使用带有BGP的ECMP在Cisco安全访问和IOS XE路由器之间配置网络隧道

目录

简介

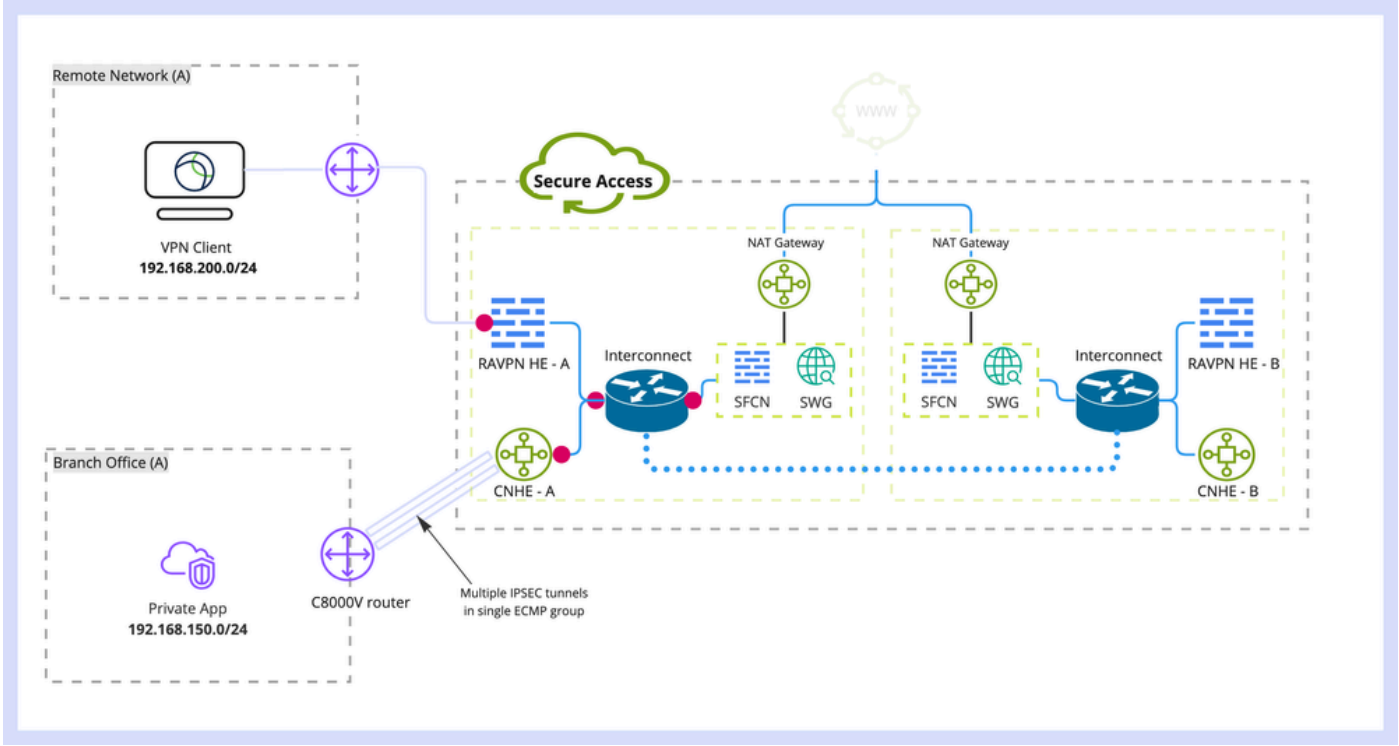
本文档介绍使用BGP和ECMP对Cisco安全访问和Cisco IOS XE之间的IPSec VPN隧道进行配置和故障排除所需的步骤。

