BGPでECMPを使用したCisco Secure AccessとIOS XEルータ間のネットワークトンネルの設定

内容

はじめに

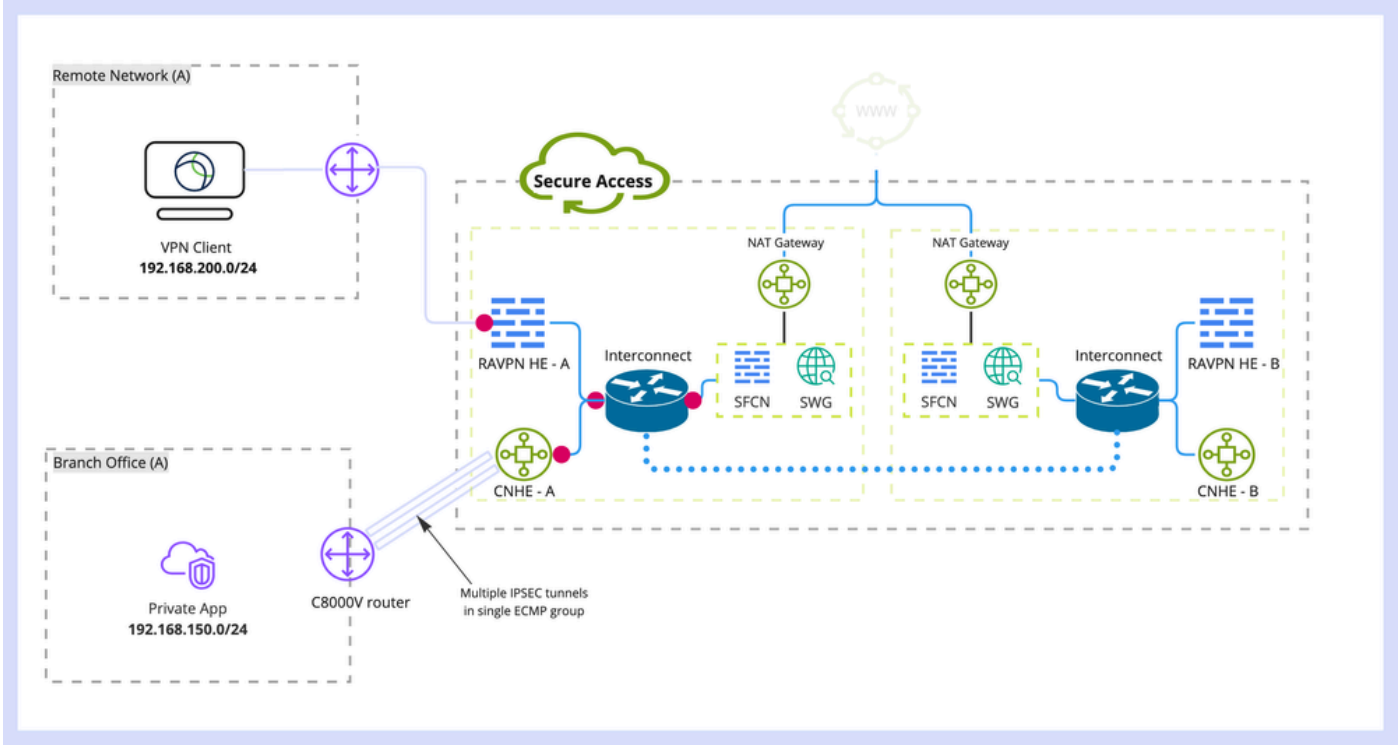
このドキュメントでは、BGPとECMPを使用してCisco Secure AccessとCisco IOS XEの間のIPSec VPNトンネルを設定およびトラブルシューティングするために必要な手順について説明します。

