Configurazione del tunnel di rete tra Cisco Secure Access e il router IOS XE con ECMP con BGP

Sommario

Introduzione

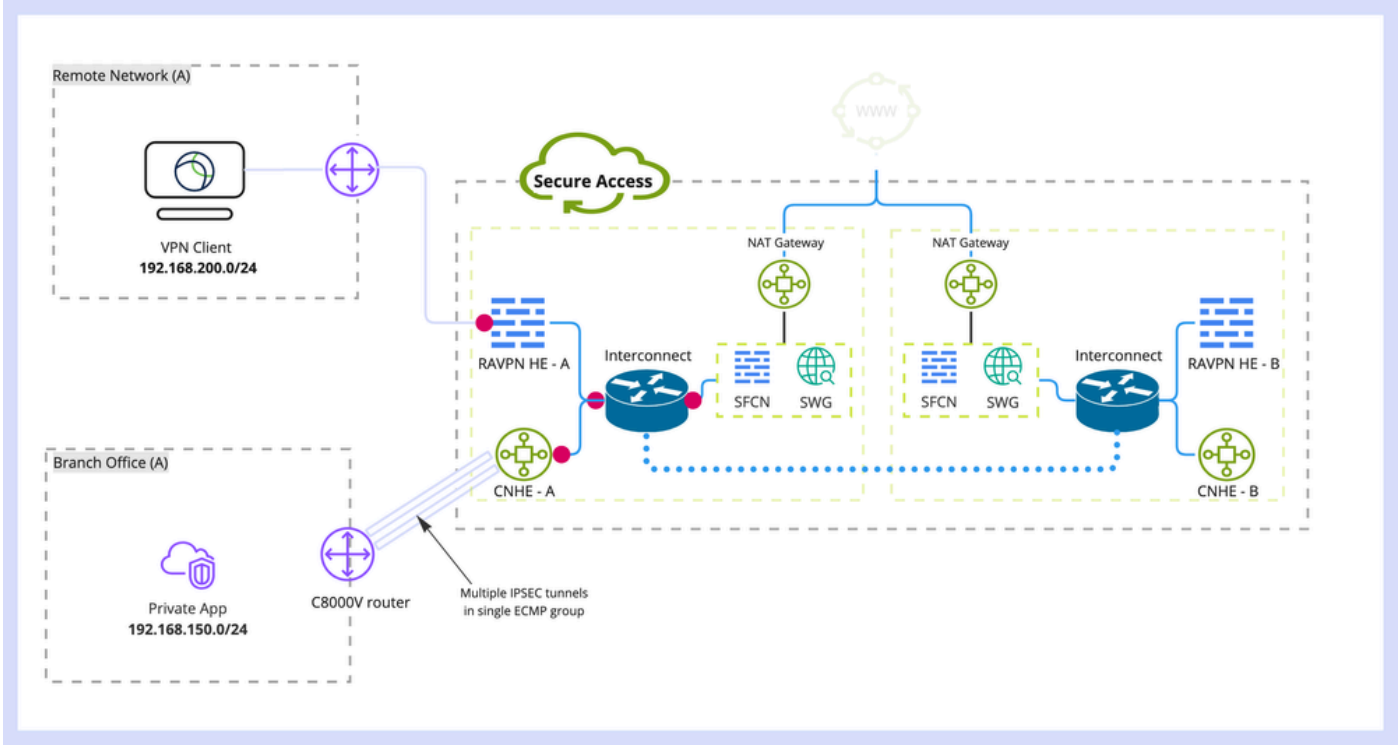
In questo documento viene descritto come configurare e risolvere i problemi relativi al tunnel VPN IPSec tra Cisco Secure Access e Cisco IOS XE con BGP e ECMP.

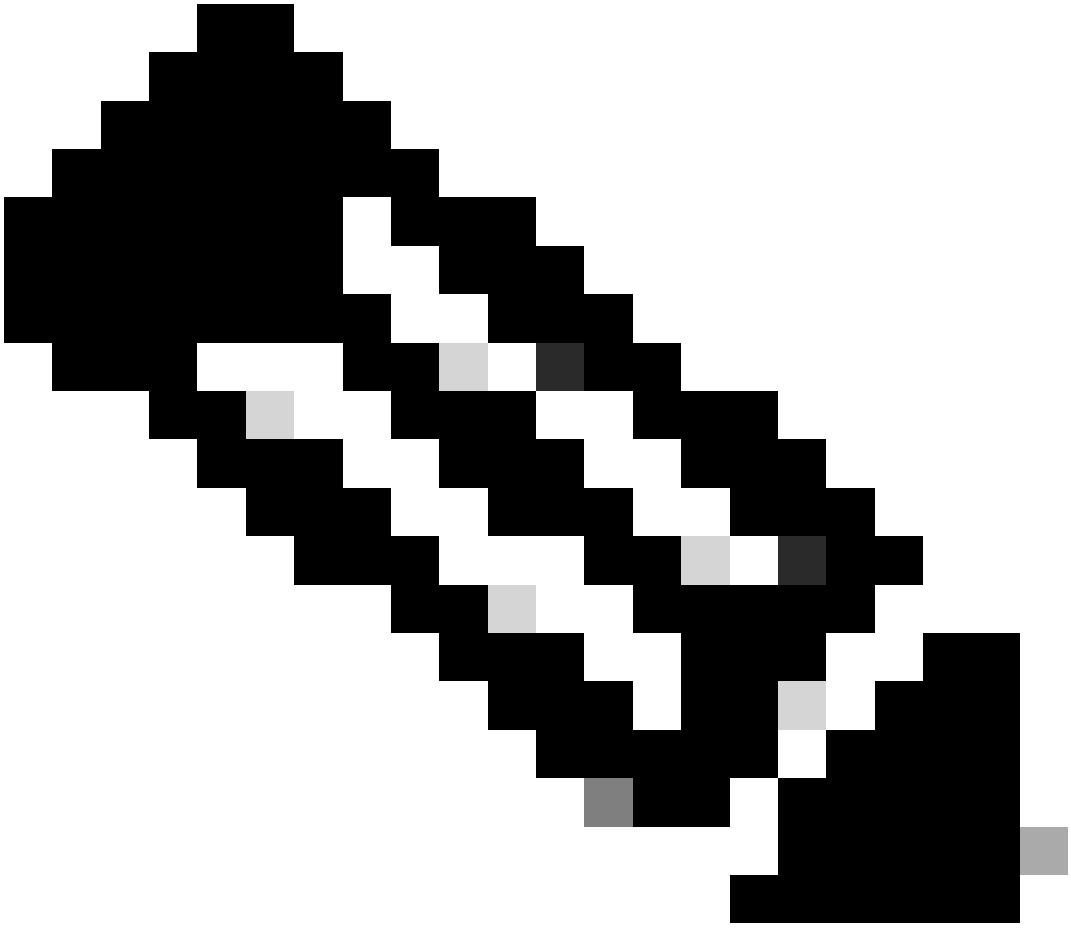
Esempio di rete

In questo esempio di laboratorio viene illustrato uno scenario in cui network 192.168.150.0/24 è il segmento LAN dietro il dispositivo Cisco IOS XE e 192.168.200.0/24 è il pool IP utilizzato dagli utenti RAVPN che si connettono all'headend Secure Access.

