Configurar NAT estático para extensão TLOC para interoperabilidade com NAT simétrico

Contents

[Introdução](#)

[Recomendações](#)

[Componentes Utilizados](#)

[Problema](#)

[Topologia](#)

- [Condições](#)

[Identifique o problema](#)

- [Etapa 1. Verificar sessões BFD](#)
- [Etapa 2. Verificar o tipo de NAT](#)
- [Etapa 3. Verificar a configuração do NAT](#)
- [Etapa 4. Verificar o IP público e a porta](#)
- [Etapa 5. Verificar as conversões de NAT](#)
- [Etapa 6. Verificar o rastreamento FIA](#)
- [Etapa 7. Verificar os contadores BFD](#)

[Solução](#)

[Verificação](#)

[Referências](#)

Introdução

Este documento descreve a configuração do NAT estático em um TLOC Extension Router usando NAT Overload para trabalhar com pares por trás do NAT simétrico.

Recomendações

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida pelo software Cisco Catalyst (SD-WAN)
- Tradução de Endereço de Rede (NAT)
- Extensão TLOC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- C8000V versão 17.15.1a

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O Guia de design do Cisco Catalyst SD-WAN destaca que determinados tipos de conversão de endereço de rede (NAT) podem afetar a formação de conexões de controle e túneis BFD.

Os dois tipos de NAT que não funcionam juntos são NAT restrito de porta/endereço e NAT simétrico. Esses tipos de NAT exigem que as sessões sejam iniciadas a partir da rede interna para permitir o tráfego em cada porta. Isso significa que o tráfego externo não pode iniciar uma conexão com a rede interna sem uma solicitação interna anterior.

Os sites por trás de um NAT simétrico frequentemente têm dificuldades para estabelecer sessões BFD com sites pares. Isso é particularmente desafiador ao fazer o peering com um site usando a extensão TLOC atrás de NAT Overload (também conhecido como NAT restrito de porta/endereço).