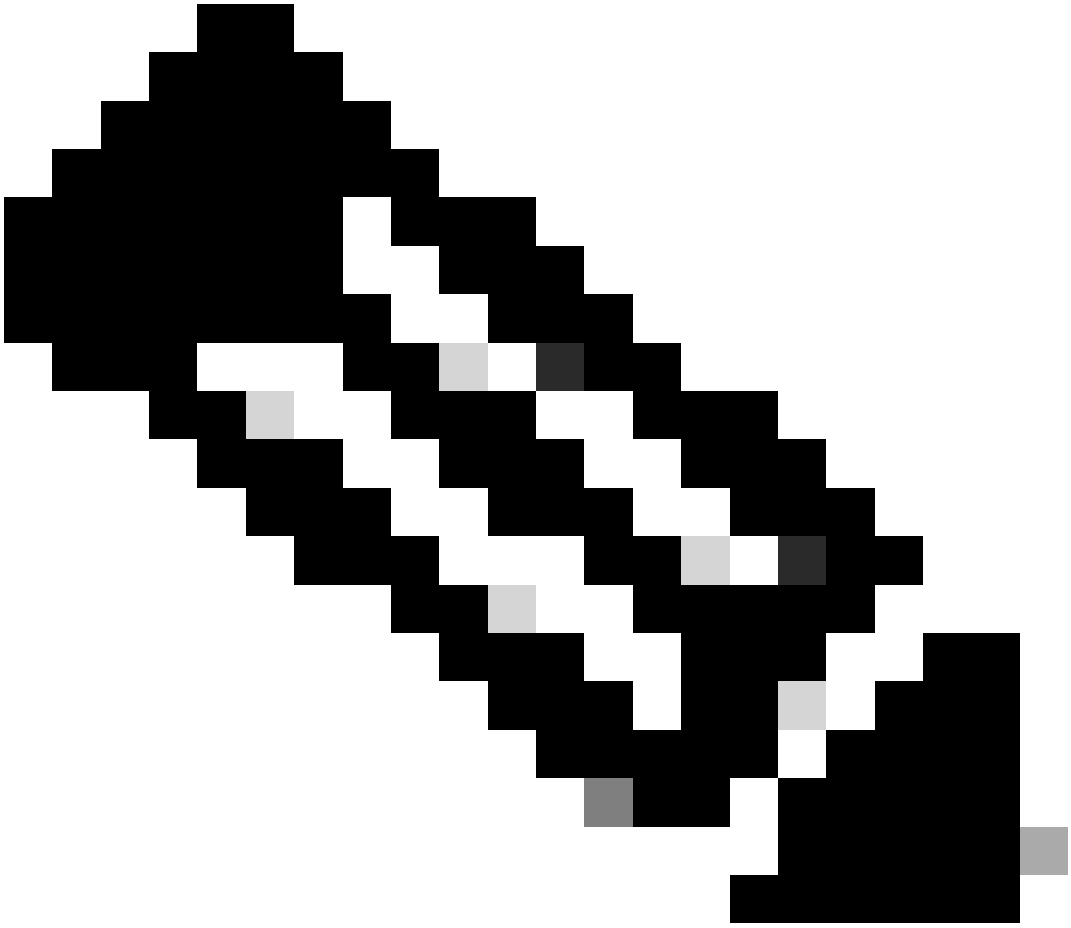
ネットワーク図

このラボ例では、ネットワーク192.168.150.0/24 がCisco IOS XEデバイスの背後にあるLANセグメントで、192.168.200.0/24 がセキュアアクセスヘッドエンドに接続するRAVPNユーザによって使用されるIPプールであるシナリオについて説明します。

最終的な目標は、Cisco IOS XEデバイスとセキュアアクセスヘッドエンド間のVPNトンネルでECMPを使用することです。

トポロジを詳しく理解するには、次の図を参照してください。


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



注：これは単なるパケットフローの例であり、他のフローや、Cisco IOS XEルータの背後にあるサブネット192.168.150.0/24からのセキュアインターネットアクセスにも同じ原則を適用できます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS XE CLIの設定と管理
- IKEv2およびIPSecプロトコルの基礎知識
- Cisco IOS XEの初期設定（IPアドレッシング、SSH、ライセンス）
- BGPとECMPに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 17.9.4aソフトウェアバージョンを実行するC8000V
- Windows PC
- シスコセキュアアクセス組織

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

セキュアアクセスのネットワークトンネルには、1つのトンネルにつき1 Gbpsの帯域幅制限があります。アップストリーム/ダウンストリームのインターネット帯域幅が1 Gbpsよりも高く、これを完全に利用したい場合は、同じセキュアアクセスデータセンターで複数のトンネルを設定し、それらを単一のECMPグループにグループ化することで、この制限を克服する必要があります。

1つのSecure Access DC内の1つのネットワークトンネルグループで複数のトンネルを終端する場合、デフォルトでは、セキュアアクセスヘッドエンドの観点からECMPグループが形成されます。
つまり、セキュアアクセスヘッドエンドがオンプレミスのVPNデバイスに向けてトラフィックを送信すると、トンネル間でロードバランシングが行われます（BGPピアから正しいルートが受信されると仮定）。

オンプレミスVPNデバイスで同じ機能を実現するには、単一のルータで複数のVTIインターフェイスを設定し、適切なルーティング設定が適用されていることを確認する必要があります。

