Configurar o túnel de rede entre o Cisco Secure Access e o IOS XE Router usando ECMP com BGP

Contents

Introdução

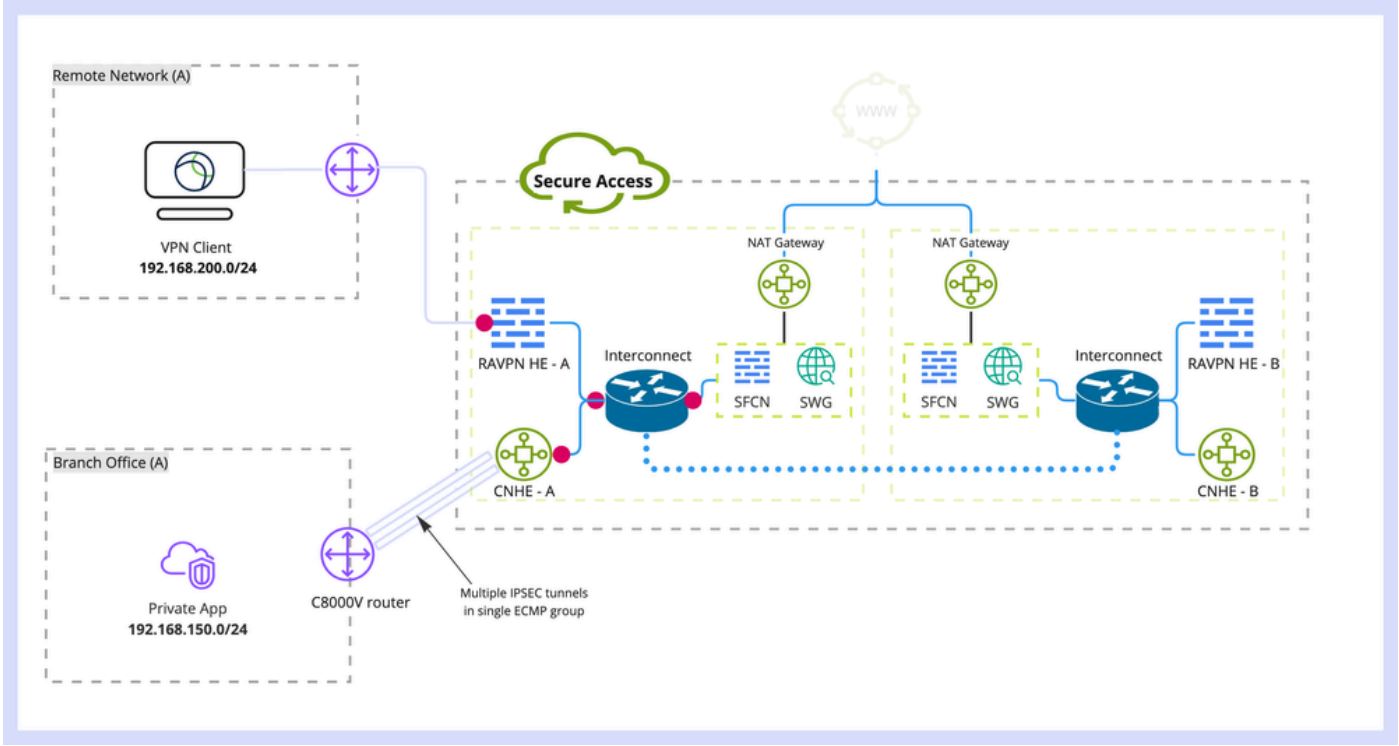
Este documento descreve as etapas necessárias para configurar e solucionar problemas de túnel VPN IPSec entre o Cisco Secure Access e o Cisco IOS XE usando BGP e ECMP.