Il nostro obiettivo finale è quello di utilizzare il protocollo ECMP sui tunnel VPN tra il dispositivo Cisco IOS XE e l'headend Secure Access.

Per una migliore comprensione della topologia, fare riferimento al diagramma:


Remote Network (A)
VPN Client
192.168.200.0/24
Secure Access
NAT Gateway
NAT Gateway
RAVPN HE - A
Interconnect
SFCN
SWG
SFCN
SWG
Interconnect
RAVPN HE - B
CNHE - A
CNHE - B
Branch Office (A)
Private App
192.168.150.0/24
C8000V router
Multiple IPSEC tunnels
in single ECMP group



Nota: questo è solo un flusso di pacchetto di esempio, è possibile applicare gli stessi principi a qualsiasi altro flusso e a Secure Internet Access dalla subnet 192.168.150.0/24 dietro il router Cisco IOS XE.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione e gestione della CLI di Cisco IOS XE
- Conoscenze base dei protocolli IKEv2 e IPSec
- Configurazione iniziale di Cisco IOS XE (indirizzo IP, SSH, licenza)
- Conoscenze base di BGP ed ECMP

Componenti usati

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

- C800V con versione software 17.9.4a
- PC Windows
- Organizzazione Cisco Secure Access

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.

Premesse

I tunnel di rete in accesso sicuro hanno un limite di larghezza di banda di 1 Gbps per tunnel singolo. Se la larghezza di banda Internet upstream/downstream è superiore a 1 Gbps e si desidera utilizzarla completamente, è necessario superare questo limite configurando più tunnel con lo stesso centro dati ad accesso sicuro e raggruppandoli in un unico gruppo ECMP.

Quando si terminano più tunnel con il gruppo di tunnel di rete singolo (all'interno di un singolo controller di dominio ad accesso sicuro), per impostazione predefinita questi tunnel formano il gruppo ECMP dal punto di vista dell'headend ad accesso sicuro.
Ciò significa che, una volta che l'headend Secure Access invia il traffico verso il dispositivo VPN locale, esegue il bilanciamento del carico tra i tunnel (presupponendo che i peer BGP ricevano le route corrette).

Per ottenere la stessa funzionalità sul dispositivo VPN locale, è necessario configurare più interfacce VTI su un singolo router e verificare che venga applicata la configurazione di routing corretta.

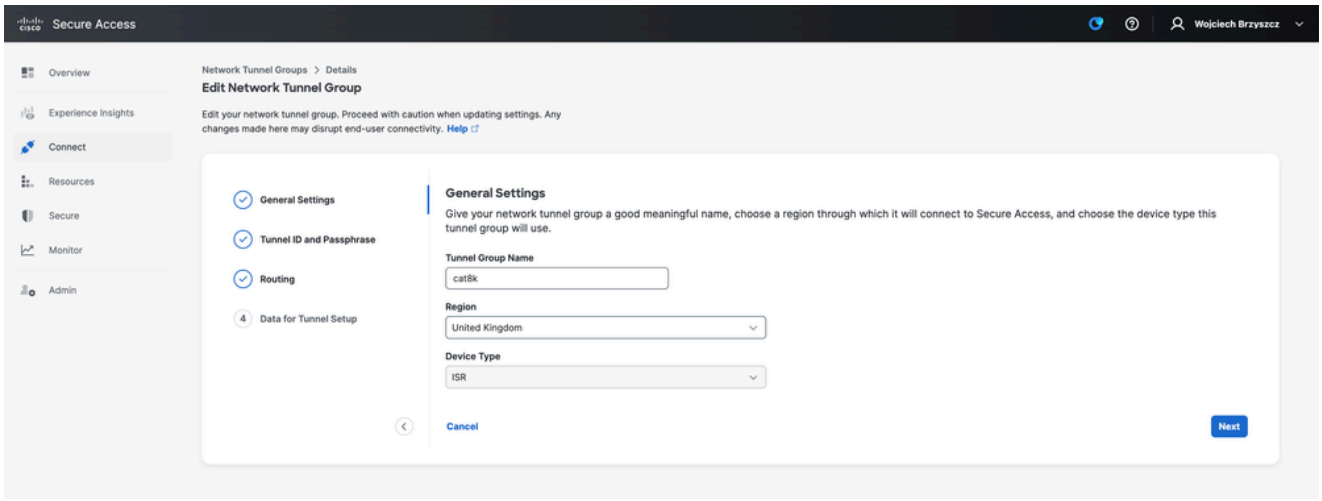
In questo articolo viene descritto lo scenario, con la spiegazione di ogni passaggio richiesto.

Configurazione

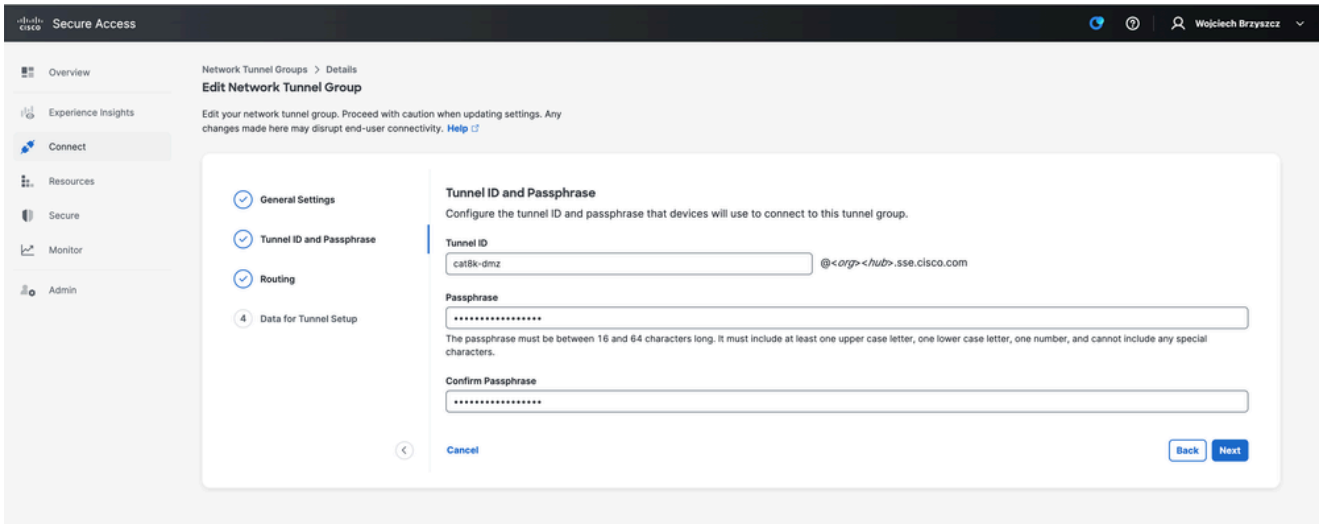
Configurazione Secure Access

Non è necessario applicare una configurazione speciale sul lato Secure Access per formare un gruppo ECMP da più tunnel VPN con protocollo BGP.
Passaggi necessari per configurare Network Tunnel Group.

