配置双ISP拓扑，在同一区域配置两个集线器和四个辐条

目录

简介

本文档介绍如何使用SD-WAN向导配置在同一区域包含两个集线器和四个分支的双ISP拓扑。

先决条件

支持的软件和硬件平台

经理	FTD	支持的平台
• FMC >= 7.6.0和FMC REST API • cdFMC >= 7.6.0	• 集线器FTD >= 7.6.0 • 分支FTD >= 7.3.0	FMC >= 7.6.0可以管理的所有平台

• FDM — 不支持		

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御
- 思科安全防火墙管理中心
- 软件定义广域网(SD-WAN)

使用的组件

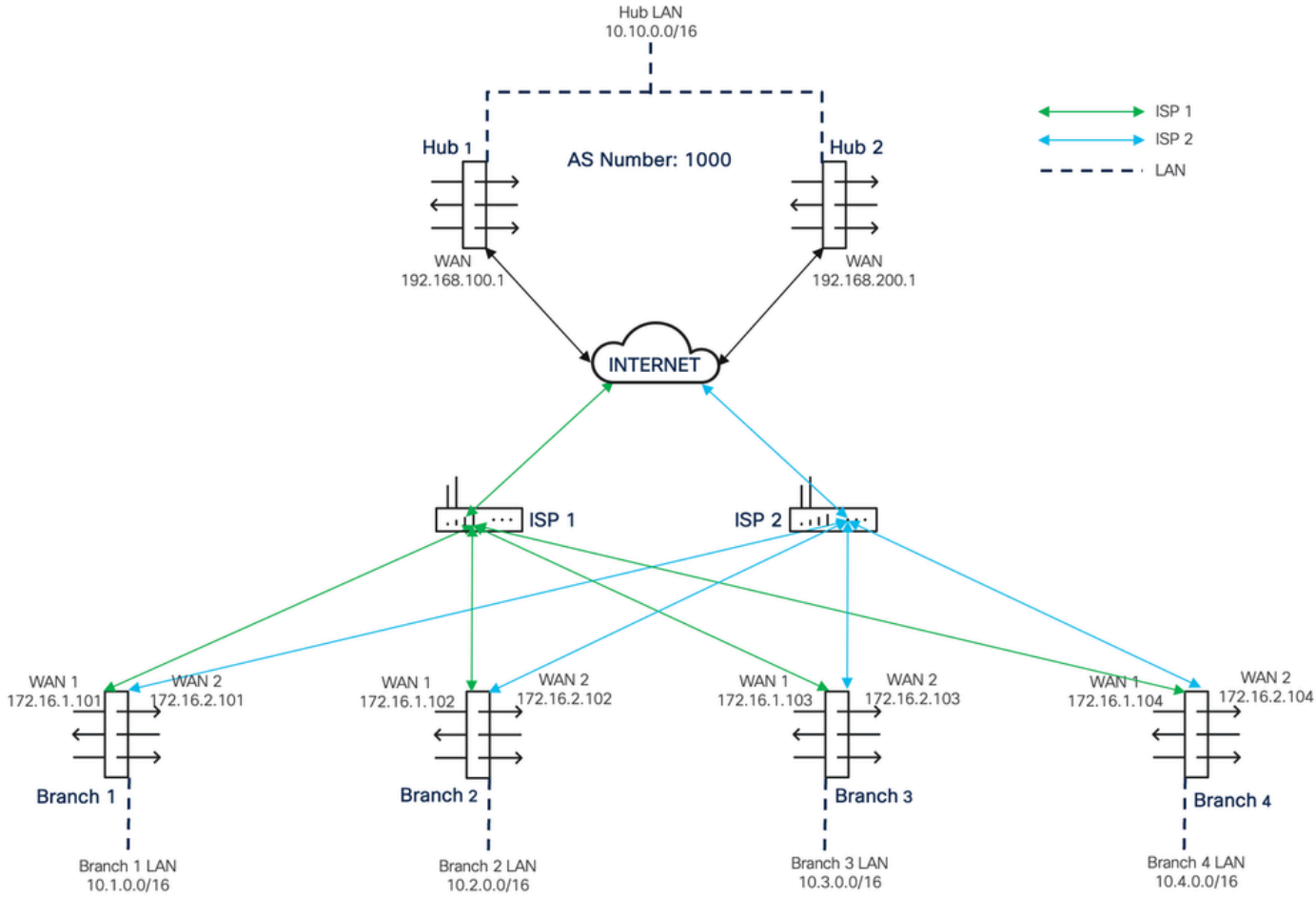
本文档中的信息基于以下软件和硬件版本：

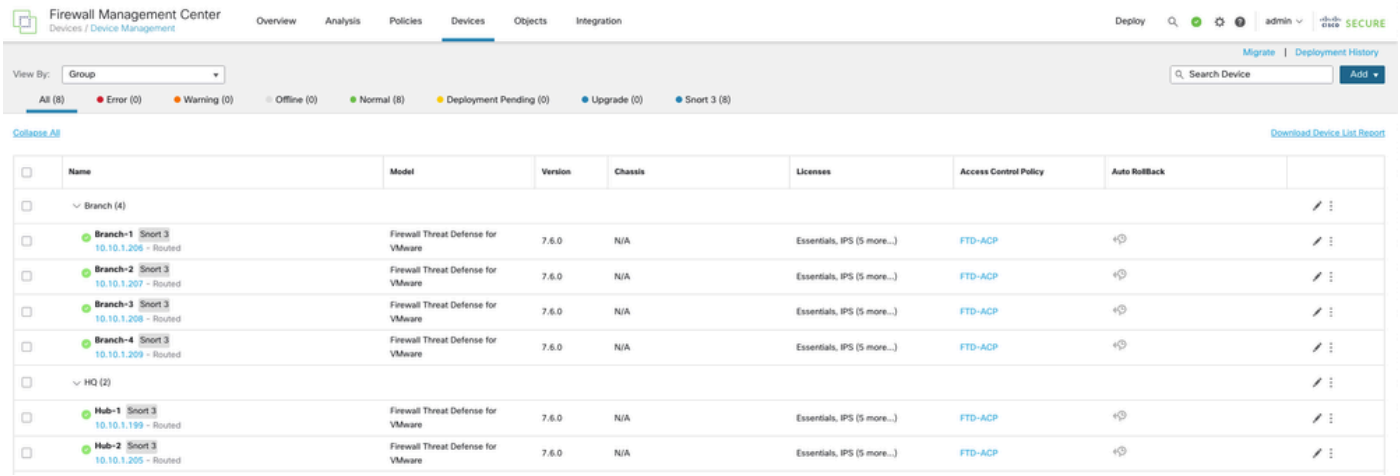
- FTD版本7.6.0
- FMC版本7.6.0

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。