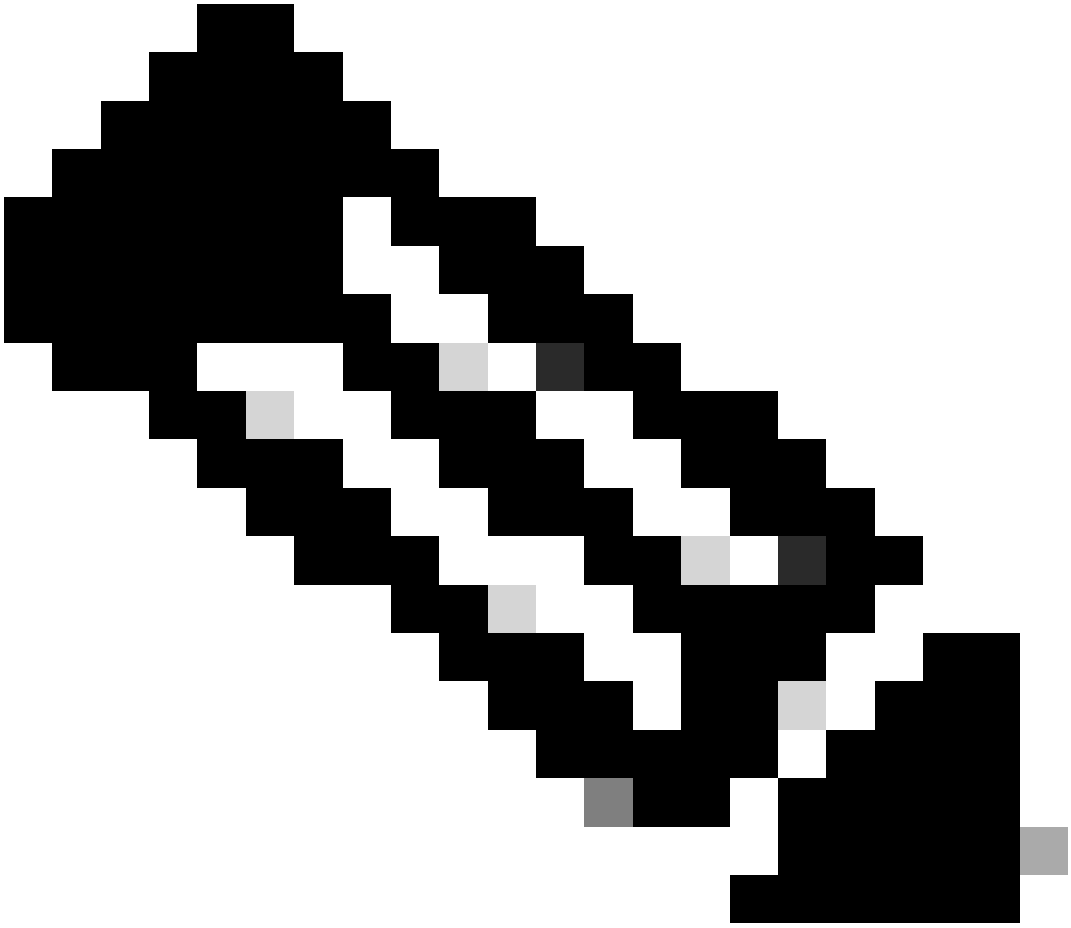
Diagrama de Rede

Neste exemplo de laboratório, discutiremos o cenário em que a rede 192.168.150.0/24 é um segmento de LAN atrás do dispositivo Cisco IOS XE e 192.168.200.0/24 é um pool de IP usado por usuários RAVPN que se conectam ao headend do Secure Access.

Nosso objetivo final é utilizar o ECMP em túneis VPN entre o dispositivo Cisco IOS XE e o headend de acesso seguro.

Para entender melhor a topologia, consulte o diagrama:


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



Observação: este é apenas um exemplo de fluxo de pacotes, você pode aplicar os mesmos princípios a qualquer outro fluxo e à sub-rede Secure Internet Access de 192.168.150.0/24 atrás do roteador Cisco IOS XE.

Pré-requisitos

Requisitos

Recomenda-se que você tenha conhecimento destes tópicos:

- Configuração e gerenciamento do Cisco IOS XE CLI
- Conhecimento básico dos protocolos IKEv2 e IPSec
- Configuração inicial do Cisco IOS XE (endereçamento IP, SSH, licença)
- Conhecimento básico de BGP e ECMP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C8000V executando a versão de software 17.9.4a
- PC Windows
- Organização Cisco Secure Access

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os túneis de rede no acesso seguro têm uma limitação de largura de banda de 1 Gbps por túnel único. Se a largura de banda da Internet de upstream/downstream for maior que 1 Gbps e você quiser utilizá-la totalmente, será necessário superar essa limitação configurando vários túneis com o mesmo data center de acesso seguro e agrupando-os em um único grupo ECMP.

Quando você encerra vários túneis com um único Network Tunnel Group (dentro de um único Secure Access DC), eles formam, por padrão, o grupo ECMP da perspectiva do headend do Secure Access.
O que significa que, uma vez que o headend do acesso seguro envia tráfego para o dispositivo VPN local, ele faz o balanceamento de carga entre os túneis (supondo que as rotas corretas sejam recebidas dos peers BGP).

Para obter a mesma funcionalidade no dispositivo VPN local, você precisaria configurar várias interfaces VTI em um único roteador e garantir que a configuração de roteamento apropriada seja aplicada.

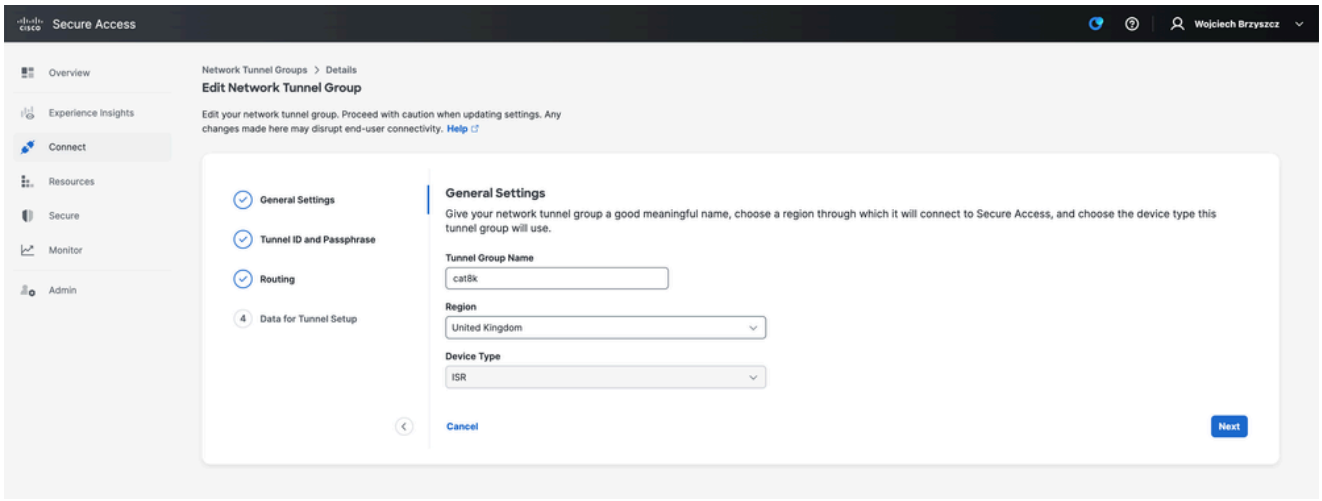
Este artigo descreve o cenário, com explicação de cada etapa necessária.

