Configuración de NAT estática para la extensión TLOC para la interoperabilidad con NAT simétrica

Contenido

Introducción

Este documento describe la configuración de NAT estática en un router de extensión TLOC mediante sobrecarga NAT para trabajar con pares detrás de NAT simétrica.

Recomendaciones

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- traducción de Dirección de Red (NAT)
- Extensión TLOC

Componentes Utilizados

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

- C8000V versión 17.15.1a

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.

Problema

La Guía de Diseño de Cisco Catalyst SD-WAN destaca que ciertos tipos de Traducción de Direcciones de Red (NAT) pueden afectar la formación de Conexiones de Control y Túneles BFD.

Los dos tipos de NAT que no funcionan juntos son NAT restringida de puerto/dirección y NAT simétrica. Estos tipos de NAT requieren que las sesiones se inicien desde la red interna para permitir el tráfico en cada puerto. Esto significa que el tráfico externo no puede iniciar una conexión a la red interna sin una solicitud previa desde el interior.

Los sitios detrás de una NAT simétrica a menudo experimentan dificultades para establecer sesiones BFD con sitios pares. Esto es particularmente difícil cuando se compara con un sitio que usa la extensión TLOC detrás de la sobrecarga de NAT (también conocida como NAT restringida de puerto/dirección).

