Configurar a topologia ISP dupla com dois hubs e quatro spokes na mesma região

Contents

Introdução

Este documento descreve como configurar uma topologia ISP dupla com dois hubs e quatro spokes na mesma região usando o assistente de SD-WAN.

Pré-requisitos

Plataformas de software e hardware suportadas

Gerenciador	FTD	Plataformas suportadas
• FMC >= 7.6.0 e FMC REST API	• FTD de Hub >= 7.6.0 • FTD spoke >= 7,3,0	Todas as plataformas que o FMC >= 7.6.0 pode gerenciar

• cdFMC >= 7.6.0 • FDM - Sem Suporte		

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças do Cisco Secure Firewall
- Cisco Secure Firewall Management Center
- WAN definida por software (SD-WAN)

Componentes Utilizados

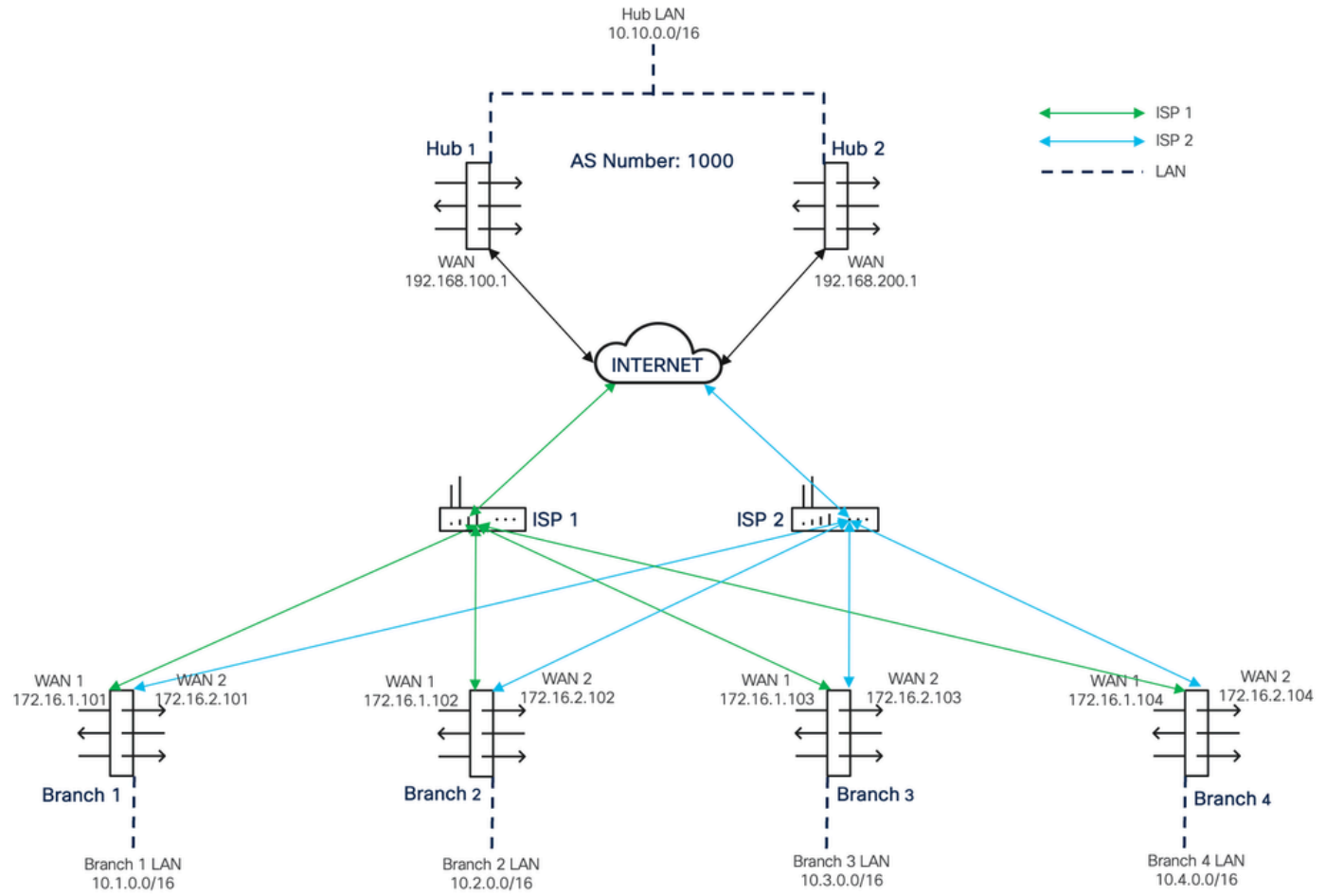
As informações neste documento são baseadas nestas versões de software e hardware:

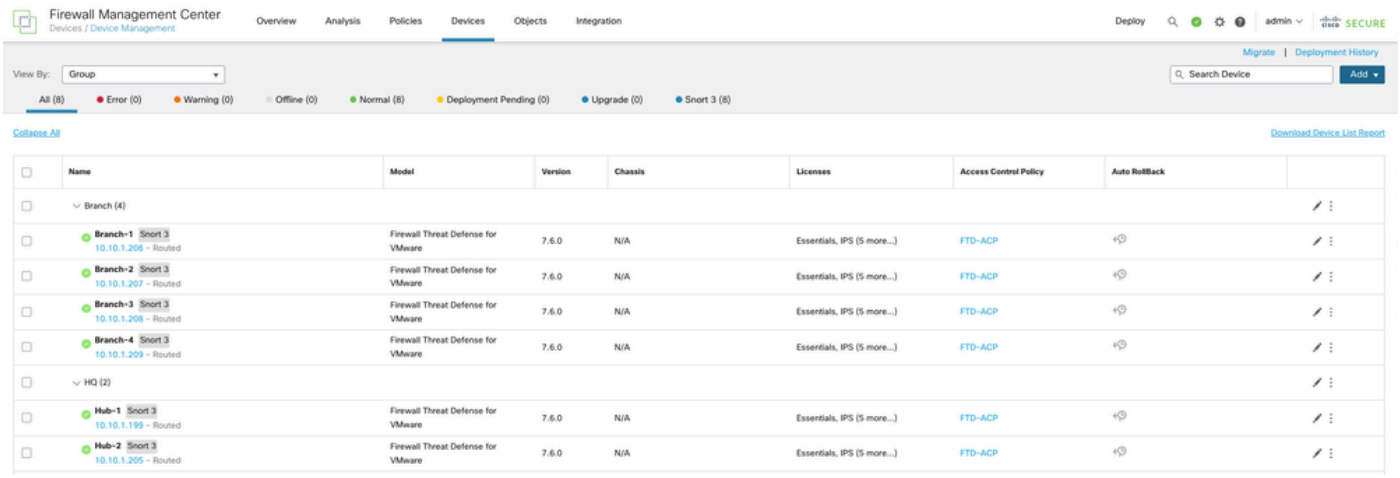
- FTD versão 7.6.0
- FMC versão 7.6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