Configurar

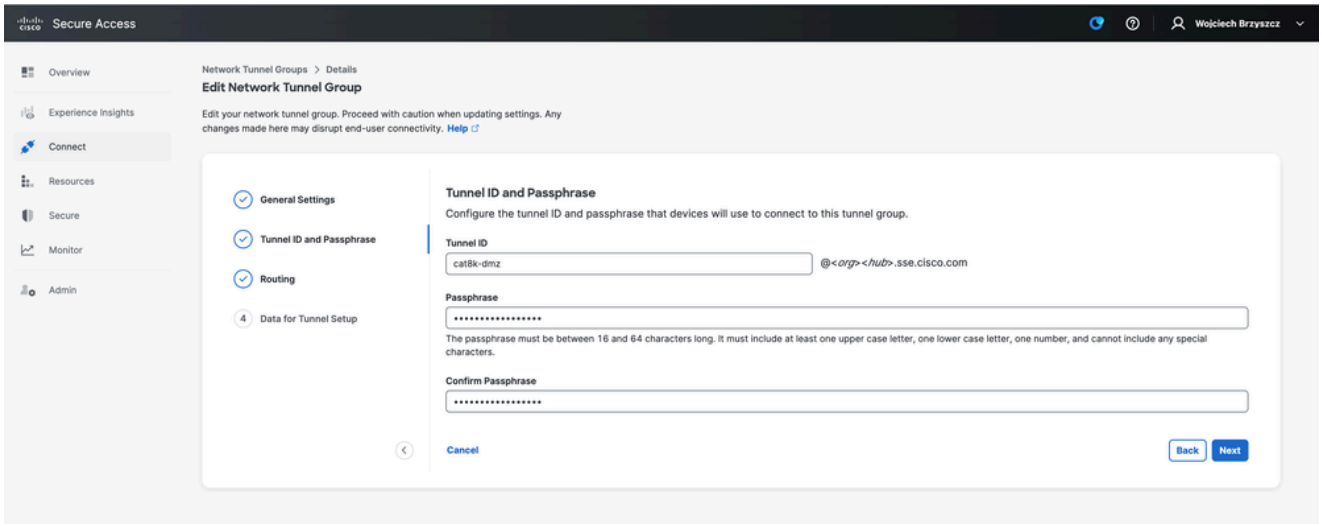
Configuração de acesso seguro

Não há configuração especial que precise ser aplicada no lado do acesso seguro, para formar o grupo ECMP de vários túneis VPN usando o protocolo BGP.
Etapas necessárias para configurar o Network Tunnel Group.

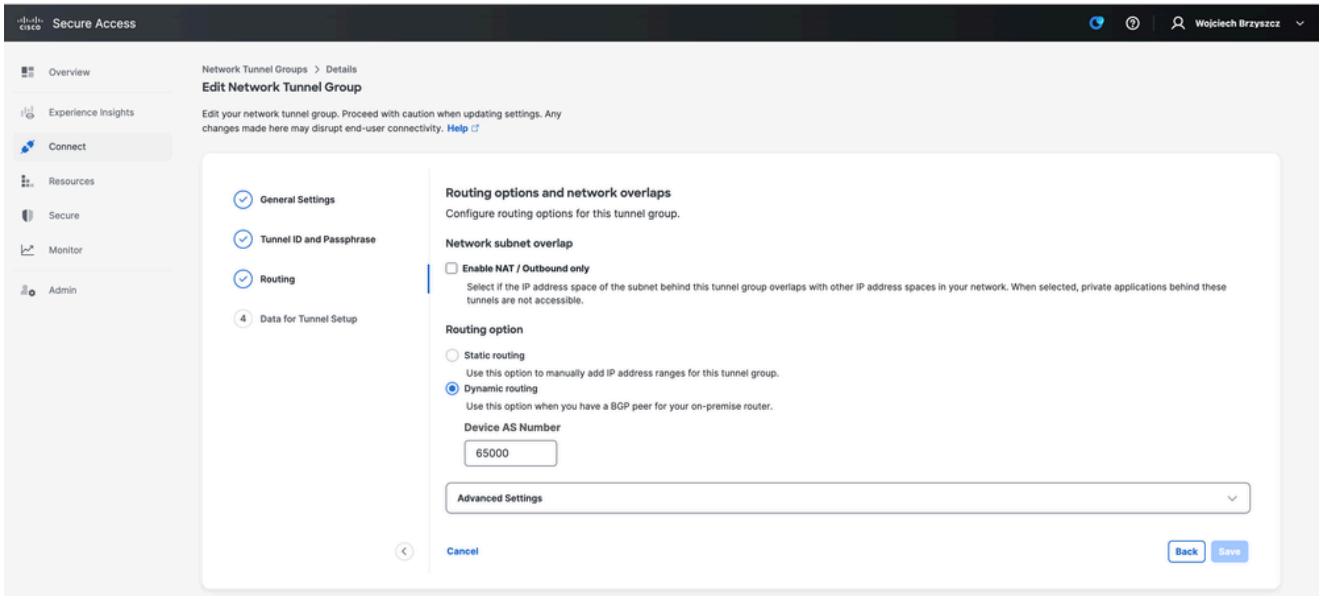
1. Crie um novo Grupo de Túneis de Rede (ou edite o existente).



2. Especifique a ID do túnel e a senha:



3. Configure as opções de roteamento, especifique o roteamento dinâmico e insira seu número AS interno. Neste cenário de laboratório, o ASN é igual a 65000.



