Configuración del tiempo de espera de conexión para tráfico específico en ASA con ASDM

Contenido

Introducción

Este documento describe la configuración del tiempo de espera de conexión en ASA y ASDM para un protocolo de aplicación específico como HTTP, HTTPS, FTP o cualquier otro protocolo. El tiempo de espera de la conexión es el período de inactividad tras el cual un firewall o un dispositivo de red finaliza una conexión inactiva para liberar recursos y mejorar la seguridad. De antemano, la primera pregunta es: ¿Cuál es el requisito para esta configuración? Si las aplicaciones tienen la configuración adecuada de keepalive de TCP, a menudo no es necesario configurar el tiempo de espera de conexión en un firewall. Sin embargo, si las aplicaciones carecen de la configuración adecuada de keepalive o del tiempo de espera, en ese caso la configuración del tiempo de espera de la conexión en un firewall es crucial para administrar los recursos, mejorar la seguridad, mejorar el rendimiento de la red, garantizar el cumplimiento y optimizar la experiencia del usuario.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Lista de control de acceso (ACL)

- Política de servicio
- Tiempo de espera de conexión

Componentes Utilizados

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

- ASA 9.17(1)
- ASDM 7.17(1)

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.

Valores predeterminados

Nota: Tiempo de espera predeterminado

El tiempo de espera embrionario predeterminado es de 30 segundos.

El tiempo de espera inactivo medio cerrado predeterminado es de 10 minutos.

El valor predeterminado de dcd max_retries es 5.

El valor predeterminado de dcd retry_interval es de 15 segundos.

El tiempo de espera de inactividad predeterminado de tcp es de 1 hora.

El tiempo de espera inactivo udp predeterminado es de 2 minutos.

El tiempo de espera icmp inactivo predeterminado es de 2 segundos.

El tiempo de espera sip inactivo predeterminado es de 30 minutos.

El tiempo de espera inactivo sip_media predeterminado es de 2 minutos.

El tiempo de espera de inactividad esp y ha predeterminado es de 30 segundos.

Para todos los demás protocolos, el tiempo de espera inactivo predeterminado es de 2 minutos.

Para no agotar el tiempo de espera, introduzca 0:0:0.

Configurar tiempo de espera de conexión

ASDM

Si un tráfico determinado tiene una tabla de conexión, tiene un tiempo de espera inactivo específico; por ejemplo, en este artículo, cambiamos el tiempo de espera de conexión para el tráfico DNS.

A continuación, se detallan muchas opciones para configurar el tiempo de espera de conexión para un tráfico específico, teniendo en cuenta el diagrama de red de este tráfico:

