Statische NAT configureren voor TLOC-uitbreiding voor interoperabiliteit met Symmetric NAT

Inhoud

Inleiding

Dit document beschrijft het configureren van statische NAT op een TLOC Extension Router met behulp van NAT Overload om te werken met collega's achter Symmetric NAT.

Aanbevelingen

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Network Address Translation (NAT)
- TLOC-extensie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- C8000V versie 17.15.1a

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

De Cisco Catalyst SD-WAN Design Guide benadrukt dat bepaalde typen Network Address Translation (NAT) de vorming van besturingsverbindingen en BFD-tunnels kunnen beïnvloeden.

De twee typen NAT die niet samenwerken zijn Port/Address Restricted NAT en Symmetric NAT. Deze NAT-typen vereisen dat sessies worden gestart vanuit het interne netwerk om verkeer op elke poort mogelijk te maken. Dit betekent dat extern verkeer geen verbinding met het interne netwerk kan maken zonder een voorafgaand verzoek van binnenuit.

Sites achter een symmetrische NAT ondervinden vaak problemen bij het opzetten van BFD-sessies met peer-sites. Dit is met name een uitdaging bij het peering met een site met behulp van TLOC Extension achter NAT Overload (ook bekend als Port / Address Restricted NAT).

Topologie

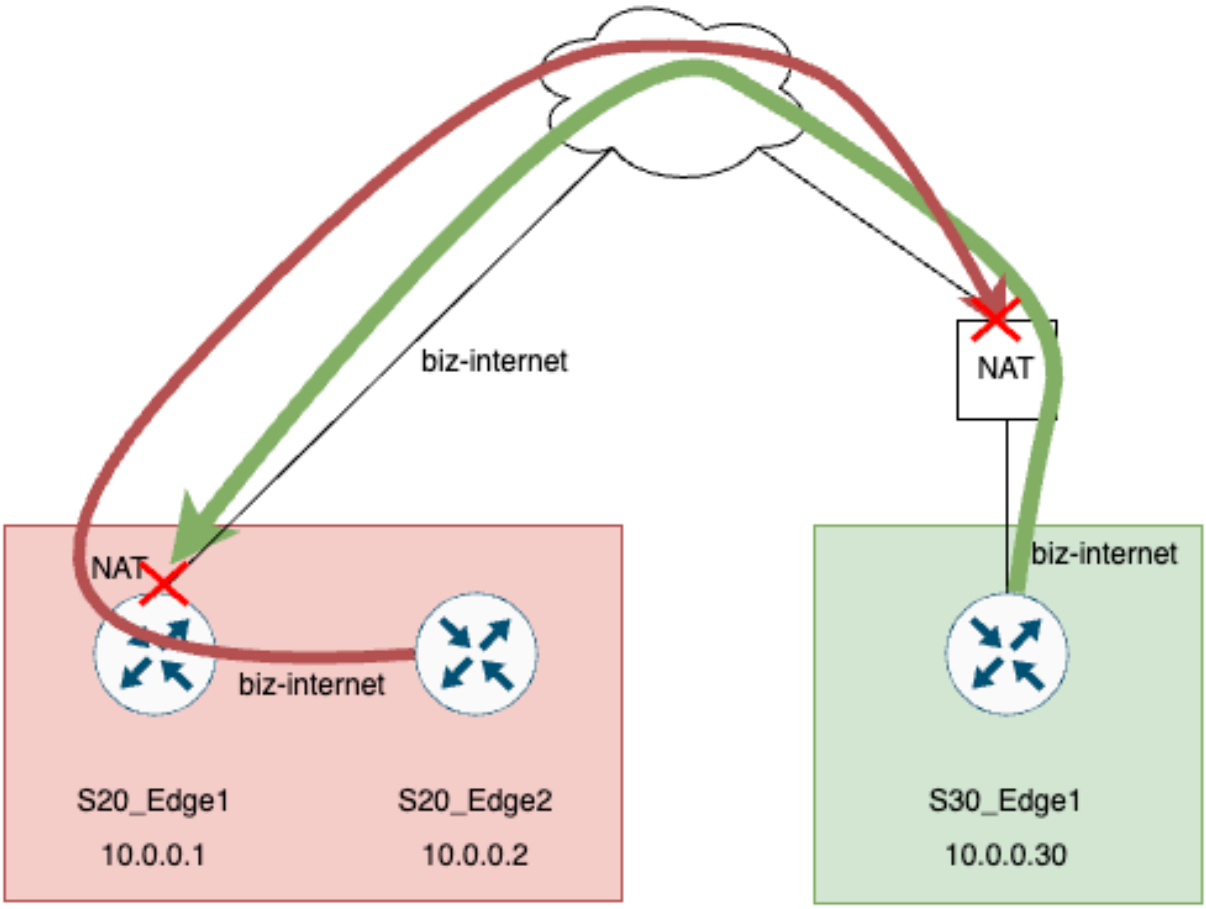
Voorwaarden

1. S30_Edge1 bevindt zich achter een symmetrische NAT

2. S20_Edge2 bevindt zich achter de TLOC-extensie waarbij S20_Edge1 NAT Overload (PAT) gebruikt om de NAT-stromen van Edge2 uit te voeren.

Dit resulteert in de BFD-hellos die op het Symmetric NAT-apparaat en de S20_Edge1 worden gedropt omdat er geen sessie aanwezig is voor de onbekende poort van de peer.

Het S20_Edge1-apparaat toont Implicit ACL Drop voor deze hellos omdat ze niet overeenkomen met een sessie in de NAT-tabel.



Identificeer het probleem

Stap 1. BFD-sessies controleren

Uit de show sdwan bfd sessies output op S30_Edge1, wordt gezien dat de BFD sessie naar S20_Edge2, 10.0.0.2 is gedaald.

```
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
```