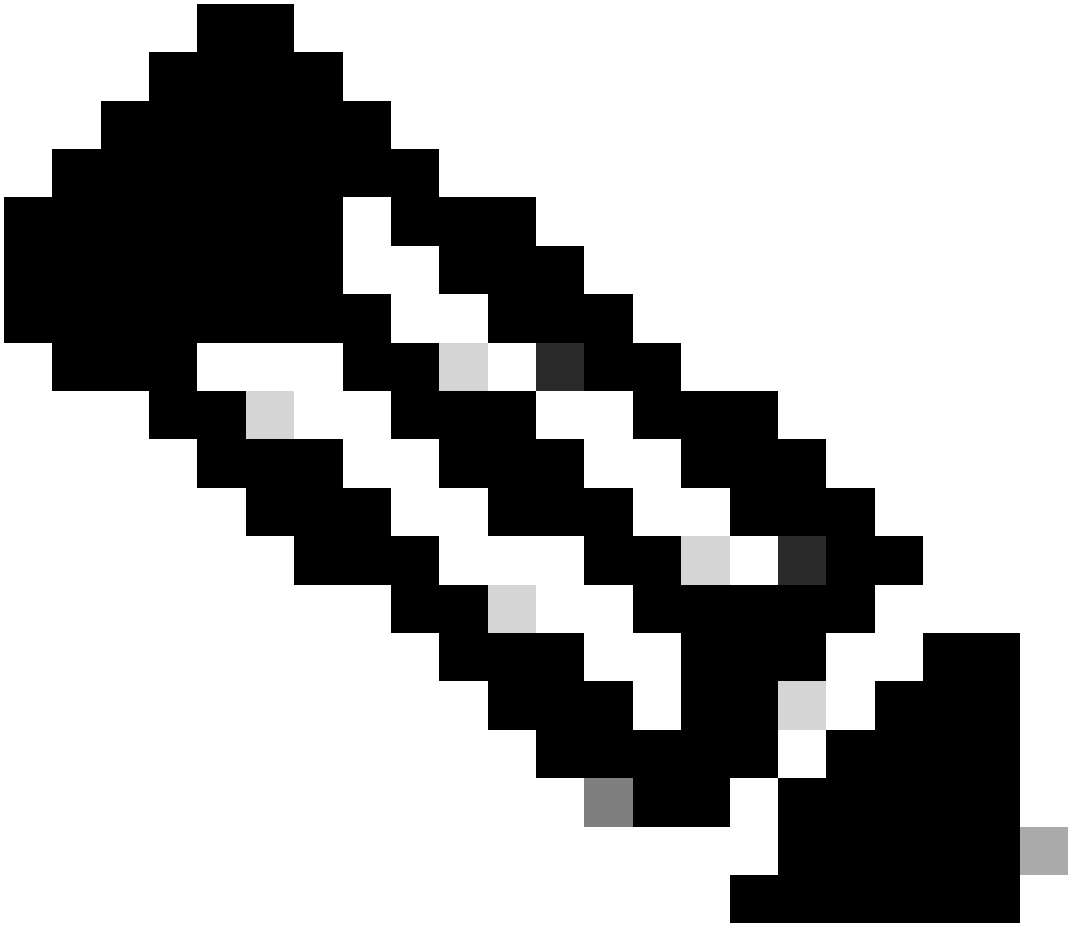
网络图

在本实验示例中，我们将讨论以下场景：网络192.168.150.0/24 是Cisco IOS XE设备后面的LAN网段，192.168.200.0/24 是连接到Secure Access前端的RAVPN用户使用的IP池。

我们的最终目标是在Cisco IOS XE设备和安全访问前端之间的VPN隧道上使用ECMP。

为了更好地了解拓扑，请参阅下图：


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



注意：这只是一个数据包流示例，您可以对任何其他流应用相同原理，并对Cisco IOS XE路由器后的192.168.150.0/24子网的Secure Internet Access应用相同原理。

先决条件

要求

建议您了解以下主题：

- Cisco IOS XE CLI配置和管理
- IKEv2和IPSec协议基础知识
- 初始Cisco IOS XE配置（IP寻址、SSH、许可证）
- BGP和ECMP基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行17.9.4a软件版本的C8000V
- Windows电脑
- 思科安全访问组织

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全访问中的网络隧道的带宽限制为每条隧道1Gbps。如果您的上游/下游Internet带宽高于1Gbps，并且您希望充分利用它，则需要通过配置多个隧道与同一安全访问数据中心，并将它们分组到单个ECMP组中来克服此限制。

当您使用单个网络隧道组（在单个安全访问DC内）终止多个隧道时，默认情况下，从安全访问头端角度来看，这些隧道形成ECMP组。
这意味着，一旦安全访问前端向本地VPN设备发送流量，它将在隧道之间实现负载均衡（假设从BGP对等体收到正确的路由）。

