Konfigurieren von Netzwerktunneln zwischen Cisco Secure Access und IOS XE Router mit ECMP und BGP

Inhalt

Einleitung

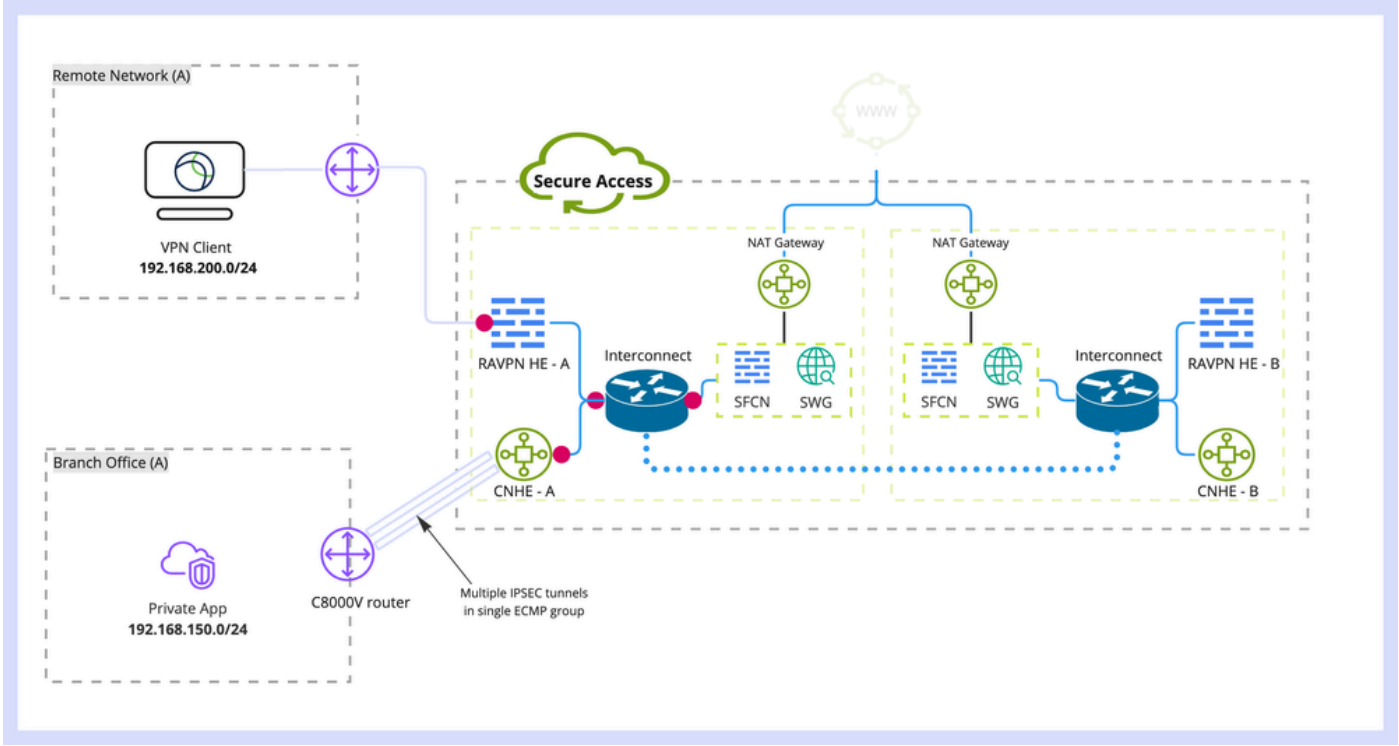
In diesem Dokument werden die erforderlichen Schritte zur Konfiguration und Fehlerbehebung des IPSec VPN-Tunnels zwischen Cisco Secure Access und Cisco IOS XE mithilfe von BGP und ECMP beschrieben.