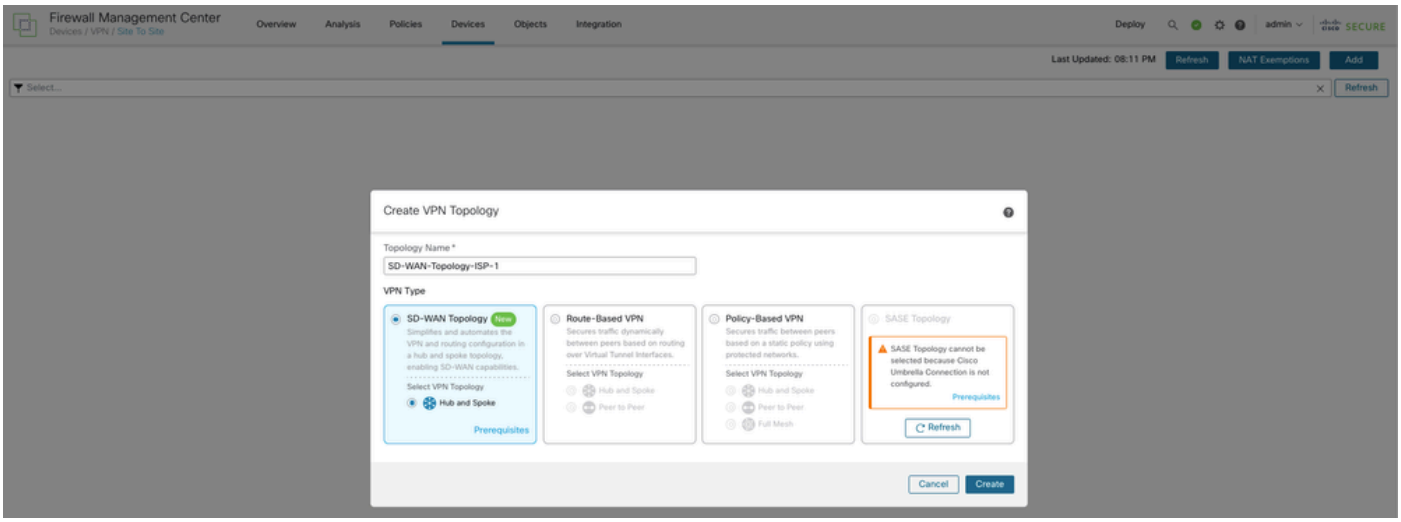
Diagrama de Rede





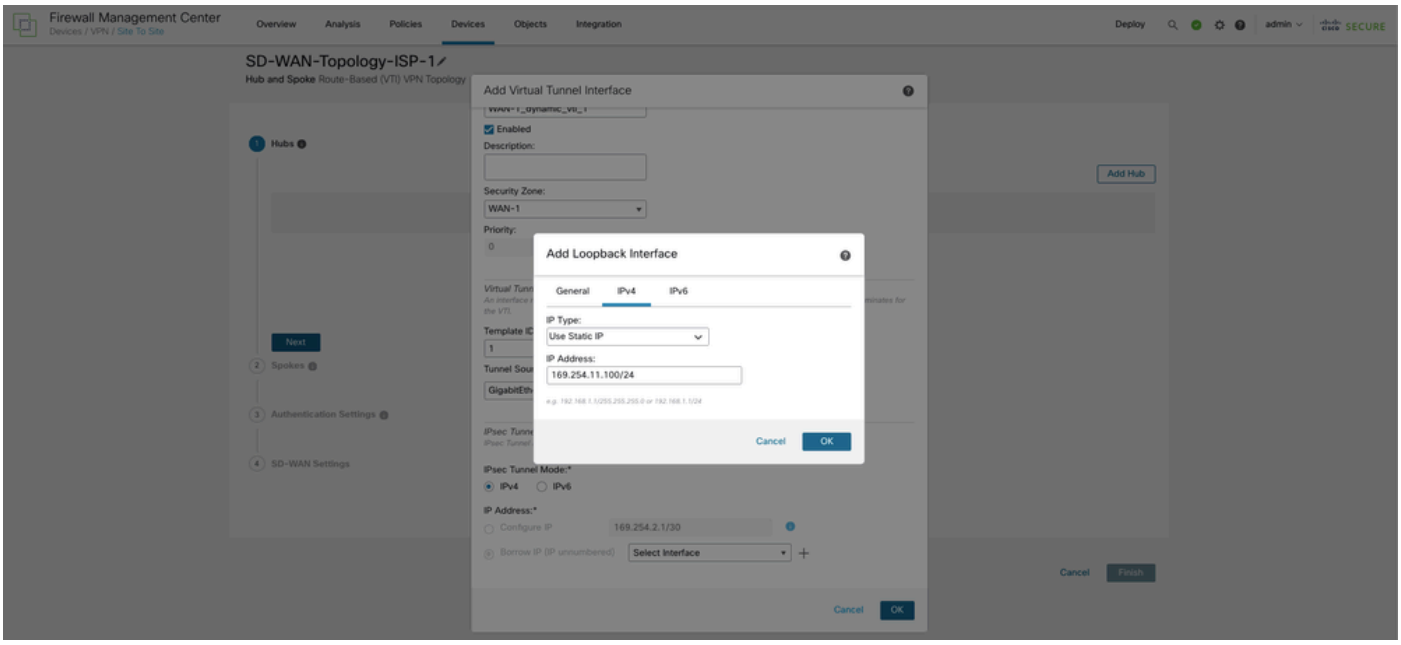
Etapa 1. Criar uma topologia SD-WAN com WAN-1 como a interface VPN

Navegue até Devices > VPN > Site To Site. Selecione Add e insira um nome adequado no campo Topology Name para a primeira topologia com WAN-1 como a interface VPN. Escolha SD-WAN Topology e selecione Create.

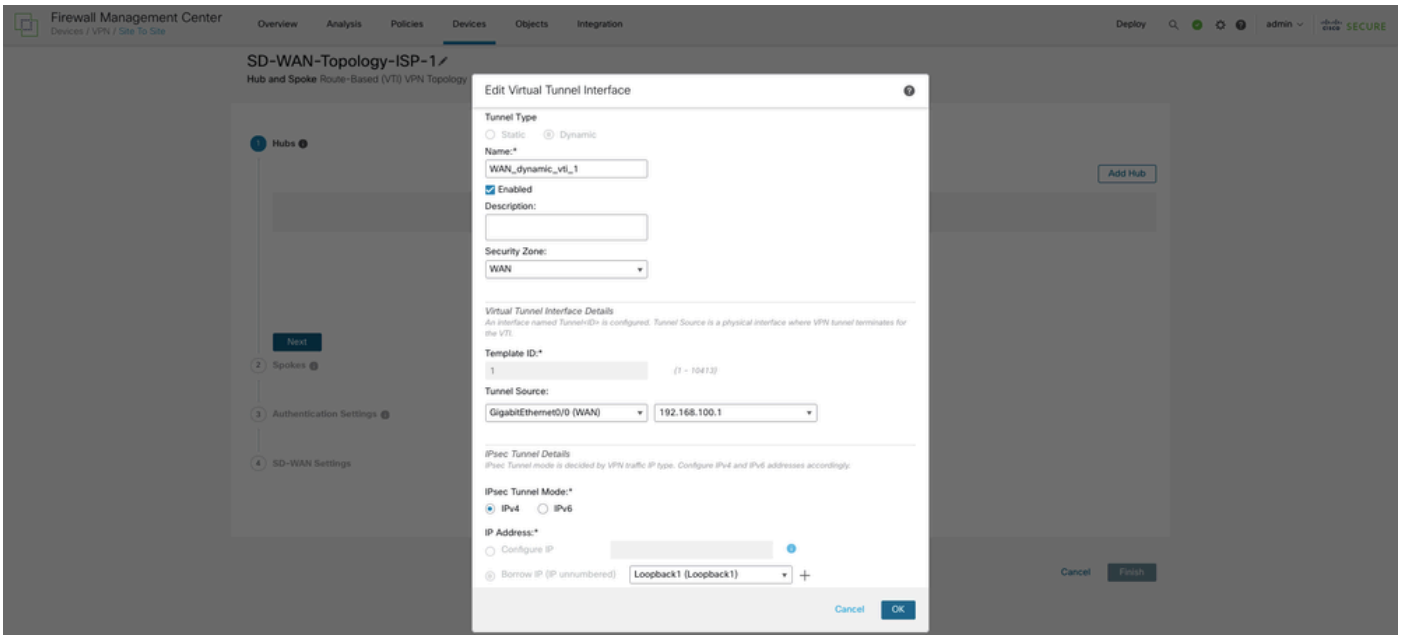


Etapa 2. Configurar o Dynamic Virtual Tunnel Interface (DVTI) no hub principal

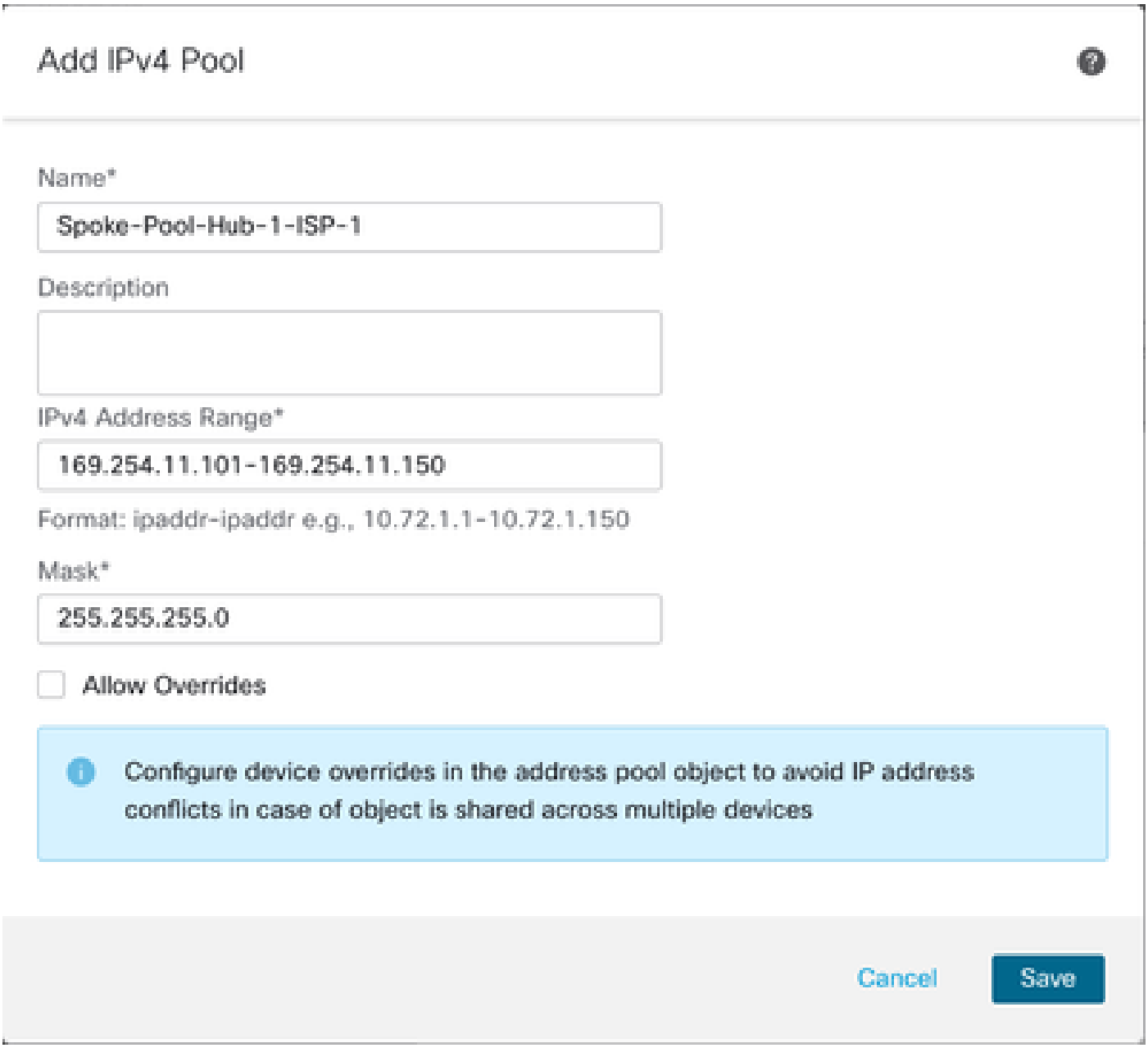
Selecione Add Hub e escolha o hub principal na lista suspensa Device. Selecione o ícone + ao lado de Dynamic Virtual Tunnel Interface (DVTI). Configure um nome, zona de segurança e ID de modelo e atribua WAN-1 como a interface Tunnel Source para o DVTI.