Stap 2. Controleer het NAT-type

Aan de onderkant van de uitgang is de NAT Type A te zien op S30_Edge1. Dit duidt op Symmetric NAT. Let ook op de openbare IP 172.16.1.34 en poort 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    ::
```

Stap 3. Controleer de NAT-configuratie

Uit de topologie is bekend dat S20_Edge2 achter de TLOC-extensie zit. Op dit punt kunnen we controleren op de PAT-configuratie op de S20_Edge1.

NAT-overbelastingsconfiguratie is al aanwezig op 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
```

Stap 4. Controleer de openbare IP- en poort

Selecteer show sdwan control local properties output op S20_Edge2 om het publieke IP en poort 172.16.1.18 en poort 5063 te zien

```
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   ::
```

Stap 5. Controleer de NAT-vertalingen

Controleer nu de NAT-vertalingen op het S20_Edge1-apparaat. Er is alleen een NAT-sessie naar de geadverteerde IP- en poort voor S30_Edge1, IP 172.16.1.34 en poort 31048. Gezien wat we weten over symmetrische NAT, is dit niet het geval. Er moet ten minste één andere poort zijn dan 31048 (geen standaard SD-WAN-poort zoals 12346), zo niet een andere IP AND-poortcombinatie.

```
 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
```

Stap 6. FIA-tracering controleren

Voer een FIA-trace uit om te controleren of pakketten worden gedropt op S20_Edge1. Houd er rekening mee dat het IP-adres misschien niet hetzelfde is als het geadverteerde IP-adres, maar in dit geval voor de eenvoud wel.

```
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)
```

Controleer pakket 8 om te zien of dit het vermoedelijke pakket is.

```
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
```

Dit lijkt het pakket van S30_Edge1 te zijn.

Als we terugkijken op de NAT-tabel in stap 6, kunnen we zien dat er geen sessie is voor dit pakket. Dat is de reden voor de daling.

Stap 7. BFD-tellers controleren

BFD-pakketten van S20_Edge2 worden niet gezien op S30_Edge1 omdat ze buiten het apparaat, op het NAT-apparaat, worden gedropt. De BFD Tx/Rx-tellers kunnen worden gecontroleerd via de opdracht show sdwan tunnel statistics.

