

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Plataformas de software e hardware suportadas](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapa 1. Criar uma topologia SD-WAN com WAN-1 como a interface VPN](#)

[Etapa 2. Configurar o Dynamic Virtual Tunnel Interface \(DVTI\) no hub principal](#)

[Etapa 3. Configurar o Dynamic Virtual Tunnel Interface \(DVTI\) no hub secundário](#)

[Etapa 4. Configurar os raios](#)

[Etapa 5. Definir as configurações de autenticação](#)

[Etapa 6. Definir as configurações de SD-WAN](#)

[Etapa 7. Criar uma topologia SD-WAN com WAN-2 como a interface VPN](#)

[Etapa 8. Configurar regiões ECMP](#)

[Etapa 9. Modificar a Preferência Local de BGP no Hub](#)

[Verificar](#)

[Verifique o status do túnel](#)

[Verificar interfaces de túnel virtual](#)

[Verifique o balanceamento de carga do tráfego de VPN](#)

[Verificar a redundância dupla do ISP](#)

[Verificar a Redundância no Nível do Hub](#)

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

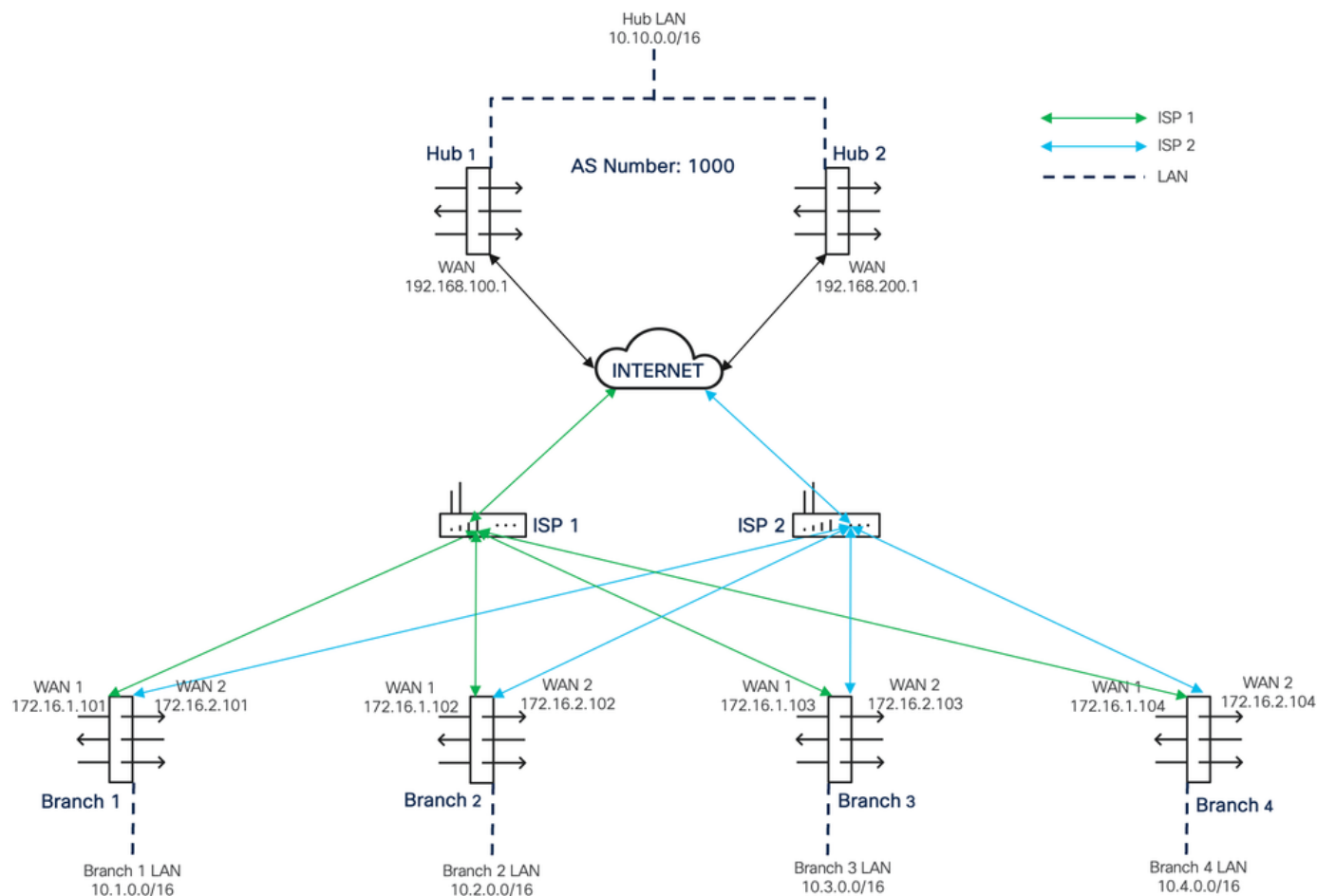
As informações neste documento são baseadas nestas versões de software e hardware:

- 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



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy admin SECURE

View By: Group

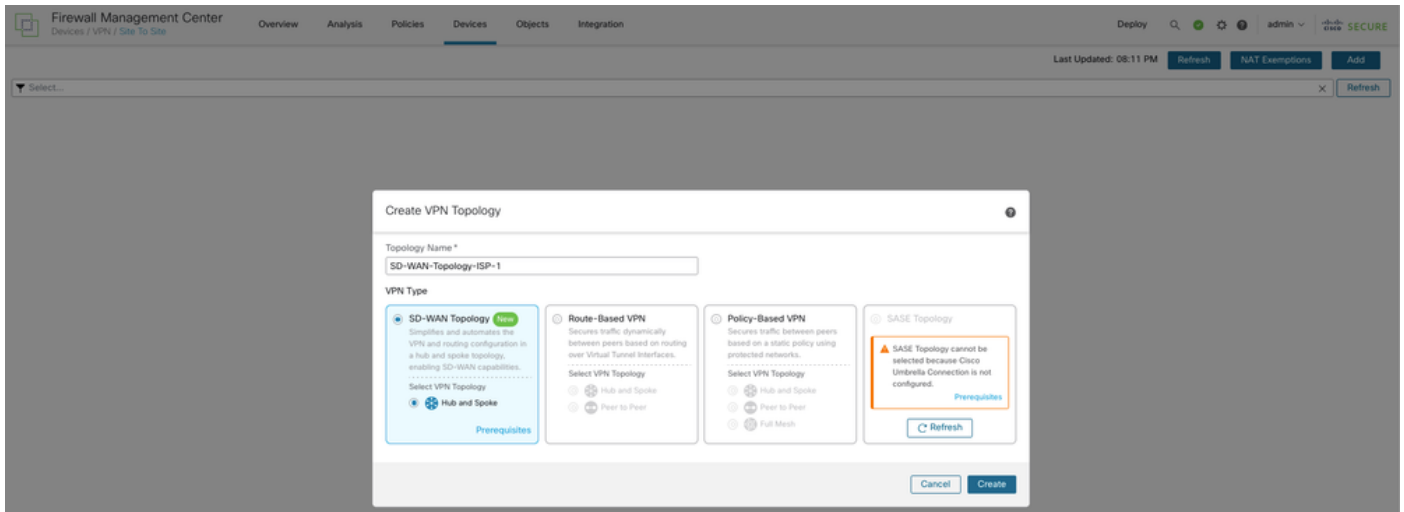
All (8)
Error (0)
Warning (0)
Offline (0)
Normal (8)
Deployment Pending (0)
Upgrade (0)
Snort 3 (8)

[Collapse All](#) [Download Device List Report](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback	
☐	▼ Branch (4)							
☐	Branch-1 Snort 3 10.10.1.206 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-2 Snort 3 10.10.1.207 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-3 Snort 3 10.10.1.208 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-4 Snort 3 10.10.1.209 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	▼ HQ (2)							
☐	Hub-1 Snort 3 10.10.1.199 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Hub-2 Snort 3 10.10.1.205 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		

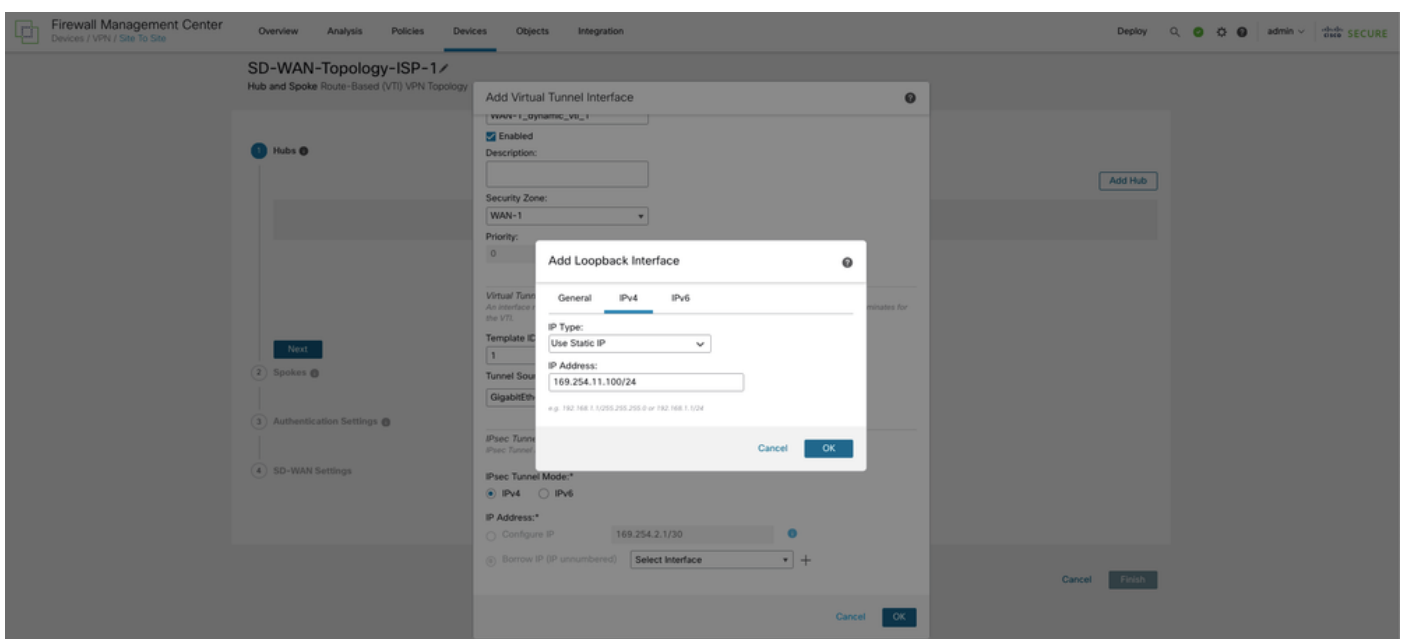
Etapa 1. Criar uma topologia SD-WAN com WAN-1 como a interface VPN

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.

