ECMP와 BGP를 사용하여 Cisco Secure Access와 IOS XE Router 간의 네트워크 터널 구성

목차

소개

네트워크 다이어그램

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

구성

- 보안 액세스 컨피그레이션
- Cisco IOS XE 컨피그레이션
  - IKEv2 및 IPsec 매개변수
  - 가상 터널 인터페이스
  - BGP 라우팅

다음을 확인합니다.

- 보안 액세스 대시보드
- Cisco IOS XE 라우터

관련 정보

소개

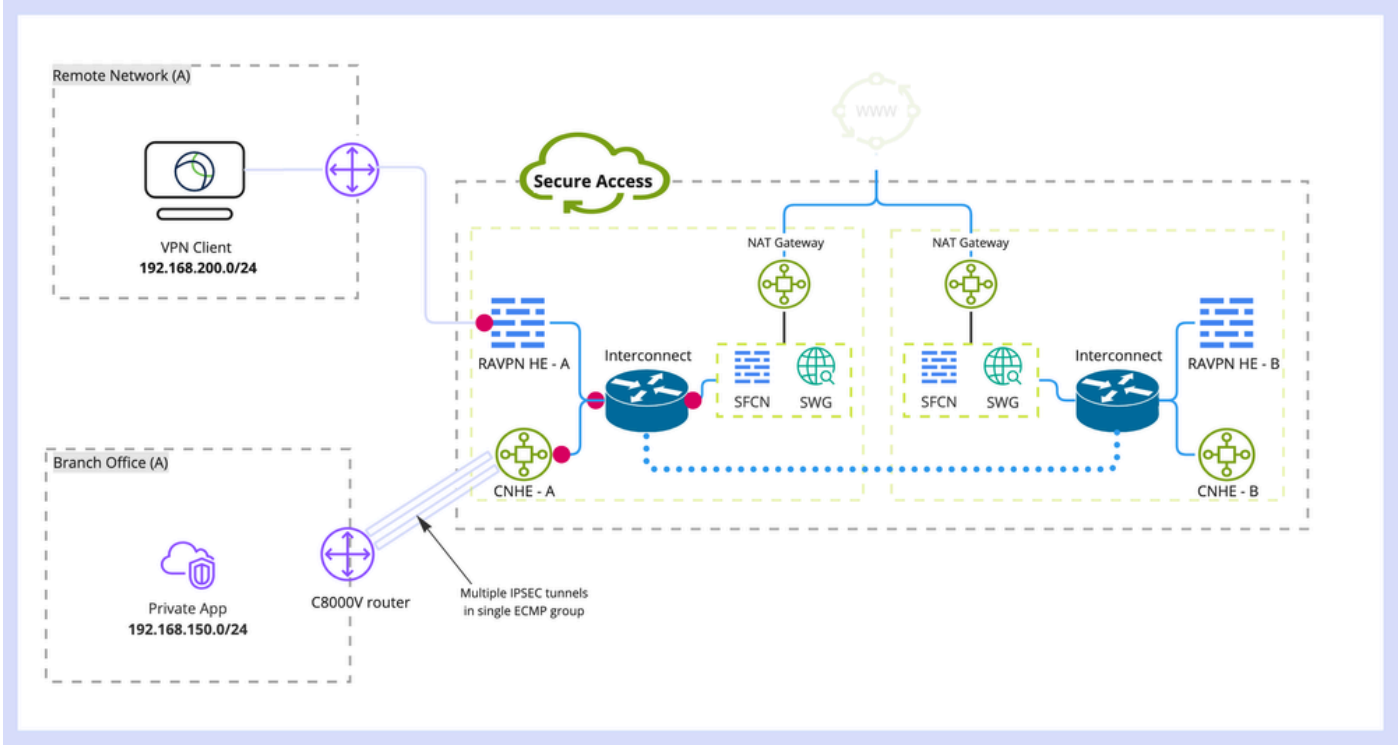
이 문서에서는 BGP 및 ECMP를 사용하여 Cisco Secure Access와 Cisco IOS XE 간의 IPSec VPN 터널을 구성하고 문제를 해결하는 데 필요한 단계를 설명합니다.

