تكوين نفق الشبكة بين موجه IOS XE والوصول الآمن من Cisco باستخدام ECMP مع BGP

المحتويات

- المقدمة
- الرسم التخطيطي للشبكة
- المتطلبات الأساسية
  - المتطلبات
  - المكونات المستخدمة
- معلومات أساسية
- التكوين
  - تكوين الوصول الآمن
  - تكوين Cisco من IOS XE
    - معلمات IKEv2 و IPsec
    - واجهات الأنفاق الظاهرية
    - توجيه BGP
- التحقق من الصحة
  - معلومات الوصول الآمن حول
  - الموجه Cisco IOS XE Router
- معلومات ذات صلة

المقدمة

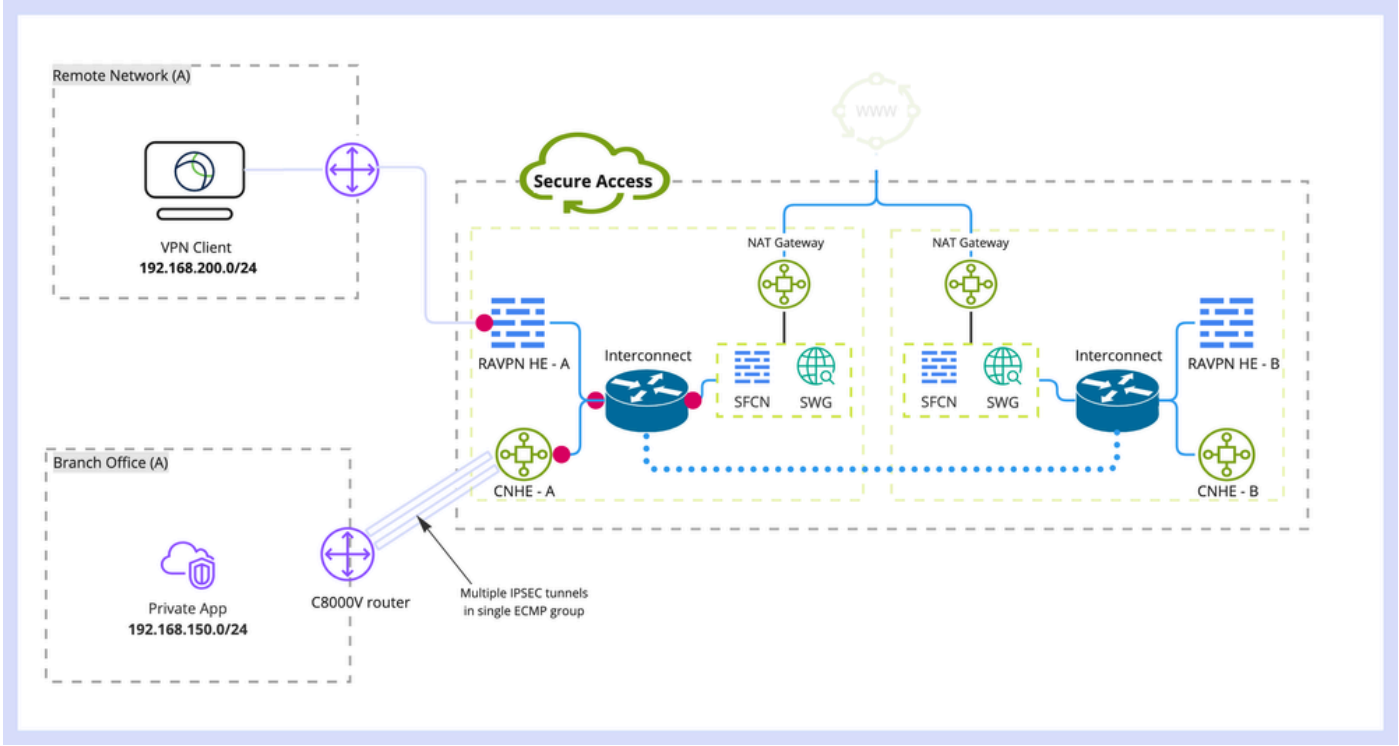
يصف هذا المستند الخطوات المطلوبة لتكوين نفق VPN IPSec واستكشاف أخطائه وإصلاحها بين Cisco Secure Access و Cisco IOS XE باستخدام BGP و ECMP.

