Configuration d'un tunnel réseau entre Cisco Secure Access et le routeur IOS XE à l'aide d'ECMP avec BGP

Table des matières

Introduction

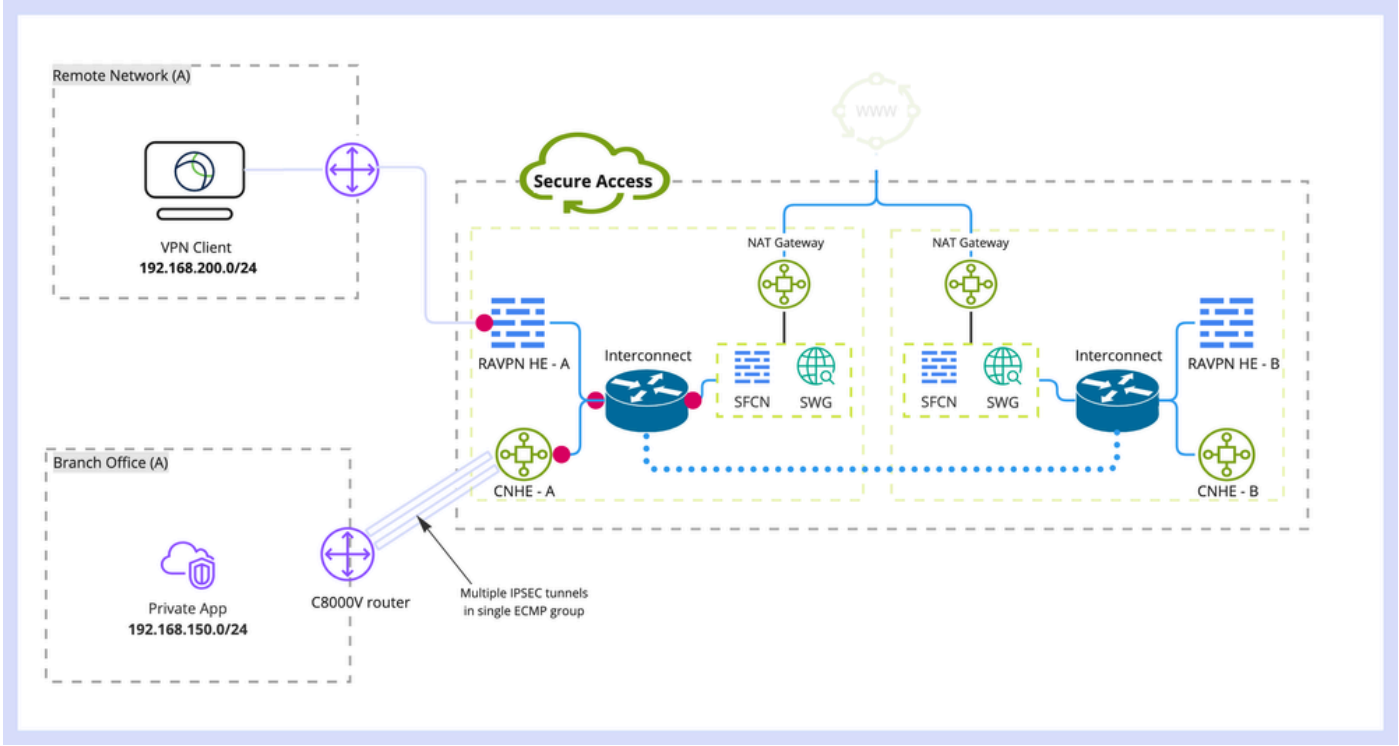
Ce document décrit les étapes requises pour configurer et dépanner un tunnel VPN IPSec entre Cisco Secure Access et Cisco IOS XE en utilisant BGP et ECMP.