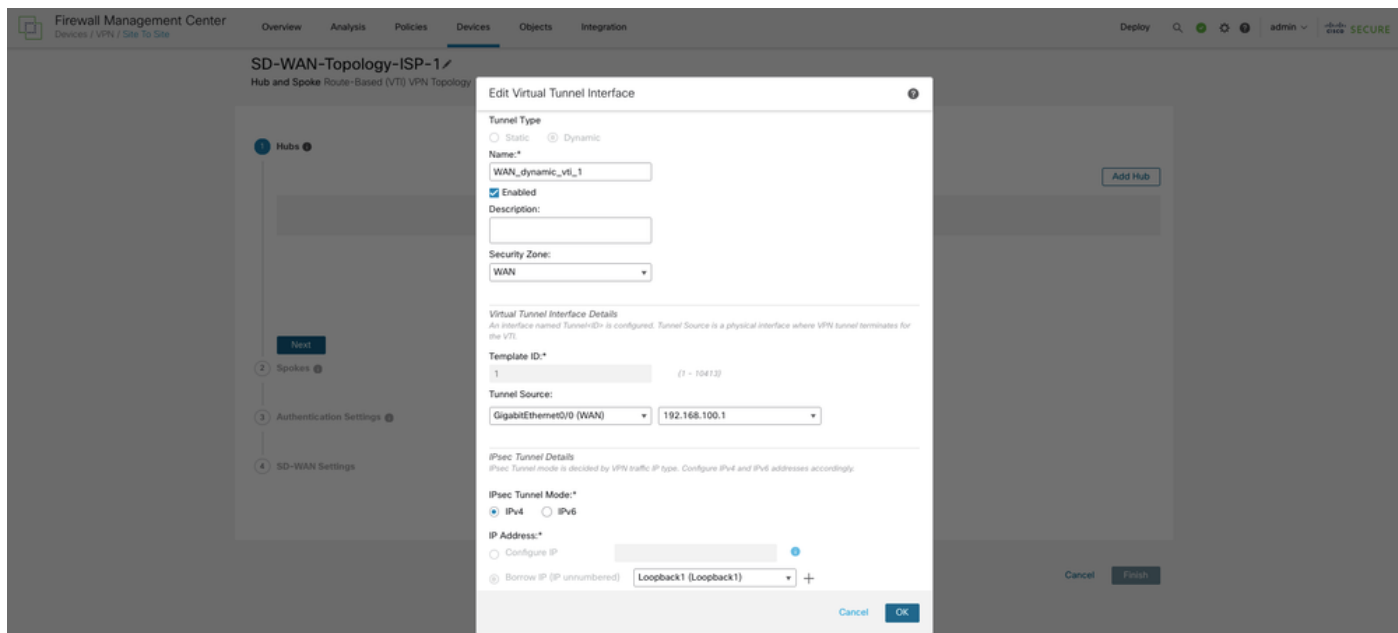


Etapa 2. Configurar o Dynamic Virtual Tunnel Interface (DVTI) no hub principal

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.