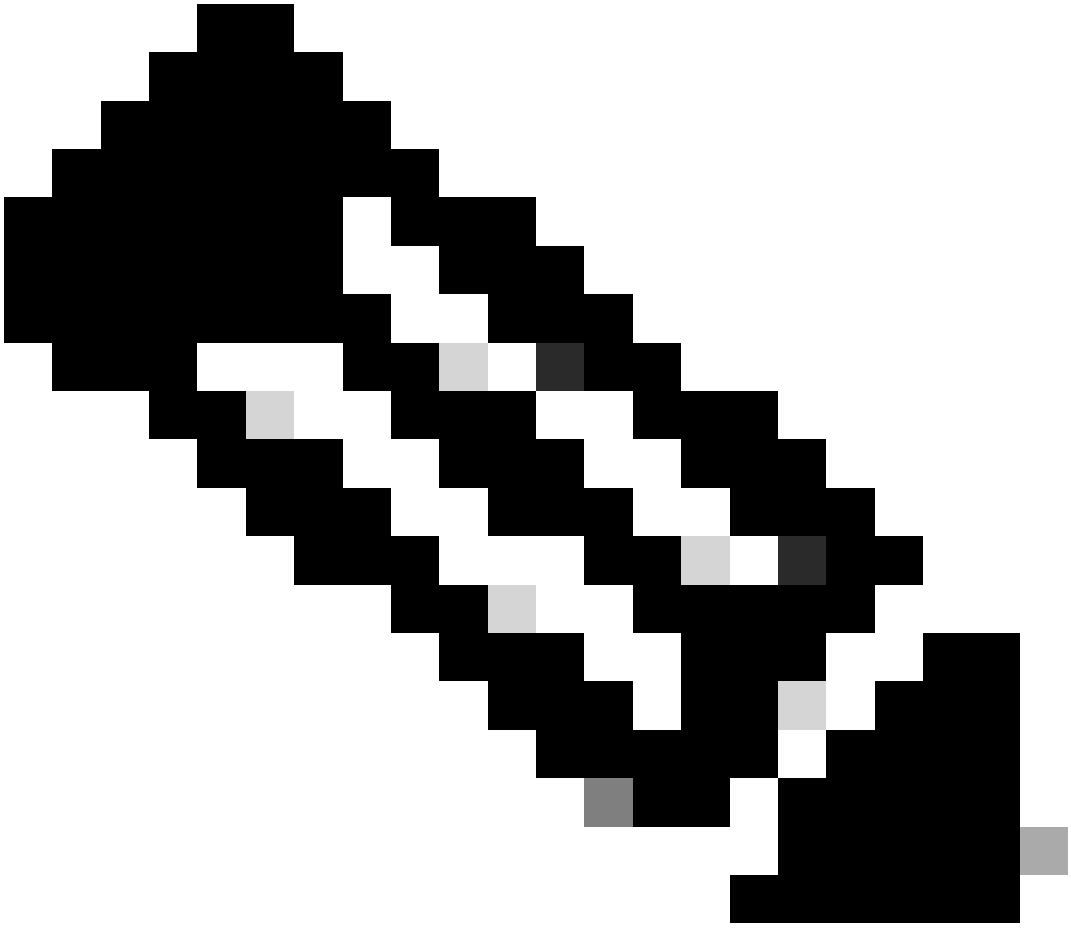
Netzwerkdiagramm

In diesem Lab-Beispiel werden wir ein Szenario behandeln, in dem das Netzwerk 192.168.150.0/24 ein LAN-Segment hinter dem Cisco IOS XE-Gerät ist und 192.168.200.0/24 ein IP-Pool ist, der von RAVPN-Benutzern verwendet wird, die eine Verbindung mit dem Secure Access-Headend herstellen.

Unser Ziel ist es, ECMP in VPN-Tunneln zwischen dem Cisco IOS XE-Gerät und dem Secure Access-Headend zu verwenden.

Um die Topologie besser zu verstehen, schauen Sie bitte in das Diagramm:


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



Hinweis: Dies ist nur ein Beispiel für einen Paketfluss. Sie können die gleichen Prinzipien auf alle anderen Flüsse und auf den sicheren Internetzugriff vom Subnetz 192.168.150.0/24 hinter dem Cisco IOS XE-Router anwenden.

Voraussetzungen

Anforderungen

Es wird empfohlen, dass Sie über Kenntnisse in den folgenden Themen verfügen:

- Konfiguration und Verwaltung der Cisco IOS XE CLI
- Grundkenntnisse der IKEv2- und IPSec-Protokolle
- Erstkonfiguration von Cisco IOS XE (IP-Adressierung, SSH, Lizenz)
- Grundlegende Kenntnisse über BGP und ECMP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V mit 17.9.4a-Softwareversion
- Windows-PC
- Cisco Secure Access-Organisation

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Netzwerktunnel in Secure Access verfügen über eine Bandbreitenbeschränkung von 1 Gbit/s pro Tunnel. Wenn Ihre Upstream-/Downstream-Internetbandbreite größer als 1 Gbit/s ist und Sie sie vollständig nutzen möchten, müssen Sie diese Einschränkung überwinden, indem Sie mehrere Tunnel mit demselben Rechenzentrum für sicheren Zugriff konfigurieren und sie in einer einzigen ECMP-Gruppe gruppieren.

Wenn Sie mehrere Tunnel mit einer einzigen Netzwerk-Tunnelgruppe (innerhalb eines einzigen sicheren Zugangs-Rechenzentrums) terminieren, bilden diese standardmäßig die ECMP-Gruppe aus Sicht des Secure Access-Headends.
Sobald das Secure Access-Headend Datenverkehr an das standortbasierte VPN-Gerät sendet, erfolgt ein Lastausgleich zwischen den Tunneln (vorausgesetzt, die richtigen Routen werden von BGP-Peers empfangen).

Um die gleiche Funktionalität für das lokale VPN-Gerät zu erreichen, müssen Sie mehrere VTI-Schnittstellen auf einem einzigen Router konfigurieren und sicherstellen, dass die richtige Routing-Konfiguration angewendet wird.

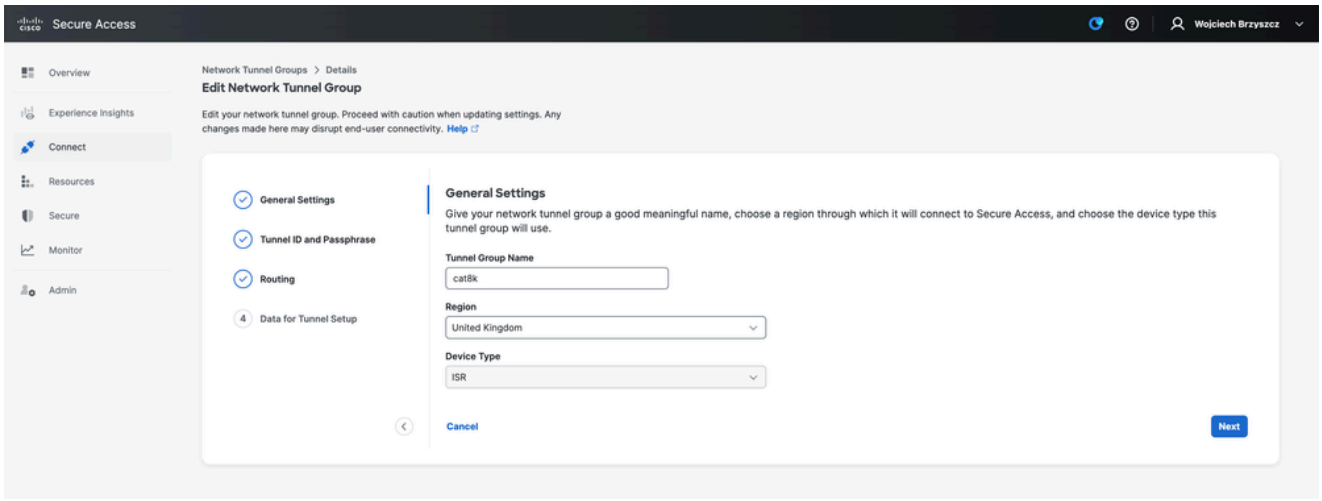
In diesem Artikel wird ein Szenario beschrieben, in dem die einzelnen erforderlichen Schritte erläutert werden.

