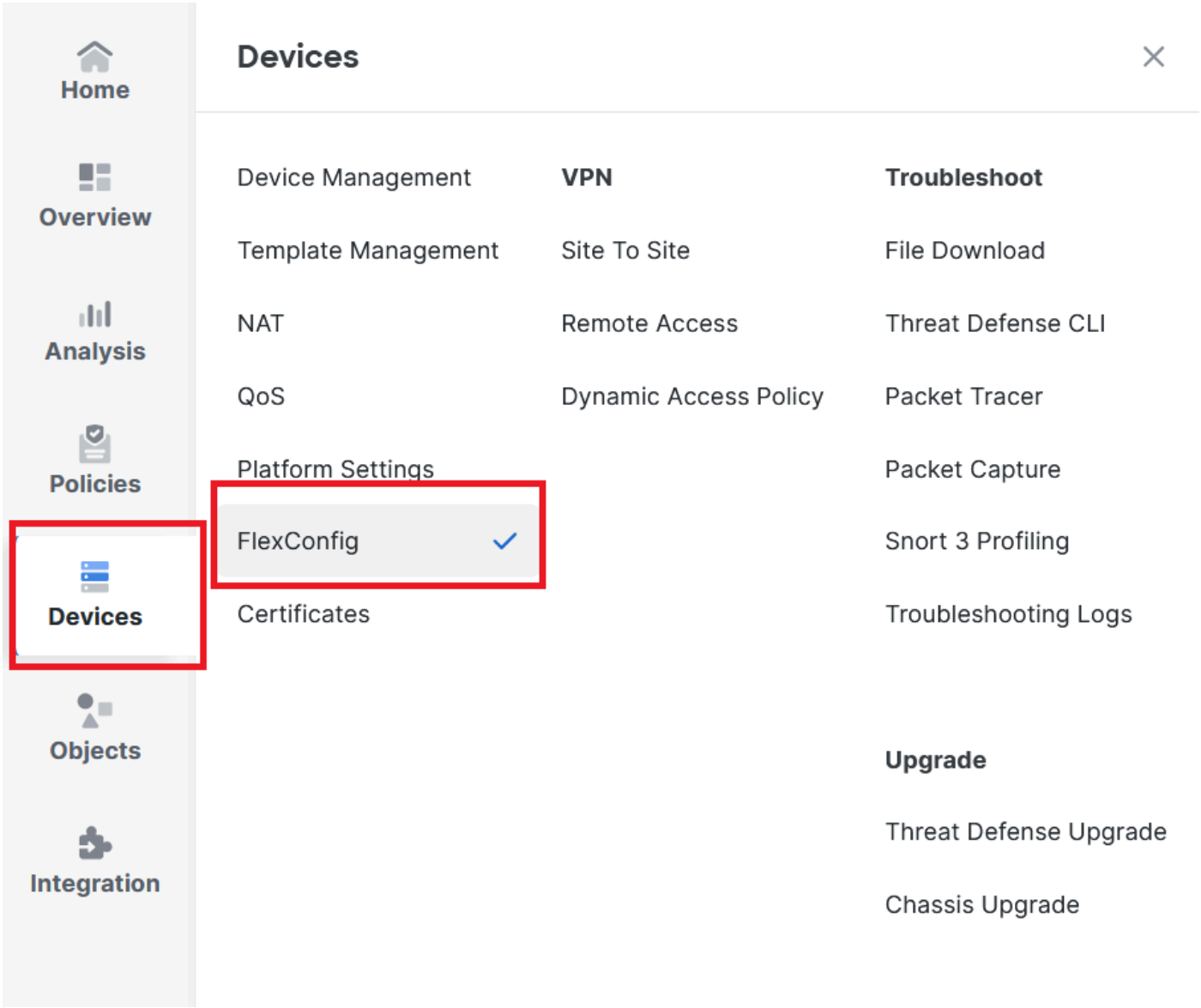

Imagen 10. Ruta al menú de la política FlexConfig

Paso 12. Cree una nueva política FlexConfig o seleccione una política ya asignada a su FTD.

Imagen 1. Editar o crear una nueva política FlexConfig

Paso 13. Agregue su objeto FlexConfig a la directiva, guarde e implemente.