4. Anote os detalhes do túnel na seção Data for Tunnel Setup.

configuração do Cisco IOS XE

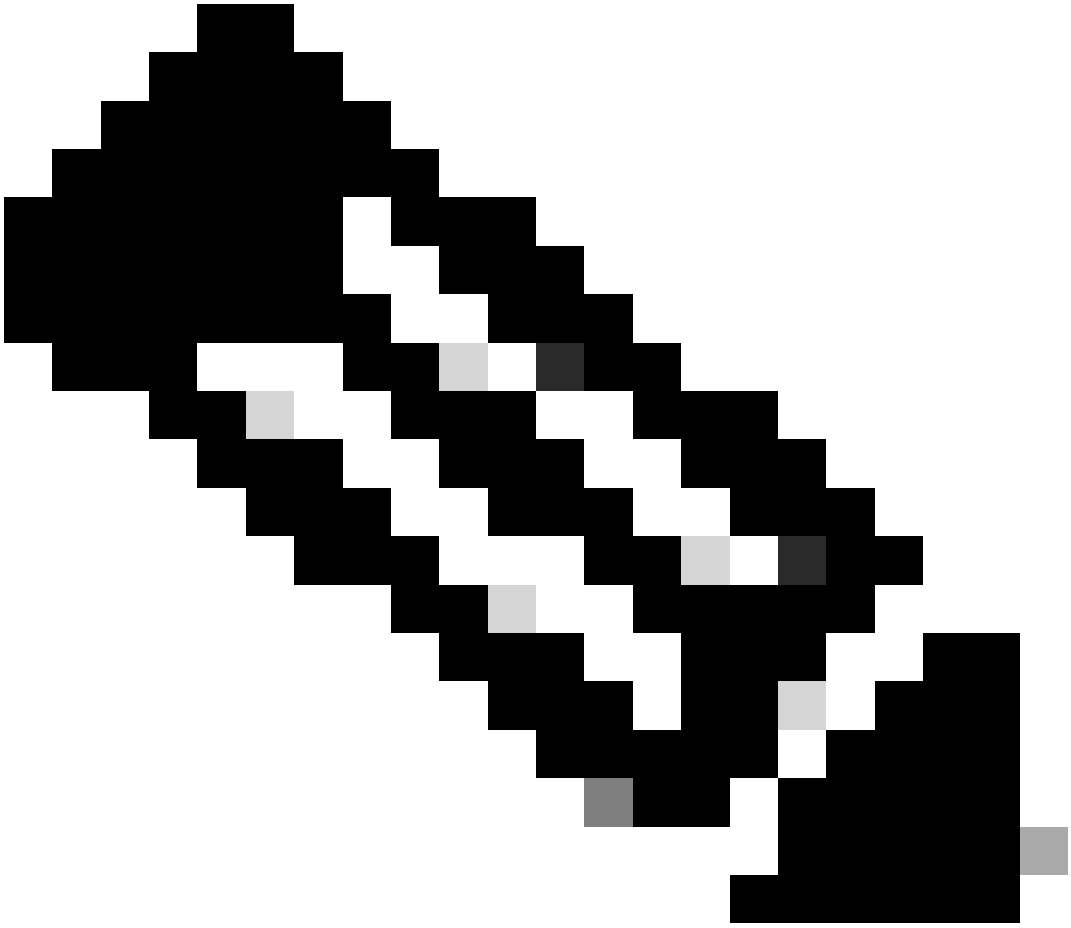
Esta seção aborda a configuração de CLI que precisa ser aplicada no roteador Cisco IOS XE, a fim de configurar adequadamente túneis IKEv2, vizinhança BGP e balanceamento de carga ECMP através de interfaces de túnel virtual.
Cada seção é explicada e as advertências mais comuns são mencionadas.

Parâmetros IKEv2 e IPsec

Configurar a Política IKEv2 e a Proposta IKEv2. Esses parâmetros definem quais algoritmos são usados para 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
```



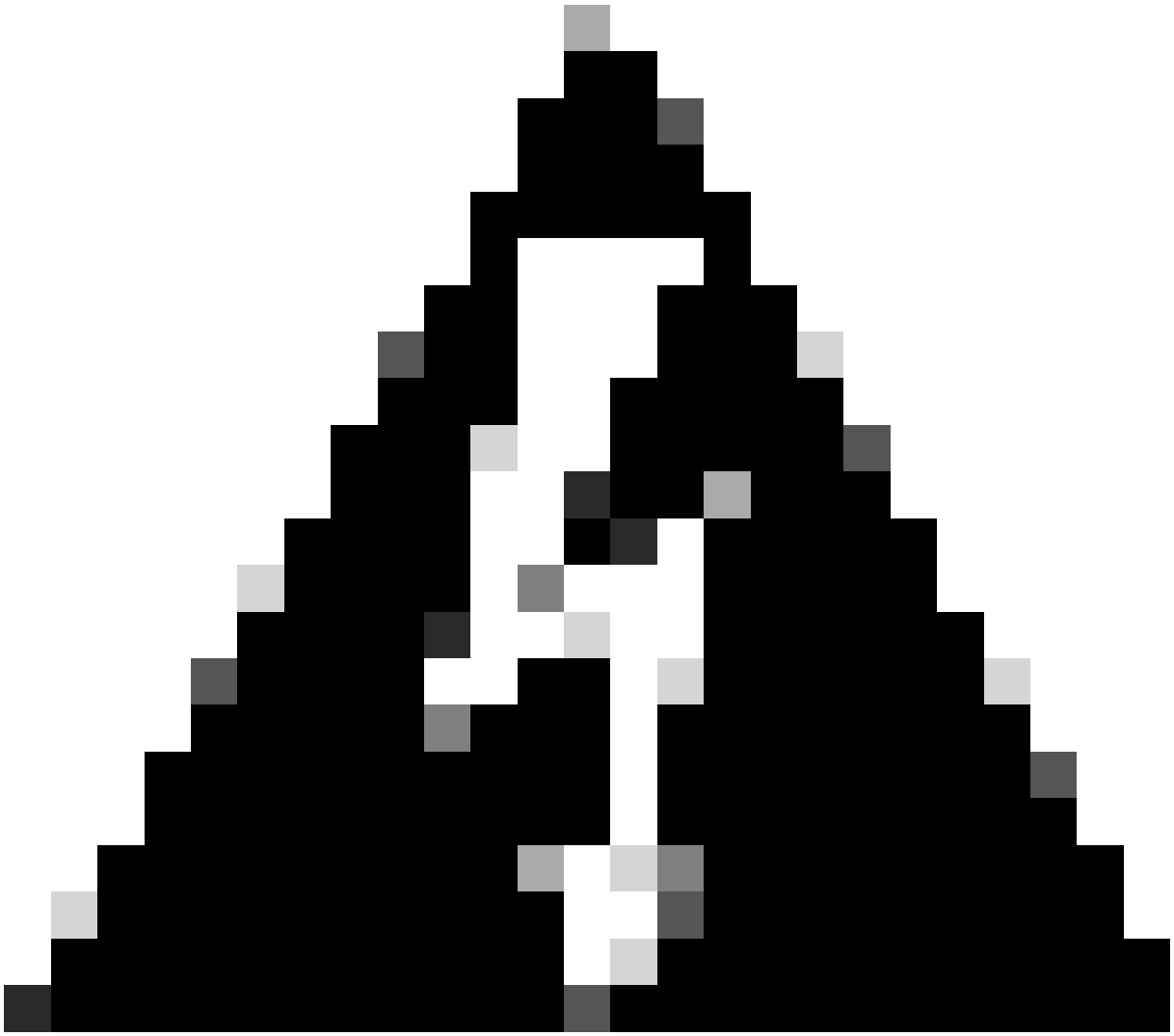
Observação: os parâmetros sugeridos e ideais são marcados em negrito nos documentos SSE: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Definir o chaveiro IKEv2 que define o endereço IP do ponto inicial e a chave pré-compartilhada usada para autenticar com o ponto inicial 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>
```