Konfigurieren

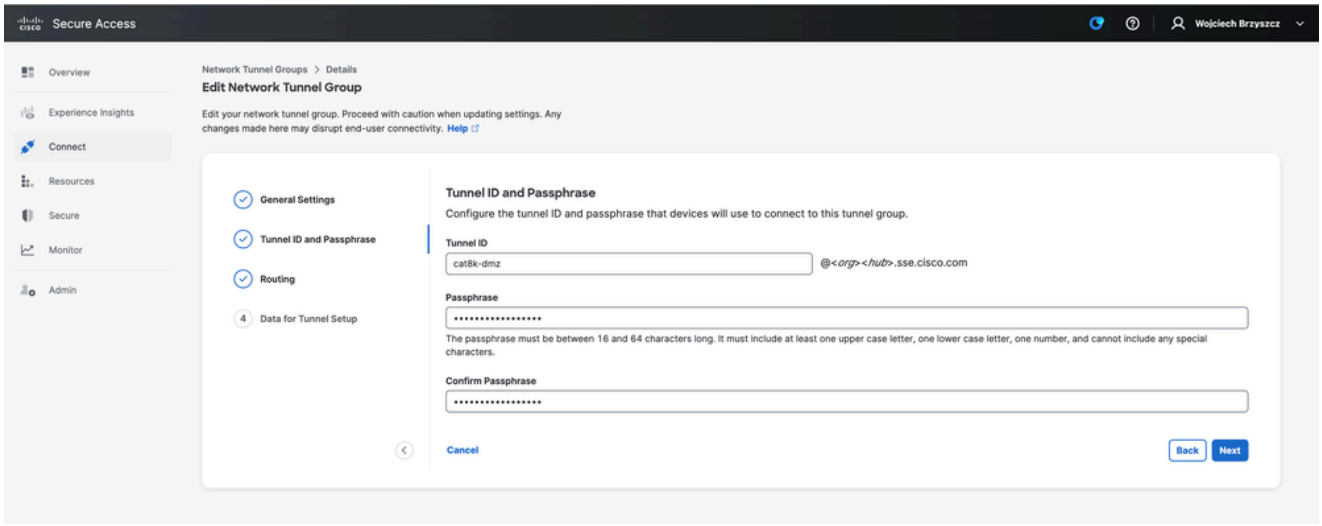
Konfiguration des sicheren Zugriffs

Für den sicheren Zugriff muss keine spezielle Konfiguration angewendet werden, um mithilfe des BGP-Protokolls eine ECMP-Gruppe aus mehreren VPN-Tunneln zu bilden.
Erforderliche Schritte zum Konfigurieren der Netzwerk-Tunnelgruppe.

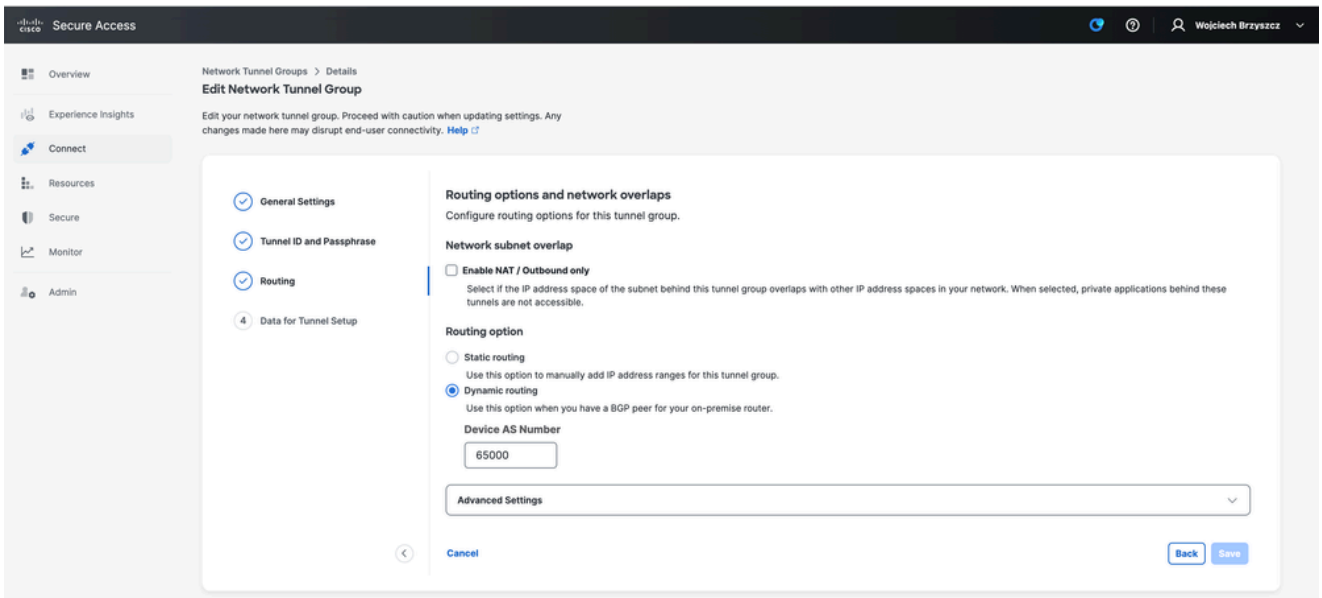
1. Erstellen Sie eine neue Netzwerk-Tunnelgruppe (oder bearbeiten Sie eine vorhandene).



2. Tunnel-ID und Passphrase angeben:



3. Konfigurieren Sie Routing-Optionen, geben Sie Dynamic Routing an, und geben Sie Ihre interne AS-Nummer ein. In diesem Übungsszenario entspricht ASN 65000.