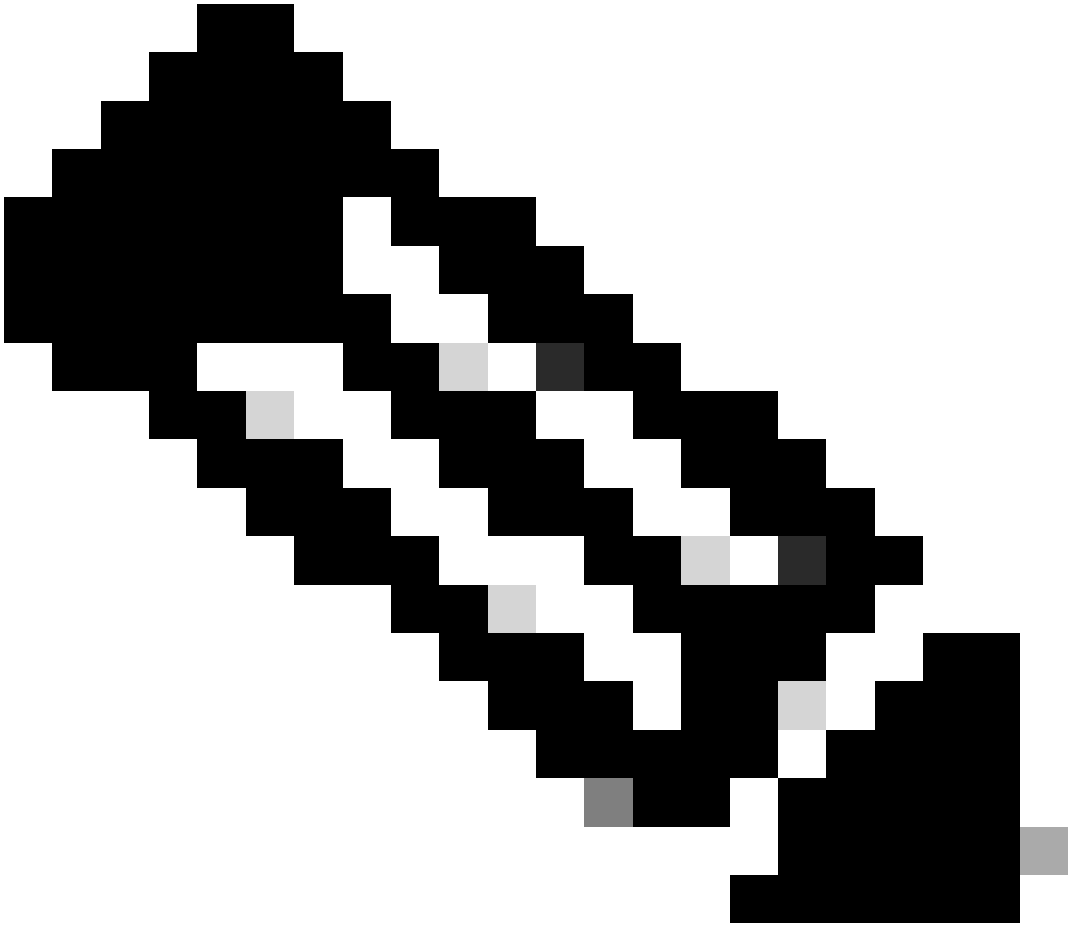
الرسم التخطيطي للشبكة

في مثال المختبر هذا، سنناقش سيناريو حيث تكون الشبكة 192.168.150.0/24 عبارة عن شبكة LAN خلف جهاز Cisco IOS XE، و192.168.200.0/24 هي تجمع IP المستخدم من قبل مقطع شبكة RAPN المتصلين بمنفذ آمن. مستخدمي

يتمثل هدفنا النهائي في إستخدام ECMP على أنفاق الشبكة الخاصة الظاهرية (VPN) بين جهاز Cisco IOS XE ومحطة الاستقبال والبث الخاصة بالوصول الآمن.

من أجل فهم المخطط بشكل أفضل، يرجى الرجوع إلى المخطط:


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



ملاحظة: هذا مجرد مثال على تدفق الحزم، يمكنك تطبيق نفس المبادئ على أي تدفقات أخرى، وعلى الوصول الآمن إلى الإنترنت من الشبكة الفرعية 192.168.150.0/24 خلف موجه Cisco IOS XE.

المتطلبات الأساسية

المتطلبات

يوصى بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين واجهة سطر الأوامر (CLI) IOS XE من Cisco وإدارتها
- معرفة أساسية ببروتوكولات IKEv2 و IPSec
- تكوين Cisco IOS XE الأولي (عنونة IP، SSH، الترخيص)
- معرفة أساسية ب BGP و ECMP

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- C8000V تشغيل إصدار برنامج 17.9.4a
- كمبيوتر Windows
- مؤسسة الوصول الآمن من Cisco

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتسم أنفاق الشبكة في الوصول الآمن بنطاق ترددي عريض يصل إلى 1 جيجابت في الثانية لكل نفق واحد. إذا كان عرض نطاق الإنترنت أعلى من الخادم/الخادم بمعدل 1 جيجابت في الثانية، وتريد إستخدامه بالكامل، فستحتاج إلى التغلب على هذا الحد من خلال تكوين أنفاق متعددة بنفس مركز بيانات الوصول الآمن وتجميعها في مجموعة ECMP واحدة.

عند إنهاء عدة أنفاق باستخدام مجموعة نفق الشبكة الأحادية (ضمن تيار مستمر وصول آمن واحد)، فإنها بشكل افتراضي مجموعة ECMP من منظور وحدة الاستقبال والبث الخاصة بالوصول الآمن.
وهو ما يعني أنه بمجرد إرسال وحدة الاستقبال والبث الخاصة بالوصول الآمن لحركة مرور البيانات نحو جهاز VPN المحلي، فإنه يقوم بموازنة التحميل بين الأنفاق (بافتراض تلقي المسارات الصحيحة من أقران BGP).

لتحقيق نفس الوظيفة على جهاز VPN المحلي، ستحتاج إلى تكوين واجهات VTI متعددة على موجه واحد، وتأكد من تطبيق تكوين التوجيه المناسب.

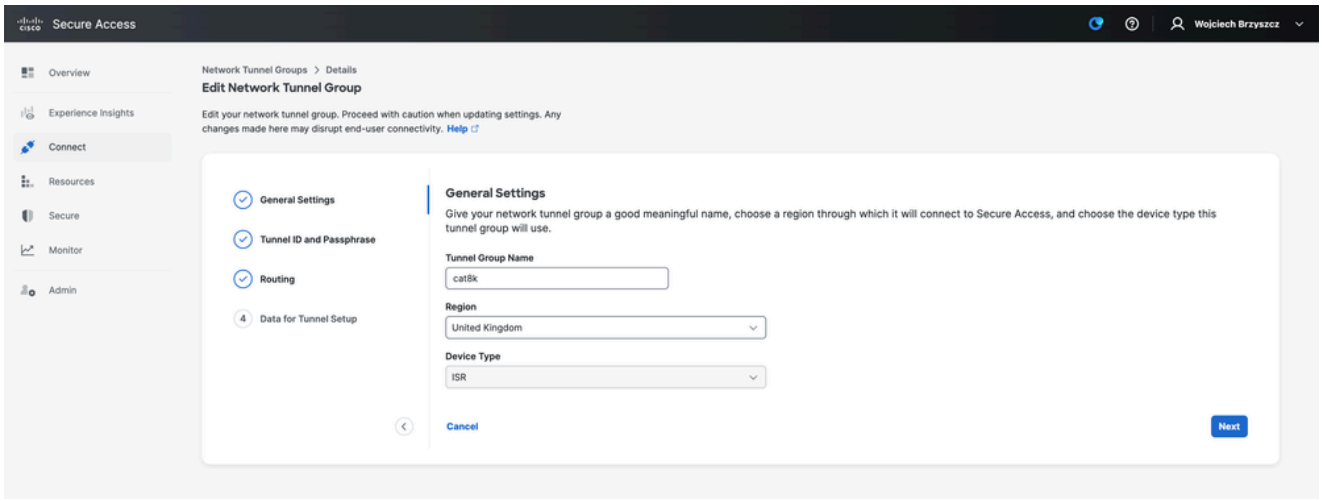
وتصف هذه المقالة السيناريو، مع شرح لكل خطوة مطلوبة.