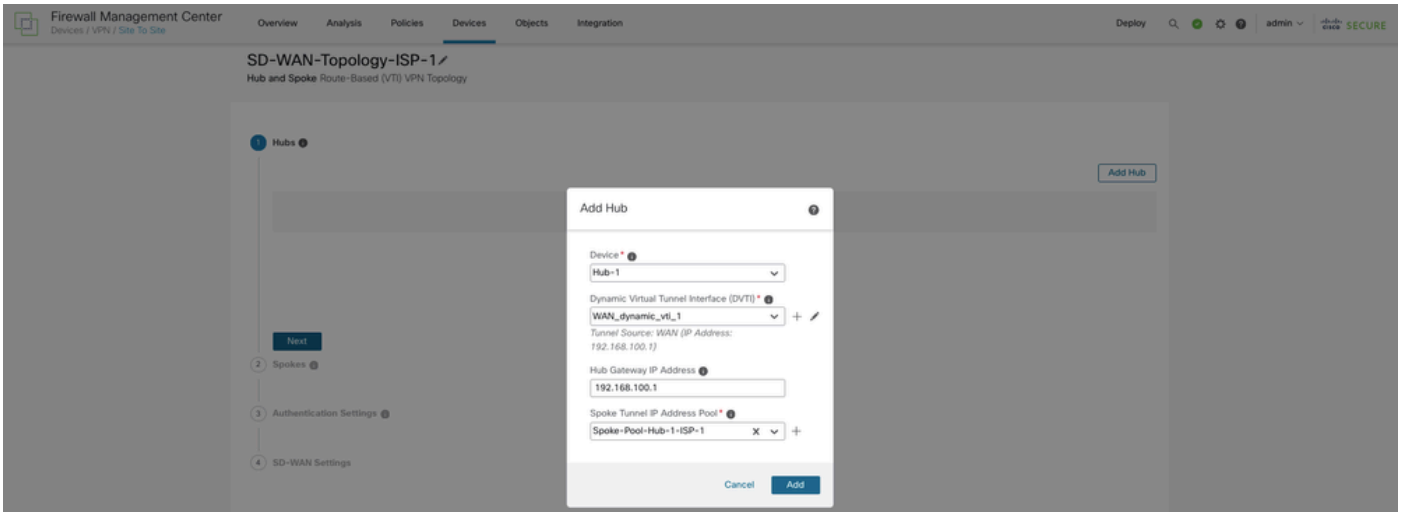
Escolha uma interface física ou de loopback na lista suspensa IP emprestado. Na topologia atual, o DVTI herda um endereço IP de interface de loopback. Selecione OK.



Escolha um pool de endereços ou selecione o ícone + ao lado de Spoke Tunnel IP Address Pool para criar um novo pool de endereços. Quando você adiciona spokes, o assistente gera automaticamente interfaces de túnel spoke e atribui endereços IP a essas interfaces spoke a partir desse pool de endereços IP.

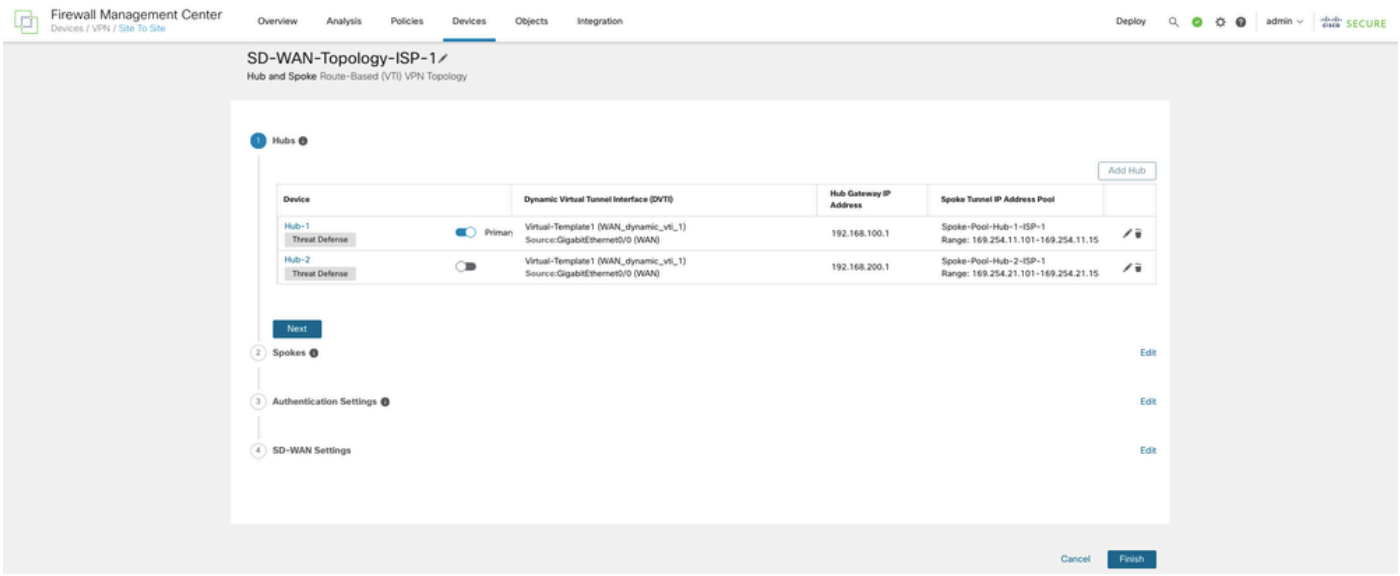


Quando a configuração do hub principal estiver concluída, selecione Add para salvar o hub principal na topologia.



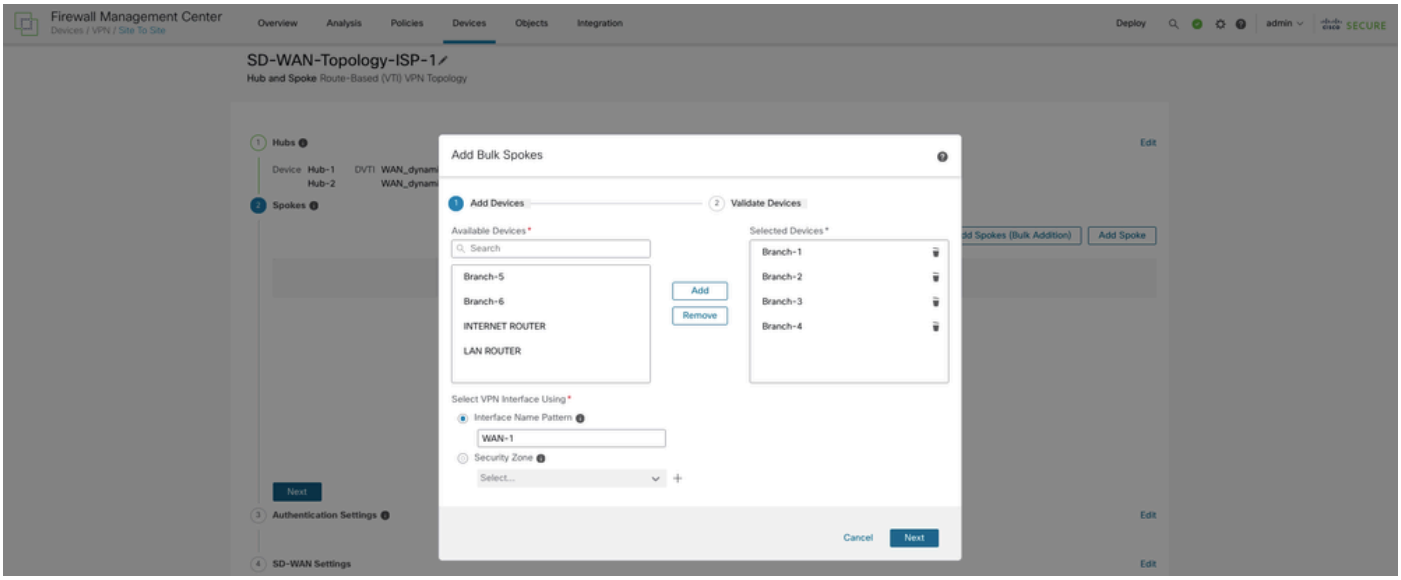
Etapa 3. Configurar o Dynamic Virtual Tunnel Interface (DVTI) no hub secundário

Agora selecione Add Hub novamente para configurar o hub secundário na topologia com WAN-1 como a interface VPN repetindo as etapas 1 e 2. Selecione Next.