4. Notieren Sie Tunnel-Details aus dem Abschnitt "Daten für Tunnel-Setup".

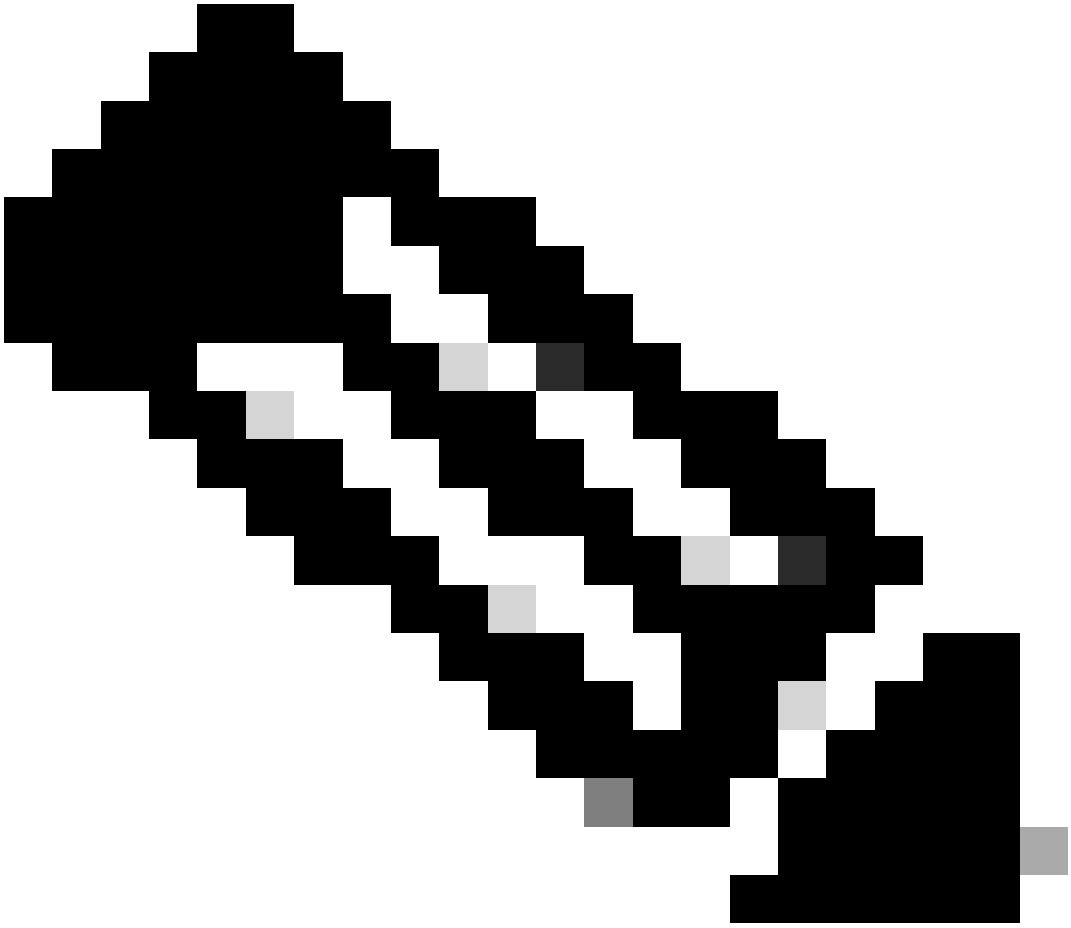
Cisco IOS XE-Konfiguration

In diesem Abschnitt wird die CLI-Konfiguration beschrieben, die auf den Cisco IOS XE-Router angewendet werden muss, um IKEv2-Tunnel, die BGP-Nachbarschaft und den ECMP-Lastenausgleich über virtuelle Tunnelschnittstellen hinweg ordnungsgemäß zu konfigurieren. Jeder Abschnitt wird erläutert, und die häufigsten Vorbehalte werden genannt.

IKEv2- und IPsec-Parameter

Konfigurieren der IKEv2-Richtlinie und des IKEv2-Vorschlags Diese Parameter legen fest, welche Algorithmen für IKE SA verwendet werden (Phase 1):

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

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



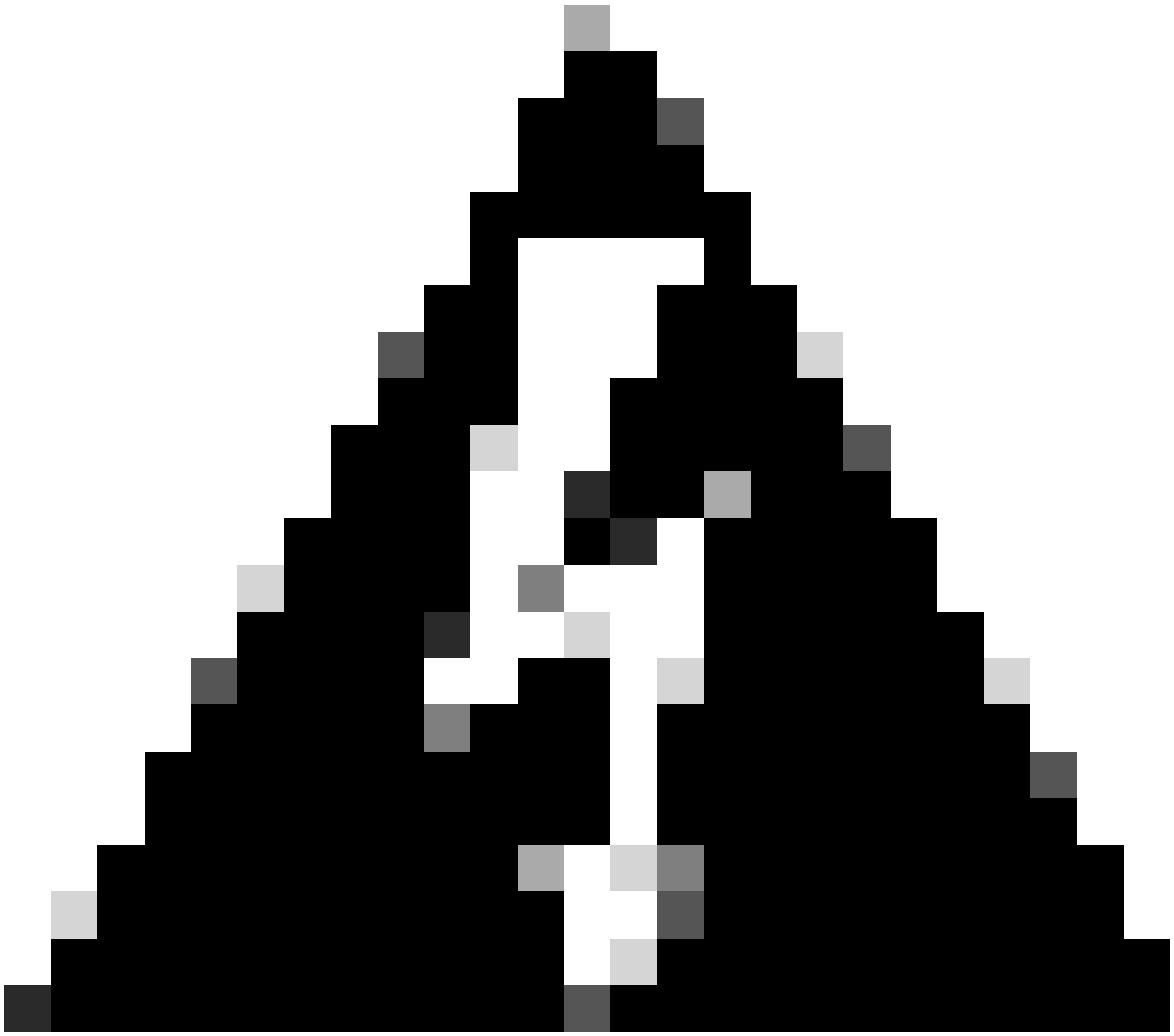
Hinweis: Empfohlene und optimale Parameter sind in den SSE-Dokumenten fett markiert: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Definieren Sie einen IKEv2-Keyring, der die Headend-IP-Adresse und den Pre-Shared Key für die Authentifizierung mit dem SSE-Headend definiert:

```
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>
```

