通过BGP和ECMP配置安全访问IOS XE隧道

目录

简介

网络图

先决条件

- 要求
- 使用的组件

背景信息

配置

- 安全访问配置
- Cisco IOS XE配置
  - IKEv2和IPsec参数
- 配置IKEv2配置文件对
  - 虚拟隧道接口
  - BGP路由

验证

- 安全访问控制面板
- 思科IOS XE路由器

相关信息

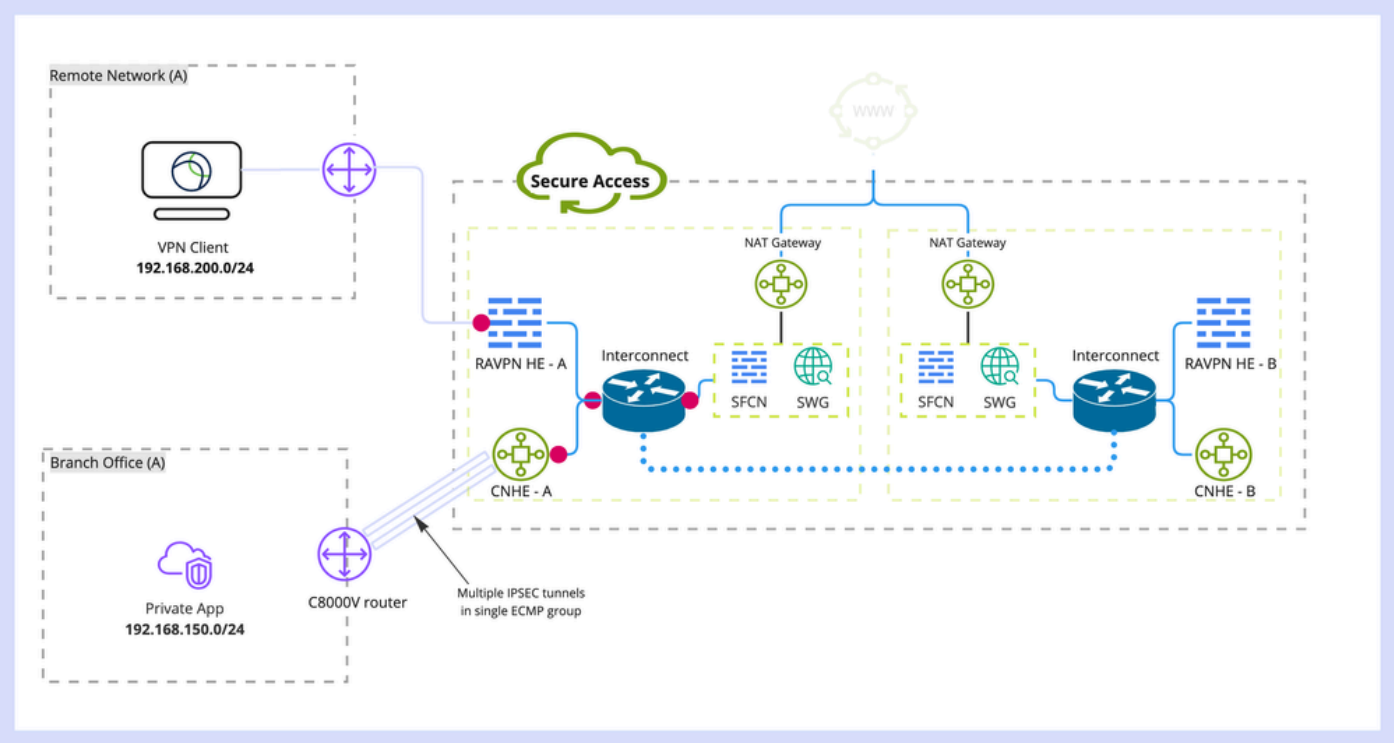
简介

本文档介绍使用BGP和ECMP在Cisco Secure Access和Cisco IOS XE之间配置IPSec VPN隧道并对其进行故障排除所需的步骤。

网络图

在本实验示例中，此场景显示网络192.168.150.0/24在Cisco IOS XE设备后面具有LAN网段，而192.168.200.0/24具有由连接到安全访问头端的用户的RAVPN使用的IP池。