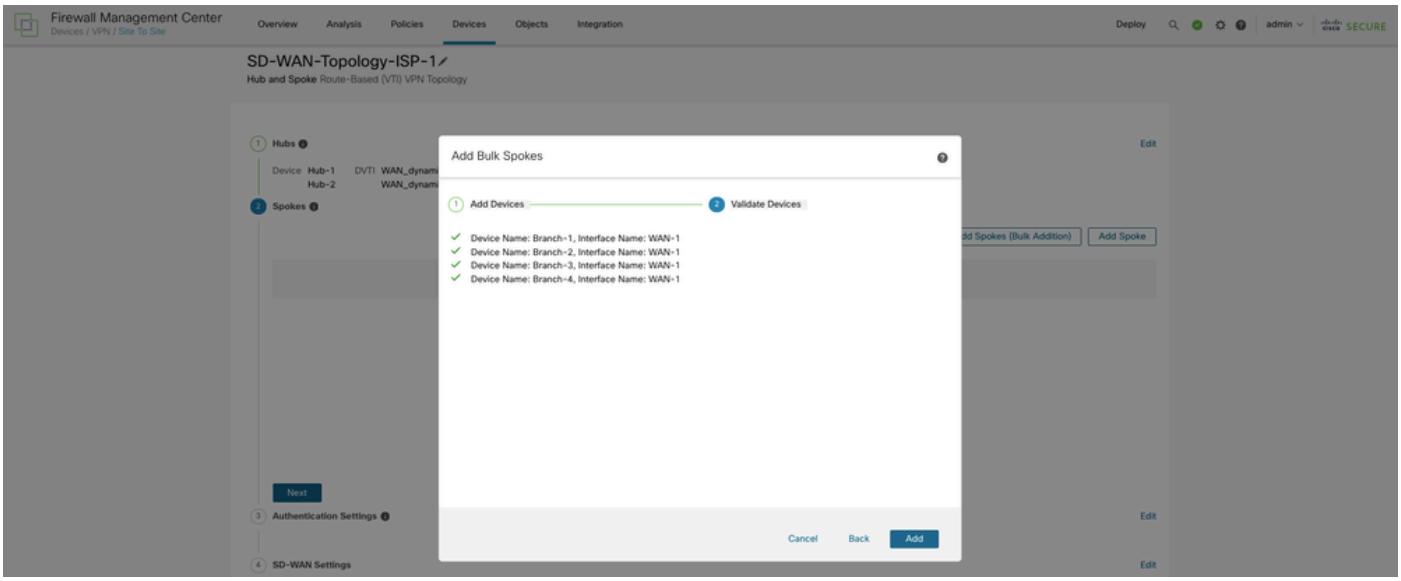


Etapa 4. Configurar os raios

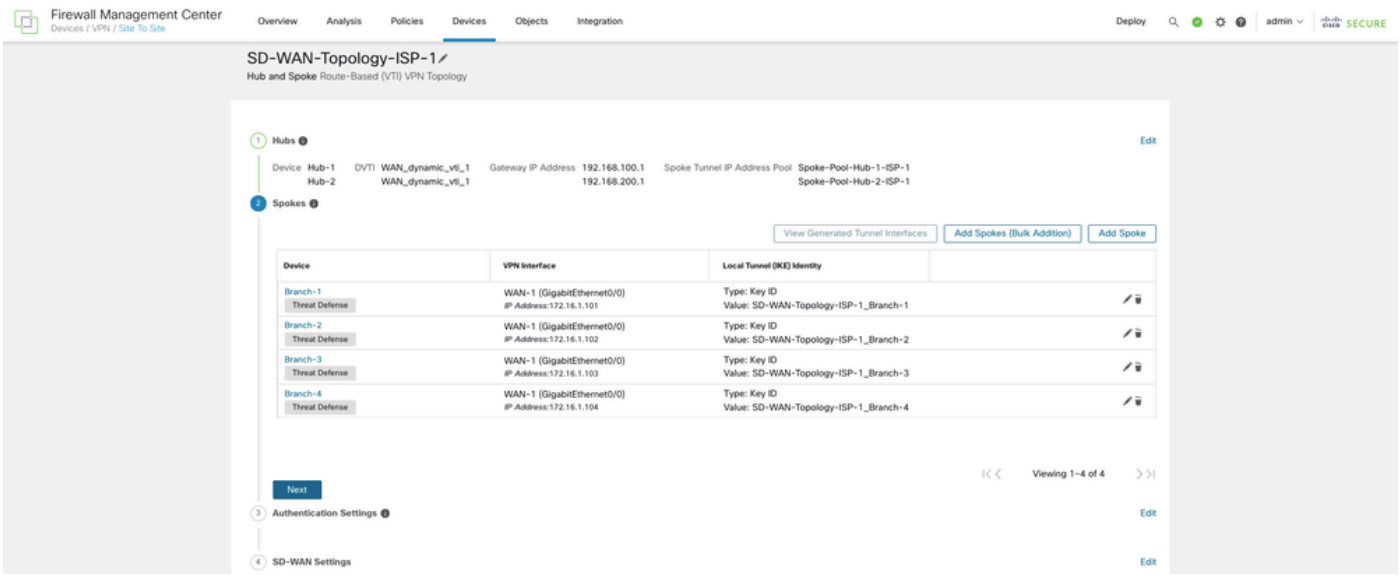
Selecione Add Spoke para adicionar um único dispositivo spoke ou clique em Add Spokes (Bulk Addition) para adicionar vários spokes à sua topologia. A topologia atual usa a última opção para adicionar vários FTDs de filial à topologia. Na caixa de diálogo Add Bulk Spokes, selecione os FTDs necessários para adicionar como spokes. Selecione um Padrão de Nome de Interface comum que corresponda ao nome lógico de WAN-1 em todos os spokes ou a Zona de Segurança associada à WAN-1.



Selecione Avançar para que o assistente valide se os spokes têm interfaces com o padrão especificado ou a zona de segurança.

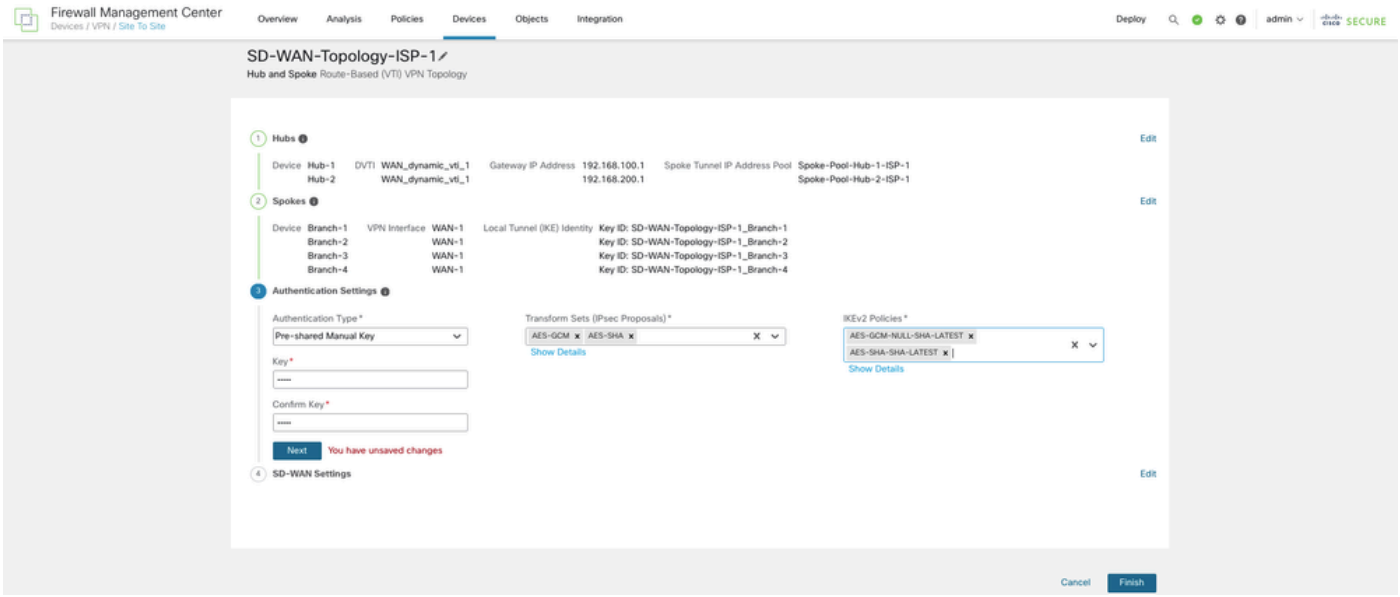


Selecione Add e o assistente selecionará automaticamente o hub DVTI como o endereço IP origem do túnel para cada spoke.