Konfigurieren Sie zwei IKEv2-Profile.
Sie definieren, welche IKE-Identität verwendet wird, um eine Übereinstimmung mit dem Remote-

Peer herzustellen, und welche IKE-Identität der lokale Router an den Peer sendet.
Die IKE-Identität des SSE-Headends ist vom IP-Adresstyp und entspricht der öffentlichen IP-Adresse des SSE-Headends.



Warnung: Um mehrere Tunnel mit derselben Netzwerk-Tunnelgruppe auf SSE-Seite einzurichten, müssen alle dieselbe lokale IKE-Identität verwenden.
Cisco IOS XE unterstützt dieses Szenario nicht, da pro Tunnel ein eindeutiges Paar lokaler und Remote-IKE-Identitäten erforderlich ist.
Um diese Einschränkung zu umgehen, wurde das SSE-Headend so erweitert, dass es IKE-ID im folgenden Format akzeptiert:
<tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

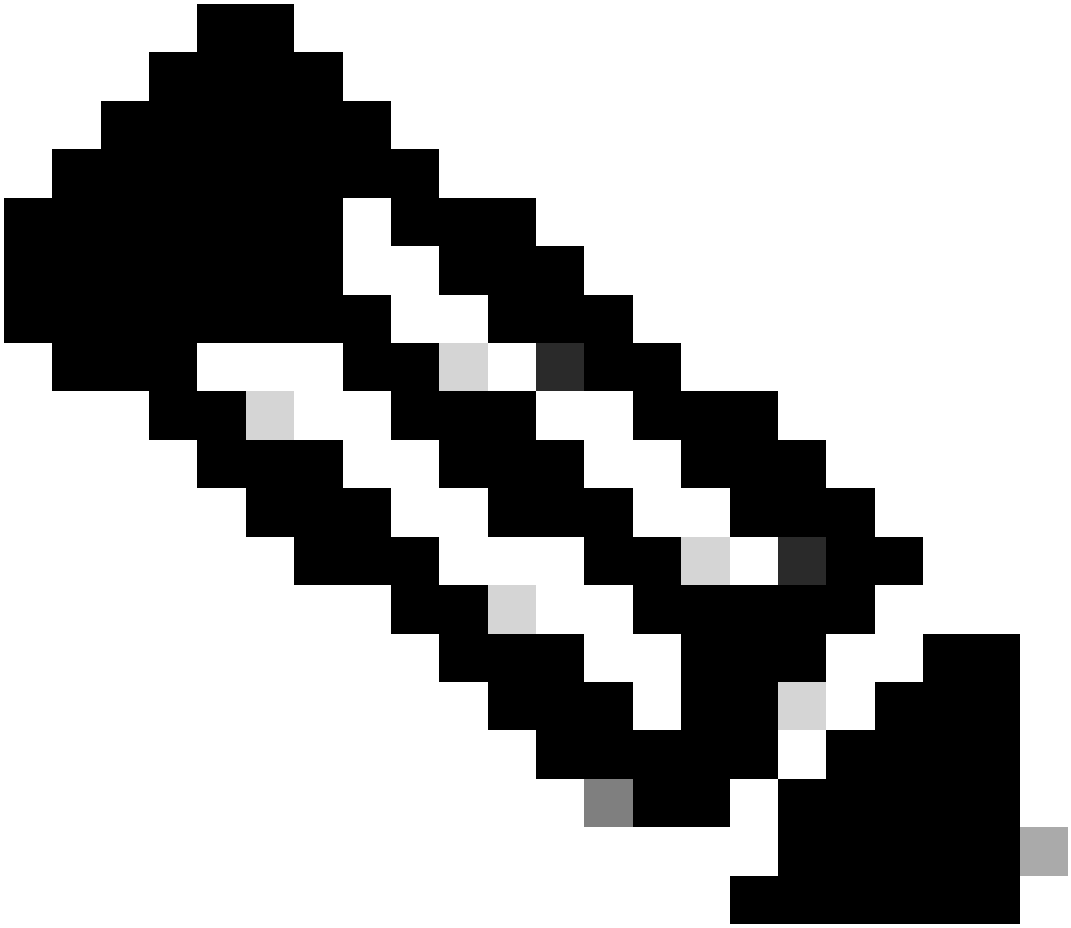
Im besprochenen Übungsszenario wurde die Tunnel-ID als cat8k-dmz definiert.
Im normalen Szenario wird der Router so konfiguriert, dass die lokale IKE-Identität als cat8k-dmz@8195165-622405748-sse.cisco.com gesendet wird.

Um jedoch mehrere Tunnel mit derselben Netzwerk-Tunnelgruppe einzurichten, werden lokale

IKE-IDs verwendet:

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

Beachten Sie das Suffix, das jeder Zeichenfolge hinzugefügt wird (tunnel1 und tunnel2).



> Hinweis: Die genannten lokalen IKE-Identitäten dienen lediglich als Beispiel in diesem Lab-Szenario. Sie können jedes Suffix definieren, das Sie wünschen, stellen Sie einfach sicher, dass die Anforderungen erfüllt werden.

```
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
```

IPSec-Transformationssatz konfigurieren Diese Einstellung definiert Algorithmen, die für die IPsec-Sicherheitszuordnung verwendet werden (Phase 2):

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

Konfigurieren Sie IPSec-Profile, die IKEv2-Profile mit Transformationssätzen verknüpfen:

```
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
```

Virtuelle Tunnelschnittstellen

In diesem Abschnitt wird die Konfiguration von virtuellen Tunnelschnittstellen und Loopback-Schnittstellen, die als Tunnelquelle verwendet werden, beschrieben.

