Configurer la NAT statique pour l'extension TLOC pour l'interopérabilité avec la NAT symétrique

Table des matières

Introduction

Ce document décrit la configuration de la NAT statique sur un routeur d'extension TLOC utilisant la surcharge NAT pour travailler avec des homologues derrière la NAT symétrique.

Recommandations

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco Catalyst
- Traduction d'adresses réseau (NAT)
- Extension TLOC

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- C8000V version 17.15.1a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

Le Guide de conception SD-WAN de Cisco Catalyst souligne que certains types de traduction d'adresses de réseau (NAT) peuvent avoir un impact sur la formation de connexions de contrôle et de tunnels BFD.

Les deux types de NAT qui ne fonctionnent pas ensemble sont NAT limitée aux ports/adresses et NAT symétrique. Ces types de NAT nécessitent que les sessions soient lancées à partir du réseau interne pour autoriser le trafic sur chaque port. Cela signifie que le trafic externe ne peut pas initier une connexion au réseau interne sans une demande préalable de l'intérieur.

Les sites derrière une NAT symétrique rencontrent fréquemment des difficultés à établir des sessions BFD avec des sites homologues. Cela est particulièrement difficile lors de l'appairage avec un site utilisant l'extension TLOC derrière la surcharge NAT (également connue sous le nom de NAT avec restriction de port/adresse).