Etapa 5. Configurar as Definições de Autenticação

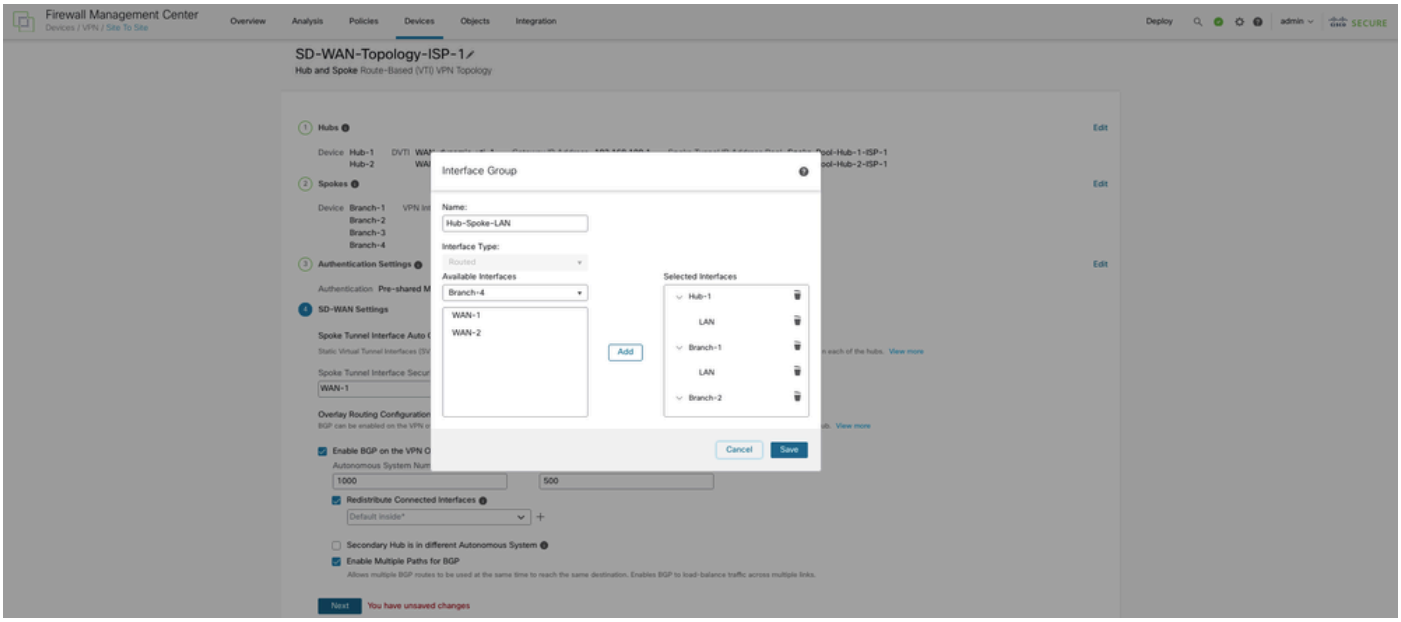
Selecione Avançar para definir as Configurações de autenticação. Para a autenticação do dispositivo, você pode selecionar uma chave pré-compartilhada manual, uma chave pré-compartilhada gerada automaticamente ou um certificado na lista suspensa Authentication Type. Escolha um ou mais algoritmos nas listas suspensas Transform Sets e IKEv2 Policies.



Etapa 6. Definir as configurações de SD-WAN

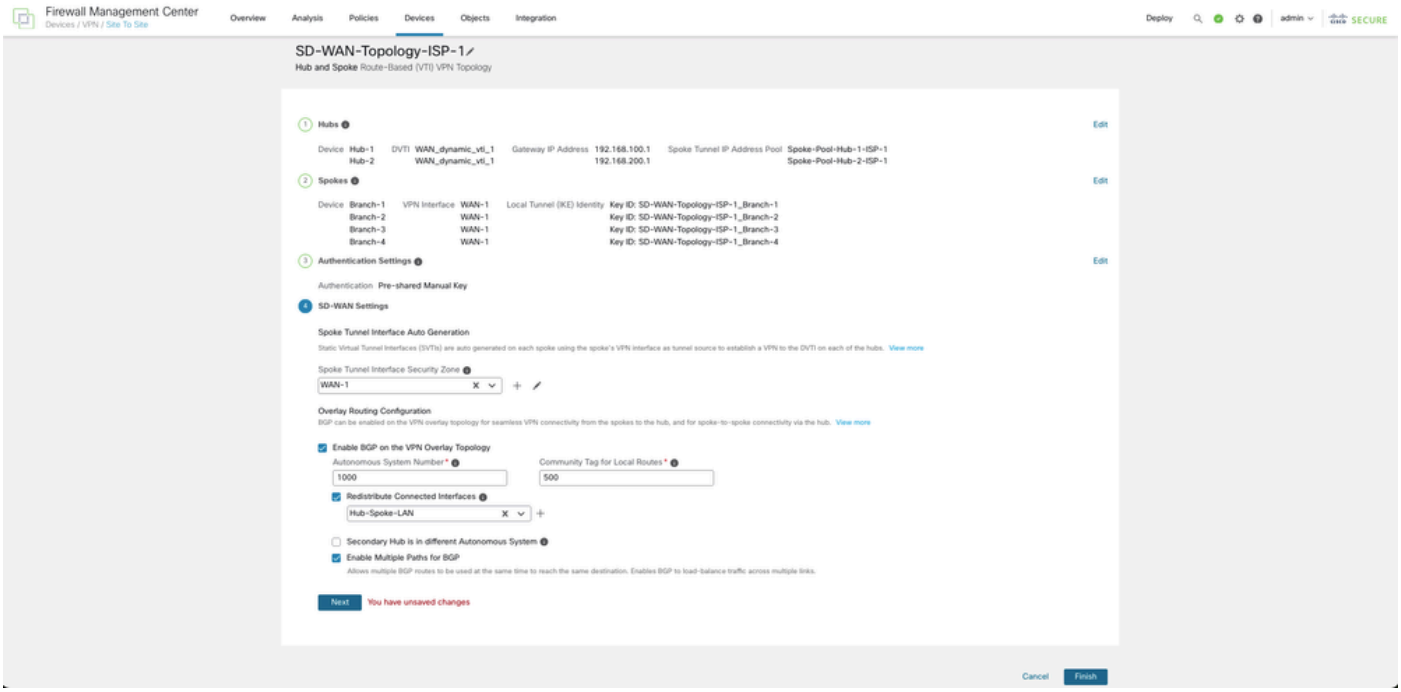
Selecione Next para configurar Configurações de SD-WAN. Essa etapa envolve a geração automática de interfaces de túnel spoke e a configuração BGP da rede de sobreposição. Na lista suspensa Spoke Tunnel Interface Security Zone, escolha uma zona de segurança ou selecione + para criar uma zona de segurança à qual o assistente adiciona automaticamente as interfaces de túnel virtual estático (SVTIs) geradas automaticamente pelos spokes.

Marque a caixa de seleção Enable BGP on the VPN Overlay Topology para automatizar as configurações do BGP entre a interface de túnel de sobreposição. No campo Autonomous System Number, insira um número de Autonomous System (AS). Marque a caixa de seleção Redistribute Connected Interfaces e escolha um grupo de interface na lista suspensa ou selecione + para criar um grupo de interface com interfaces LAN conectadas dos hubs e spokes para redistribuição de rota BGP na topologia de sobreposição.

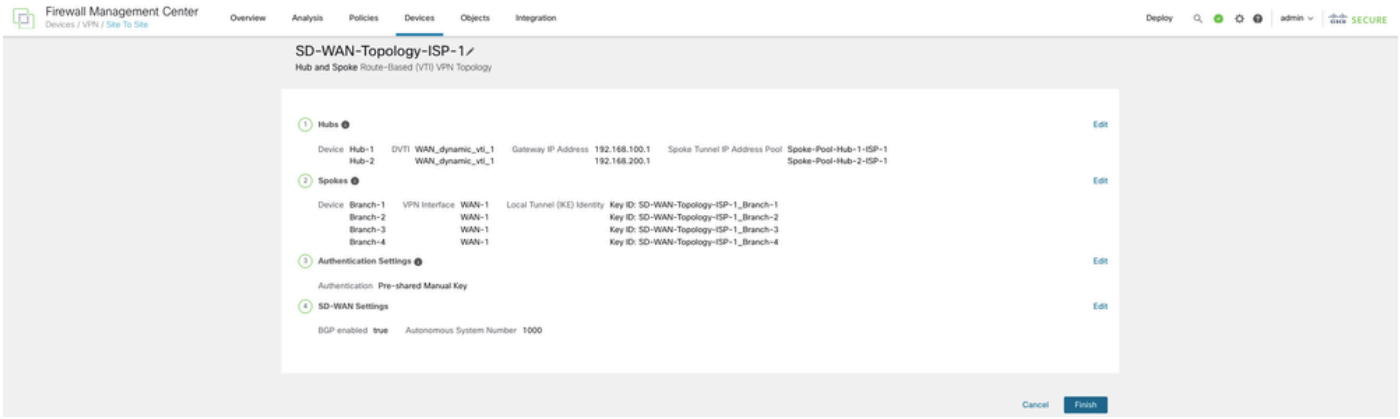


No campo Community Tag for Local Routes, insira o atributo de comunidade BGP para marcar