Configure o par de perfis IKEv2.
Eles definem que tipo de identidade IKE deve ser usada para corresponder ao peer remoto e que

identidade IKE o roteador local está enviando ao peer.
A identidade IKE do headend SSE é do tipo de endereço IP e é igual ao IP público do headend SSE.



Aviso: Para estabelecer vários túneis com o mesmo Network Tunnel Group no lado SSE, todos devem usar a mesma identidade IKE local.
O Cisco IOS XE não suporta tal cenário, pois requer um par exclusivo de identidades IKE locais e remotas por túnel.
Para superar essa limitação, o headend do SSE foi aprimorado para aceitar o ID do IKE no formato: <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

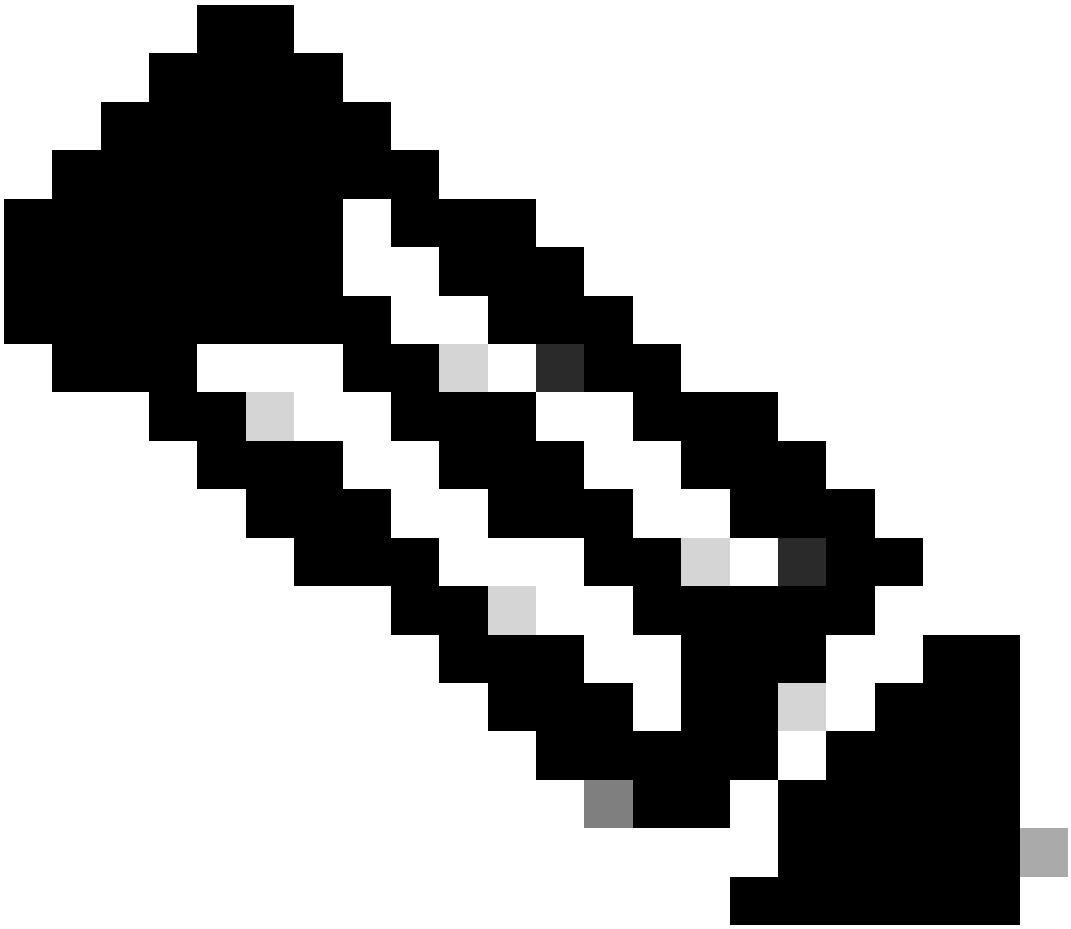
---

No cenário do laboratório discutido, o ID do túnel foi definido como cat8k-dmz.
No cenário normal, configuraríamos o roteador para enviar a identidade IKE local como cat8k-dmz@8195165-622405748-sse.cisco.com

No entanto, para estabelecer vários túneis com o mesmo Network Tunnel Group, serão usadas IDs IKE locais:

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

Observe o sufixo adicionado a cada string (tunnel1 e tunnel2)



> Observação: as identidades IKE locais mencionadas são apenas exemplos usados neste cenário de laboratório. Você pode definir qualquer sufixo que desejar, apenas certifique-se de atender aos requisitos.

```
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
```

Configurar o conjunto de transformação IPSec. Essa configuração define os algoritmos usados para a Associação de Segurança IPsec (fase 2):

