

使用帶BGP的ECMP配置Cisco安全訪問和IOS XE路由器之間的網路隧道

目錄

[簡介](#)

[網路圖表](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[安全訪問配置](#)

[Cisco IOS XE配置](#)

[IKEv2和IPsec引數](#)

[虛擬通道介面](#)

[BGP路由](#)

[驗證](#)

[安全訪問控制台](#)

[Cisco IOS XE路由器](#)

[相關資訊](#)

簡介

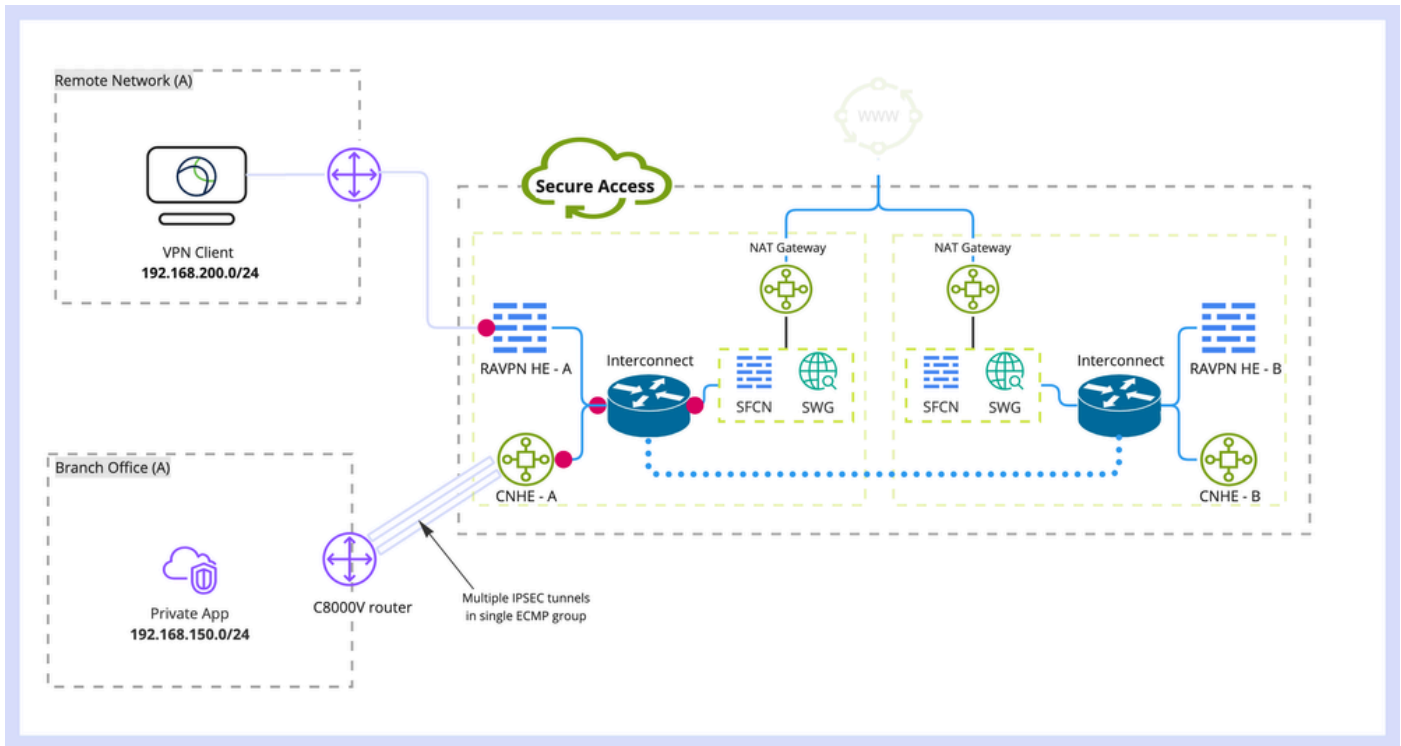
本文檔介紹使用BGP和ECMP配置思科安全訪問和思科IOS XE之間的IPSec VPN隧道並排除其故障所需的步驟。