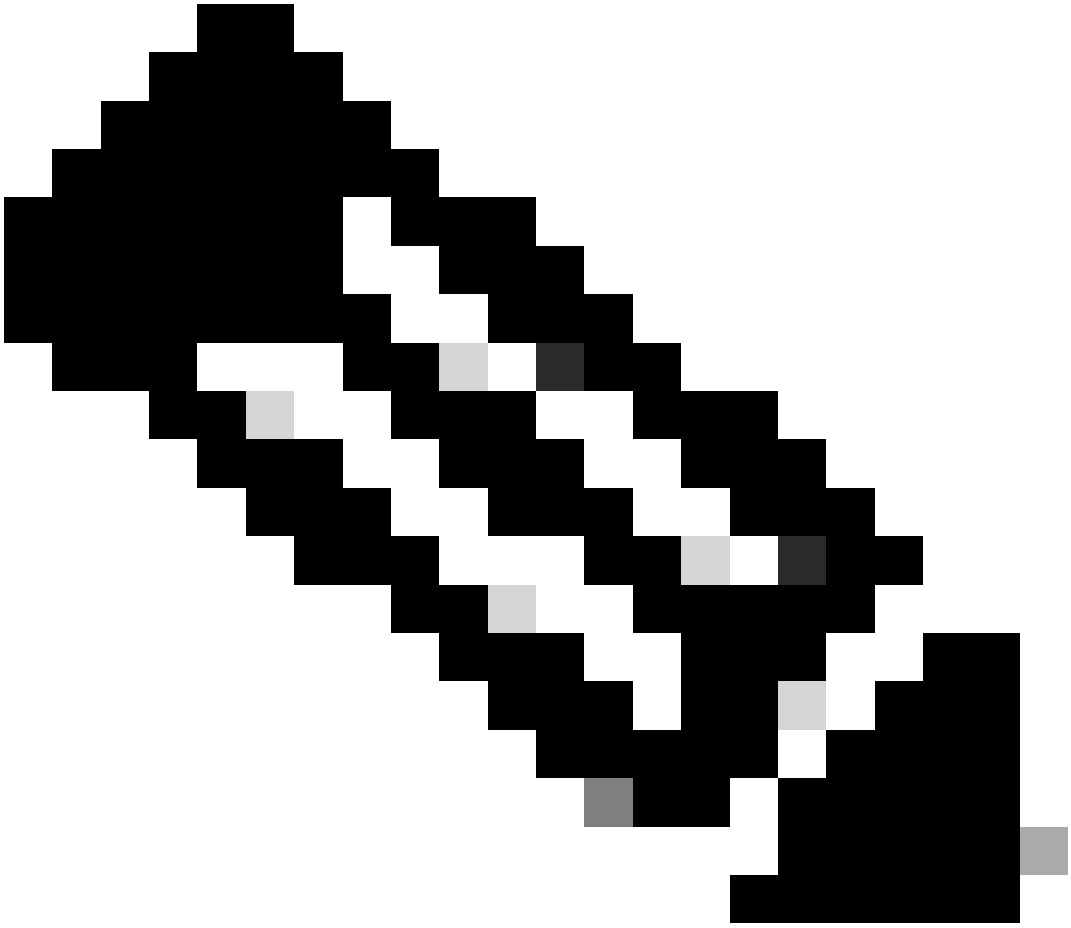
네트워크 다이어그램

이 실습에서는 네트워크 192.168.150.0/24 이 Cisco IOS XE 디바이스 뒤의 LAN 세그먼트이고, 192.168.200.0/24 이 Secure Access 헤드엔드에 연결하는 RAVPN 사용자가 사용하는 IP 풀인 시나리오에 대해 설명하겠습니다.

Cisco의 최종 목표는 Cisco IOS XE 디바이스와 Secure Access 헤드엔드 간의 VPN 터널에서 ECMP를 활용하는 것입니다.

토폴로지를 더 잘 이해하려면 다음 다이어그램을 참조하십시오.


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



참고: 이는 패킷 흐름의 예입니다. 다른 모든 흐름에 동일한 원칙을 적용하고 Cisco IOS XE 라우터를 지원하는 192.168.150.0/24 서브넷에서 인터넷 액세스를 보호할 수 있습니다.

사전 요구 사항

요구 사항

다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco IOS XE CLI 구성 및 관리
- IKEv2 및 IPSec 프로토콜에 대한 기본 지식
- 초기 Cisco IOS XE 컨피그레이션(IP 주소 지정, SSH, 라이센스)
- BGP 및 ECMP에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 17.9.4a 소프트웨어 버전을 실행하는 C8000V
- 윈도 PC
- Cisco Secure Access 조직

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Secure Access의 네트워크 터널은 단일 터널당 1Gbps의 대역폭 제한이 있습니다. 업스트림/다운스트림 인터넷 대역폭이 1Gbps보다 크고 이 대역폭을 충분히 활용하려는 경우, 동일한 Secure Access Data Center로 여러 터널을 구성하고 이를 단일 ECMP 그룹으로 그룹화하면 이러한 제한을 극복해야 합니다.

단일 네트워크 터널 그룹(단일 Secure Access DC 내)으로 여러 터널을 종료할 경우 Secure Access 헤드엔드 관점에서 기본적으로 ECMP 그룹에서 터널이 생성됩니다.
즉, Secure Access 헤드엔드가 온프레미스 VPN 디바이스로 트래픽을 전송하면 터널 간에 로드 밸런싱이 이루어집니다(BGP 피어에서 올바른 경로를 수신했다고 가정).

온프레미스 VPN 디바이스에서 동일한 기능을 사용하려면 단일 라우터에서 여러 VTI 인터페이스를 구성하고 적절한 라우팅 컨피그레이션이 적용되었는지 확인해야 합니다.

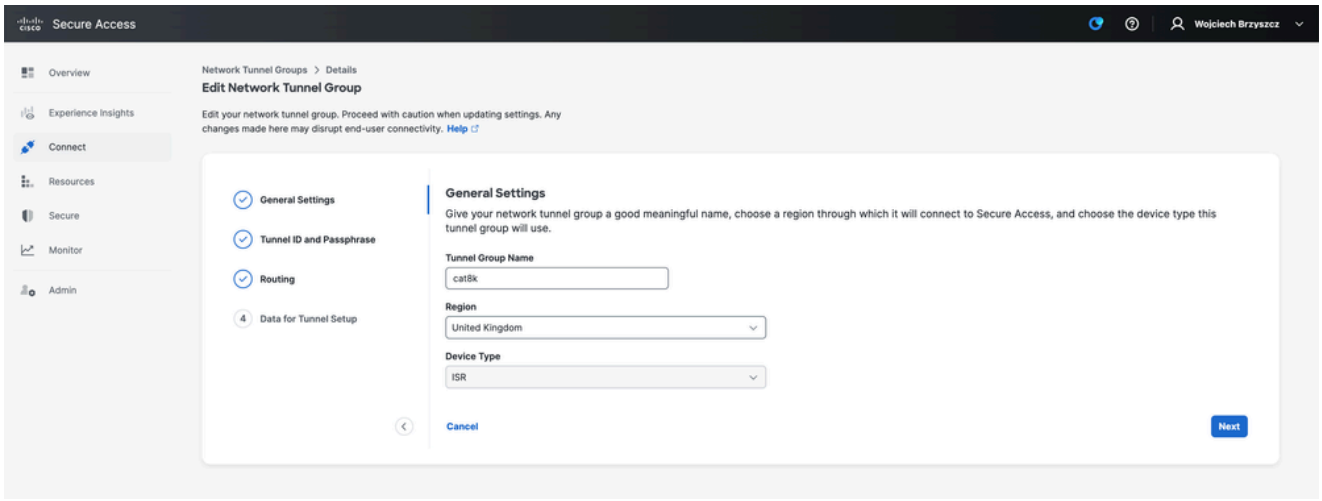
이 문서에서는 시나리오에 대해 설명하고 각 필수 단계에 대해 설명합니다.

