Configuración del túnel de red entre Cisco Secure Access y el router IOS XE mediante ECMP con BGP

Contenido

Introducción

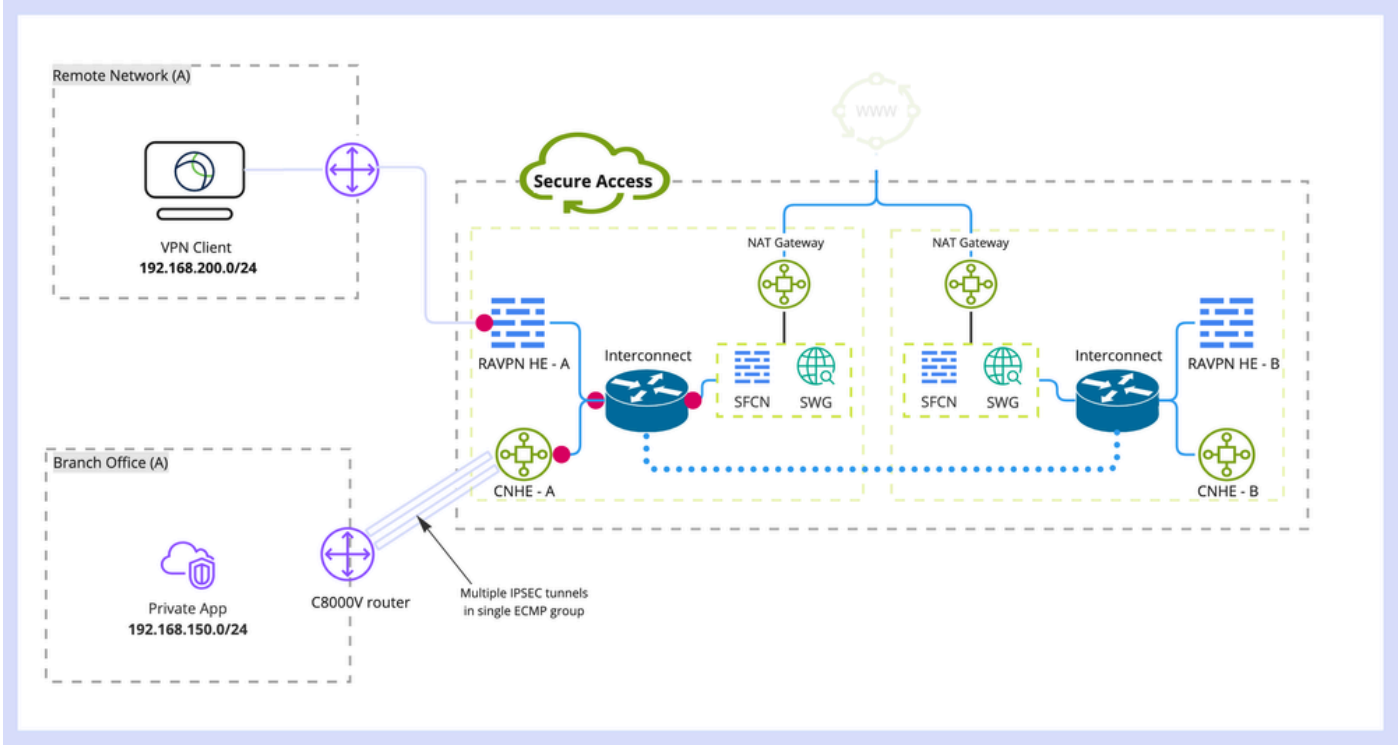
Este documento describe los pasos necesarios para configurar y resolver problemas del túnel VPN IPSec entre Cisco Secure Access y Cisco IOS XE mediante BGP y ECMP.