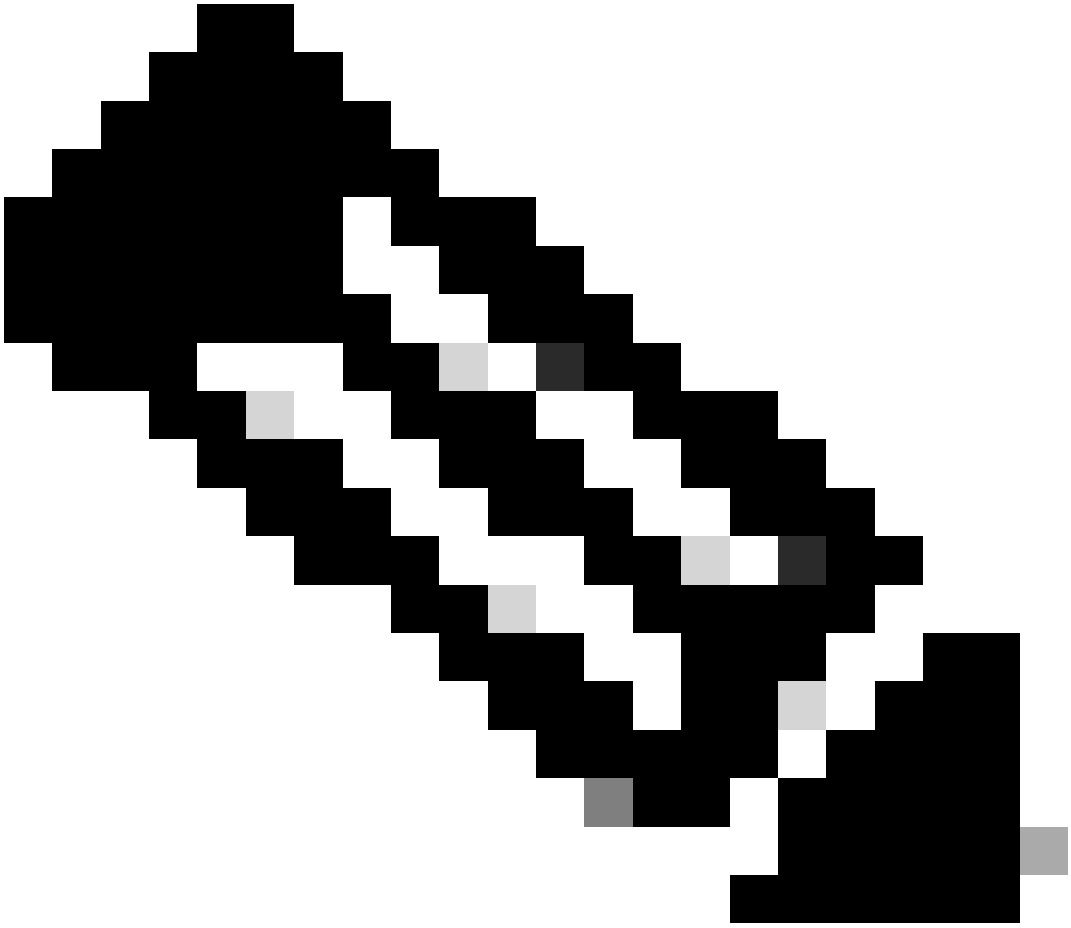
Diagramme du réseau

Dans cet exemple de travaux pratiques, nous allons aborder un scénario dans lequel le réseau 192.168.150.0/24 est un segment LAN derrière le périphérique Cisco IOS XE, et 192.168.200.0/24 est un pool IP utilisé par les utilisateurs RAVPN se connectant à la tête de réseau d'accès sécurisé.

Notre objectif final est d'utiliser le protocole ECMP sur les tunnels VPN entre le périphérique Cisco IOS XE et la tête de réseau Secure Access.

Afin de mieux comprendre la topologie, veuillez vous reporter au schéma :


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



Remarque : il s'agit d'un exemple de flux de paquets. Vous pouvez appliquer les mêmes principes à tous les autres flux et à l'accès Internet sécurisé à partir du sous-réseau 192.168.150.0/24 derrière le routeur Cisco IOS XE.

Conditions préalables

Exigences

Il est recommandé que vous ayez des connaissances sur les sujets suivants :

- Configuration et gestion de l'interface de ligne de commande Cisco IOS XE
- Connaissances de base des protocoles IKEv2 et IPSec
- Configuration initiale de Cisco IOS XE (adressage IP, SSH, licence)
- Connaissances de base de BGP et ECMP

Composants utilisés

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

- C8000V exécutant la version logicielle 17.9.4a
- PC Windows
- Organisation Cisco Secure Access

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.

Informations générales

Les tunnels réseau dans Secure Access ont une limitation de bande passante de 1 Gbit/s par tunnel unique. Si votre bande passante Internet en amont/aval est supérieure à 1 Gbit/s et que vous souhaitez l'utiliser pleinement, vous devez surmonter cette limitation en configurant plusieurs tunnels avec le même data center à accès sécurisé et en les regroupant dans un seul groupe ECMP.

Lorsque vous terminez plusieurs tunnels avec le groupe de tunnels réseau unique (au sein d'un contrôleur de domaine d'accès sécurisé unique), ils forment par défaut le groupe ECMP du point de vue de la tête de réseau d'accès sécurisé.
Ce qui signifie qu'une fois que la tête de réseau d'accès sécurisé envoie le trafic vers le périphérique VPN sur site, elle équilibre la charge entre les tunnels (en supposant que les routes correctes sont reçues des homologues BGP).

Afin d'obtenir la même fonctionnalité sur le périphérique VPN sur site, vous devez configurer plusieurs interfaces VTI sur un seul routeur et vous assurer que la configuration de routage appropriée est appliquée.

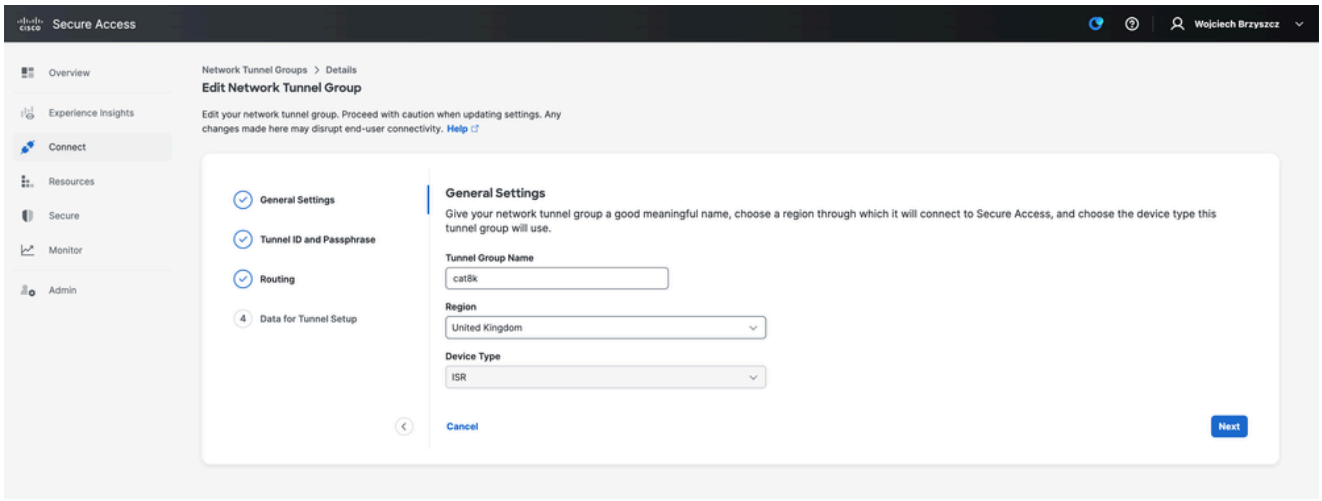
Cet article décrit le scénario, avec une explication de chaque étape requise.