구성

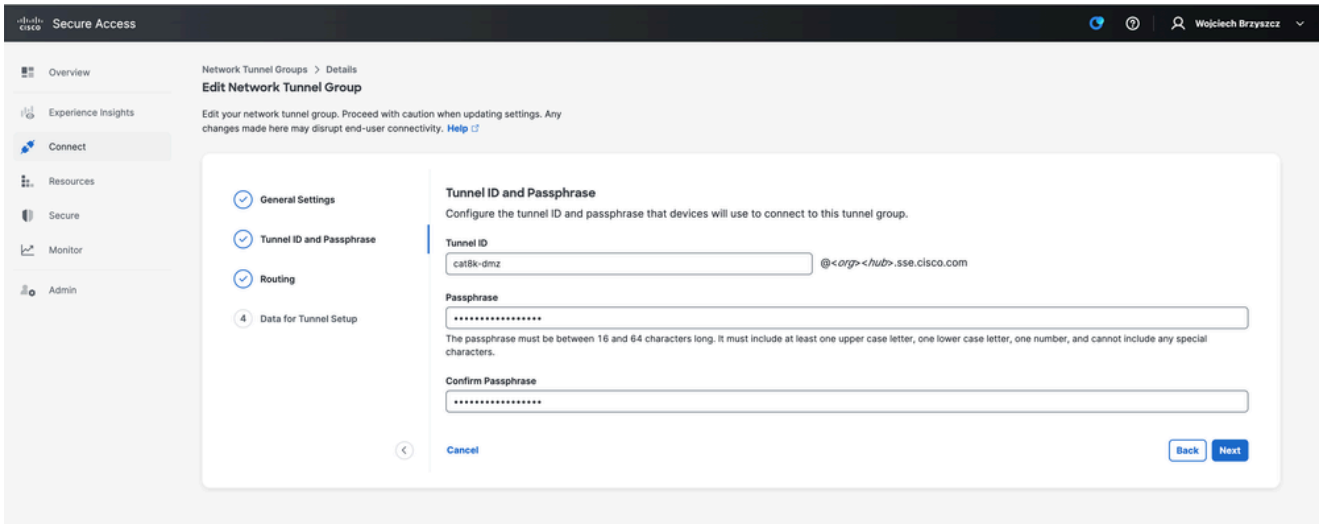
보안 액세스 컨피그레이션

BGP 프로토콜을 사용하여 여러 VPN 터널에서 ECMP 그룹을 형성하기 위해 보안 액세스 측에 적용해야 하는 특수 컨피그레이션은 없습니다.
네트워크 터널 그룹을 구성하는 데 필요한 단계입니다.

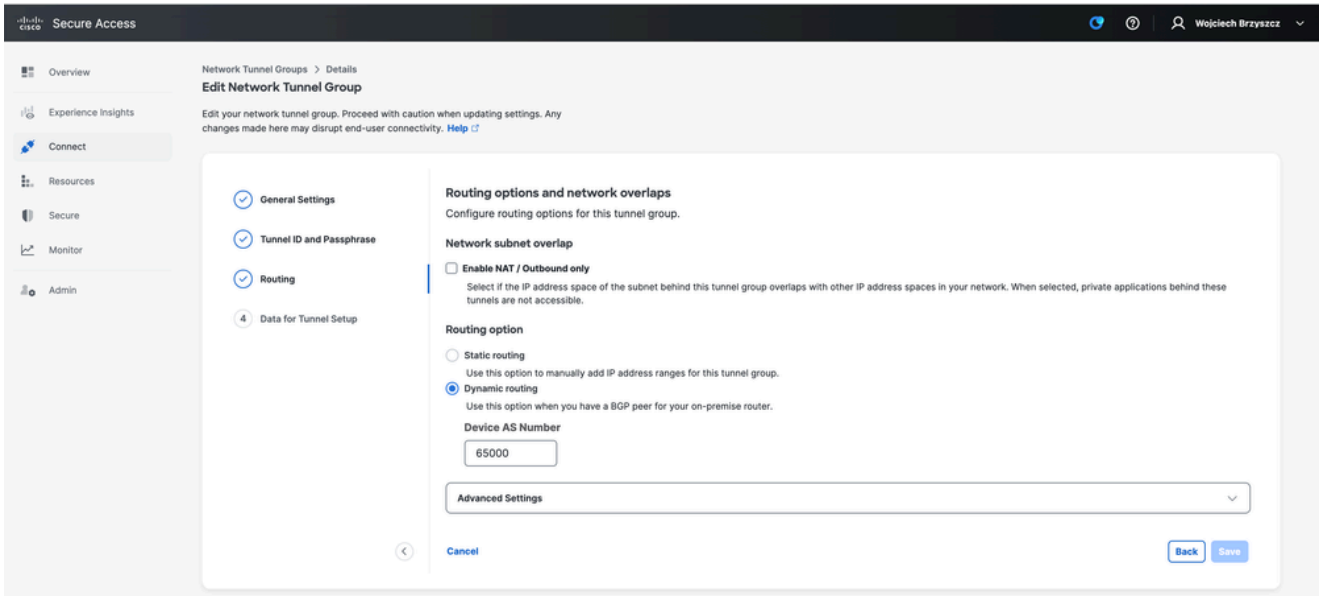
1. 새 네트워크 터널 그룹을 생성하거나 기존 터널 그룹을 수정합니다.



2. 터널 ID 및 암호 지정:



3. 라우팅 옵션을 구성하고 동적 라우팅을 지정하고 내부 AS 번호를 입력합니다. 이 Lab 시나리오에서는 ASN이 65000과 같습니다.