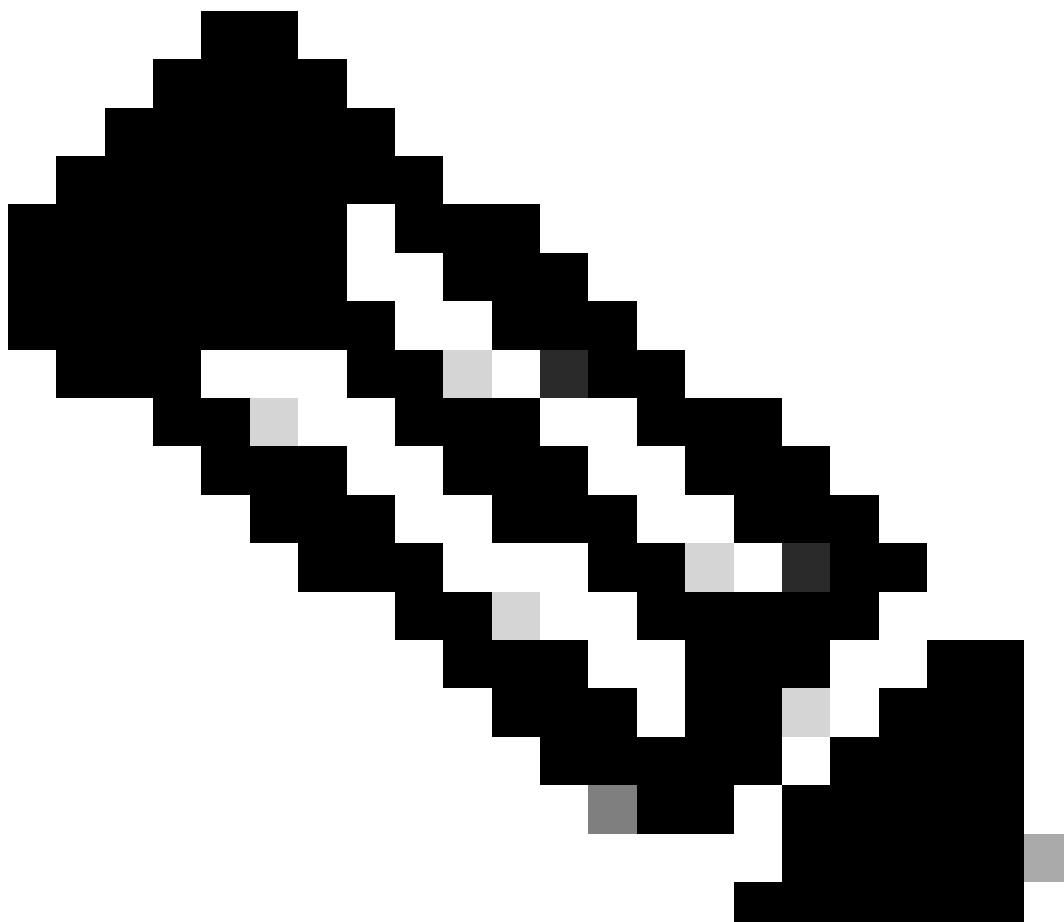
網路圖表

在本實驗示例中，我們將討論以下場景：網路192.168.150.0/24 是Cisco IOS XE裝置後的LAN網段，192.168.200.0/24 是連線到安全訪問前端的RAVPN使用者使用的IP池。

我們的最終目標是在Cisco IOS XE裝置與安全訪問前端之間的VPN隧道上使用ECMP。

為了更好地瞭解拓撲，請參閱圖：





注意：這只是一個資料包流示例，您可以對任何其他資料流和Cisco IOS XE路由器後的192.168.150.0/24子網的安全網際網路訪問應用相同的原則。

必要條件

需求

建議您瞭解以下主題：

- Cisco IOS XE CLI組態和管理
- IKEv2和IPSec協定的基本知識
- 初始Cisco IOS XE配置（IP定址、SSH、許可證）
- BGP和ECMP的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行17.9.4a軟體版本的C8000V
- Windows電腦
- 思科安全訪問組織

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

安全訪問中的網路隧道的頻寬限制為每條隧道1Gbps。如果您的上游/下游Internet頻寬高於1Gbps，並且您想充分利用它，則需要透過為同一安全訪問資料中心配置多個隧道，並將它們分組到單個ECMP組中來克服此限制。