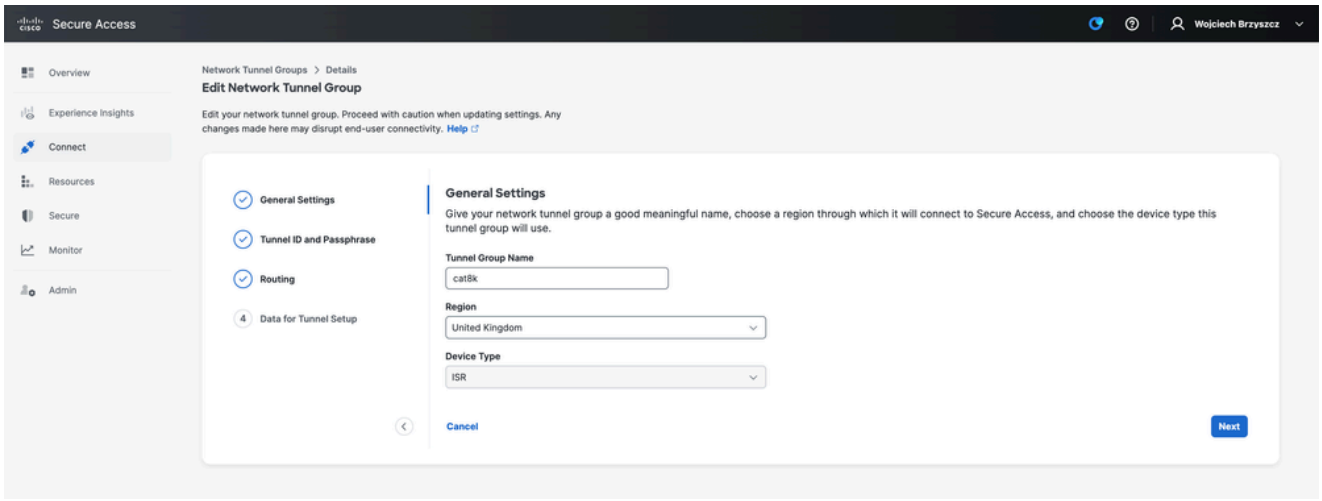
この記事では、シナリオと、必要な各手順について説明します。

設定

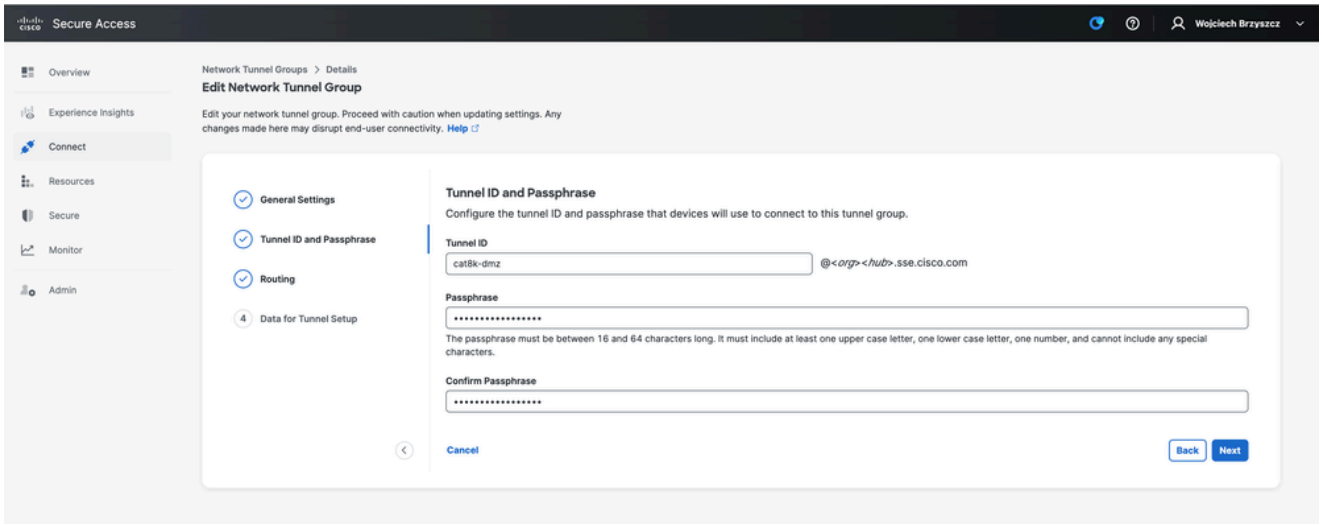
セキュアアクセスの設定

BGPプロトコルを使用して複数のVPNトンネルからECMPグループを形成するために、セキュアアクセス側に適用する必要がある特別な設定はありません。
ネットワークトンネルグループの設定に必要な手順。

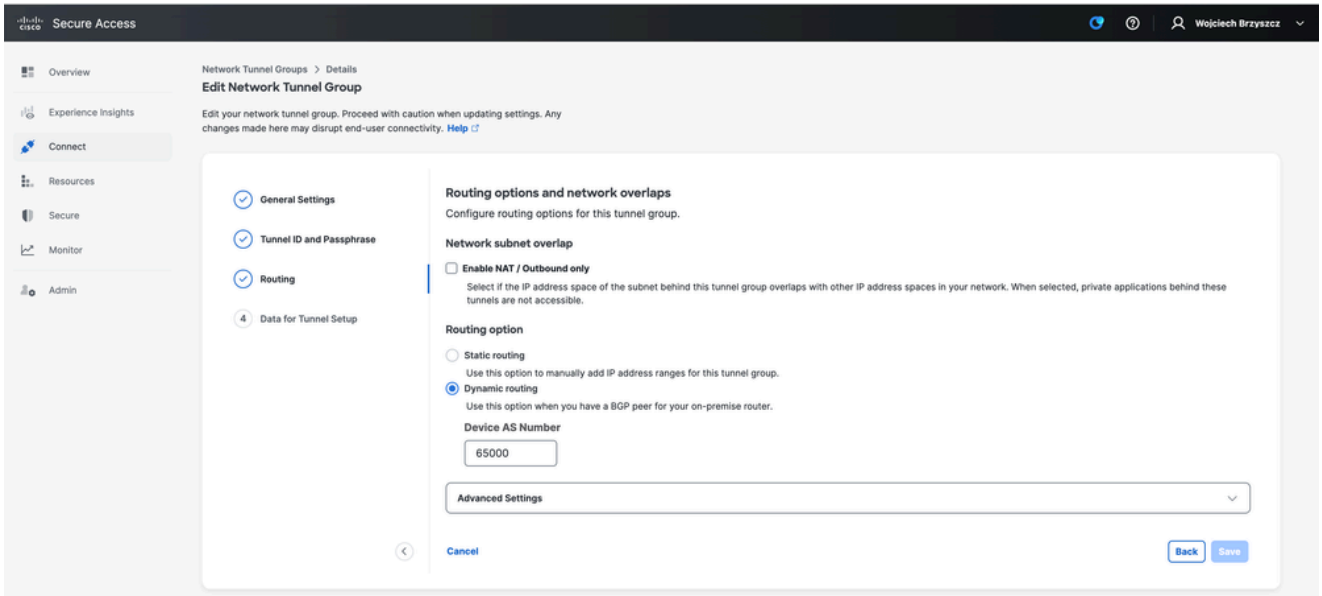
1. 新しいネットワークトンネルグループを作成します（または既存のグループを編集します）。