4. Data for Tunnel Setup(터널 설정을 위한 데이터) 섹션에서 터널 세부사항을 기록해 둡니다.

Cisco IOS XE 컨피그레이션

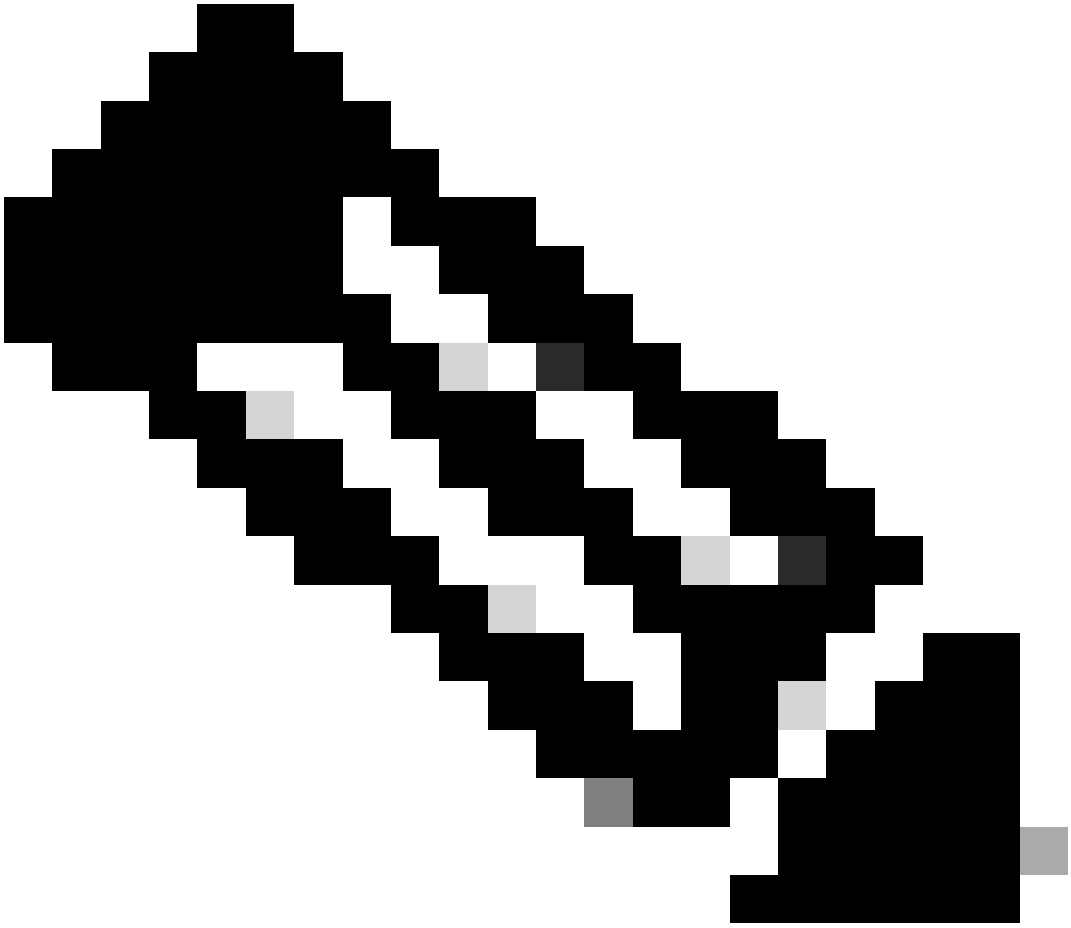
이 섹션에서는 가상 터널 인터페이스 전반에 걸쳐 IKEv2 터널, BGP 인접 관계 및 ECMP 로드 밸런싱을 올바르게 구성하기 위해 Cisco IOS XE 라우터에 적용해야 하는 CLI 컨피그레이션에 대해 설명합니다.
각 섹션에 대해 설명하고 대부분의 일반적인 주의 사항을 언급합니다.

IKEv2 및 IPsec 매개변수

IKEv2 정책 및 IKEv2 제안을 구성합니다. 이러한 매개변수는 IKE SA에 사용되는 알고리즘을 정의합니다(1단계).

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

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



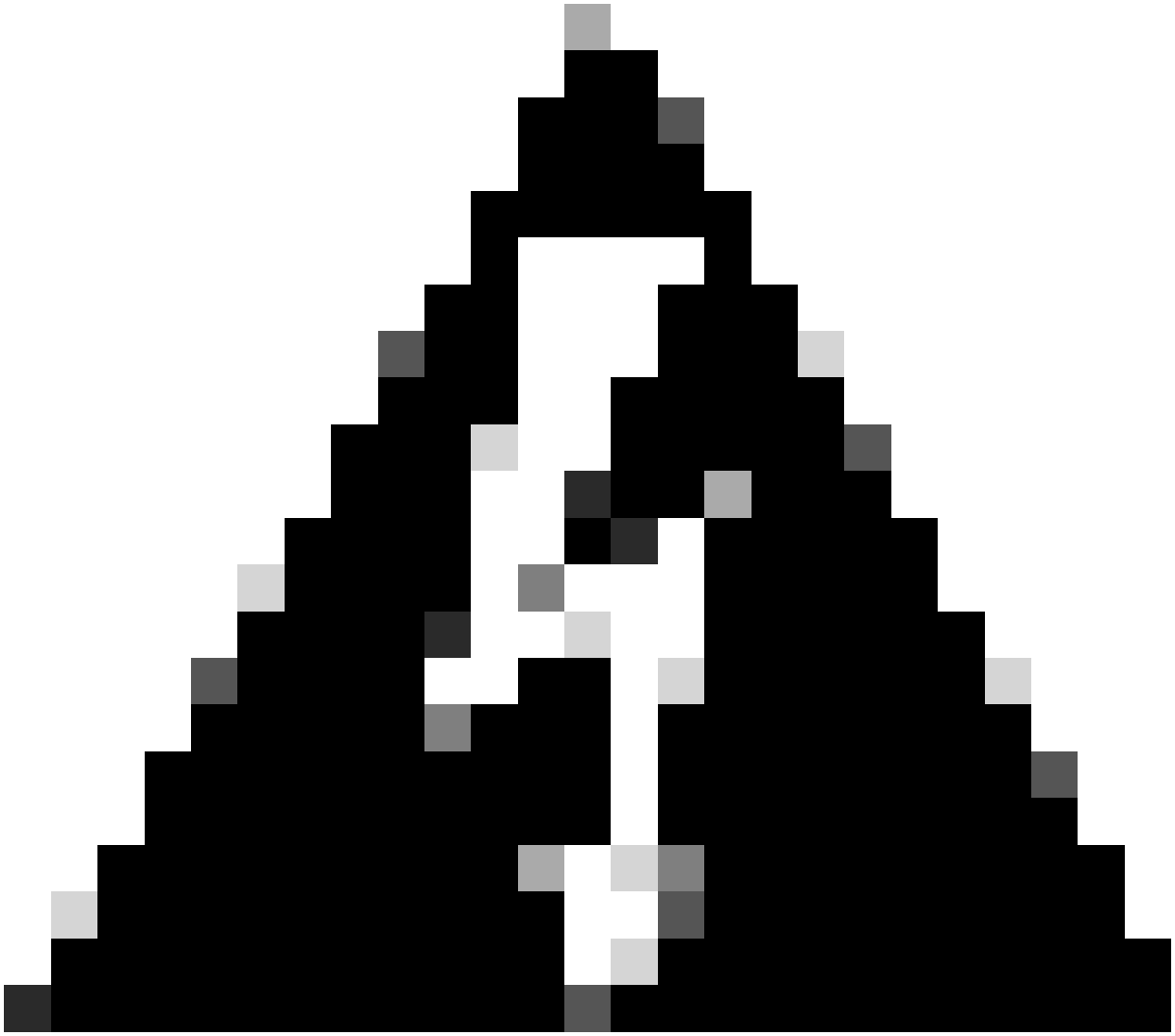
참고: SSE 문서에서 권장 및 최적 매개변수는 굵게 표시됩니다.
https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