當您使用單個網路隧道組（在單個安全接入DC內）終止多個隧道時，預設情況下從安全接入頭端角度它們形成ECMP組。

這意味著，一旦安全訪問頭端向本地VPN裝置傳送流量，它就會在隧道之間實現負載均衡（假設從BGP對等體收到正確的路由）。

為了在內部部署VPN裝置上實現相同的功能，您需要在一個路由器上配置多個VTI介面，並確保應用正確的路由配置。

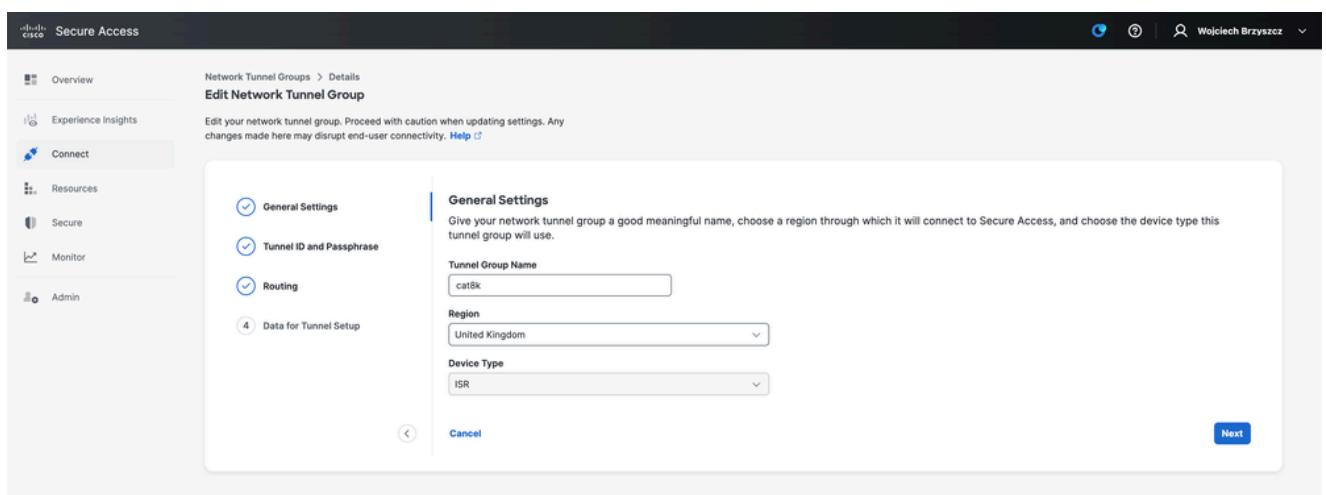
本文介紹場景，以及每個必要步驟的說明。

設定

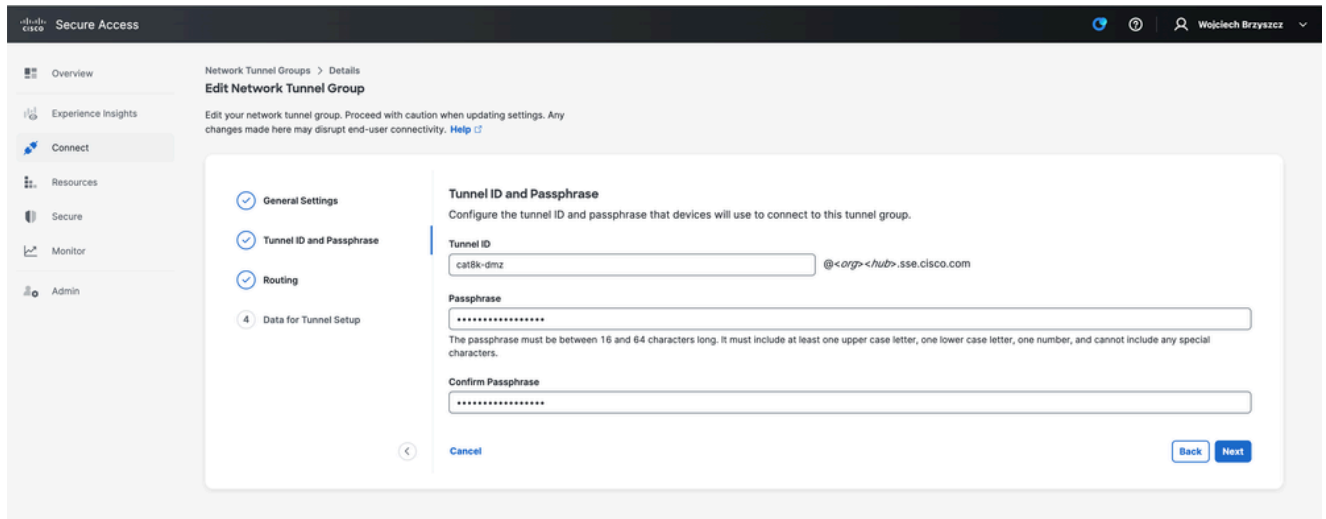
安全訪問配置

無需在安全訪問端應用特殊配置，即可使用BGP協定從多個VPN隧道形成ECMP組。配置網路隧道組所需的步驟。