2. トンネルIDとパスフレーズを指定します。



3. Routingオプションを設定し、Dynamic Routingを指定して、内部AS番号を入力します。このラボシナリオでは、ASNは65000に等しくなります。



4. 「トンネル設定のデータ」セクションのトンネルの詳細を書き留めます。

Cisco IOS XEの設定

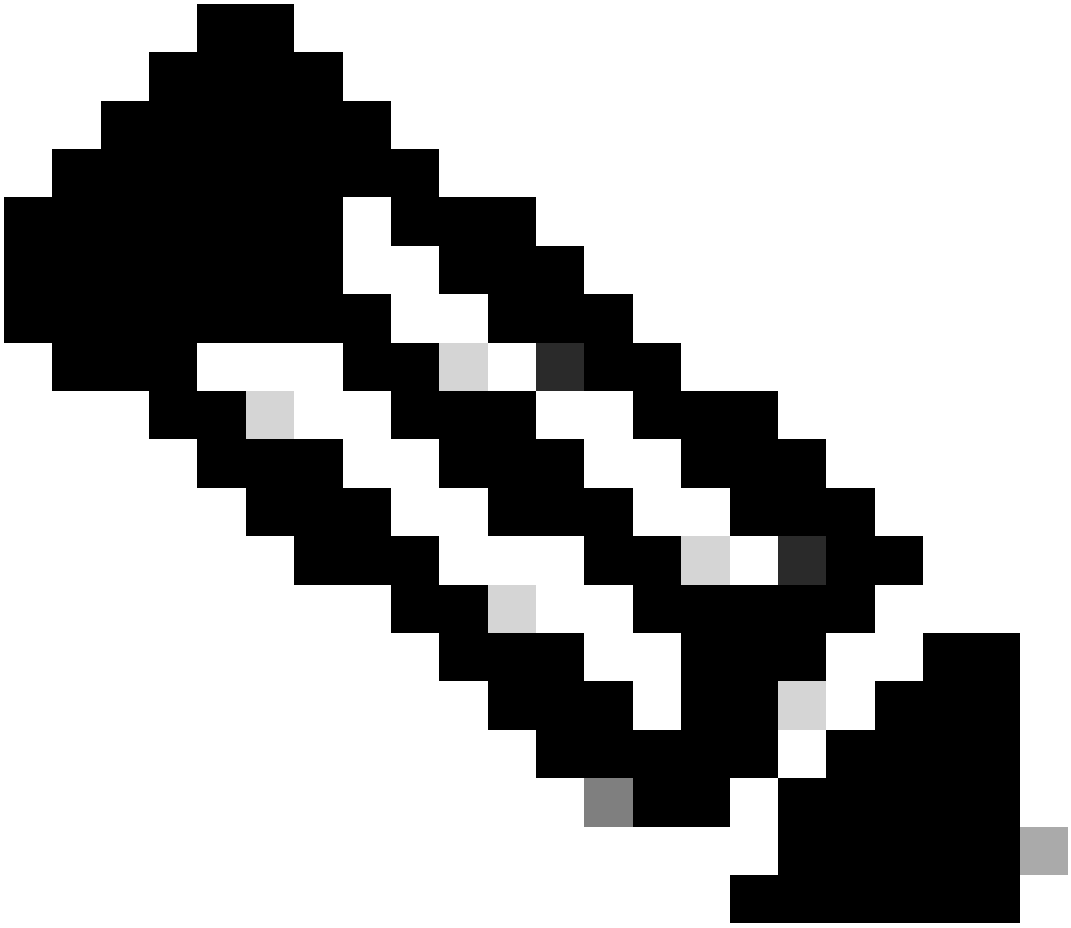
このセクションでは、仮想トンネルインターフェイス間でIKEv2トンネル、BGPネイバーシップ、およびECMPロードバランシングを適切に設定するためにCisco IOS XEルータに適用する必要があるCLI設定について説明します。
各セクションについて説明し、最も一般的な注意事項を記載します。

IKEv2およびIPsecパラメータ

IKEv2ポリシーとIKEv2プロポーザルを設定します。これらのパラメータは、IKE SA（フェーズ1）に使用されるアルゴリズムを定義します。

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

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



注：推奨されるパラメータと最適なパラメータは、SSEドキュメントで太字で示されています。https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