التكوين

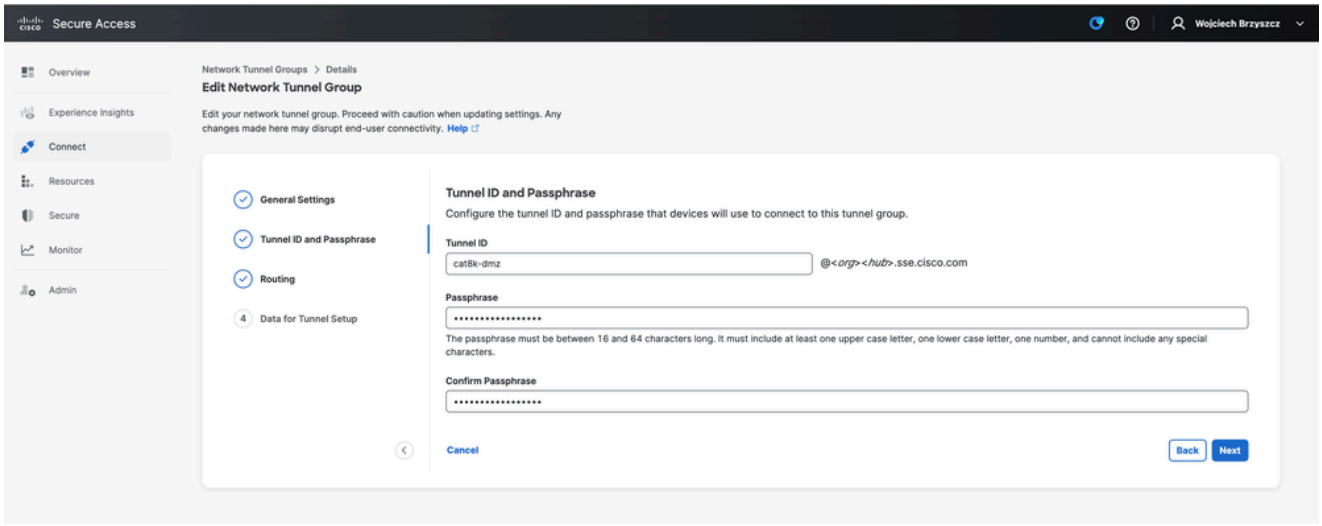
تكوين الوصول الآمن

لا يوجد تكوين خاص يلزم تطبيقه على جانب الوصول الآمن، لتكوين مجموعة ECMP من أنفاق شبكات VPN متعددة باستخدام بروتوكول BGP.
الخطوات المطلوبة لتكوين مجموعة نفق الشبكة.

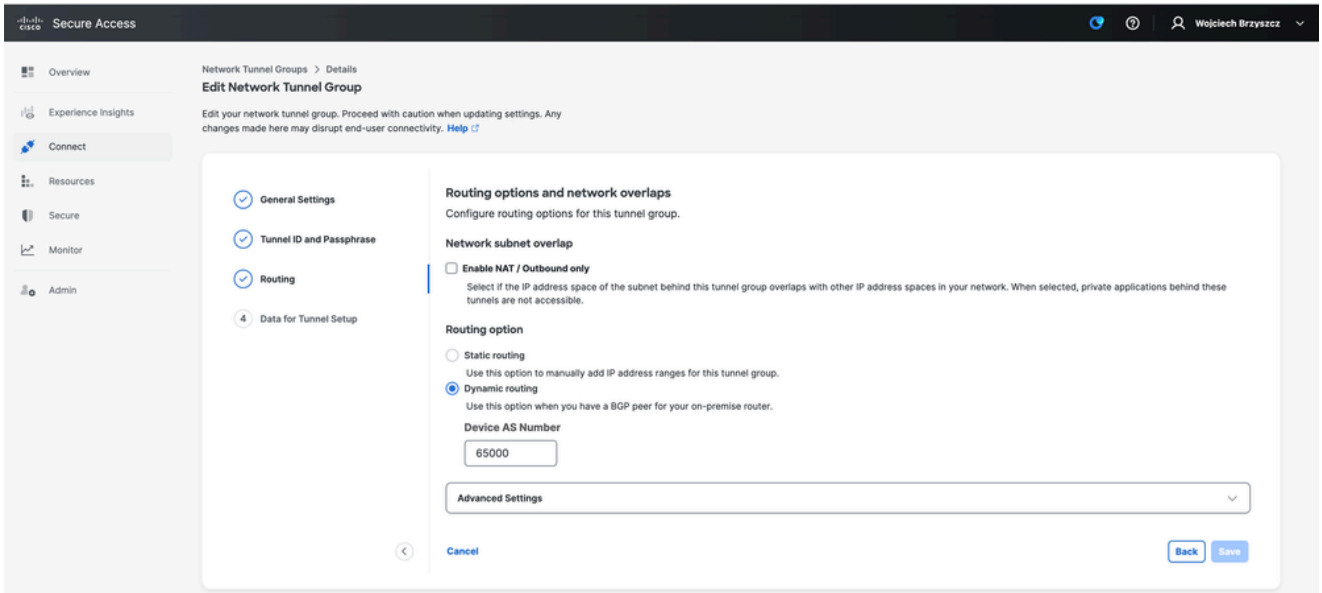
1. إنشاء مجموعة نفق شبكة جديدة (أو تحرير واحدة موجودة).



2. حدد معرف النفق عبارة المرور:



3. قم بتكوين خيارات التوجيه، وتحديد التوجيه الديناميكي، وأدخل رقم AS الداخلي الخاص بك. في سيناريو المختبر هذا، يساوي ASN 65000.



4. لاحظ تفاصيل النفق للأسفل من قسم بيانات إعداد النفق.