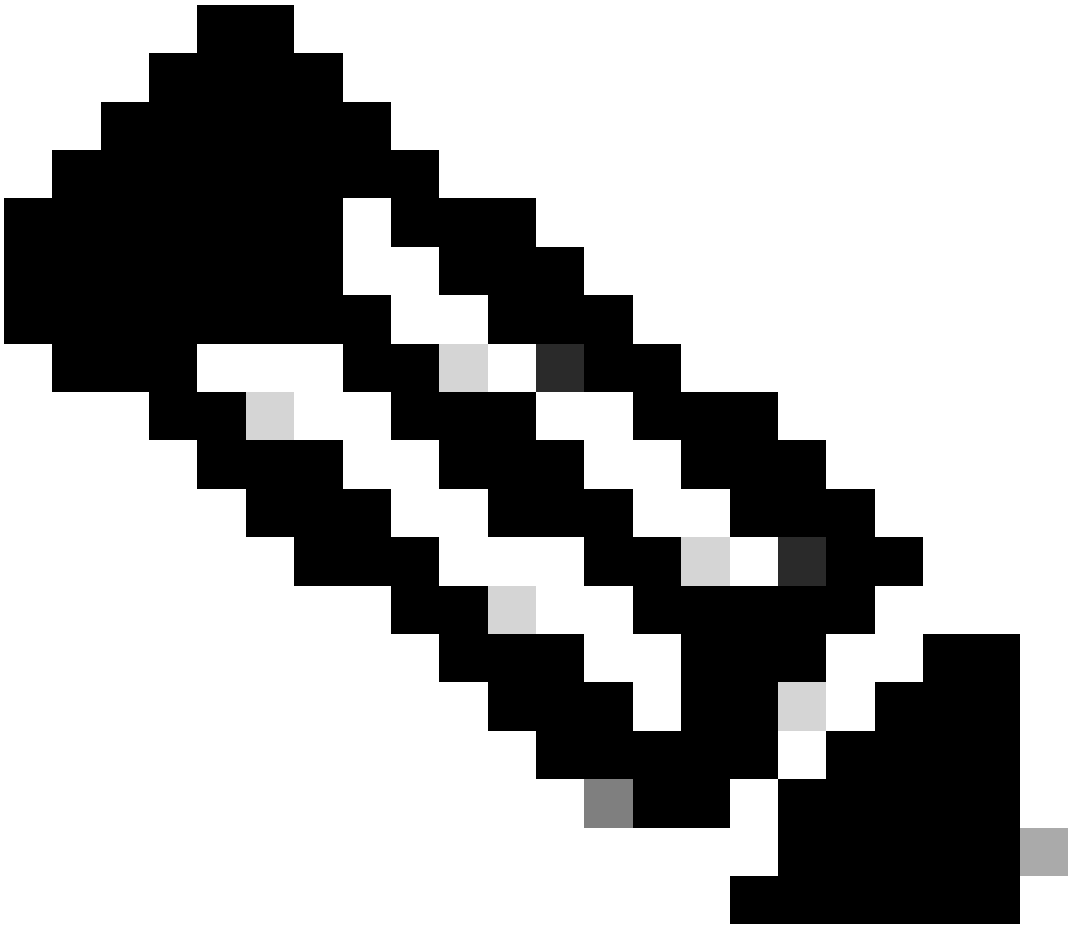
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts             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

Oplossing

Om dit op te lossen, kan een statische NAT worden geconfigureerd bovenop de NAT Overload (PAT) op S20_Edge1 naar NAT All Control en BFD Packets naar een enkele IP/Port-combinatie.