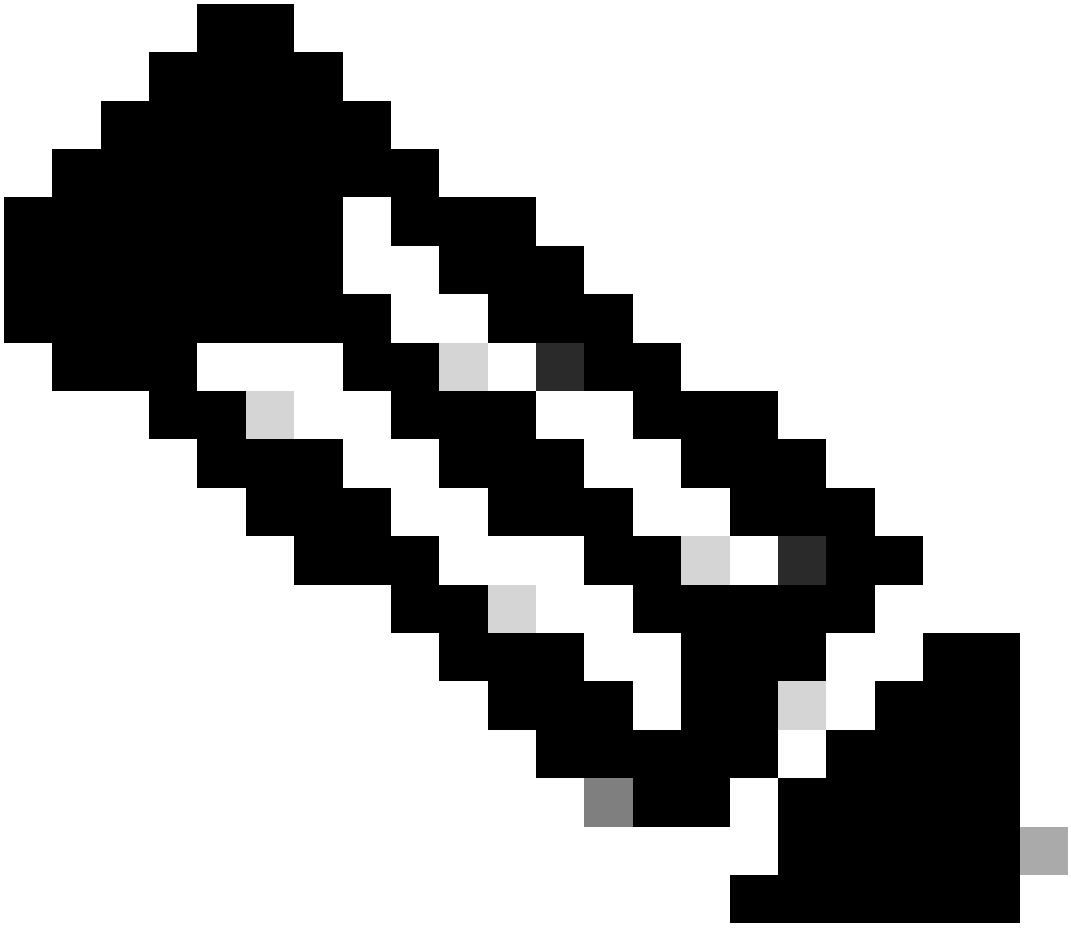
Diagrama de la red

En este ejemplo de laboratorio, vamos a discutir el escenario donde la red 192.168.150.0/24 es el segmento de LAN detrás del dispositivo Cisco IOS XE, y 192.168.200.0/24 es el conjunto de IP utilizado por los usuarios de RAVPN que se conectan a la cabecera de Secure Access.

Nuestro objetivo final es utilizar ECMP en túneles VPN entre el dispositivo Cisco IOS XE y la cabecera Secure Access.

Para entender mejor la topología, consulte el 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



Nota: Este es solo un ejemplo de flujo de paquetes, puede aplicar los mismos principios a cualquier otro flujo y a Secure Internet Access desde la subred 192.168.150.0/24 detrás del router Cisco IOS XE.

Prerequisites

Requirements

Se recomienda que tenga conocimiento de estos temas:

- Configuración y gestión de CLI de Cisco IOS XE
- Conocimientos básicos de los protocolos IKEv2 e IPSec
- Configuración inicial de Cisco IOS XE (direccionamiento IP, SSH, licencia)
- Conocimientos básicos de BGP y ECMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8000V con versión de software 17.9.4a
- PC con Windows
- Organización Cisco Secure Access

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los túneles de red de Secure Access tienen una limitación de ancho de banda de 1 Gbps por túnel único. Si el ancho de banda de Internet de flujo ascendente/descendente es superior a 1 Gbps y desea utilizarlo por completo, debe superar esta limitación configurando varios túneles con el mismo Data Center de Secure Access y agrupándolos en un único grupo ECMP.

Cuando finaliza varios túneles con el único grupo de túnel de red (dentro de un único DC de Secure Access), estos forman de forma predeterminada el grupo ECMP desde la perspectiva de cabecera de Secure Access.
Lo que significa que una vez que la cabecera de Secure Access envía el tráfico hacia el dispositivo VPN en las instalaciones, se equilibra la carga entre los túneles (suponiendo que se reciban las rutas correctas de los peers BGP).

Para lograr la misma funcionalidad en el dispositivo VPN local, debe configurar varias interfaces VTI en un único router y asegurarse de que se aplica la configuración de routing adecuada.

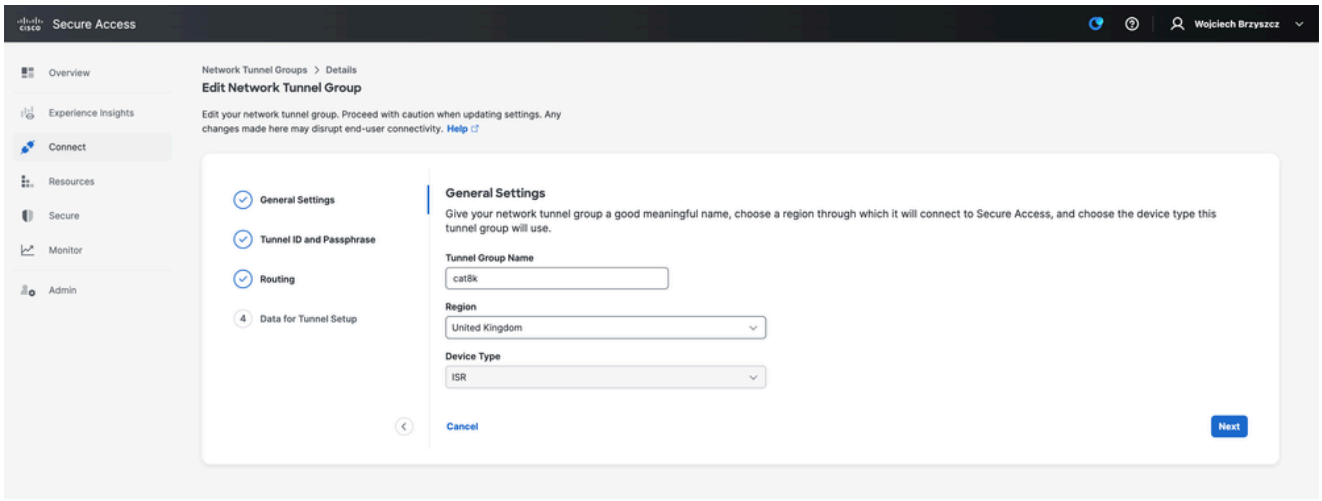
En este artículo se describe el escenario, con una explicación de cada paso necesario.