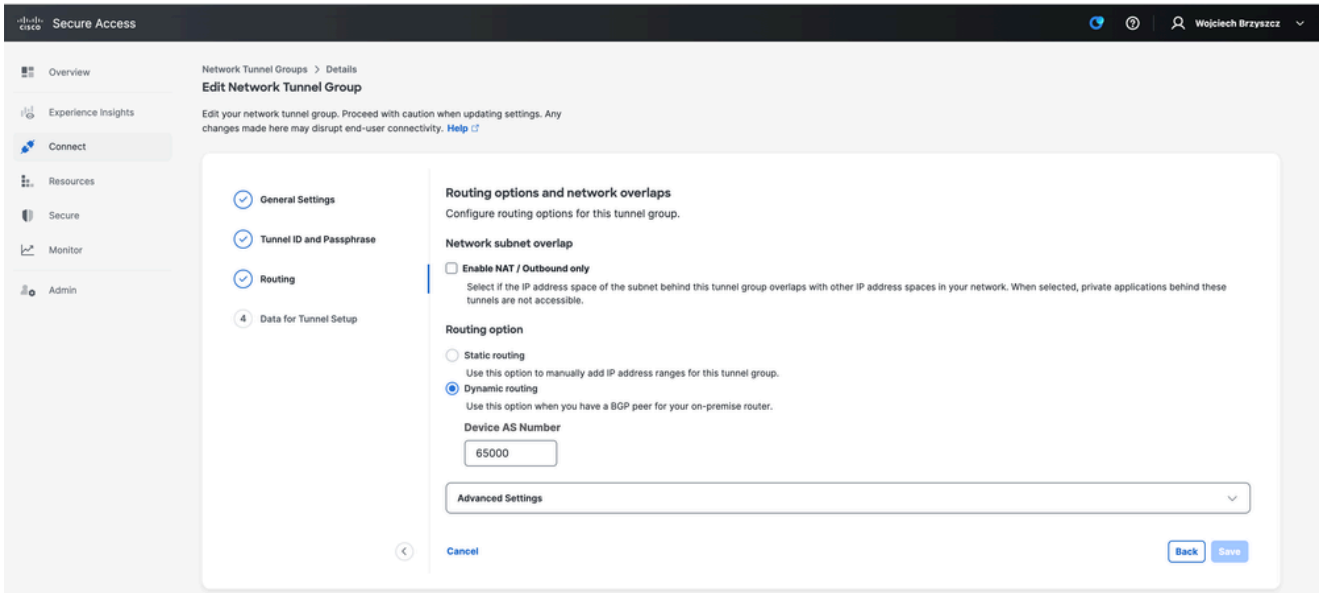
1. Creare un nuovo gruppo tunnel di rete (o modificarne uno esistente).



2. Specificare ID tunnel e passphrase:



3. Configurare le opzioni di instradamento, specificare l'instradamento dinamico e immettere il numero AS interno. In questo scenario di laboratorio, la rete ASN è pari a 65000.



4. Annotare i dettagli del tunnel nella sezione Dati per la configurazione del tunnel.

Cisco IOS XE configuration

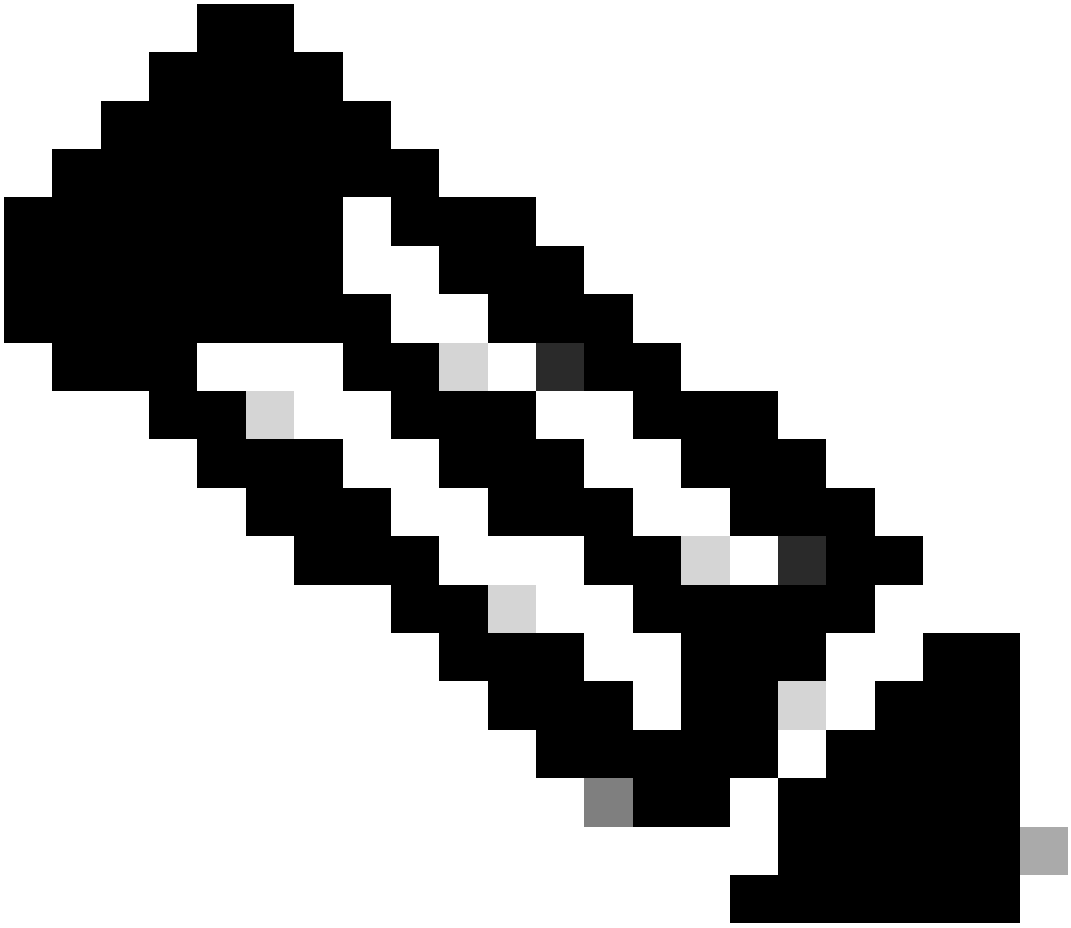
In questa sezione viene descritta la configurazione CLI che deve essere applicata al router Cisco IOS XE per configurare correttamente i tunnel IKEv2, il vicinato BGP e il bilanciamento del carico ECMP sulle interfacce del tunnel virtuale.
Ogni sezione viene spiegata e vengono indicate le avvertenze più comuni.