Configurer

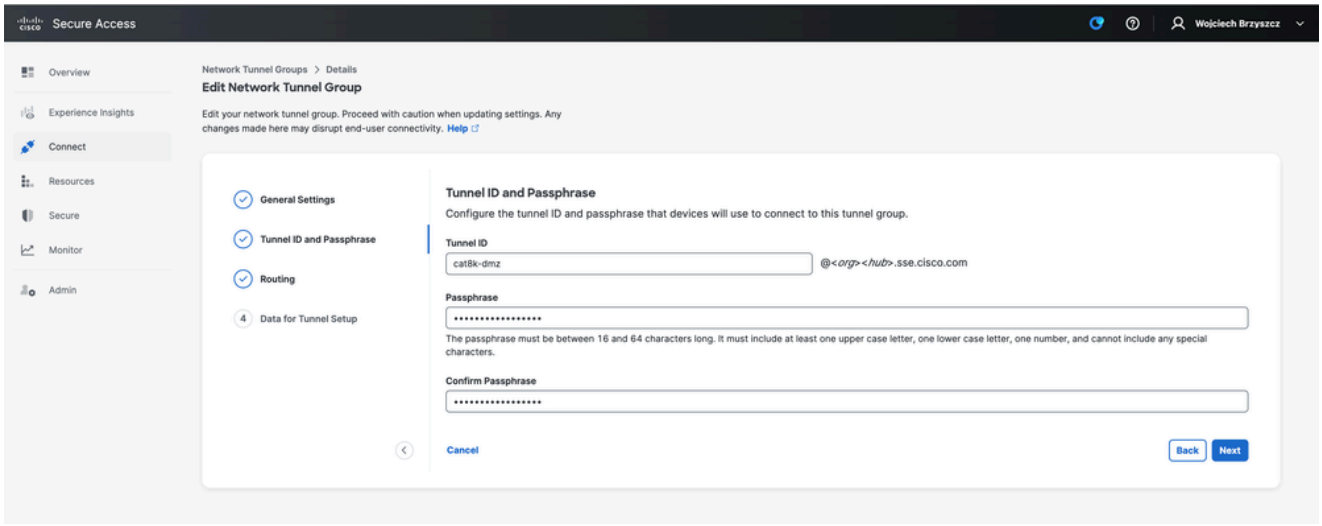
Configuration d'accès sécurisé

Aucune configuration spéciale n'a besoin d'être appliquée du côté de l'accès sécurisé, afin de former un groupe ECMP à partir de plusieurs tunnels VPN utilisant le protocole BGP.
Étapes requises pour configurer le groupe de tunnels réseau.

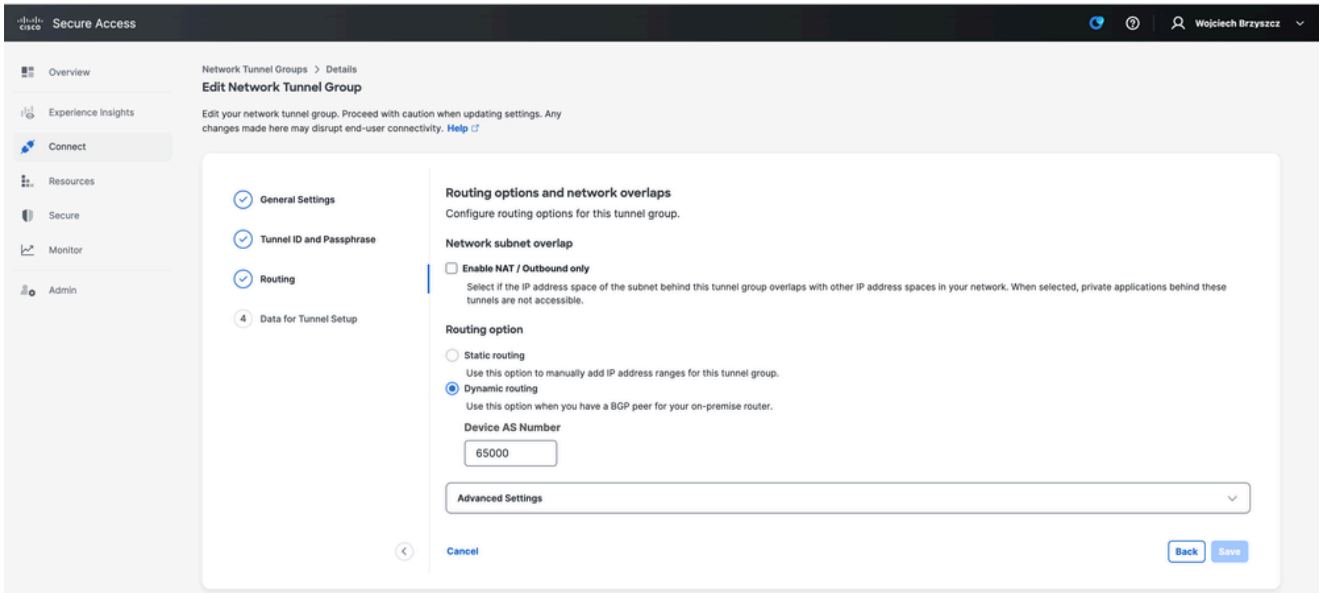
1. Créez un nouveau groupe de tunnels réseau (ou modifiez-en un existant).