تكوين IOS XE من Cisco

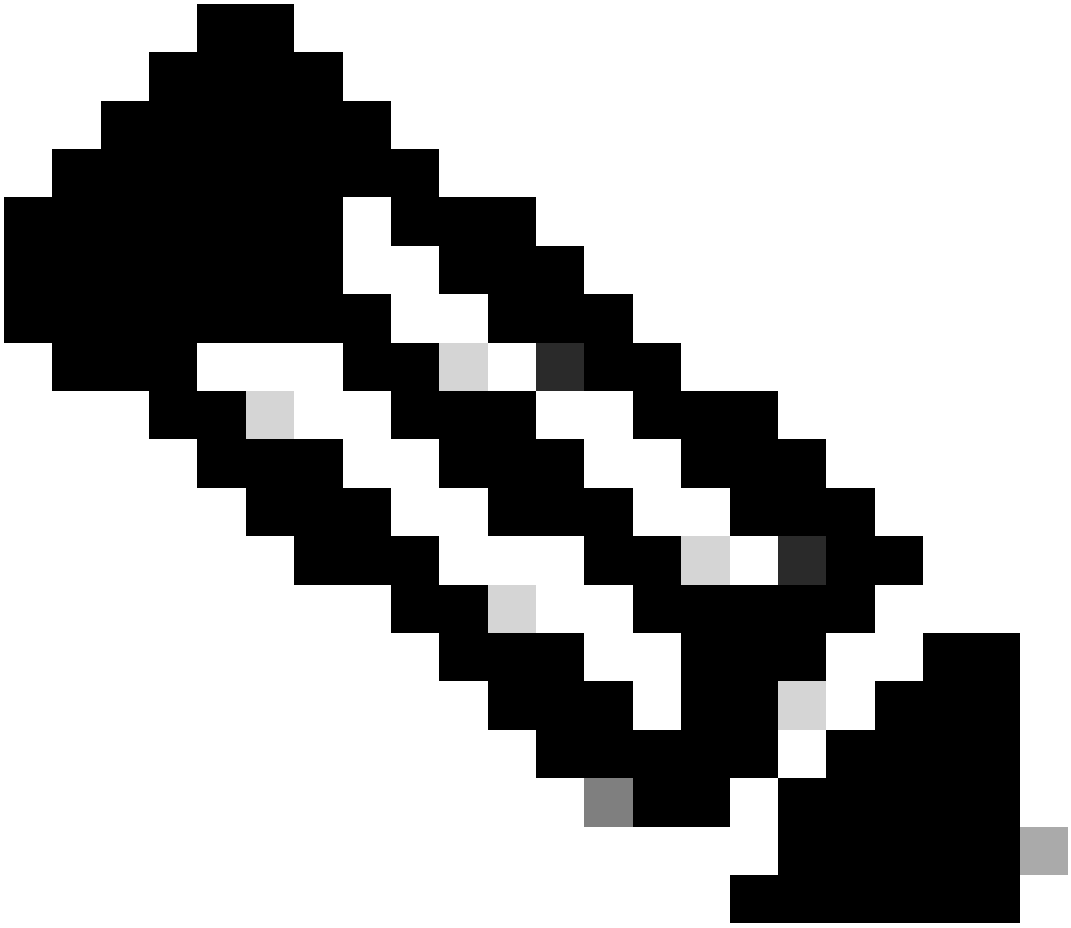
يغطي هذا القسم تكوين واجهة سطر الأوامر (CLI) الذي يلزم تطبيقه على موجه Cisco IOS XE، من أجل تكوين أنفاق IKEv2 بشكل صحيح، وجوار BGP وموازنة حمل ECMP عبر واجهات النفق الظاهرية.
يتم شرح كل قسم ويتم ذكر معظم التنبيهات الشائعة.

معلمات IKEv2 و IPsec

تكوين نهج IKEv2 واقتراح IKEv2. تحدد هذه المعلمات الخوارزميات المستخدمة للطرازIKE SA (المرحلة 1):

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

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



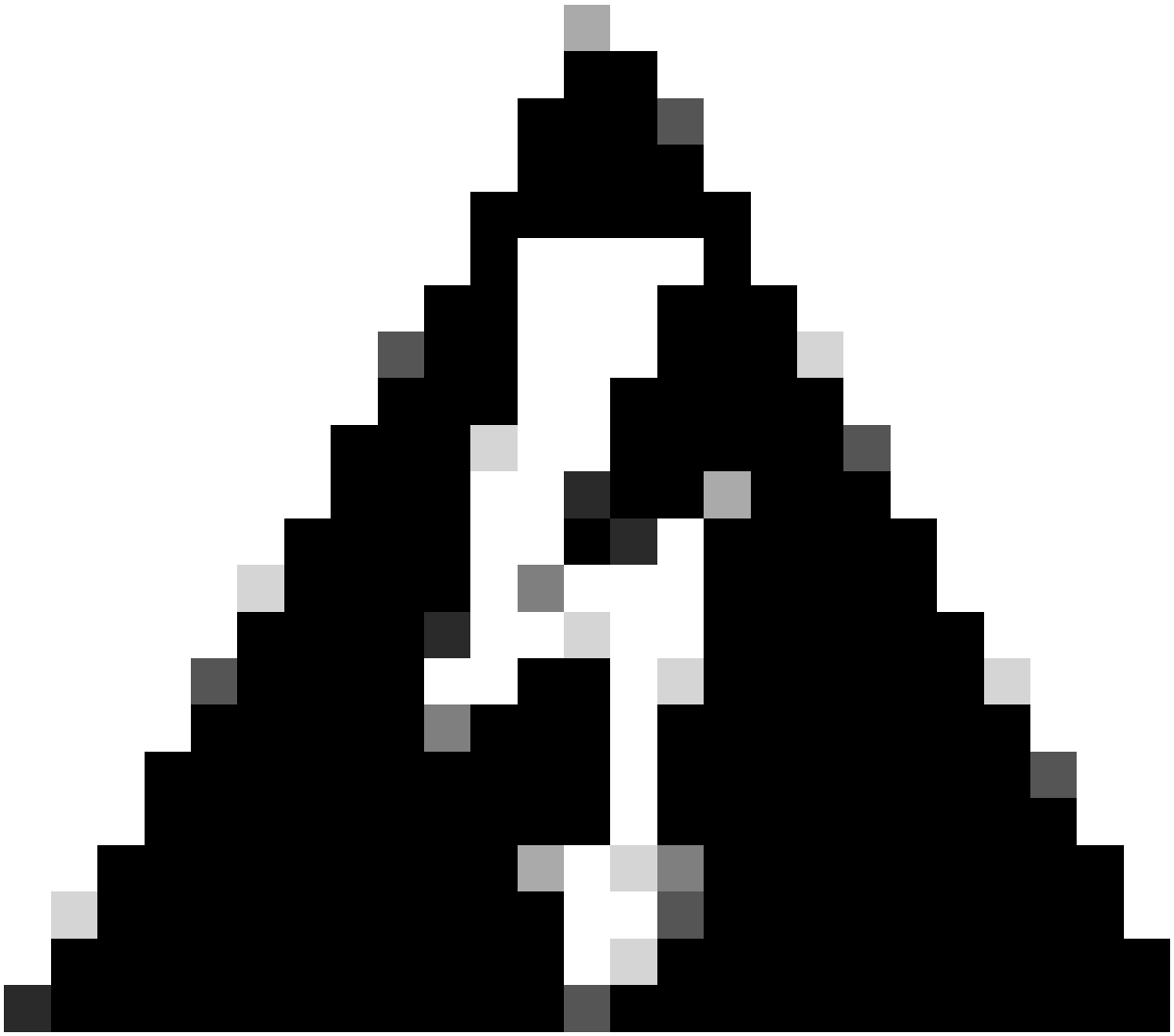
ملاحظة: تم وضع علامة باخط العريض على المعلمات المقترحة والمثالية في مستندات SSE: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