Parametri IKEv2 e IPsec

Configurare il criterio IKEv2 e la proposta IKEv2. Tali parametri definiscono gli algoritmi utilizzati per IKE SA (fase 1):

```
crypto ikev2 proposal sse-proposal
encryption aes-gcm-256
prf sha256
group 19 20

crypto ikev2 policy sse-pol
proposal sse-proposal
```



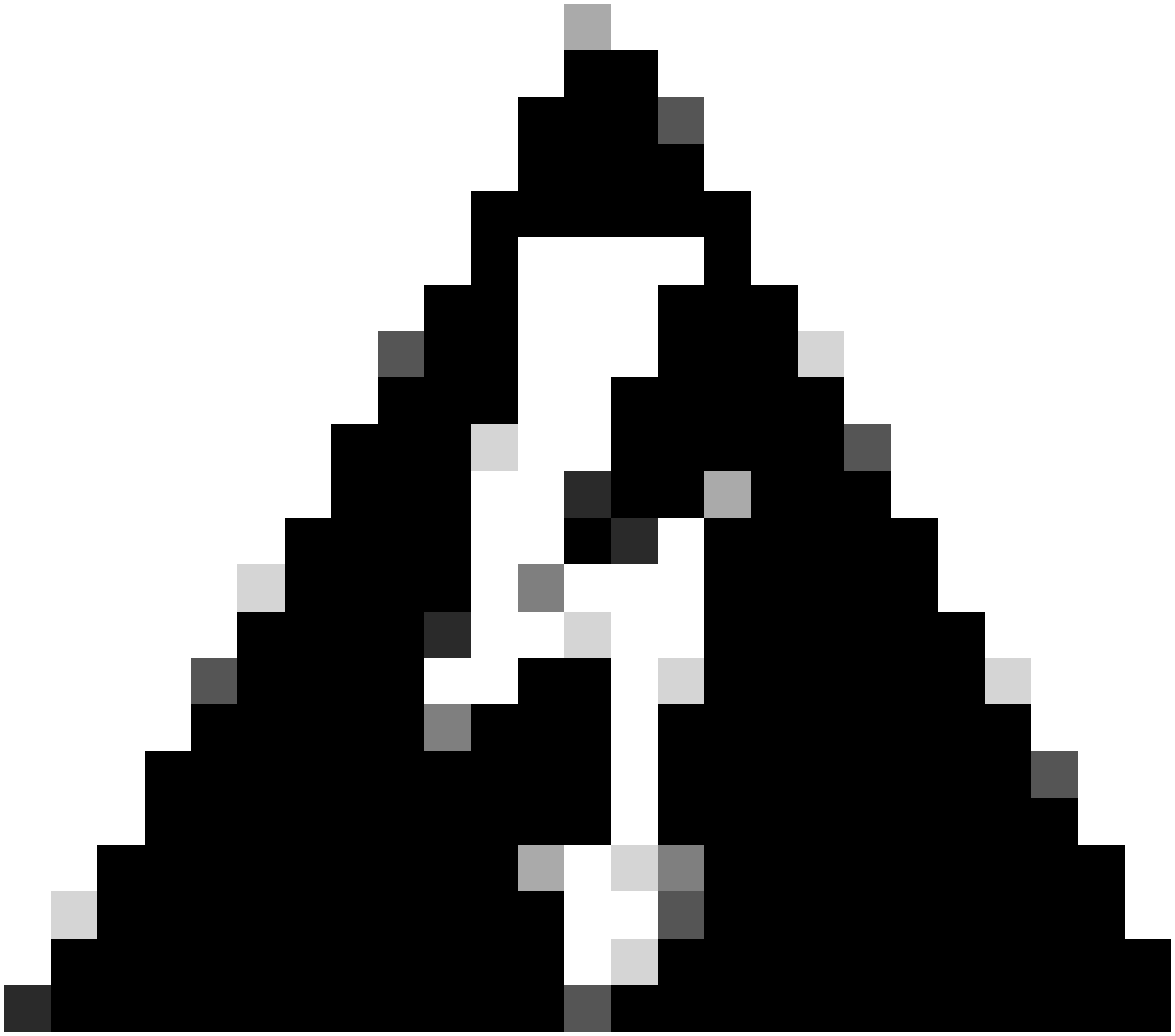
Nota: i parametri consigliati e ottimali sono indicati in grassetto nei documenti SSE: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Definire il keyring IKEv2 che definisce l'indirizzo IP dell'headend e la chiave precondivisa utilizzata per l'autenticazione con l'headend SSE:

```
crypto ikev2 keyring sse-keyring
 peer sse
 address 35.179.86.116
 pre-shared-key local <boring_generated_password>
 pre-shared-key remote <boring_generated_password>
```

Configurare una coppia di profili IKEv2.
Definiscono il tipo di identità IKE da utilizzare per la corrispondenza con il peer remoto e l'identità

IKE inviata dal router locale al peer.
L'identità IKE dell'headend SSE è di tipo indirizzo IP ed è uguale all'IP pubblico dell'headend SSE.



Avviso: per stabilire più tunnel con lo stesso Network Tunnel Group sul lato SSE, tutti devono utilizzare la stessa identità IKE locale.
Cisco IOS XE non supporta questo scenario, in quanto richiede una coppia univoca di identità IKE locali e remote per tunnel.
Per superare questo limite, l'headend SSE è stato migliorato in modo da accettare l'ID IKE nel formato: <ID_tunnel>+<suffisso>@<org><hub>.sse.cisco.com

