Configurazione di NAT statico per estensione TLOC per l'interoperabilità con NAT simmetrico

Sommario

Introduzione

In questo documento viene descritto come configurare un NAT statico su un router di estensione TLOC usando l'overload NAT per funzionare con i peer dietro un NAT simmetrico.

Consigli

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- C800V versione 17.15.1a

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

La Guida alla progettazione di Cisco Catalyst SD-WAN sottolinea come alcuni tipi di NAT (Network Address Translation) possano influire sulla formazione delle connessioni di controllo e dei tunnel BFD.

I due tipi di NAT che non funzionano insieme sono NAT con restrizioni di porta/indirizzo e NAT simmetrico. Questi tipi di NAT richiedono l'avvio di sessioni dalla rete interna per consentire il traffico su ciascuna porta. Questo significa che il traffico esterno non può avviare una connessione alla rete interna senza una precedente richiesta da parte dell'interno.

I siti che si trovano dietro un NAT simmetrico incontrano spesso difficoltà a stabilire sessioni BFD con siti peer. Ciò è particolarmente difficile quando si esegue il peering con un sito che utilizza l'estensione TLOC dietro l'overload NAT (nota anche come NAT con restrizioni di porta/indirizzo).

Topologia

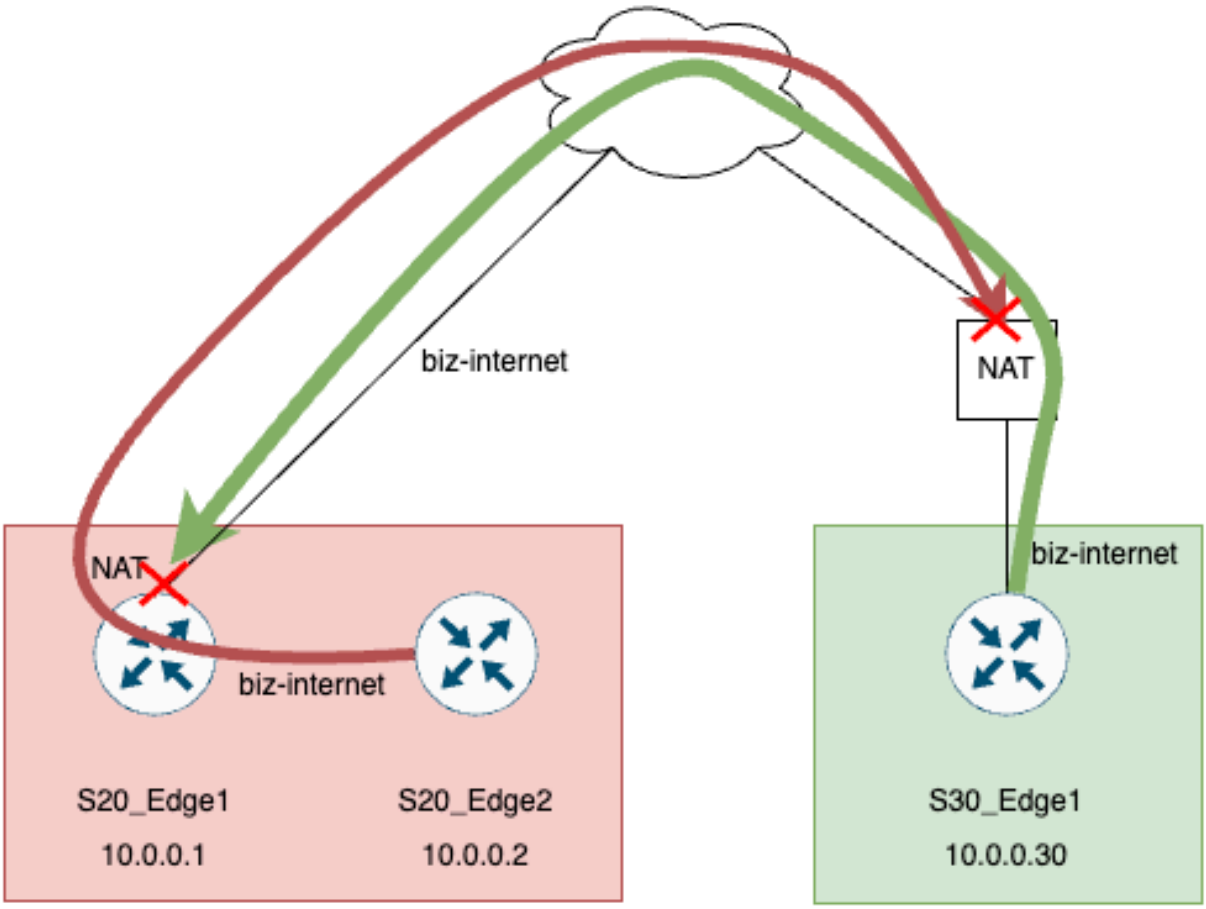
Condizioni

1. S30_Edge1 è dietro un NAT simmetrico

2. S20_Edge2 si trova dietro l'estensione TLOC, dove S20_Edge1 sta utilizzando NAT Overload (PAT) per NAT i flussi da Edge2.

Il risultato è che gli helper BFD vengono scartati sul dispositivo NAT simmetrico e sul S20_Edge1 perché non è presente alcuna sessione per la porta sconosciuta dal peer.

Il dispositivo S20_Edge1 mostra la perdita implicita di ACL per questi hellos perché non corrispondono ad alcuna sessione nella tabella NAT.



Identificazione del problema

Passaggio 1. Controllare le sessioni BFD

