Netwerktunnel tussen Cisco Secure Access en IOS XE router configureren met behulp van ECMP en BGP

Inhoud

Inleiding

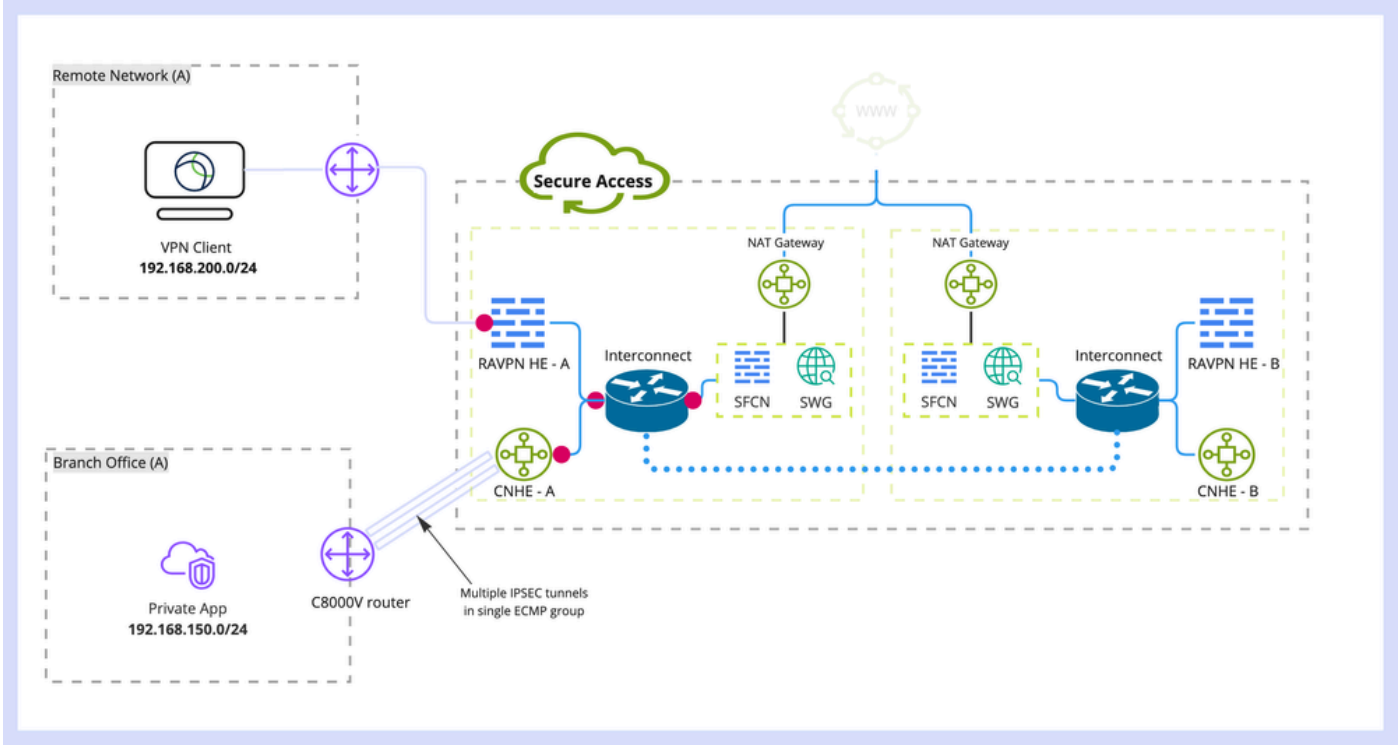
Dit document beschrijft de stappen die nodig zijn om IPSec VPN-tunnels tussen Cisco Secure Access en Cisco IOS XE te configureren en problemen op te lossen met behulp van BGP en ECMP.