قم بتعريف حلقة المفاتيح IKEv2 التي تحدد عنوان IP لنقطة الاستقبال والبث والمفاتيح المشترك مسبقا المستخدم للمصادقة باستخدام وحدة الاستقبال والبث الخاصة ب 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>
```

تشكيل زوج من توصيفات IKEv2.

وهم يحددون نوع هوية IKE التي يتم إستخدامها لمطابقة النظير البعيد، وما يرسله الموجه المحلي لهوية IKE إلى النظير.
تنتمي هوية IKE الخاصة بوحدة الاستقبال والبث الخاصة ب SSE إلى نوع عنوان IP، وهي تساوي IP العام الخاص بوحدة الاستقبال والبث الخاصة ب SSE.



تحذير: لإنشاء أنفاق متعددة باستخدام مجموعة نفق الشبكة نفسها على جانب SSE، يجب أن تستخدم جميعها نفس هوية IKE المحلية.
لا يدعم Cisco IOS XE هذا السيناريو، نظرا لأنه يتطلب زوج فريد من هويات IKE المحلية والبعيدة لكل نفق.
للتغلب على هذه القيود، تم تحسين وحدة الاستقبال والبث الخاصة ب SSE لقبول معرف IKE بالتنسيق: <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

---

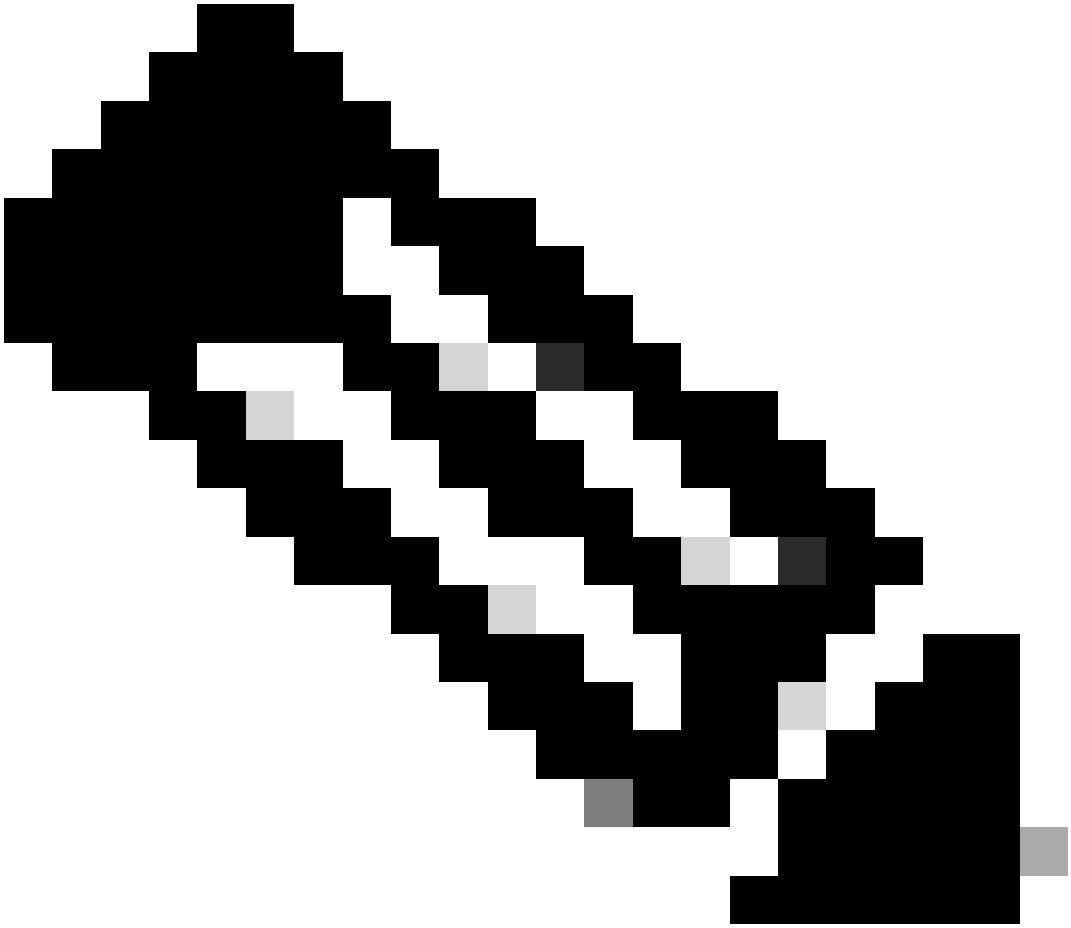
في سيناريو المختبر الذي تمت مناقشته، تم تعريف معرف النفق على أنه cat8k-dmz.
في السيناريو العادي، نقوم بتكوين الموجه لإرسال هوية IKE المحلية على هيئة cat8k-dmz@8195165-622405748-sse.cisco.com

ومع ذلك، لإنشاء أنفاق متعددة باستخدام مجموعة نفق الشبكة نفسها، سيتم إستخدام

معرفات IKE المحلية:

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

لاحظ اللاحقة التي تمت إضافتها إلى كل سلسلة (tunnel1 و tunnel2)



ملاحظة: إن هوية IKE المحلية المذكورة هي مجرد مثال مستخدم في سيناريو هذا المختبر. يمكنك تحديد أي لاحقة تريدها، فقط تأكد من استيفاء المتطلبات.