Topología

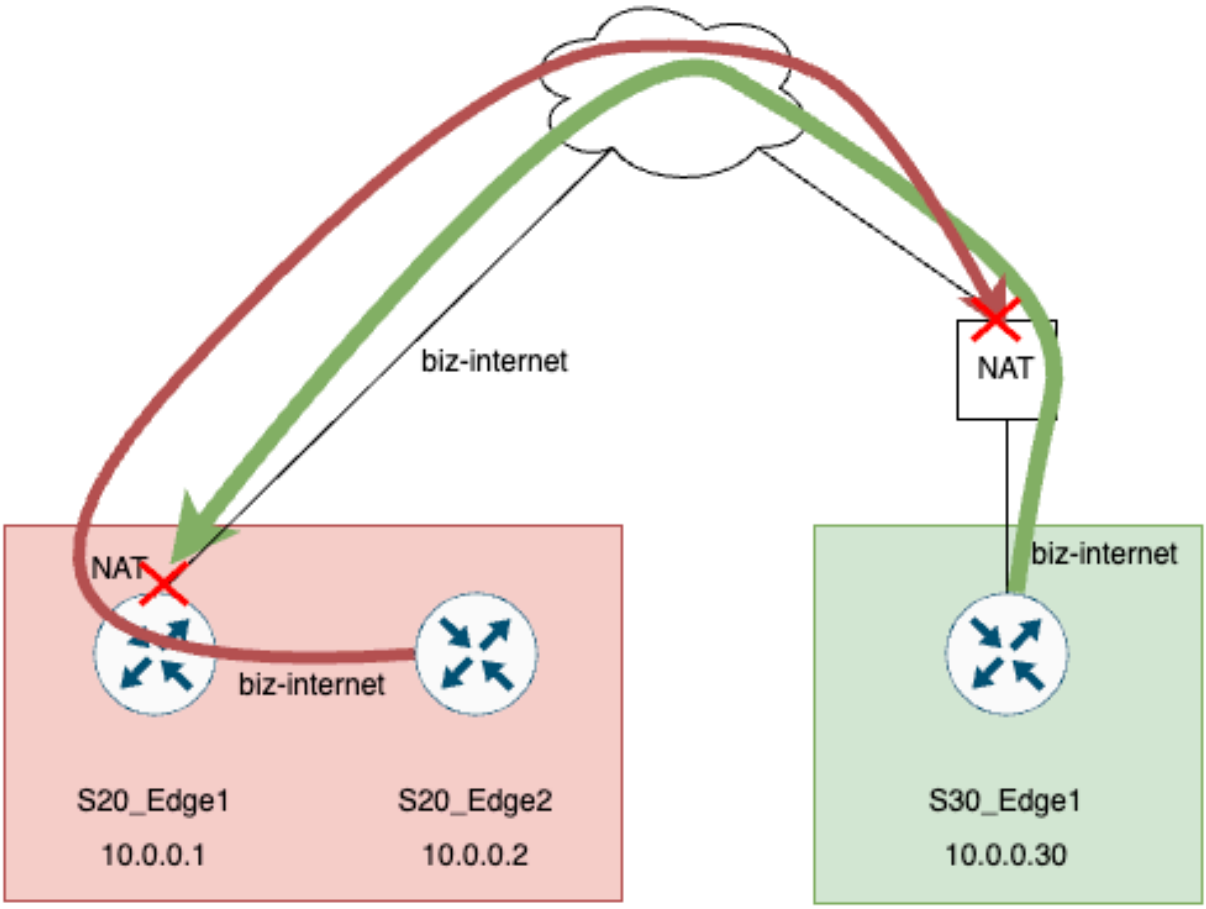
Condiciones

1. S30_Edge1 está detrás de una NAT simétrica

2. S20_Edge2 está detrás de la extensión TLOC donde S20_Edge1 está usando sobrecarga NAT (PAT) para NAT los flujos desde Edge2.

Esto hace que los saludos BFD se descarten en el dispositivo NAT simétrico y en el S20_Edge1 debido a que no hay ninguna sesión presente para el puerto desconocido del par.

El dispositivo S20_Edge1 muestra el descarte implícito de ACL para estos saludos debido a que no coinciden con ninguna sesión de la tabla NAT.



Identificar el problema

Paso 1. Comprobar las sesiones BFD

En el resultado de show sdwan bfd sessions en S30_Edge1, se observa que la sesión BFD a S20_Edge2, 10.0.0.2, está inactiva.

```
S30_Edge1#show sdwan bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
-----------------------------------------------------------------------------------------------------
10.0.0.2         20          down        biz-internet     biz-internet     192.168.30.2
10.0.0.1         20          up          biz-internet     biz-internet     192.168.30.2
```

Paso 2. Verifique el tipo de NAT

En la parte inferior de la salida, el tipo A de NAT se ve en S30_Edge1. Esto indica NAT simétrica. Observe también la IP pública 172.16.1.34 y el puerto 31048.

```
S30_Edge1# show sdwan control local-properties



site-id                           30
domain-id                         1
protocol                          dtls
tls-port                          0
system-ip                         10.0.0.30




 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                         PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet1              172.16.1.34     31048  192.168.30.2    ::
```

Paso 3. Verifique la configuración de NAT

Desde la topología se sabe que S20_Edge2 está detrás de la extensión TLOC. En este momento podemos verificar la configuración de PAT en el S20_Edge1.

La configuración de sobrecarga de NAT ya está presente en S20_Edge1

```
S20_Edge1#sh run int gi1
interface GigabitEthernet1
 description biz-internet
 ip dhcp client default-router distance 1
 ip address 192.168.20.2 255.255.255.0
 no ip redirects
 ip nat outside
 load-interval 30
 negotiation auto
 arp timeout 1200
end


S20_Edge1#sh run | i nat
```

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
```

Paso 4. Verifique la IP pública y el puerto

Verifique el resultado de show sdwan control local properties en S20_Edge2 para ver la IP pública y el puerto 172.16.1.18 y el puerto 5063

```
S20_Edge2#show sdwan control local-properties
```

```
site-id                           20
domain-id                         1
protocol                          dtls
tls-port                          0
system-ip                         10.0.0.2
```

```
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                           PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                  IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet2.100          172.16.1.18     5063   192.168.100.2   ::
```

Paso 5. Verifique las traducciones NAT

Ahora verifique las traducciones NAT en el dispositivo S20_Edge1. Solo hay una sesión NAT a la IP anunciada y al puerto para S30_Edge1, IP 172.16.1.34 y el puerto 31048. Considerando lo que sabemos sobre NAT simétrica, este no es el caso. Debe haber al menos un puerto diferente de 31048 (no un puerto SD-WAN estándar como 12346), si no una combinación de IP Y puerto

diferente.

```
 S20_Edge1#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.69:12346     172.16.1.69:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.102:12446    172.16.0.102:12446
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.50:12346     172.16.1.50:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.202:12346    172.16.0.202:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.82:12346     172.16.1.82:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.34:31048     172.16.1.34:31048
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.201:12346    172.16.0.201:12346
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.0.101:12446    172.16.0.101:12446
udp  192.168.20.2:5063     192.168.100.2:12346   172.16.1.98:12346     172.16.1.98:12346
```

Paso 6. Comprobar el seguimiento de FIA

Ejecute un seguimiento FIA sólo para verificar que los paquetes se están descartando en S20_Edge1. Tenga en cuenta que la IP puede no ser la misma que la anunciada, pero en este caso para simplificar, lo es.