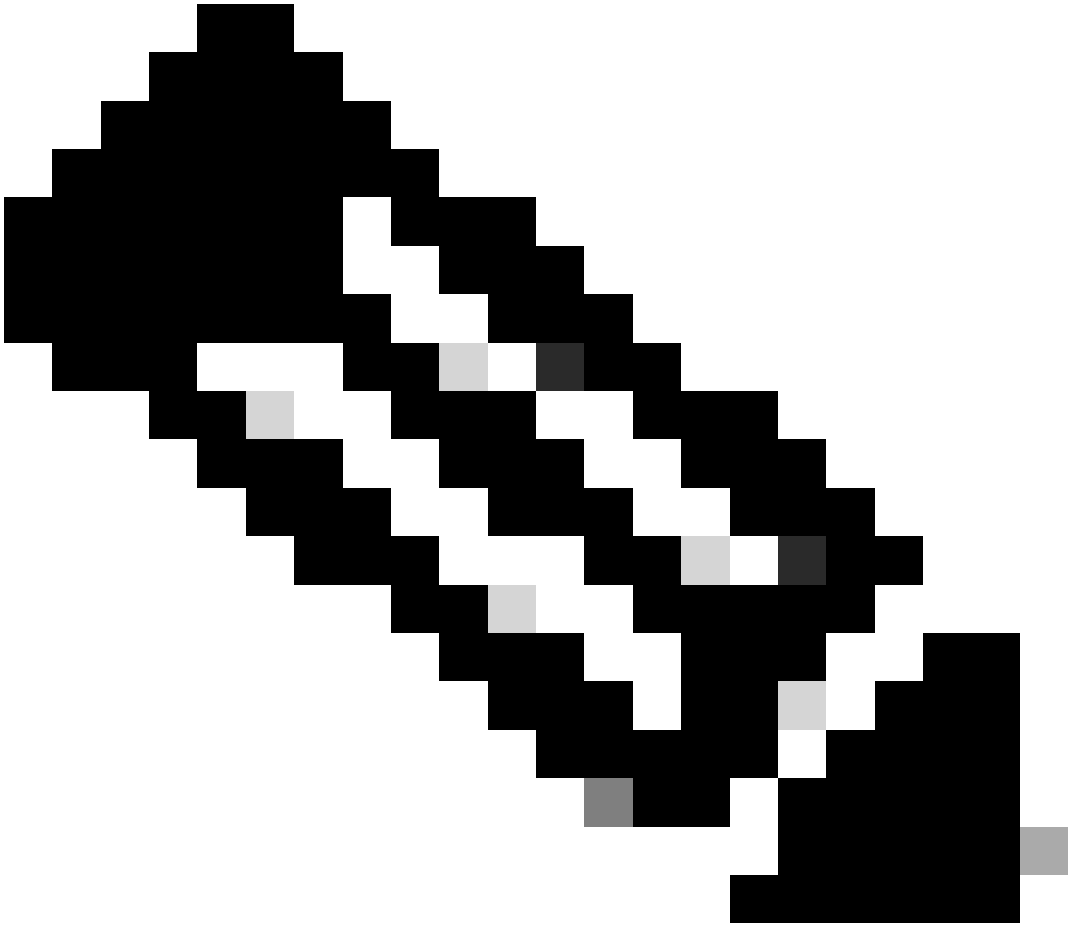
Netwerkdiagram

In dit laboratoriumvoorbeeld, gaan wij scenario bespreken waar het netwerk 192.168.150.0/24 LAN segment achter Cisco IOS XE apparaat is, en 192.168.200.0/24 is IP pool die door gebruikers RAVPN wordt gebruikt die met Veilig Access uiteinde verbinden.

Ons einddoel is het gebruik van ECMP in VPN-tunnels tussen Cisco IOS XE-apparaat en Secure Access head-end.

Om de topologie beter te begrijpen, gelieve te verwijzen naar het diagram:


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



Opmerking: dit is slechts een voorbeeldpakketstroom, u kunt dezelfde principes toepassen op alle andere stromen en op Secure Internet Access van 192.168.150.0/24 subnettoegang achter Cisco IOS XE router.

Voorwaarden

Vereisten

Aanbevolen wordt dat u kennis van deze onderwerpen hebt:

- Cisco IOS XE CLI-configuratie en -beheer
- Basiskennis van IKEv2- en IPSec-protocollen
- Eerste Cisco IOS XE-configuratie (IP-adressering, SSH, licentie)
- Basiskennis van BGP en ECMP

Gebruikte componenten

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

- C800V met 17.9.4a-softwareversie
- Windows-pc
- Cisco Secure Access-organisatie

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.

Achtergrondinformatie

Netwerktunnels in Secure Access hebben een bandbreedtebeperking van 1 Gbps per enkele tunnel. Als uw upstream/downstream internetbandbreedte hoger is dan 1 Gbps en u wilt deze volledig gebruiken, dan dient u deze beperking te overwinnen door meerdere tunnels te configureren met hetzelfde Secure Access Data Center en ze te groeperen in één ECMP-groep.

Wanneer u meerdere tunnels beëindigt met de enkele Network Tunnel Group (binnen één Secure Access DC), worden deze standaard van de ECMP-groep afgesloten vanuit het perspectief van Secure Access head-end.
Dat betekent dat zodra Secure Access-head-end verkeer naar het VPN-apparaat op locatie stuurt, het werklastverdeling tussen de tunnels (ervan uitgaande dat de juiste routes worden ontvangen van BGP-peers).

Om dezelfde functionaliteit op het VPN-apparaat op locatie te bereiken, moet u meerdere VTI-interfaces op één router configureren en ervoor zorgen dat de juiste routerconfiguratie wordt toegepast.

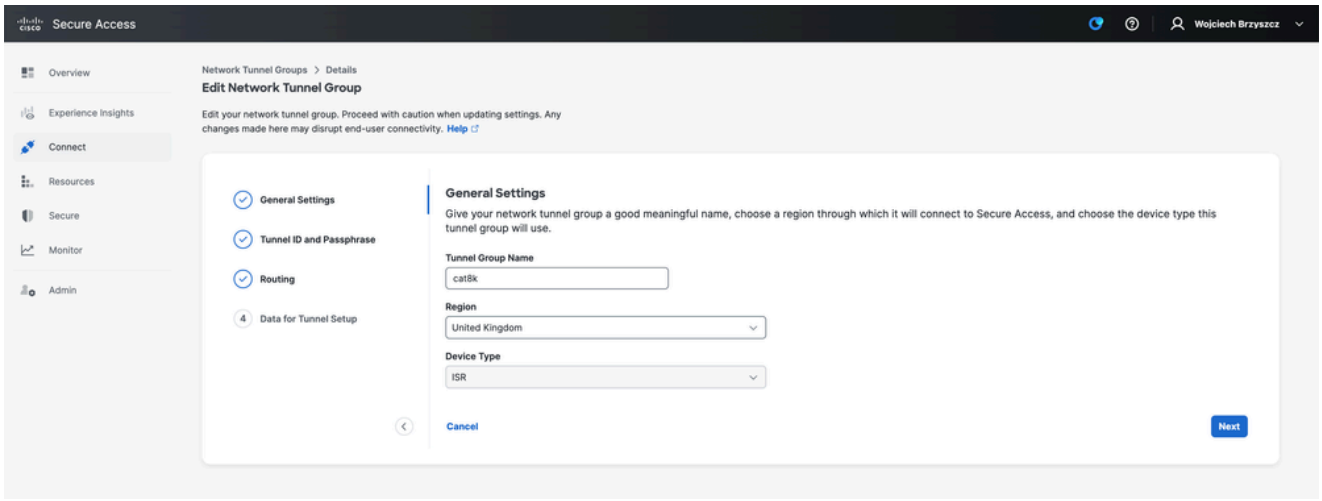
Dit artikel beschrijft scenario, met uitleg van elke vereiste stap.