```
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
```

تكوين مجموعة تحويل IPSec. يحدد هذا الإعداد الخوارزميات المستخدمة لاقتران أمان IPsec (المرحلة 2):

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

تشكيل توصيفات IPSec التي ترتبط توصيفات IKEv2 بمجموعات تحويل:

```
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
```

واجهات الأنفاق الظاهرية

يغطي هذا القسم تكوين واجهات النفق الظاهرية، وواجهات الاسترجاع المستخدمة كمصدر للنفق.

في سيناريو المختبر الذي تمت مناقشته، نحتاج إلى إنشاء واجهة VTI مع النظير الواحد باستخدام نفس عنوان IP العام. أيضا، يحتوي جهاز Cisco IOS XE لديه واجهة مخرج واحدة فقط GigabitEthernet1.

Cisco IOS XE لا يسمح بتشكيل أكثر من واحد VTI مع نفس مصدر وغاية النفق.

in order to تخطي هذا التحدي، أنت يستطيع استعملت loopback قارن وتعريفهم كمصدر النفق في VTI شخصي.

هناك القليل من الخيارات لتحقيق اتصال IP بين الاسترجاع وعنوان IP العام لـ SSE:

1. قم بتخصيص عنوان IP القابل للتوجيه بشكل عام لواجهة الاسترجاع (يتطلب ملكية مساحة عنوان IP العامة)
2. قم بتخصيص عنوان IP الخاص لواجهة الاسترجاع وحركة مرور NAT بشكل ديناميكي

باستخدام مصدر IP للاسترجاع.

3. إستخدام واجهات VASI (غير مدعومة على الديد من الأنظمة الأساسية، كما أنها مرهقة للإعداد واستكشاف الأخطاء وإصلاحها)

في هذا السيناريو، سنناقش الخيار الثاني.

قم بتكوين واجهتي إسترجاع، وأضف الأمر "ip nat inside" تحت كل منهما.

```
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
```

تعريف قائمة التحكم في الوصول إلى NAT الديناميكي وبيان الحمل الزائد لـ NAT:

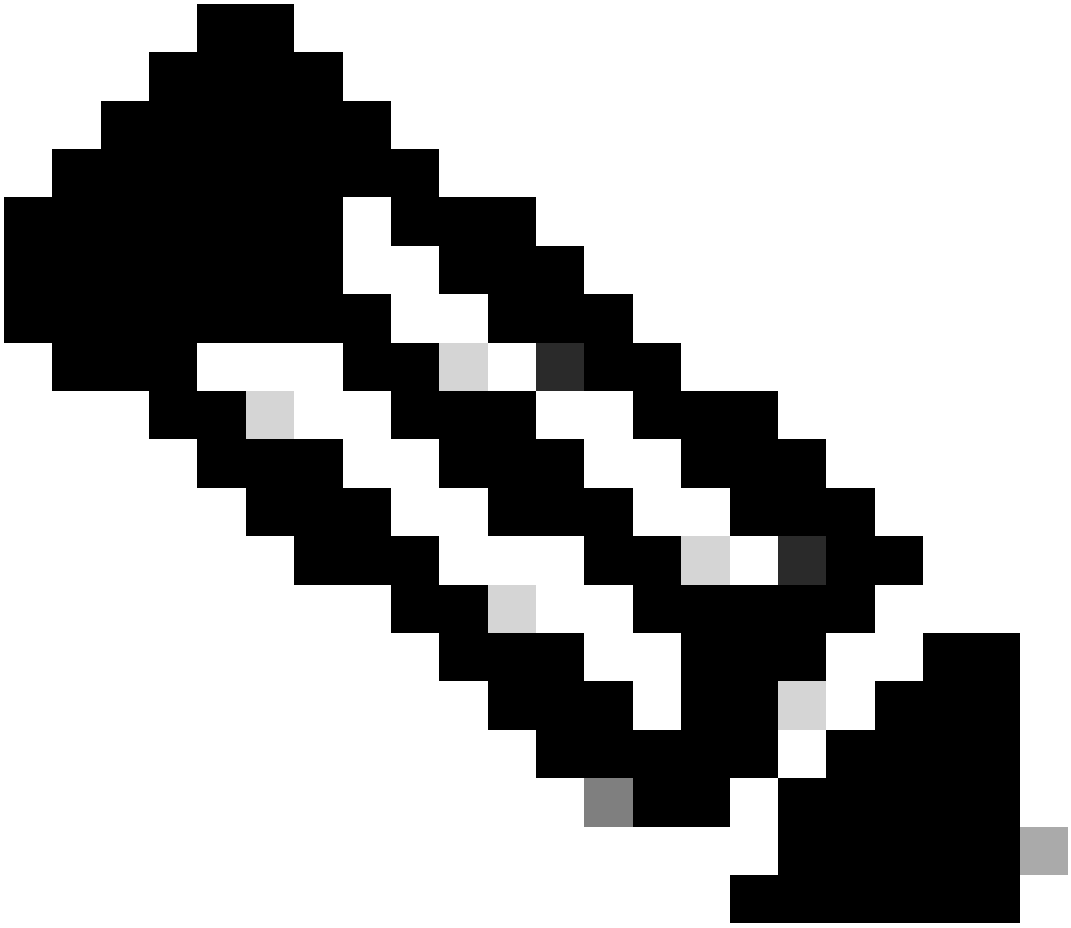
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

تكوين واجهات النفق الظاهرية.