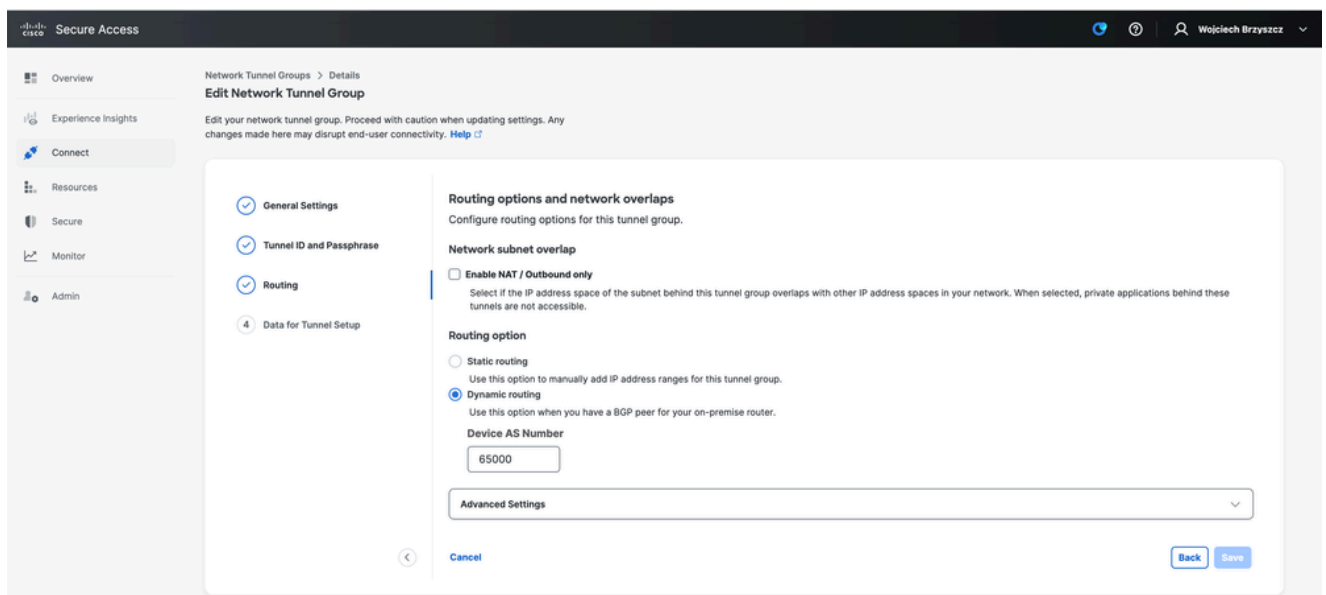
1. 建立新的網路隧道組（或編輯現有隧道組）。



2. 指定隧道ID和複雜密碼：



3. 配置Routing選項，指定Dynamic Routing，並輸入您的內部AS編號。在本實驗中，ASN等於65000。



4. 從Data for Tunnel Setup部分記下隧道詳細資訊。

Cisco IOS XE配置

本節介紹需要在Cisco IOS XE路由器上應用的CLI配置，以便正確配置跨虛擬隧道介面的IKEv2隧道、BGP鄰居關係和ECMP負載均衡。

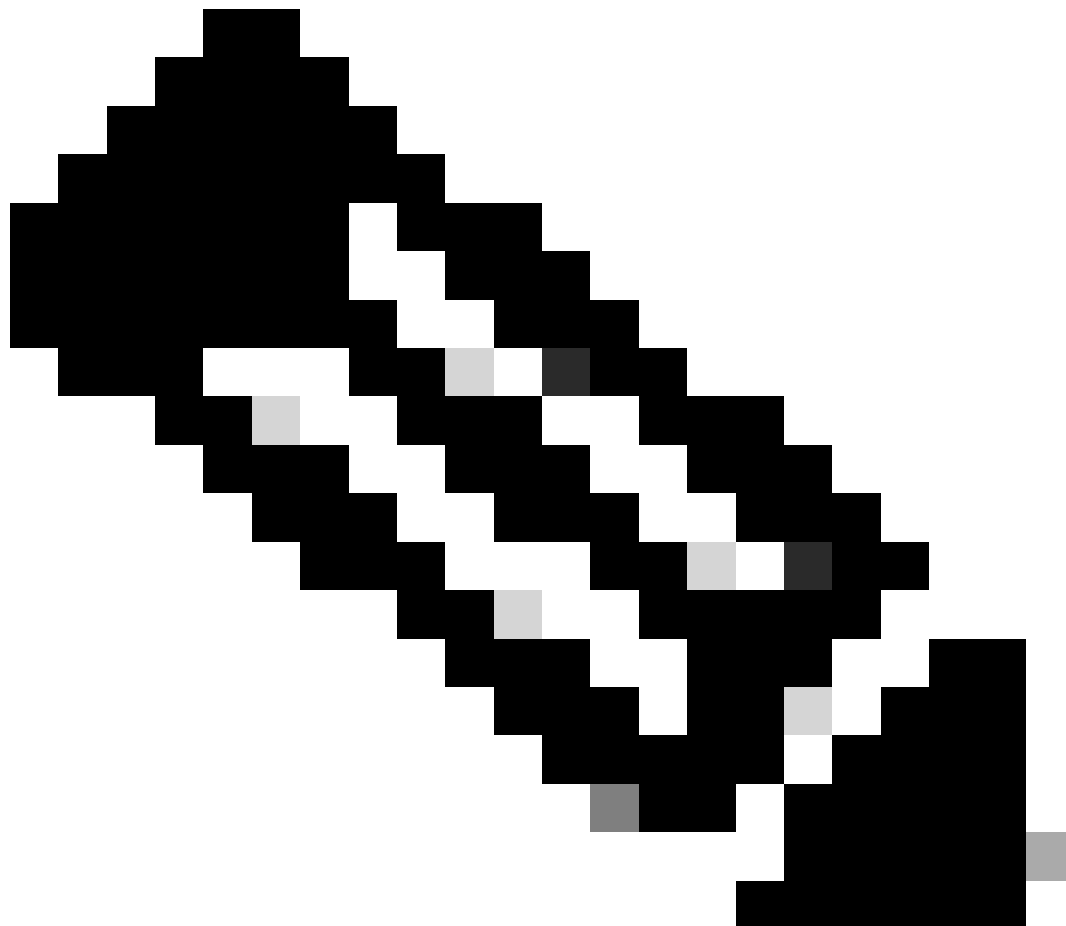
每個部分都有說明，並且還提到了最常見的警告。

IKEv2和IPsec引數

配置IKEv2策略和IKEv2提議。這些引數定義用於IKE SA的演算法（第1階段）：

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

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



註：SSE文檔中的建議引數和最佳引數以粗體標示：<https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters>

定義IKEv2金鑰環，它定義頭端IP地址和用於與SSE頭端進行身份驗證的預共用金鑰：

```
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>
```