Add IPv4 Pool



Name*

Spoke-Pool-Hub-1-ISP-1

Description

IPv4 Address Range*

169.254.11.101-169.254.11.150

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

☐ Allow Overrides

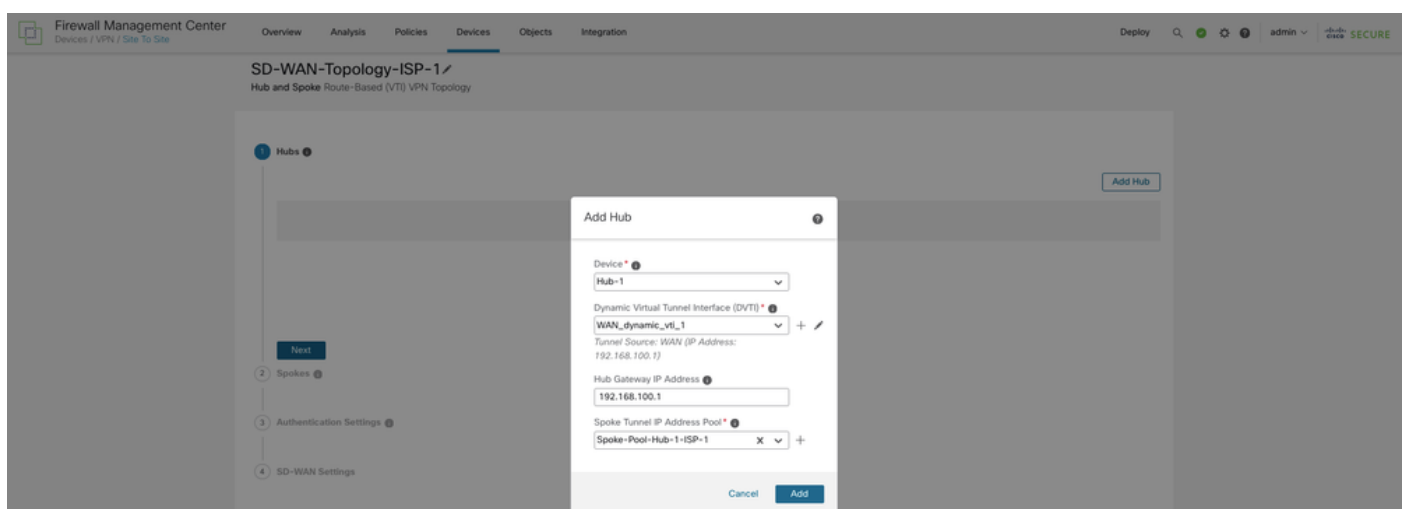


Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Cancel

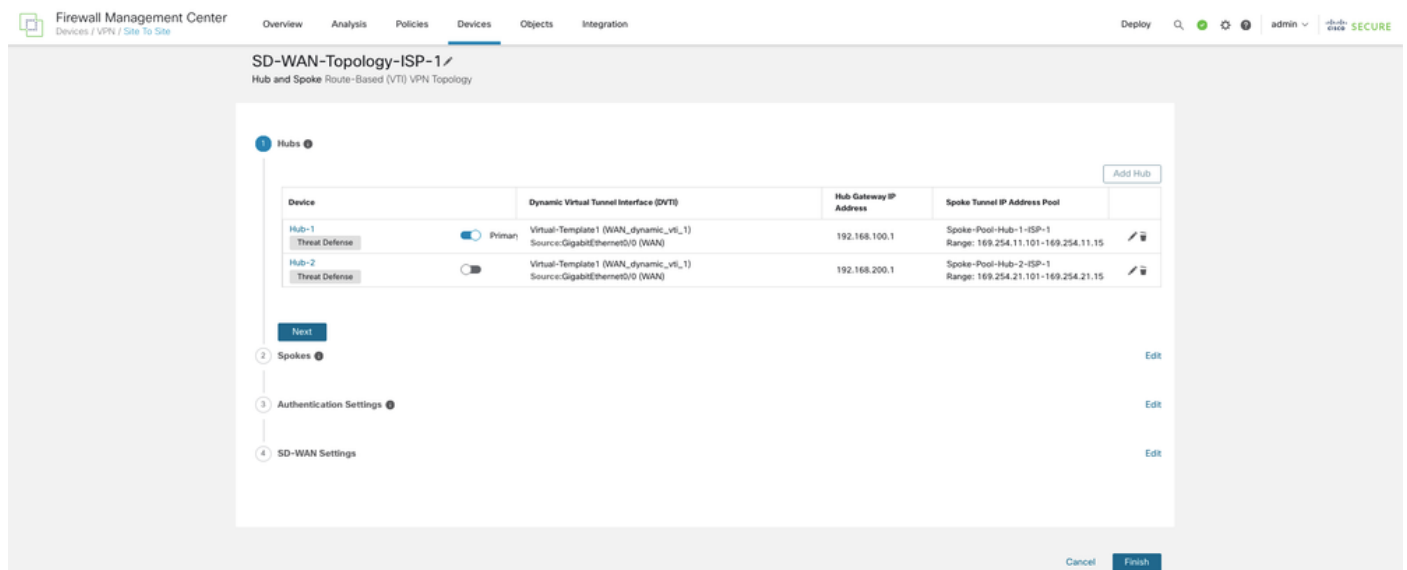
Save

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



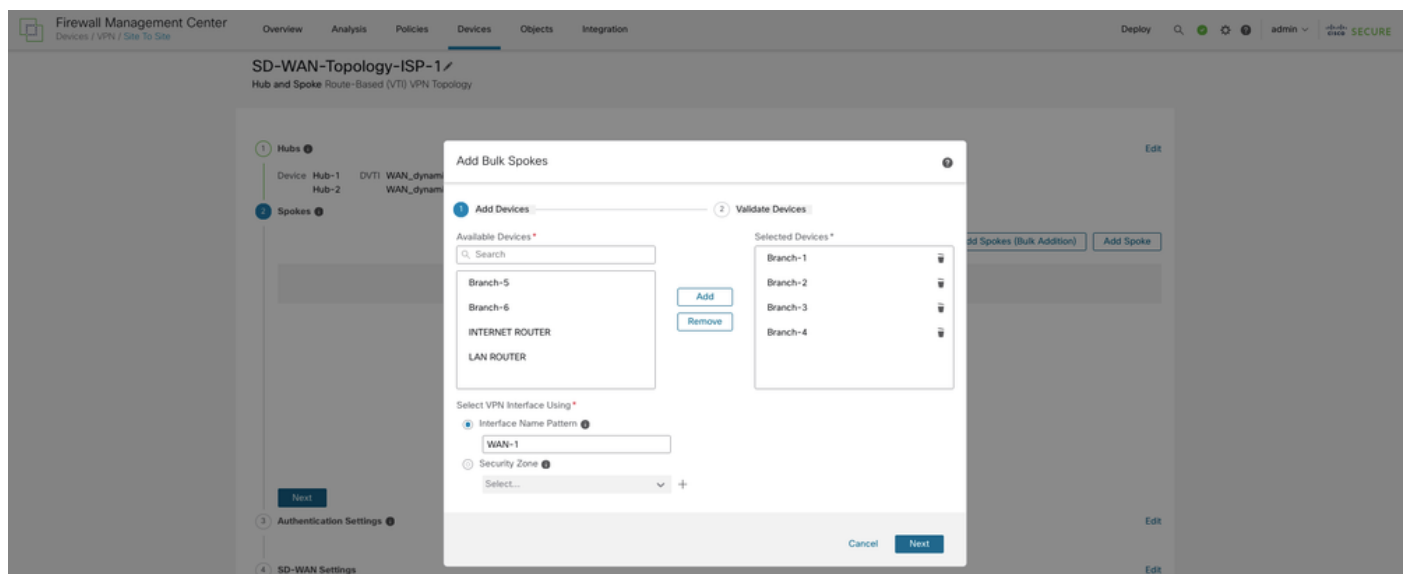
Etapa 3. Configurar o Dynamic Virtual Tunnel Interface (DVTI) no hub secundário

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.