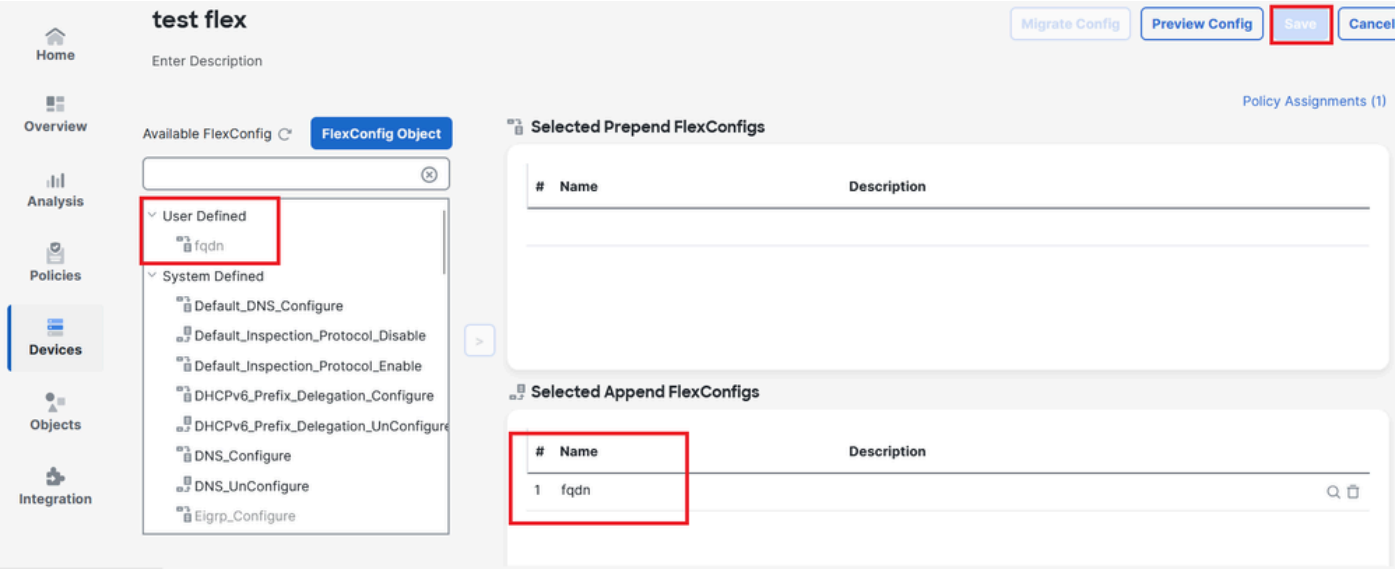

Imagen 12. Se ha agregado el objeto FlexConfig a la política FlexConfig

Verificación

Su interfaz de ingreso tiene la ruta de política con route-map generado automáticamente.

```
<#root>

firepower#

show run interface gi0/0


!
interface GigabitEthernet0/0
 nameif inside
 security-level 0
 ip address 10.100.151.2 255.255.255.0

policy-route route-map FMC_GENERATED_PBR_1727116778384
```

El route-map contiene la ACL seleccionada con la interfaz de destino utilizada.

```
<#root>

firepower#

show run route-map FMC_GENERATED_PBR_1727116778384


!
route-map FMC_GENERATED_PBR_1727116778384 permit 5

match ip address fqdn


set adaptive-interface cost outside
```

La lista de acceso contiene el host utilizado como referencia y la regla adicional que ha agregado mediante FlexConfig.

```
<#root>

firepower#

show run access-list fqdn


access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10

access-list fqdn extended permit ip any object cisco.com
```

Puede hacer un seguimiento de paquetes desde la interfaz de ingreso como fuente para verificar que se alcanza la fase PBR.

```
<#root>

firepower#

packet-tracer input inside tcp 10.100.150.1 12345 fqdn cisco.com 443


Mapping FQDN cisco.com to IP address 72.163.4.161


[...]
Phase: 3

Type: PBR-LOOKUP


Subtype: policy-route
Result: ALLOW
Elapsed time: 1137 ns

Config:


route-map FMC_GENERATED_PBR_1727116778384 permit 5


 match ip address fqdn


 set adaptive-interface cost outside


Additional Information:


 Matched route-map FMC_GENERATED_PBR_1727116778384, sequence 5, permit
```

```
 Found next-hop 10.100.150.1 using egress ifc outside

[...]
Result:
input-interface: inside(vrfid:0)

input-status: up
input-line-status: up
output-interface: outside(vrfid:0)

output-status: up
output-line-status: up
Action: allow
Time Taken: 140047752 ns
```

Problemas comunes

PBR deja de funcionar después de una segunda implementación

Verifique si la lista de acceso aún contiene la regla de objeto FQDN.

En este caso, puede ver que la regla ya no está aquí.

```
firepower# show run access-list fqdn
access-list fqdn extended permit ip host 192.0.2.10 host 192.0.2.10
firepower#
```

Verifique que el objeto FlexConfig esté configurado como Deployment: Everytime y Type: Append. La regla se aplica cada vez en futuras implementaciones.

FQDN no resuelto

Cuando intenta hacer ping al FQDN, aparece un mensaje sobre un nombre de host no válido.

```
<#root>
firepower#
ping cisco.com

               ^
ERROR: % Invalid Hostname
```

Verifique la configuración de DNS. Debe tener servidores DNS accesibles en su grupo de servidores y las interfaces de búsqueda de dominio deben poder alcanzarlos.

```
<#root>

firepower#

show run dns


dns domain-lookup outside


DNS server-group DefaultDNS
DNS server-group dns

name-server 208.67.222.222


name-server 208.67.220.220


dns-group dns

firepower#

ping 208.67.222.222


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.67.222.222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 170/202/280 ms
firepower#

ping cisco.com


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.163.4.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/190 ms.
```

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).