Dall'output delle sessioni bfd show sdwan su S30_Edge1, si rileva che la sessione BFD su S20_Edge2, 10.0.0.2 è inattiva.

```
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
```

Passaggio 2. Controllare il tipo NAT

Nella parte inferiore dell'output, il NAT di tipo A è visibile su S30_Edge1. Ciò indica un NAT simmetrico. Notare anche le porte pubbliche IP 172.16.1.34 e 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    ::
```

Passaggio 3. Controllare la configurazione NAT

Dalla topologia è noto che S20_Edge2 si trova dietro l'estensione TLOC. A questo punto è possibile verificare la configurazione PAT su S20_Edge1.

La configurazione di overload NAT è già presente in 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
```

Passaggio 4. Controllare l'indirizzo IP e la porta pubblici

Selezionare show sdwan control local properties output su S20_Edge2 per visualizzare l'IP pubblico, la porta 172.16.1.18 e la 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   ::
```

Passaggio 5. Controllare le traduzioni NAT

Controllare le conversioni NAT sul dispositivo S20_Edge1. Esiste solo una sessione NAT per l'IP e la porta annunciati per S30_Edge1, IP 172.16.1.34 e porta 31048. Considerando le informazioni di cui disponiamo su NAT simmetrico, non è questo il caso. Deve essere presente almeno una porta diversa da 31048 (non una porta SD-WAN standard come 12346), se non una diversa

combinazione di porte IP AND.

```
 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
```

Passaggio 6. Controllare la traccia FIA

Eseguire una traccia FIA solo per verificare che i pacchetti vengano scartati su S20_Edge1. Tenere presente che l'indirizzo IP non deve essere necessariamente lo stesso di quello pubblicizzato, ma in questo caso, per semplicità, lo è.

```
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)
```

Controllare il pacchetto 8 per verificare se si tratta del pacchetto sospetto.