配置

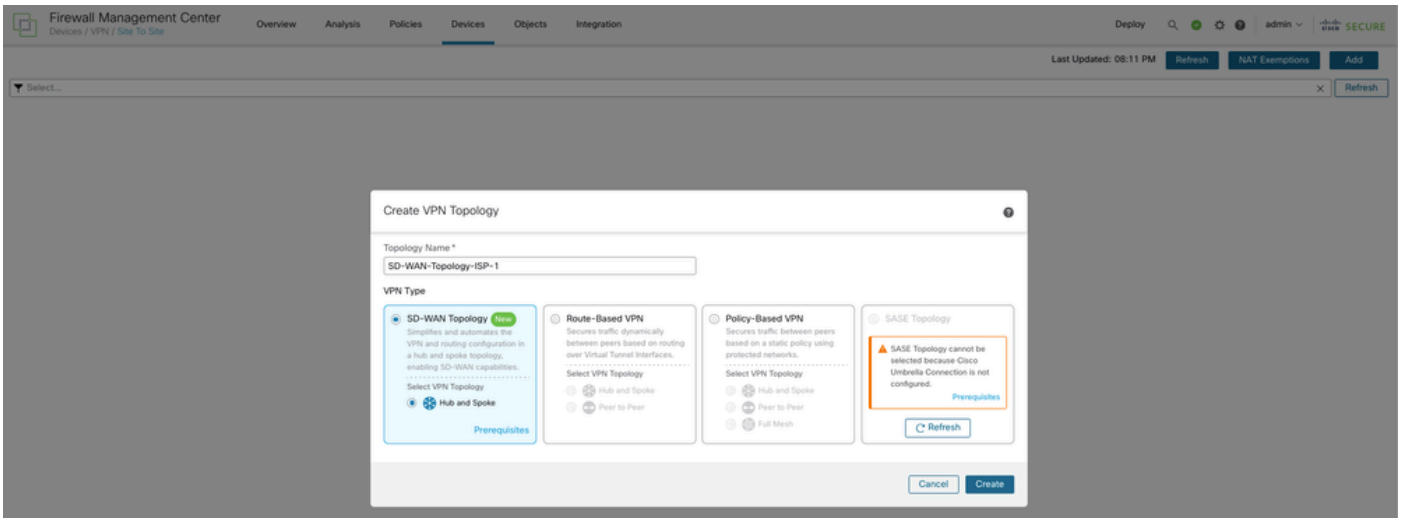
网络图





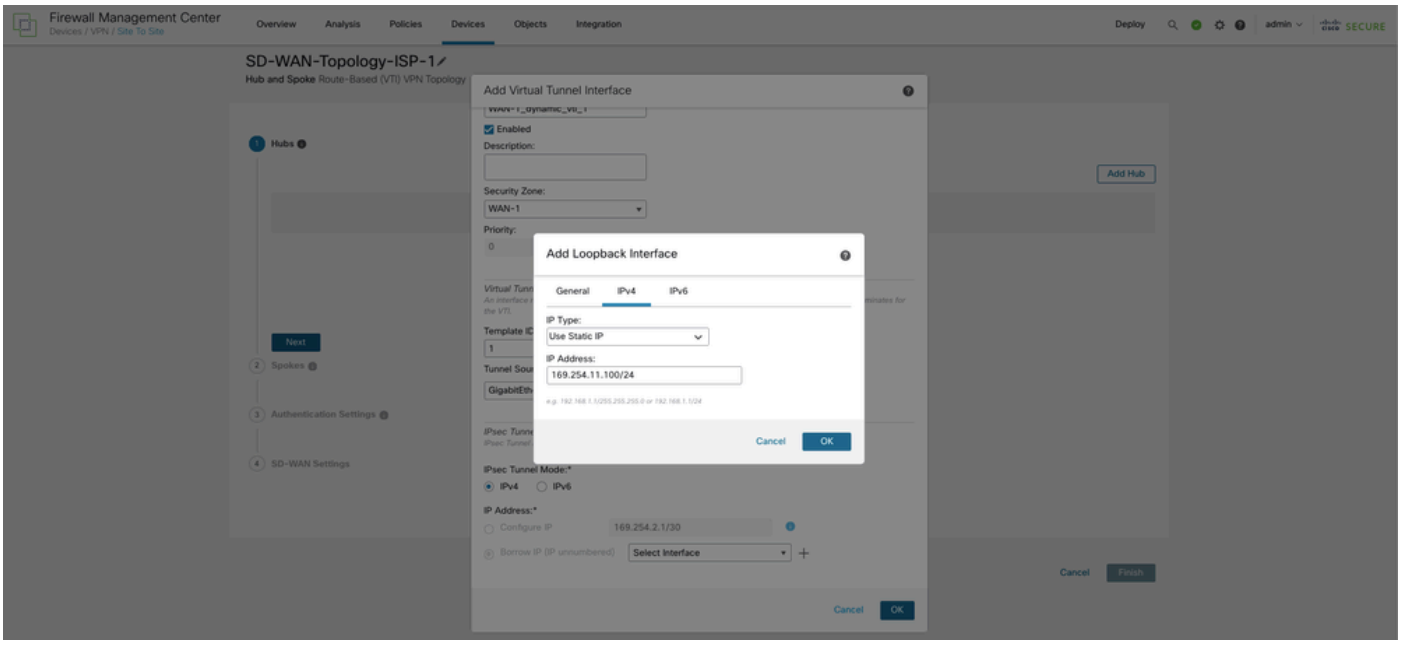
步骤1.创建以WAN-1作为VPN接口的SD-WAN拓扑

导航到设备> VPN >站点到站点。选择Add，在Topology Name字段中输入第一个以WAN-1作为VPN接口的拓扑的合适名称。选择SD-WAN Topology，然后选择Create。

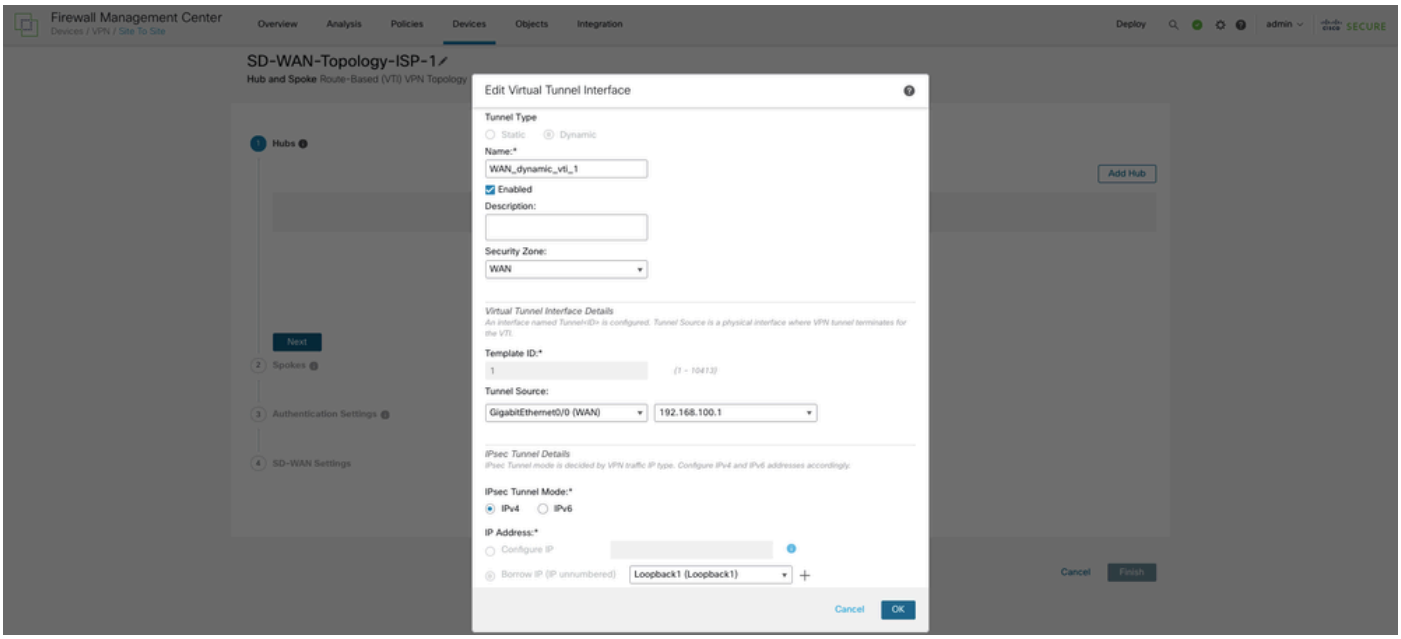


步骤2.在主中心上配置动态虚拟隧道接口(DVTI)

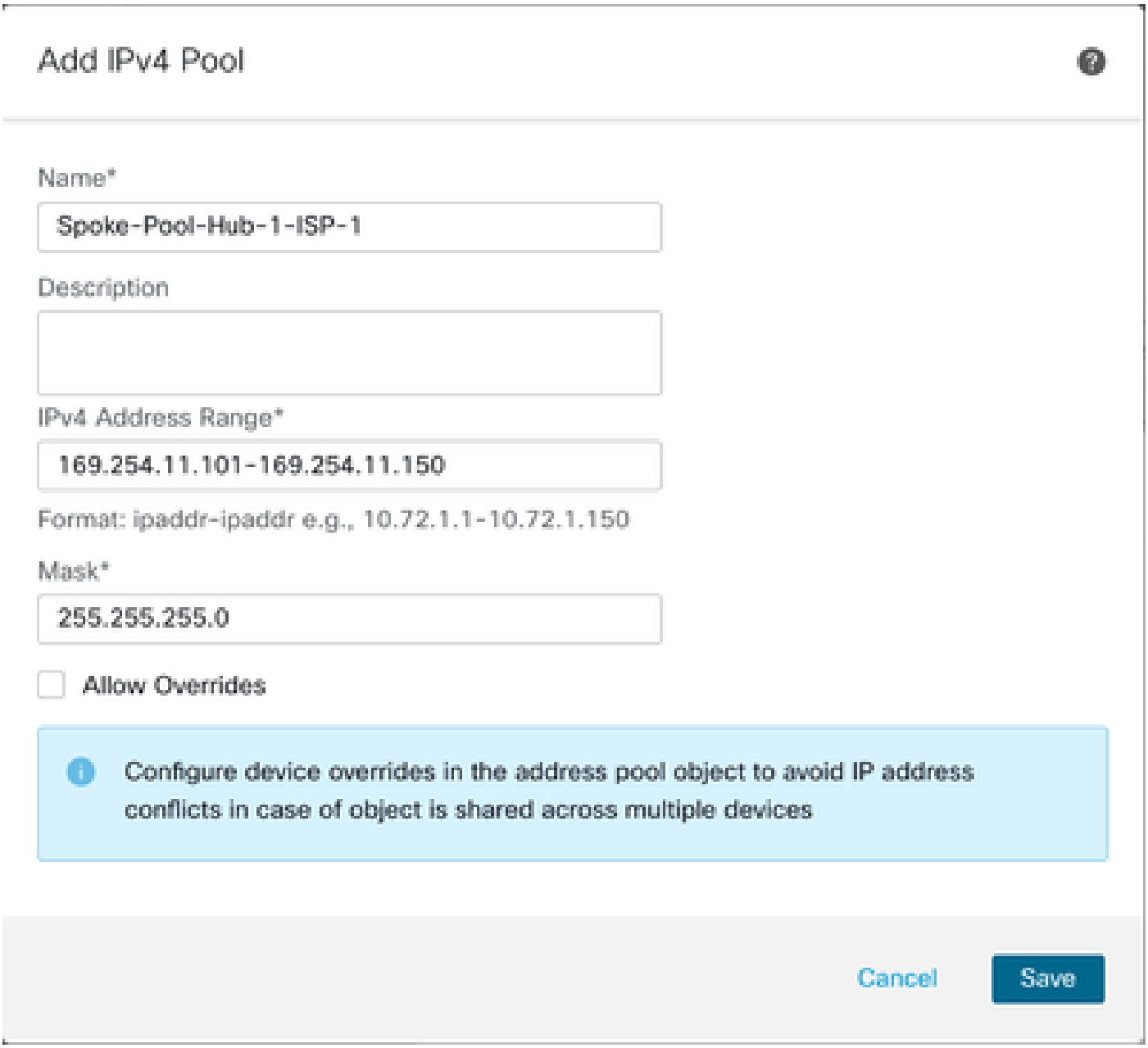
选择Add Hub，然后从Device下拉列表中选择主集线器。选择Dynamic Virtual Tunnel Interface(DVTI)旁边的+图标。 配置名称、安全区域和模板ID，并将WAN-1分配为DVTI的Tunnel Source接口。