2. Spécifiez l'ID de tunnel et la phrase secrète :



3. Configurez les options de routage, spécifiez le routage dynamique et entrez votre numéro AS interne. Dans ce scénario de travaux pratiques, ASN est égal à 65000.



4. Notez les détails du tunnel dans la section Données pour la configuration du tunnel.

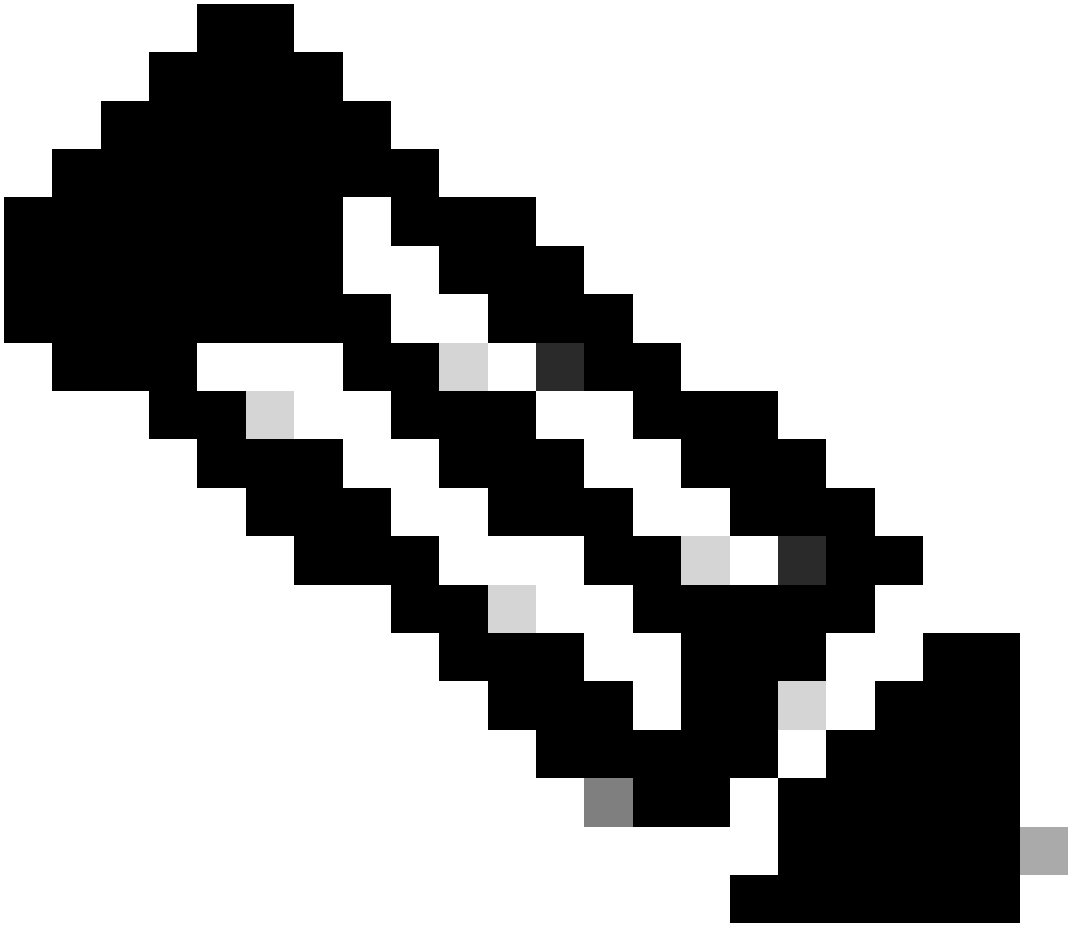
Configuration de Cisco IOS XE

Cette section couvre la configuration CLI qui doit être appliquée sur le routeur Cisco IOS XE, afin de configurer correctement les tunnels IKEv2, le voisinage BGP et l'équilibrage de charge ECMP sur les interfaces de tunnel virtuel.
Chaque section est expliquée et les avertissements les plus courants sont mentionnés.

Paramètres IKEv2 et IPsec

Configurer la stratégie IKEv2 et la proposition IKEv2 Ces paramètres définissent les algorithmes utilisés pour IKE SA (phase 1) :