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

Configure perfis IPSec que vinculam perfis IKEv2 com Conjuntos de Transformações:

```
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 túnel virtual

Esta seção aborda a configuração de interfaces de túnel virtual e interfaces de loopback usadas como origem do túnel.

No cenário de laboratório discutido, precisamos estabelecer duas interfaces VTI com um único peer usando o mesmo endereço IP público. Além disso, nosso dispositivo Cisco IOS XE tem apenas uma interface de saída GigabitEthernet1.

O Cisco IOS XE não suporta a configuração de mais de um VTI com a mesma origem de túnel e destino de túnel.

Para superar essa limitação, você pode usar interfaces de loopback e defini-las como origem de túnel no respectivo VTI.

Há poucas opções para obter conectividade IP entre o loopback e o endereço IP público SSE:

1. Atribuir um endereço IP roteável publicamente à interface de loopback (requer a propriedade do espaço de endereço IP público)
2. Atribua um endereço IP privado à interface de loopback e tráfego NAT dinâmico com origem

de IP de loopback.
3. Usar interfaces VASI (não suportadas em muitas plataformas, incômodas para configurar e solucionar problemas)

Neste cenário, discutiremos a segunda opção.

Configure duas interfaces de loopback e adicione o comando "ip nat inside" em cada uma delas.

```
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
```

Defina a lista de controle de acesso NAT dinâmica e a instrução de sobrecarga NAT:

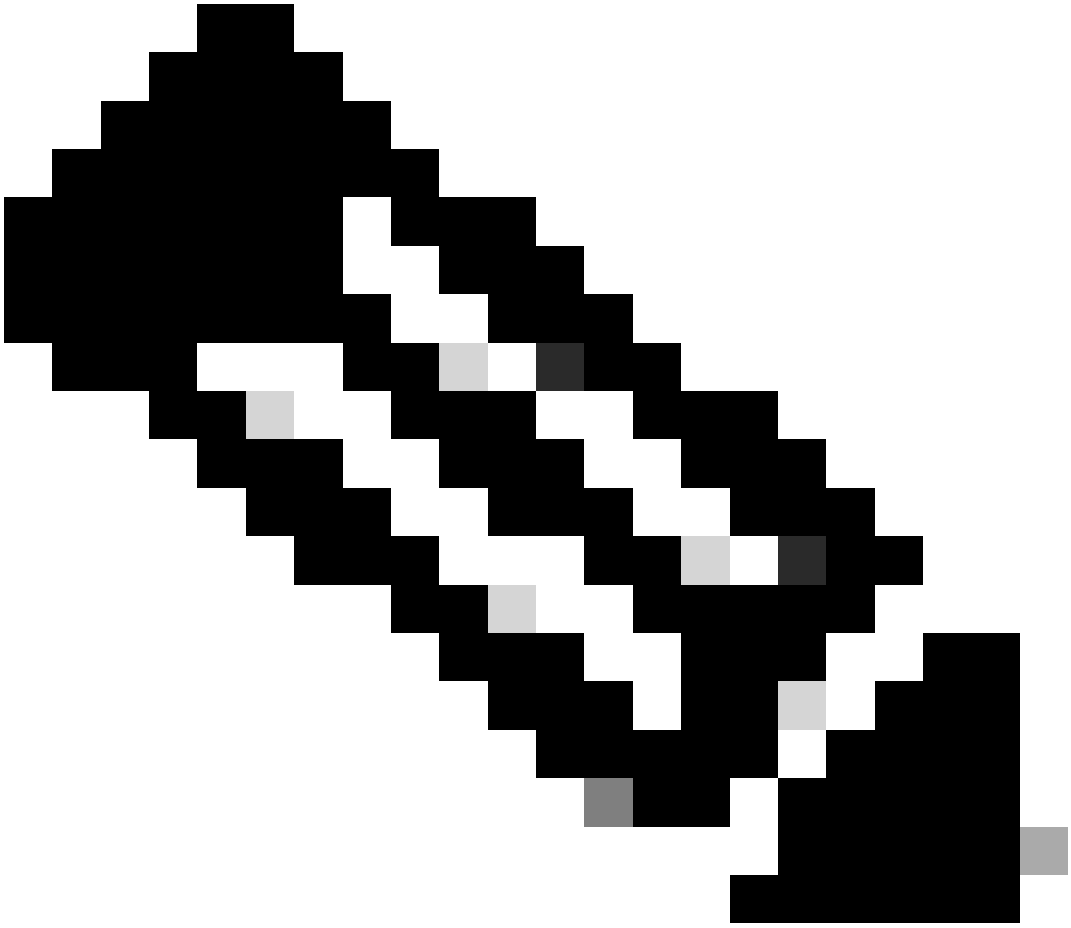
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

Configure as interfaces de túnel virtual.