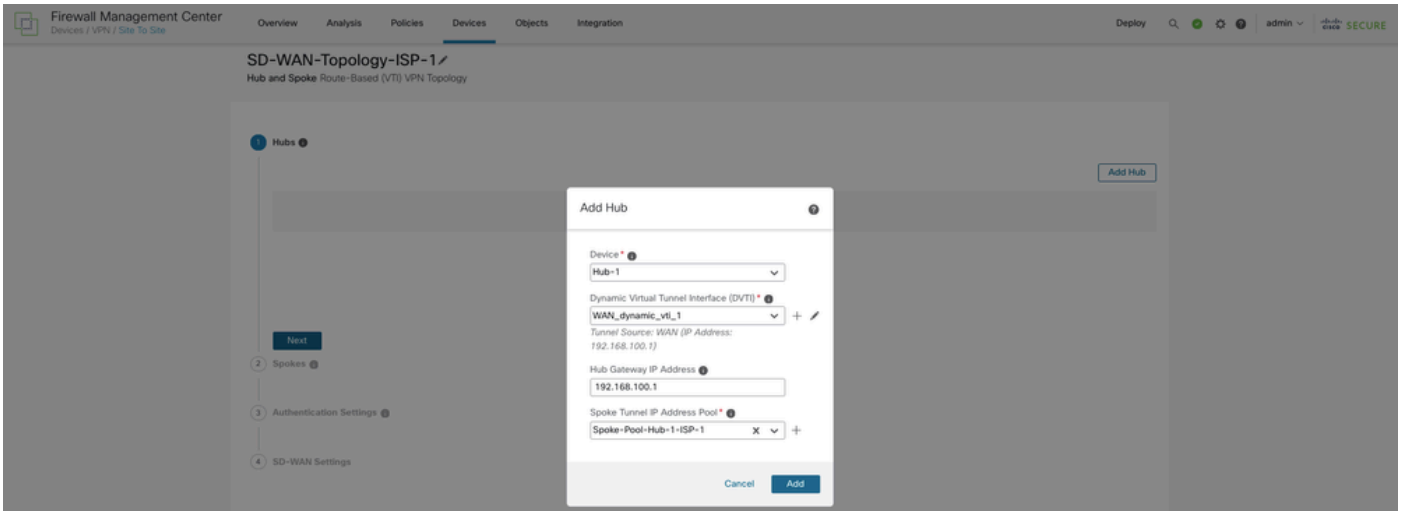
从借用IP下拉列表中选择物理或环回接口。在当前拓扑中，DVTI继承环回接口IP地址。选择“确定”。



选择地址池或选择分支隧道IP地址池旁边的+图标以创建新地址池。添加分支时，向导会自动生成分支隧道接口，并从此IP地址池将IP地址分配给这些分支接口。

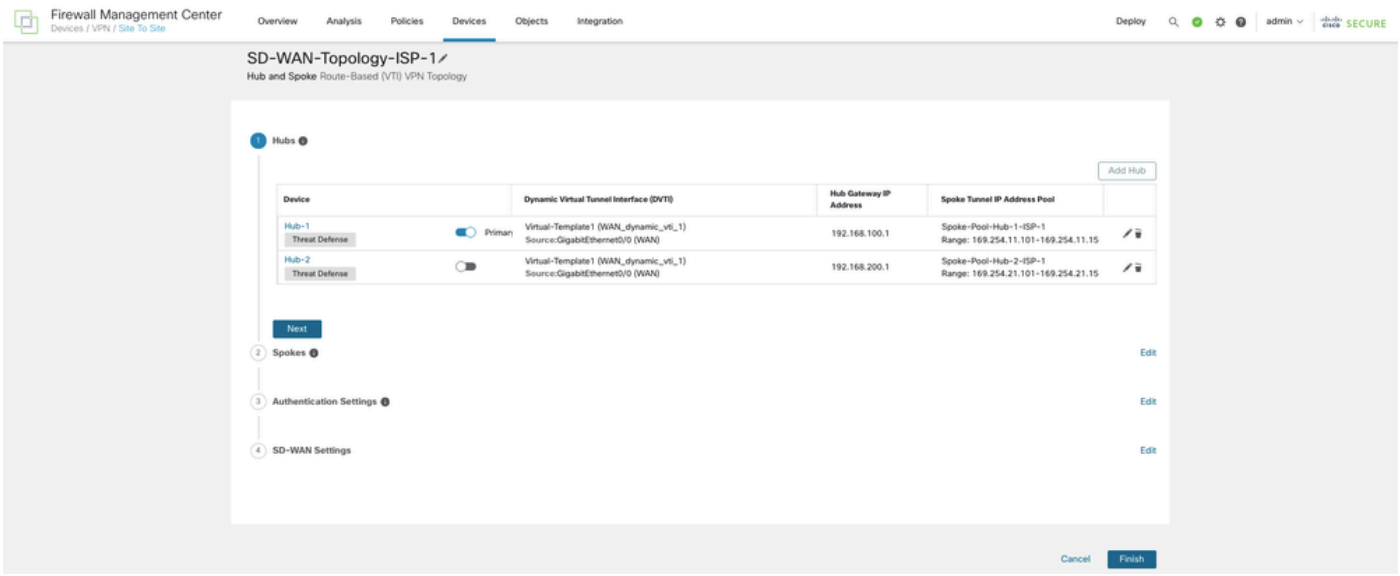


主集线器配置完成后，选择Add将主集线器保存在拓扑中。



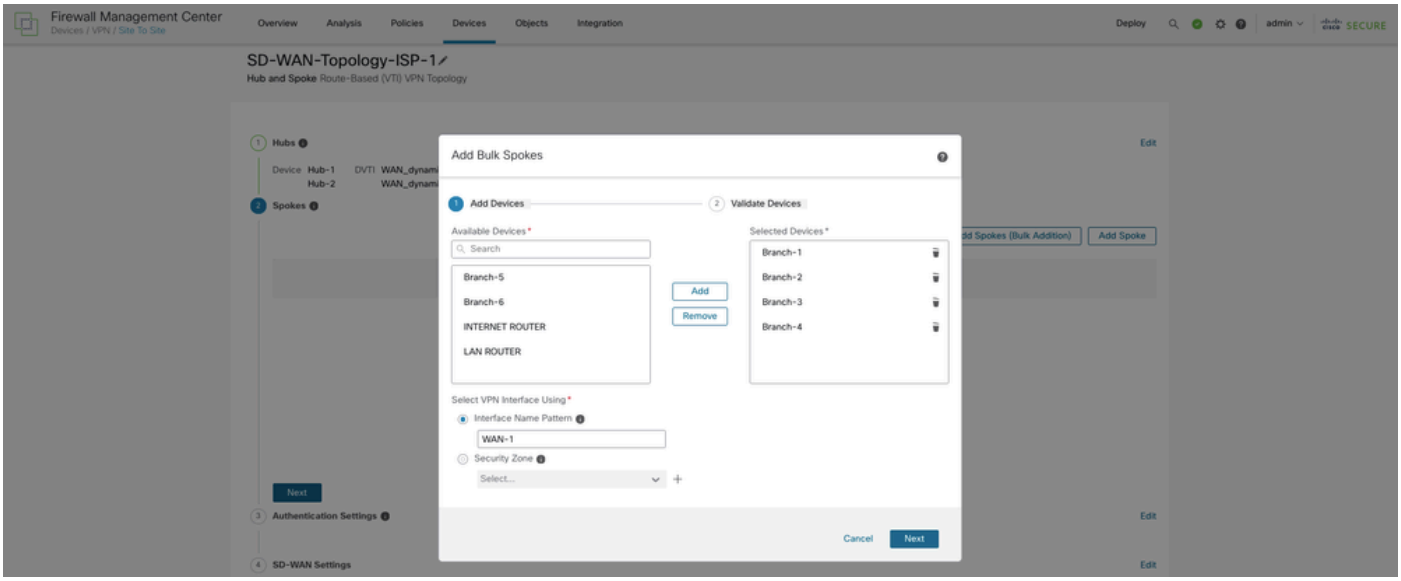
步骤3.在辅助集线器上配置动态虚拟隧道接口(DVTI)