Configureren

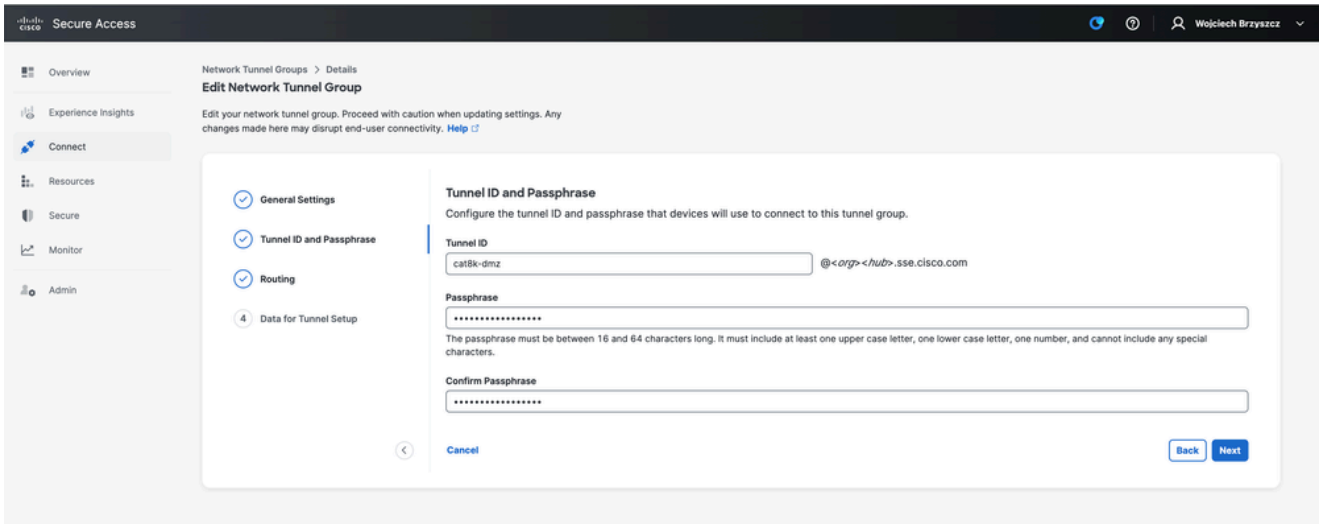
Configuratie van beveiligde toegang

Er is geen speciale configuratie die moet worden toegepast aan de kant van Secure Access om met behulp van het BGP-protocol een ECMP-groep te vormen vanuit meerdere VPN-tunnels. Stappen vereist om de Network Tunnel Group te configureren.

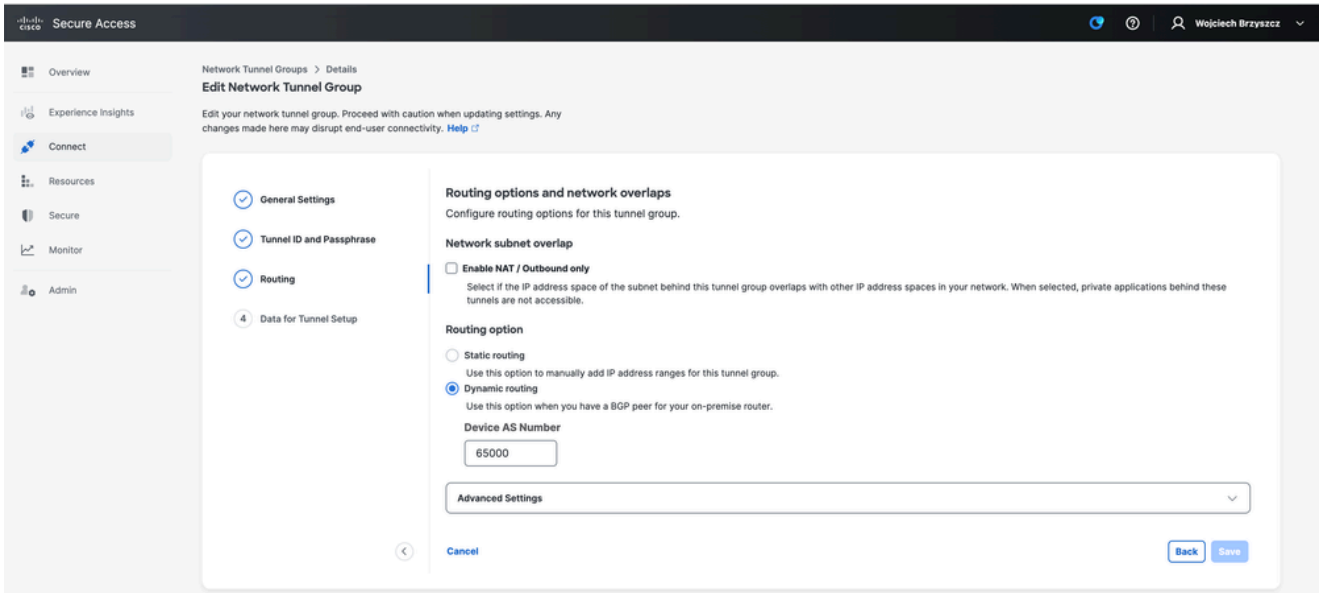
1. Een nieuwe netwerktunnelgroep maken (of bestaande groep bewerken).



2. Tunnel-id en wachtwoord opgeven:



3. Configureer Routing-opties, specificeer Dynamic Routing en voer uw interne AS-nummer in. In dit laboratoriumscenario is ASN gelijk aan 65000.