Configurar

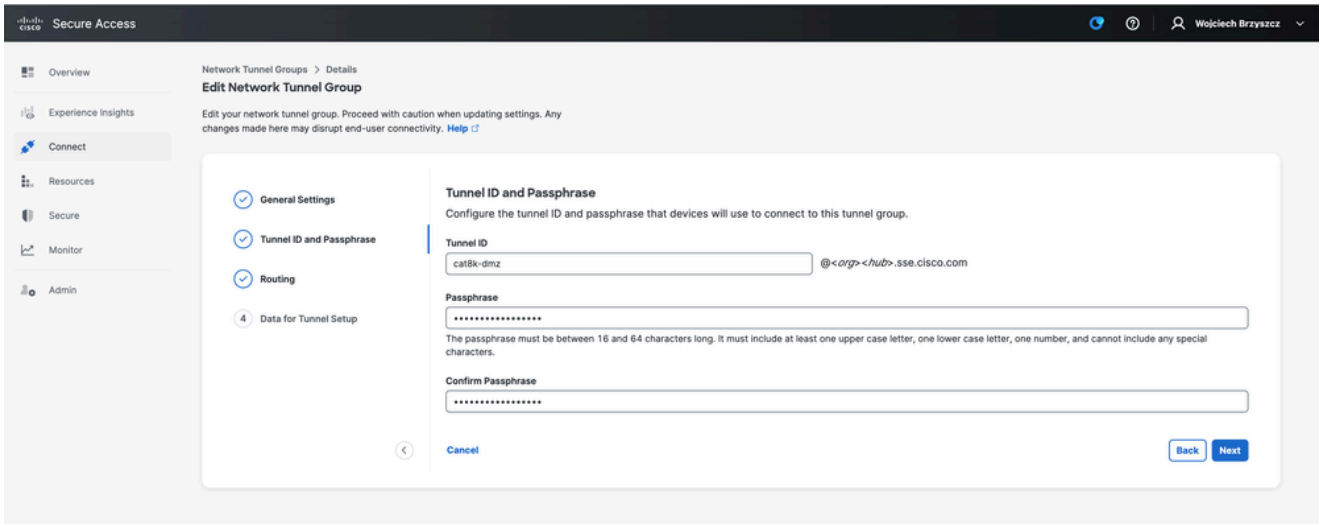
Configuración de Secure Access

No hay ninguna configuración especial que deba aplicarse en el lado de Secure Access, para formar el grupo ECMP desde varios túneles VPN usando el protocolo BGP.
Pasos necesarios para configurar el grupo de túnel de red.

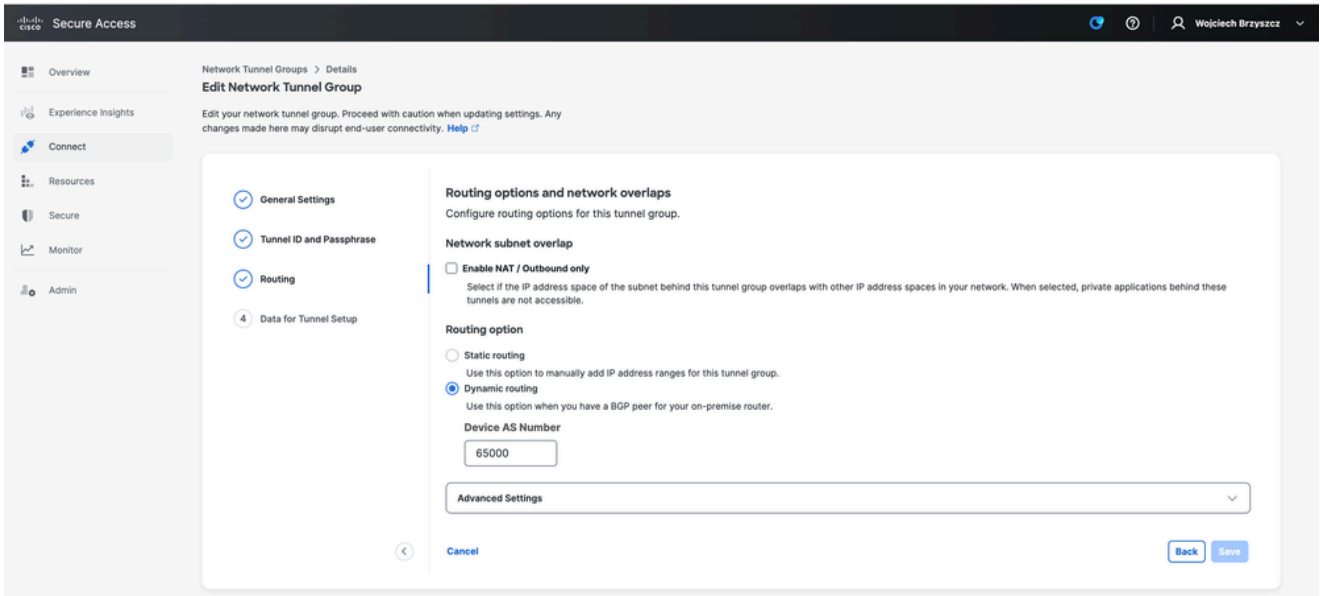
1. Cree un nuevo grupo de túnel de red (o edite uno existente).



2. Especifique ID de túnel y frase de contraseña:



3. Configure las opciones de ruteo, especifique el ruteo dinámico e ingrese su número de AS interno. En este escenario de laboratorio, el ASN es igual a 65000.