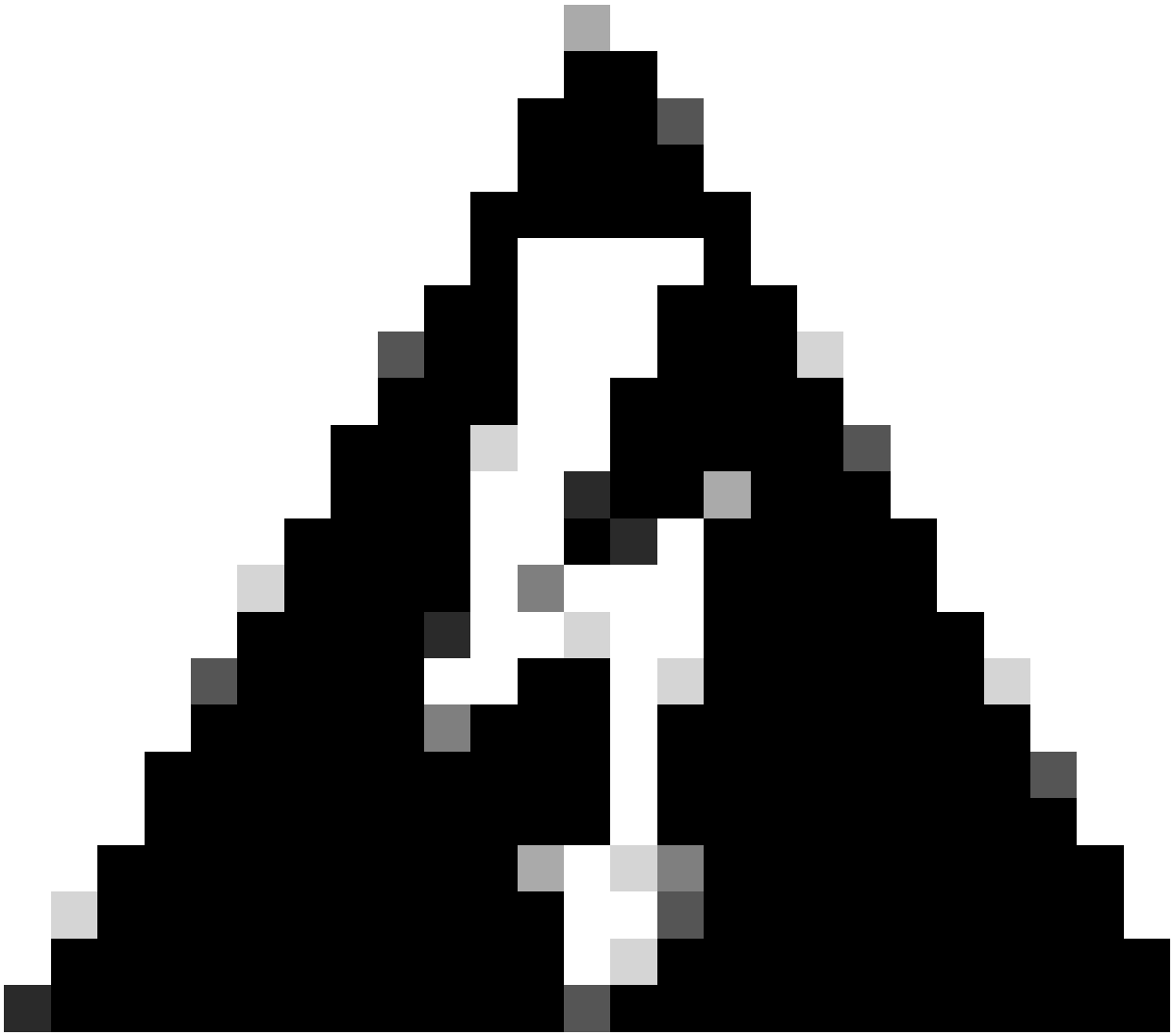
---

ヘッドエンドIPアドレスを定義するIKEv2キーリング、およびSSEヘッドエンドでの認証に使用する事前共有キーを定義します。

```
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>
```

IKEv2プロファイルのペアを設定します。
リモートピアの照合に使用するIKE IDのタイプと、ローカルルータがピアに送信するIKE IDを定

義する
SSEヘッドエンドのIKE IDはIPアドレスタイプであり、SSEヘッドエンドのパブリックIPと同じです。



警告: SSE側の同じネットワークトンネルグループで複数のトンネルを確立するには、それらがすべて同じローカルIKE IDを使用する必要があります。
Cisco IOS XEは、トンネルごとにローカルおよびリモートIKE IDの一意のペアを必要とするため、このようなシナリオをサポートしません。
この制限を克服するために、SSEヘッドエンドが次の形式のIKE IDを受け入れるように拡張されました： <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

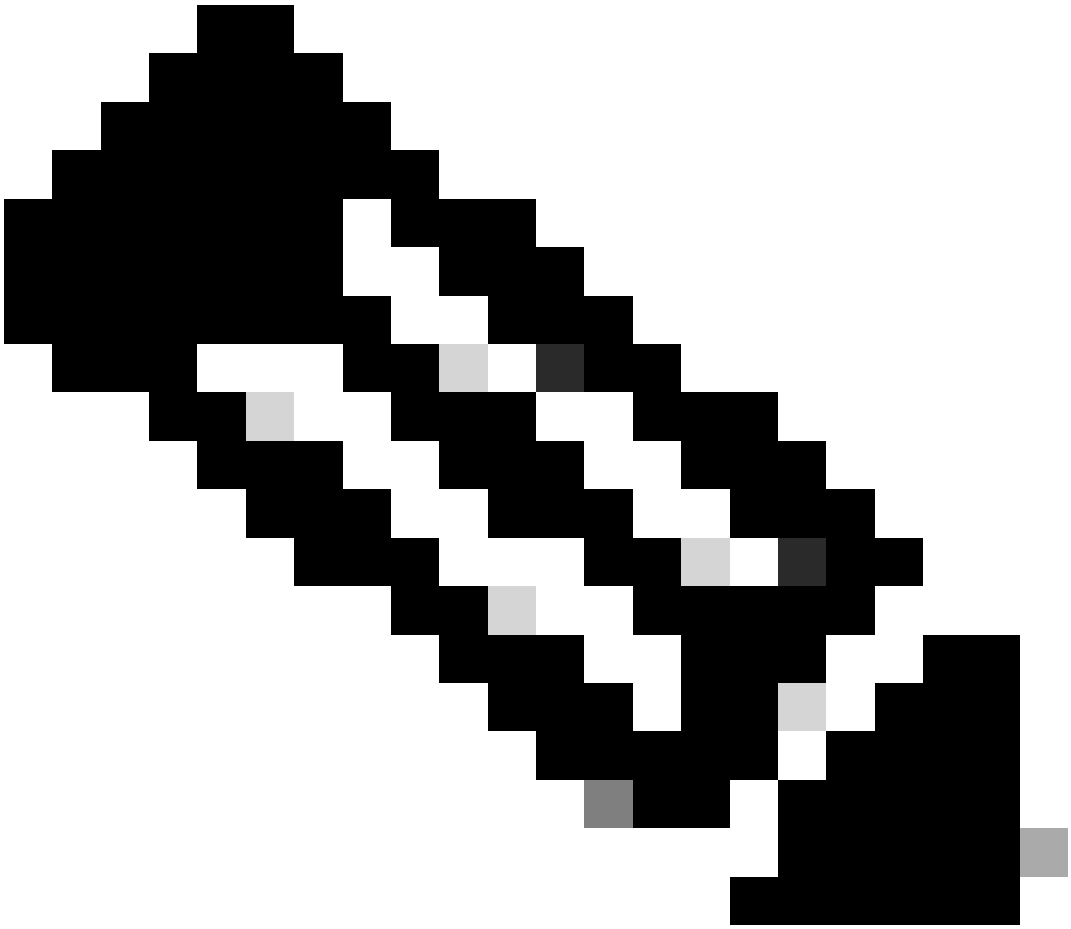
---

説明したラボシナリオでは、トンネルIDはcat8k-dmzとして定義されています。
通常のシナリオでは、ローカルIKE IDをcat8k-dmz@8195165-622405748-sse.cisco.comとして送信するようにルータを設定します。

ただし、同じネットワークトンネルグループで複数のトンネルを確立するには、ローカルIKE IDを使用します。

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

各文字列（tunnel1とtunnel2）に追加されたサフィックスに注意してください



注：上記のローカルIKE IDは、このラボシナリオで使用されている例です。任意のサフィックスを定義できます。要件を満たしていることを確認してください。

```
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トランスフォームセットを設定します。この設定は、IPSecセキュリティアソシエーション（フェーズ2）に使用されるアルゴリズムを定義します。

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

IKEv2プロファイルとトランスフォームセットをリンクするIPSecプロファイルを設定します。