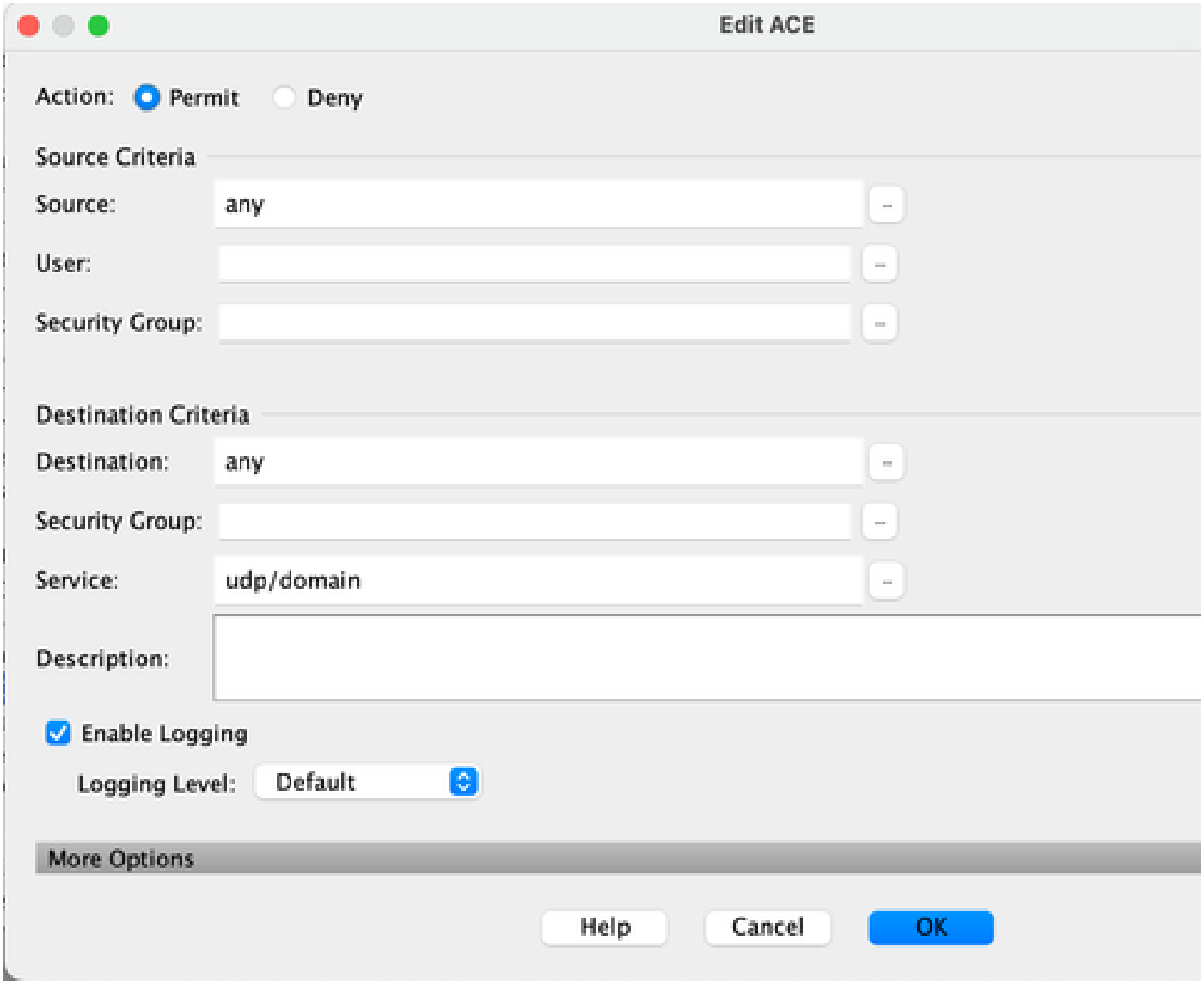
Cliente ----- [Interfaz: MNG] Firewall [Interfaz: OUT] ----- Servidor

Existe la posibilidad de asignar una ACL a la interfaz.