现在重复步骤1和2，再次选择Add Hub以配置拓扑中以WAN-1作为VPN接口的辅助集线器。选择Next。

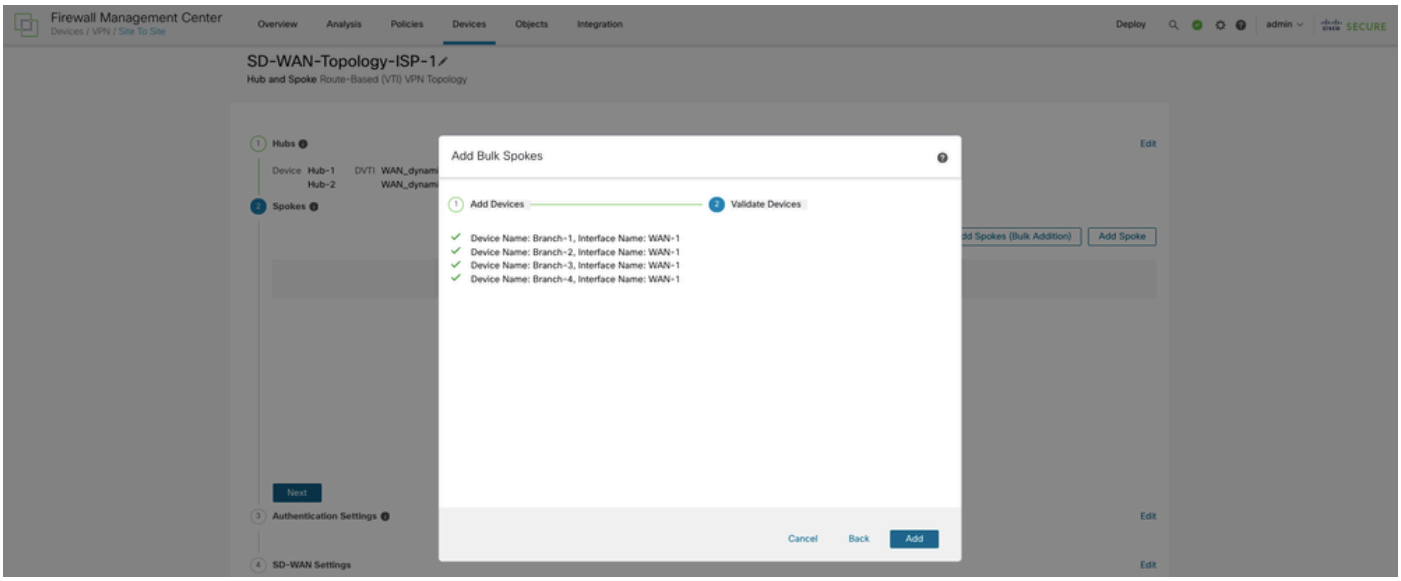


步骤4.配置辐条

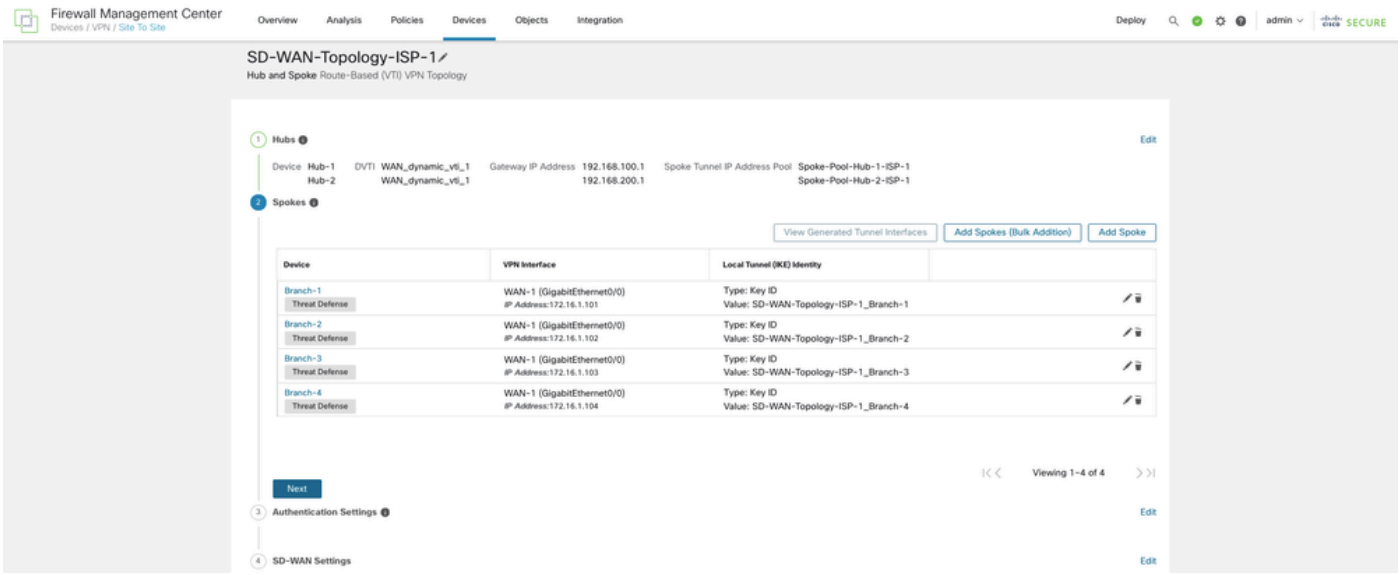
选择Add Spoke以添加单个分支设备，或单击Add Spoke(Bulk Addition)以向拓扑中添加多个分支。当前拓扑使用后一个选项将多个分支机构FTD添加到拓扑。在添加批量辐条对话框中，选择要作为辐条添加的所需FTD。选择与所有辐射点上WAN-1的逻辑名称匹配的通用接口名称模式或与WAN-1相关联的安全区域。



选择下一步，以便向导验证辐射点是否具有指定模式或安全区域的接口。

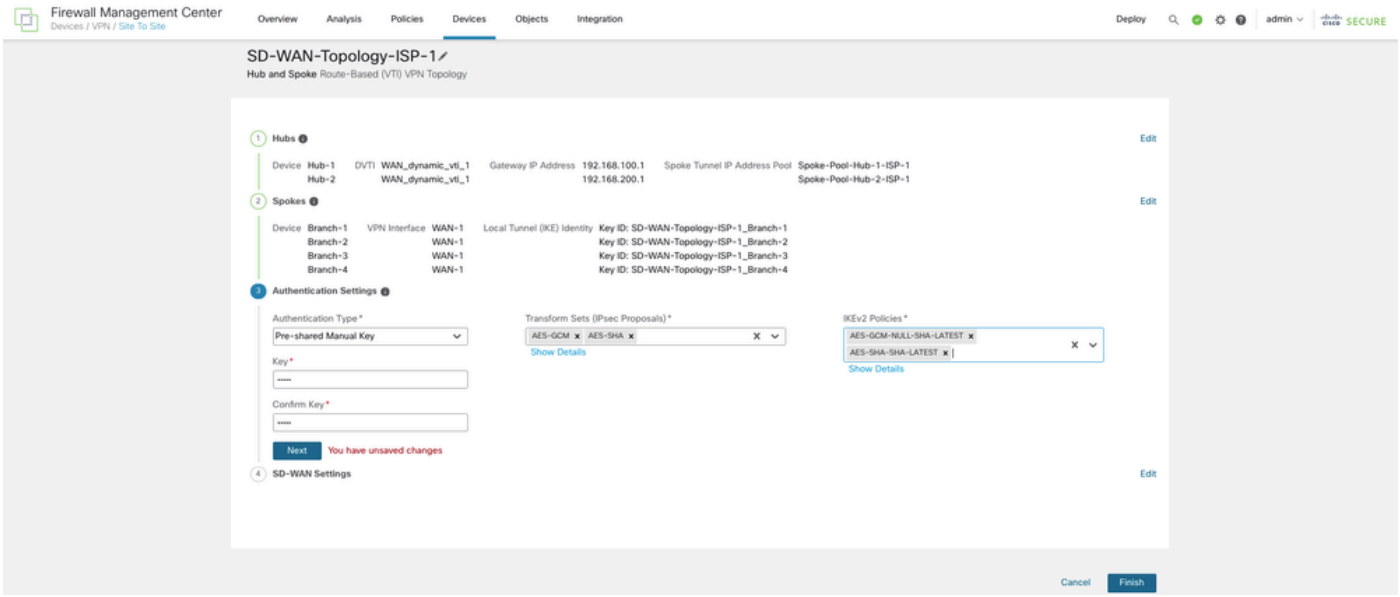


选择Add，向导会自动选择中心DVTI作为每个分支的隧道源IP地址。



步骤5.配置身份验证设置

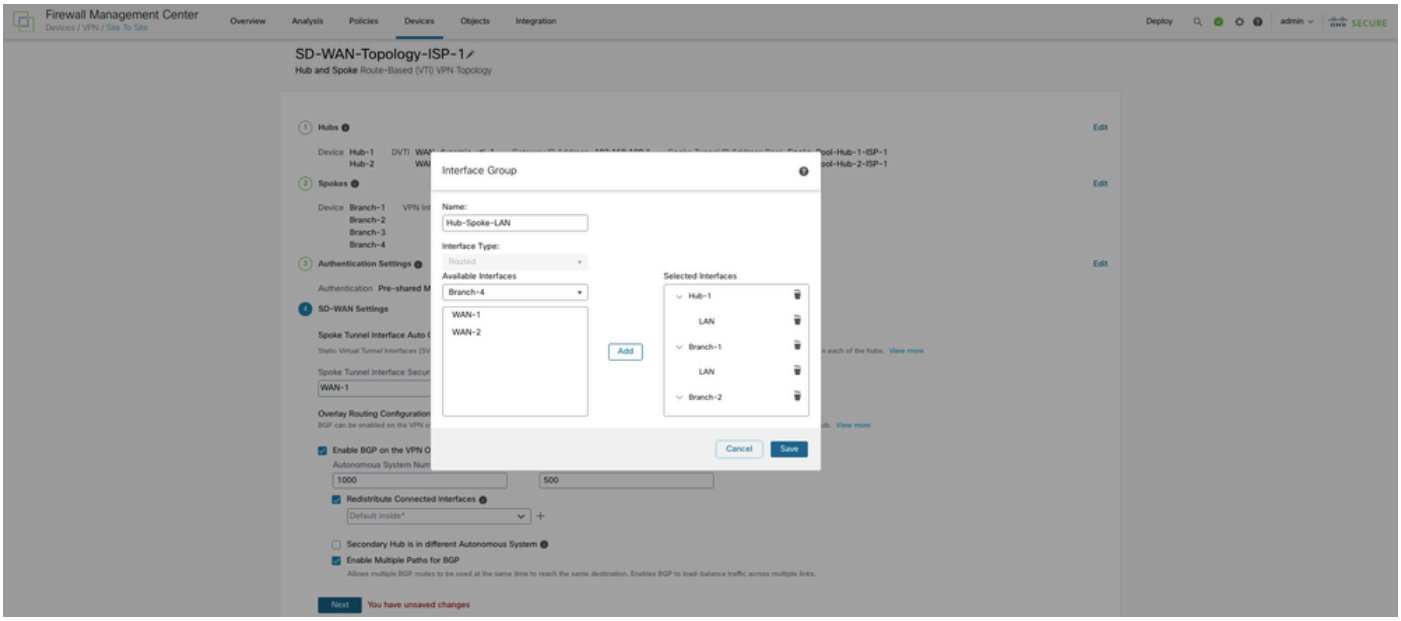
选择Next以配置Authentication Settings。对于设备身份验证，您可以在Authentication Type下拉列表中选择手动预共享密钥、自动生成的预共享密钥或证书。从转换集和IKEv2策略下拉列表中选择一个或多个算法。