4. Anote los detalles del túnel en la sección Datos para la Configuración del Túnel.

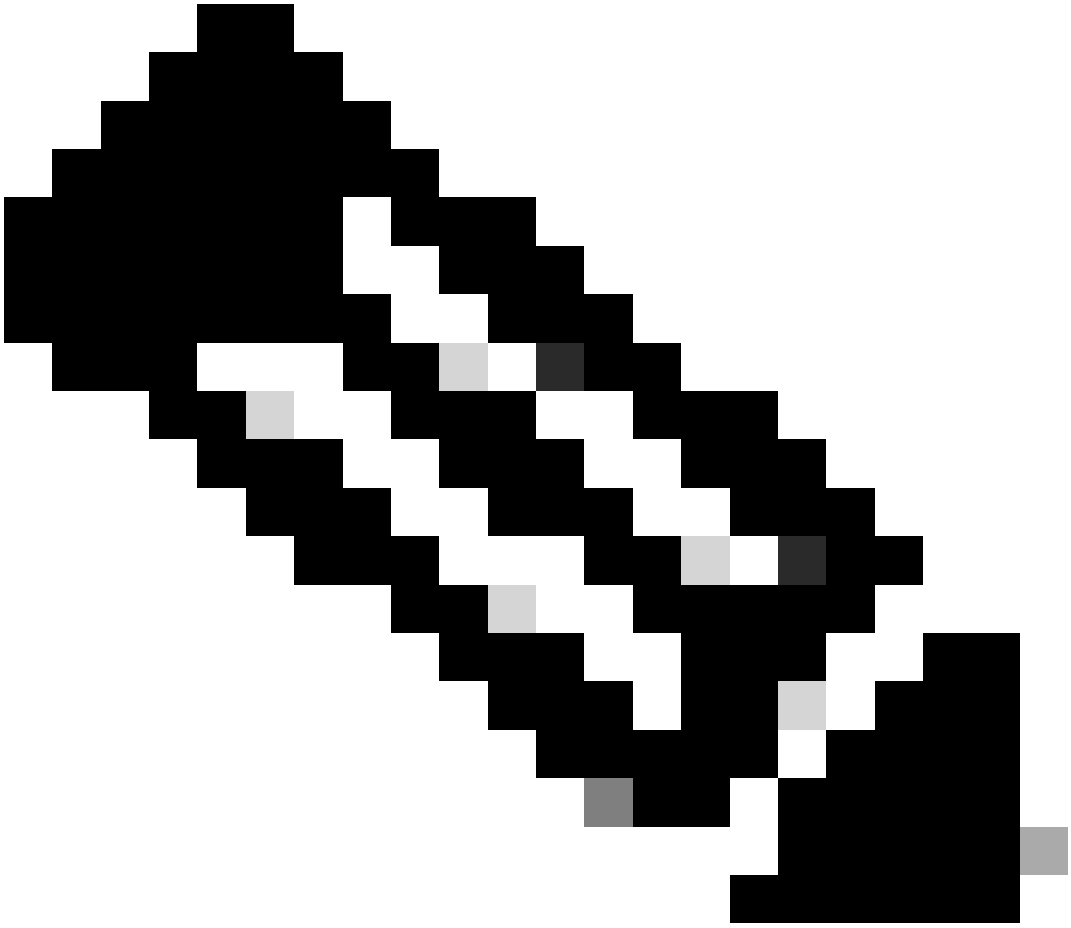
Configuración de Cisco IOS XE

Esta sección trata sobre la configuración de CLI que debe aplicarse en el router Cisco IOS XE, para configurar correctamente los túneles IKEv2, la vecindad BGP y el balanceo de carga ECMP a través de las interfaces de túnel virtual.
Se explica cada sección y se mencionan las advertencias más comunes.