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

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



Remarque : les paramètres suggérés et optimaux sont indiqués en gras dans les documents SSE : https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Définissez le porte-clés IKEv2 qui définit l'adresse IP de tête de réseau et la clé pré-partagée utilisée pour l'authentification avec la tête de réseau 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>
```

Configurez une paire de profils IKEv2.

Ils définissent le type d'identité IKE à utiliser pour correspondre à l'homologue distant et l'identité IKE que le routeur local envoie à l'homologue.
L'identité IKE de la tête de réseau SSE est de type adresse IP et est égale à l'adresse IP publique de la tête de réseau SSE.

Avertissement : pour établir plusieurs tunnels avec le même groupe de tunnels réseau côté SSE, ils doivent tous utiliser la même identité IKE locale.
Cisco IOS XE ne prend pas en charge un tel scénario, car il nécessite une paire unique d'identités IKE locales et distantes par tunnel.
Afin de surmonter cette limitation, la tête de réseau SSE a été améliorée pour accepter l'ID IKE au format : <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

---

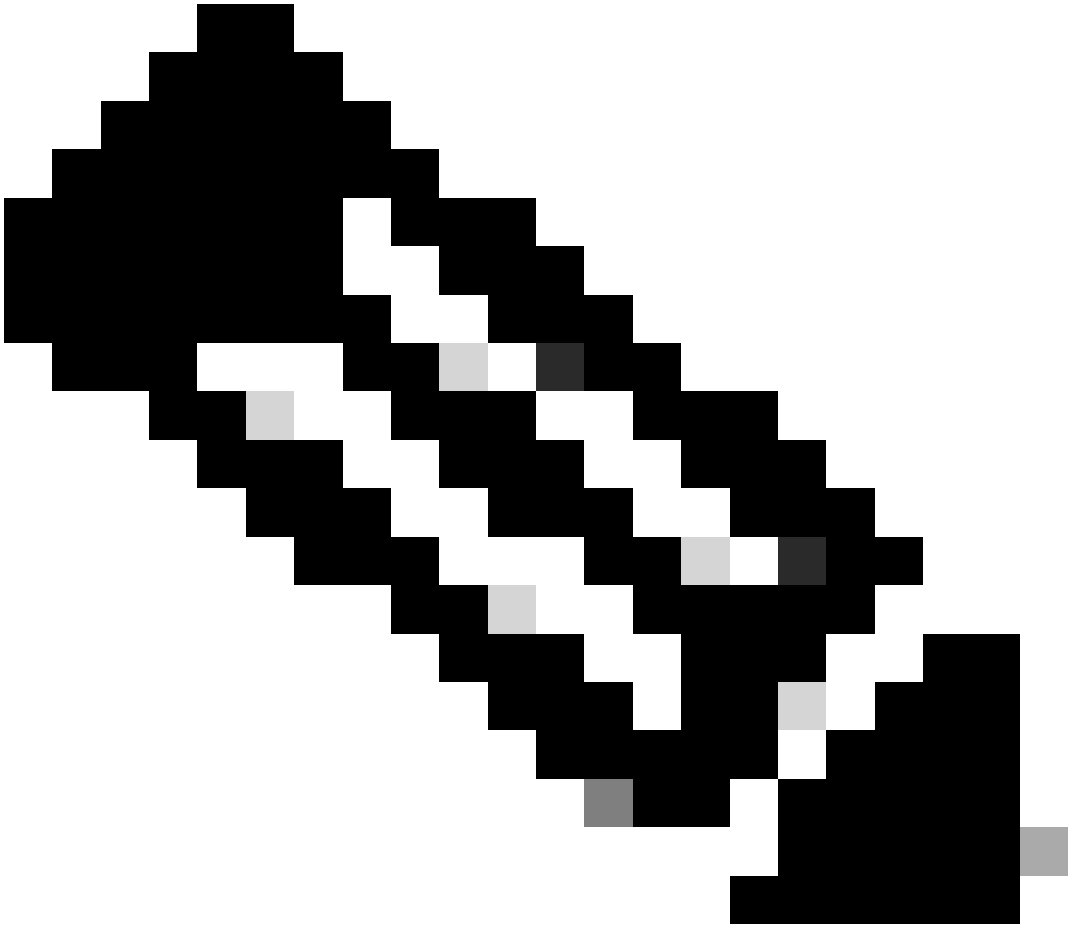
Dans le scénario de TP discuté, l'ID de tunnel a été défini comme cat8k-dmz.
Dans un scénario normal, nous configurerions le routeur pour envoyer l'identité IKE locale comme cat8k-dmz@8195165-622405748-sse.cisco.com

Cependant, afin d'établir plusieurs tunnels avec le même groupe de tunnels réseau, des ID IKE

locaux vont être utilisés :

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

Notez le suffixe ajouté à chaque chaîne (tunnel1 et tunnel2)



> Remarque : les identités IKE locales mentionnées ne sont utilisées qu'à titre d'exemple dans ce scénario de travaux pratiques. Vous pouvez définir n'importe quel suffixe que vous souhaitez, assurez-vous juste de répondre aux exigences.

```
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
```

Configurez le jeu de transformation IPSec. Ce paramètre définit les algorithmes utilisés pour l'association de sécurité IPsec (phase 2) :

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

Configurez les profils IPSec qui lient les profils IKEv2 aux ensembles de transformation :

```
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
```

Interfaces de tunnel virtuel

Cette section traite de la configuration des interfaces de tunnel virtuel et des interfaces de bouclage utilisées comme source de tunnel.

Dans le scénario de travaux pratiques présenté, nous devons établir deux interfaces VTI avec un homologue unique utilisant la même adresse IP publique. En outre, notre périphérique Cisco IOS XE ne dispose que d'une interface de sortie GigabitEthernet1.

Cisco IOS XE ne prend pas en charge la configuration de plusieurs VTI avec la même source et la même destination de tunnel.

Afin de surmonter cette limitation, vous pouvez utiliser des interfaces de bouclage et les définir comme source de tunnel dans les VTI respectifs.

Il existe peu d'options pour obtenir une connectivité IP entre le bouclage et l'adresse IP publique SSE :

1. Attribuer une adresse IP routable publiquement à l’interface de bouclage (nécessite la

propriété de l’espace d’adressage IP public)
2. Attribuez une adresse IP privée à l’interface de bouclage et au trafic NAT dynamique via la source IP de bouclage.
3. Utiliser des interfaces VASI (non prises en charge sur de nombreuses plates-formes, difficiles à configurer et à dépanner)

Dans ce scénario, nous allons discuter de la deuxième option.

Configurez deux interfaces de bouclage et ajoutez la commande « ip nat inside » sous chacune d’elles.