要在本地VPN设备上实现相同的功能，需要在单个路由器上配置多个VTI接口，并确保应用正确的路由配置。

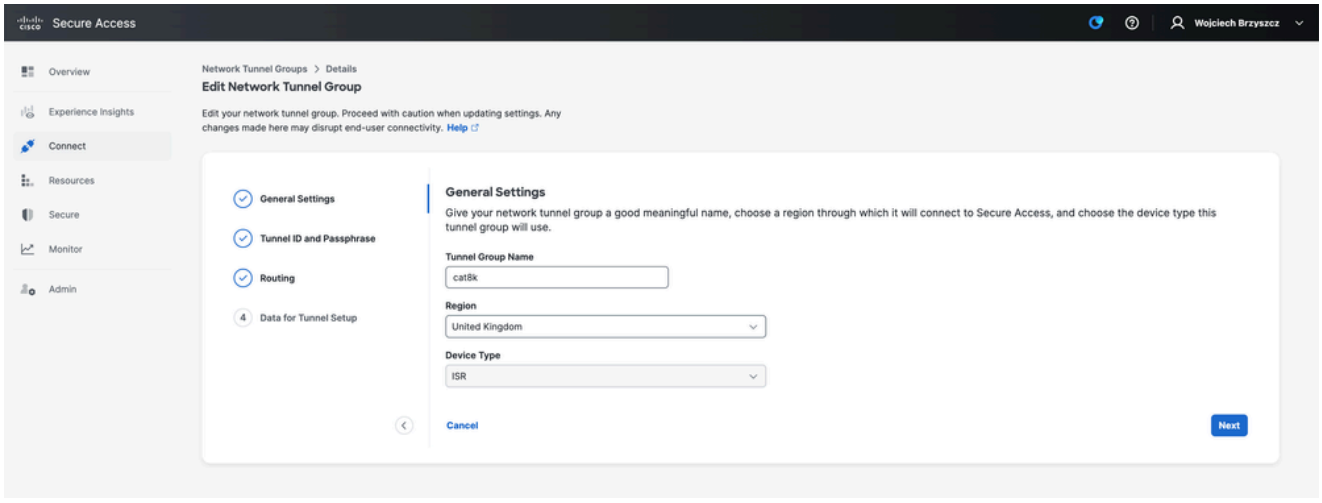
本文包括场景，以及每个必要步骤的说明。

配置

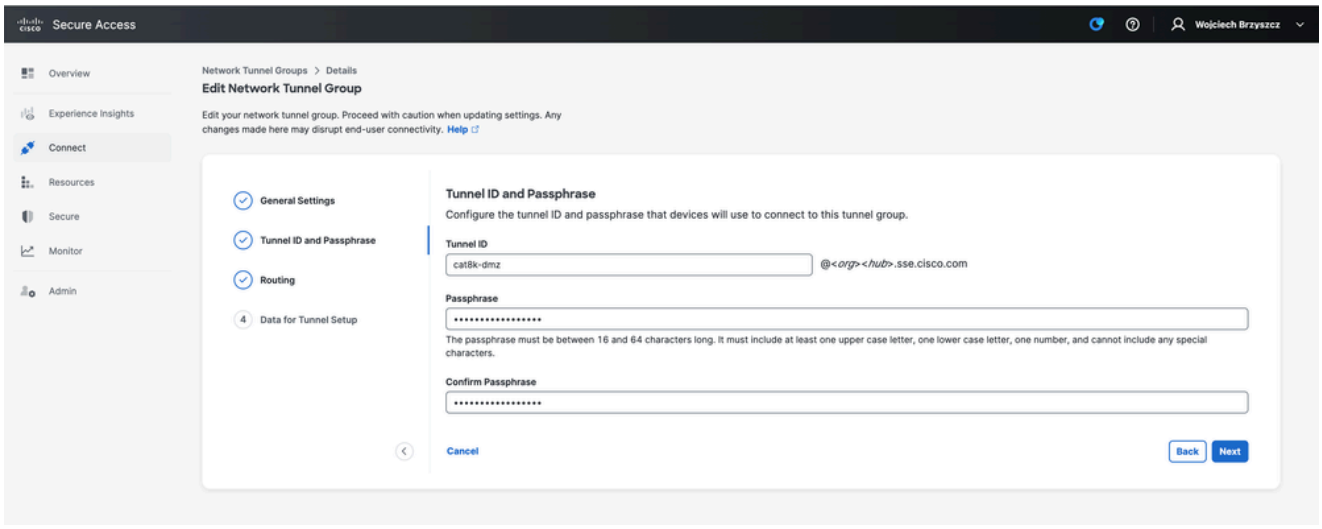
安全访问配置

无需在安全访问端应用特殊配置，即可使用BGP协议从多个VPN隧道形成ECMP组。
配置网络隧道组所需的步骤。

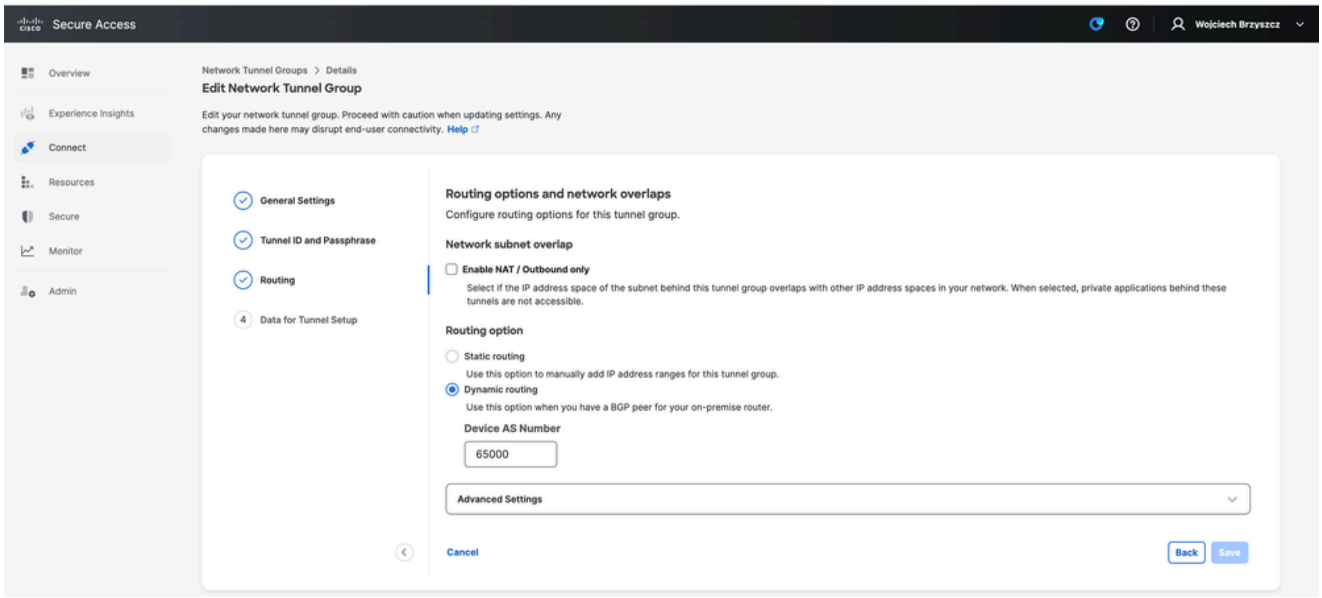
1. 创建新的网络隧道组（或编辑现有隧道组）。



2. 指定Tunnel ID和口令：



3. 配置路由选项，指定动态路由，然后输入您的内部AS编号。在本实验场景中，ASN等于65000。



4. 记下隧道设置的数据部分中的隧道详细信息。

Cisco IOS XE配置