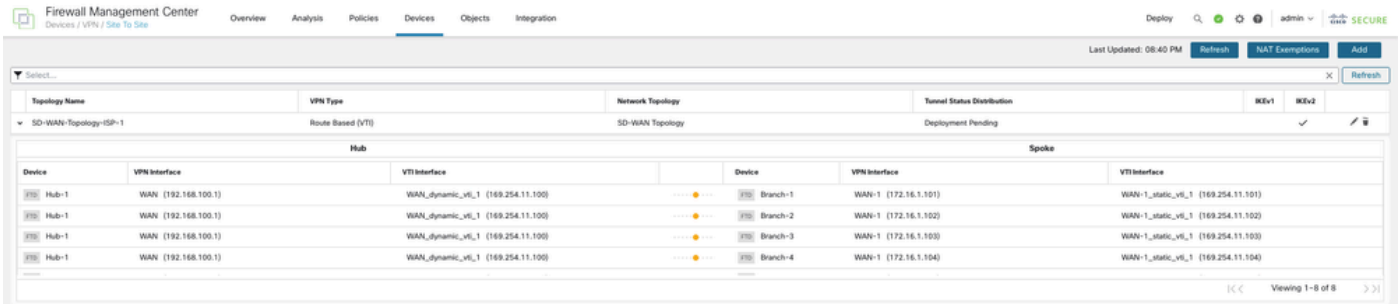
rotas locais conectadas e redistribuídas. Este atributo permite uma filtragem de rota fácil. Marque a caixa de seleção O hub secundário está no sistema autônomo diferente se você tiver um hub secundário em um AS diferente. Por fim, marque a caixa de seleção Enable Multiple Paths for BGP para permitir que o BGP faça o balanceamento de carga do tráfego em vários links.



Clique em Finish para salvar e validar a topologia SD-WAN.

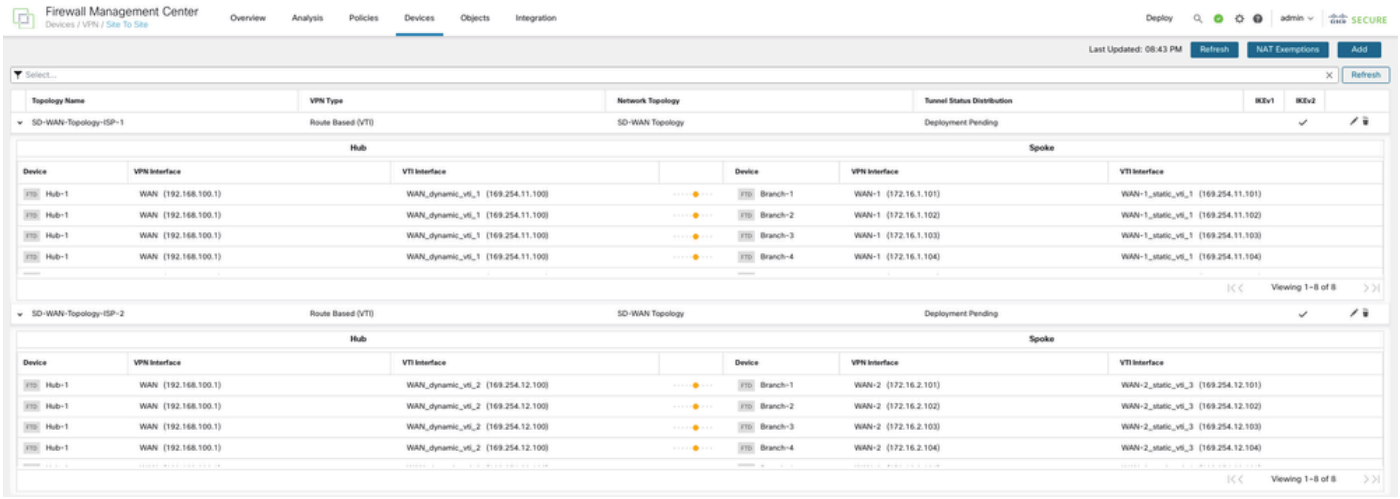


Você pode visualizar a topologia em Devices > Site-to-site VPN. O número total de túneis na primeira topologia de SD-WAN é 8.



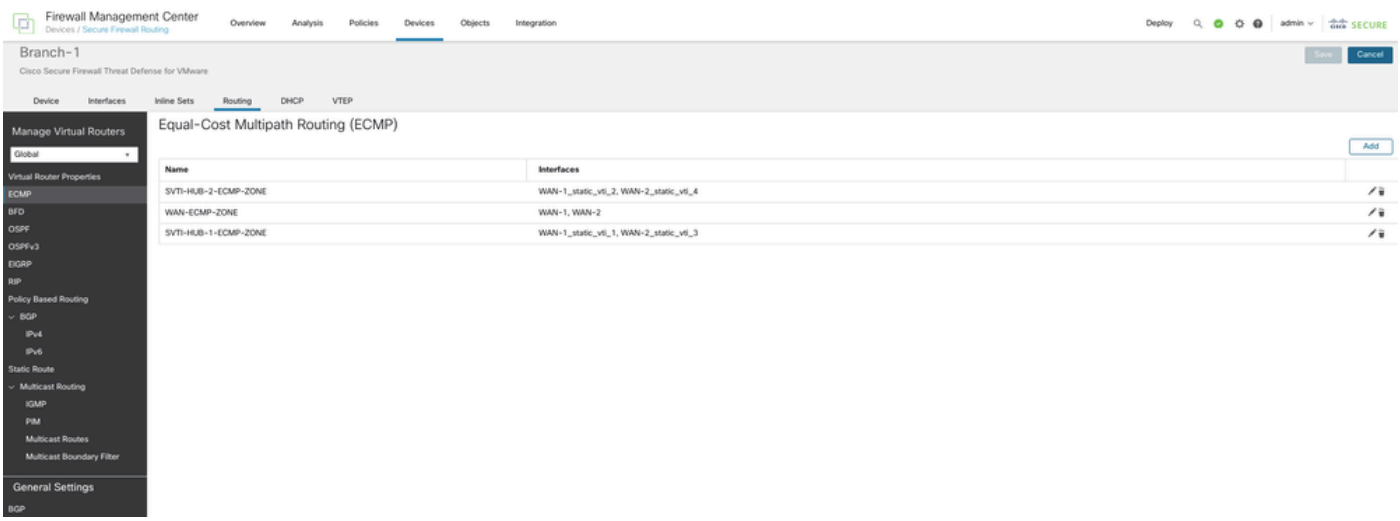
Etapa 7. Criar uma topologia SD-WAN com WAN-2 como a interface VPN

Repita as etapas de 1 a 6 para configurar uma topologia SD-WAN com WAN-2 como a interface VPN. O número total de túneis na segunda topologia SD-WAN é 8. As topologias finais devem se parecer com a imagem mostrada abaixo.



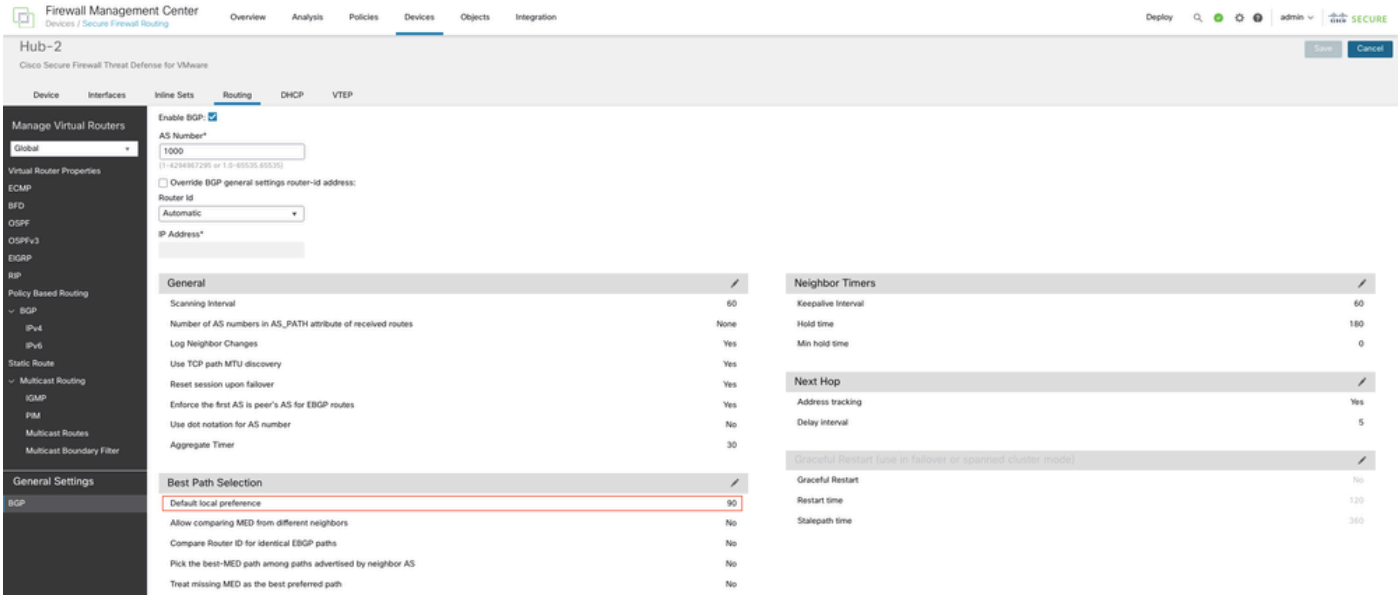
Etapa 8. Configurar regiões ECMP

Em cada filial, navegue para Roteamento > ECMP e configure Zonas ECMP (Equal-Cost Multi-Path) para as interfaces WAN e os SVTIs que se conectam ao hub principal e secundário, como mostrado abaixo. Isso pode fornecer redundância de link e permitir o balanceamento de carga do tráfego VPN.