```
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
```

Sembra essere il pacchetto da S30_Edge1.

Facendo un nuovo controllo sulla tabella NAT nel passaggio 6, si osserverà che non esiste una sessione per questo pacchetto. Questa è la ragione della caduta.

Passaggio 7. Controllare i contatori BFD

I pacchetti BFD da S20_Edge2 non vengono visualizzati in S30_Edge1 perché vengono scartati all'esterno del dispositivo, sul dispositivo NAT. I contatori BFD Tx/Rx possono essere controllati con il comando show sdwan tunnel statistics.

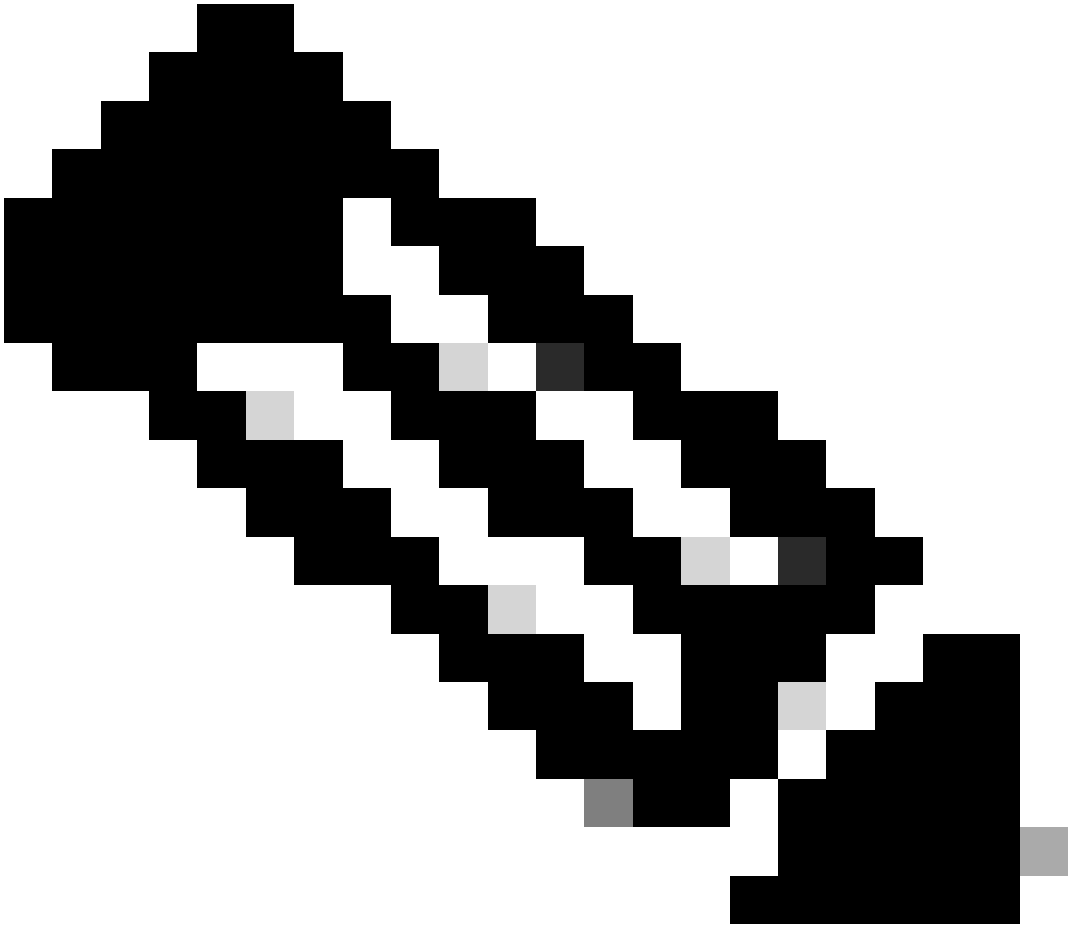
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
 system-ip            10.0.0.2
 local-color          biz-internet
 remote-color         biz-internet
 tunnel-mtu           1438
 tx_pkts              10
 tx_octets            1060
 rx_pkts             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

Soluzione

Per risolvere questo problema, è possibile configurare un NAT statico in cima al NAT Overload (PAT) su S20_Edge1 in modo che NAT tutti i pacchetti Control e BFD siano configurati su una singola combinazione IP/porta.

1. In primo luogo, è necessario disabilitare la port-hopping su questo colore, o a livello di sistema su S20_Edge2.

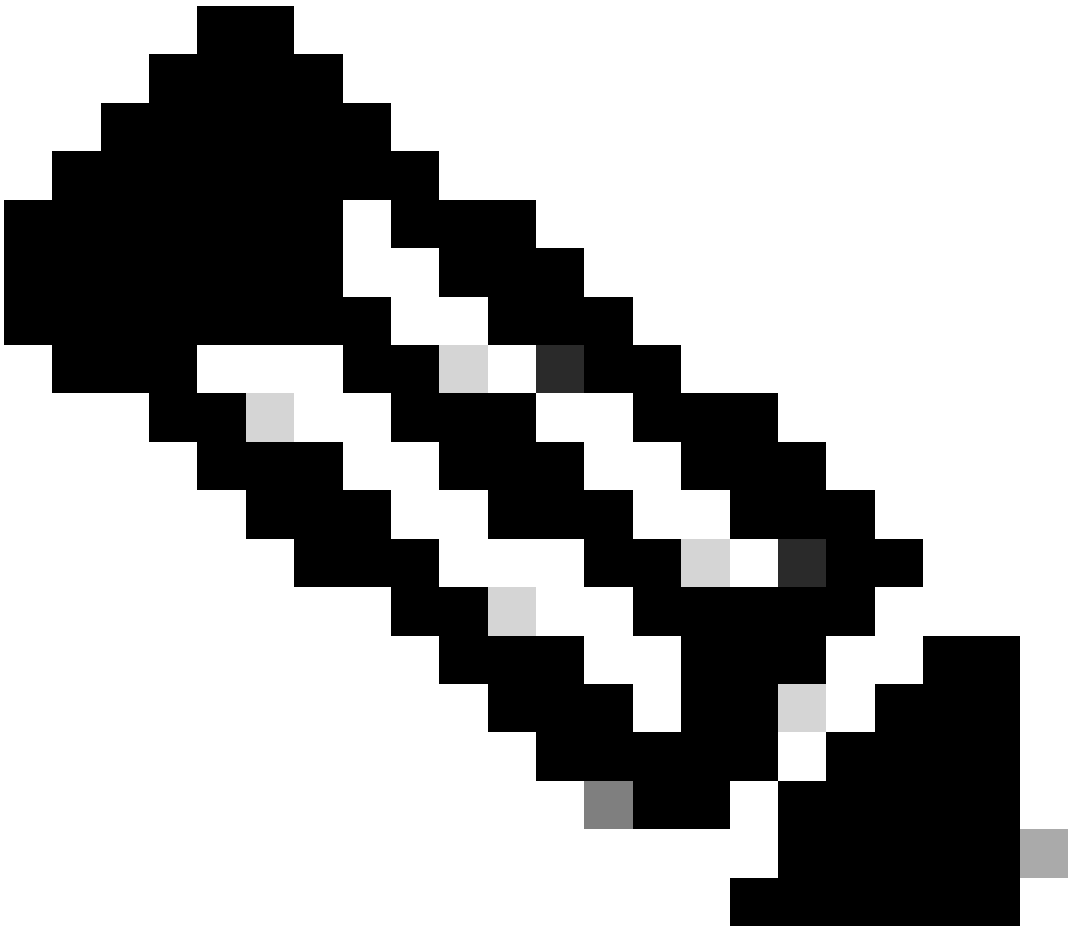
È inoltre consigliabile aggiungere un offset porta per S20_Edge2, in modo che S20_Edge1 e S10_Edge2 non utilizzino la stessa porta di origine per le connessioni di controllo o i tunnel BFD.



> Nota: Questa configurazione può essere eseguita tramite la CLI del router o tramite un modello aggiuntivo di vManage CLI.

```
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: Dopo questa configurazione, verificare che S20_Edge2 stia utilizzando la porta base 12347 selezionando show sdwan control local-properties. Se non si utilizza la porta base, usare il comando clear sdwan control port-index per ripristinare la porta base. In questo modo, la porta non può essere modificata se è in esecuzione su una porta superiore e viene riavviata in seguito. Il comando clear reimposta le connessioni di controllo e i tunnel bfd.

---

2. Configurare il NAT statico su 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. Cancellare le traduzioni NAT su S20_Edge1.

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

Verifica

1. Controllare le sessioni BFD su uno dei peer.

```
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. Controllare le sessioni NAT su 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
```

Ora si è visto che tutte le connessioni di controllo e i tunnel BFD sono NAT per l'IP e la porta configurati, 192.168.20.2:12347. Anche la connessione a 172.16.1.34 è a una porta completamente diversa da quella annunciata a vSmart da S30_Edge1. Vedere la porta 50890.

3. Notare nell'output show sdwan control local properties restituito da S30_Edge1 che l'IP e la porta annunciati sono 172.16.1.34 e 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    ::
```

Riferimenti

[Guida alla progettazione di Cisco Catalyst SD-WAN]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).