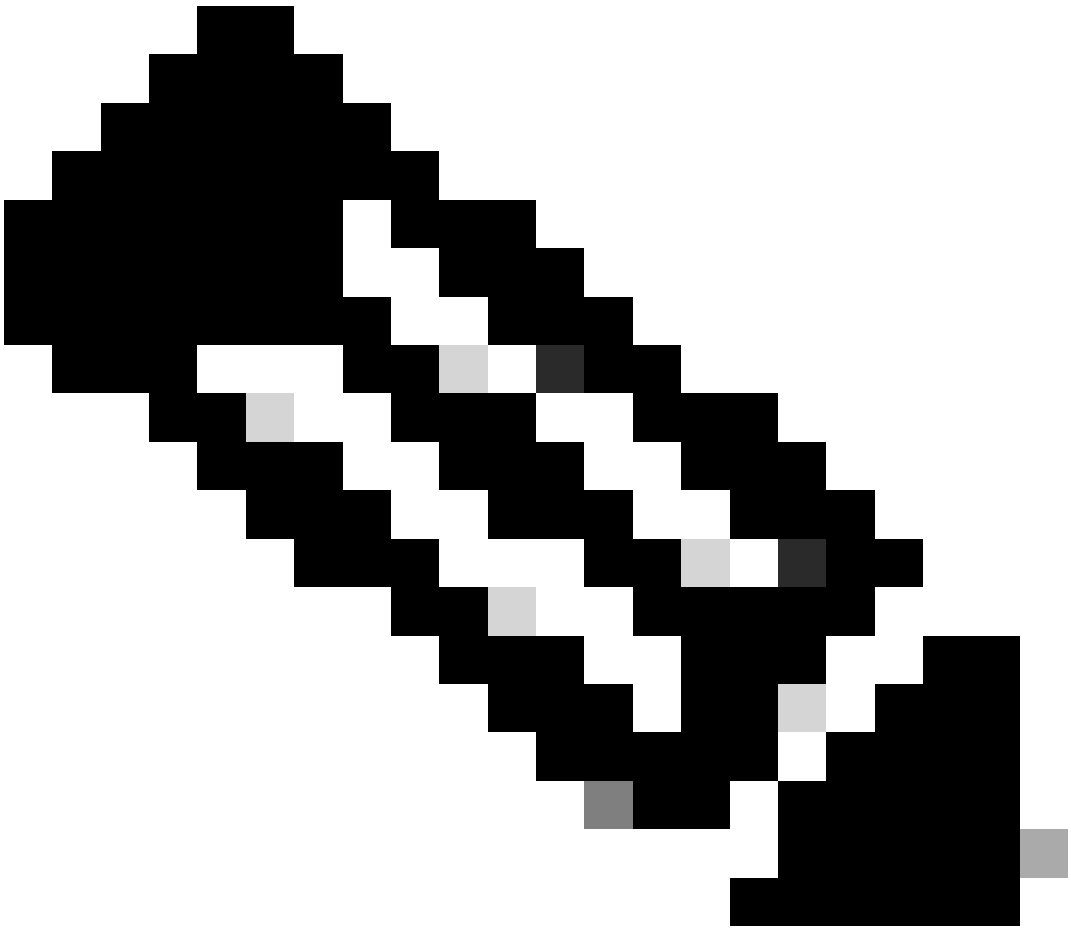
本节介绍需要应用于Cisco IOS XE路由器的CLI配置，以便正确配置跨虚拟隧道接口的IKEv2隧道、BGP邻居关系和ECMP负载均衡。
对每个部分都进行了说明，并提到了最常见的警告。

IKEv2和IPsec参数

配置IKEv2策略和IKEv2提议。这些参数定义用于IKE SA的算法（第1阶段）：

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

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



注意：建议参数和最佳参数在SSE文档中用粗体标记：https://docs.sse.cisco.com/sse-user-guide/docs/supported-ipsec-parameters