4. Noteer de tunnelgegevens uit de sectie Gegevens voor tunnelinstelling.

Cisco IOS XE-configuratie

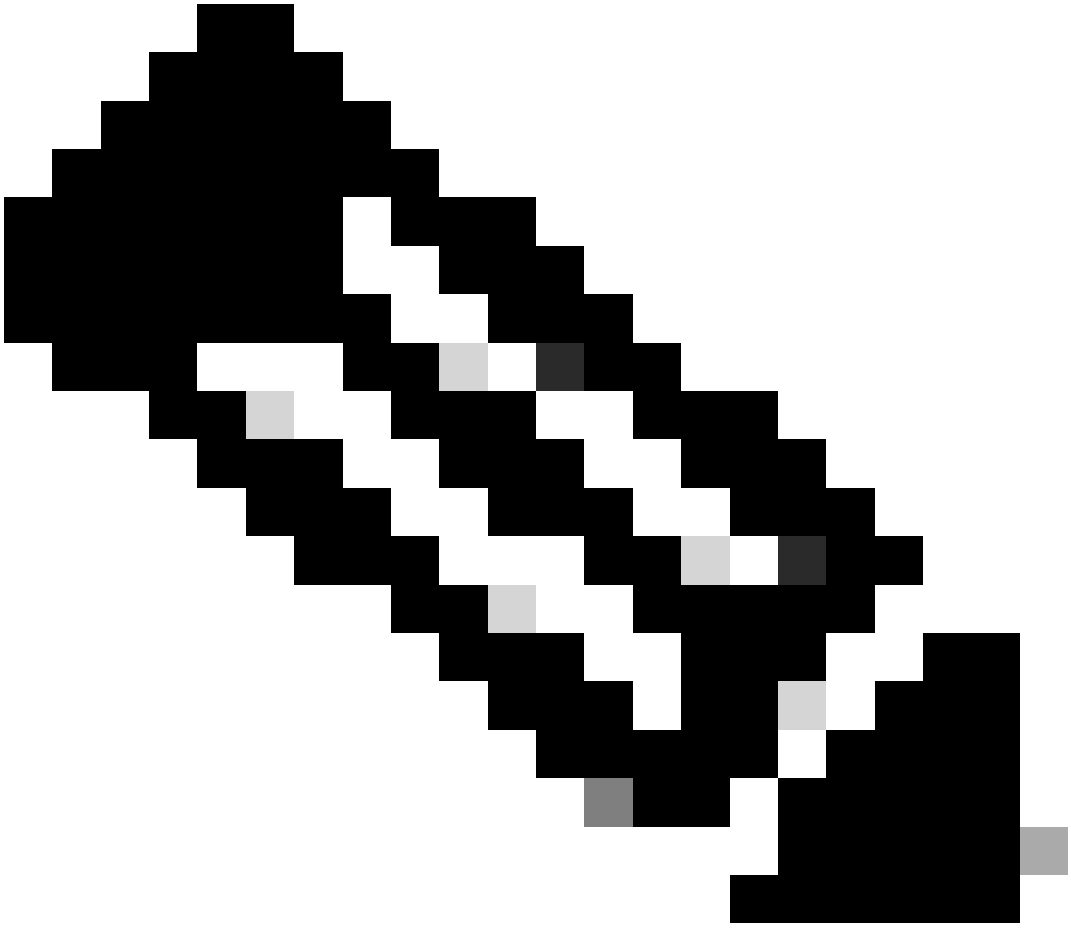
Deze sectie behandelt CLI-configuratie die op Cisco IOS XE-router moet worden toegepast om IKEv2-tunnels, BGP-buurten en ECMP-taakverdeling over virtuele tunnelinterfaces goed te kunnen configureren.
Elke sectie wordt uitgelegd en de meeste gebruikelijke voorbehouden worden vermeld.

IKEv2- en IPsec-parameters

Configureer het IKEv2-beleid en het IKEv2-voorstel. Deze parameters definiëren welke algoritmen worden gebruikt voor 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
```



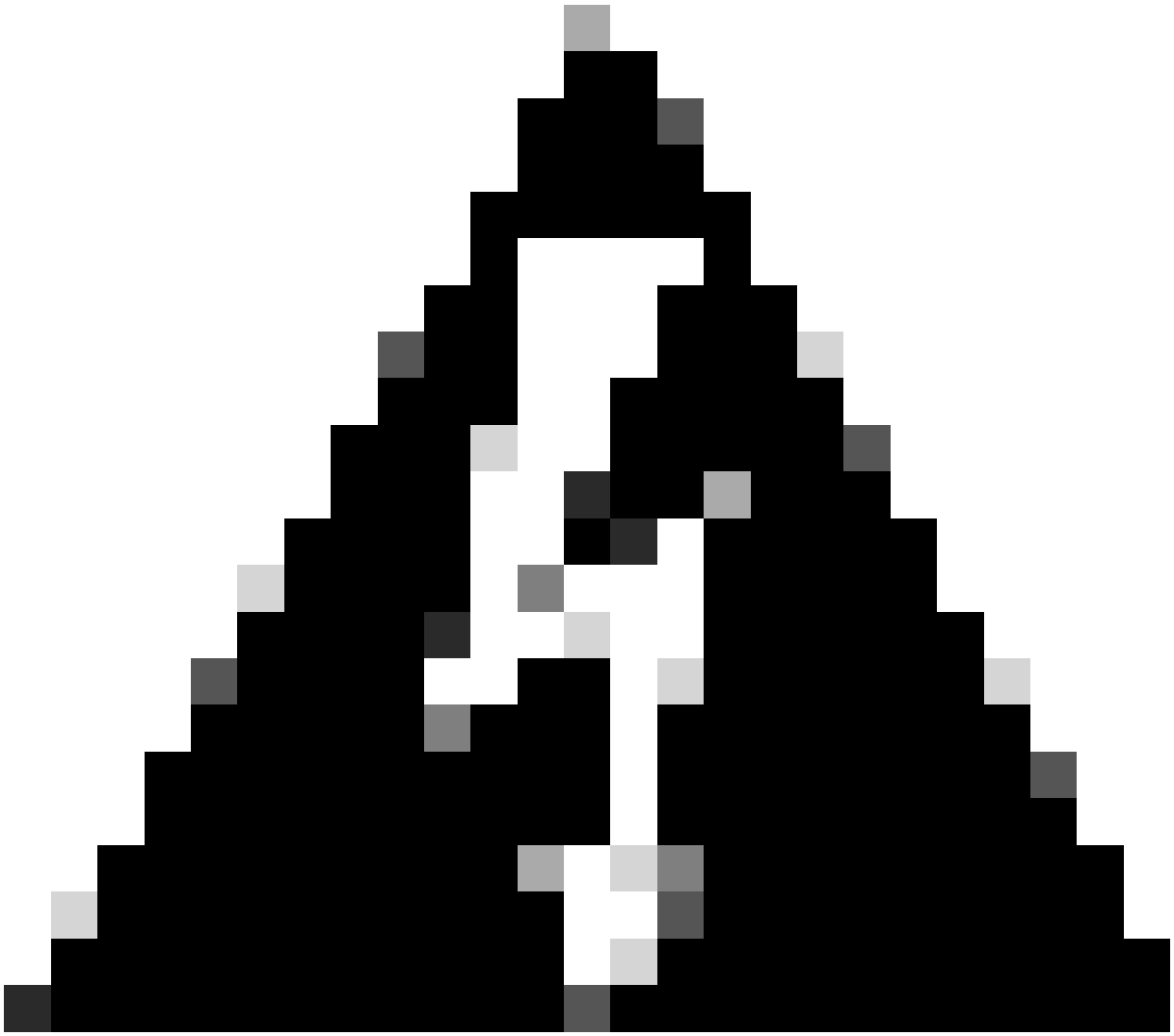
Opmerking: De voorgestelde en optimale parameters zijn vet weergegeven in SSE docs: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Definieer IKEv2-sleutelring die het IP-adres van het head-end en de vooraf gedeelde sleutel definieert die wordt gebruikt voor de verificatie met SSE-head-end:

```
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>
```

Configureer twee IKEv2-profielen.
Zij bepalen welk type van IKE identiteit wordt gebruikt om verre peer aan te passen, en welke

lokale router van de IKE-identiteit naar de peer verzendt.
IKE-identiteit van SSE-head-end is van het IP-adrestype en is gelijk aan openbare IP van de SSE-head-end.



Waarschuwing: om meerdere tunnels met dezelfde Network Tunnel Group aan SSE-kant te maken, moeten ze allemaal dezelfde lokale IKE-identiteit gebruiken.
Cisco IOS XE ondersteunt een dergelijk scenario niet, omdat hiervoor een uniek paar lokale en externe IKE-identiteiten per tunnel nodig is.
Om deze beperking te overwinnen, is SSE head-end verbeterd om IKE-id in het formaat te accepteren: <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

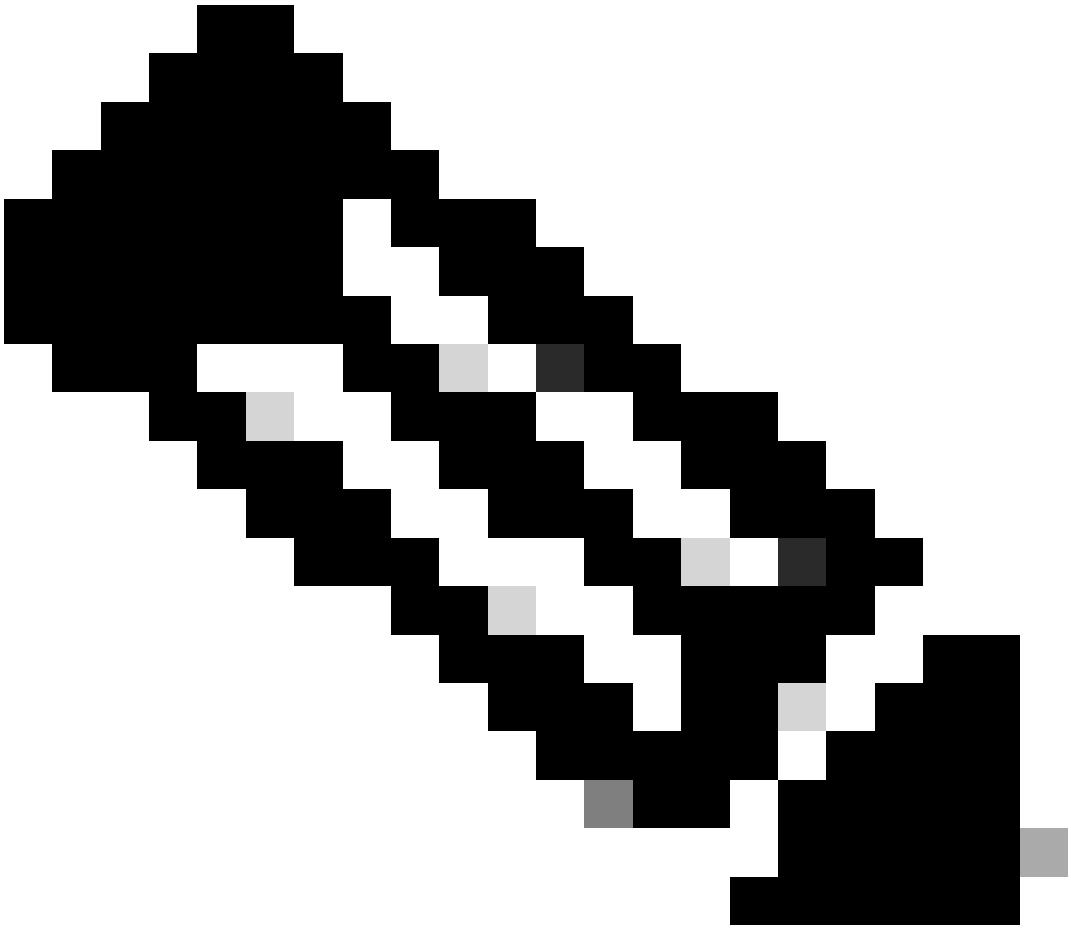
---

In besproken labscenario werd tunnel-ID gedefinieerd als cat8k-dmz.
In normaal scenario zouden we router configureren om lokale IKE-identiteit te verzenden als cat8k-dmz@8195165-622405748-sse.cisco.com

Echter, om meerdere tunnels met dezelfde Network Tunnel Group te maken, worden lokale IKE ID's gebruikt:

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

Let op het achtervoegsel dat aan elke string is toegevoegd (tunnel1 en tunnel2)



> Opmerking: De genoemde lokale IKE-identiteiten zijn slechts een voorbeeld dat in dit laboratoriumscenario wordt gebruikt. U kunt elk achtervoegsel dat u wilt definiëren, maar zorg ervoor dat het aan de vereisten voldoet.