```
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
```

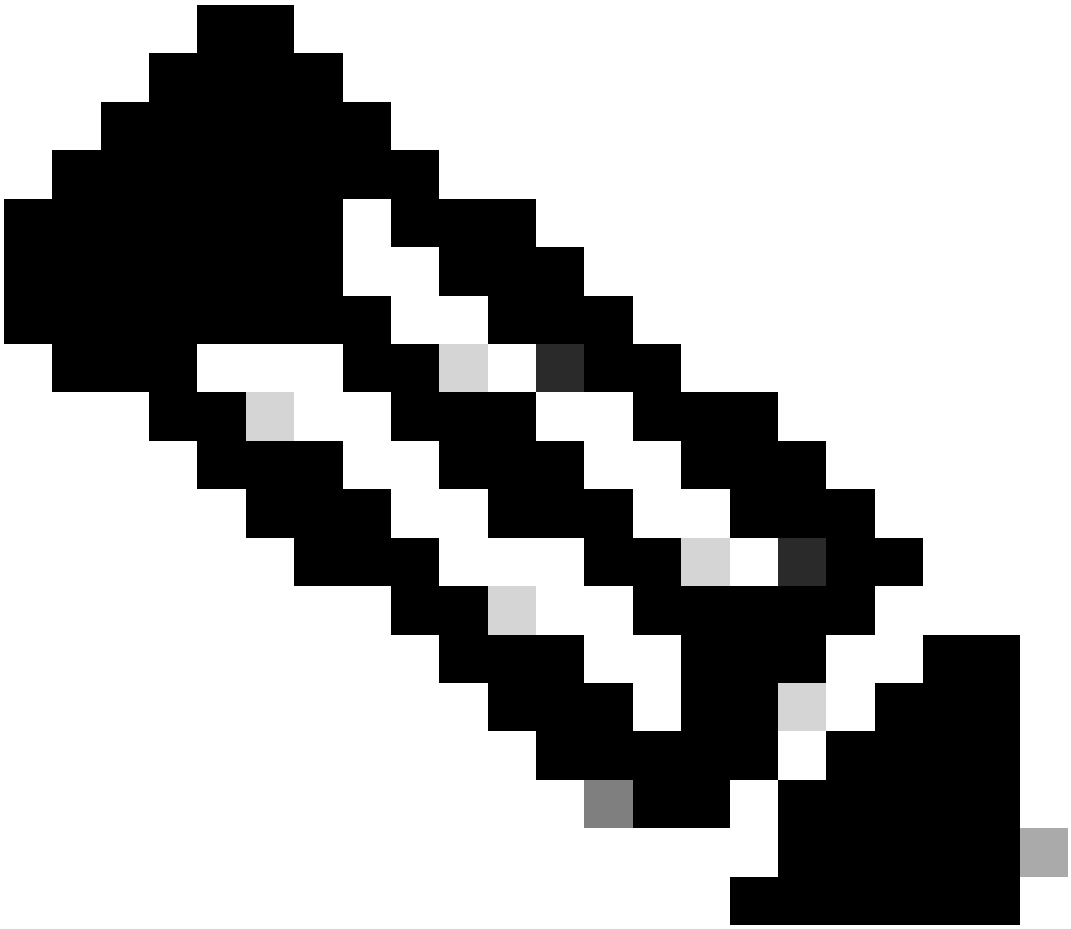
Définissez la liste de contrôle d'accès NAT dynamique et l'instruction de surcharge NAT :

```
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
```

Configurer les interfaces de tunnel virtuel