```
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
```

仮想トンネル インターフェイス

このセクションでは、仮想トンネルインターフェイスの設定と、トンネル送信元として使用されるループバックインターフェイスについて説明します。

説明したラボシナリオでは、同じパブリックIPアドレスを使用する単一のピアで2つのVTIインターフェイスを確立する必要があります。また、Cisco IOS XEデバイスには、出力インターフェイスGigabitEthernet1が1つだけあります。

Cisco IOS XEは、同じトンネル送信元とトンネル宛先を持つ複数のVTIの設定をサポートしていません。

この制限を克服するために、ループバックインターフェイスを使用して、それぞれのVTIでトンネル送信元として定義できます。

ループバックとSSEパブリックIPアドレス間のIP接続を実現するには、いくつかのオプションがあります。

1. 公的にルーティング可能なIPアドレスをループバックインターフェイスに割り当てる（パブリックIPアドレス空間の所有権が必要）
2. プライベートIPアドレスをループバックインターフェイスに割り当て、ループバックIPソースを使用してトラフィックを動的にNATします。

3. VASIインターフェイスを使用する（多くのプラットフォームではサポートされておらず、セットアップとトラブルシューティングが煩雑）

このシナリオでは、2番目のオプションについて説明します。

2つのループバックインターフェイスを設定し、それぞれの下に「ip nat inside」コマンドを追加する

```
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
```

ダイナミックNATアクセスコントロールリスト(ACL)とNATオーバーロード文を定義します。

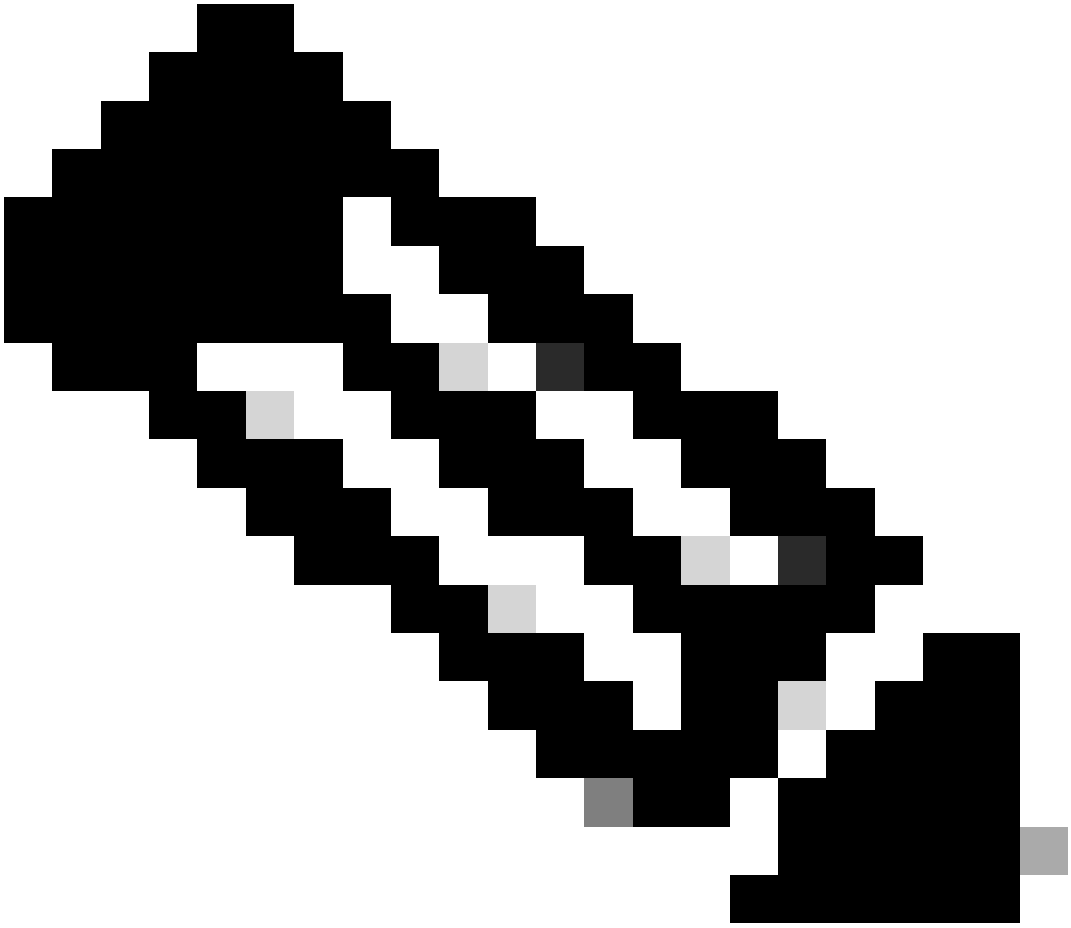
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

仮想トンネルインターフェイスを設定します。