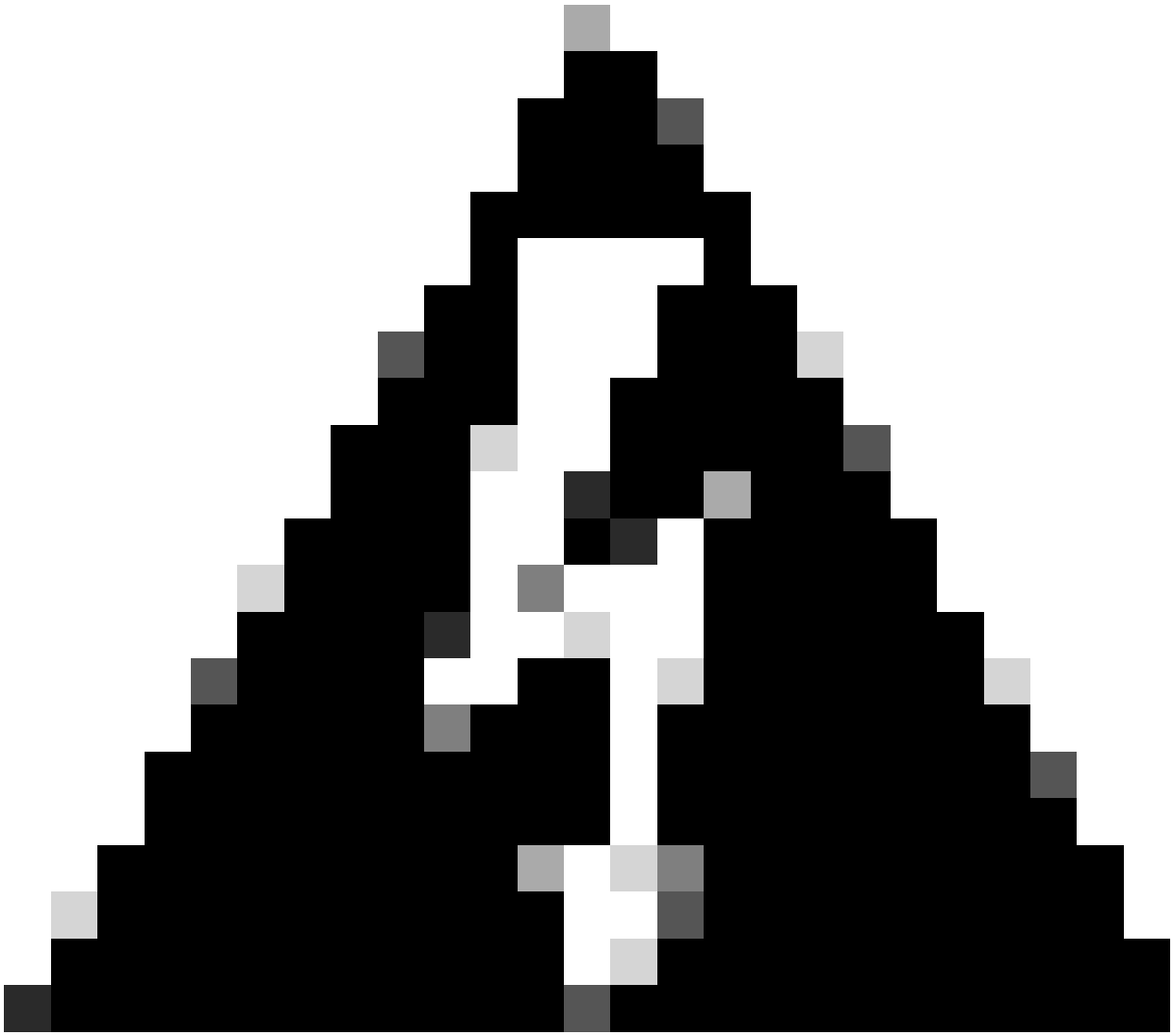
---

定义IKEv2密钥环，用于定义头端IP地址和用于与SSE头端进行身份验证的预共享密钥：

```
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配置文件对。
它们定义了用于匹配远程对等体的IKE身份类型，以及发送到对等体的IKE身份本地路由器。
SSE头端的IKE身份是IP地址类型，并且等于SSE头端的公共IP。



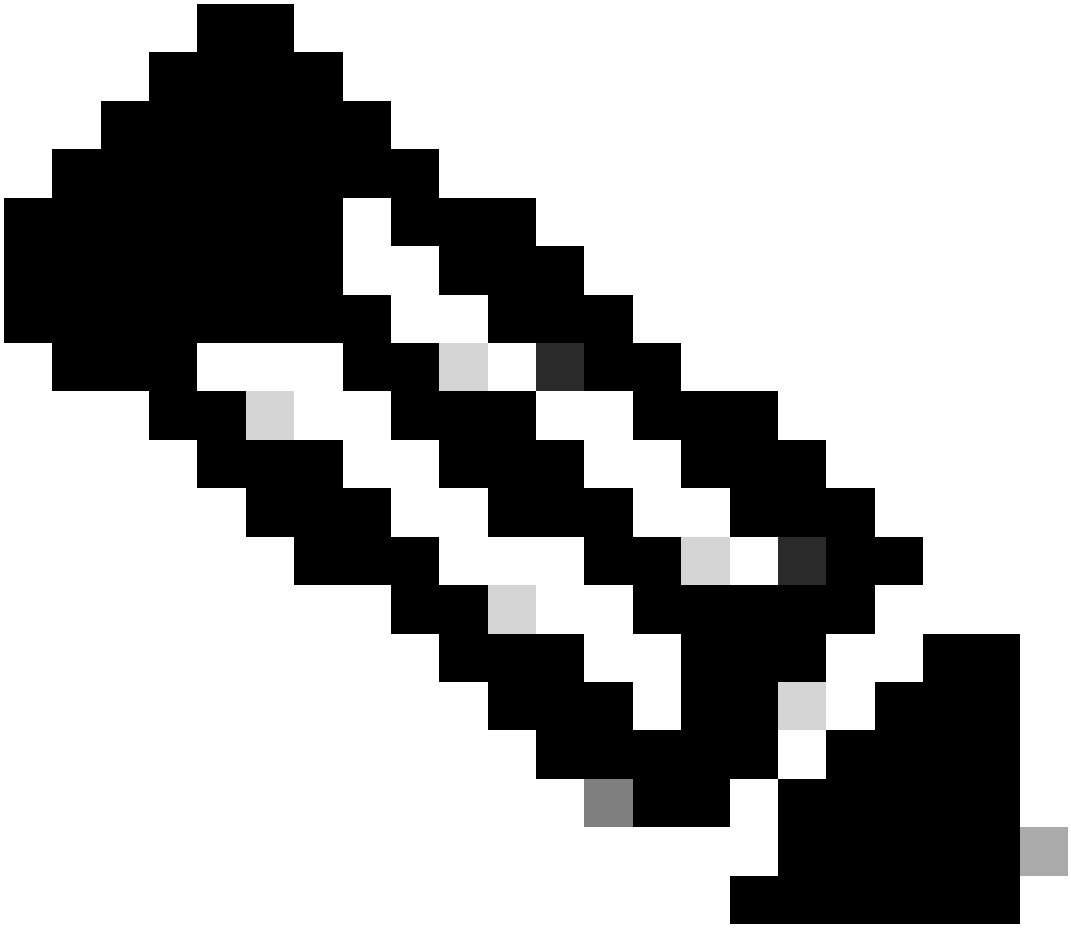
警告：要在SSE端建立具有相同网络隧道组的多个隧道，这些隧道必须使用相同的本地IKE身份。
Cisco IOS XE不支持此类场景，因为它要求每个隧道具有唯一的本地和远程IKE身份对。
为了克服此限制，SSE头端被增强为接受IKE ID的格式
：<tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

在所讨论的实验场景中，隧道ID定义为cat8k-dmz。
在正常情况下，我们会将路由器配置为以cat8k-dmz@8195165-622405748-sse.cisco.com形式发送本地IKE身份

但是，为了使用同一网络隧道组建立多个隧道，将使用本地IKE ID：

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

注意添加到每个字符串的后缀（tunnel1和tunnel2）



> 注意：提到的本地IKE身份只是本实验场景中的示例。您可以定义所需的任何后缀，只需确保满足要求即可。