SSE 헤드엔드로 인증하는 데 사용되는 헤드엔드 IP 주소 및 사전 공유 키를 정의하는 IKEv2 키링을 정의합니다.

```
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 프로파일 쌍을 구성합니다.
원격 피어와 일치시키는 데 어떤 유형의 IKE ID를 사용할지, 어떤 IKE ID 로컬 라우터가 피어로 전

송할지를 정의합니다.
SSE 헤드엔드의 IKE ID는 IP 주소 유형이며 SSE 헤드엔드의 공용 IP와 같습니다.



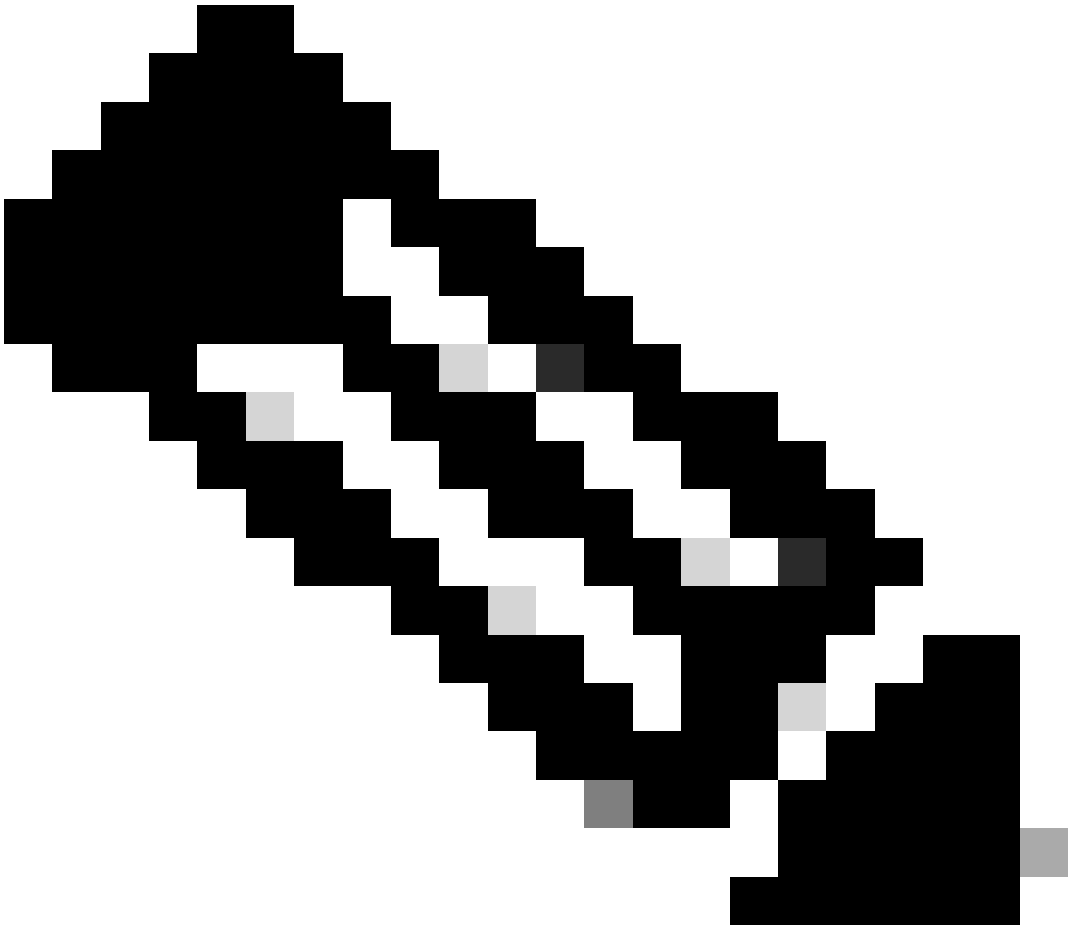
경고: SSE 측에서 동일한 네트워크 터널 그룹을 사용하여 여러 터널을 설정하려면 모든 터널이 동일한 로컬 IKE ID를 사용해야 합니다.
Cisco IOS XE는 터널당 고유한 로컬 및 원격 IKE ID 쌍이 필요하므로 이러한 시나리오를 지원하지 않습니다.
이러한 제한을 극복하기 위해 SSE 헤드엔드가 <tunneld_id>+<suffix>@<org><hub>.sse.cisco.com 형식의 IKE ID를 허용하도록 향상되었습니다.

논의된 실습 시나리오에서 터널 ID는 cat8k-dmz로 정의되었습니다.
일반적인 시나리오에서는 로컬 IKE ID를 cat8k-dmz@8195165-622405748-sse.cisco.com으로 전송하도록 라우터를 구성합니다

그러나 동일한 네트워크 터널 그룹으로 여러 터널을 설정하려면 로컬 IKE ID가 사용됩니다.

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

각 문자열(tunnel1 및 tunnel2)에 추가된 접미사를 확인합니다



참고: 언급된 로컬 IKE ID는 이 실습 시나리오에서 사용된 예시일 뿐입니다. 원하는 접미사를 정의할 수 있습니다. 요구 사항을 충족시키기만 하면 됩니다.

```
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 변형 집합을 구성합니다. 이 설정은 IPsec 보안 연결에 사용되는 알고리즘을 정의합니다(2단계).