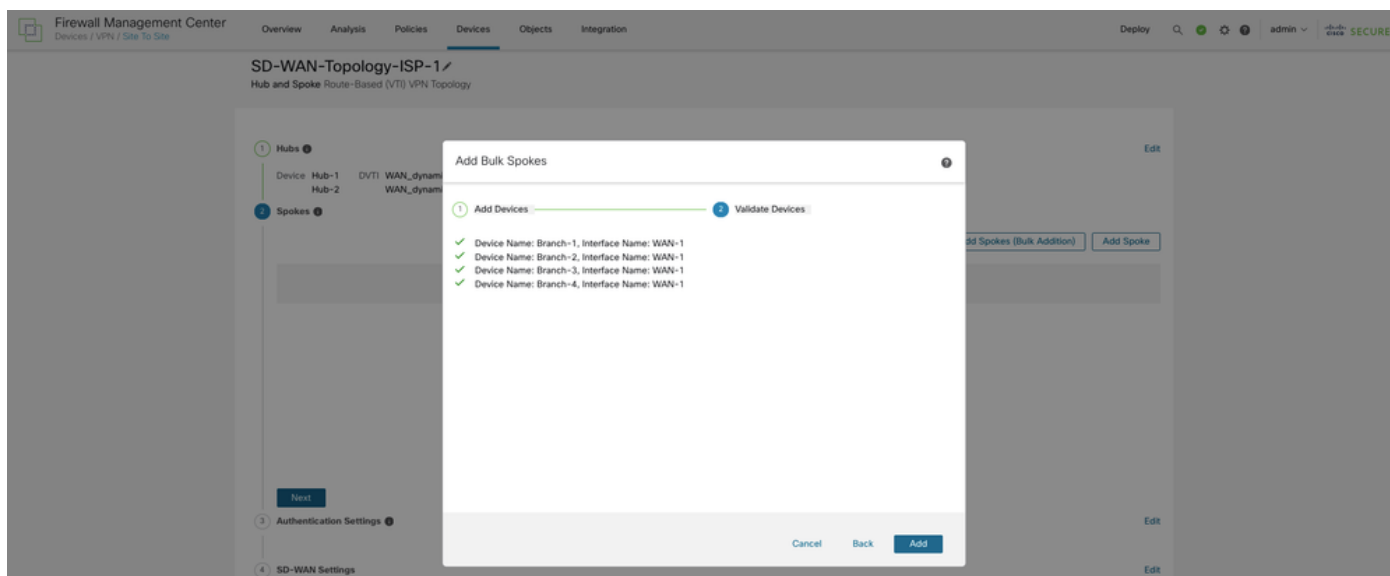


Etapa 4. Configurar os raios

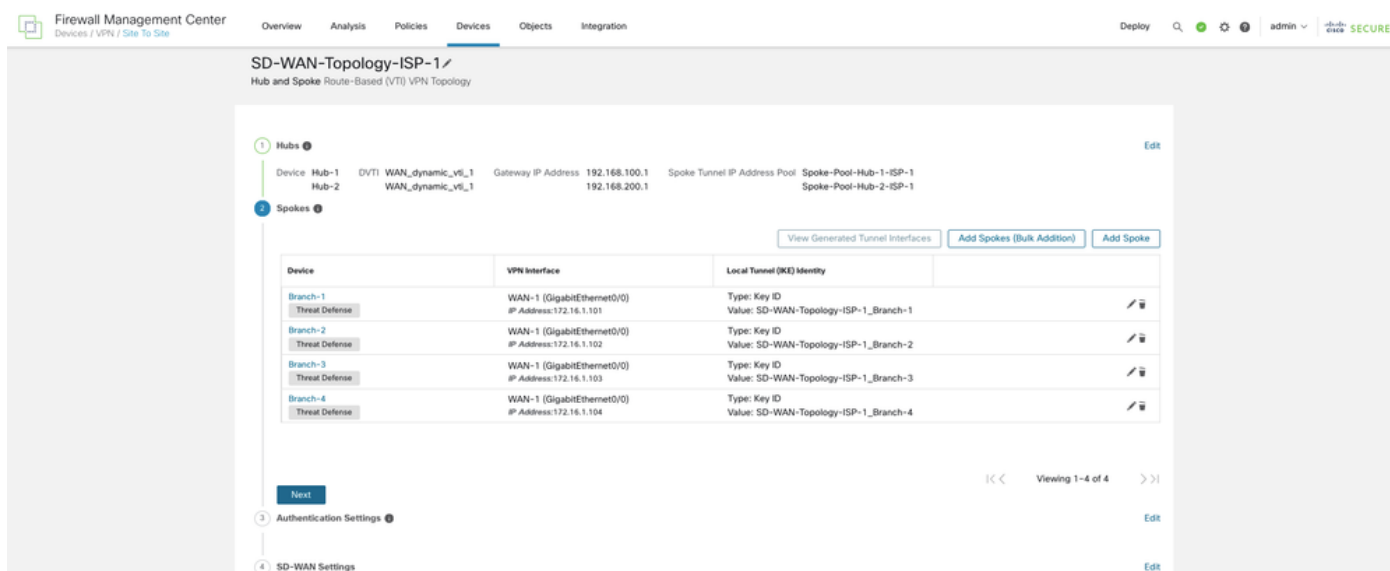
Selecione Add Spoke para adicionar um único dispositivo spoke ou clique em Add Spokes (Bulk Addition) para adicionar vários spokes à sua topologia. A topologia atual usa a última opção para adicionar vários FTDs de filial à topologia. Na caixa de diálogo Add Bulk Spokes, selecione os FTDs necessários 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.