```
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转换集。此设置定义用于IPsec安全关联（第2阶段）的算法：

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

配置将IKEv2配置文件与转换集链接的IPSec配置文件：

```
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
```

虚拟隧道接口

本节介绍虚拟隧道接口和用作隧道源的环回接口的配置。

在所讨论的实验场景中，我们需要使用相同的公有IP地址与同一个对等体建立两个VTI接口。此外，我们的Cisco IOS XE设备只有一个出口接口GigabitEthernet1。

Cisco IOS XE不支持使用相同的隧道源和隧道目标配置多个VTI。

为了克服此限制，您可以使用环回接口并将其定义为各个VTI中的隧道源。

在环回和SSE公有IP地址之间实现IP连接的方法很少：

1. 将可公开路由的IP地址分配给环回接口（需要拥有公有IP地址空间）
2. 将私有IP地址分配给环回接口并动态分配具有环回IP源的NAT流量。
3. 使用VASI接口（许多平台不支持，设置和故障排除非常繁琐）

在此场景中，我们将讨论第二个选项。

配置两个环回接口，并在每个接口下添加“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
```

定义动态NAT访问控制列表和NAT过载语句：

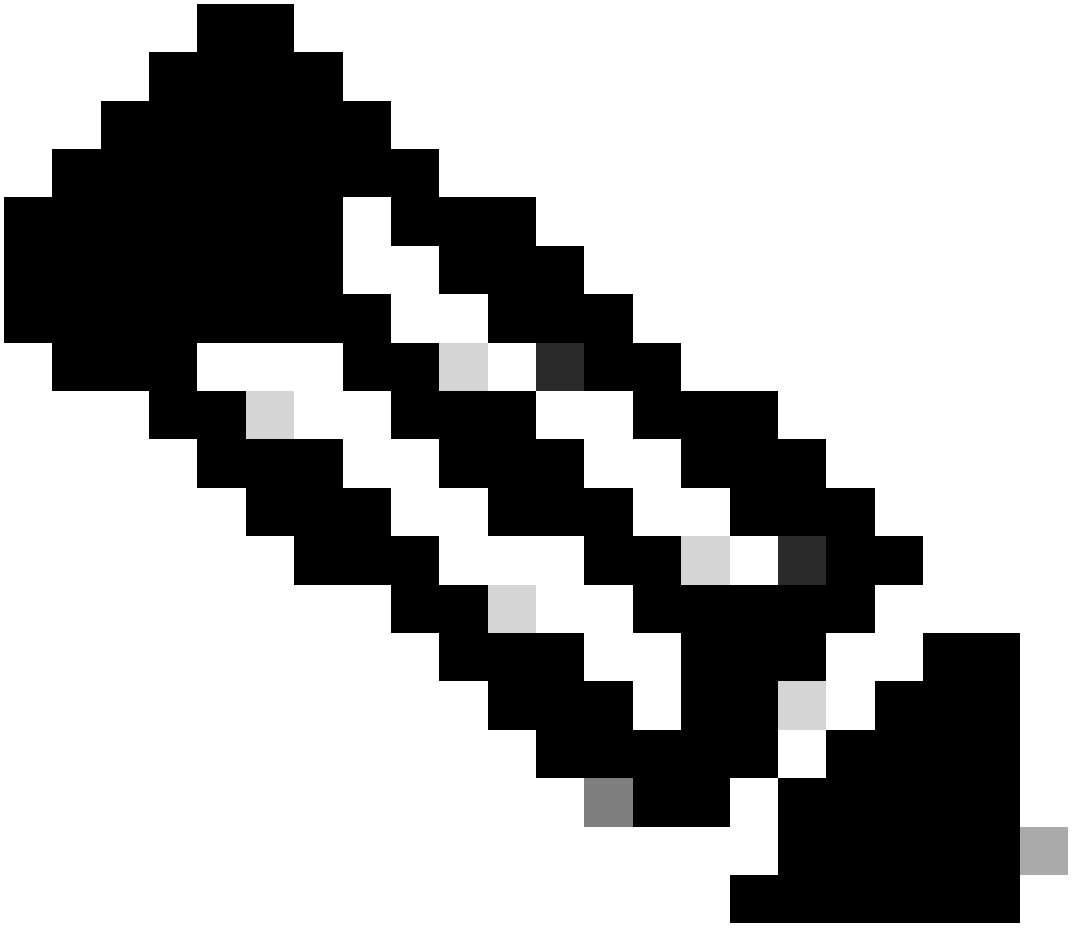
```
ip access-list extended NAT
10 permit ip 10.1.1.0 0.0.0.255 any