```
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
```



ملاحظة: في سيناريو المعمل الموضح، تأتي عناوين IP التي تم تعيينها إلى VTIs من شبكات فرعية غير متداخلة بقيمة 169.254.0.0/24.
يمكنك إستخدام مساحة شبكة فرعية أخرى، ولكن هناك متطلبات معينة متعلقة ب BGP تتطلب مساحة العنوان تلك.

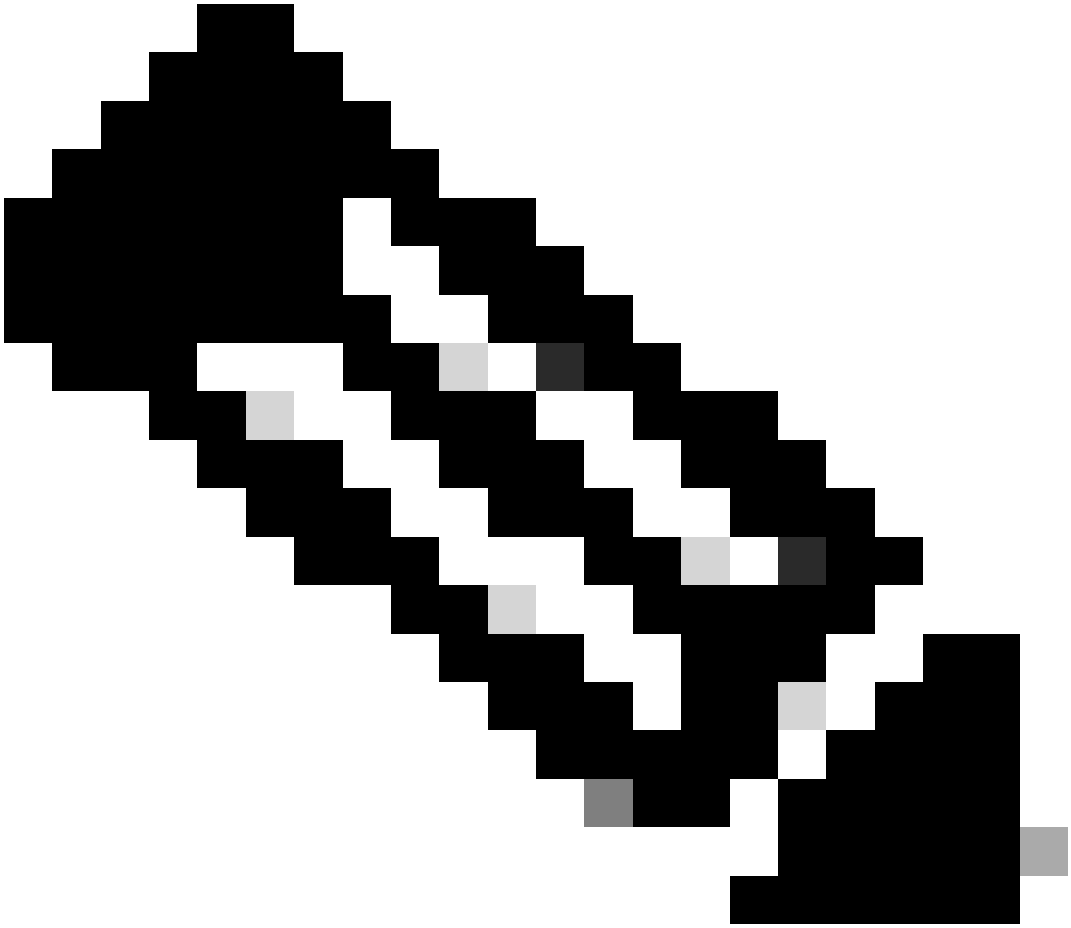
توجيه BGP

يغطي هذا القسم جزء التكوين المطلوب لإنشاء منطقة جوار BGP باستخدام وحدة الاستقبال والبث الخاصة ب SSE.
عمليات BGP على وحدة الاستقبال والبث ل SSE يتم الاستماع إليها على أي IP من الشبكة الفرعية 169.254.0.0/24 .
من أجل إنشاء نظرة عامة على بروتوكول BGP عبر كل من VTIs، سنقوم بتحديد جارتين، 169.254.0.9 (Tunnel1) و169.254.0.13 (Tunnel2).
تحتاج أيضا إلى تحديد AS البعيد وفقا للقيمة التي تم رؤيتها في لوحة معلومات 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

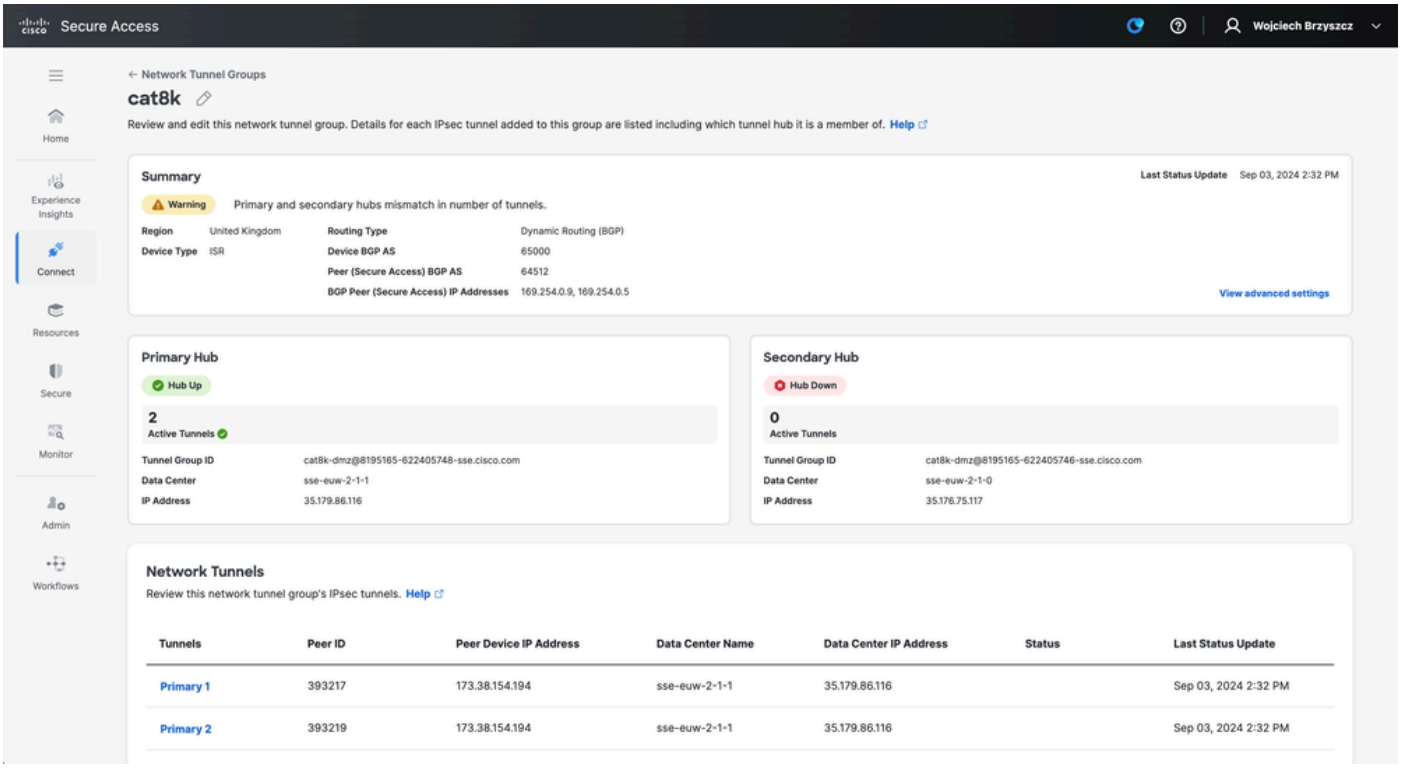


ملاحظة: يجب أن تكون المسارات التي يتم تلقيها من كل النظامين متماثلة تمامًا. يقوم الموجه بشكل افتراضي بتثبيت واحد منهم فقط في جدول التوجيه.
للسماح بتثبيت أكثر من مسار متكرر واحد في جدول التوجيه (وتمكين ECMP)، يجب تكوين الحد الأقصى للمسارات <عدد المسارات>"

التحقق من الصحة

لوحة معلومات الوصول الآمن

يجب أن ترى نفقين أساسيين في لوحة معلومات SSE:



الموجه Cisco IOS XE Router

تحقق من أن كلا النفقين في حالة الاستعداد من جانب 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
```