Topologie

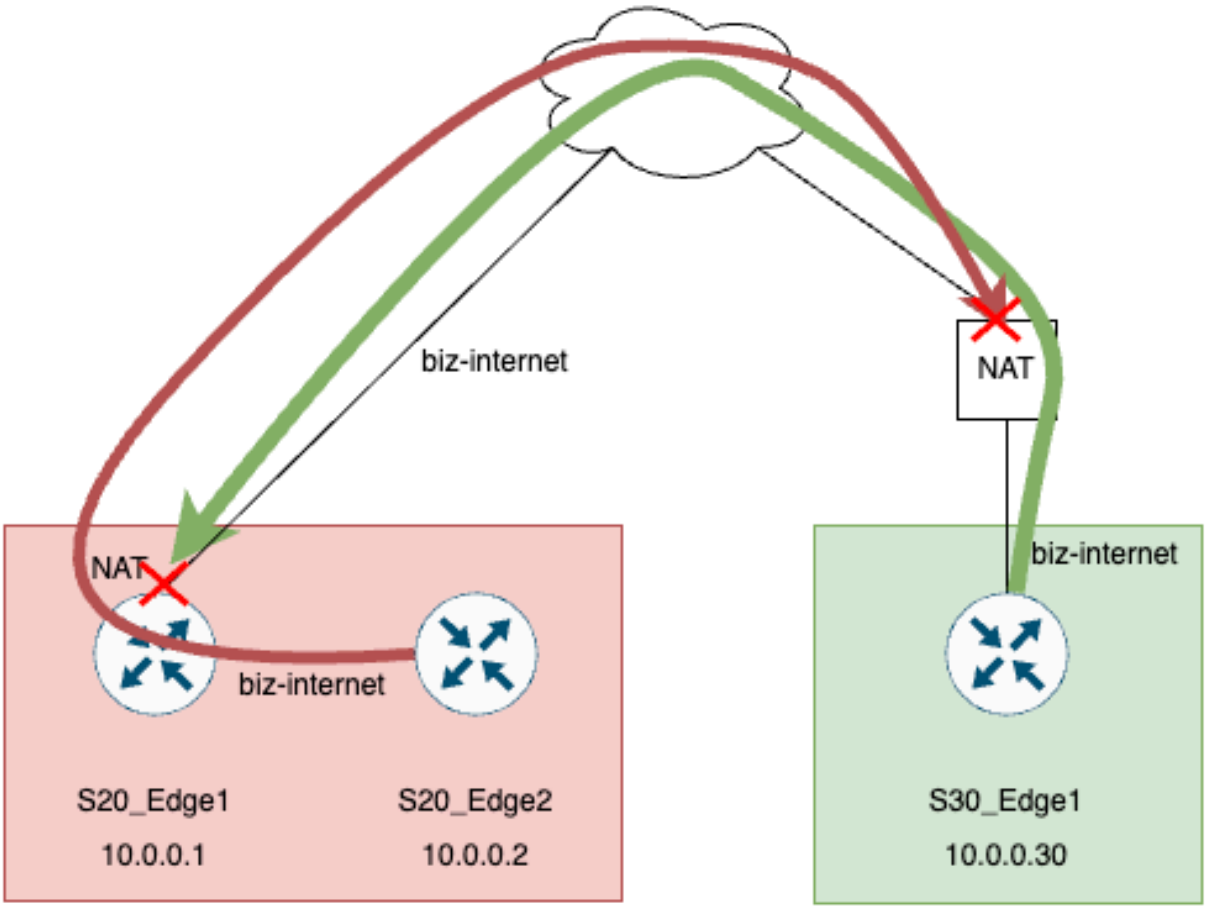
Conditions

1. S30_Edge1 se trouve derrière une NAT symétrique

2. S20_Edge2 se trouve derrière l'extension TLOC, où S20_Edge1 utilise la surcharge NAT (PAT) pour NAT les flux à partir d'Edge2.

Cela entraîne l'abandon des messages Hello BFD sur le périphérique NAT symétrique et sur S20_Edge1 en raison de l'absence de session pour le port inconnu de l'homologue.

Le périphérique S20_Edge1 affiche une suppression de liste de contrôle d'accès implicite pour ces paquets Hello, car ils ne correspondent à aucune session dans la table NAT.



Identification du problème

Étape 1 : vérification des sessions BFD

D'après le résultat de la commande show sdwan bfd sessions sur S30_Edge1, il apparaît que la session BFD vers S20_Edge2, 10.0.0.2 est inactive.

```
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
```

Étape 2. Vérification du type NAT

Au bas de la sortie, le type A de NAT est visible sur S30_Edge1. Ceci indique une NAT symétrique. Notez également l'adresse IP publique 172.16.1.34 et le port 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    ::
```

Étape 3 : vérification de la configuration NAT

La topologie indique que S20_Edge2 se trouve derrière l'extension TLOC. À ce stade, nous pouvons vérifier la configuration PAT sur S20_Edge1.

La configuration de surcharge NAT est déjà présente sur 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
```

Étape 4. Vérification de l’adresse IP et du port publics

Vérifiez la sortie show sdwan control local properties sur S20_Edge2 pour voir l'IP publique et le port 172.16.1.18 et le port 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   ::
```

Étape 5. Vérification des traductions NAT

Vérifiez maintenant les traductions NAT sur le périphérique S20_Edge1. Il n’y a qu’une session NAT vers l’IP et le port annoncés pour S30_Edge1, l’IP 172.16.1.34 et le port 31048. Compte tenu de ce que nous savons de la NAT symétrique, ce n’est pas le cas. Il doit y avoir au moins un port différent de 31048 (pas un port SD-WAN standard comme 12346), sinon une combinaison IP ET

port différente.

```
 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
```

Étape 6. Vérifier la trace FIA

Exécutez une trace FIA uniquement pour vérifier que les paquets sont abandonnés sur S20_Edge1. Gardez à l'esprit que l'adresse IP ne doit pas être la même que celle annoncée, mais dans ce cas, pour des raisons de simplicité, elle l'est.

```
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)
```

Vérifiez le paquet 8 pour voir s'il s'agit du paquet suspecté.