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

配置虚拟隧道接口。

```
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：在所述的实验场景中，分配给VTI的IP地址来自非重叠子网169.254.0.0/24。您可以使用其他子网空间，但某些与BGP相关的要求需要此类地址空间。

BGP路由

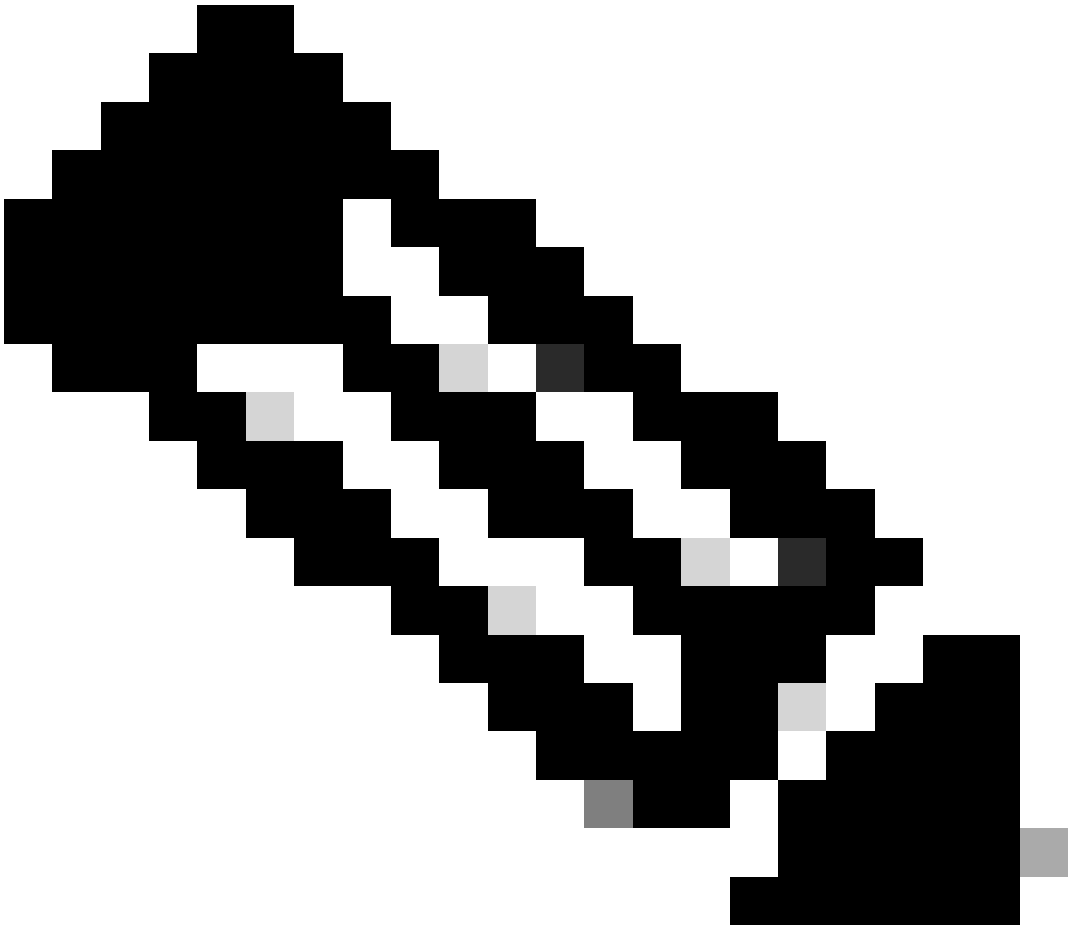
本节介绍与SSE头端建立BGP邻居关系所需的配置部分。
SSE头端上的BGP进程侦听子网中的任何IP 169.254.0.0/24 的多播地址发送一次邻居消息。
要在两个VTI上建立BGP对等，我们将定义两个邻居169.254.0.9 (Tunnel1)和169.254.0.13 (Tunnel2)。
此外，您需要根据SSE控制面板中显示的值指定远程AS。

<#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

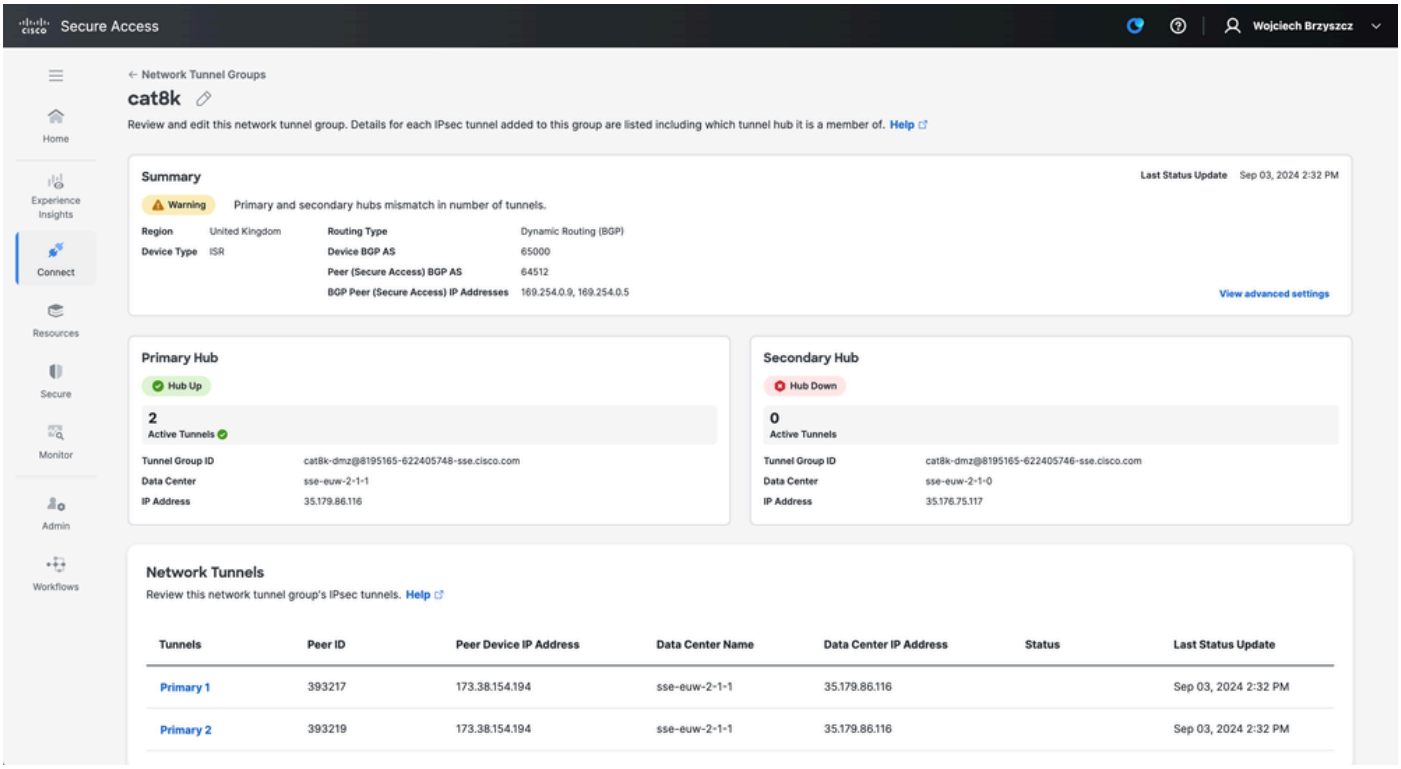


注意：从两个对等体接收的路由必须完全相同。默认情况下，路由器在路由表中仅安装其中一个。
要允许路由表中安装多个重复路由（并启用ECMP），您必须配置“maximum-paths <number of routes>”

验证

安全访问控制面板

您必须在SSE控制面板中看到两个主隧道：



思科IOS XE路由器

从Cisco IOS XE端验证两个隧道均处于READY状态：

<#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
```