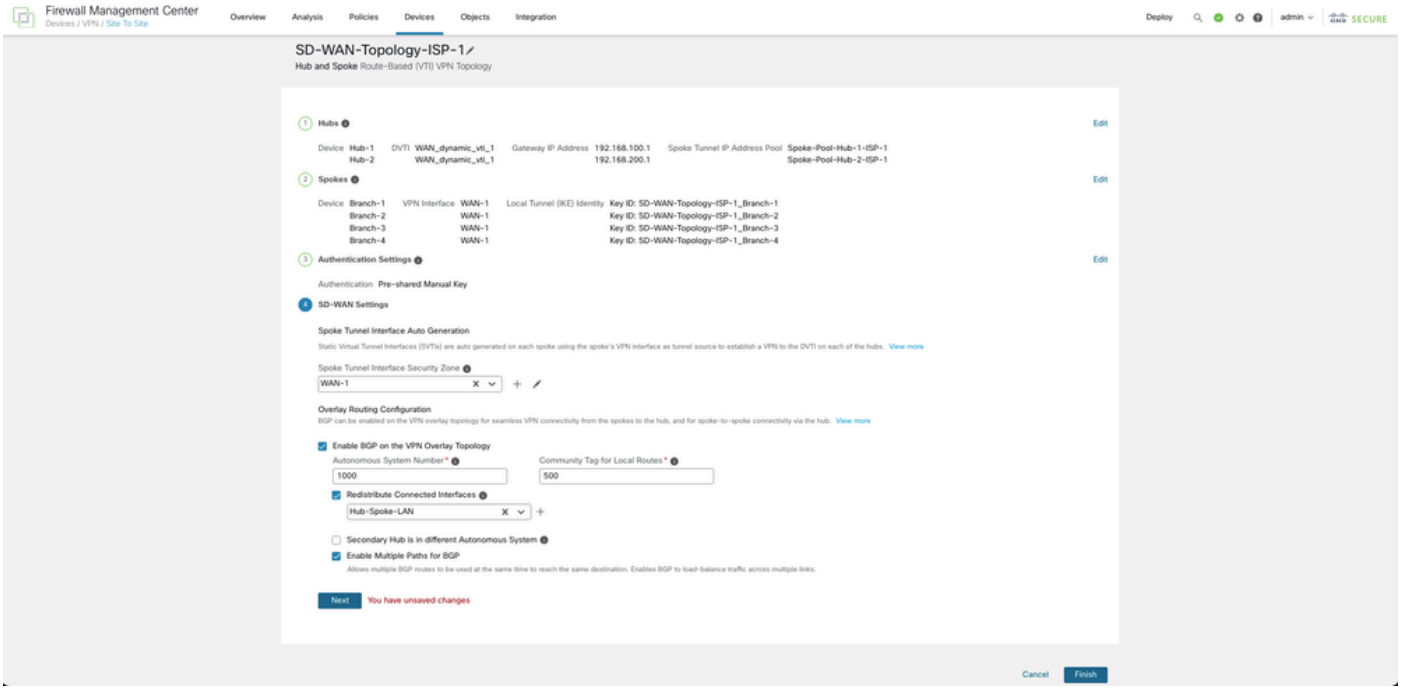
步骤6.配置SD-WAN设置

选择下一步以配置SD-WAN设置。此步骤涉及分支隧道接口的自动生成以及重叠网络的BGP配置。从Spoke Tunnel Interface Security Zone下拉列表中，选择安全区域或选择+以创建安全区域，向导会自动将分支的自动生成的静态虚拟隧道接口(SVTI)添加到安全区域。

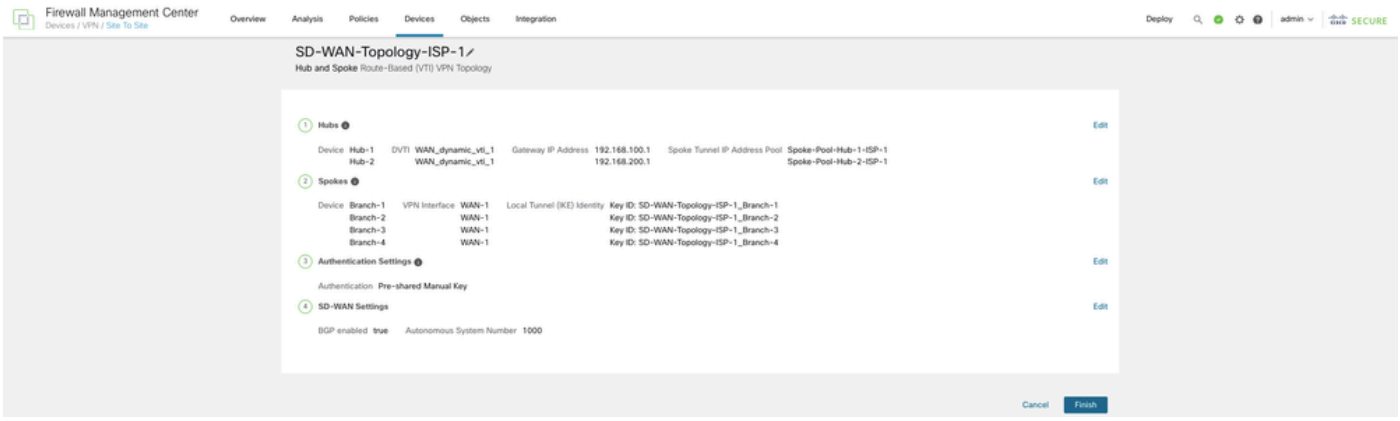
选中在VPN重叠拓扑上启用BGP复选框以自动执行重叠隧道接口之间的BGP配置。在自主系统编号字段中，输入自主系统(AS)编号。选中Redistribute Connected Interfaces复选框，然后从下拉列表中选择接口组，或选择+，使用集线器的已连接LAN接口和分支创建一个接口组，以便在重叠拓扑中重分配BGP路由。



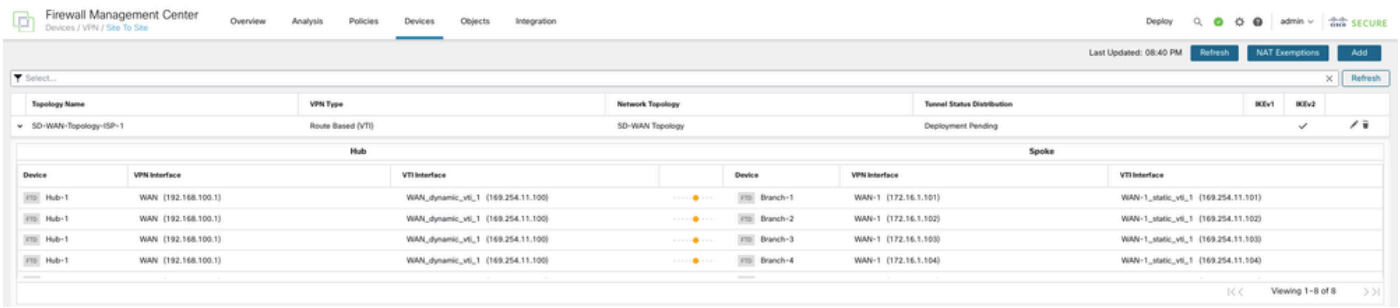
在Community Tag for Local Routes字段中，输入BGP社区属性以标记已连接和重分发的本地路由。此属性可实现轻松的路由过滤。如果不同AS中有一个辅助集线器，请选中Secondary Hub is in the Different Autonomous System复选框。最后，选中Enable Multiple Paths for BGP复选框，以启用BGP在多个链路之间对流量进行负载均衡。