```
S20_Edge1#debug platform condition ipv4 172.16.1.34/32 both
S20_Edge1#debug platform condition start
S20_Edge1#debug platform packet packet 1024 fia
S20_Edge1#debug platform packet packet 1024 fia-trace
S20_Edge1#show platform packet summary
Pkt   Input                     Output                    State  Reason
0     Gi2.100                   Gi1                       FWD
1     internal0/0/recycle:0     Gi1                       FWD
2     Gi2.100                   Gi1                       FWD
3     internal0/0/recycle:0     Gi1                       FWD
4     Gi2.100                   Gi1                       FWD
5     internal0/0/recycle:0     Gi1                       FWD
6     Gi2.100                   Gi1                       FWD
7     internal0/0/recycle:0     Gi1                       FWD
8     Gi1                       Gi1                       DROP   479 (SdwanImplicitAclDrop)
```

Verifique el paquete 8 para ver si este es el paquete sospechoso.

```
S20_Edge1#show platform packet packet 8
Packet: 8           CBUG ID: 482
Summary
  Input     : GigabitEthernet1
  Output    : GigabitEthernet1
  State     : DROP 479 (SdwanImplicitAclDrop)
  Timestamp
    Start   : 6120860350139 ns (04/18/2025 02:35:03.873687 UTC)
    Stop    : 6120860374021 ns (04/18/2025 02:35:03.873710 UTC)
Path Trace
  Feature: IPV4(Input)
```

```
    Input       : GigabitEthernet1
    Output      :



    Source      : 172.16.1.34
    Destination : 192.168.20.2
    Protocol    : 17 (UDP)
      SrcPort   : 3618
      DstPort   : 12346
```

Este parece ser el paquete de S30_Edge1.

Volviendo a verificar en la tabla NAT en el paso 6, podemos ver que no hay sesión para este paquete. Esa es la razón de la caída.

Paso 7. Verifique los contadores BFD

Los paquetes BFD de S20_Edge2 no se verán en S30_Edge1 debido a que se descartarán fuera del dispositivo, en el dispositivo NAT. Los contadores BFD Tx/Rx se pueden verificar mediante el comando show sdwan tunnel statistics.

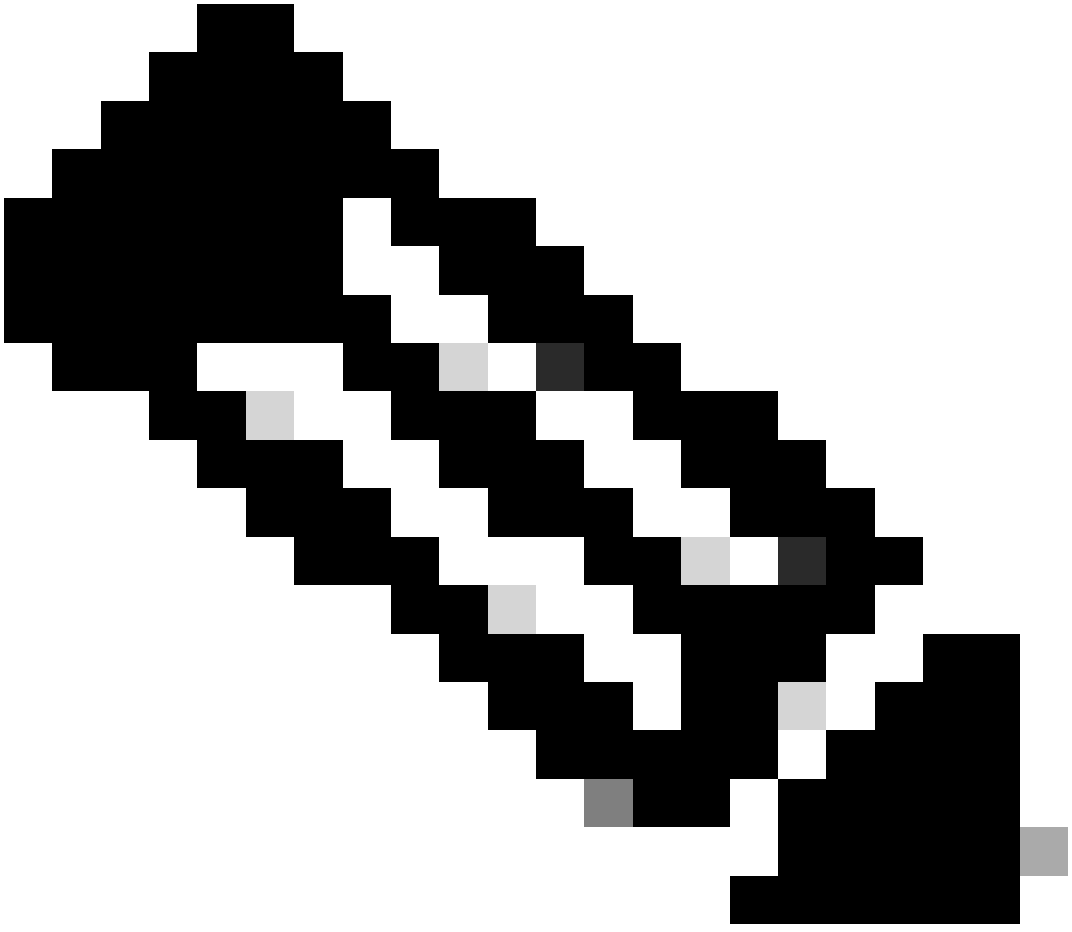
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts              0   <<<<<<<<<<<<<
 rx_octets            0
 tcp-mss-adjust       1358
 ipv6_tx_pkts         0
 ipv6_tx_octets       0
 ipv6_rx_pkts         0
 ipv6_rx_octets       0
 tx_ipv4_mcast_pkts   0
 tx_ipv4_mcast_octets 0
 rx_ipv4_mcast_pkts   0
 rx_ipv4_mcast_octets 0
 tx-ipv6-mcast-pkts   0
 tx-ipv6-mcast-octets 0
 rx-ipv6-mcast-pkts   0
 rx-ipv6-mcast-octets 0
```