Parámetros IKEv2 e IPsec

Configuración de la política IKEv2 y la propuesta IKEv2. Estos parámetros definen qué algoritmos se utilizan 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
```



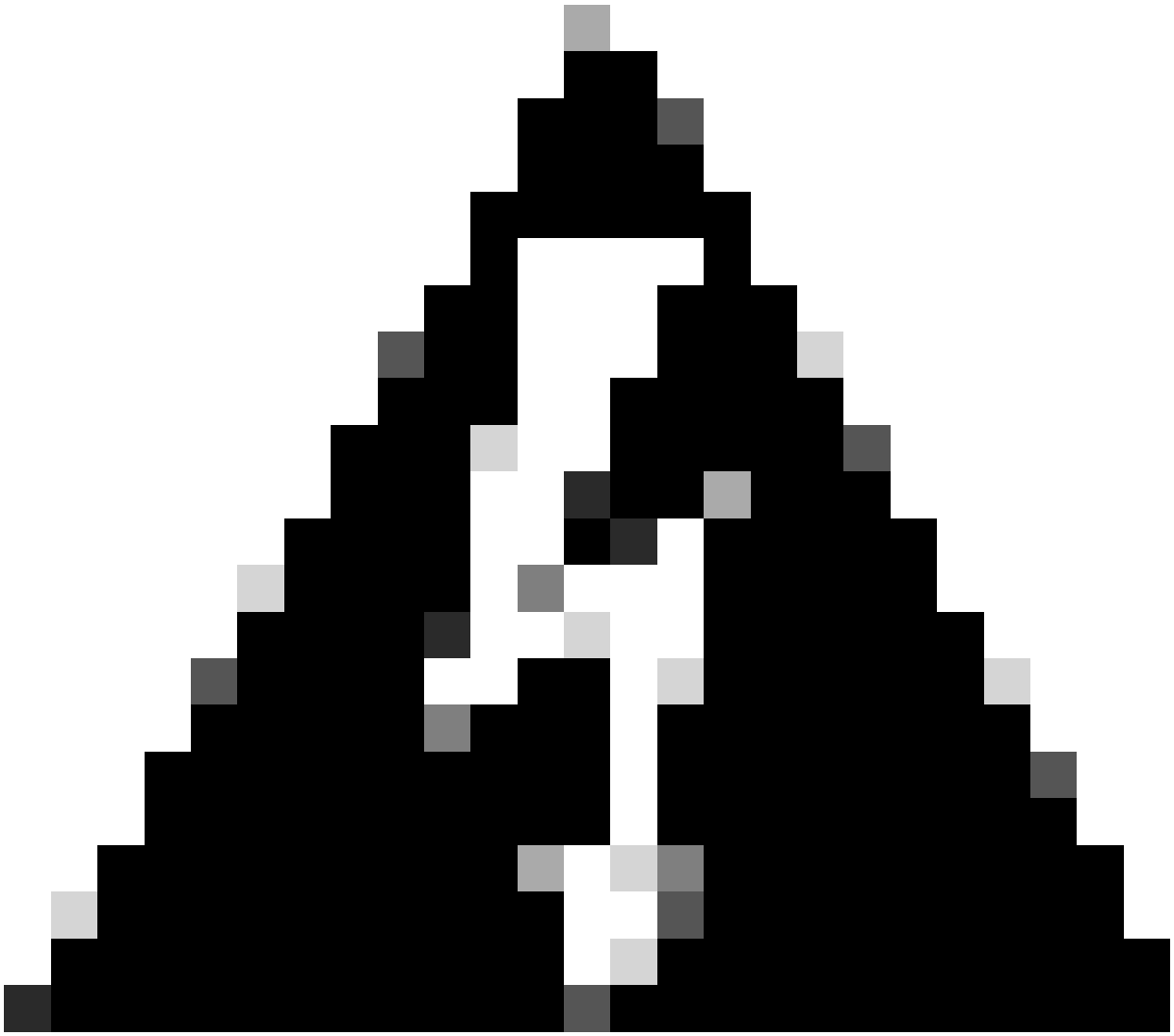
Nota: Los parámetros recomendados y óptimos se indican en negrita en los documentos de SSE: https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

Defina el anillo de claves IKEv2 que define la dirección IP de cabecera y la clave precompartida utilizada para autenticarse con la cabecera 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 un par de perfiles IKEv2.
Definen qué tipo de identidad IKE se debe utilizar para hacer coincidir el par remoto y qué

identidad IKE está enviando el router local al par.
La identidad IKE de la cabecera SSE es del tipo de dirección IP y es igual a la IP pública de la cabecera SSE.



Advertencia: Para establecer varios túneles con el mismo grupo de túnel de red en el lado SSE, todos deben utilizar la misma identidad IKE local.
Cisco IOS XE no admite este escenario, ya que requiere un par único de identidades IKE locales y remotas por túnel.
Para superar esta limitación, la cabecera SSE se ha mejorado para aceptar la ID de IKE con el formato: <tunneld_id>+<sufix>@<org><hub>.sse.cisco.com

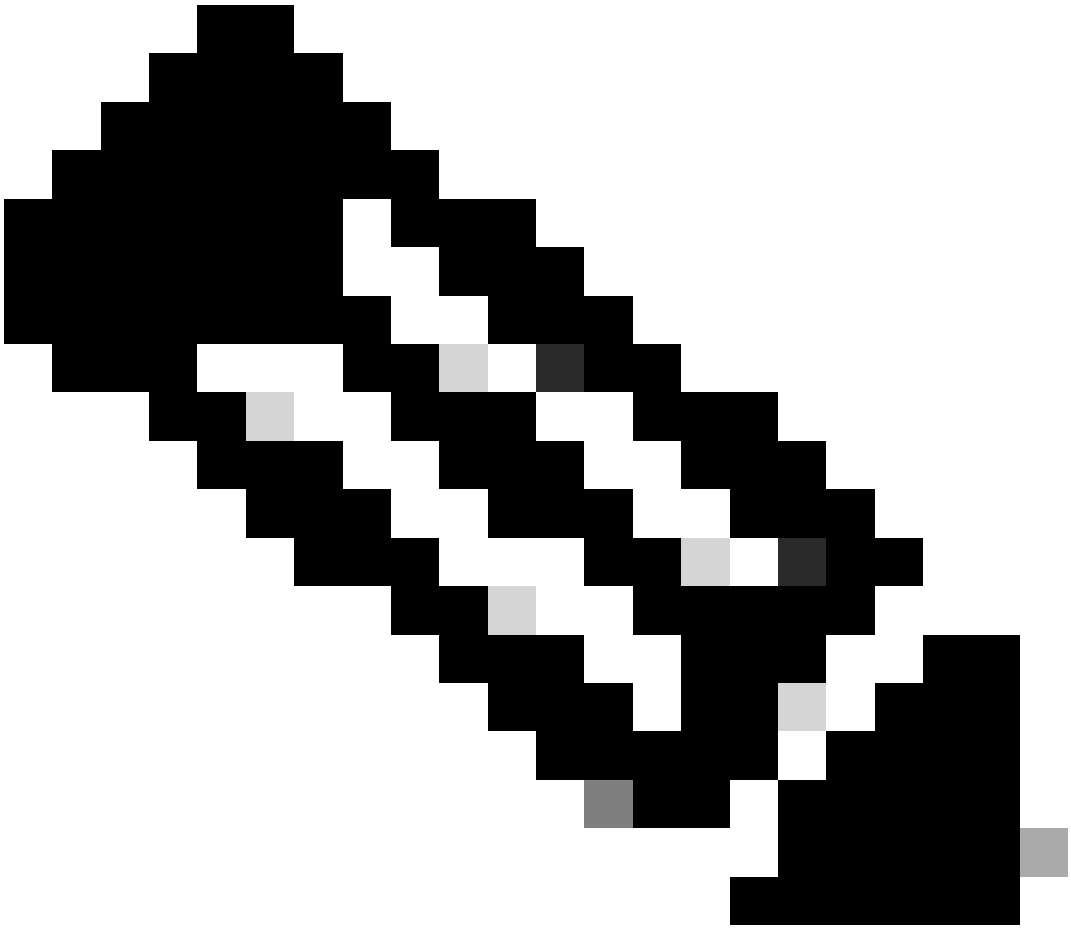
---

En el escenario de laboratorio analizado, el ID de túnel fue definido como cat8k-dmz.
En el escenario normal, configuraríamos el router para enviar la identidad IKE local como cat8k-dmz@8195165-622405748-sse.cisco.com

Sin embargo, para establecer varios túneles con el mismo grupo de túnel de red, se utilizarán ID de IKE locales:

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

Observe el sufijo agregado a cada cadena (tunnel1 y tunnel2)



> Nota: las identidades IKE locales mencionadas son solo un ejemplo que se utiliza en este escenario de laboratorio. Puede definir cualquier sufijo que desee, solo asegúrese de cumplir con los 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
```

Configuración del conjunto de transformación IPSec. Esta configuración define los algoritmos utilizados para la Asociación de seguridad IPsec (fase 2):