验证两个对等体的BGP邻居关系都已启用：

```
<#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
```

验证路由器从BGP获取正确的路由（并且路由表中至少安装了两个下一跳）。

```
<#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
```

启动流量并验证两个隧道均已使用，您会看到两个隧道的encaps和decap计数器都在增加。

```
<#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，您可以在两个VTI接口上收集数据包捕获，以确保流量在VTI之间实现负载均衡。阅读本文中的说明，了解如何在Cisco IOS XE设备上配置嵌入式数据包捕获。
在本示例中，源IP地址为192.168.150.1的Cisco IOS XE路由器后面的主机从192.168.200.0/24子网向多个IP发送ICMP请求。

如您所见，ICMP请求在隧道之间均衡负载。

<#root>

```
wbrzyszc-cat8k#
```

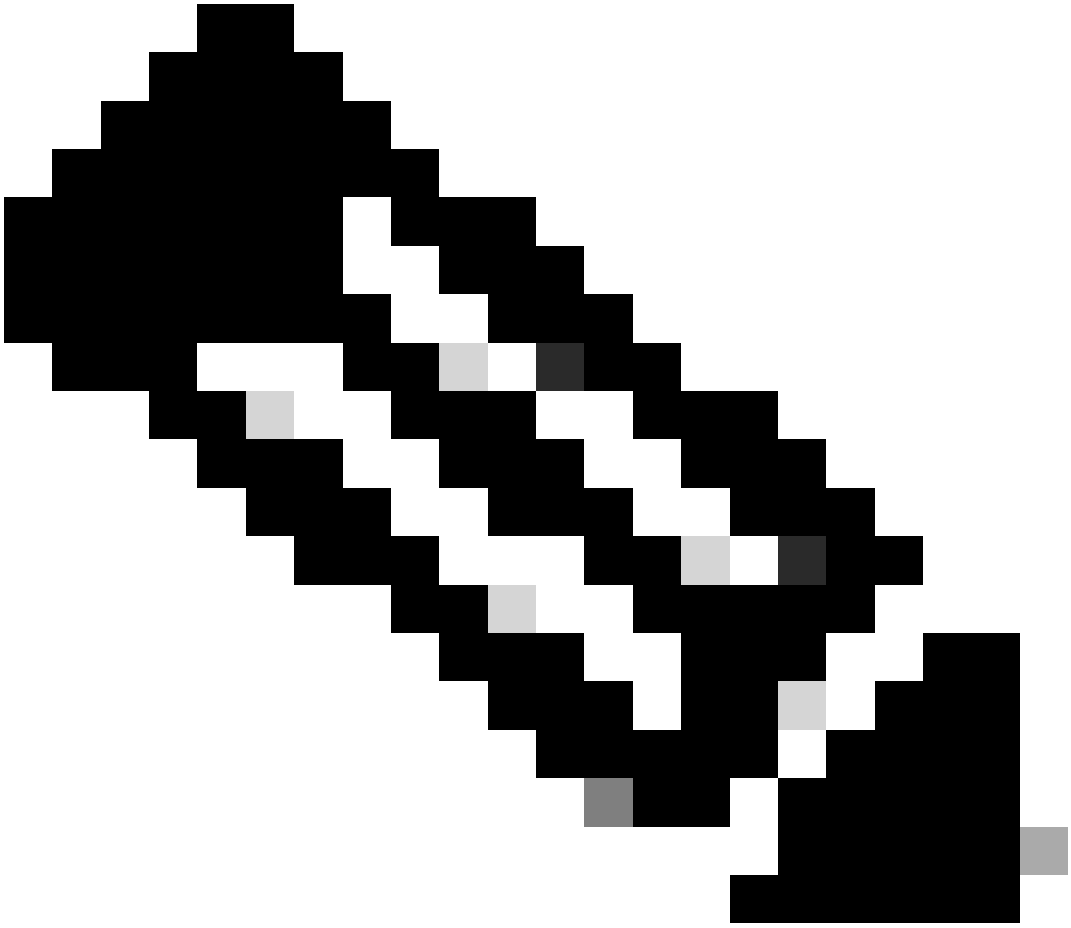
show monitor capture Tunnel1 buffer brief

```
----------------------------------------------------------------------------
#   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路由器上有多个ECMP负载均衡机制。默认情况下，启用基于目标的负载均衡，这样可确保流向同一目标IP的流量始终采用同一路径。
您可以配置每个数据包的负载均衡，这会随机地对甚至相同目标IP的数据流进行负载均衡。

相关信息

- 安全访问用户指南
- 如何收集嵌入式数据包捕获
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。