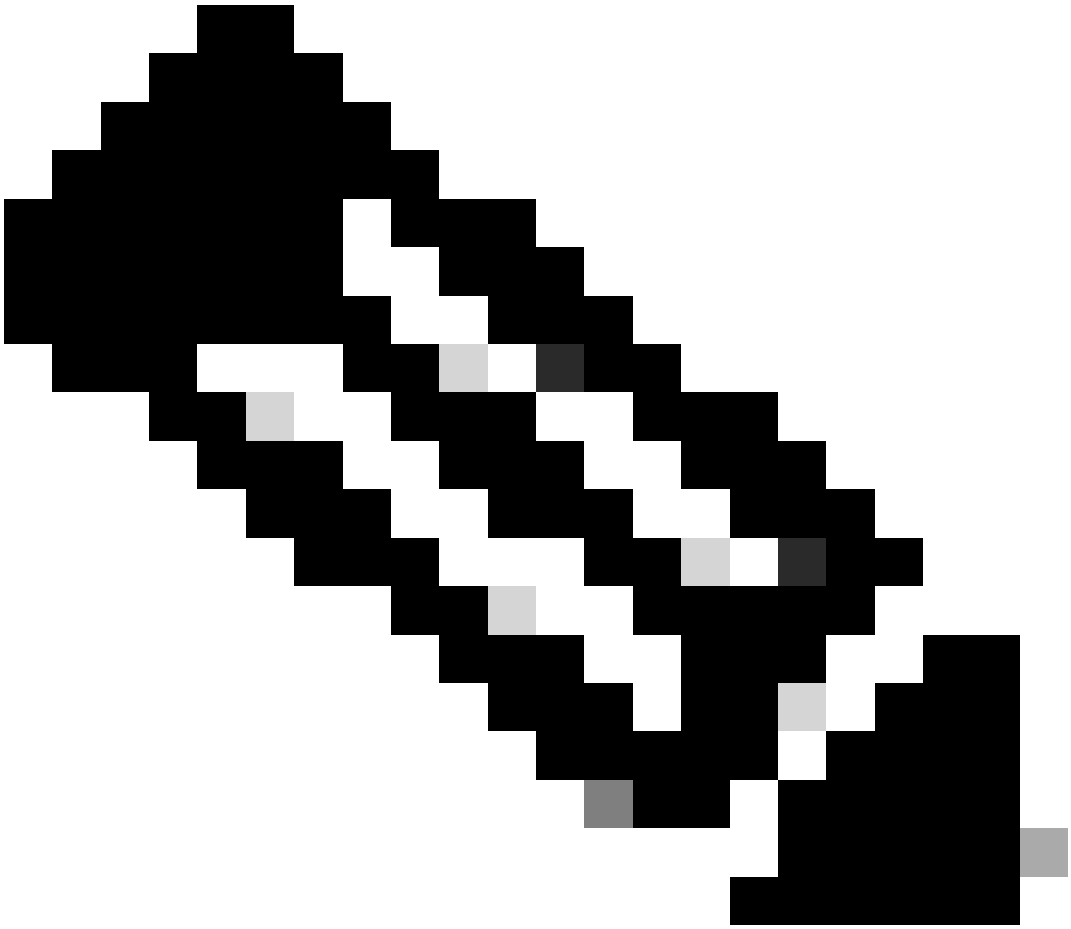
---

Nello scenario di laboratorio descritto, l'ID del tunnel è stato definito come cat8k-dmz.
In uno scenario normale, è necessario configurare il router per inviare l'identità IKE locale come cat8k-dmz@8195165-622405748-sse.cisco.com

Tuttavia, per stabilire più tunnel con lo stesso Network Tunnel Group, vengono utilizzati gli ID IKE locali:

cat8k-dmz+tunnel1@8195165-622405748-sse.cisco.com e cat8k-dmz+tunnel2@8195165-622405748-sse.cisco.com

Notare il suffisso aggiunto a ciascuna stringa (tunnel1 e tunnel2)



> Nota: le identità IKE locali citate sono solo un esempio di quelle utilizzate in questo scenario di laboratorio. È possibile definire qualsiasi suffisso desiderato, solo assicurarsi di soddisfare i requisiti.

```
crypto ikev2 profile sse-ikev2-profile-tunnel1
 match identity remote address 35.179.86.116 255.255.255.255
 identity local email cat8k-dmz+tunnel1@8195165-622405748-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local sse-keyring
 dpd 10 2 periodic

crypto ikev2 profile sse-ikev2-profile-tunnel2
 match identity remote address 35.179.86.116 255.255.255.255
```

```
 identity local email cat8k-dmz+tunnel2@8195165-622405748-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local sse-keyring
 dpd 10 2 periodic
```

Configurare il set di trasformazioni IPSec. Questa impostazione definisce gli algoritmi utilizzati per l'associazione di protezione IPSec (fase 2):

```
crypto ipsec transform-set sse-transform esp-gcm 256
mode tunnel
```

Configurare i profili IPSec che collegano i profili IKEv2 ai set di trasformazioni:

```
crypto ipsec profile sse-ipsec-profile-1
set transform-set sse-transform
set ikev2-profile sse-ikev2-profile-tunnel1

crypto ipsec profile sse-ipsec-profile-2
set transform-set sse-transform
set ikev2-profile sse-ikev2-profile-tunnel2
```

Interfacce tunnel virtuale

In questa sezione viene descritta la configurazione delle interfacce del tunnel virtuale e delle interfacce di loopback utilizzate come origine del tunnel.

Nello scenario di laboratorio descritto, è necessario stabilire due interfacce VTI con il singolo peer utilizzando lo stesso indirizzo IP pubblico. Inoltre, il nostro dispositivo Cisco IOS XE ha solo un'interfaccia in uscita Gigabit Ethernet1.

Cisco IOS XE non supporta la configurazione di più VTI con la stessa origine e destinazione del tunnel.

Per superare questo limite, è possibile utilizzare le interfacce di loopback e definirle come origine del tunnel nella VTI corrispondente.

Esistono poche opzioni per ottenere la connettività IP tra loopback e l'indirizzo IP pubblico SSE:

1. Assegna indirizzo IP instradabile pubblicamente all'interfaccia di loopback (richiede la proprietà dello spazio degli indirizzi IP pubblico)
2. Assegnare l'indirizzo IP privato all'interfaccia di loopback e all'origine IP di loopback del

traffico NAT in modo dinamico.
3. Usa interfacce VASI (non supportate su molte piattaforme, complicate da configurare e risolvere i problemi)

In questo scenario, discuteremo della seconda opzione.