Topologia

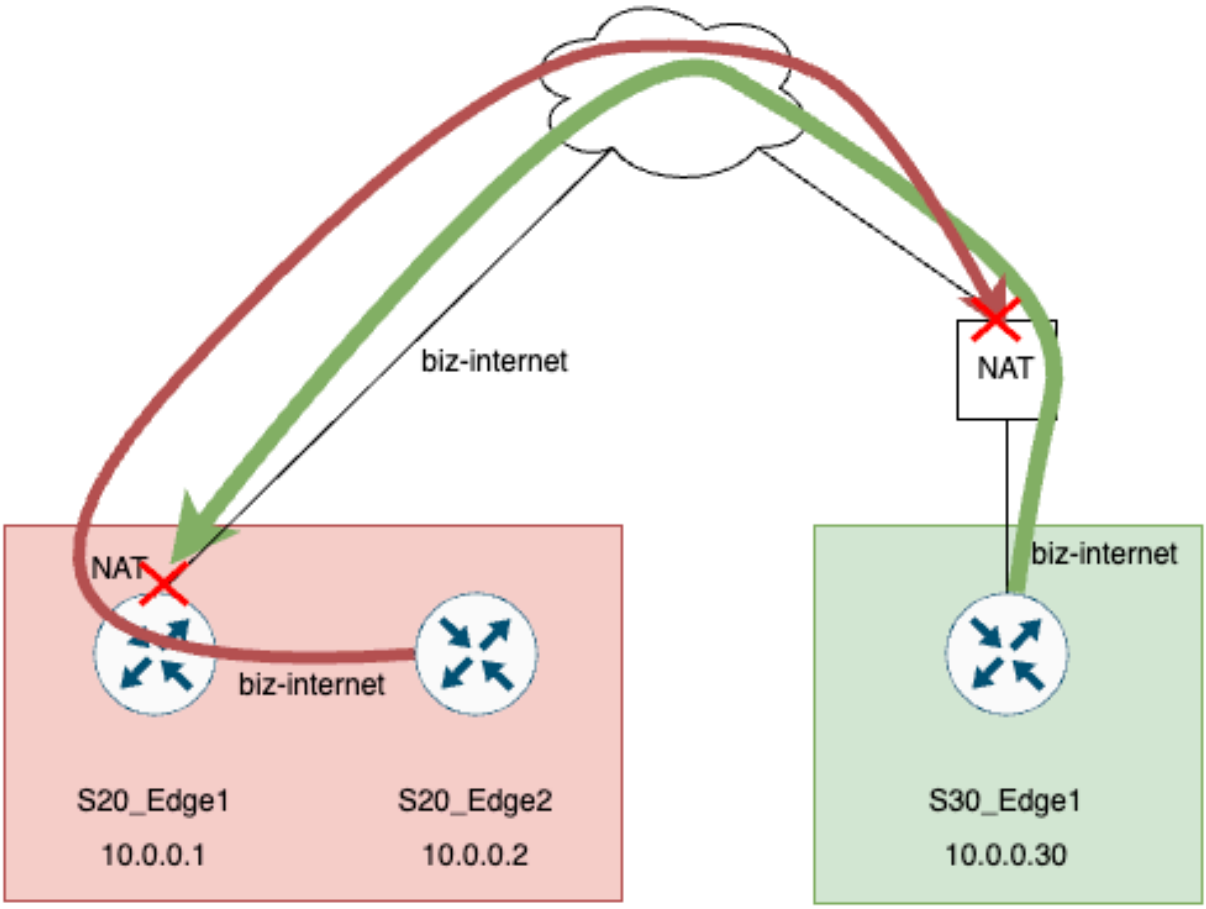
Condições

1. S30_Edge1 está atrás de um NAT simétrico

2. S20_Edge2 está atrás da extensão TLOC, onde S20_Edge1 está usando NAT Overload (PAT) para executar NAT nos fluxos de Edge2.

Isso faz com que as saudações de BFD sejam descartadas no dispositivo NAT simétrico e em S20_Edge1, pois nenhuma sessão está presente para a porta desconhecida do peer.

O dispositivo S20_Edge1 mostra a Eliminação de ACL implícita para essas saudações porque elas não correspondem a nenhuma sessão na tabela NAT.



Identifique o problema

Etapa 1. Verificar sessões BFD

A partir da saída do comando show sdwan bfd sessions em S30_Edge1, observa-se que a sessão BFD para S20_Edge2, 10.0.0.2, está inoperante.

```
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
```

Etapa 2. Verificar o tipo de NAT

Na parte inferior da saída, o NAT Tipo A é visto em S30_Edge1. Isso indica NAT simétrico. Observe também o IP público 172.16.1.34 e a porta 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    ::
```

Etapa 3. Verificar a configuração do NAT

A partir da topologia, sabe-se que S20_Edge2 está por trás da extensão TLOC. Neste ponto, podemos verificar a configuração PAT em S20_Edge1.

A configuração de sobrecarga de NAT já está presente em 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
```

Etapa 4. Verificar o IP público e a porta

Verifique a saída show sdwan control local properties em S20_Edge2 para ver o IP público e a porta 172.16.1.18 e a porta 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   ::
```

Etapa 5. Verificar as conversões de NAT

Agora, verifique as conversões de NAT no dispositivo S20_Edge1. Há apenas uma sessão NAT para o IP e a porta anunciados para S30_Edge1, IP 172.16.1.34 e a porta 31048. Considerando o que sabemos sobre o NAT simétrico, este não é o caso. Deve haver pelo menos uma porta diferente de 31048 (não uma porta SD-WAN padrão, como 12346), se não houver uma

combinação diferente de IP E porta.

```
 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
```

Etapa 6. Verificar o rastreamento FIA

Execute um rastreamento FIA apenas para verificar se os pacotes estão sendo descartados em S20_Edge1. Tenha em mente que o IP pode não ser o mesmo que o anunciado, mas, neste caso, para simplificar, é.