Im beschriebenen Lab-Szenario müssen wir zwei VTI-Schnittstellen mit einem Peer unter Verwendung derselben öffentlichen IP-Adresse einrichten. Unser Cisco IOS XE-Gerät verfügt zudem nur über eine Ausgangsschnittstelle GigabitEthernet1.

Cisco IOS XE unterstützt keine Konfiguration von mehr als einem VTI mit derselben Tunnelquelle und demselben Tunnelziel.

Um diese Einschränkung zu umgehen, können Sie Loopback-Schnittstellen verwenden und diese als Tunnelquelle in den jeweiligen VTIs definieren.

Es gibt nur wenige Optionen, um eine IP-Verbindung zwischen Loopback und öffentlichen SSE-IP-Adressen herzustellen:

1. Zuweisen einer öffentlich routbaren IP-Adresse zu einer Loopback-Schnittstelle (erfordert

das Eigentum an öffentlichem IP-Adressraum)
2. Weisen Sie der Loopback-Schnittstelle eine private IP-Adresse zu, und führen Sie dynamisch NAT-Datenverkehr über die Loopback-IP-Quelle durch.
3. Verwendung von VASI-Schnittstellen (wird auf vielen Plattformen nicht unterstützt, aufwändige Einrichtung und Fehlerbehebung)

In diesem Szenario werden wir über die zweite Option sprechen.

Konfigurieren Sie zwei Loopback-Schnittstellen, und fügen Sie jeweils den Befehl "ip nat inside" hinzu.

```
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
```

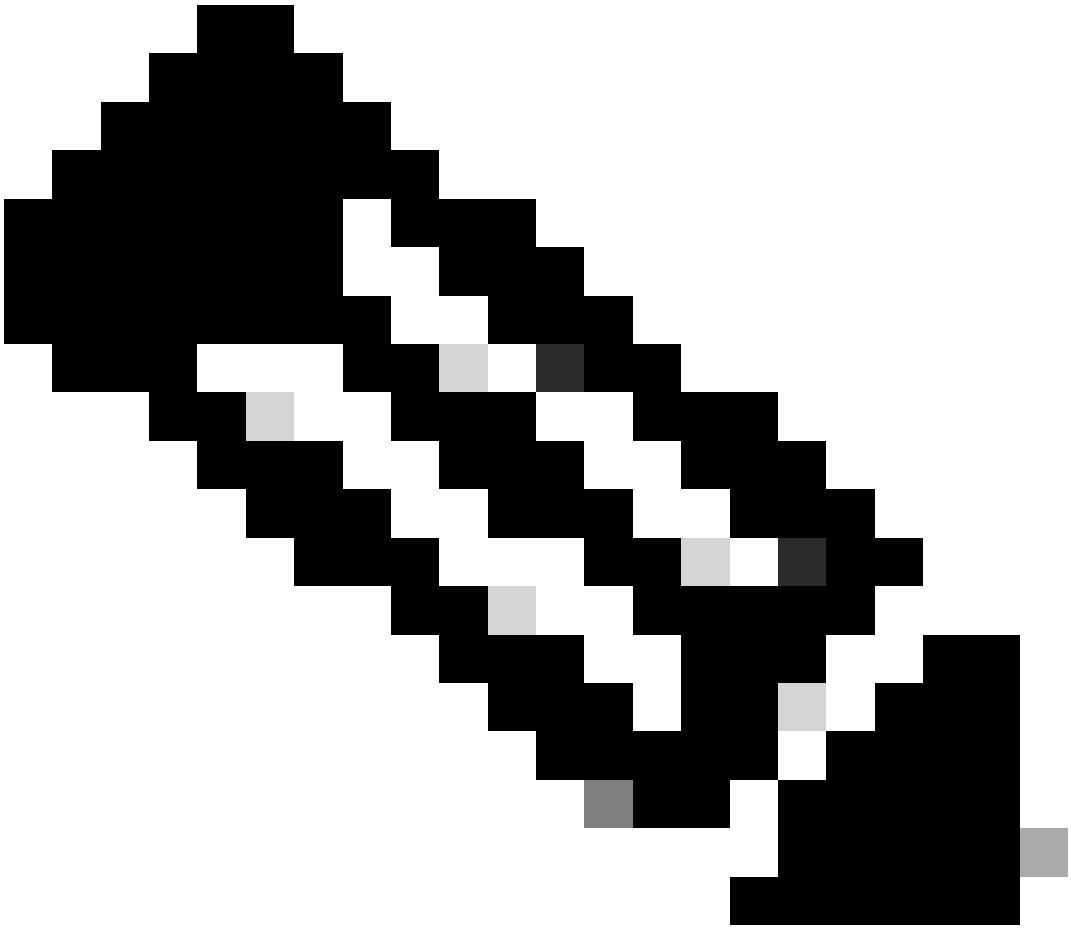
Definieren einer dynamischen NAT-Zugriffskontrollliste und einer NAT-Überlastungsanweisung:

```
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
```

Konfigurieren virtueller Tunnelschnittstellen

```
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
```



> Hinweis: Im beschriebenen Übungsszenario stammen die VTIs zugewiesenen IP-Adressen aus sich nicht überlappenden Subnetzen von 169.254.0.0/24.
> Sie können anderen Subnetzbereich verwenden, aber es gibt bestimmte BGP-Anforderungen, die einen solchen Adressbereich erfordern.