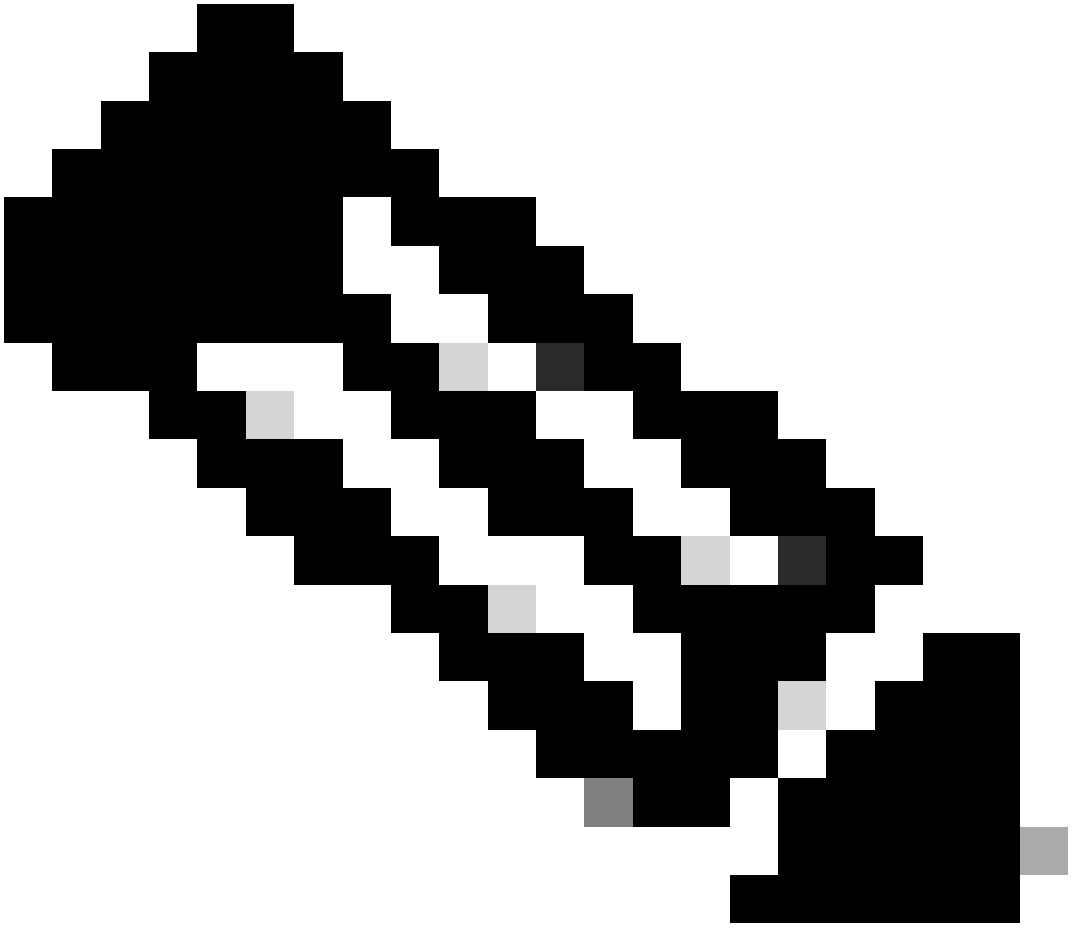
1. Ten eerste moet poorthopping op deze kleur worden uitgeschakeld of voor het hele systeem op S20_Edge2.

Een poortoffset wordt ook toegevoegd als een best practice voor S20_Edge2, zodat S20_Edge1 en S10_Edge2 niet dezelfde bronpoort gebruiken voor besturingsverbindingen of BFD-tunnels.



> Opmerking: deze configuratie kan worden uitgevoerd via de CLI van de router of via een vManage CLI-invoegtoepassing.

```
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
```



Opmerking: controleer of S20_Edge2 na deze configuratie de basispoort 12347 gebruikt door lokale eigenschappen van de sdwan-besturingselementen weer te geven. Als de basispoort niet wordt gebruikt, gebruikt u de opdracht Poort-index van controlepoort wissen om de poort terug te zetten naar de basispoort. Dit voorkomt dat de poort verandert als deze op een hogere poort wordt uitgevoerd en later opnieuw wordt opgestart. Met de opdracht Clear worden de besturingsverbindingen en de BFD-tunnels gereset.

---

2. Configureer de statische NAT op 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. Wis de NAT-vertalingen op S20_Edge1.

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

Verificatie

1. Controleer de BFD-sessies op een van de 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. Controleer de NAT-sessies op 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
```

Nu wordt gezien dat alle besturingsverbindingen en BFD-tunnels NAT zijn voor de geconfigureerde IP en poort, 192.168.20.2:12347. Ook de verbinding met 172.16.1.34 is naar een volledig andere poort dan geadverteerd aan vSmart door S30_Edge1. Zie poort 50890.

3. Merk op in de show sdwan control local properties output van S30_Edge1 dat de geadverteerde IP en poort 172.16.1.34 en poort 60506 zijn.

```
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    ::
```

Referenties

[Cisco Catalyst SD-WAN-ontwerphandleiding]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.