```
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 o pacote 8 para ver se este é o pacote suspeito.

```
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 o pacote de S30_Edge1.

Voltando à tabela NAT na etapa 6, podemos ver que não há sessão para esse pacote. Essa é a razão da queda.

Etapa 7. Verificar os contadores BFD

Pacotes BFD de S20_Edge2 não serão vistos em S30_Edge1 porque serão descartados fora do dispositivo, no dispositivo NAT. Os contadores BFD Tx/Rx podem ser verificados através do comando show sdwan tunnel statistics.

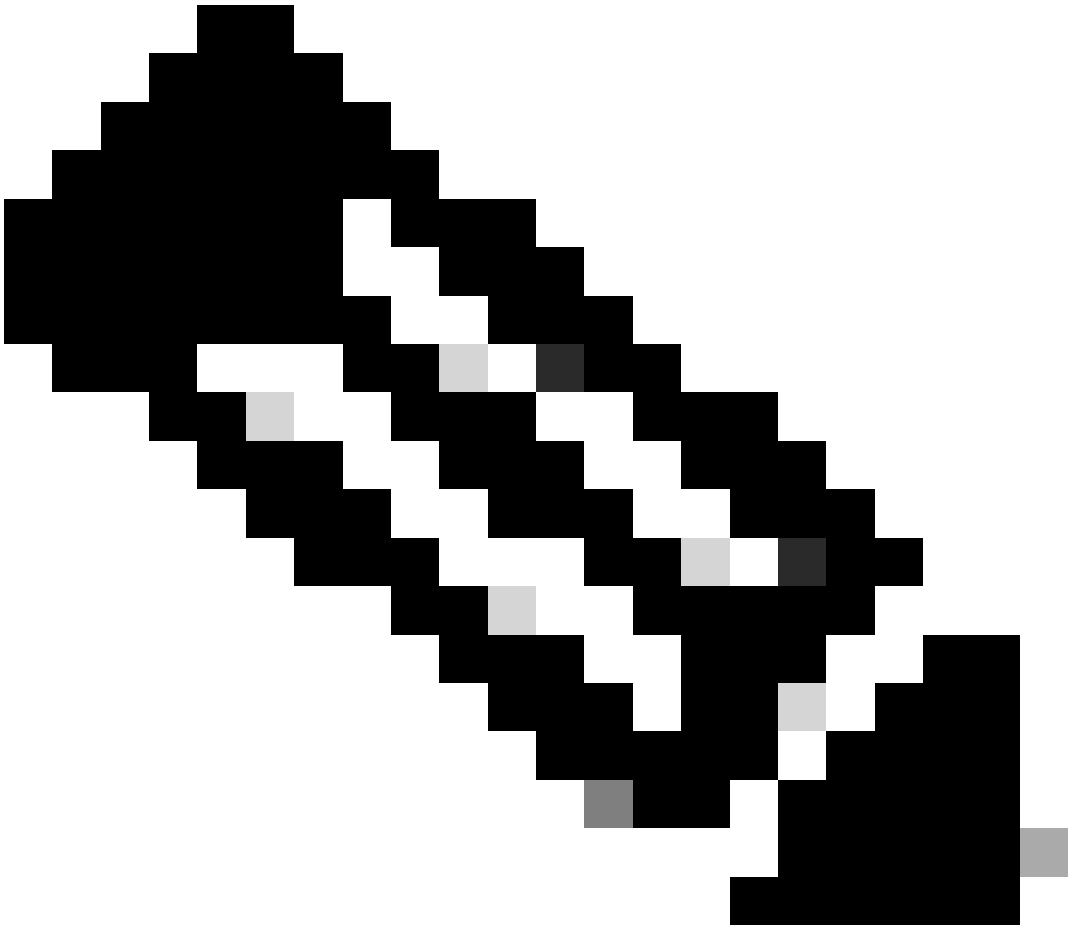
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts              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
```

Solução

Para resolver isso, um NAT estático pode ser configurado sobre a sobrecarga de NAT (PAT) em S20_Edge1 para NAT de todos os pacotes de controle e BFD para uma única combinação de IP/porta.