Configurare due interfacce loopback e aggiungere il comando "ip nat inside" sotto ciascuna di esse.

```
interface Loopback1
ip address 10.1.1.38 255.255.255.255
ip nat inside
end

interface Loopback2
ip address 10.1.1.70 255.255.255.255
ip nat inside
end
```

Definire l'elenco di controllo di accesso NAT dinamico e l'istruzione di sovraccarico NAT:

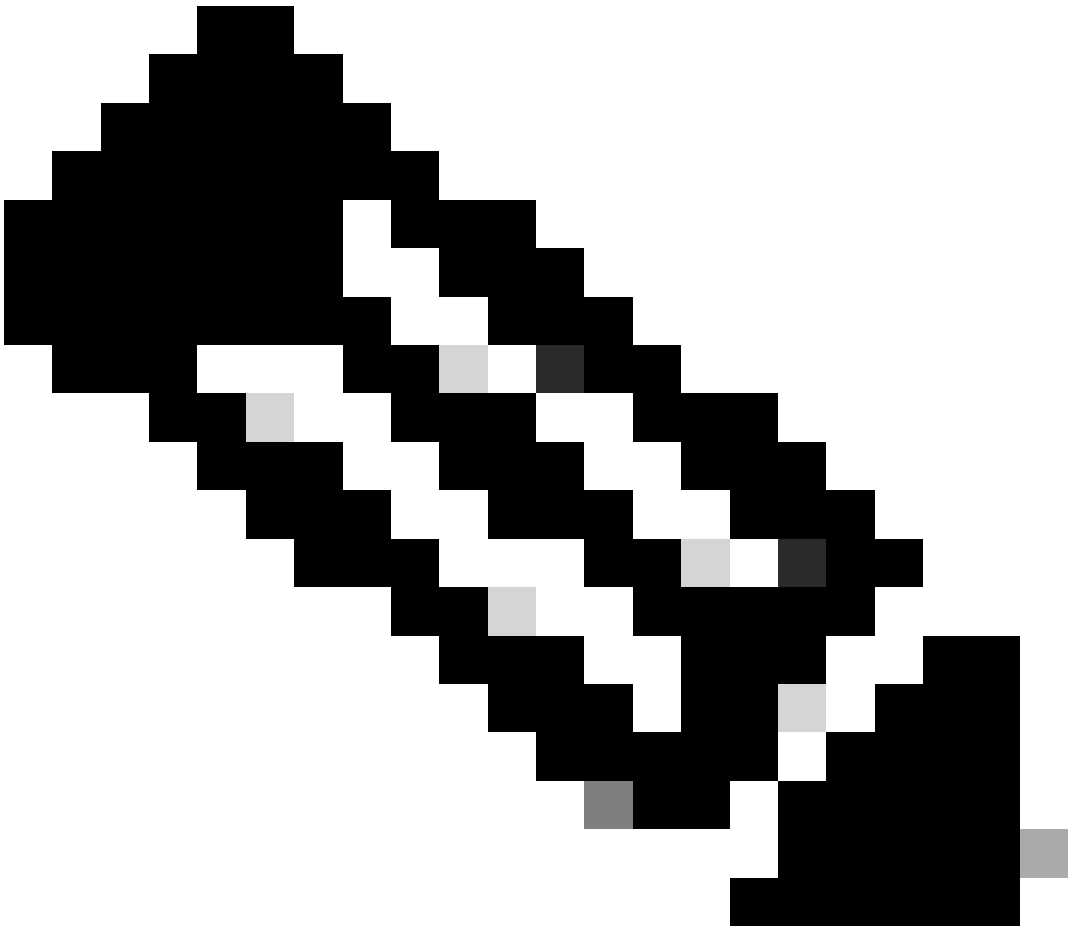
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

ip nat inside source list NAT interface GigabitEthernet1 overload
```

Configurare le interfacce del tunnel virtuale.

```
interface Tunnel1
ip address 169.254.0.10 255.255.255.252
tunnel source Loopback1
tunnel mode ipsec ipv4
tunnel destination 35.179.86.116
tunnel protection ipsec profile sse-ipsec-profile-1
end

!
interface Tunnel2
ip address 169.254.0.14 255.255.255.252
tunnel source Loopback2
tunnel mode ipsec ipv4
tunnel destination 35.179.86.116
tunnel protection ipsec profile sse-ipsec-profile-2
end
```



Nota: nello scenario lab descritto, gli indirizzi IP assegnati alle VTI provengono da subnet non sovrapposte 169.254.0.0/24.
È possibile utilizzare altro spazio subnet, ma per alcuni requisiti correlati a BGP è necessario tale spazio di indirizzi.

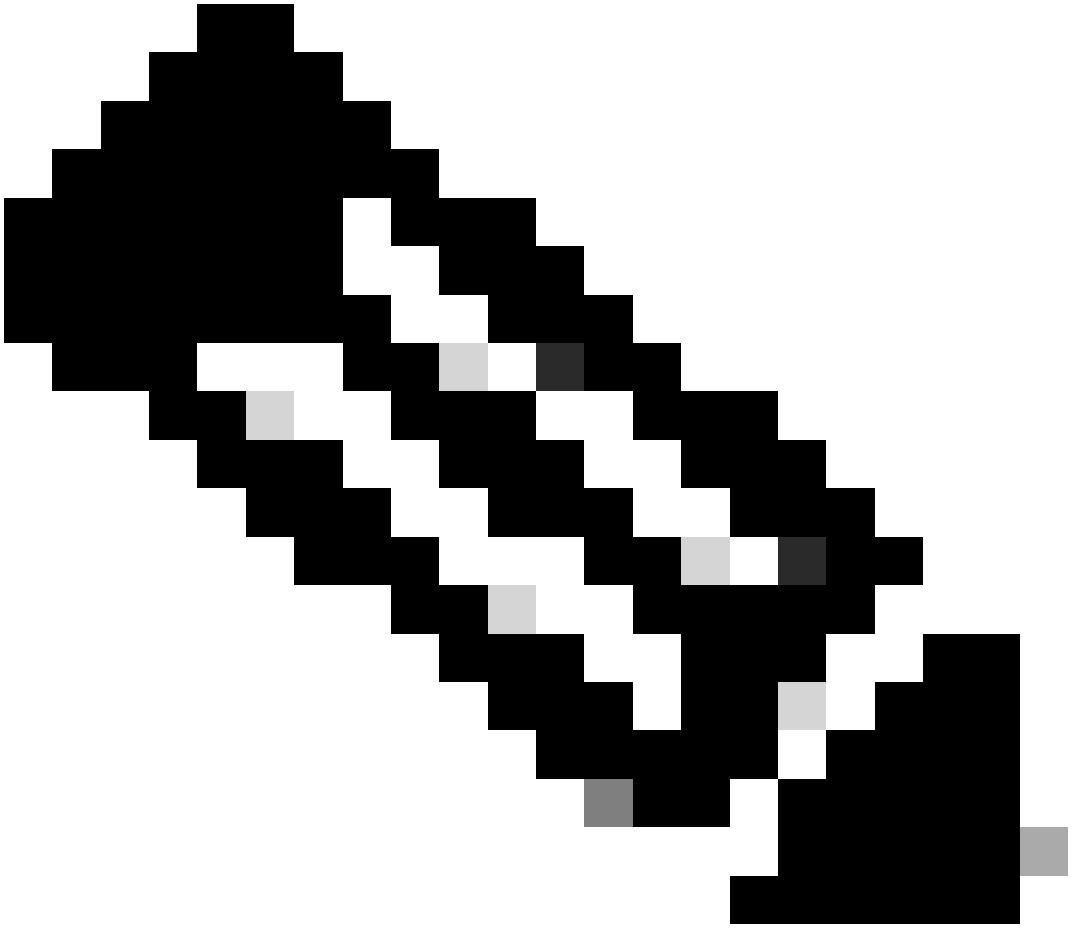
Routing BGP

In questa sezione viene descritta la parte di configurazione necessaria per stabilire una relazione di vicinanza BGP con l'headend SSE.
Il processo BGP sull'headend SSE è in ascolto su qualsiasi IP dalla subnet 169.254.0.0/24 .
Per stabilire il peering BGP su entrambe le VTI, verranno definiti due router adiacenti: 169.254.0.9 (Tunnel1) e 169.254.0.13 (Tunnel2).
Inoltre, è necessario specificare l'AS remoto in base al valore visualizzato nel dashboard SSE.

<#root>