配置IKEv2配置檔案對。

它們定義了用於匹配遠端對等體的IKE身份型別，以及本地路由器正在向對等體傳送的IKE身份型別。

。SSE頭端的IKE標識為IP地址型別，並且等於SSE頭端的公有IP。



警告：為了在SSE端使用相同的網路隧道組建立多個隧道，這些隧道必須使用相同的本地IKE身份。

Cisco IOS XE不支援此類方案，因為它要求每個隧道具有唯一的本地和遠端IKE標識對。

為了克服此限制，SSE頭端已增強為接受IKE ID的格式

：`<tunneld_id>+<suffix>@<org><hub>.sse.cisco.com`

在所討論的實驗場景中，隧道ID定義為cat8k-dmz。

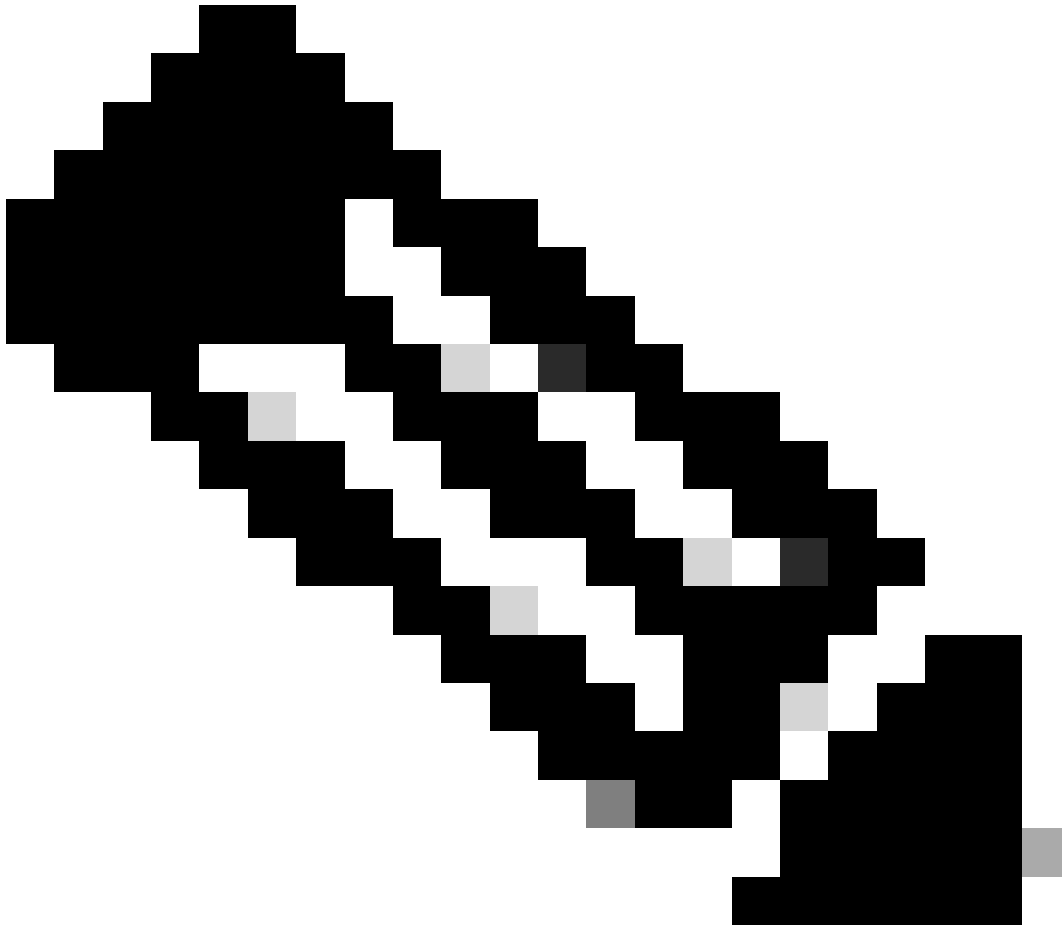
在正常情況下，我們會將路由器配置為以cat8k-dmz@8195165-622405748-sse.cisco.com形式傳送

本地IKE標識

但是，為了使用相同的網路隧道組建立多個隧道，將使用本地IKE ID：

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

請注意增加到每個字串 (tunnel1和tunnel2) 的字尾



注意：此處提及的本地IKE標識只是用於本實驗方案的示例。您可以定義任何想要的尾碼，只要確保符合要求即可。

```
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
```

配置IPSec轉換集。此設定定義用於IPsec安全關聯 (第2階段) 的演算法：

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

配置使用轉換集連線IKEv2配置檔案的IPSec配置檔案：

```
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
```

虛擬通道介面

本節介紹虛擬隧道介面的配置以及用作隧道源的環回介面。

在所討論的實驗場景中，我們需要使用相同的公共IP地址與單個對等體建立兩個VTI介面。此外，我們的Cisco IOS XE裝置只有一個出口介面GigabitEthernet1。

Cisco IOS XE不支援使用相同的隧道源和隧道目標配置多個VTI。

為了克服此限制，您可以使用環回介面並將它們定義為相應VTI中的隧道源。

在環回和SSE公共IP地址之間實現IP連線的方法很少：

1. 將可公開路由的IP地址分配給環回介面 (需要擁有公有IP地址空間)
2. 為環回介面分配專用IP地址，並動態分配具有環回IP源的NAT流量。
3. 使用VASI介面 (許多平台不支援，安裝及故障診斷繁瑣)

在此場景中，我們將討論第二個選項。

配置兩個環回介面，並在每個介面下增加「ip nat inside」命令。

```
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
```

定義動態NAT訪問控制清單和NAT過載語句：

```
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
```

配置虛擬隧道介面。

```
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
```



注意：在所述的實驗場景中，分配給VTI的IP地址來自169.254.0.0/24的非重疊子網。您可以使用其他子網空間，但是某些與BGP相關的要求需要此類地址空間。