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

Configure los perfiles IPSec que enlazan perfiles IKEv2 con conjuntos de transformación:

```
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 sección trata sobre la configuración de las interfaces de túnel virtual y las interfaces de loopback utilizadas como origen del túnel.

En la situación de laboratorio descrita, necesitamos establecer dos interfaces VTI con el mismo par utilizando la misma dirección IP pública. Además, nuestro dispositivo Cisco IOS XE solo tiene una interfaz de salida GigabitEthernet1.

Cisco IOS XE no admite la configuración de más de un VTI con el mismo origen y destino de túnel.

Para superar esta limitación, puede utilizar las interfaces de loopback y definirlas como origen de túnel en la VTI respectiva.

Existen pocas opciones para lograr la conectividad IP entre el loopback y la dirección IP pública SSE:

1. Asignar dirección IP públicamente enrutable a interfaz de bucle invertido (requiere la propiedad de espacio de dirección IP pública)

2. Asigne una dirección IP privada a la interfaz de bucle invertido y al tráfico NAT dinámico mediante el origen IP de bucle invertido.
3. Usar interfaces VASI (no admitidas en muchas plataformas, engorroso de configurar y solucionar problemas)

En este escenario, vamos a discutir la segunda opción.

Configure dos interfaces de loopback y agregue el comando "ip nat inside" debajo de cada una de ellas.

```
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
```

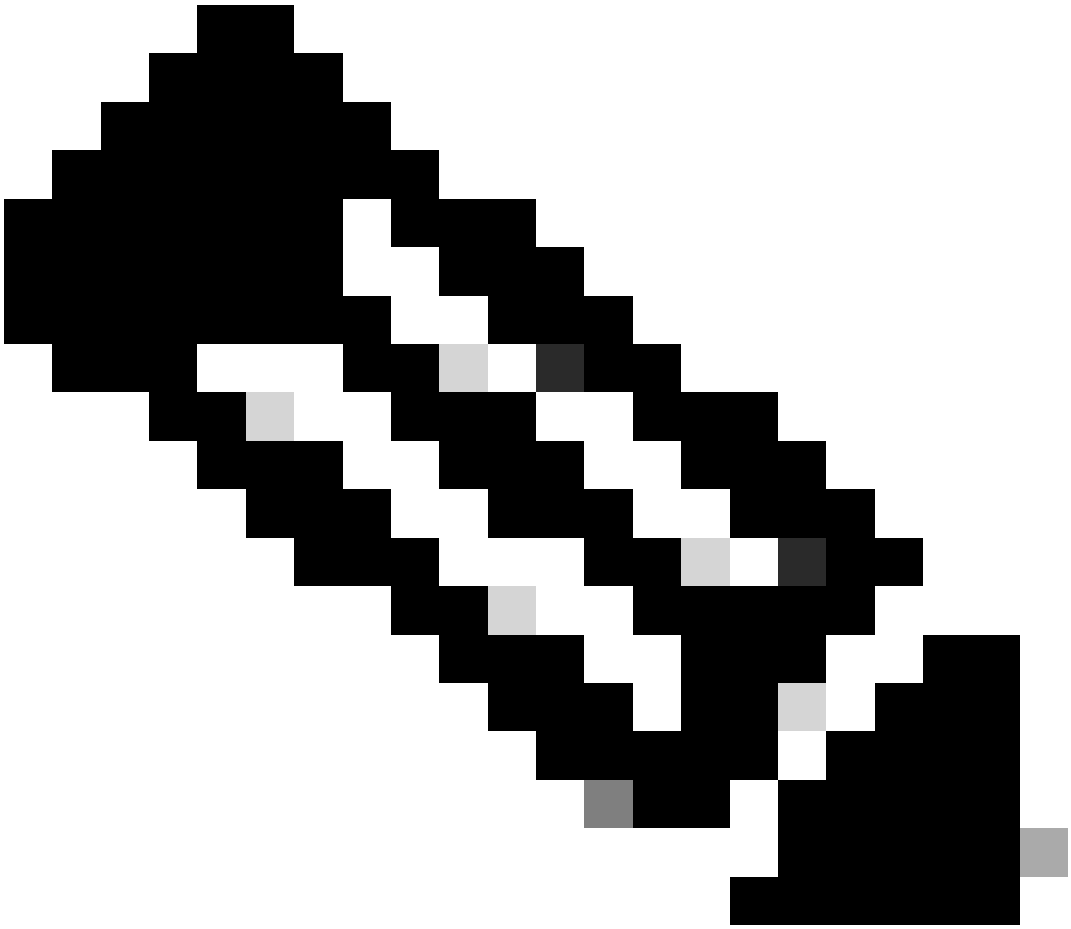
Defina la lista de control de acceso NAT dinámica y la sentencia de sobrecarga NAT:

```
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
```

Configuración de 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
```



> Nota: En el escenario de laboratorio descrito, las direcciones IP asignadas a las VTI provienen de subredes no superpuestas de 169.254.0.0/24.
> Puede utilizar otro espacio de subred, pero hay ciertos requisitos relacionados con BGP que requieren dicho espacio de dirección.