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

IKEv2 프로필을 변형 집합과 연결하는 IPSec 프로필을 구성합니다.

```
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
```

가상 터널 인터페이스

이 섹션에서는 가상 터널 인터페이스 및 터널 소스로 사용되는 루프백 인터페이스의 컨피그레이션에 대해 설명합니다.

논의된 랩 시나리오에서는 동일한 공용 IP 주소를 사용하여 단일 피어와 2개의 VTI 인터페이스를 설정해야 합니다. 또한 Cisco IOS XE 디바이스에는 이그레스 인터페이스 GigabitEthernet1만 있습니다.

Cisco IOS XE는 터널 소스와 터널 대상이 동일한 둘 이상의 VTI 컨피그레이션을 지원하지 않습니다.

이러한 제한을 극복하기 위해 루프백 인터페이스를 사용하고 각 VTI에서 터널 소스로 정의할 수 있습니다.

루프백과 SSE 공용 IP 주소 간에 IP 연결을 구현하는 옵션은 거의 없습니다.

1. 루프백 인터페이스에 공개적으로 라우팅 가능한 IP 주소 할당(공용 IP 주소 공간에 대한 소유권 필요)
2. 루프백 인터페이스에 사설 IP 주소를 할당하고 루프백 IP 소스를 통해 동적으로 NAT 트래픽을 할당합니다.
3. VASI 인터페이스 사용(많은 플랫폼에서는 지원되지 않으며 설정 및 문제 해결이 번거롭습니

다.)

이 시나리오에서는 두 번째 옵션에 대해 설명합니다.

두 개의 루프백 인터페이스를 구성하고 각 인터페이스 아래에 "ip nat inside" 명령을 추가합니다.

```
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
```

동적 NAT Access-Control List 및 NAT 오버로드 명령문을 정의합니다.

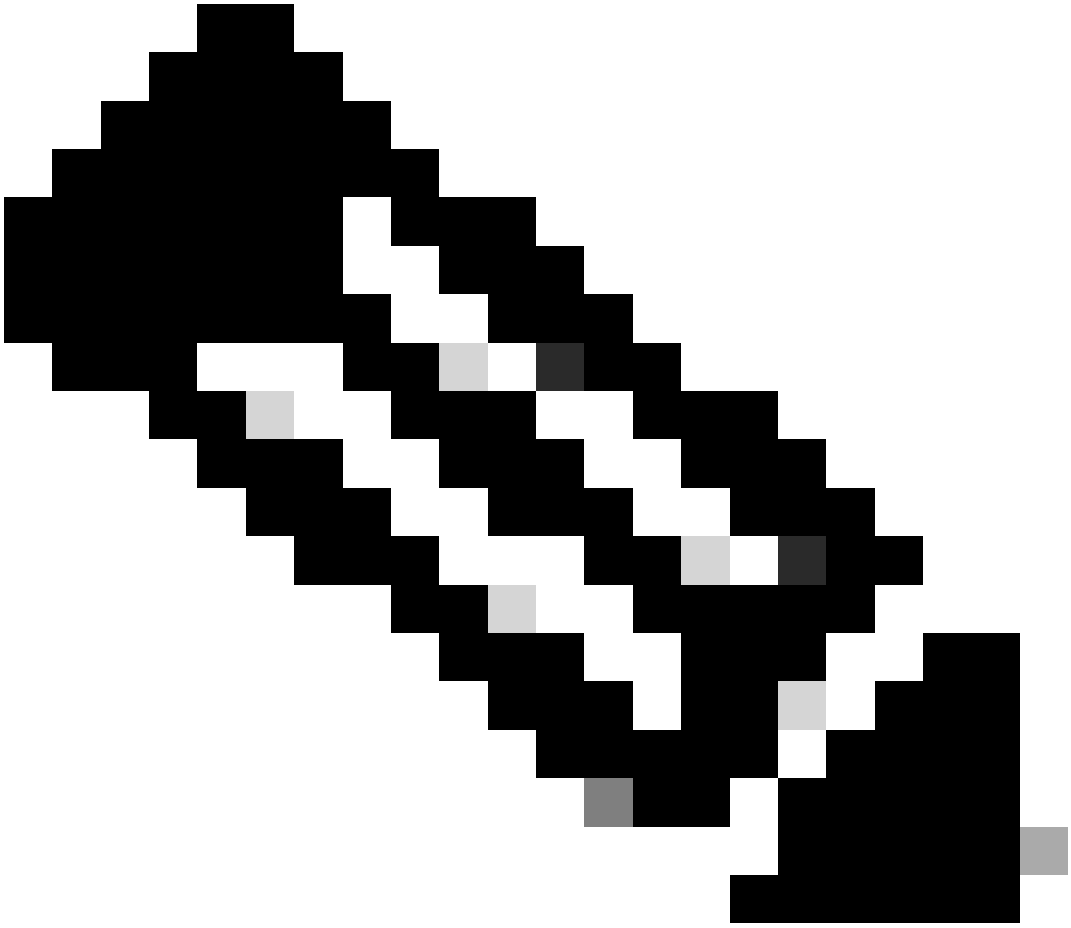
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

가상 터널 인터페이스를 구성합니다.

```
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
```



참고: 설명된 실습 시나리오에서 VTI에 할당된 IP 주소는 169.254.0.0/24의 겹치지 않는 서브넷에서 가져옵니다.
다른 서브넷 공간을 사용할 수 있지만 BGP와 관련하여 이러한 주소 공간이 필요한 특정 요구 사항이 있습니다.