BGP路由

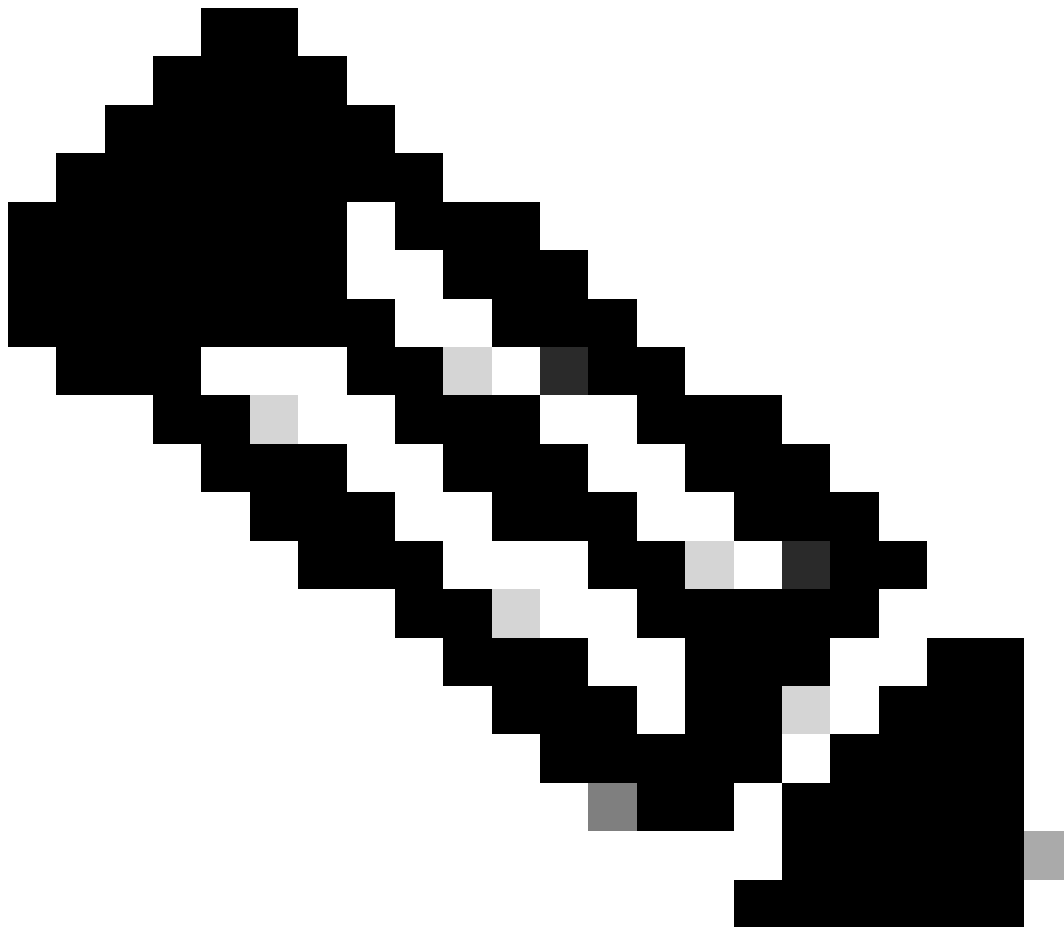
本節介紹建立具有SSE頭端的BGP鄰居關係所需的配置部分。SSE頭端上的BGP進程偵聽子網中的任何IP 169.254.0.0/24。為了建立兩個VTI上的BGP對等關係，我們將定義兩個鄰居169.254.0.9 (Tunnel1)和169.254.0.13 (Tunnel2)。此外，您需要根據SSE控制台中顯示的值指定遠端AS。

<#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
```



注意：從兩個對等體接收的路由必須完全相同。預設情況下，路由器在路由表中僅安裝其中一個。

要允許路由表中安裝多個重複路由（並啟用ECMP），必須配置「maximum-paths <number of routes>」

驗證

安全訪問控制台

您必須在SSE控制台中看到兩個主隧道：

Summary Last Status Update Sep 03, 2024 2:32 PM

Warning Primary and secondary hubs mismatch in number of tunnels.

Region	United Kingdom	Routing Type	Dynamic Routing (BGP)
Device Type	ISR	Device BGP AS	65000
		Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5

[View advanced settings](#)

Primary Hub
Hub Up
2 Active Tunnels

Secondary Hub
Hub Down
0 Active Tunnels

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	393217	173.38.154.194	sse-euw-2-1-1	35.179.86.116		Sep 03, 2024 2:32 PM
Primary 2	393219	173.38.154.194	sse-euw-2-1-1	35.179.86.116		Sep 03, 2024 2:32 PM

Cisco IOS XE路由器

從Cisco IOS XE端驗證兩個隧道是否均處於READY狀態：

<#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
```

驗證兩個對等點的BGP鄰居關係是否均為UP：

```
<#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
```

驗證路由器是否從BGP獲知正確的路由（並且路由表中至少安裝了兩個下一跳）。

```
<#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
```