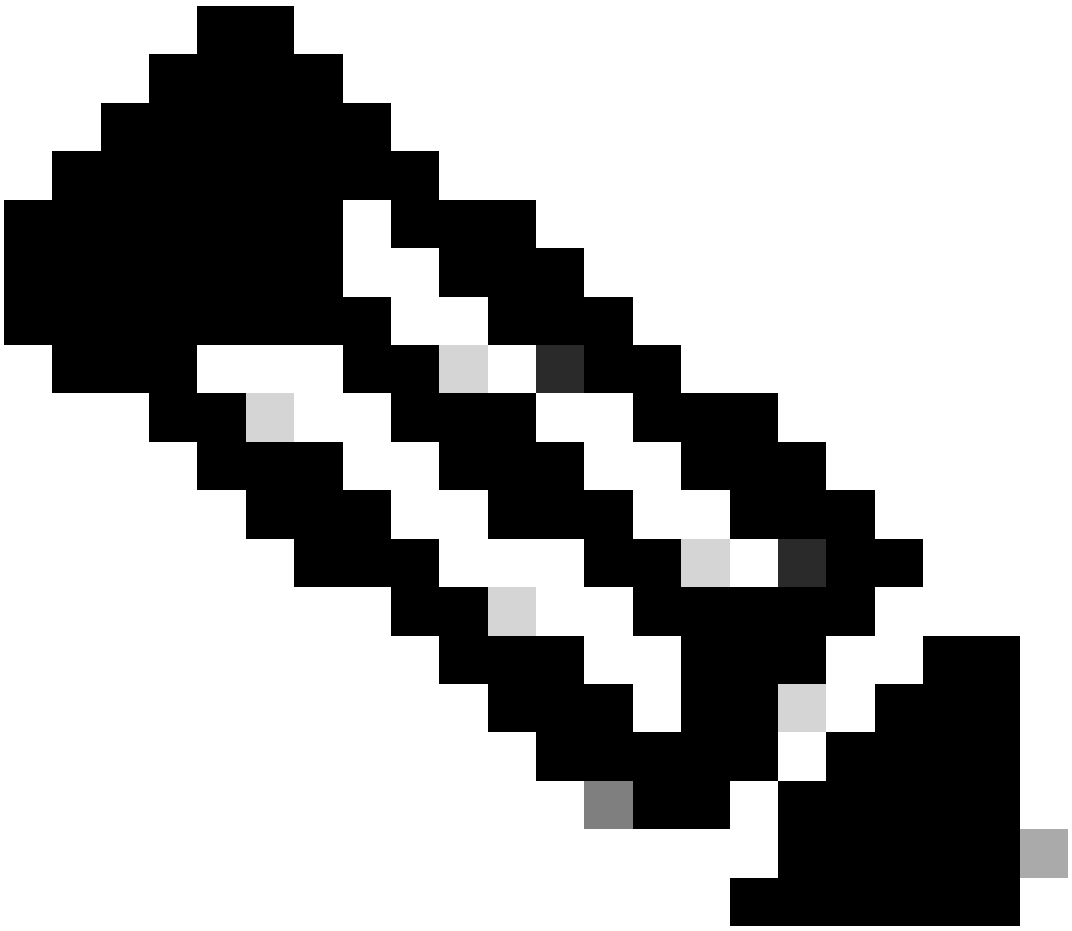
Routing BGP

Esta sección cubre la parte de configuración necesaria para establecer la vecindad BGP con la cabecera SSE.
El proceso BGP en la cabecera SSE escucha en cualquier IP desde la subred 169.254.0.0/24.
Para establecer el peering BGP sobre ambos VTI, vamos a definir dos vecinos 169.254.0.9 (Túnel 1) y 169.254.0.13 (Túnel 2).
Además, debe especificar el AS remoto de acuerdo con el valor visto en el panel 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