Solución

Para resolver esto, se puede configurar una NAT estática sobre la sobrecarga de NAT (PAT) en S20_Edge1 para NAT todo el control y paquetes BFD en una sola combinación de IP/puerto.

1. Primero, será necesario inhabilitar el salto de puerto en este color, o en todo el sistema en S20_Edge2.

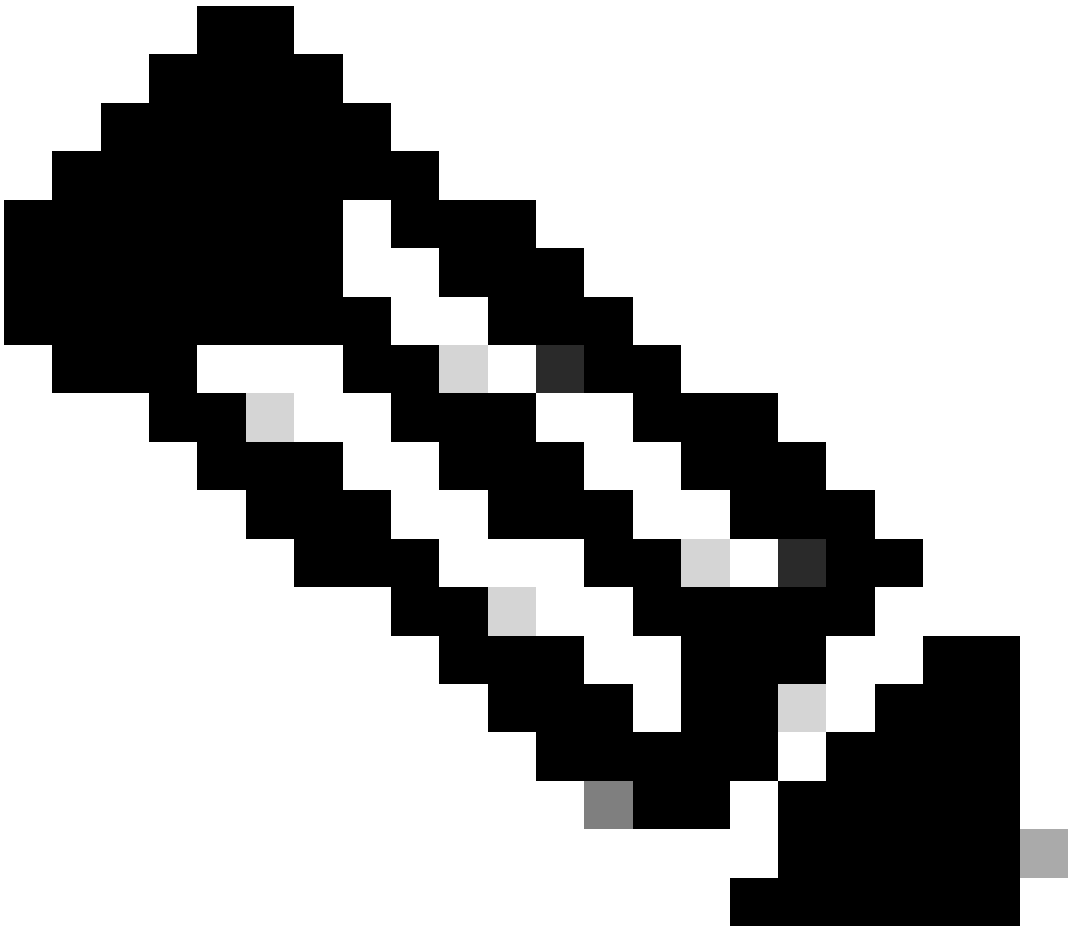
También se agregará un desplazamiento de puerto como práctica recomendada para S20_Edge2, de modo que S20_Edge1 y S10_Edge2 no utilizan el mismo puerto de origen para las conexiones de control o los túneles BFD.