单击Finish保存并验证SD-WAN拓扑。

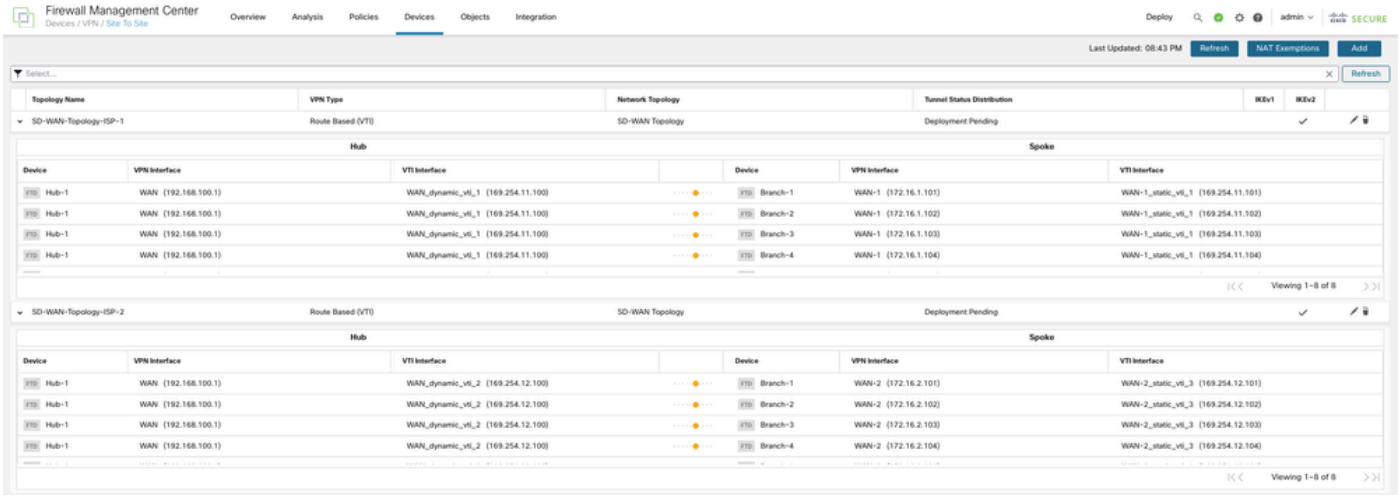


您可以在Devices > Site-to-site VPN下查看拓扑。第一个SD-WAN拓扑中的隧道总数为8。



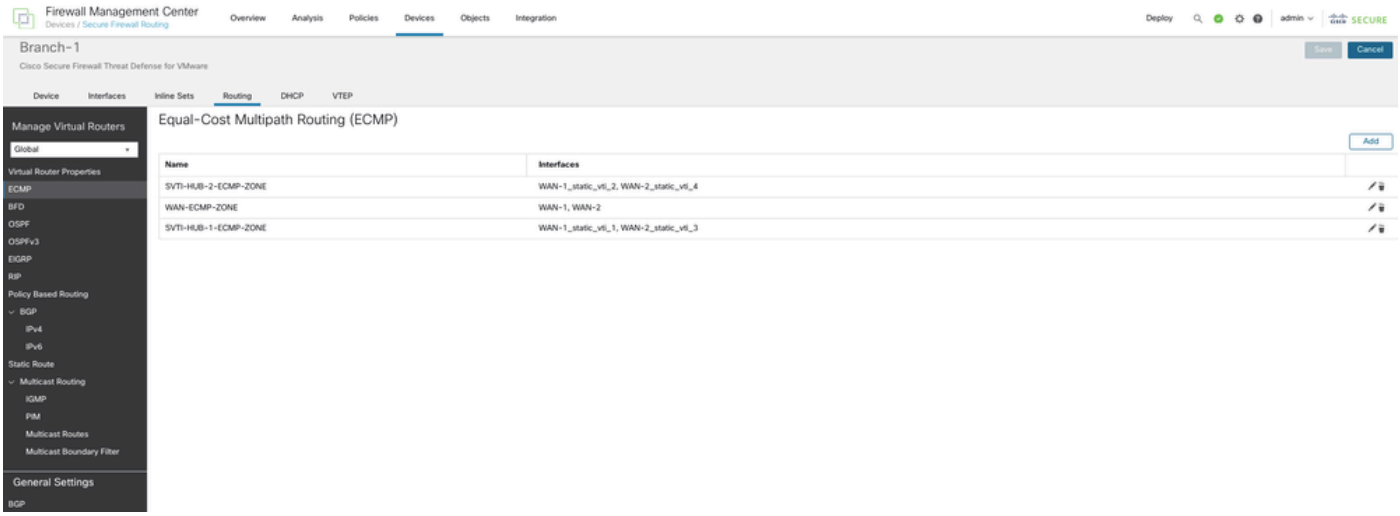
步骤7.创建以WAN-2作为VPN接口的SD-WAN拓扑

重复步骤1至6，配置以WAN-2作为VPN接口的SD-WAN拓扑。第二个SD-WAN拓扑中的隧道总数为8。最终的拓扑必须如下所示。



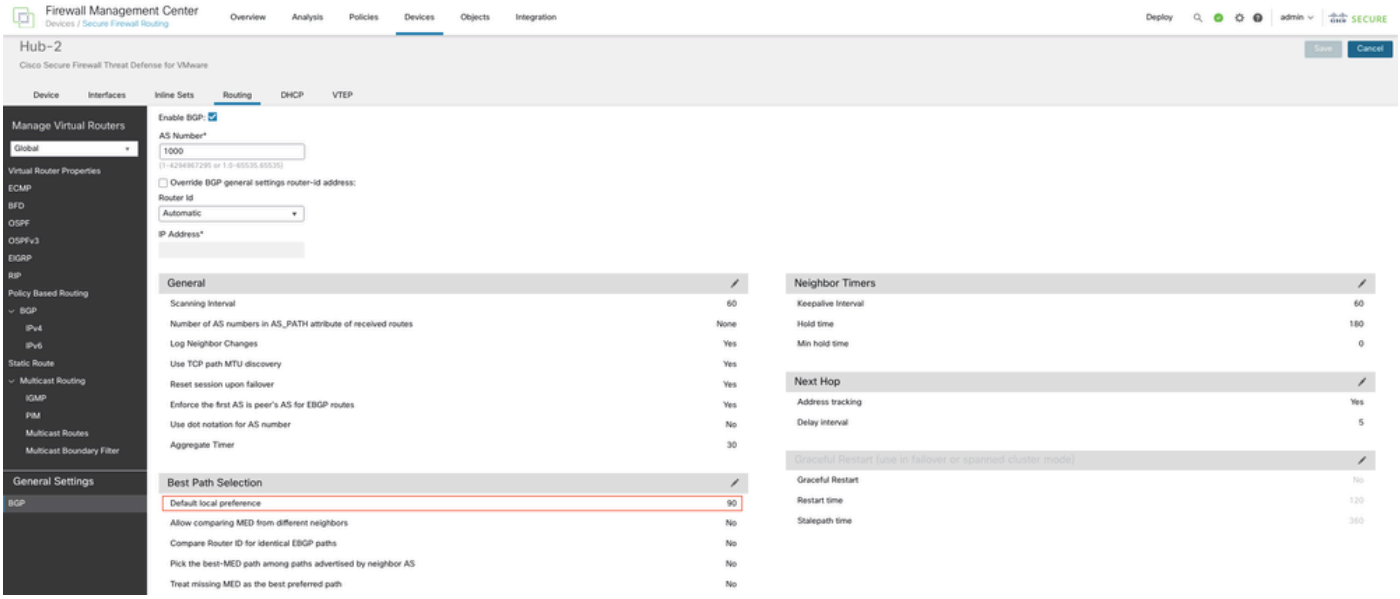
步骤8.配置ECMP区域

在每个分支上，导航到Routing > ECMP，并为连接到主集线器和辅助集线器的WAN接口和SVTI配置ECMP（等价多路径）区域，如下所示。这可以提供链路冗余并启用VPN流量的负载均衡。



步骤9.修改集线器上的BGP本地首选项

在辅助集线器上导航到Routing > General Settings > BGP。选择Enable BGP，配置AS Number，并将Best Path Selection下的默认本地首选项值设置为小于在主集线器上配置的值。选择Save。这可确保首选通往主集线器的路由，而不是通往辅助集线器的路由。当主集线器关闭时，通往辅助集线器的路由将接管其工作。