Paso 1: Crear una ACL

Podemos asignar origen, destino o servicio

ASDM > Configuration > Firewall > Advanced > ACL Manager

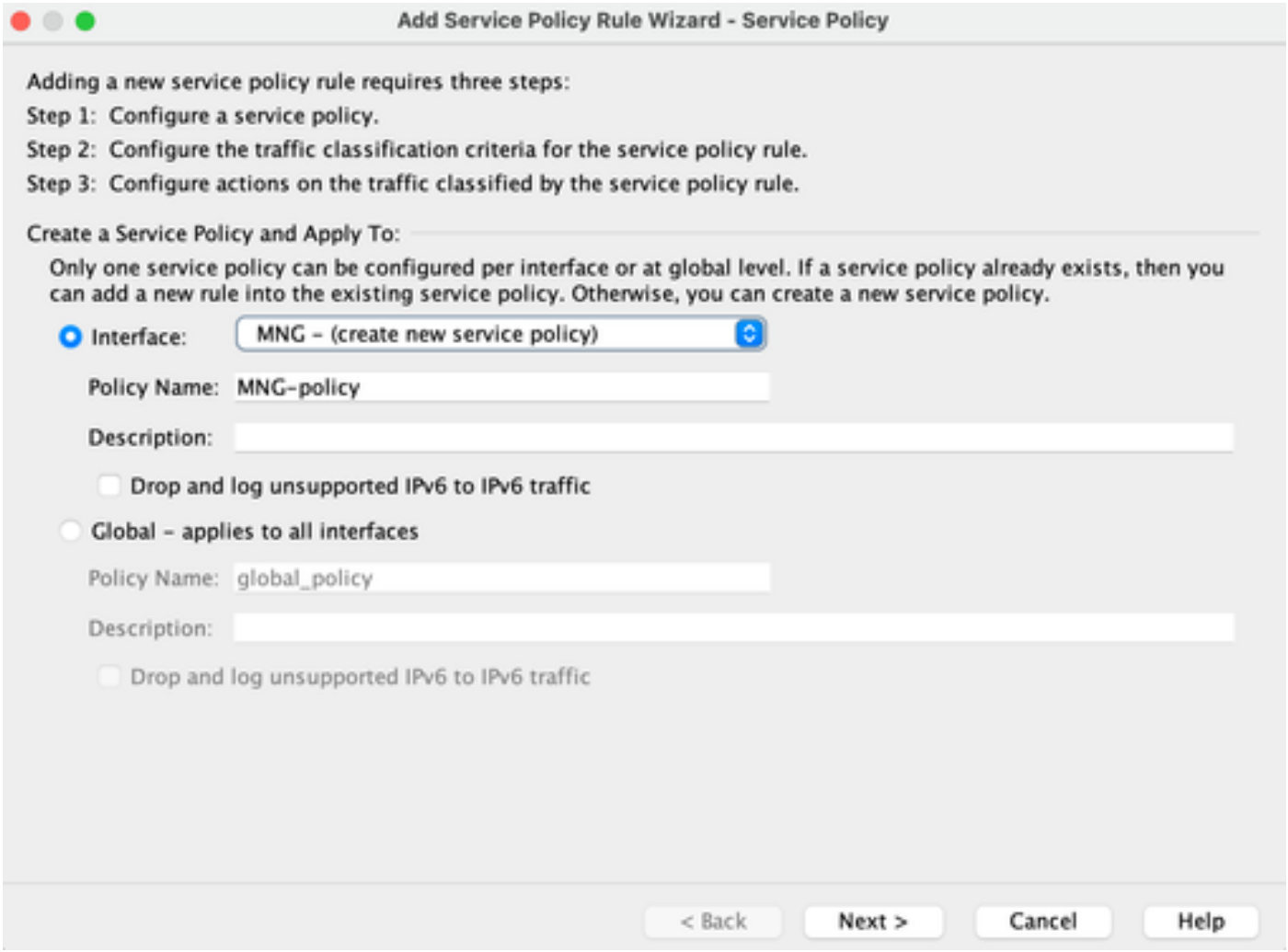


Paso 2: Crear regla de política de servicio

Puede saltarse el último paso si ya tiene su ACL o puede asignar uno de esos parámetros

(origen, destino o servicio) a la política de servicio de la interfaz.