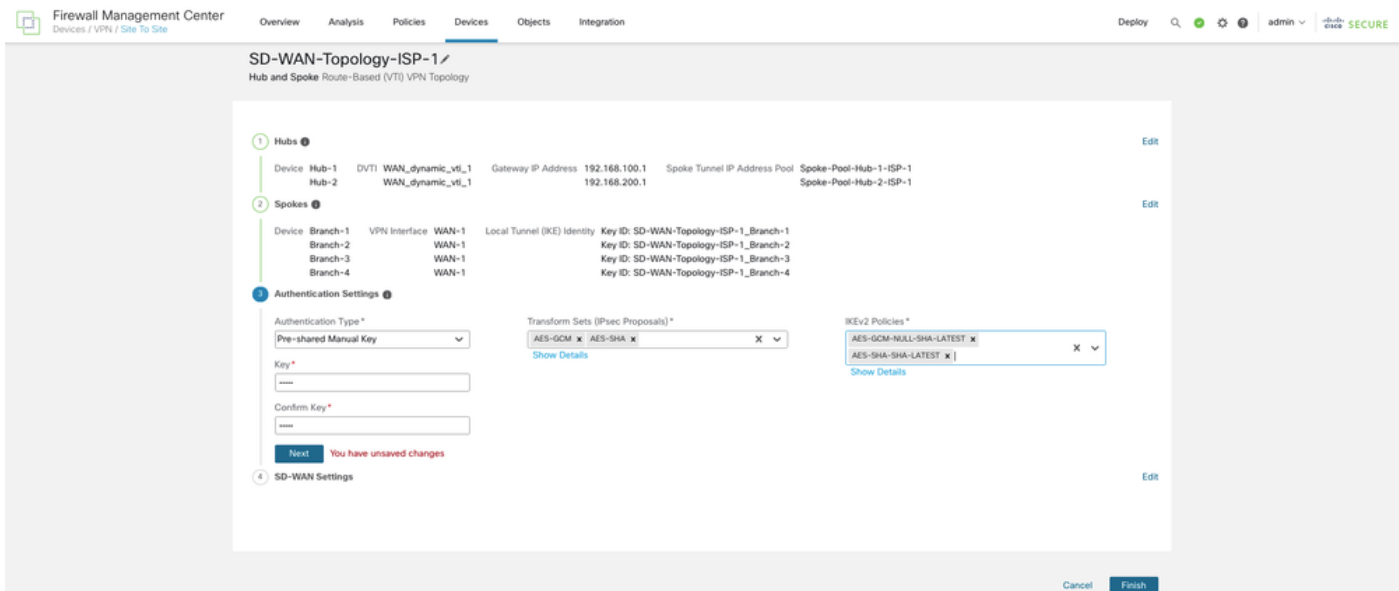


Selecione Add e o assistente selecionará automaticamente o hub DVTI como o endereço IP origem do túnel para cada spoke.



Etapa 5. Configurar as Definições de Autenticação

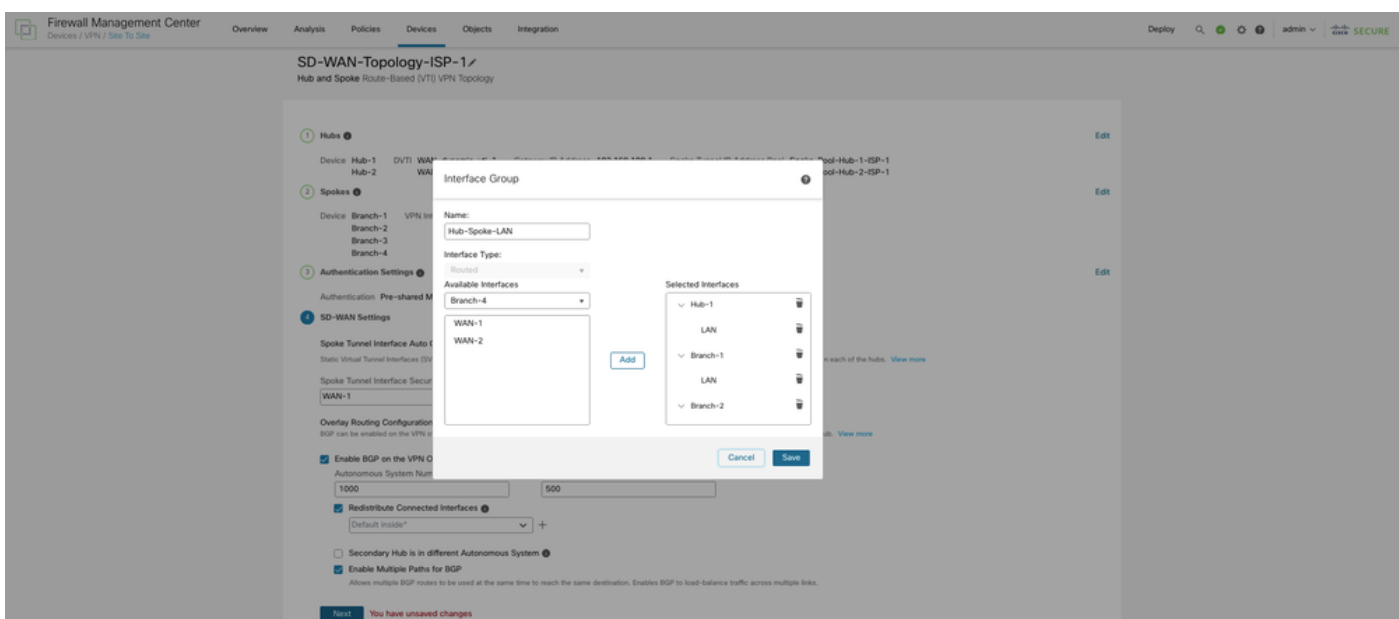
Selecione Avançar para definir as Configurações de autenticação. Para a autenticação do dispositivo, você pode selecionar uma chave pré-compartilhada manual, uma chave pré-compartilhada gerada automaticamente ou um certificado na lista suspensa Authentication Type. Escolha um ou mais algoritmos nas listas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

SD-WAN-Topology-ISP-1
Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs [Edit](#)

Device	Virtual Interface	Gateway IP Address	Spoke Tunnel IP Address Pool
Hub-1	DVTI WAN_dynamic_vti_1	192.168.100.1	Spoke-Pool-Hub-1-ISP-1
Hub-2	WAN_dynamic_vti_1	192.168.200.1	Spoke-Pool-Hub-2-ISP-1

2 Spokes [Edit](#)

Device	VPN Interface	Local Tunnel (IKE) Identity	Key ID
Branch-1	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-1	
Branch-2	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-2	
Branch-3	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-3	
Branch-4	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-4	

3 Authentication Settings [Edit](#)

Authentication: Pre-shared Manual Key

4 SD-WAN Settings [Edit](#)

Spoke Tunnel Interface Auto Generation
Static Virtual Tunnel Interfaces (VTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)

Spoke Tunnel Interface Security Zone: WAN-1

Overlay Routing Configuration
BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ **Enable BGP on the VPN Overlay Topology**