```
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
```



> Remarque : dans le scénario de travaux pratiques décrit, les adresses IP attribuées aux interfaces virtuelles proviennent de sous-réseaux sans chevauchement de 169.254.0.0/24.
> Vous pouvez utiliser d'autres espaces de sous-réseau, mais certaines exigences liées au protocole BGP nécessitent un tel espace d'adressage.

Routage BGP

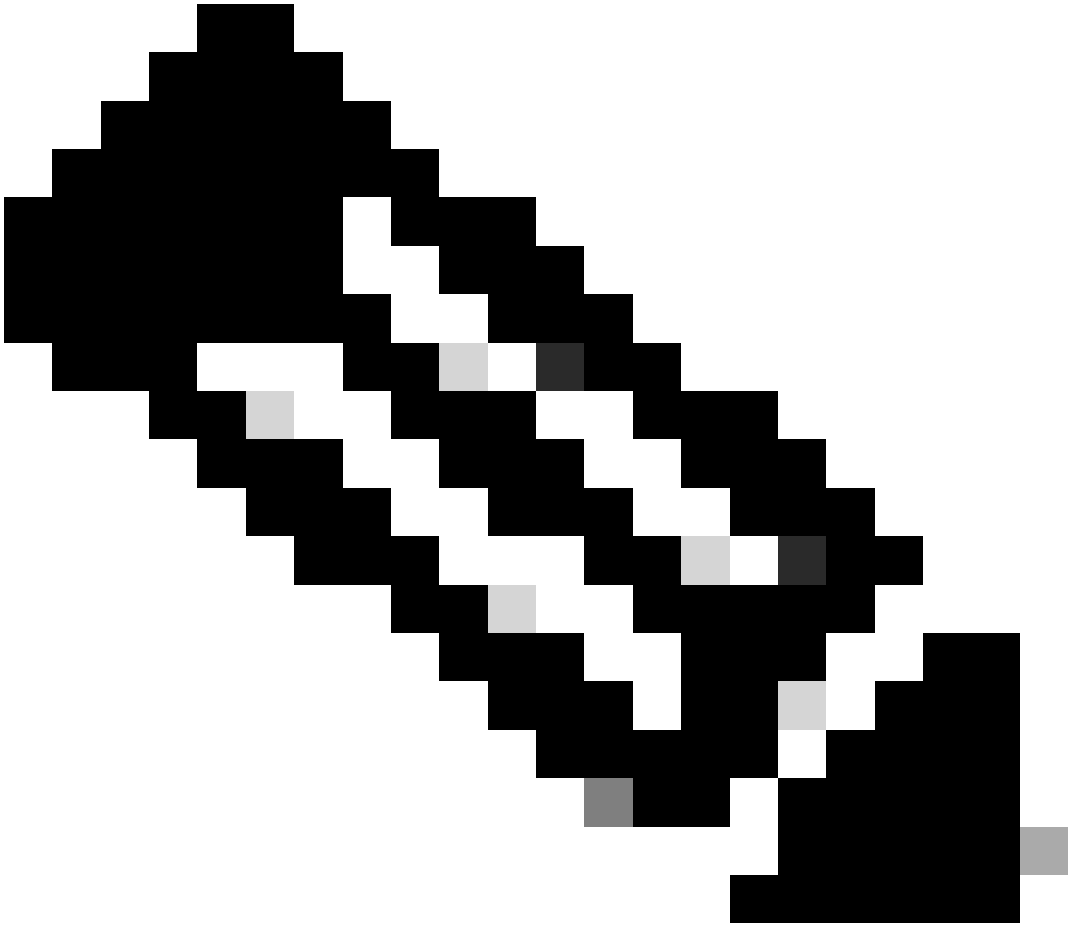
Cette section couvre la partie configuration requise pour établir un voisinage BGP avec la tête de réseau SSE.
Le processus BGP sur la tête de réseau SSE écoute toutes les adresses IP du sous-réseau 169.254.0.0/24 .

Afin d'établir l'appairage BGP sur les deux VTI, nous allons définir deux voisins 169.254.0.9 (Tunnel1) et 169.254.0.13 (Tunnel2).
Vous devez également spécifier le système autonome distant en fonction de la valeur affichée dans le tableau de bord 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

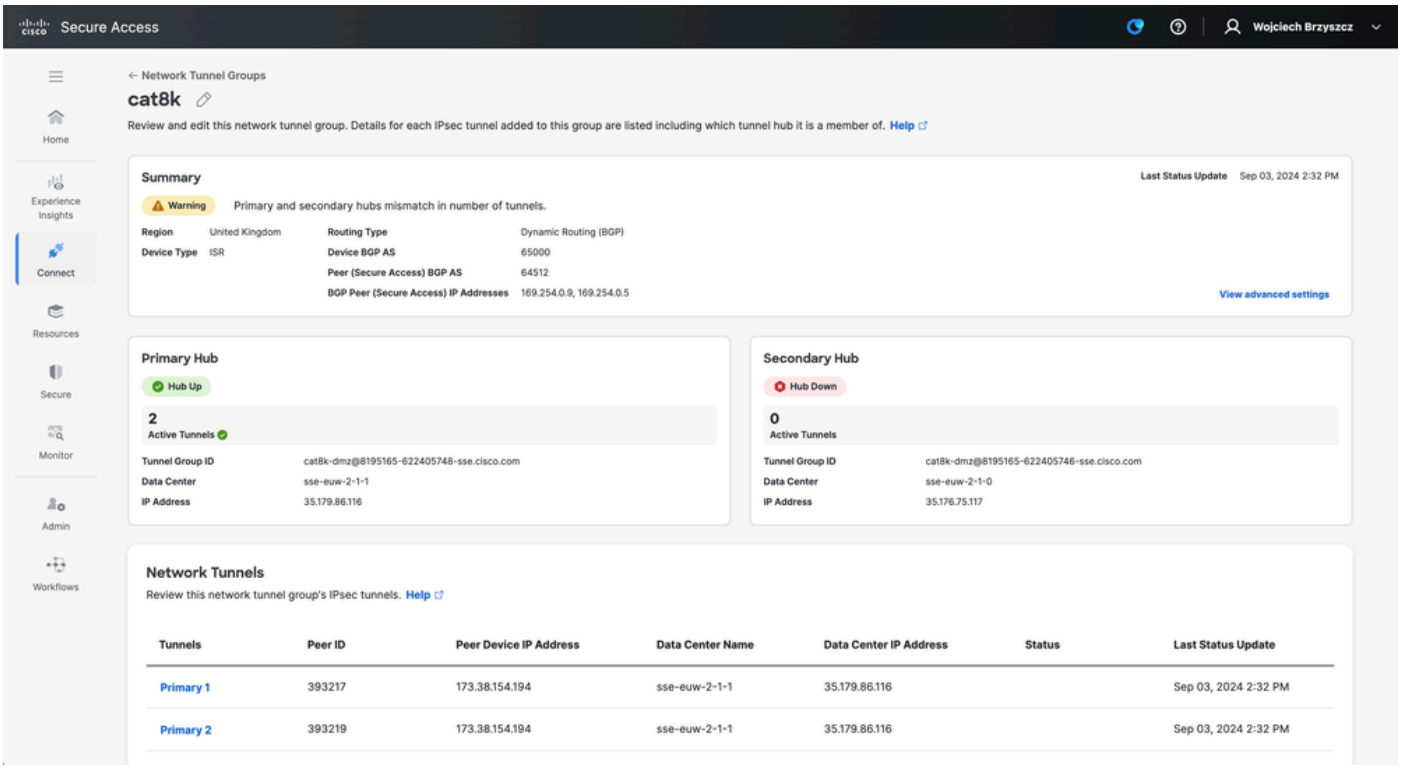


Remarque : les routes reçues des deux homologues doivent être exactement identiques. Par défaut, le routeur n'installe qu'un seul d'entre eux dans la table de routage.
Afin de permettre l'installation de plus d'une route dupliquée dans la table de routage (et activer ECMP), vous devez configurer "maximum-paths <nombre de routes>"

Vérifier

Tableau de bord Secure Access

Vous devez voir deux tunnels principaux dans le tableau de bord SSE :



Routeur Cisco IOS XE

Vérifiez que les deux tunnels sont à l'état READY du côté de 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
```