```
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
```



Observação: no cenário de laboratório descrito, os endereços IP atribuídos aos VTIs são de sub-redes sem sobreposição de 169.254.0.0/24.
Você pode usar outro espaço de sub-rede, mas há certos requisitos relacionados ao BGP que requerem tal espaço de endereço.

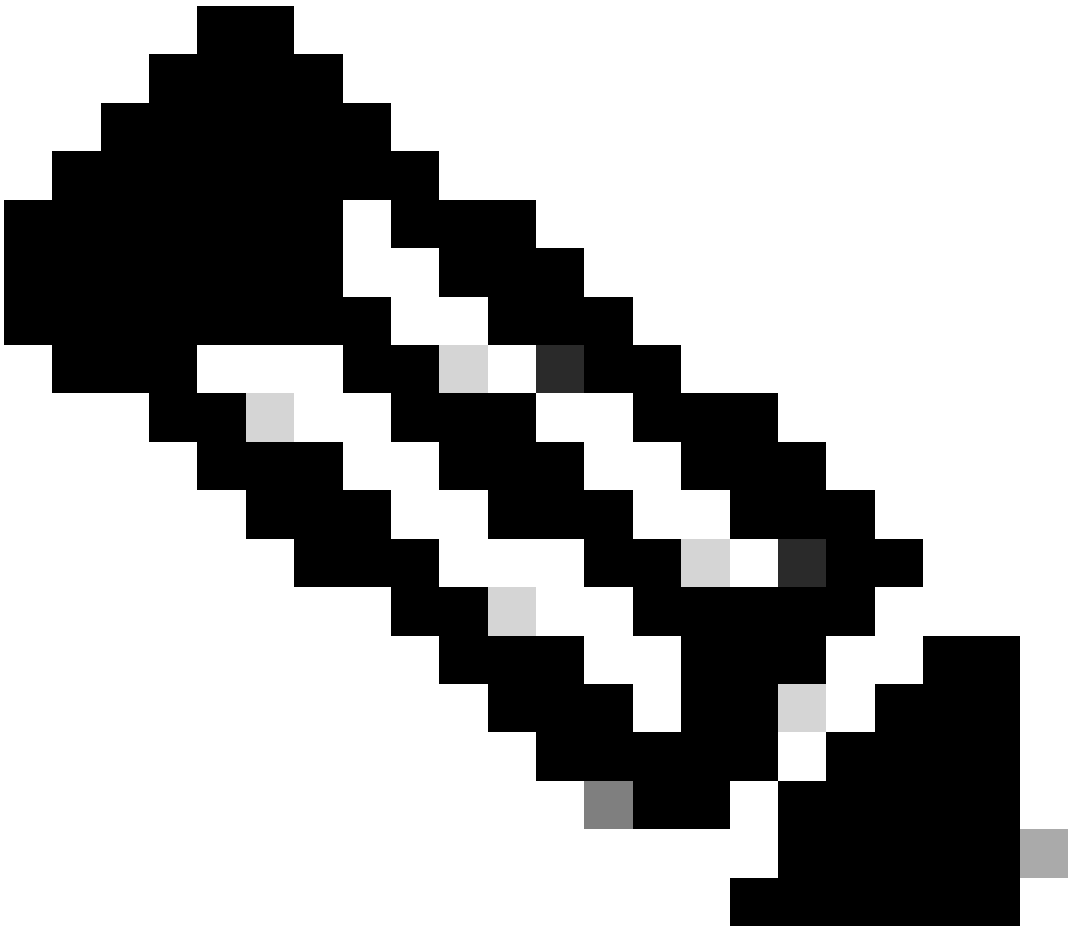
Roteamento BGP

Esta seção aborda a parte de configuração necessária para estabelecer a vizinhança BGP com o headend SSE.
O processo BGP no headend SSE escuta em qualquer IP da sub-rede 169.254.0.0/24.
Para estabelecer o peering BGP em ambos os VTIs, vamos definir dois vizinhos 169.254.0.9 (Tunnel1) e 169.254.0.13 (Tunnel2).
Além disso, você precisa especificar o AS remoto de acordo com o valor visto no painel do 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

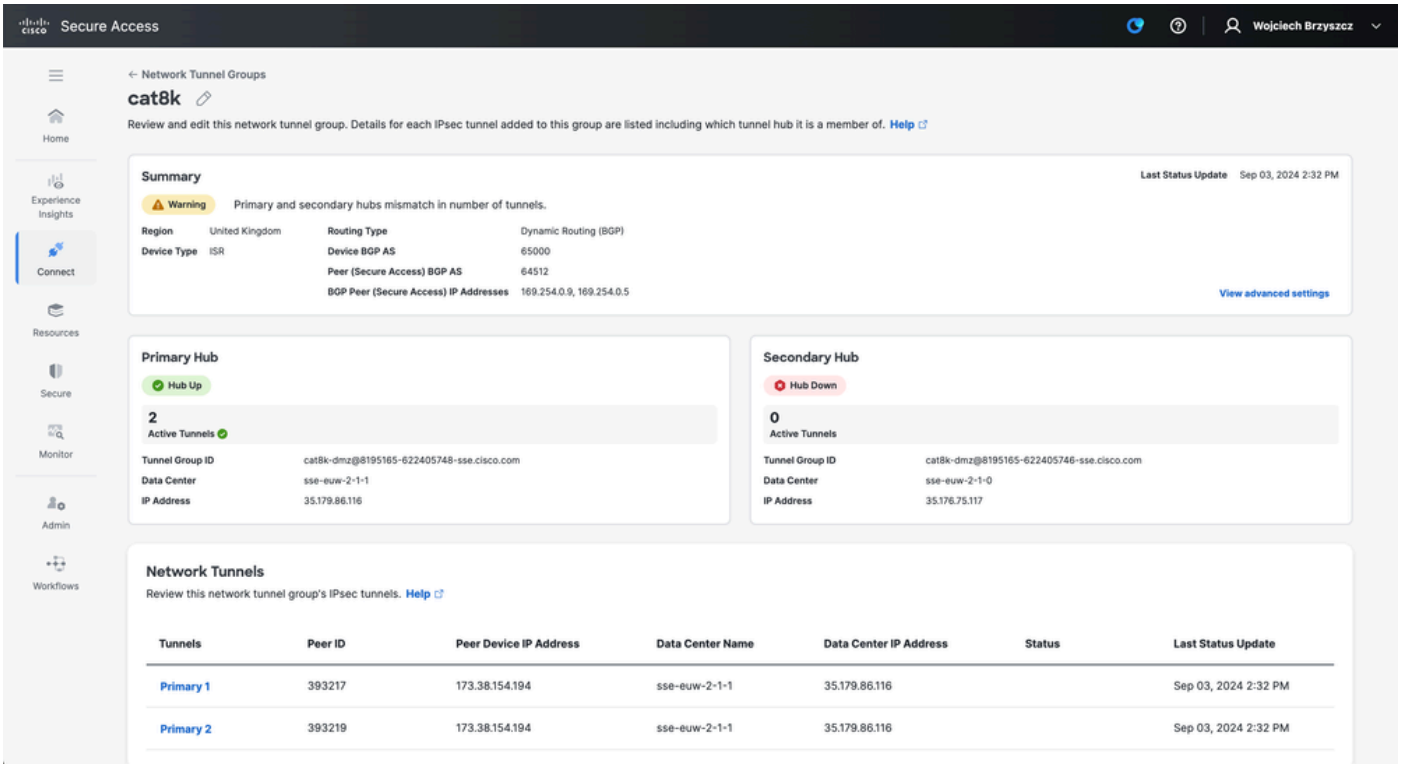


Observação: as rotas recebidas de ambos os peers devem ser exatamente as mesmas. Por padrão, o roteador instala apenas um deles na tabela de roteamento.
Para permitir que mais de uma rota duplicada seja instalada na tabela de roteamento (e habilitar o ECMP), você deve configurar "maximum-paths <número de rotas>"

Verificar

Painel de acesso seguro

Você deve ver dois túneis primários no painel SSE:



Roteador Cisco IOS XE

Verifique se ambos os túneis estão no estado READY do lado do 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
```