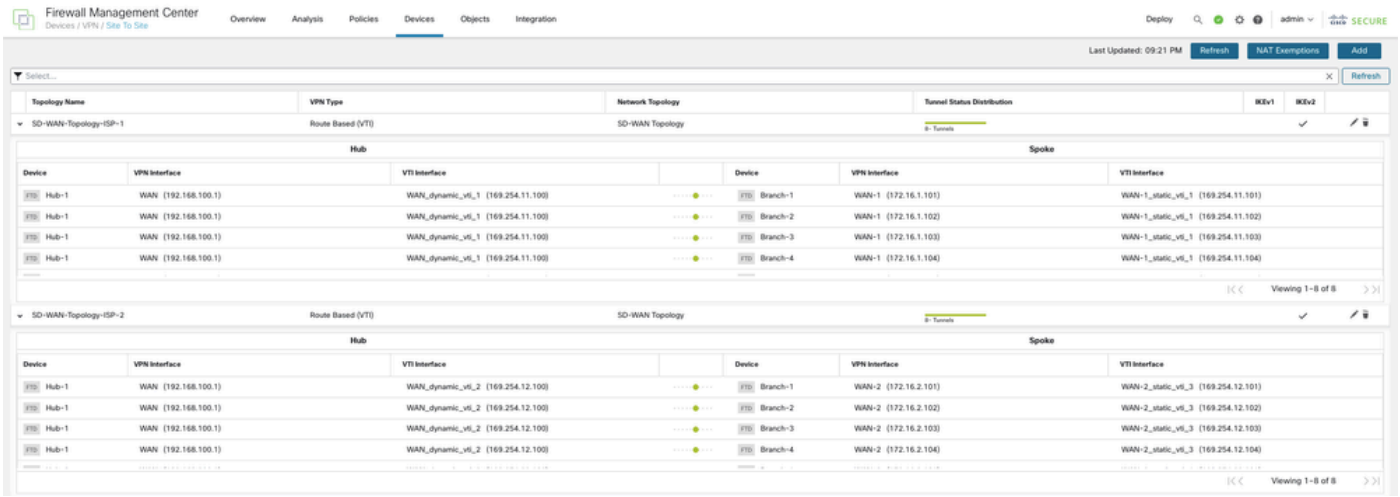


将配置部署到所有设备。

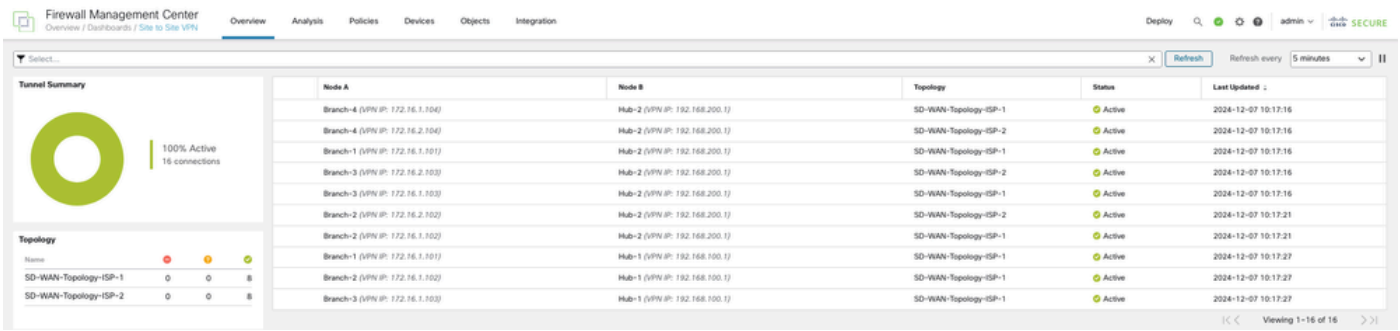
验证

验证隧道状态

要验证SD-WAN拓扑的VPN隧道是否已启用，请选择Device > VPN > Site-to-Site。

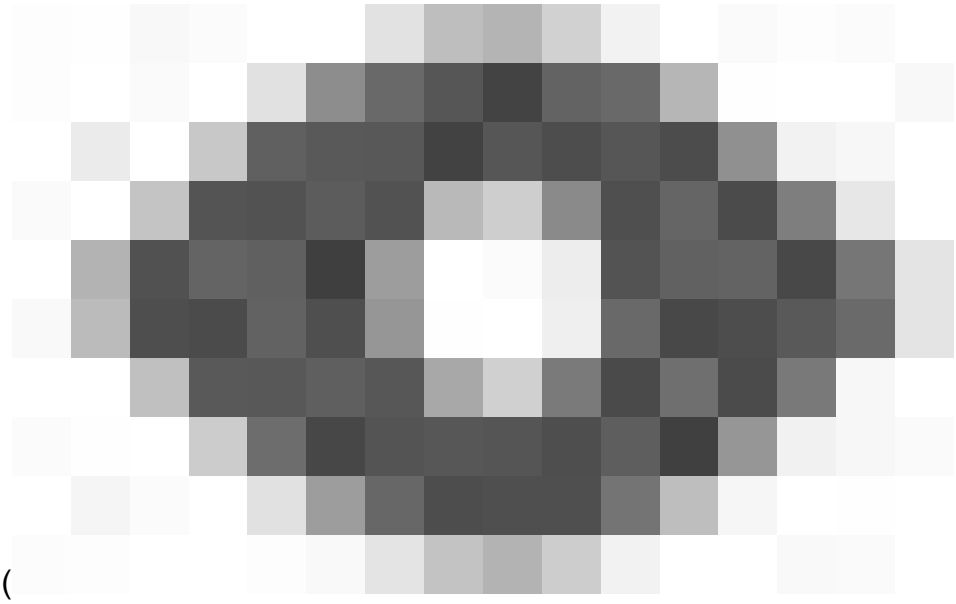


要查看SD-WAN VPN隧道的详细信息，请选择Overview > Dashboards > Site-to-site VPN。



要查看每个VPN隧道的详细信息，请执行以下操作：

1. 将鼠标悬停在隧道上。



2. 选择View Full Information(
)图标。系统将显示一个包含隧道详细信息和其他操作的窗格。

3. 选择侧窗格中的CLI Details选项卡以查看show命令和IPsec安全关联的详细信息。

A: Branch-1 ⟷ B: Hub-1

Topology: SD-WAN-Topology-ISP-2 | Status: Active

General | CLI Details | Packet Tracer

Refresh | Maximize view

Summary

Node A (172.16.2.101/500)		Node B (192.168.100.1/500)	
Transmitted:	8.46 KB (8664 B)	Transmitted:	5.98 KB (6123 B)
Received:	27.73 KB (28400 B)	Received:	7.68 KB (7868 B)

IPsec Security Associations (2)

0.0.0.0/0.0.0.0/0/0		0.0.0.0/0.0.0.0/0/0	
Settings:	L2L,Tunnel,IKEv2,...	Settings:	L2L,Tunnel,IKEv2,VTI
Encaps/Encrypt:	140 / 140 pkts	Encaps/Encrypt:	92 / 92 pkts
Dcaps/Decrypt:	232 / 232 pkts	Dcaps/Decrypt:	96 / 96 pkts

Remaining Lifetime for SPI ID: 0x5B2983A9

Outbound:	3.69 GB (3962871000 B) 12:47:26 (26246 sec)	Inbound:	3.65 GB (3916794000 B) 12:50:26 (26426 sec)

Remaining Lifetime for SPI ID: 0x0F4EA9C0

Inbound:	3.99 GB (4285416000 B) 12:47:26 (26246 sec)	Outbound:	3.69 GB (3962874000 B) 12:50:26 (26426 sec)

0.0.0.0/0.0.0.0/0/0		
Settings:	L2L,Tunnel,IKEv2,...	
Encaps/Encrypt:	96 / 96 pkts	Info is not available for Extranet device
Dcaps/Decrypt:	92 / 92 pkts	

Remaining Lifetime for SPI ID: 0x1DEFCB21

Outbound:	4.03 GB (4331514000 B) 12:50:25 (26425 sec)	Inbound:	No data

Remaining Lifetime for SPI ID: 0x53B1AE47

Inbound:	3.65 GB (3916794000 B) 12:50:25 (26425 sec)	Outbound:	No data

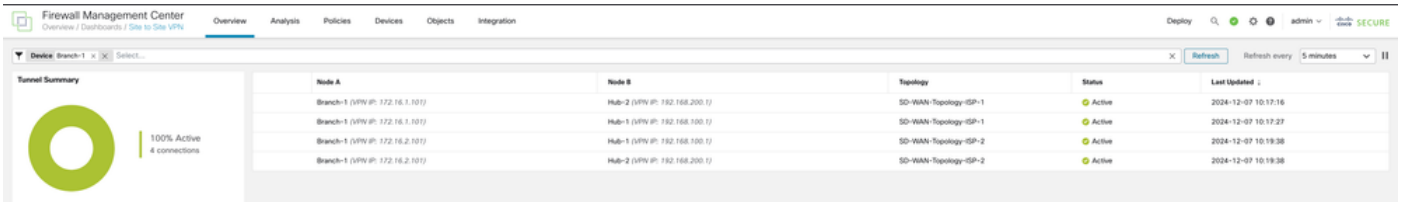
Branch-1 (VPN Interface IP: 172.16.2.101)

```
show crypto ipsec sa peer 192.168.100.1
```

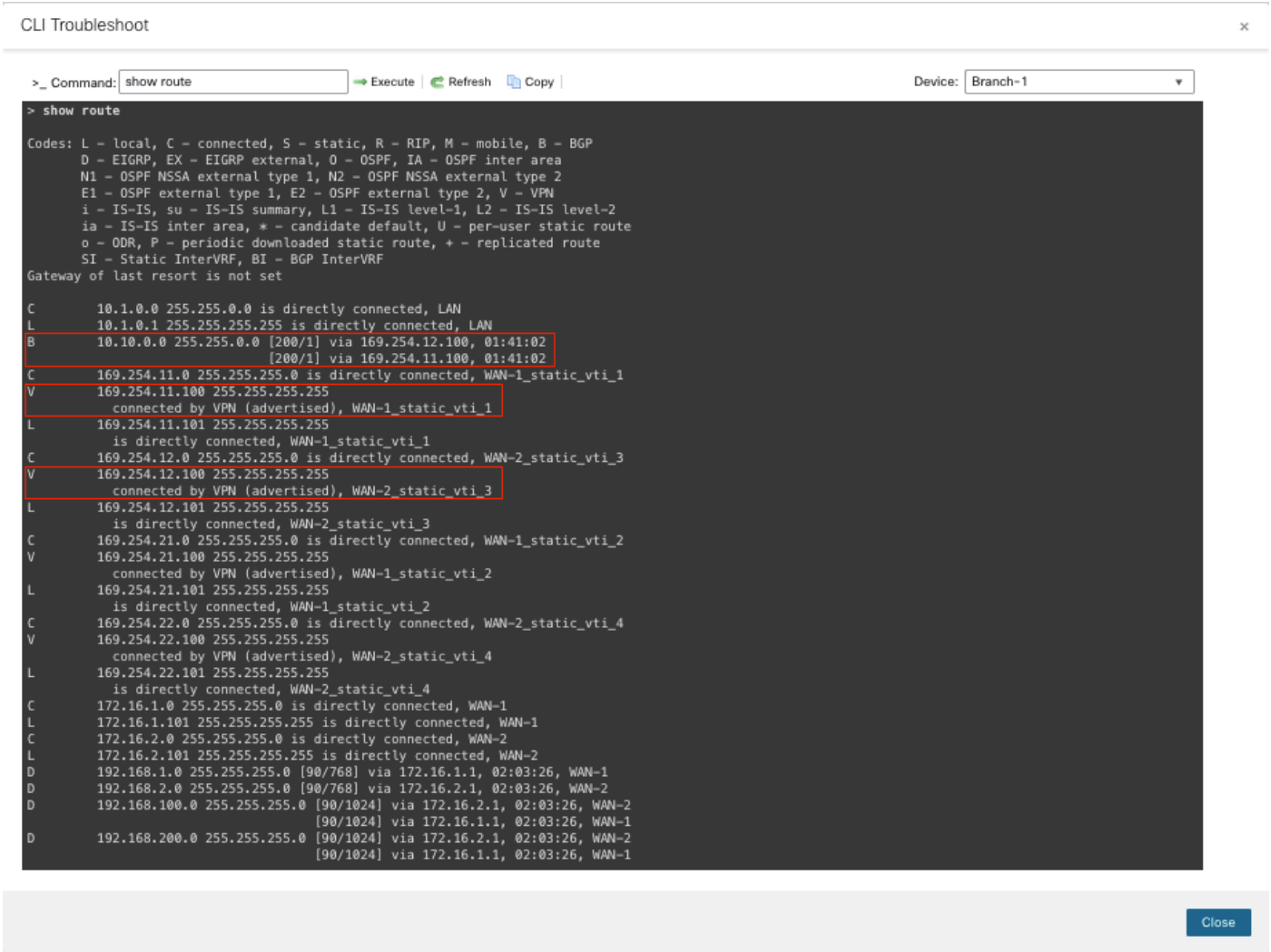
WAN-2_static_vti_3 - SVTI通过ISP 2连接到集线器1
WAN-1_static_vti_2 - SVTI通过ISP 1连接到集线器2
WAN-2_static_vti_4 - SVTI通过ISP 2连接到集线器2

检验VPN流量的负载均衡

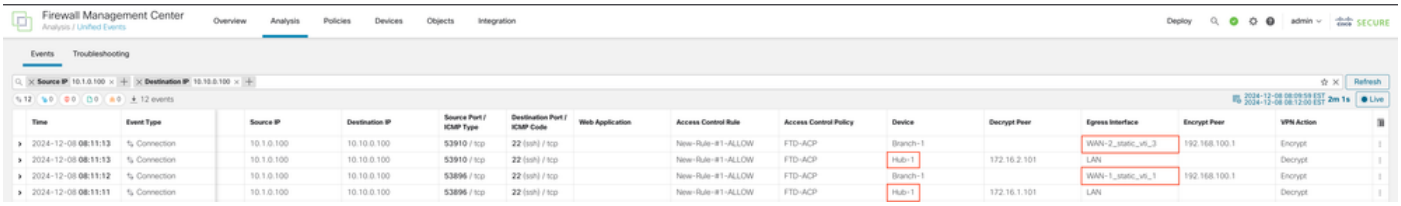
在Site to Site VPN控制面板中可以查看隧道状态。理想情况下，所有隧道都必须处于活动状态：