啟動流量並驗證兩個通道都已使用，您會看到兩個通道的封裝和解除封裝計數器增加。

```
<#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
```

或者，您可以收集兩個VTI介面上的資料包捕獲，以確保流量在VTI之間實現負載均衡。閱讀[本文檔](#)中的說明以在Cisco IOS XE裝置上配置嵌入式資料包捕獲。

在示例中，源IP為192.168.150.1的Cisco IOS XE路由器後面的主機從192.168.200.0/24子網向多個IP傳送ICMP請求。

如您所見，ICMP請求在隧道之間均衡負載。

```
<#root>
```

```
wbrzyszc-cat8k#
```

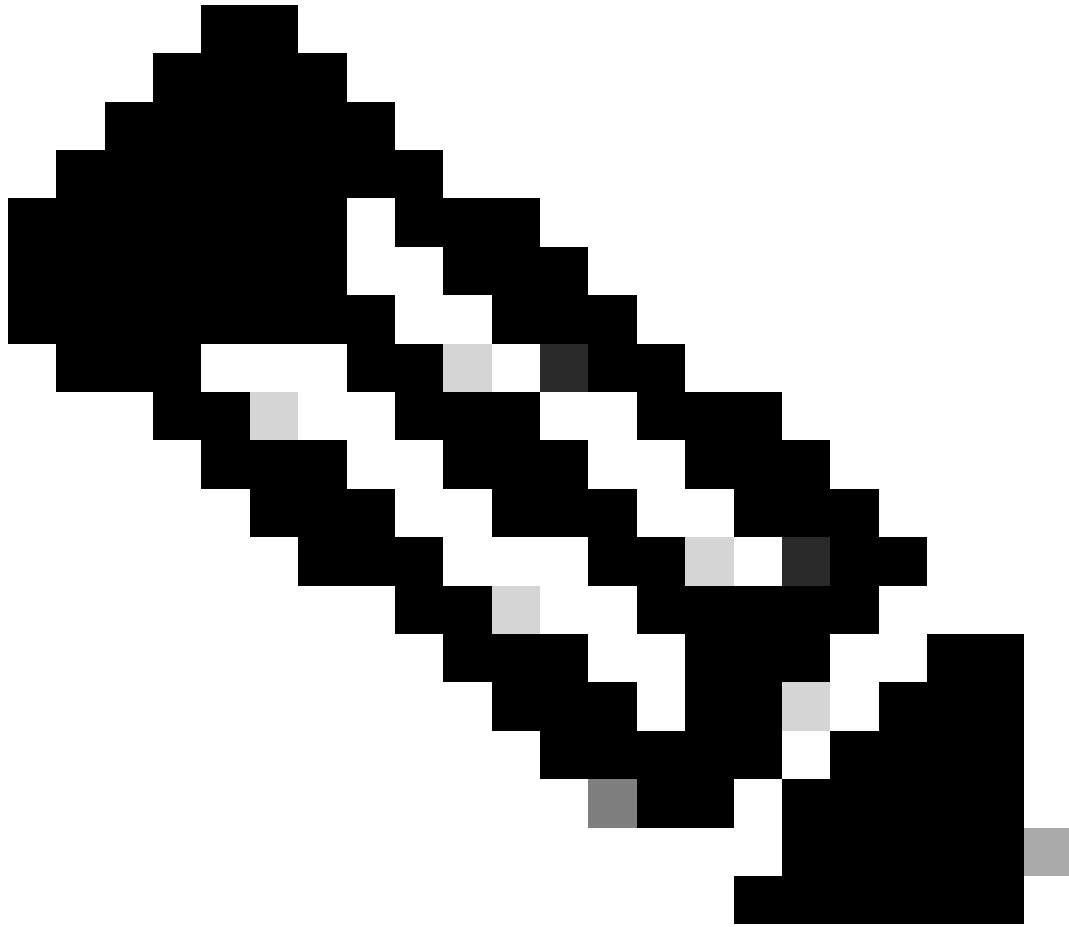
```
show monitor capture Tunnel1 buffer brief
```

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



注意：Cisco IOS XE路由器上有多個ECMP負載均衡機制。預設情況下，啟用每個目標的負載均衡，這樣可確保發往同一目標IP的流量始終採用同一路徑。您可以配置per-packet負載均衡，即使對於相同的目標IP，這種均衡也會隨機對流量進行負載均衡。

相關資訊

- [Secure Access使用手冊](#)
- [如何收集嵌入式資料包捕獲](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。