BGP-Routing

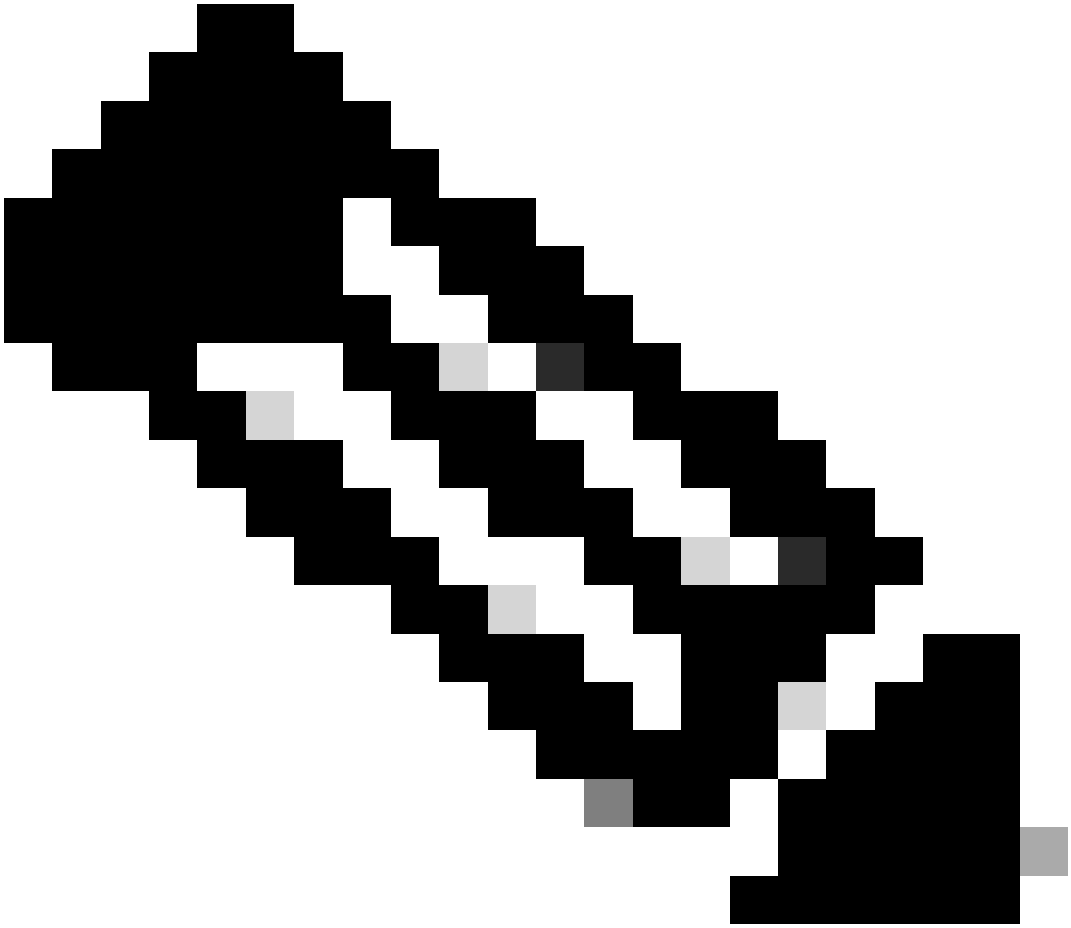
In diesem Abschnitt wird der erforderliche Konfigurationsteil zur Einrichtung einer BGP-Nachbarschaft mit dem SSE-Headend beschrieben.
Der BGP-Prozess am SSE-Headend hört alle IP-Adressen vom Subnetz ab. 169.254.0.0/24.
Um BGP-Peering für beide VTIs einzurichten, werden zwei Nachbarn definiert: 169.254.0.9 (Tunnel1) und 169.254.0.13 (Tunnel2).

Außerdem müssen Sie das Remote-AS entsprechend dem im SSE-Dashboard angezeigten Wert angeben.

<#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



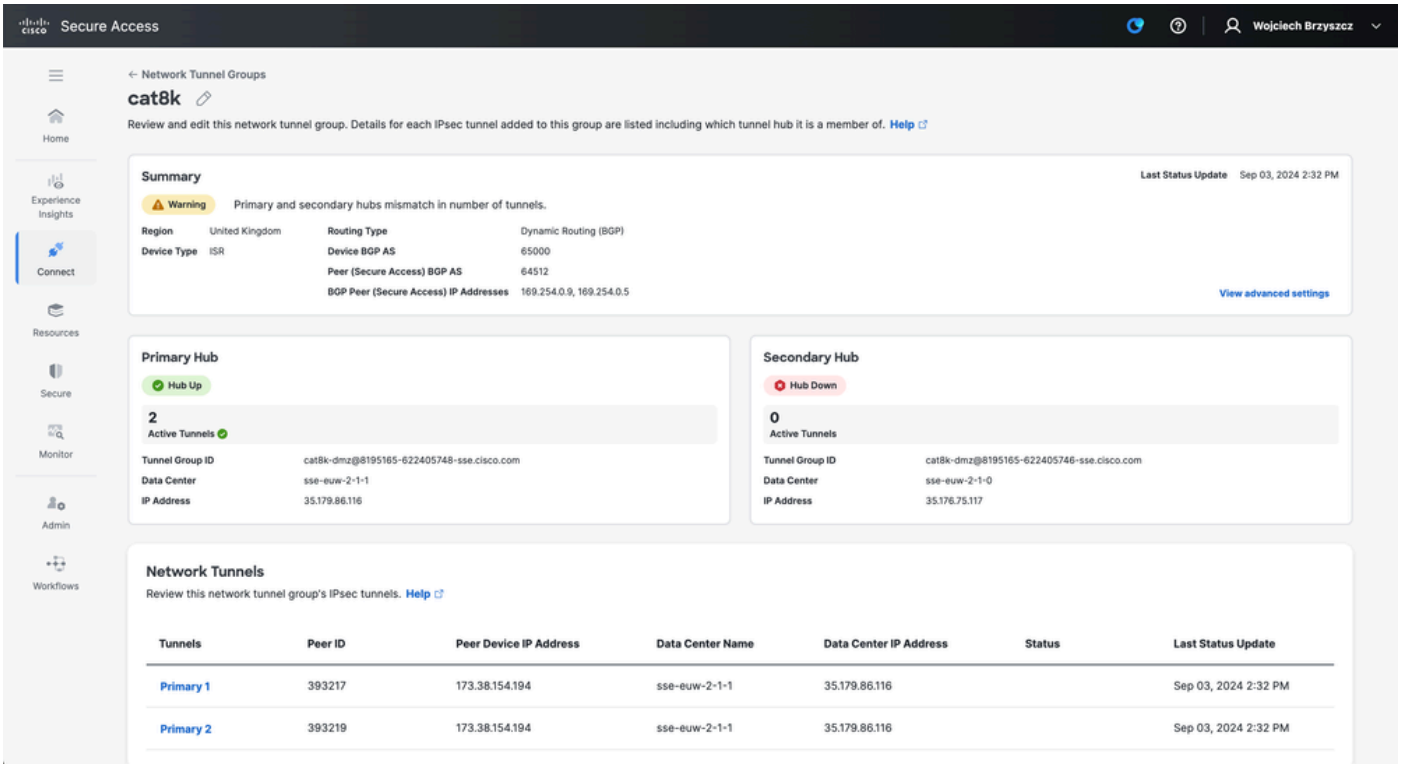
Hinweis: Die von beiden Peers empfangenen Routen müssen identisch sein. Standardmäßig installiert der Router nur eine dieser Komponenten in der Routing-Tabelle.