```
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
```

Configuratie van IPSec-transformatieset. Deze instelling definieert algoritmen die worden gebruikt voor IPsec Security Association (fase 2):

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

Configureer IPSec-profielen waarin IKEv2-profielen worden gekoppeld aan Transformatiesets:

```
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
```

Virtuele tunnelinterfaces

Deze sectie behandelt configuratie van de Virtuele Interfaces van de Tunnel, en interfaces Loopback die als tunnelbron worden gebruikt.

In besproken labscenario moeten we twee VTI-interface met de enkele peer opzetten met hetzelfde openbare IP-adres. Bovendien heeft ons Cisco IOS XE-apparaat slechts één uitgang met Gigabit Ethernet1.

Cisco IOS XE biedt geen ondersteuning voor de configuratie van meer dan één VTI met dezelfde tunnelbron en dezelfde tunnelbestemming.

Om deze beperking te overwinnen, kunt u Loopback interfaces gebruiken en ze definiëren als tunnelbron in respectieve VTI.

Er zijn weinig opties om IP-verbinding te bereiken tussen Loopback en SSE publieke IP-adres:

1. Wijs publiekelijk routable IP-adres toe aan de Loopback-interface (vereist eigendom van publieke IP-adresruimte)
2. Wijs privé IP-adres toe aan de Loopback-interface en dynamisch aan NAT-verkeer met

behulp van Loopback IP-bron.
3. Gebruik VASI-interfaces (niet ondersteund op veel platforms, moeilijk in te stellen en problemen op te lossen)

In dit scenario gaan we het hebben over de tweede optie.

Configureer twee Loopback-interfaces en voeg onder elk ervan de opdracht "ip Nat inside" toe.

```
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
```

Definieer dynamische NAT-toegangscontrolelijst en NAT-overbelastingsverklaring:

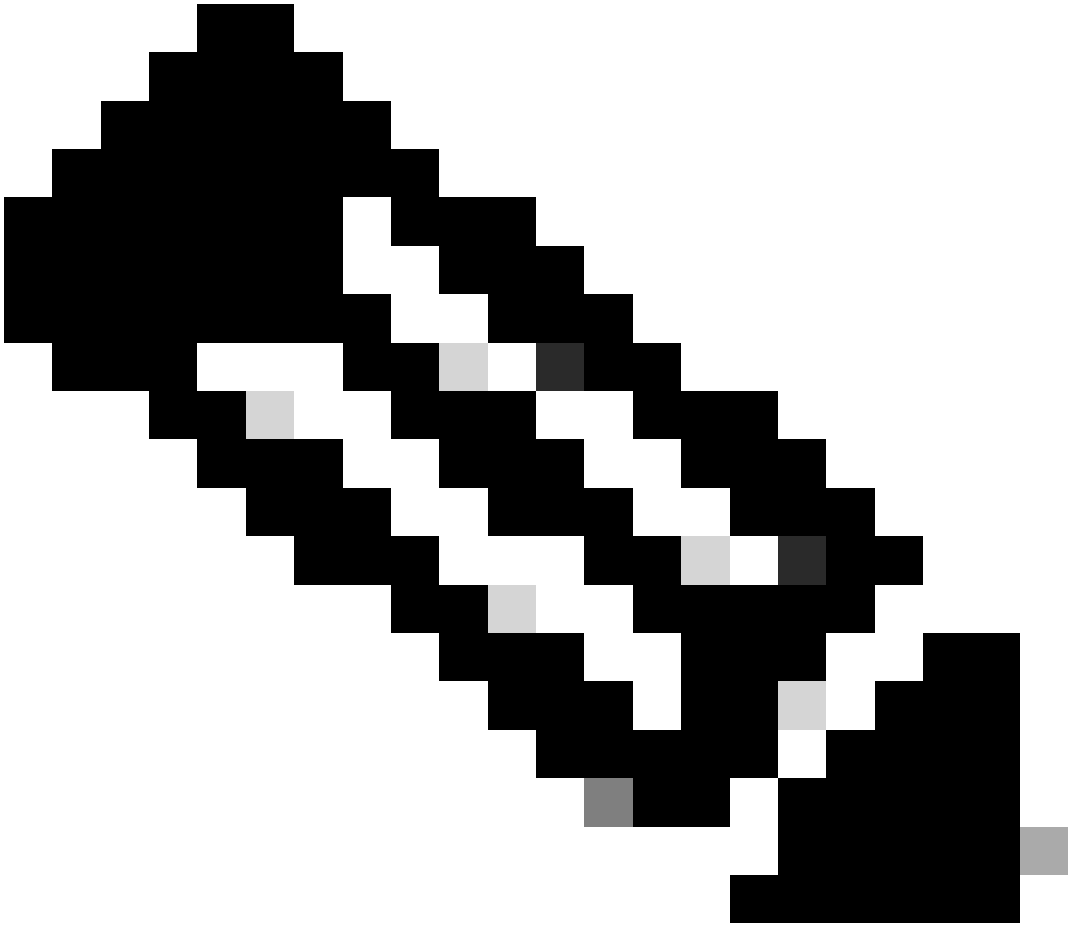
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

Virtuele tunnelinterfaces configureren.