Vérifiez que le voisinage BGP est UP avec les deux homologues :

<#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
```

Vérifiez que le routeur apprend les routes appropriées à partir de BGP (et qu'il y a au moins deux sauts suivants installés dans la table de routage).

<#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
```

Lancez le trafic et vérifiez que les deux tunnels sont utilisés et que les compteurs d'encapsulation et de désencapsulation augmentent pour les deux.

<#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
```

Vous pouvez éventuellement collecter la capture de paquets sur les deux interfaces VTI pour vous assurer que la charge du trafic est équilibrée entre les interfaces VTI. Lisez les instructions de cet article pour configurer la capture de paquets intégrée sur le périphérique Cisco IOS XE.
Dans l'exemple, l'hôte derrière le routeur Cisco IOS XE avec l'adresse IP source 192.168.150.1 envoyait des requêtes ICMP à plusieurs adresses IP à partir du sous-réseau 192.168.200.0/24.

Comme vous le voyez, les requêtes ICMP sont équilibrées en charge entre les tunnels.

<#root>

```
wbrzyszc-cat8k#
```

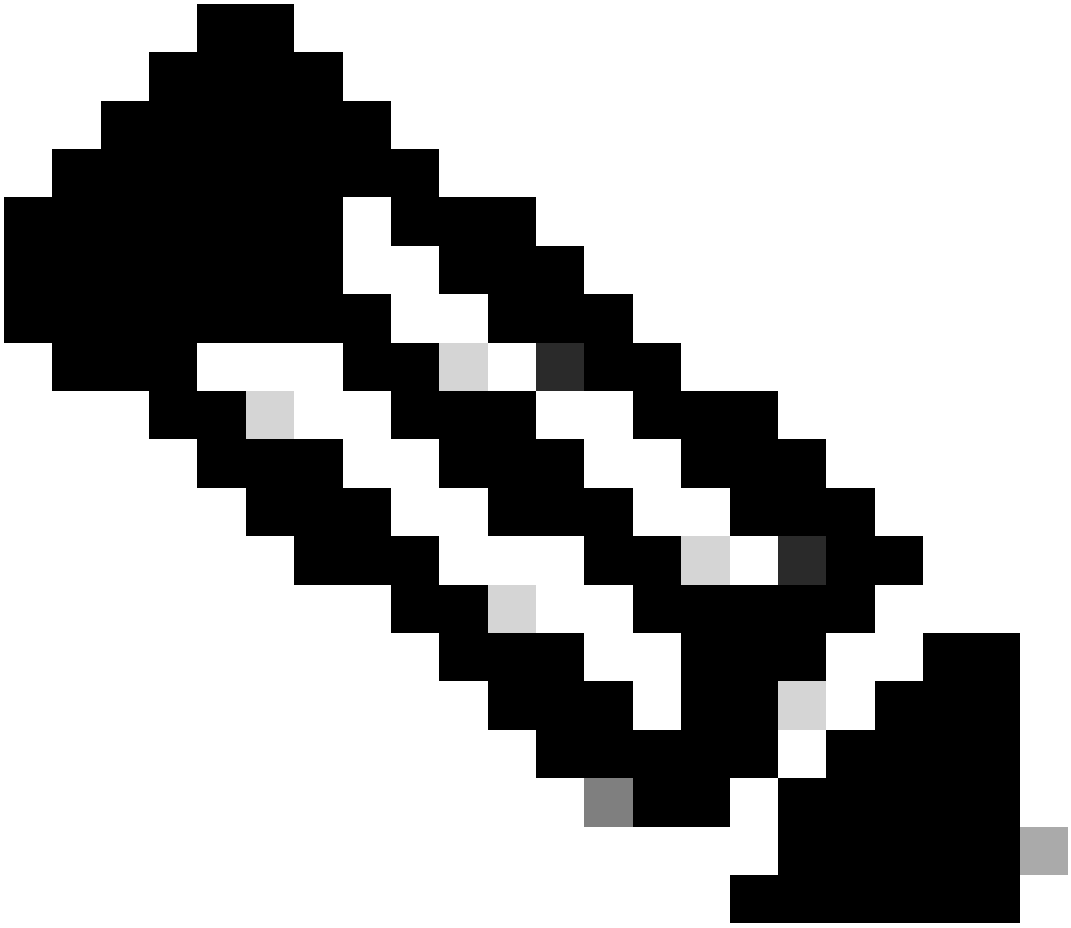
show monitor capture Tunnel1 buffer brief

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



Remarque : il existe plusieurs mécanismes d'équilibrage de charge ECMP sur les routeurs Cisco IOS XE. Par défaut, l'équilibrage de charge par destination est activé, ce qui garantit que le trafic vers la même adresse IP de destination emprunte toujours le même chemin.
Vous pouvez configurer l'équilibrage de charge par paquet, qui équilibrerait de manière aléatoire la charge du trafic même pour la même adresse IP de destination.

Informations connexes

- Guide de l'utilisateur Secure Access
- Comment collecter la capture de paquets intégrée
- Assistance et documentation techniques - Cisco Systems

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.