> Nota: Esta configuración se puede realizar a través de la CLI del router o a través de una plantilla de complementos de la CLI de vManage.

```
S20_Edge2#config-t
S20_Edge2(config)# system
```

```
S20_Edge2(config-system)# no port-hop
S20_Edge2(config-system)# port-offset 1
S20_Edge2(config-system)# commit
```



Nota: Asegúrese de que el S20_Edge2 esté usando el puerto base 12347 después de esta configuración al verificar show sdwan control local-properties. Si no está utilizando el puerto base, utilice el comando clear sdwan control port-index para restablecer el puerto nuevamente al puerto base. Esto evita que el puerto cambie si se estaba ejecutando en un puerto superior y luego se reinicia más tarde. El comando clear restablecerá las conexiones de control y los túneles bfd.

---

2. Configure la NAT estática en S20_Edge1.

```
S20_Edge1#config-t
S20_Edge1(config)# ip nat inside source static udp 192.168.100.2 12347 192.168.20.2 12347 egress-interf
S20_Edge1(config)# commit
```

3. Borre las traducciones NAT en S20_Edge1.

```
S20_Edge1#clear ip nat translation *
```

Verificación

1. Verifique las sesiones BFD en uno de los pares.

```
S30_Edge1#show sdwan bfd sessions
                                      SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
-------------------------------------------------------------------------------------------------------
10.0.0.2         20          up          biz-internet     biz-internet     192.168.30.2
```

2. Verifique las sesiones NAT en S20_Edge1.

```
S20_Edge1#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  192.168.20.2:12347    192.168.100.2:12347   ---                   ---
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.202:12346    172.16.0.202:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.50:12346     172.16.1.50:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.102:12446    172.16.0.102:12446
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.34:50890     172.16.1.34:50890
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.69:12346     172.16.1.69:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.98:12346     172.16.1.98:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.101:12446    172.16.0.101:12446
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.201:12346    172.16.0.201:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.1.82:12346     172.16.1.82:12346
udp  192.168.20.2:12347    192.168.100.2:12347   172.16.0.1:13046      172.16.0.1:13046
Total number of translations: 11
```

Ahora se ve que todas las conexiones de control y los túneles BFD son NAT a la IP y al puerto configurados, 192.168.20.2:12347. Además, la conexión a 172.16.1.34 es a un puerto completamente diferente del anunciado a vSmart por S30_Edge1. Consulte el puerto 50890.

3. Observe en la salida show sdwan control local properties de S30_Edge1 que la IP y el puerto anunciados son 172.16.1.34 y el puerto 60506.

```
S30_Edge1#show sdwan control local-properties
```

```
site-id                         30
domain-id                       1
protocol                        dtls
tls-port                        0
system-ip                       10.0.0.30
```

```
 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                         PUBLIC          PUBLIC PRIVATE         PRIVATE
INTERFACE                IPv4            PORT   IPv4            IPv6

-------------------------------------------------------------------------------------------------------------
GigabitEthernet1              172.16.1.34     60506  192.168.30.2    ::
```

Referencias

[Guía de diseño de SD-WAN de Cisco Catalyst]

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).