ASDM > Configuration > Firewall > Service Policy rules

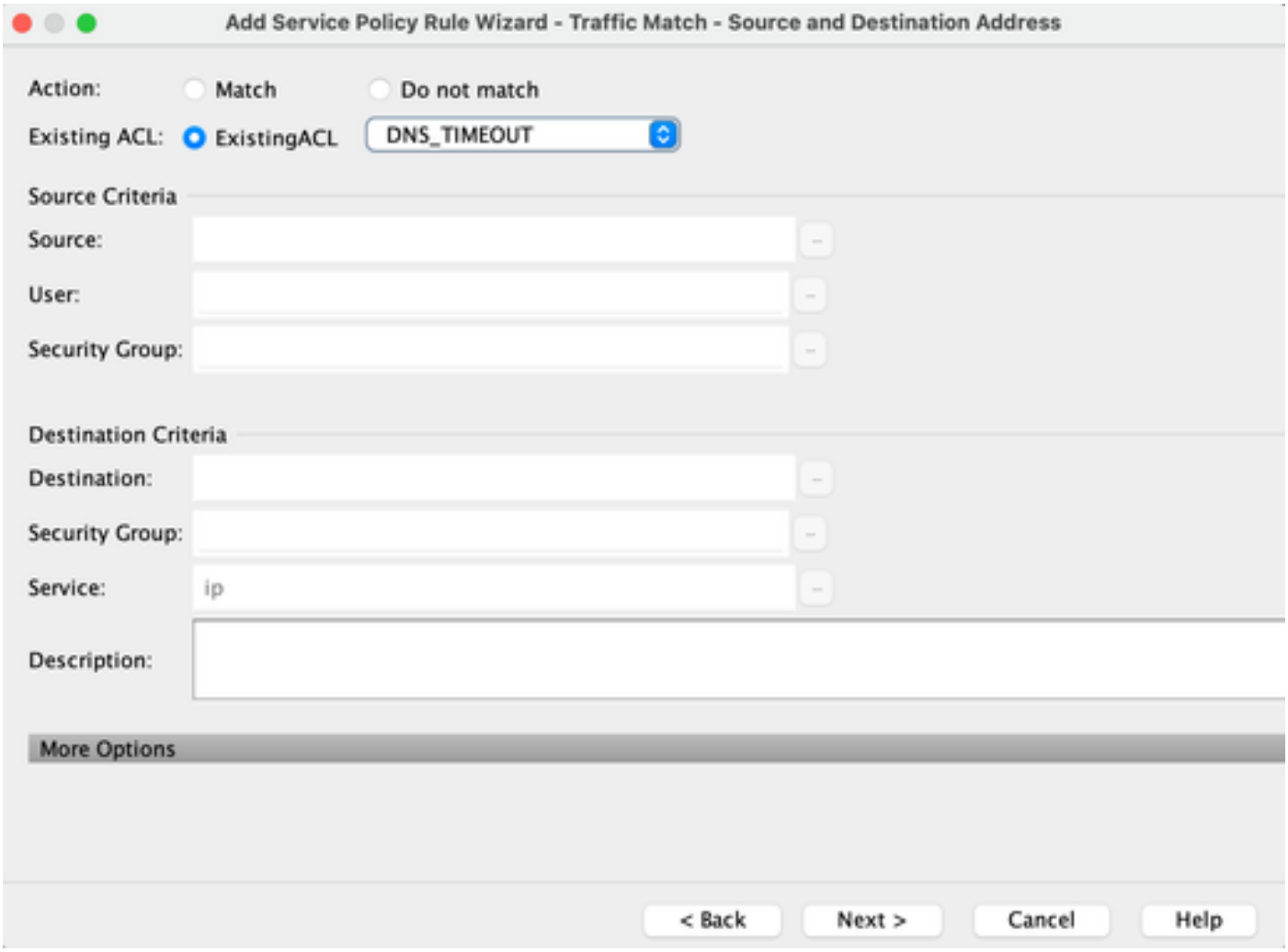


Paso 3: Crear clase de tráfico

Existe la posibilidad de elegir la dirección IP de origen y de destino (utiliza ACL)