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。要更好地了解拓扑，请参阅下图：



注意：这是一个数据包流示例，您可以将相同的原则应用到任何其他流量以及来自Cisco IOS XE路由器后面的192.168.150.0/24子网的安全互联网访问。

先决条件

要求

您必须了解以下主题：

- 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编址、SSH、许可证）
- BGP和ECMP基础知识

使用的组件

本文档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1 Gbps。如果您的上游/下游Internet带宽高于1 Gbps并且您想要充分利用它，则必须使用同一安全访问数据中心配置多个隧道，方法是将这些隧道分组到单个ECMP组中。

当您终止具有单个网络隧道组（在单个安全访问DC内）的多个隧道时，默认情况下，它们从安全访问头端角度形成ECMP组。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）。

要通过本地VPN设备实现相同的功能，您必须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。本文涵盖这些场景，并对每个步骤进行说明。

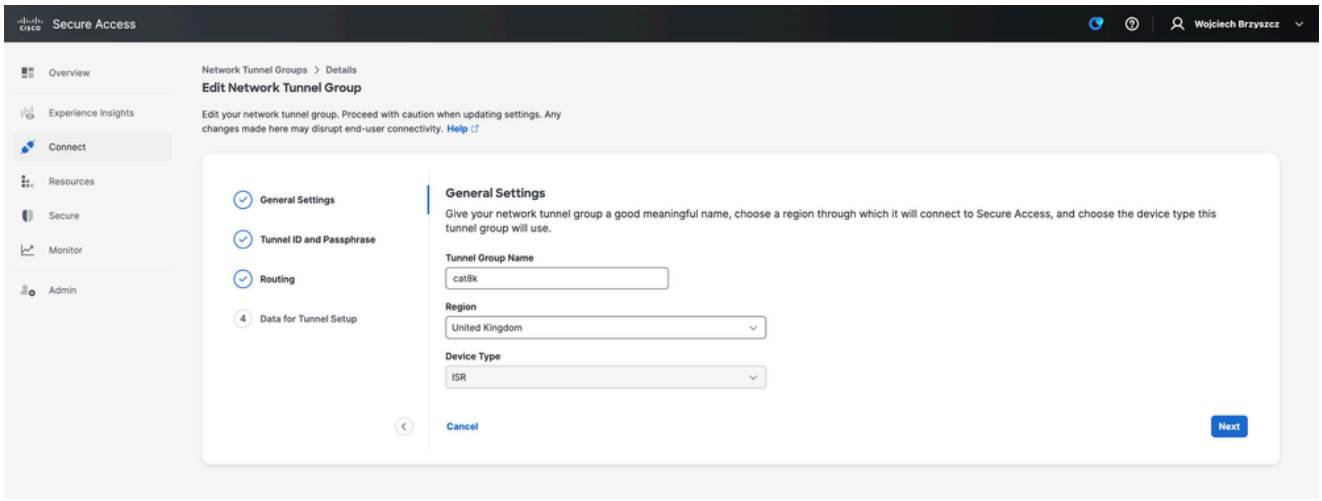
配置

安全访问配置

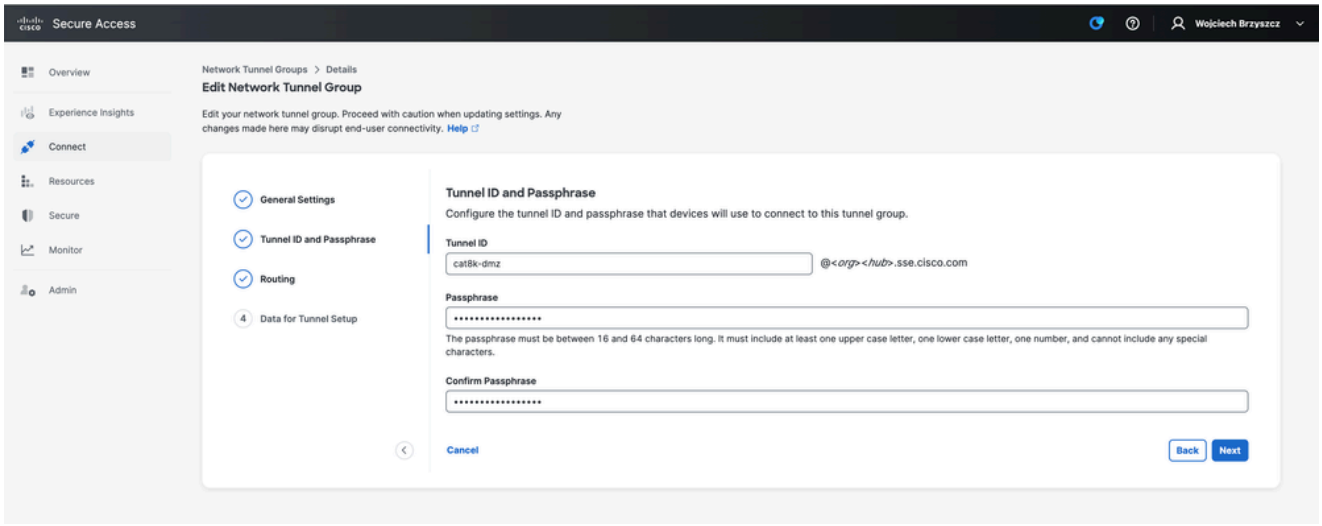
安全访问端必须应用特殊配置，才能使用BGP协议从多个VPN隧道中形成ECMP组。

配置网络隧道组：

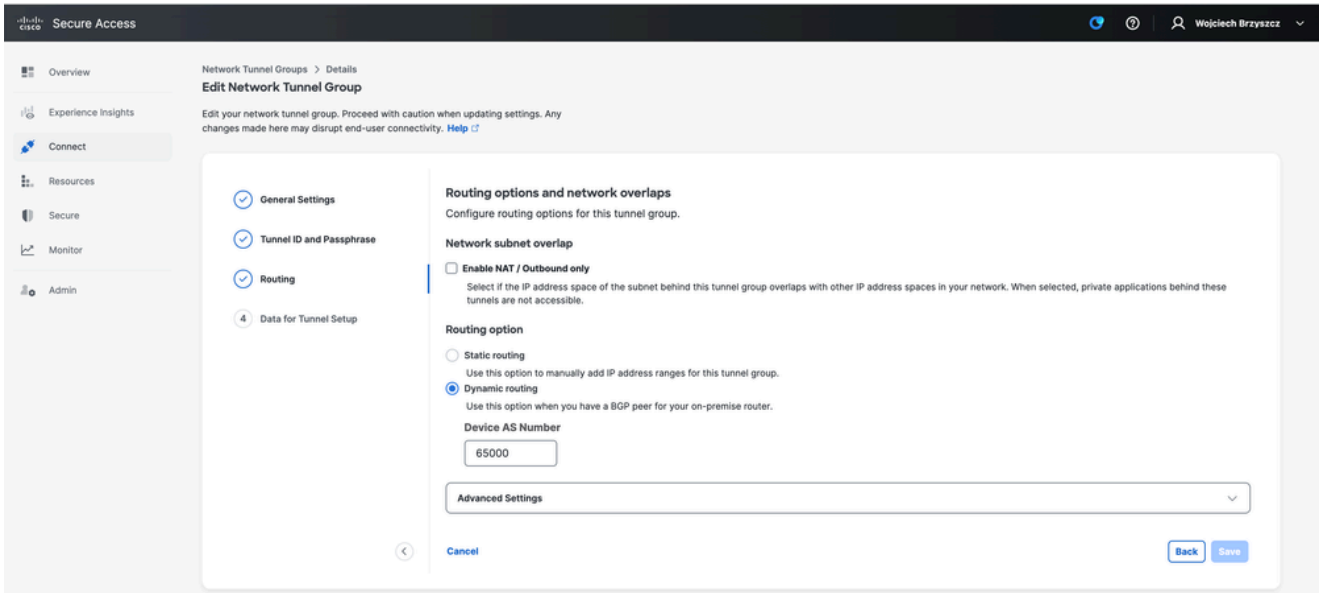
1. 创建新的网络隧道组（或编辑现有隧道组）：



2. 指定Tunnel ID和口令：



3. 配置Routing选项，指定Dynamic Routing，然后输入您的内部AS编号。在本实验场景中，ASN等于65000:



4. 请注意Data for Tunnel Setup部分中的隧道详细信息。

Cisco IOS XE配置

本节介绍必须在Cisco IOS XE路由器上应用的CLI配置。要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。

每个部分都有说明，并提及最常见的警告。

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：请参阅支持的IPsec参数SSE指南中以粗体标记的建议和最佳参数。

定义IKEv2密钥环，解释头端IP地址和用于通过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

这定义要使用的IKE身份类型、匹配远程对等体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，等于SSE头端的公共IP。



警告：要在SSE端使用相同的网络隧道组建立多个隧道，它们都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头端进行了增强，以接受以下格式的IKE ID:<tunneld_id>+<suffix>@<org><hub>.sse.cisco.com

---

如实验场景所述，隧道ID定义为：cat8k-dmz。在正常情况下，您将配置路由器以如下方式发送本地IKE身份：cat8k-dmz@8195165-622405748-sse.cisco.com。

但是，要使用相同的网络隧道组建立多个隧道，应使用本地IKE ID:和cat8k-dmz+tunnel2@8195165-622405748-sse.cisco.com。

添加到每个字符串的后缀：（tunnel1和tunnel2）。



注意：如前所述，本地IKE身份是本实验场景中的示例。您可以定义您喜欢的任何后缀，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

本节介绍用作隧道源的虚拟隧道接口和环回接口的配置。在前面讨论的实验场景中，您必须使用相同的公有IP地址与单个对等体建立两个VTI接口。此外，Cisco IOS XE设备只有一个出口接口GigabitEthernet1。Cisco IOS XE不支持使用同一隧道源和隧道目标配置多个VTI。

要克服此限制，您可以使用环回接口并将其定义为各个VTI中的隧道源。

环回和SSE公有IP地址之间实现IP连接有几种选择：

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. 为环回接口分配私有IP地址，并使用环回IP源动态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，接下来的讨论步骤将详细介绍第二个选项。
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：如实验场景中所述，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，但是某些要求与BGP相关，BGP需要地址空间。

BGP路由

本部分介绍与SSE头端建立BGP邻居关系所需的配置步骤。SSE头端上的BGP进程侦听来自子网169.254.0.0/24的任何IP。要在两个VTI上建立BGP对等，需要定义两个邻居"169.254.0.9(Tunnel1)和169.254.0.13(Tunnel2)。 此外，必须指定SSE控制面板中看到的Remote AS值。

从2025年11月开始，所有新创建的安全访问组织必须默认使用公共ASN 32644在网络隧道组中使用BGP对等。在2025年11月之前建立的现有组织可以继续使用Private ASN 64512，该专用ASN 64512以前是为安全访问BGP对等体保留的。