```
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
```



注：説明されているラボシナリオでは、VTIに割り当てられたIPアドレスは、169.254.0.0/24の重複しないサブネットからのものです。
他のサブネット空間を使用することもできますが、そのようなアドレス空間を必要とするBGPに関する特定の要件があります。

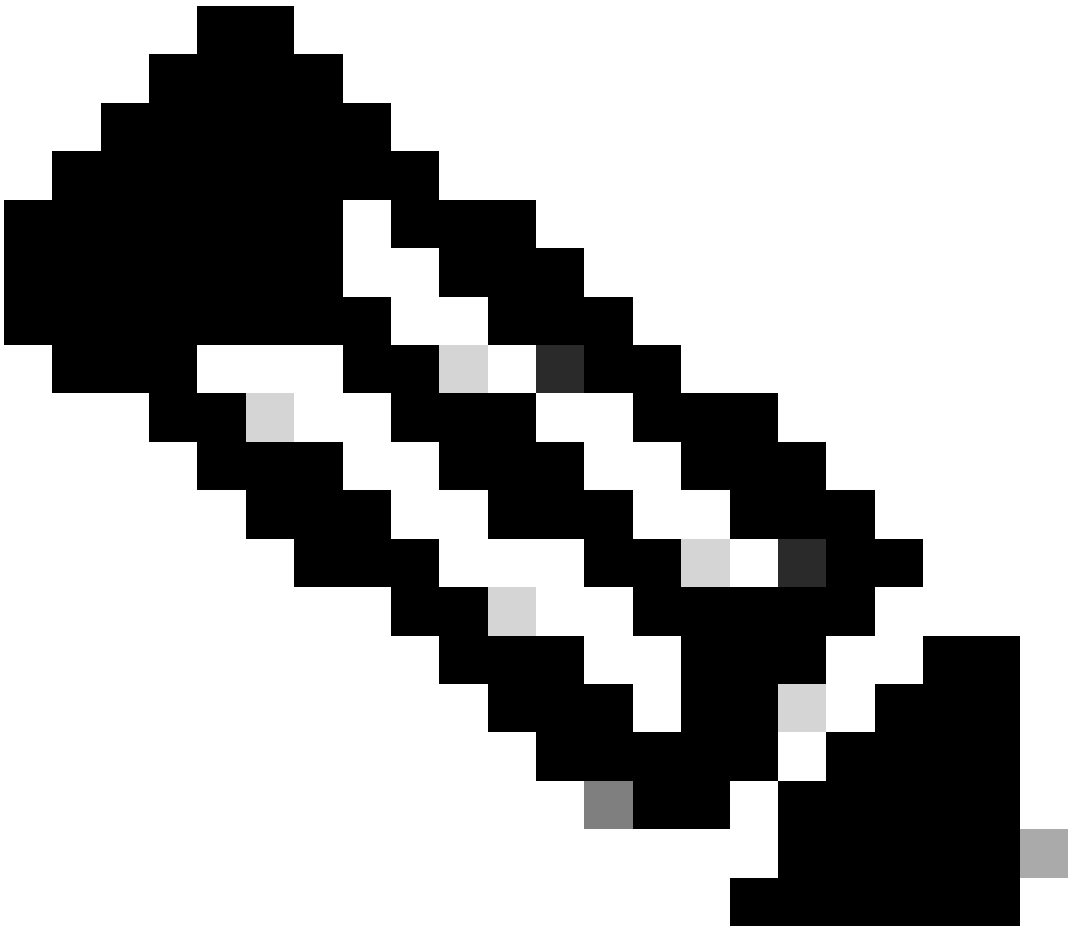
BGPルーティング

このセクションでは、SSEヘッドエンドとのBGPネイバーシップを確立するために必要な設定部分について説明します。
SSEヘッドエンドのBGPプロセスがサブネットからの任意のIPをリッスンする 169.254.0.0/24.
両方のVTIでBGPピアリングを確立するために、2つのネイバー169.254.0.9(Tunnel1)(Tunnel1)と169.254.0.13(Tunnel2)を定義します。
また、SSEダッシュボードに表示される値に従ってリモートASを指定する必要もあります。

<#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

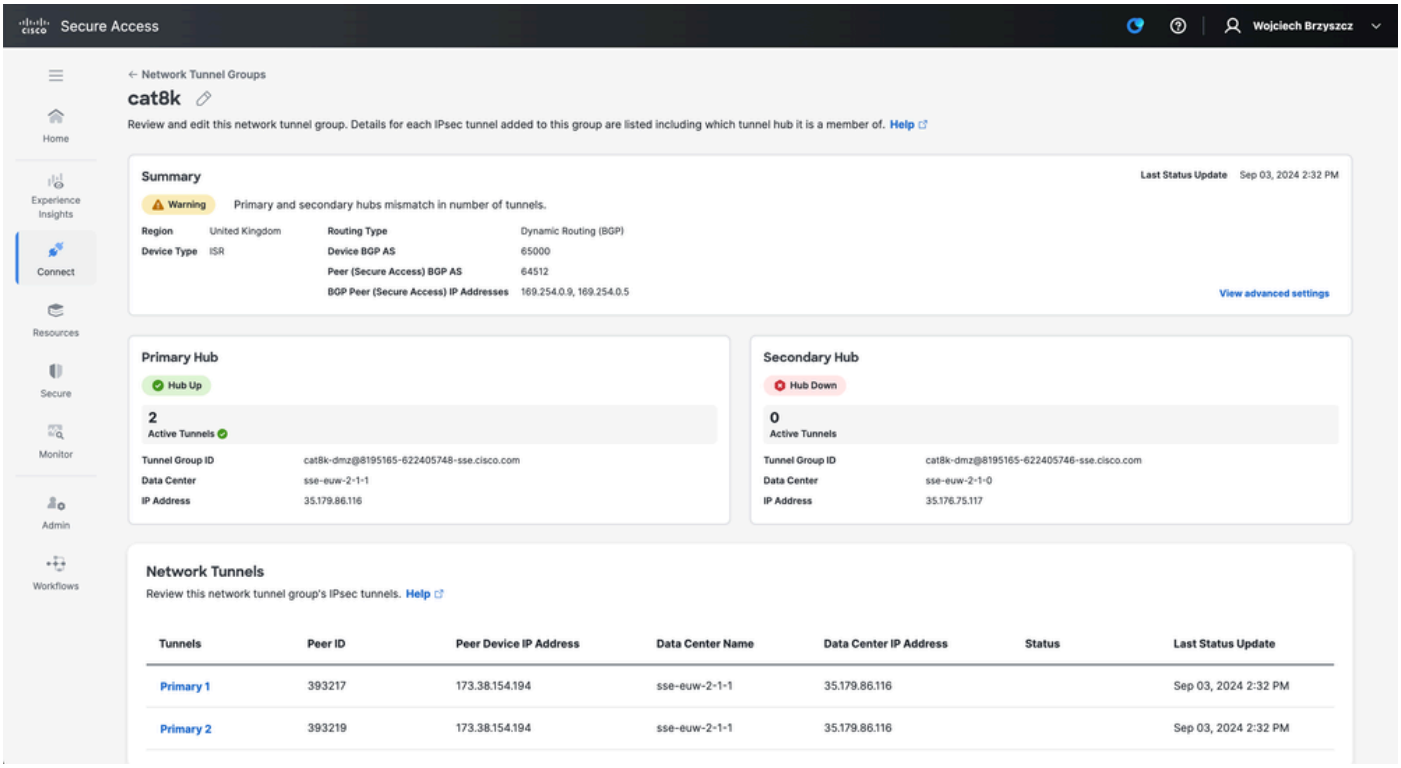


注：両方のピアから受信するルートは、完全に同じである必要があります。デフォルトでは、ルータはそのうちの1つだけをルーティングテーブルにインストールします。ルーティングテーブルに複数の重複ルートを登録できるようにするには（さらにECMPを有効にするには）、「maximum-paths <number of routes>」を設定する必要があります

確認

セキュアアクセスダッシュボード

SSEダッシュボードに2つのプライマリトンネルが表示されている必要があります。



Cisco IOS XEルータ

Cisco IOS XE側から両方のトンネルがREADY状態であることを確認します。

<#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
```