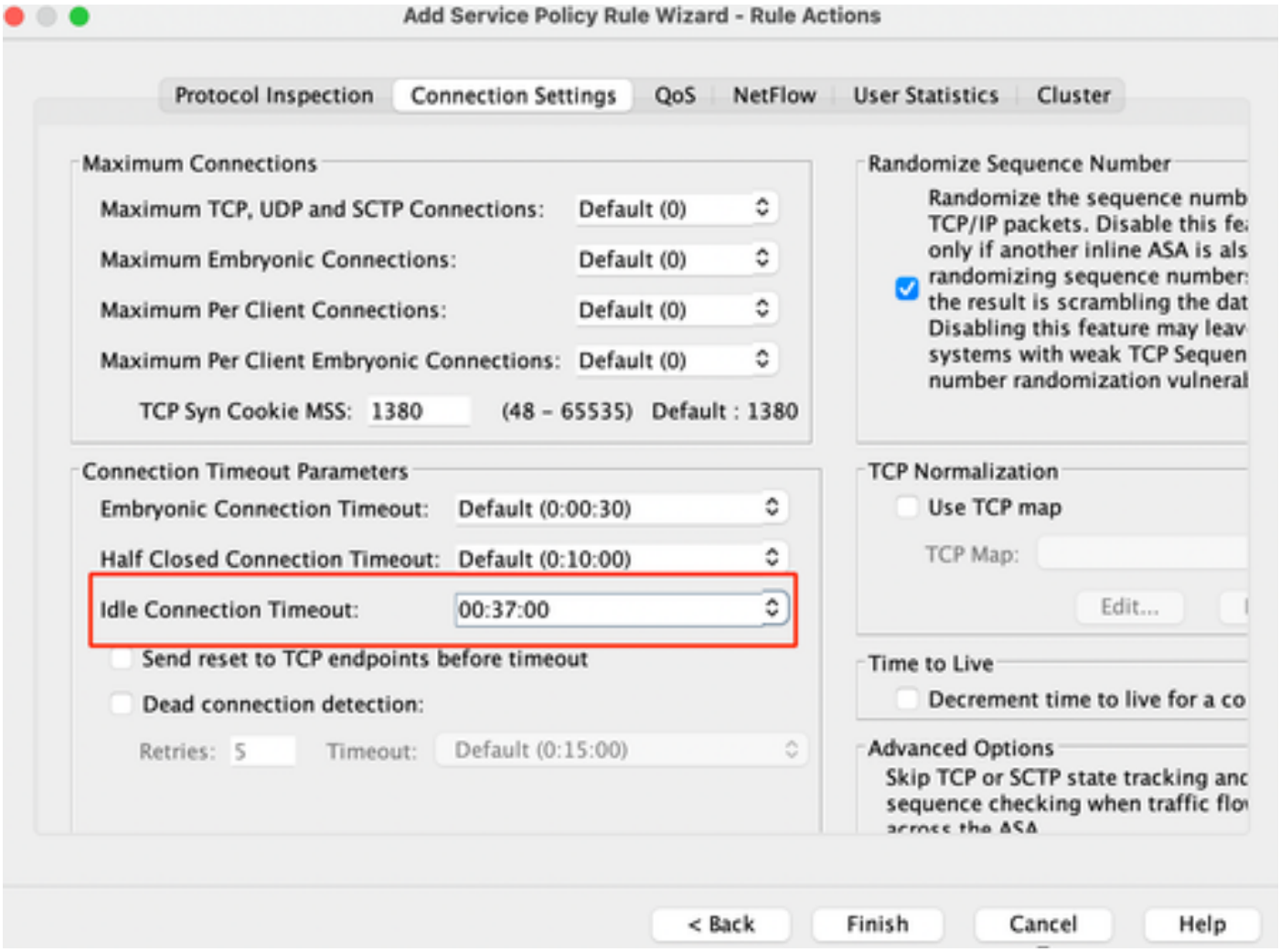
Paso 4: Asignar ACL

En este paso, puede asignar la ACL existente o seleccionar condiciones de coincidencia (origen, destino o servicio)



Paso 5: Configure el parámetro Idle Timeout

De acuerdo con el formato válido HH:MM:SS, configure el tiempo de espera inactivo.



Borre las conexiones para ese tráfico en particular:

#clear conn addressIntroduzca una dirección IP o un intervalo de direcciones IP

#clear conn protocolIngrese esta palabra clave para borrar solamente las consolas SCP/TCP/UDP

CLI ASA

Puede configurar todos estos parámetros mediante la CLI:

ACL:

access-list DNS_TIMEOUT extended permit udp any any eq domain

Mapa de clases:

class-map MNG-class
match access-list DNS_TIMEOUT

Policy-map:

policy-map MNG-policy
class MNG-class
set connection timeout idle 0:37:00

Aplique Policy-map en la interfaz:

service-policy MNG-policy interface MNG

Verificación

Consejo: Si ejecutamos este comando, podemos confirmar el tiempo de espera de conexión del tráfico DNS:

ASA CLI > enable mode > show conn long

Ejemplo: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle 17s, uptime 17s, timeout 2m0s, bytes 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle 40s, uptime 40s, timeout 2m0s, bytes 36

Luego, después de la configuración, podemos confirmar la configuración del tiempo de espera inactivo:

Ejemplo: show conn long address 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle 8s, uptime 8s, timeout 37m0s, bytes 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle 5s, uptime 5s, timeout 37m0s, bytes 41

Referencias

Configuración de la conexión

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).