首选到主集线器的路由。Branch 1上的show route命令表明，VPN流量在ISP 1和ISP 2上的两个SVTI之间负载均衡到主集线器：

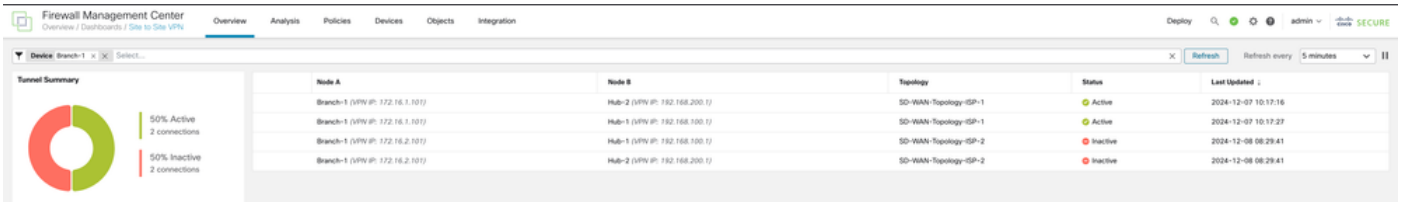


在Unified Events中可以看到为实际VPN流量所采用的出口接口



检验双ISP冗余

当ISP-2关闭时，隧道状态表明通过ISP-1的隧道处于活动状态：



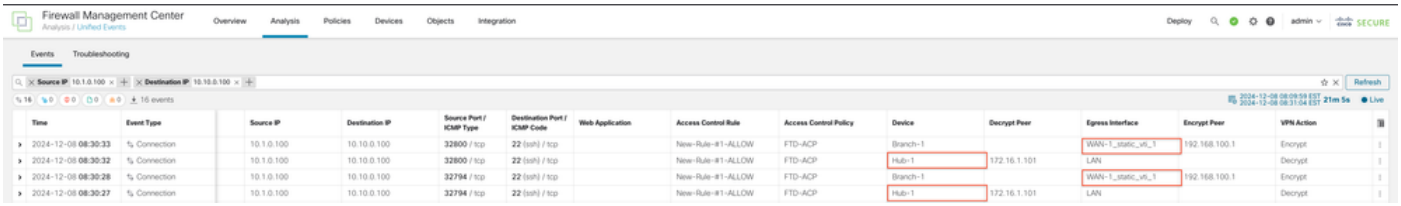
首选到主集线器的路由。Branch 1上的show route命令表明VPN流量通过ISP-1上的SVTI路由到主集线器：

CLI Troubleshoot

>_ Command: show route | Execute | Refresh | Copy | Device: Branch-1

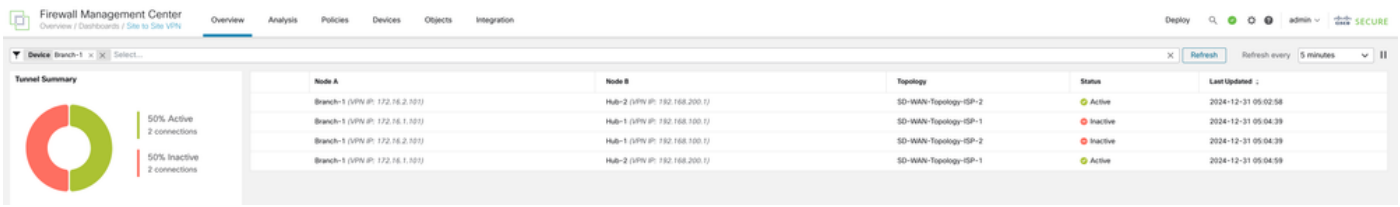
```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        10.1.0.0 255.255.0.0 is directly connected, LAN
L        10.1.0.1 255.255.255.255 is directly connected, LAN
B        10.10.0.0 255.255.0.0 [200/1] via 169.254.11.100, 00:04:02
C        169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V        169.254.11.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_1
L        169.254.11.101 255.255.255.255
           is directly connected, WAN-1_static_vti_1
C        169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V        169.254.21.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_2
L        169.254.21.101 255.255.255.255
           is directly connected, WAN-1_static_vti_2
C        172.16.1.0 255.255.255.0 is directly connected, WAN-1
L        172.16.1.101 255.255.255.255 is directly connected, WAN-1
D        172.16.2.0 255.255.255.0 [90/1280] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 22:12:57, WAN-1
D        192.168.2.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
```

在Unified Events中可以看到为实际VPN流量所采用的出口接口

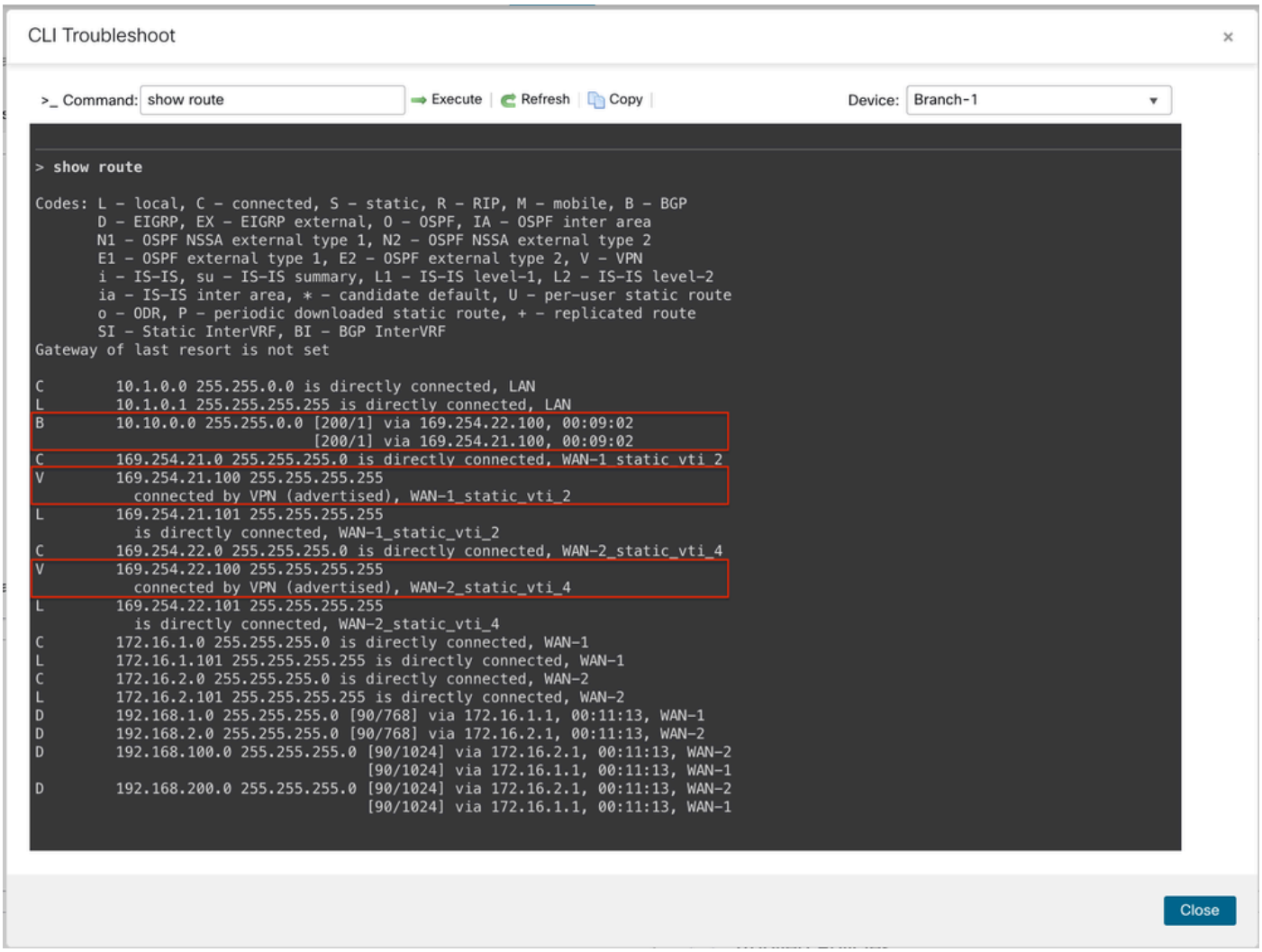


检验中心级冗余

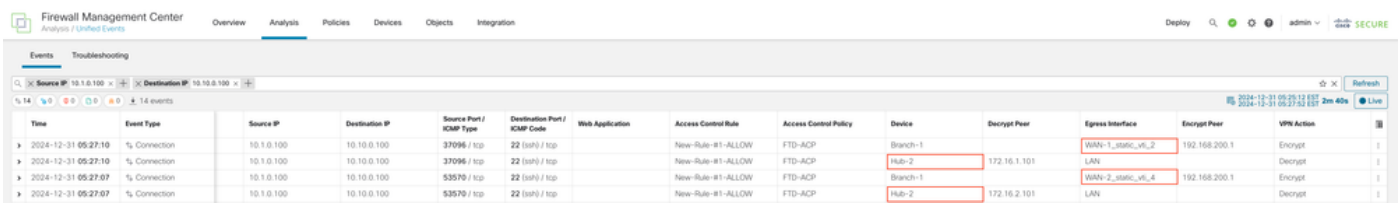
当主集线器关闭时，隧道状态表明通向辅助集线器的隧道处于活动状态：



由于主集线器已关闭，因此首选通往辅助集线器的路由。Branch 1上的show route命令表明，VPN流量在ISP 1和ISP 2上的两个SVTI之间负载均衡到辅助集线器：



在Unified Events中可以看到为实际VPN流量所采用的出口接口



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）。