Etapa 9. Modificar a Preferência Local de BGP no Hub

Navegue para Routing > General Settings > BGP no hub secundário. Selecione Enable BGP, configure o AS Number e defina o valor de default local preference em Best Path Selection para um valor inferior ao configurado no hub principal. Selecione Save. Isso garante que as rotas para o hub principal tenham preferência sobre as rotas para o hub secundário. Quando o hub principal fica inativo, as rotas para o hub secundário assumem o controle.

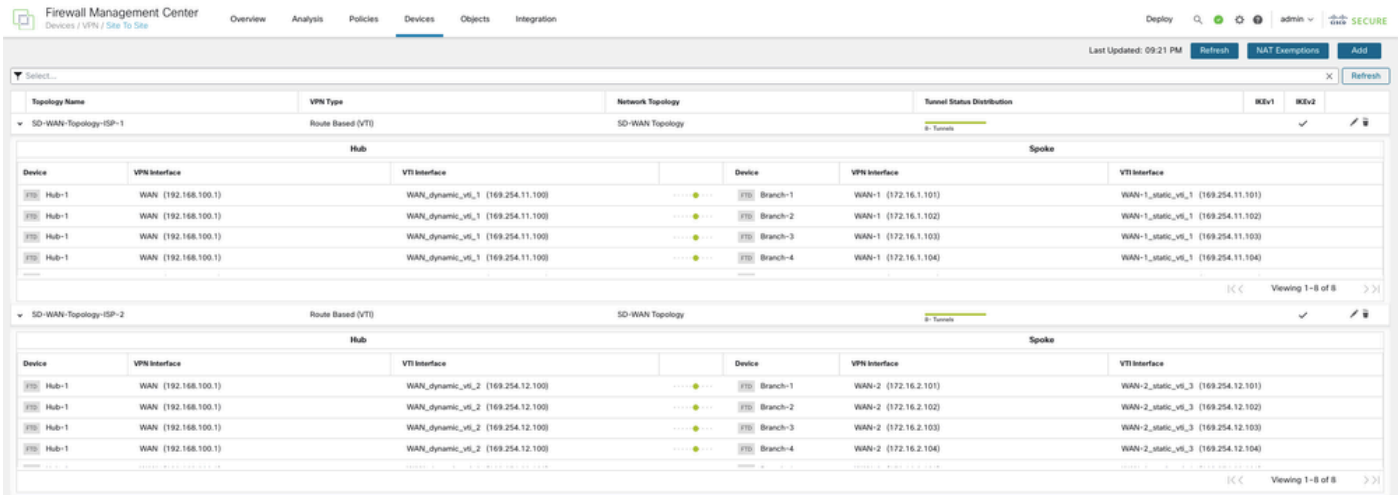


Implante as configurações em todos os dispositivos.

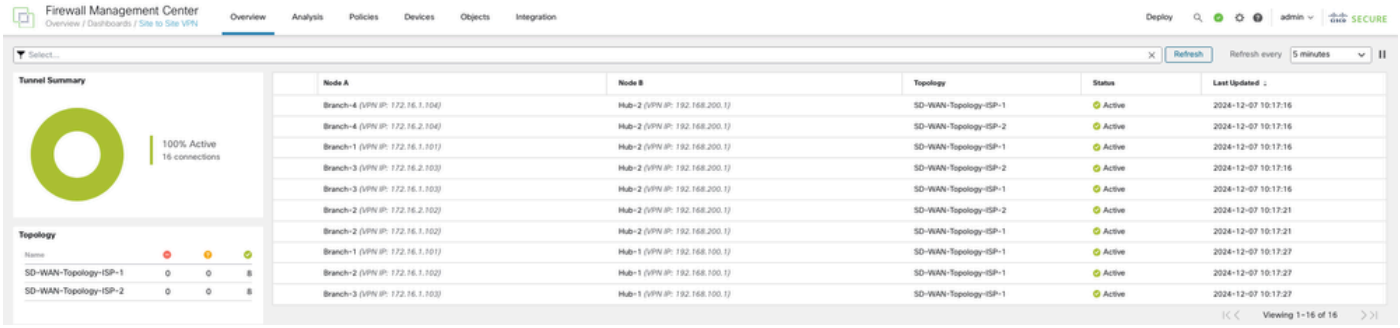
Verificar

Verifique o status do túnel

Para verificar se os túneis VPN das topologias SD-WAN estão ativos, selecione Device > VPN > Site-to-Site.

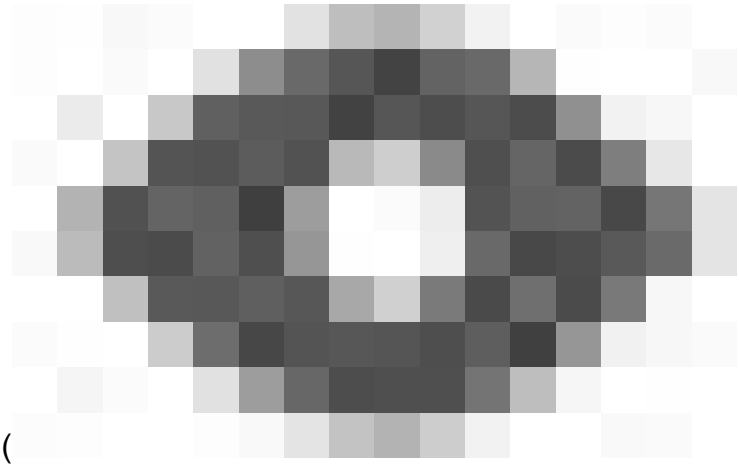


Para ver os detalhes dos túneis de VPN SD-WAN, escolha Overview > Dashboards > Site-to-site VPN.



Para ver mais detalhes de cada túnel VPN:

1. Passe o mouse sobre um túnel.



2. Selecione a opção View Full Information ( ). Um painel com detalhes do túnel e mais ações é exibido.

3. Selecione a guia Detalhes da CLI no painel lateral para exibir os comandos show e os detalhes das associações de segurança IPsec.

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

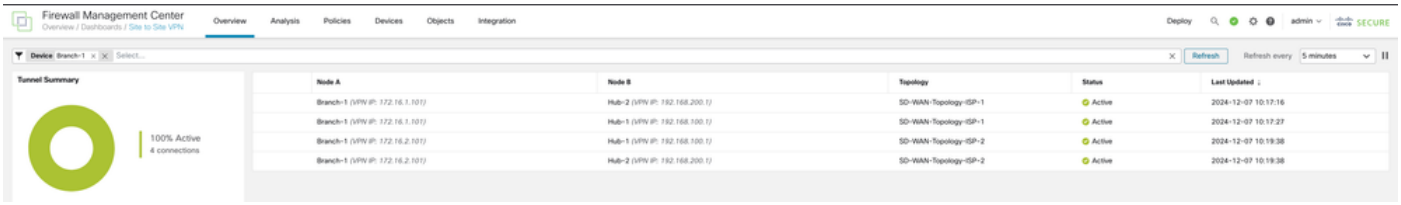
Branch-1 (VPN Interface IP: 172.16.2.101)

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

WAN-2_static_vti_3 - SVTI para hub 1 via ISP 2
WAN-1_static_vti_2 - SVTI para hub 2 via ISP 1
WAN-2_static_vti_4 - SVTI para hub 2 via ISP 2

Verifique o balanceamento de carga do tráfego de VPN

O status do túnel pode ser visto no painel VPN site a site. Idealmente, todos os túneis devem estar ativos:



As rotas para o hub principal são as preferidas. O comando show route na Filial 1 indica que o tráfego de VPN tem balanceamento de carga entre os dois SVTIs no ISP 1 e ISP 2 para o hub principal:

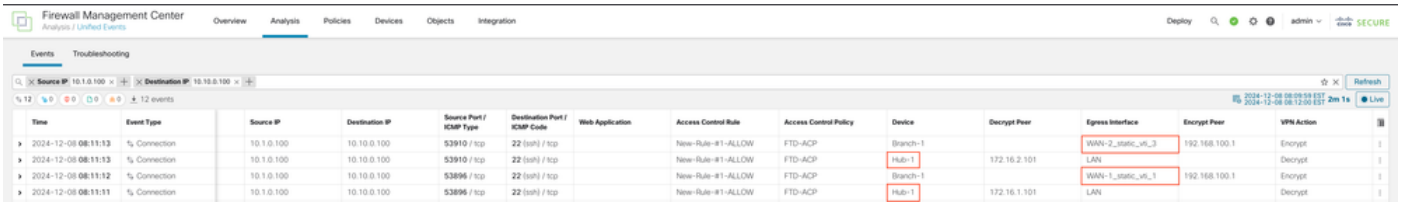
CLI Troubleshoot

>_ 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 169.254.12.100, 01:41:02
                               [200/1] via 169.254.11.100, 01:41:02
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        169.254.12.0 255.255.255.0 is directly connected, WAN-2_static_vti_3
V        169.254.12.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_3
L        169.254.12.101 255.255.255.255
           is directly connected, WAN-2_static_vti_3
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        169.254.22.0 255.255.255.0 is directly connected, WAN-2_static_vti_4
V        169.254.22.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_4
L        169.254.22.101 255.255.255.255
           is directly connected, WAN-2_static_vti_4
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
C        172.16.2.0 255.255.255.0 is directly connected, WAN-2
L        172.16.2.101 255.255.255.255 is directly connected, WAN-2
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 02:03:26, WAN-2
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
```

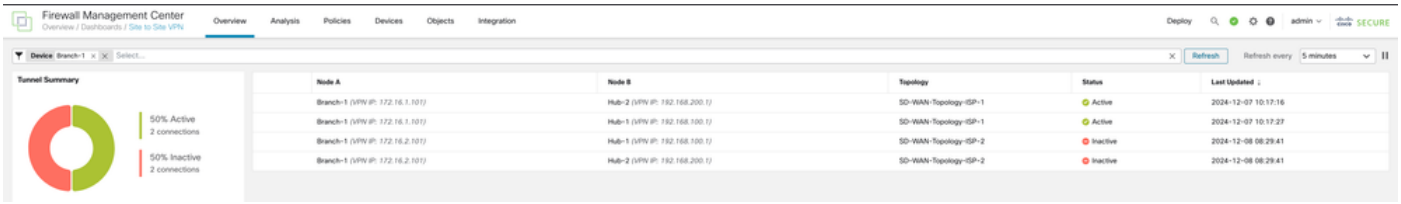
Close

A interface de saída usada para o tráfego VPN real pode ser vista em Unified Events:



Verificar a redundância dupla do ISP

Quando ISP-2 está inativo, o status do túnel indica que os túneis via ISP-1 estão ativos:



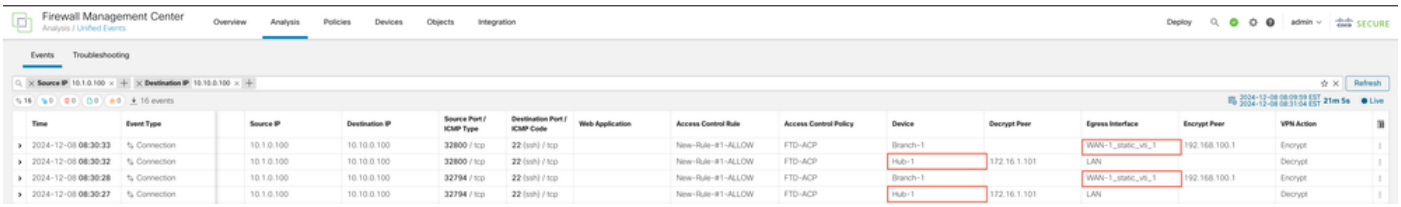
As rotas para o hub principal são as preferidas. O comando show route na Filial 1 indica que o tráfego VPN é roteado através dos SVTIs no ISP-1 para o hub principal:

CLI Troubleshoot

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

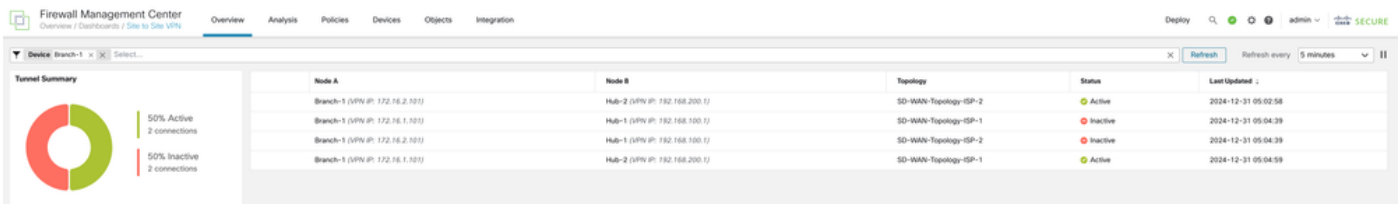
```
> show route

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
```

A interface de saída usada para o tráfego VPN real pode ser vista em Unified Events:

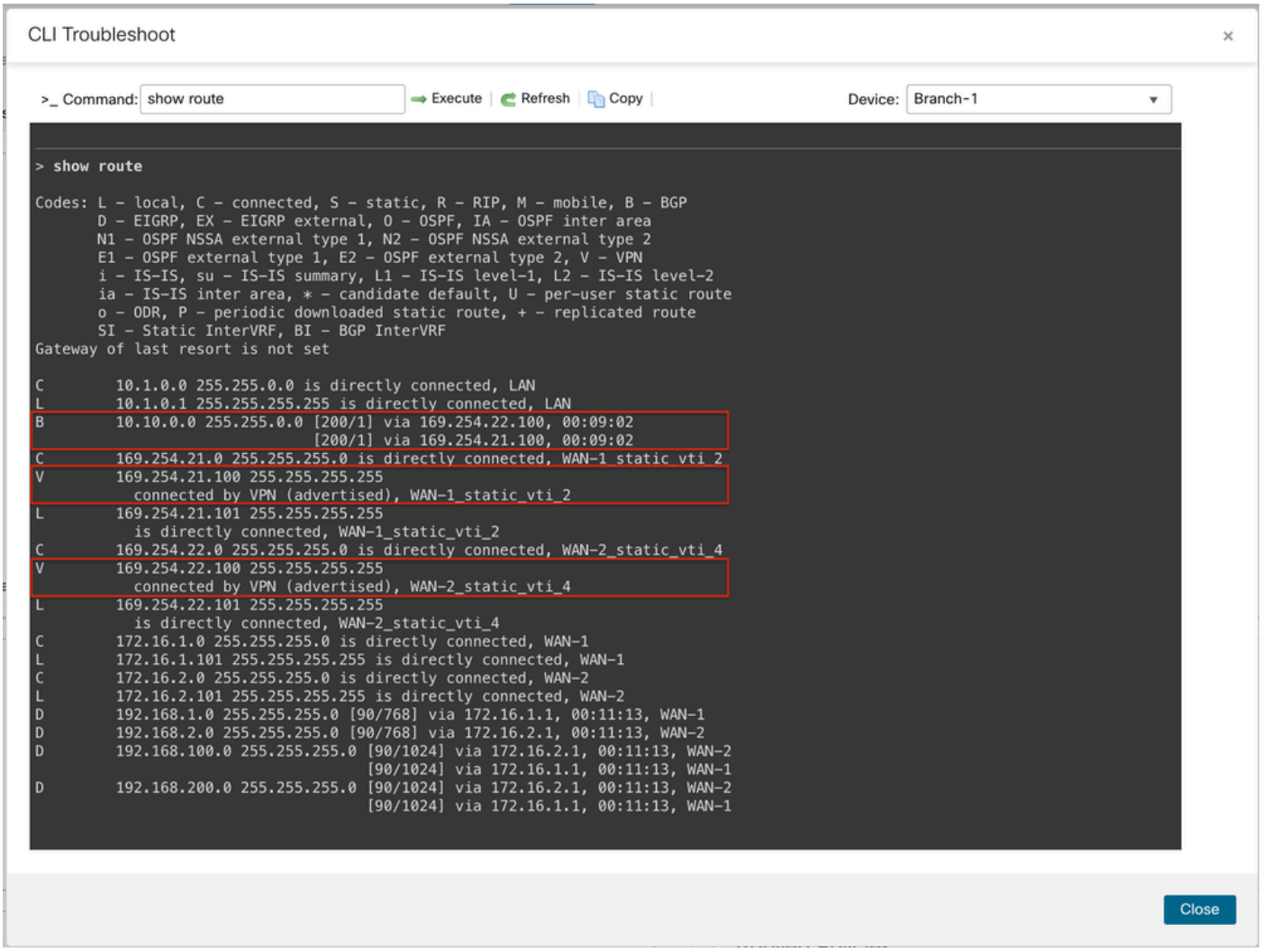


Verificar a Redundância no Nível do Hub

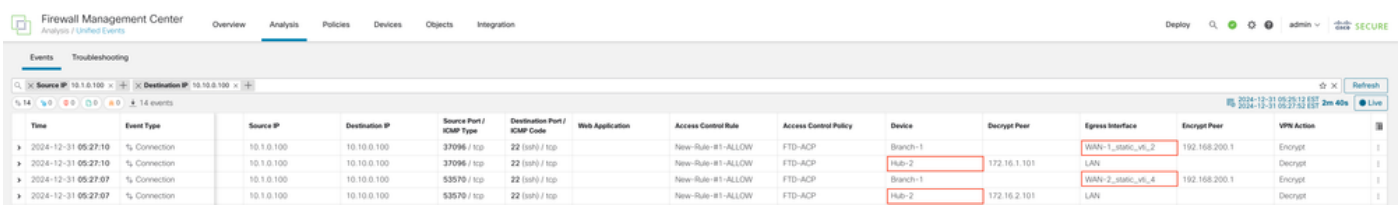
Quando o hub principal está inativo, o status do túnel indica que os túneis para o hub secundário estão ativos:



Como o hub principal está desativado, as rotas para o hub secundário são as preferidas. O comando show route na Filial 1 indica que o tráfego de VPN tem balanceamento de carga entre os dois SVTIs no ISP 1 e ISP 2 para o hub secundário:



A interface de saída usada para o tráfego VPN real pode ser vista em Unified Events:



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.