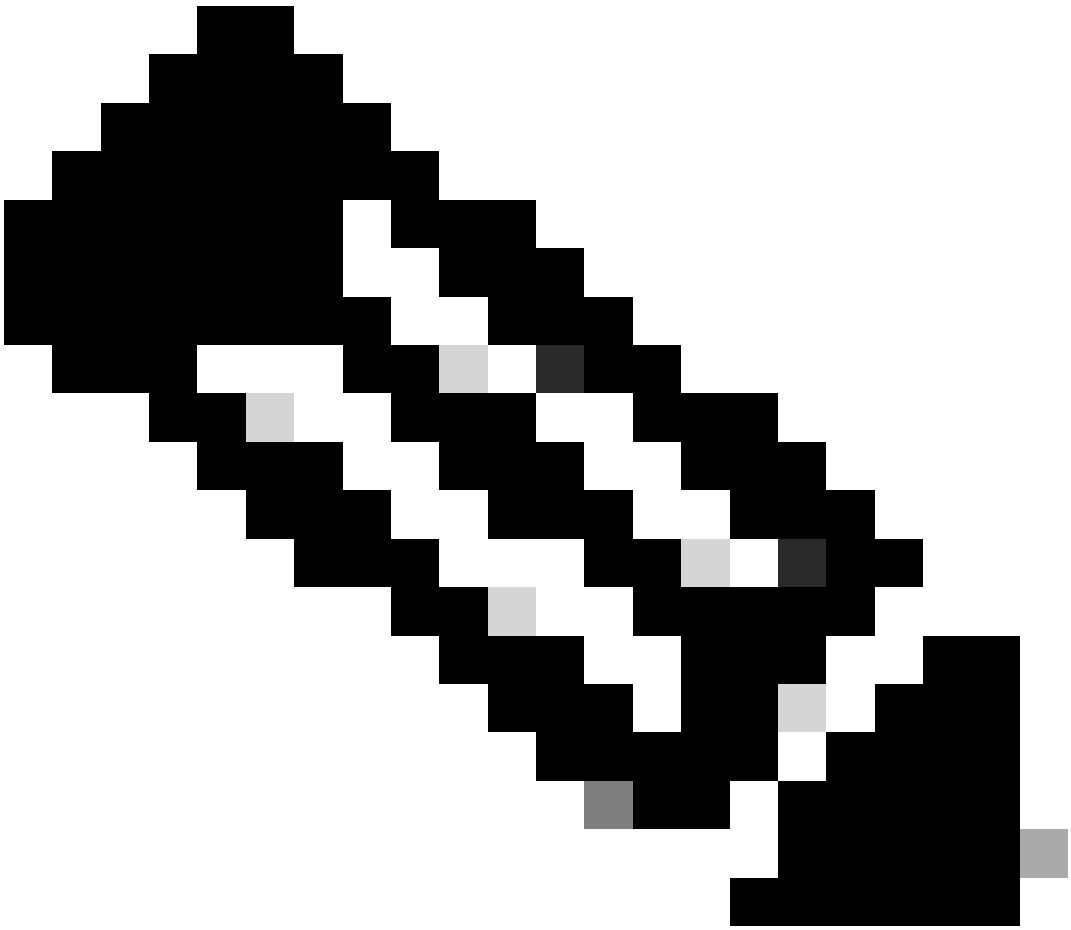
BGP 라우팅

이 섹션에서는 SSE 헤드엔드와 BGP 네이버십을 설정하는 데 필요한 컨피그레이션 부분을 다룹니다.
SSE 헤드엔드의 BGP 프로세스는 서브넷의 모든 IP에서 수신 대기 169.254.0.0/24 .
두 VTI를 통한 BGP 피어링을 설정하기 위해 두 인접 디바이스 169.254.0.9(Tunnel1)와 169.254.0.13(Tunnel2)을 정의합니다.
또한 SSE 대시보드에 표시된 값에 따라 Remote AS를 지정해야 합니다.

<#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

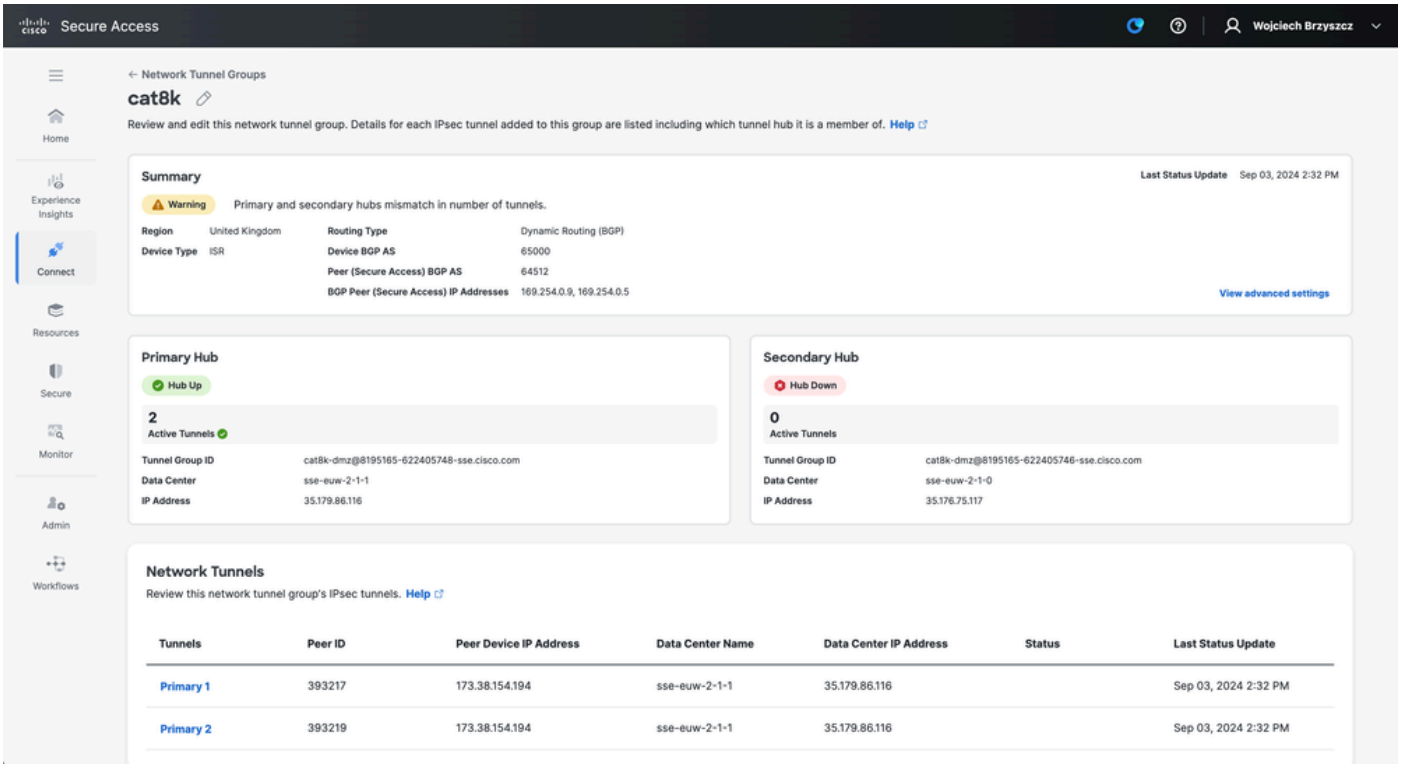


참고: 두 피어에서 수신한 경로는 정확히 동일해야 합니다. 기본적으로 라우터는 라우팅 테이블에 이 중 하나만 설치합니다.
라우팅 테이블에 두 개 이상의 중복 경로를 설치하고 ECMP를 활성화하려면 "maximum-paths <number of routes>"를 구성해야 합니다.