```
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
```



Opmerking: in het beschreven laboratoriumscenario zijn IP-adressen die aan VTI's zijn toegewezen, afkomstig van niet-overlappende subnetten van 169.254.0.0/24.
U kunt andere subnetruimte gebruiken, maar er zijn bepaalde vereisten met betrekking tot BGP die dergelijke adresruimte vereisen.

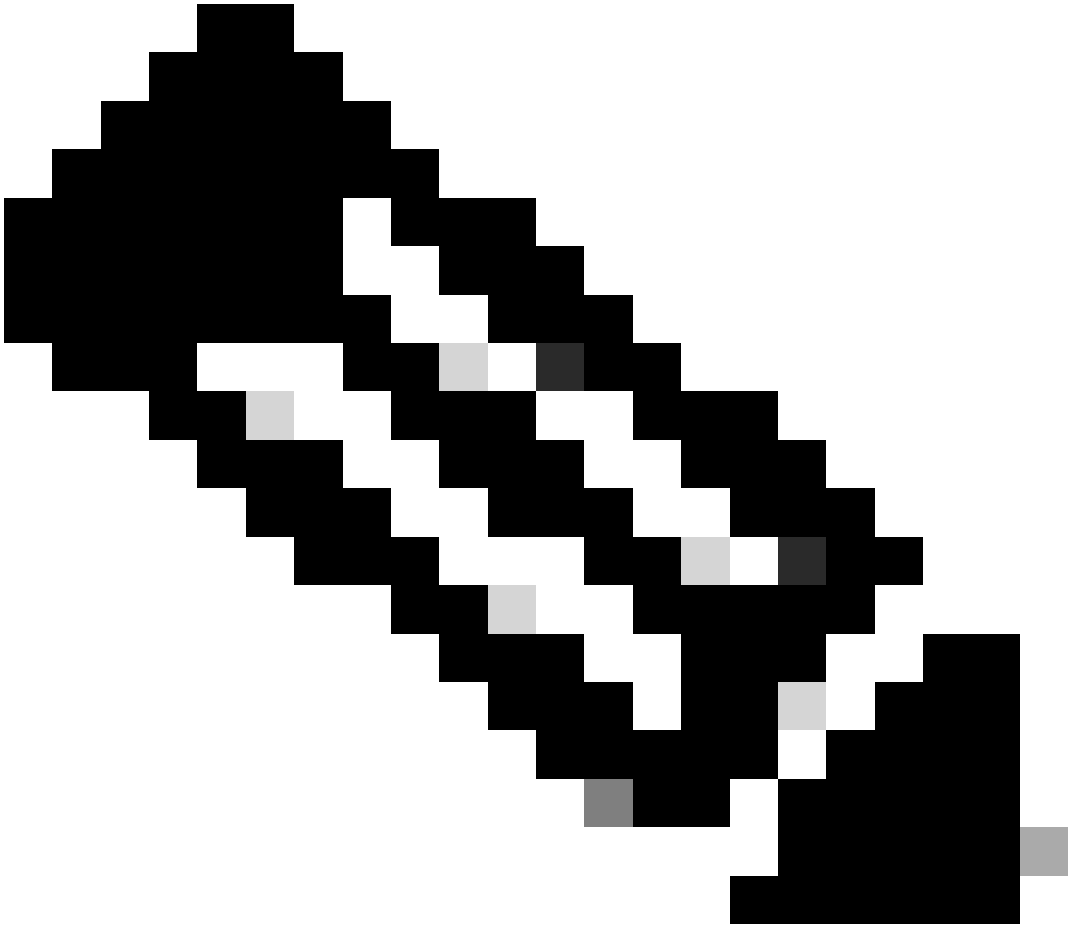
BGP-routing

Deze paragraaf behandelt het configuratieonderdeel dat nodig is om de BGP-buurt met SSE-head-end te maken.
BGP-proces op SSE-head-end luistert op elke IP van subnetwerkkaart 169.254.0.0/24 .
Om BGP peering over beide VTIs te vestigen, gaan wij twee buren 169.254.0.9 (Tunnel1) en 169.254.0.13 (Tunnel2) bepalen.
Ook moet u de Remote AS specificeren volgens de waarde die op het SSE-dashboard wordt gezien.

<#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

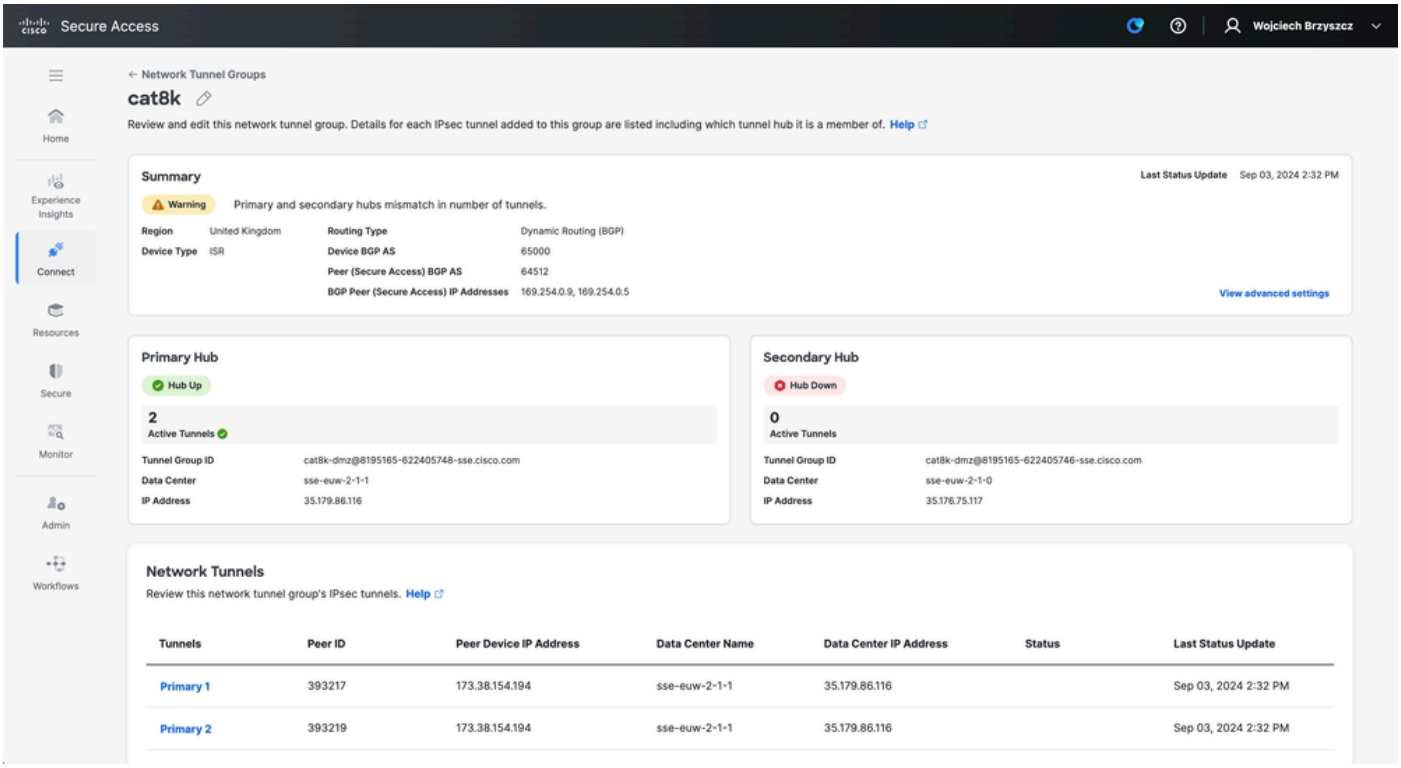


Opmerking: routers die van beide peers worden ontvangen, moeten exact hetzelfde zijn. Door standaardrouter installeert slechts één van hen in de routerlijst.
U moet "maximum-paden <aantal routes>"configureren als u meer dan één dubbele route in een routeringstabel wilt kunnen installeren (en ECMP wilt inschakelen).

Verifiëren

Secure Access Dashboard

U moet twee Primaire tunnels in SSE dashboard zien:



Cisco IOS XE router

Controleer of beide tunnels zich in de KLAAR-staat bevinden vanaf de zijde 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
```