```
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
```

Il semble que ce soit le paquet de S30_Edge1.

En vérifiant à nouveau dans la table NAT à l'étape 6, nous pouvons voir qu'il n'y a pas de session pour ce paquet. C'est la raison de cette baisse.

Étape 7. Vérification des compteurs BFD

Les paquets BFD de S20_Edge2 ne sont pas visibles sur S30_Edge1 car ils sont abandonnés en dehors du périphérique, sur le périphérique NAT. Les compteurs BFD Tx/Rx peuvent être vérifiés via la commande show sdwan tunnel statistics.

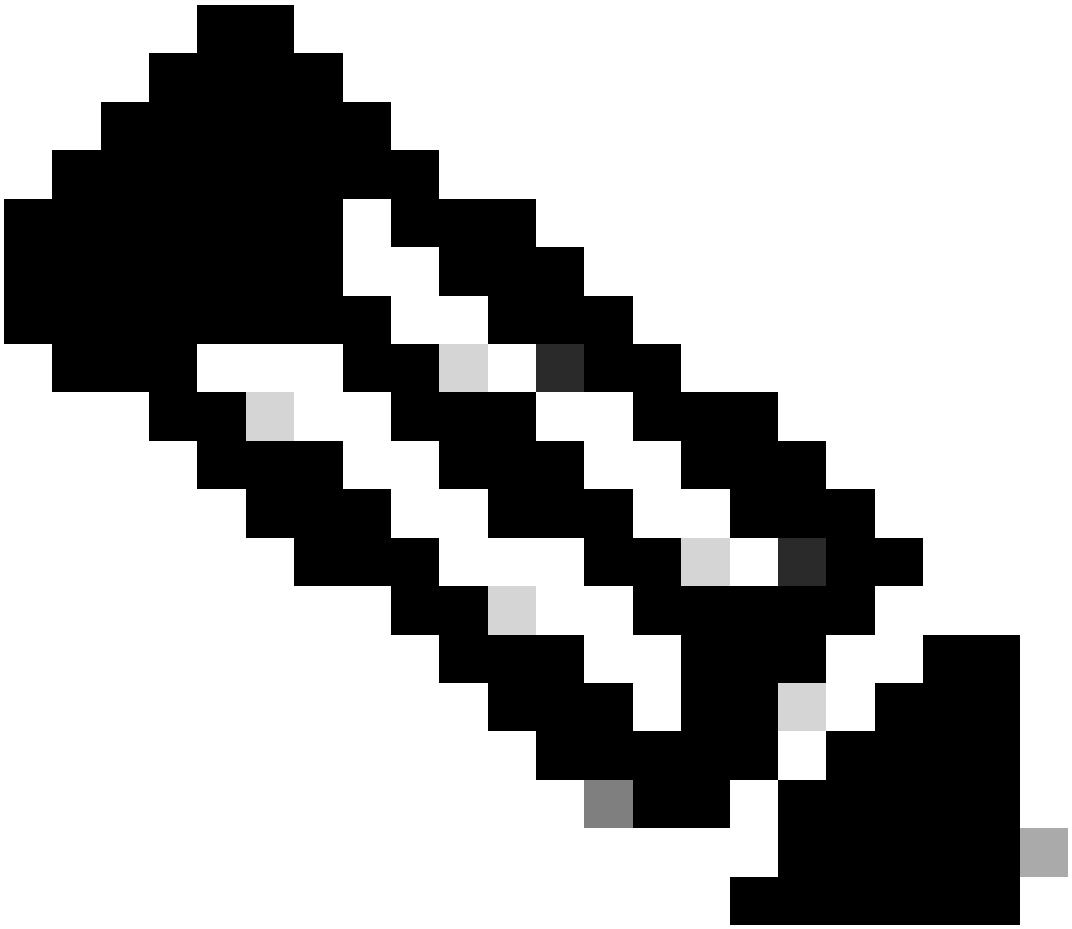
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts             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

Solution

Pour résoudre ce problème, une NAT statique peut être configurée en plus de la surcharge NAT (PAT) sur S20_Edge1 pour NAT tous les paquets de contrôle et BFD sur une seule combinaison IP/port.

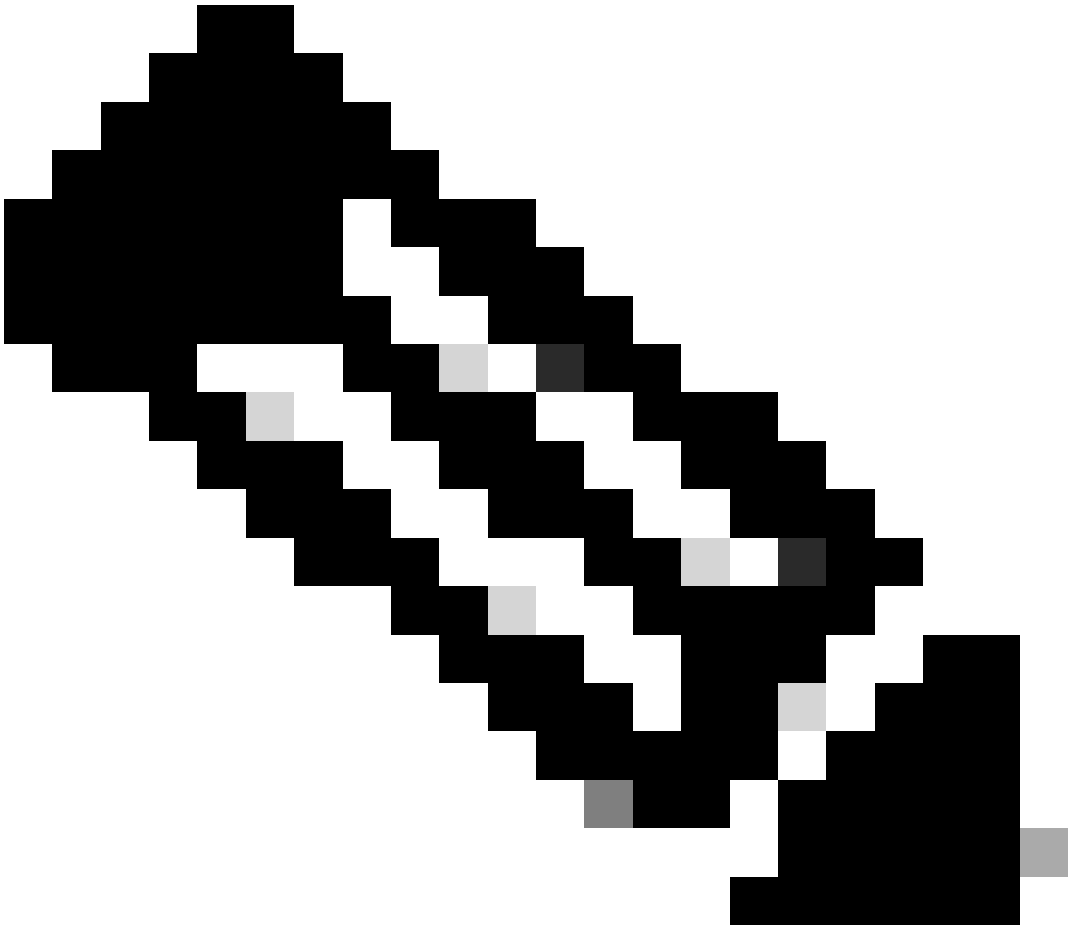
1. Tout d'abord, il peut être nécessaire de désactiver le saut de port sur cette couleur, ou à l'échelle du système sur S20_Edge2.

Il est également recommandé d'ajouter un décalage de port pour S20_Edge2 afin que S20_Edge1 et S10_Edge2 n'utilisent pas le même port source pour les connexions de contrôle ou les tunnels BFD.



> Remarque : Cette configuration peut être effectuée via l'interface de ligne de commande du routeur ou via un modèle vManage CLI Add-On.

```
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
```



Remarque : Assurez-vous que S20_Edge2 utilise le port de base 12347 après cette configuration en vérifiant show sdwan control local-properties. S'il n'utilise pas le port de base, utilisez la commande clear sdwan control port-index pour réinitialiser le port au port de base. Cela empêche le port de changer s'il était exécuté sur un port plus élevé, puis redémarre plus tard. La commande clear réinitialise les connexions de contrôle et les tunnels bfd.

---

2. Configurez la fonction NAT statique sur 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. Effacez les traductions NAT sur S20_Edge1.

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

Vérification

1. Vérifiez les sessions BFD sur l'un des homologues.

```
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. Vérifiez les sessions NAT sur 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
```

Maintenant, il est vu que toutes les connexions de contrôle et les tunnels BFD sont NAT vers l'IP et le port configurés, 192.168.20.2:12347. En outre, la connexion à 172.16.1.34 est vers un port complètement différent de celui annoncé à vSmart par S30_Edge1. Voir port 50890.

3. Notez dans la sortie show sdwan control local properties de S30_Edge1 que l'adresse IP et le port annoncés sont 172.16.1.34 et le port 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    ::
```

Références

[Guide de conception SD-WAN de Cisco Catalyst]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.