Damit mehrere doppelte Routen in der Routing-Tabelle installiert werden können (und ECMP aktiviert wird), müssen Sie "maximum-paths <Anzahl der Routen>" konfigurieren.

Überprüfung

Dashboard für sicheren Zugriff

Im SSE-Dashboard müssen zwei primäre Tunnel angezeigt werden:



Cisco IOS XE-Router

Vergewissern Sie sich, dass beide Tunnel von Cisco IOS XE-Seite aus BEREIT sind:

<#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
```

Stellen Sie sicher, dass die BGP-Nachbarschaft mit beiden Peers verfügbar ist:

<#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
```

Überprüfen Sie, ob der Router die richtigen Routen vom BGP bezieht (und in der Routing-Tabelle mindestens zwei weitere Hops installiert sind).

<#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
```

Initiieren Sie Datenverkehr, und stellen Sie sicher, dass beide Tunnel genutzt werden. Die Anzahl der Encaps und Decaps steigt für beide an.

<#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
```

Optional können Sie die Paketerfassung an beiden VTI-Schnittstellen erfassen, um sicherzustellen, dass ein Lastenausgleich zwischen den VTIs erfolgt. Lesen Sie die Anweisungen in diesem Artikel, um Embedded Packet Capture auf dem Cisco IOS XE-Gerät zu konfigurieren. Im Beispiel sendete der Host hinter dem Cisco IOS XE-Router mit der Quell-IP 192.168.150.1 ICMP-Anfragen vom 192.168.200.0/24-Subnetz an mehrere IPs.

Wie Sie sehen, wird bei ICMP-Anforderungen die Last zwischen den Tunneln gleichmäßig verteilt.

<#root>

```
wbrzyszc-cat8k#
```

show monitor capture Tunnel1 buffer brief

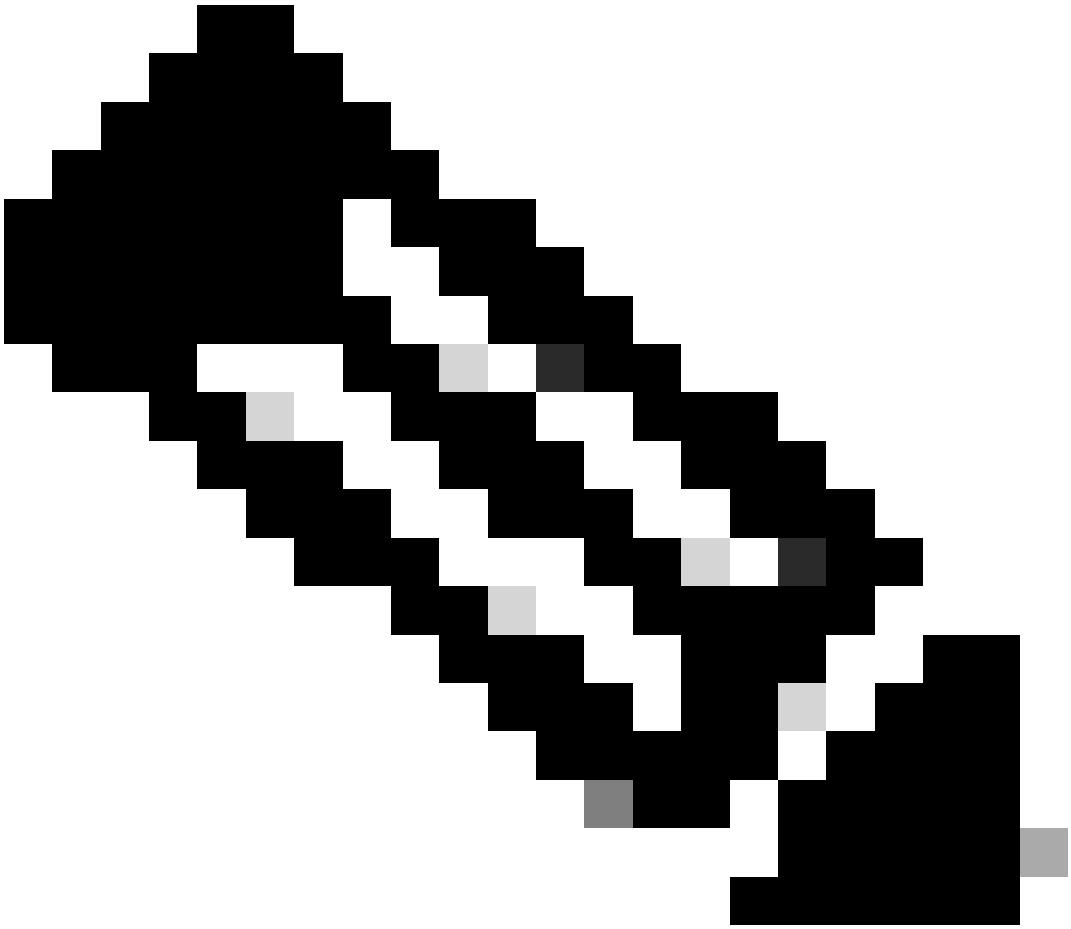
```
----------------------------------------------------------------------------
#   size   timestamp     source     destination      dscp    protocol
----------------------------------------------------------------------------
   0  114    0.000000   192.168.150.1    ->  192.168.200.2    0  BE   ICMP
   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
```



Hinweis: Es gibt mehrere ECMP-Lastverteilungsmechanismen für Cisco IOS XE-Router. Standardmäßig ist Load Balancing nach Ziel aktiviert, wodurch sichergestellt wird, dass der Datenverkehr mit derselben Ziel-IP-Adresse immer den gleichen Pfad verwendet. Sie können einen Lastenausgleich pro Paket konfigurieren, bei dem der Lastenausgleich-Datenverkehr auch für dieselbe Ziel-IP zufällig erfolgt.

Zugehörige Informationen

- Benutzerhandbuch zu Secure Access
- Sammeln von eingebetteter Paketerfassung
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.