<#root>

```
router bgp 65000
bgp log-neighbor-changes
neighbor 169.254.0.9 remote-as 32644
neighbor 169.254.0.9 ebgp-multihop 255
neighbor 169.254.0.13 remote-as 32644
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

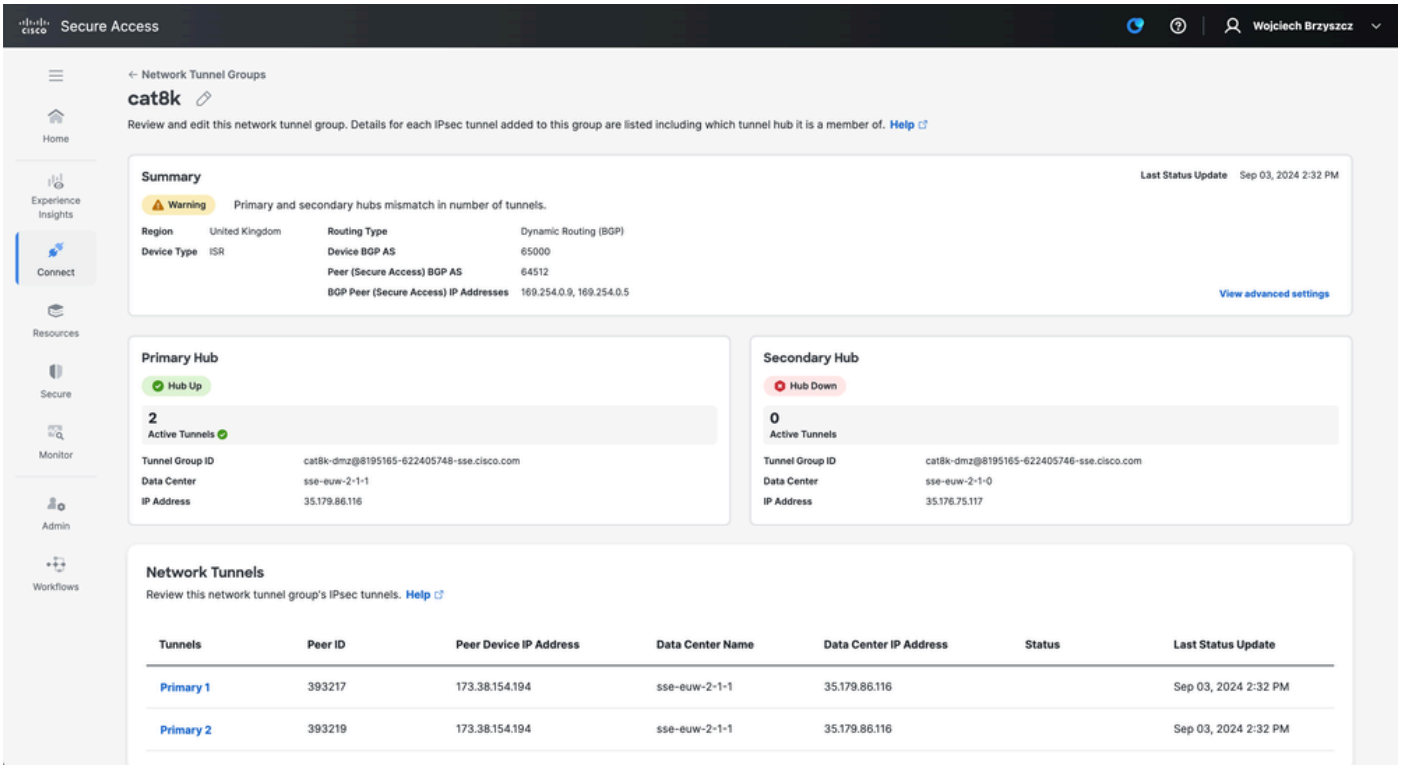
maximum-paths 2
```

注意：从两个对等体接收的路由必须完全相同。默认情况下，路由器只在路由表中安装一个。要允许路由表中安装多个重复路由（并启用ECMP），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
```

验证与两个对等体的BGP邻居关系是否为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 32644 17281 18846 160 0 0 5d23h 15
169.254.0.13 4 32644 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，您会看到这两个隧道的encaps和decaps计数器正在增加：

<#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，可以收集两个VTI接口上的数据包捕获，以确保流量在VTI之间实现负载均衡。有关在Cisco IOS XE设备上配置嵌入式数据包捕获的信息，请参阅在软件上配置和捕获嵌入式数据包指南。在本例中，源IP为192.168.150.1的CIsco IOS XE路由器后面的主机正在从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，启用按目标负载均衡，这样可确保发往同一目标IP的流量始终采用同一路径。您可以配置每数据包负载均衡，即使用同一目标IP来随机负载均衡流量。

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）。