Nota: Las rutas recibidas de ambos peers deben ser exactamente iguales. De forma

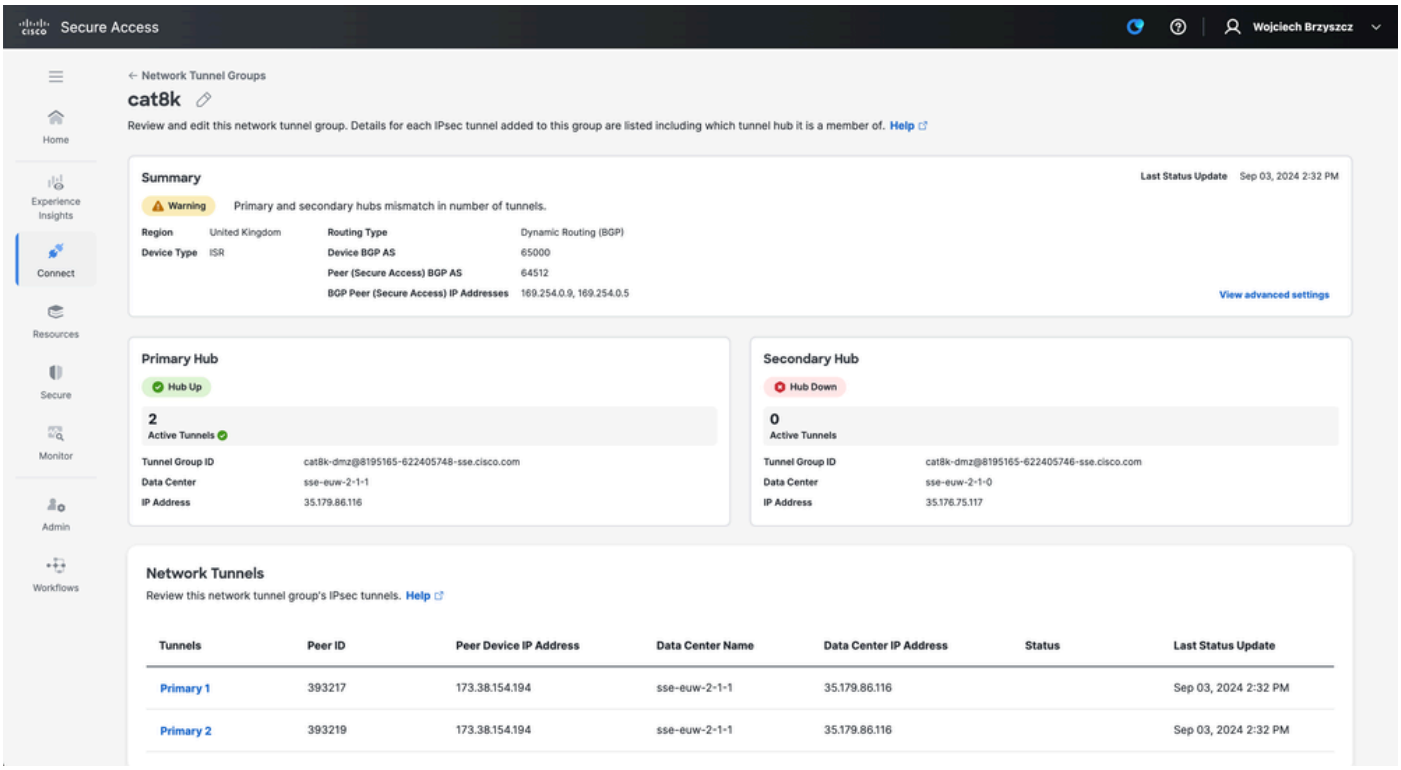
---

predeterminada, el router instala sólo uno de ellos en la tabla de ruteo.
Para permitir que se instale más de una ruta duplicada en la tabla de ruteo (y habilitar ECMP), debe configurar "maximum-paths <number of routes>"

Verificación

Panel de acceso seguro

Debe ver dos túneles primarios en el panel SSE:



Router Cisco IOS XE

Verifique que ambos túneles estén en estado READY desde el lado 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
```

Verifique que la vecindad BGP esté ACTIVA con ambos 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 que el router aprenda las rutas adecuadas de BGP (y que haya al menos dos saltos siguientes instalados en la tabla de ruteo).

<#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 el tráfico y verifique que ambos túneles se utilizan y verá que los contadores de encapsulamiento y desencapsulamiento aumentan 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, puede recopilar la captura de paquetes en ambas interfaces VTI para asegurarse de que el tráfico tenga una carga equilibrada entre las VTI. Lea las instrucciones de este artículo para configurar la captura de paquetes integrada en el dispositivo Cisco IOS XE.
En el ejemplo, el host detrás del router Cisco IOS XE con IP de origen 192.168.150.1 estaba enviando solicitudes ICMP a varias IP desde la subred 192.168.200.0/24.

Como puede ver, las solicitudes ICMP tienen la misma carga equilibrada entre los túneles.

<#root>

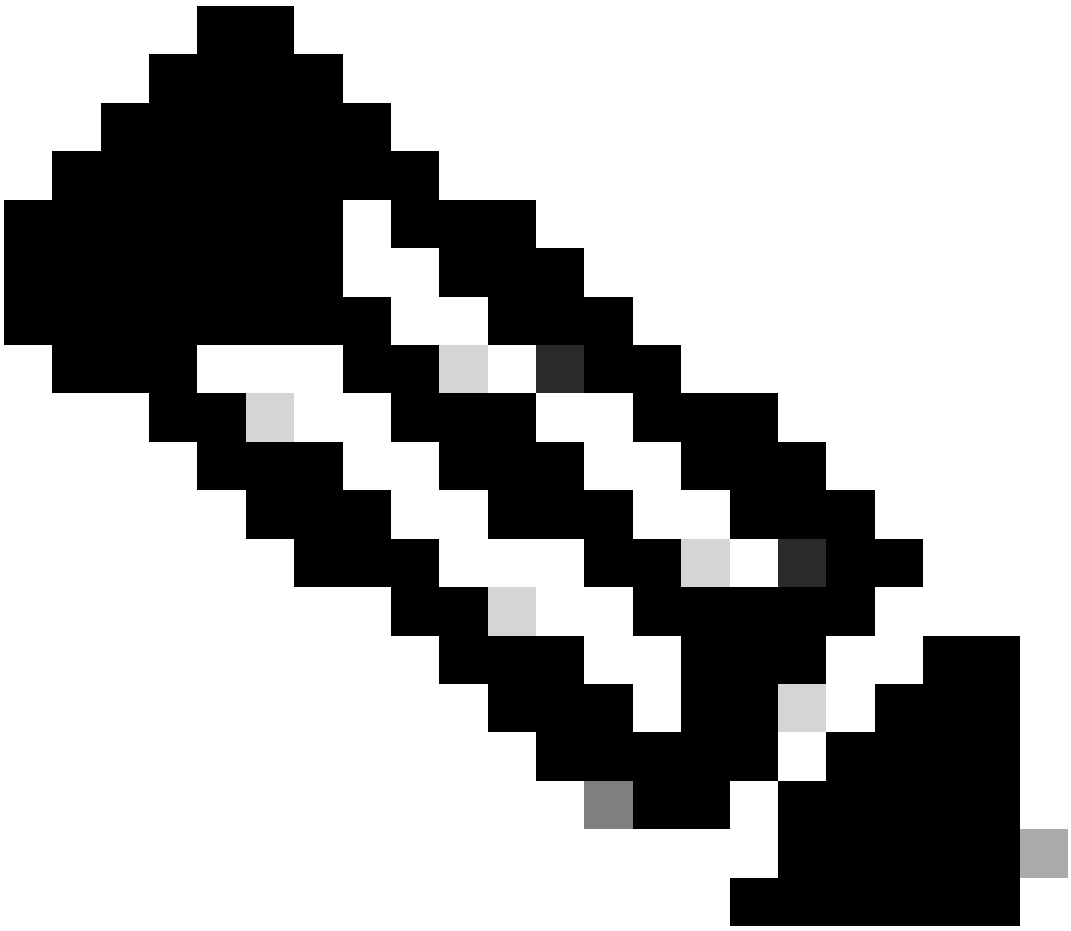
```
wbrzyszc-cat8k#
```

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
```



Nota: Hay varios mecanismos de balanceo de carga ECMP en los routers Cisco IOS XE. De forma predeterminada, el balanceo de carga por destino está habilitado, lo que garantiza que el tráfico a la misma IP de destino siempre tome la misma trayectoria. Puede configurar el balanceo de carga por paquete, que equilibraría aleatoriamente la carga del tráfico incluso para la misma IP de destino.

Información Relacionada

- Guía del usuario de Secure Access
- Cómo recopilar la captura de paquetes integrada
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).