Controleer of de BGP-groep met beide peers actief is:

<#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
```

Controleer dat de router de juiste routes van BGP leert (en er zijn minstens twee volgende hop geïnstalleerd in de routeringstabel).

<#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
```

Start het verkeer en controleer of beide tunnels worden gebruikt en u ziet dat er steeds meer omheiningen en decaps worden weergegeven voor beide.

<#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
```

Optioneel kunt u pakketvastlegging op beide VTI-interfaces verzamelen om ervoor te zorgen dat het verkeer tussen VTI's wordt gebalanceerd. Lees de instructies in dit artikel om Embedded Packet Capture te configureren op Cisco IOS XE-apparaat.
In het voorbeeld, was de gastheer achter Cisco IOS XE router met bron IP 192.168.150.1 ICMP verzoeken naar veelvoud IPs van 192.168.200.0/24 subnetnet verzenden.

Zoals u ziet, zijn ICMP-verzoeken gelijk verdeeld tussen de tunnels.

<#root>

```
wbrzyszc-cat8k#
```

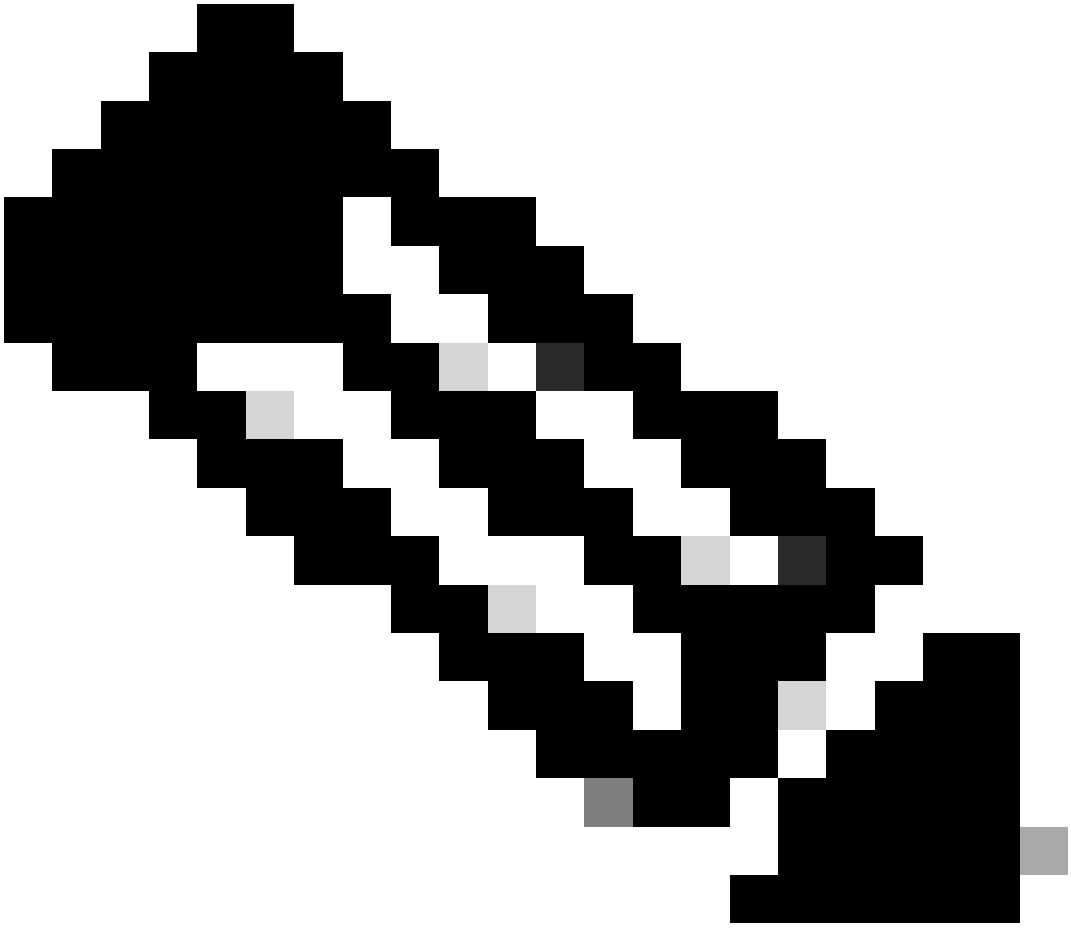
show monitor capture Tunnel1 buffer brief

```
------------------------------------------------------------------------------
#   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
```



Opmerking: er zijn meerdere ECMP-mechanismen voor taakverdeling op Cisco IOS XE-routers. Standaard is taakverdeling per bestemming ingeschakeld, waardoor verkeer naar dezelfde bestemming als IP altijd hetzelfde pad volgt.
U kunt taakverdeling per pakket configureren, waarbij willekeurig ook verkeer voor dezelfde bestemming als IP wordt geladen.

Gerelateerde informatie

- Gebruikershandleiding voor Secure Access
- Ingesloten pakketvastlegging verzamelen
- Technische ondersteuning en documentatie – Cisco Systems

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.