```
router bgp 65000
bgp log-neighbor-changes
neighbor 169.254.0.9 remote-as 64512
neighbor 169.254.0.9 ebgp-multihop 255
neighbor 169.254.0.13 remote-as 64512
neighbor 169.254.0.13 ebgp-multihop 255
!
address-family ipv4
network 192.168.150.0
neighbor 169.254.0.9 activate
neighbor 169.254.0.13 activate
```

maximum-paths 2

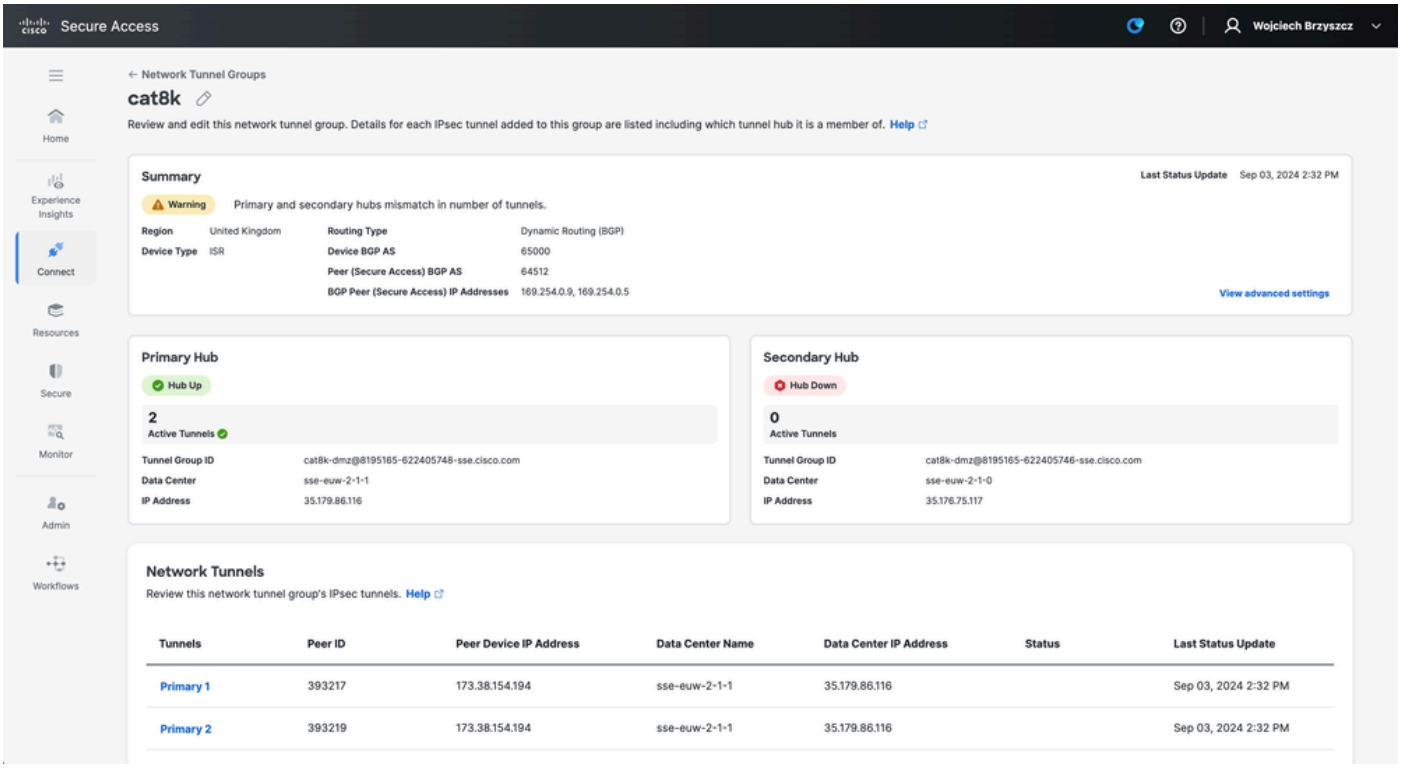


Nota: le route ricevute da entrambi i peer devono essere identiche. Per impostazione predefinita, il router ne installa solo uno nella tabella di routing.
Per consentire l'installazione di più route duplicate nella tabella di routing (e abilitare ECMP), è necessario configurare "maximum-path <number of route>"

Verifica

Dashboard di accesso protetto

Nel dashboard SSE devono essere visualizzati due tunnel primari:



Cisco IOS XE Router

Verificare che entrambi i tunnel siano in stato READY dal lato Cisco IOS XE:

```
<#root>

wbrzyszc-cat8k#

show crypto ikev2 sa


IPv4 Crypto IKEv2 SA

Tunnel-id Local          Remote             fvrf/ivrf Status
1         10.1.1.70/4500 35.179.86.116/4500 none/none READY
    Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/255 sec
    CE id: 0, Session-id: 6097
    Local spi: A15E8ACF919656C5 Remote spi: 644CFD102AAF270A

Tunnel-id Local          Remote             fvrf/ivrf Status
6         10.1.1.38/4500 35.179.86.116/4500 none/none READY
```

```
    Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/11203 sec
    CE id: 0, Session-id: 6096
    Local spi: E18CBEE82674E780 Remote spi: 39239A7D09D5B972
```

Verificare che il protocollo di vicinato BGP sia ATTIVO con entrambi i peer:

<#root>

```
wbrzyszc-cat8k#
```

show ip bgp summary

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.0.9 4 64512 17281 18846 160 0 0 5d23h 15
169.254.0.13 4 64512 17281 18845 160 0 0 5d23h 15
```

Verificare che il router apprenda le route corrette dal protocollo BGP (e che nella tabella di routing siano installati almeno due hop successivi).