다음을 확인합니다.

보안 액세스 대시보드

SSE 대시보드에 두 개의 기본 터널이 표시되어야 합니다.



Cisco IOS XE 라우터

Cisco IOS XE 측에서 두 터널이 모두 READY 상태인지 확인합니다.

```
<#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 인접 디바이스가 두 피어와 모두 UP인지 확인합니다.

```
<#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
```

라우터가 BGP에서 적절한 경로를 학습하는지 확인합니다(라우팅 테이블에 다음 홉이 최소 2개 설치되어 있음).

```
<#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
```

트래픽을 시작하고 두 터널이 모두 사용되는지 확인합니다. 두 터널 모두에 대해 캡슐과 디캡이 증가하는 것을 확인할 수 있습니다.

<#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
```

선택적으로, 트래픽이 VTI 간에 로드 밸런싱되도록 두 VTI 인터페이스에서 패킷 캡처를 수집할 수 있습니다. Cisco IOS XE 디바이스에서 Embedded Packet Capture를 구성하려면 이 문서의 지침을 읽어보십시오.
이 예에서 소스 IP 192.168.150.1을 사용하는 CIsco IOS XE 라우터 뒤의 호스트는 192.168.200.0/24 서브넷에서 여러 IP에 ICMP 요청을 전송했습니다.

보시다시피 ICMP 요청은 터널 간에 동일하게 로드 밸런싱됩니다.

<#root>

```
wbrzyszc-cat8k#
```

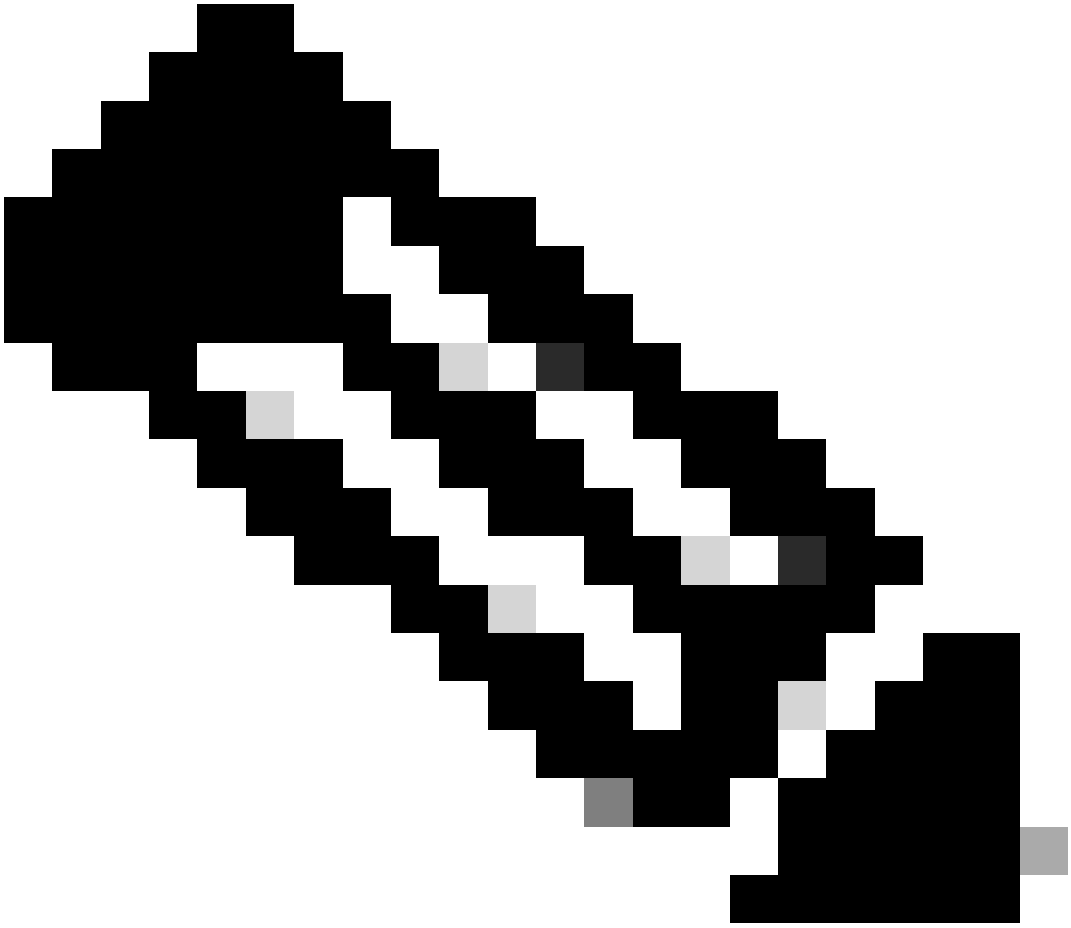
show monitor capture Tunnel1 buffer brief

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



참고: Cisco IOS XE 라우터에는 여러 ECMP 로드 밸런싱 메커니즘이 있습니다. 기본적으로 대상별 로드 밸런싱이 활성화되어 있으므로 동일한 대상 IP에 대한 트래픽은 항상 동일한 경로를 사용합니다.
동일한 목적지 IP에 대해서도 트래픽을 임의로 로드 밸런싱하는 패킷별 로드 밸런싱을 구성할 수 있습니다.

관련 정보

- Secure Access 사용 설명서
- 임베디드 패킷 캡처를 수집하는 방법
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.