Autonomous System Number: 1000 Community Tag for Local Routes: 500

☒ **Redistribute Connected Interfaces**

Hub-Spoke-LAN

☐ Secondary Hub is in different Autonomous System

☒ **Enable Multiple Paths for BGP**
Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

[Next](#) You have unsaved changes [Cancel](#) [Finish](#)

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

SD-WAN-Topology-ISP-1
Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs [Edit](#)

Device	Virtual Interface	Gateway IP Address	Spoke Tunnel IP Address Pool
Hub-1	DVTI WAN_dynamic_vti_1	192.168.100.1	Spoke-Pool-Hub-1-ISP-1
Hub-2	WAN_dynamic_vti_1	192.168.200.1	Spoke-Pool-Hub-2-ISP-1

2 Spokes [Edit](#)

Device	VPN Interface	Local Tunnel (IKE) Identity	Key ID
Branch-1	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-1	
Branch-2	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-2	
Branch-3	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-3	
Branch-4	WAN-1	Key ID: SD-WAN-Topology-ISP-1_Branch-4	

3 Authentication Settings [Edit](#)

Authentication: Pre-shared Manual Key

4 SD-WAN Settings [Edit](#)

BGP enabled: true Autonomous System Number: 1000

[Cancel](#) [Finish](#)

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

SD-WAN-Topology-ISP-1

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEx1	IKEx2
SD-WAN-Topology-ISP-1	Route Based (VTI)	SD-WAN Topology	Deployment Pending	✓	

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)

Viewing 1-8 of 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.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKv1	IKv2																																				
SD-WAN-Topology-ISP-1	Route Based (VTI)	SD-WAN Topology	Deployment Pending	✓	✓																																				
<table border="1"> <thead> <tr> <th colspan="3">Hub</th> <th colspan="3">Spoke</th> </tr> <tr> <th>Device</th> <th>VPN Interface</th> <th>VTI Interface</th> <th>Device</th> <th>VPN Interface</th> <th>VTI Interface</th> </tr> </thead> <tbody> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_1 (169.254.11.100)</td> <td>Branch-1</td> <td>WAN-1 (172.16.1.101)</td> <td>WAN-1_static_vti_1 (169.254.11.101)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_1 (169.254.11.100)</td> <td>Branch-2</td> <td>WAN-1 (172.16.1.102)</td> <td>WAN-1_static_vti_1 (169.254.11.102)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_1 (169.254.11.100)</td> <td>Branch-3</td> <td>WAN-1 (172.16.1.103)</td> <td>WAN-1_static_vti_1 (169.254.11.103)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_1 (169.254.11.100)</td> <td>Branch-4</td> <td>WAN-1 (172.16.1.104)</td> <td>WAN-1_static_vti_1 (169.254.11.104)</td> </tr> </tbody> </table>						Hub			Spoke			Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)
Hub			Spoke																																						
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)																																				
SD-WAN-Topology-ISP-2	Route Based (VTI)	SD-WAN Topology	Deployment Pending	✓	✓																																				
<table border="1"> <thead> <tr> <th colspan="3">Hub</th> <th colspan="3">Spoke</th> </tr> <tr> <th>Device</th> <th>VPN Interface</th> <th>VTI Interface</th> <th>Device</th> <th>VPN Interface</th> <th>VTI Interface</th> </tr> </thead> <tbody> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_2 (169.254.12.100)</td> <td>Branch-1</td> <td>WAN-2 (172.16.2.101)</td> <td>WAN-2_static_vti_3 (169.254.12.101)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_2 (169.254.12.100)</td> <td>Branch-2</td> <td>WAN-2 (172.16.2.102)</td> <td>WAN-2_static_vti_3 (169.254.12.102)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_2 (169.254.12.100)</td> <td>Branch-3</td> <td>WAN-2 (172.16.2.103)</td> <td>WAN-2_static_vti_3 (169.254.12.103)</td> </tr> <tr> <td>Hub-1</td> <td>WAN (192.168.100.1)</td> <td>WAN_dynamic_vti_2 (169.254.12.100)</td> <td>Branch-4</td> <td>WAN-2 (172.16.2.104)</td> <td>WAN-2_static_vti_3 (169.254.12.104)</td> </tr> </tbody> </table>						Hub			Spoke			Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_3 (169.254.12.101)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_3 (169.254.12.102)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_3 (169.254.12.103)	Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_3 (169.254.12.104)
Hub			Spoke																																						
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_3 (169.254.12.101)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_3 (169.254.12.102)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_3 (169.254.12.103)																																				
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_3 (169.254.12.104)																																				

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.

Name	Interfaces
SVTI-HUB-2-ECMP-ZONE	WAN-1_static_vti_2, WAN-2_static_vti_4
WAN-ECMP-ZONE	WAN-1, WAN-2
SVTI-HUB-1-ECMP-ZONE	WAN-1_static_vti_1, WAN-2_static_vti_3

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.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin ▾ **SECURE**

Hub-2
Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Enable BGP: ☒

AS Number*
1000
(1-4294967295 or 1.0-45535.65535)

☐ Override BGP general settings router-id address:

Router Id
Automatic

IP Address*

General

Scanning Interval 60

Number of AS numbers in AS_PATH attribute of received routes None

Log Neighbor Changes Yes

Use TCP path MTU discovery Yes

Reset session upon fallover Yes

Enforce the first AS is peer's AS for EBGp routes Yes

Use dot notation for AS number No

Aggregate Timer 30

Best Path Selection

Default local preference 90

Allow comparing MED from different neighbors No

Compare Router ID for identical EBGp paths No

Pick the best-MED path among paths advertised by neighbor AS No

Treat missing MED as the best preferred path No

Neighbor Timers

Keepalive Interval 60

Hold time 180

Min hold time 0

Next Hop

Address tracking Yes

Delay interval 5

Graceful Restart (use in failover or spanned cluster mode)

Graceful Restart No

Restart time 120

Stalepath time 360

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.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin ▾ **SECURE**

Last Updated: 09:21 PM Refresh NAT Exemptions Add

Select...