BGPネイバーシップが両方のピアでUPになっていることを確認します。

<#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
```

ルータがBGPから適切なルートを学習していること（およびルーティングテーブルに少なくとも2つのネクストホップが設定されていること）を確認します。

<#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
```

トラフィックを開始し、両方のトンネルが使用されていること、および両方のカプセル化およびカプセル化解除のカウンタが増加していることを確認します。

<#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
```

オプションで、両方のVTIインターフェイスでパケットキャプチャを収集して、トラフィックがVTI間でロードバランシングされるようにすることができます。Cisco IOS XEデバイスで組み込みパケットキャプチャを設定する方法については、この記事の説明をお読みください。
この例では、送信元IPが192.168.150.1のCISCO IOS XEルータの背後にあるホストが192.168.200.0/24サブネットから複数のIPにICMP要求を送信しています。

ICMP要求は、トンネル間で均等にロードバランシングされます。

<#root>

```
wbrzyszc-cat8k#
```

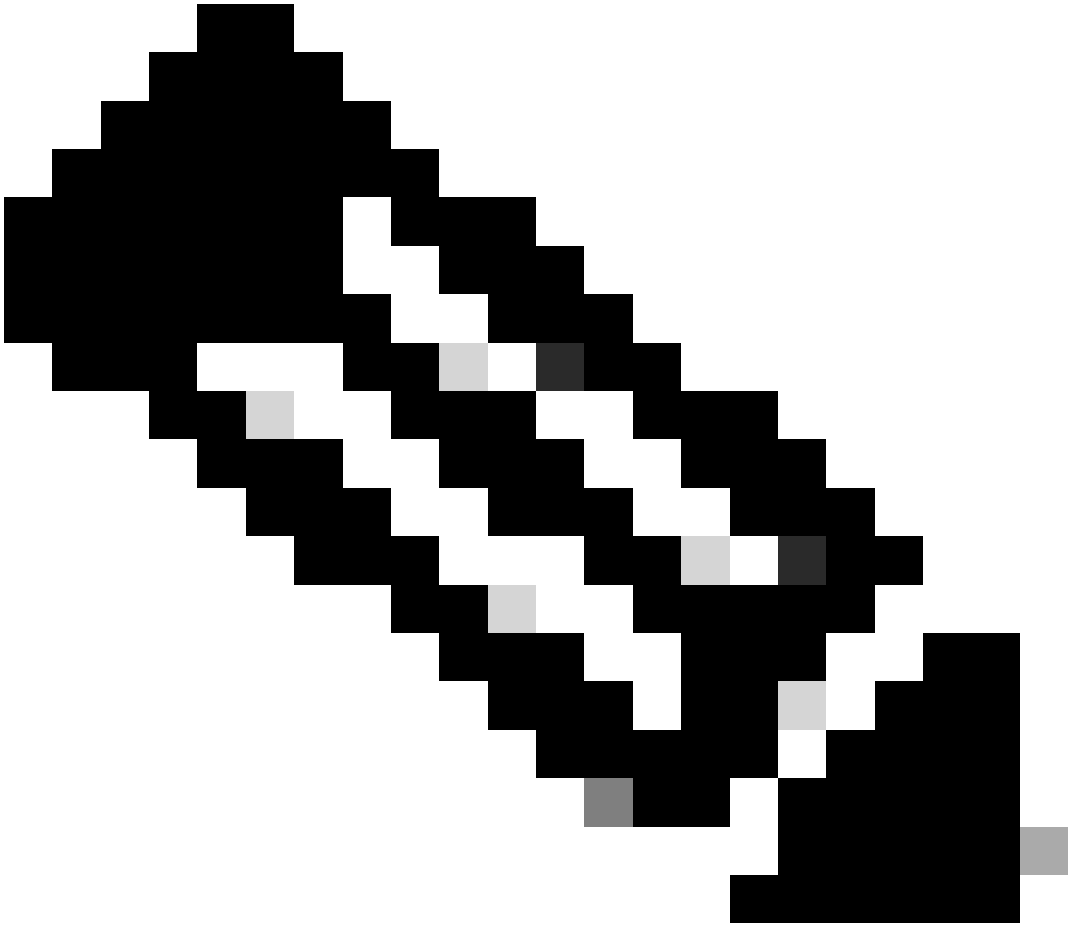
show monitor capture Tunnel1 buffer brief

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



注:Cisco IOS XEルータには、複数のECMPタプルによるロードバランシングメカニズムがあります。デフォルトでは、宛先単位のロードバランシングが有効になっています。これにより、同じ宛先IPへのトラフィックが常に同じパスを使用するようになります。パケット単位のロードバランシングを設定できます。これにより、同じ宛先IPに対してもトラフィックのロードバランシングがランダムに行われます。

関連情報

- セキュアアクセスユーザガイド
- 組み込みパケットキャプチャの収集方法
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。