<#root>

```
wbrzyszc-cat8k#
```

show ip route 192.168.200.0

```
Routing entry for 192.168.200.0/25, 2 known subnets
B 192.168.200.0 [20/0] via 169.254.0.13, 5d23h
                [20/0] via 169.254.0.9, 5d23h
B 192.168.200.128 [20/0] via 169.254.0.13, 5d23h
                  [20/0] via 169.254.0.9, 5d23h

wbrzyszc-cat8k#
```

show ip cef 192.168.200.0

```
192.168.200.0/25
    nexthop 169.254.0.9 Tunnel1
    nexthop 169.254.0.13 Tunnel2
```

Avviare il traffico e verificare che entrambi i tunnel siano utilizzati, quindi verificare che i contatori incapsula e decapsula sempre di più.

<#root>

```
wbrzyszc-cat8k#
```

show crypto ipsec sa | i peer|caps

```
current_peer 35.179.86.116 port 4500
#pkts encaps: 1881087, #pkts encrypt: 1881087, #pkts digest: 1881087
#pkts decaps: 1434171, #pkts decrypt: 1434171, #pkts verify: 1434171

current_peer 35.179.86.116 port 4500
#pkts encaps: 53602, #pkts encrypt: 53602, #pkts digest: 53602
#pkts decaps: 208986, #pkts decrypt: 208986, #pkts verify: 208986
```

Facoltativamente, è possibile raccogliere l'acquisizione dei pacchetti su entrambe le interfacce VTI per assicurarsi che il traffico tra le VTI sia bilanciato dal carico. Leggere le istruzioni in questo articolo per configurare Embedded Packet Capture sul dispositivo Cisco IOS XE.
Nell'esempio, l'host dietro il router Cisco IOS XE con indirizzo IP di origine 192.168.150.1 stava inviando richieste ICMP a più IP dalla subnet 192.168.200.0/24.

Come si può vedere, le richieste ICMP hanno lo stesso bilanciamento del carico tra i tunnel.

<#root>

```
wbrzyszc-cat8k#
```

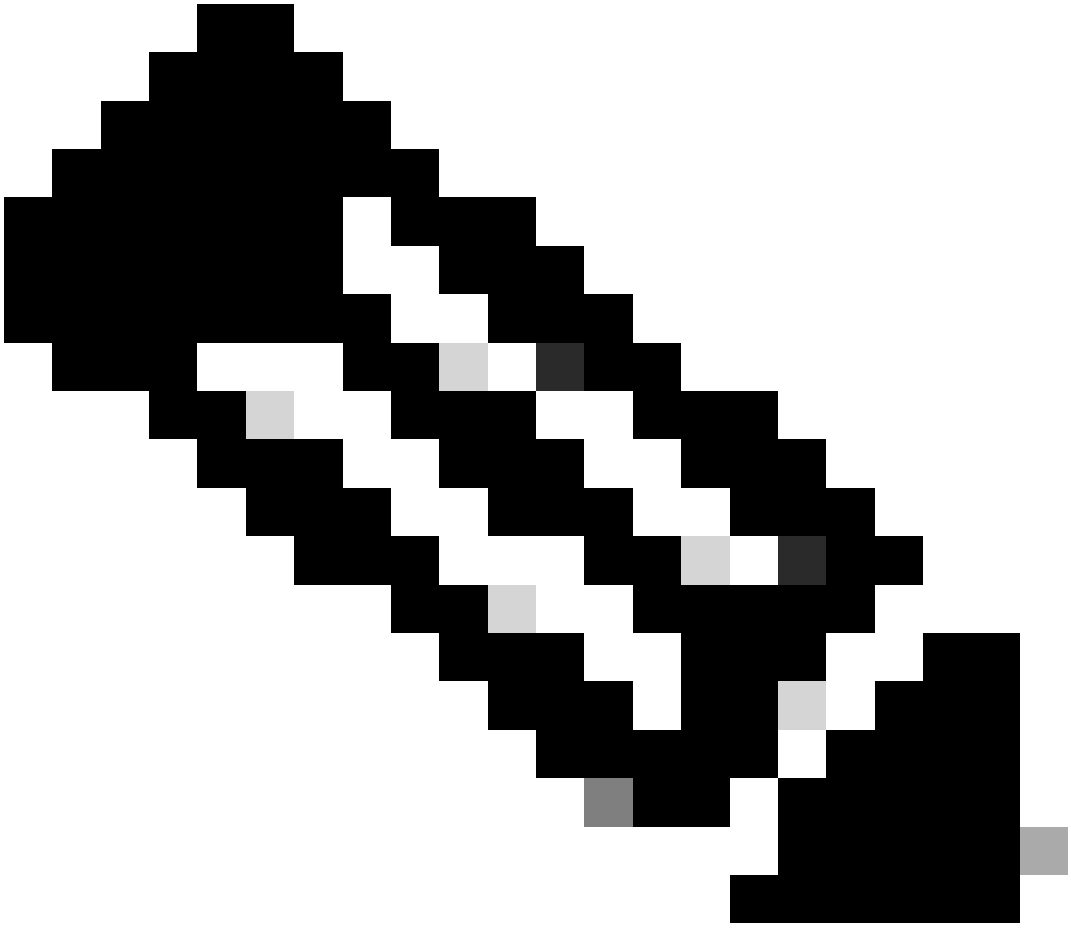
show monitor capture Tunnel1 buffer brief

```
------------------------------------------------------------------------------
#   size   timestamp     source     destination      dscp    protocol
------------------------------------------------------------------------------
   0  114    0.000000   192.168.150.1    ->  192.168.200.2    0  BE   ICMP
   1  114    0.000000   192.168.150.1    ->  192.168.200.2    0  BE   ICMP
  10  114   26.564033   192.168.150.1    ->  192.168.200.5    0  BE   ICMP
  11  114   26.564033   192.168.150.1    ->  192.168.200.5    0  BE   ICMP
```

```
wbrzyszc-cat8k#
```

show monitor capture Tunnel2 buffer brief

```
------------------------------------------------------------------------------
#   size   timestamp     source     destination      dscp    protocol
------------------------------------------------------------------------------
   0  114    0.000000   192.168.150.1    ->  192.168.200.1    0  BE   ICMP
   1  114    2.000000   192.168.150.1    ->  192.168.200.1    0  BE   ICMP
  10  114   38.191000   192.168.150.1    ->  192.168.200.3    0  BE   ICMP
  11  114   38.191000   192.168.150.1    ->  192.168.200.3    0  BE   ICMP
```



Nota: sui router Cisco IOS XE sono disponibili più meccanismi di bilanciamento del carico ECMP. Per impostazione predefinita, il bilanciamento del carico per destinazione è abilitato, in modo da assicurare che il traffico verso la stessa destinazione IP prenda sempre lo stesso percorso.
È possibile configurare il bilanciamento del carico per pacchetto, che bilancerebbe il carico del traffico in modo casuale anche per lo stesso IP di destinazione.

Informazioni correlate

- Guida per l'utente di Secure Access
- Come raccogliere Embedded Packet Capture
- Documentazione e supporto tecnico – Cisco Systems

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).