Verifique se a vizinhança BGP está UP com ambos os peers:

<#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
```

Verifique se o roteador aprende as rotas apropriadas do BGP (e se há pelo menos dois próximos saltos instalados na tabela de roteamento).

<#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
```

Inicie o tráfego e verifique se ambos os túneis são utilizados e você verá contadores encaps e decaps aumentando para ambos.

<#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
```

Opcionalmente, você pode coletar a captura de pacotes em ambas as interfaces VTI para garantir que o tráfego tenha a carga balanceada entre VTIs. Leia as instruções deste artigo para configurar o Embedded Packet Capture no dispositivo Cisco IOS XE.
No exemplo, o host atrás do roteador Cisco IOS XE com o IP de origem 192.168.150.1 estava enviando solicitações ICMP para vários IPs da sub-rede 192.168.200.0/24.

Como você pode ver, as solicitações ICMP têm a mesma carga balanceada entre os túneis.

<#root>

```
wbrzyszc-cat8k#
```

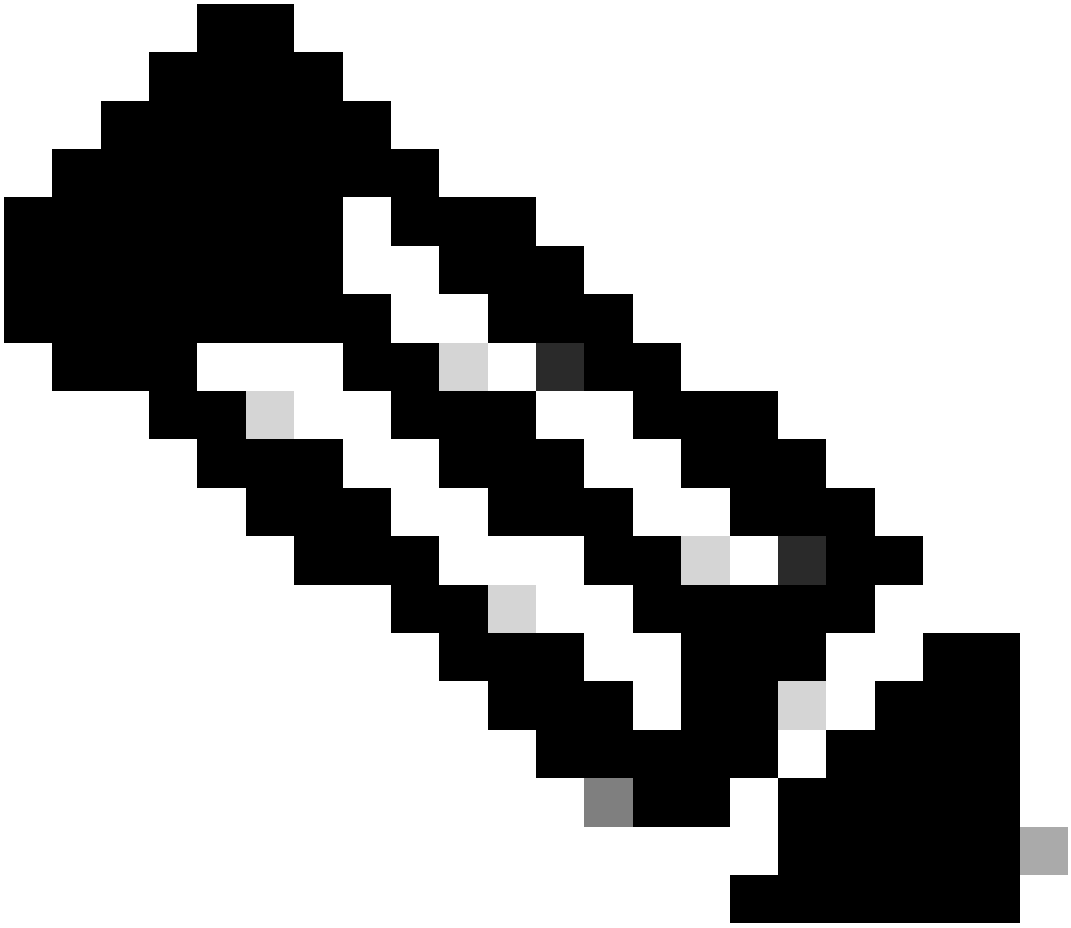
show monitor capture Tunnel1 buffer brief

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



Observação: há vários mecanismos de balanceamento de carga ECMP nos roteadores Cisco IOS XE. Por padrão, o balanceamento de carga por destino está habilitado, o que garante que o tráfego para o mesmo IP de destino sempre siga o mesmo caminho. Você pode configurar o balanceamento de carga por pacote, que balancearia aleatoriamente o tráfego até para o mesmo IP de destino.

Informações Relacionadas

- Guia do usuário do Secure Access
- Como coletar captura de pacotes incorporada
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.