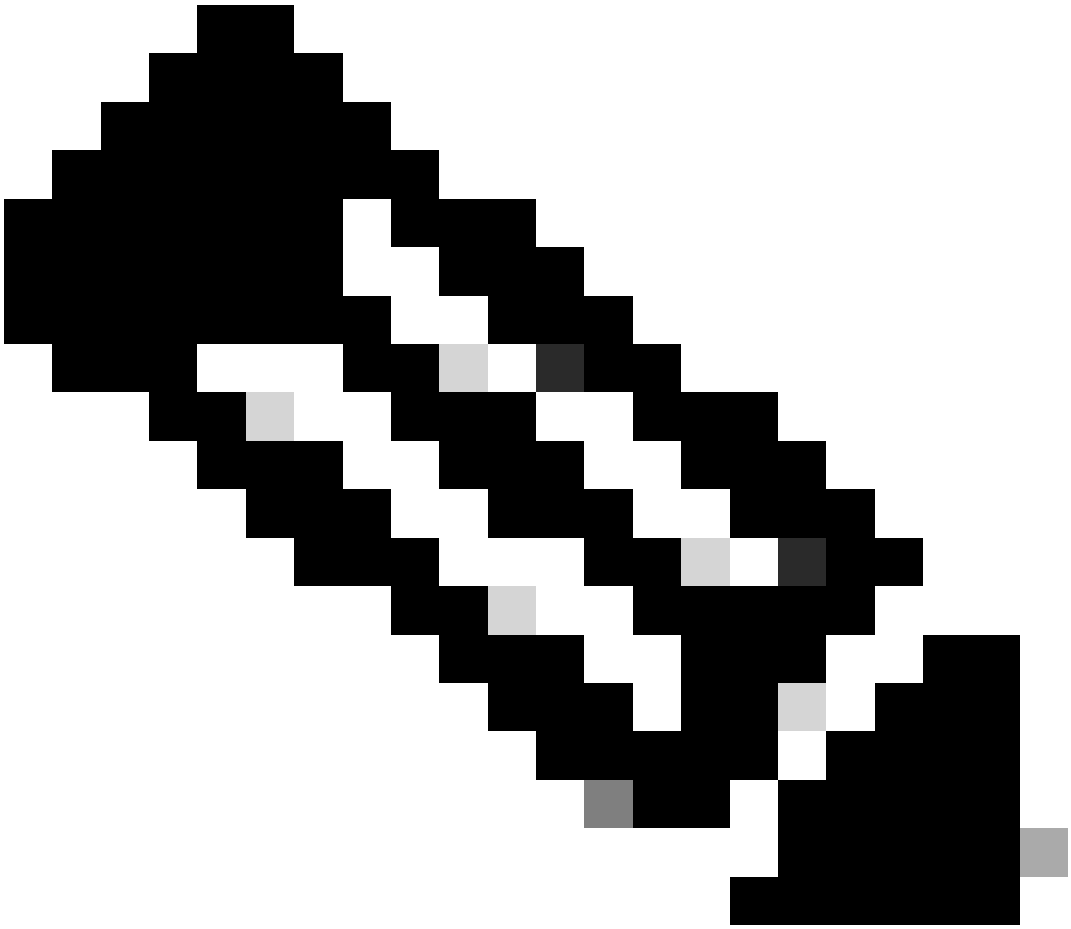
1. Primeiro, será necessário desativar o salto de porta nessa cor ou no sistema inteiro em S20_Edge2.

Um deslocamento de porta também será adicionado como uma prática recomendada para S20_Edge2 para que S20_Edge1 e S10_Edge2 não usem a mesma porta de origem para conexões de controle ou túneis BFD.



Note: Essa configuração pode ser executada por meio da CLI do roteador ou por meio de um modelo complementar da CLI do 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
```



Note: Certifique-se de que S20_Edge2 esteja usando a porta base 12347 após essa configuração, verificando show sdwan control local-properties. Se não estiver usando a porta base, use o comando clear sdwan control port-index para redefinir a porta de volta para a porta base. Isso evita que a porta seja alterada se estiver sendo executada em uma porta mais alta e, em seguida, é reinicializada mais tarde. O comando clear redefinirá as conexões de controle e os túneis bfd.

---

2. Configure o NAT estático em 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. Limpe as conversões de NAT em S20_Edge1.

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

Verificação

1. Verifique as sessões BFD em um dos peers.

```
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 as sessões de NAT em 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
```

Agora se vê que todas as conexões de controle e os Túneis BFD são NAT para o IP e a porta configurados, 192.168.20.2:12347. Além disso, a conexão com 172.16.1.34 é para uma porta completamente diferente da anunciada para vSmart por S30_Edge1. Consulte a porta 50890.

3. Observe na saída show sdwan control local properties de S30_Edge1 que o IP e a porta anunciados são 172.16.1.34 e a porta 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    ::
```

Referências

[Guia de design do Cisco Catalyst SD-WAN]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.