تحقق من أن منطقة جوار BGP تعمل مع كل النظيرين:

```
<#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
```

تحقق من أن الموجه يعلم المسارات الصحيحة من بروتوكول BGP (وهناك نقطتان تاليتين على الأقل مثبتة في جدول التوجيه).

```
<#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
```

ابدأ حركة المرور وتحقق من إستخدام كل النفقين وتشاهد عمليات التضمين وعدادات قطع الاتصال تتزايد لكليهما.

<#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
```

إختياري، يمكنك تجميع التقاط الحزمة على كل واجهات VTI للتأكد من موازنة حمل حركة المرور بين VTIs. اقرأ الإرشادات في هذه المقالة لتكوين التقاط الحزمة المضمنة على جهاز Cisco IOS XE.
في المثال، كان المضيف خلف موجه IOS XE من CiSCO مع المصدر IP 192.168.150.1 يرسل طلبات ICMP إلى عناوين IP متعددة من الشبكة الفرعية 192.168.200.0/24.

وكما ترى، يتم موازنة حمل طلبات ICMP بالتساوي بين الأنفاق.

<#root>

wbrzyszc-cat8k#

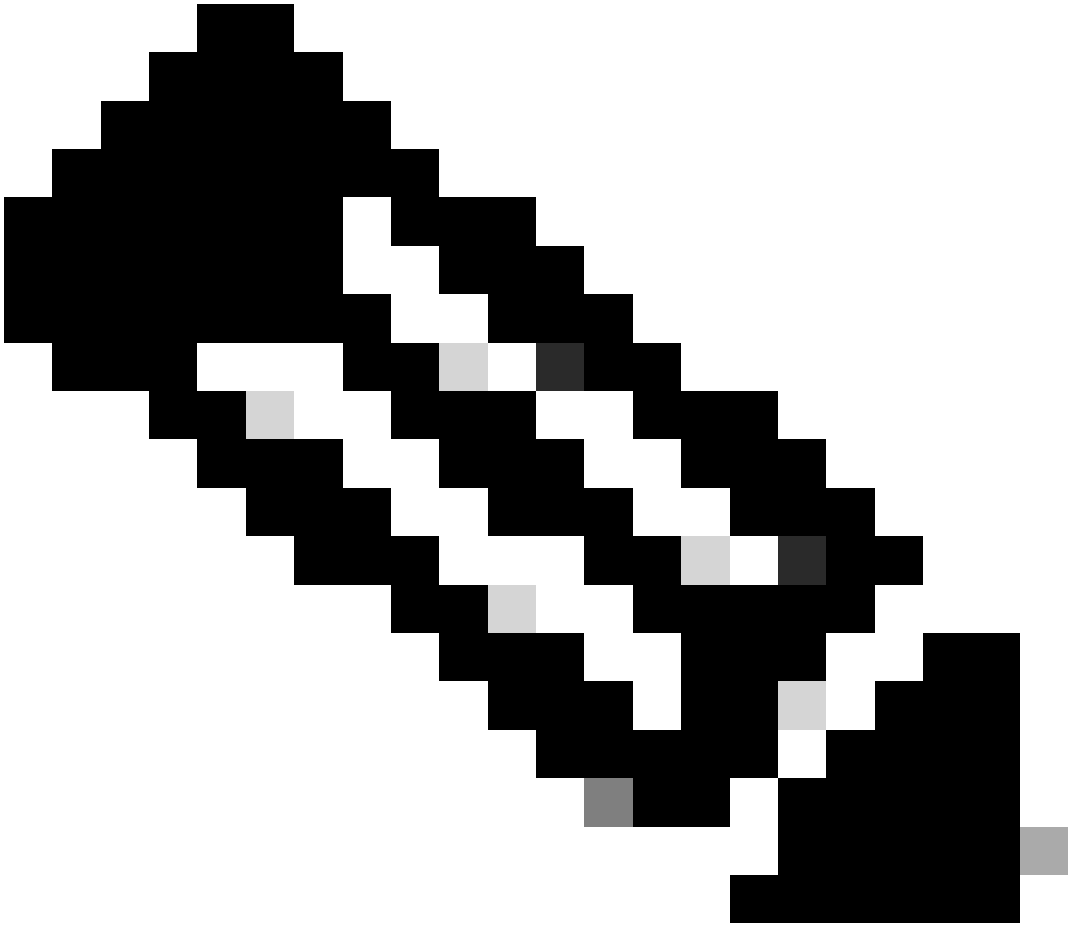
show monitor capture Tunnel1 buffer brief

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



ملاحظة: هناك آليات متعددة لموازنة حمل ECMP على موجهات Cisco IOS XE. افتراضيا، أي يضمن أن حركة المرور إلى IP نفسه غاية دائما تأخذ نفس المسار.
يمكنك تكوين موازنة الحمل لكل حزمة، والتي قد تقوم بتغيير حركة مرور موازنة التحميل عشوائيا حتى لـ IP الوجهة نفسها.

معلومات ذات صلة

- دليل مستخدم Secure Access
- كيفية تجميع التقاط الحزمة المضمنة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).