Topology Name VPN Type Network Topology Tunnel Status Distribution IKEv1 IKEv2

SD-WAN-Topology-ISP-1 Route Based (VTI) SD-WAN Topology 0 Tunnels

Hub Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)

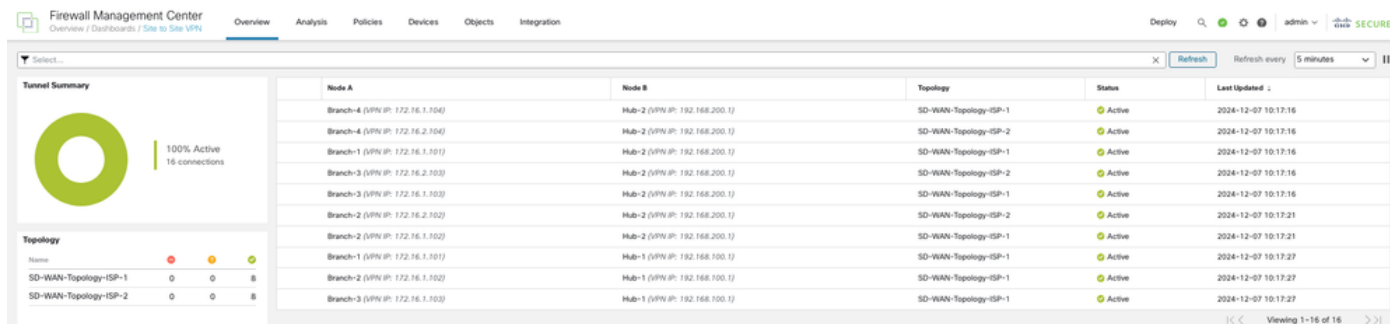
SD-WAN-Topology-ISP-2 Route Based (VTI) SD-WAN Topology 0 Tunnels

Hub Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_3 (169.254.12.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_3 (169.254.12.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_3 (169.254.12.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_3 (169.254.12.104)

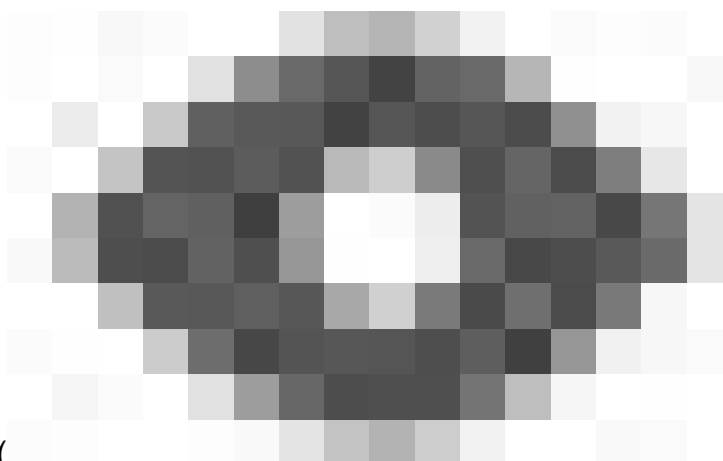
Viewing 1-8 of 8

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,...	Info is not available for Extranet device	
Encaps/Encrypt:	96 / 96 pkts		
Dcaps/Decrypt:	92 / 92 pkts		
Remaining Lifetime for SPI ID: 0x1DEFCEB21			
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:

Firewall Management Center				
Overview / Dashboards / Site to Site VPN				
Deploy 🔍 ⚙️ 👤 admin 🔒 SECURE				
Device: Branch-1 x Select...				
Refresh Refresh every 5 minutes				
Tunnel Summary				
 100% Active 4 connections				
Node A	Node B	Topology	Status	Last Updated
Branch-1 (VPN IP: 172.16.1.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-1 (VPN IP: 172.16.1.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-1 (VPN IP: 172.16.2.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:19:38
Branch-1 (VPN IP: 172.16.2.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:19:38

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:

Firewall Management Center										Deploy		admin		SECURE	
Analysis / Unified Events															
Events Troubleshooting															
Source IP: 10.1.0.100 x Destination IP: 10.10.0.100 x															
12 100% 100% 100% 100% 100% 100% 100% 100% 100%															
Time	Event Type	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Device	Decrypt Peer	Egress Interface	Encrypt Peer	VPN Action		
2024-12-08 08:11:13	% Connection	10.1.0.100	10.10.0.100	53910 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-2_static_v6_3	192.168.100.1	Encrypt		
2024-12-08 08:11:13	% Connection	10.1.0.100	10.10.0.100	53910 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.2.101	LAN		Decrypt		
2024-12-08 08:11:12	% Connection	10.1.0.100	10.10.0.100	53896 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-1_static_v6_1	192.168.100.1	Encrypt		
2024-12-08 08:11:11	% Connection	10.1.0.100	10.10.0.100	53896 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN		Decrypt		

Verificar a redundância dupla do ISP

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

Firewall Management Center												
Overview / Dashboards / Site to Site VPN												
Device: branch-1 x Select...												
Refresh Refresh every 5 minutes												
Tunnel Summary												
50% Active 2 connections 50% Inactive 2 connections												
Node A Node B Topology Status Last Updated												
Branch-1 (VPN IP: 172.16.1.101)			Hub-2 (VPN IP: 192.168.200.1)			SD-WAN-Topology-ISP-1			Active 2024-12-07 10:17:16			
Branch-1 (VPN IP: 172.16.1.101)			Hub-1 (VPN IP: 192.168.100.1)			SD-WAN-Topology-ISP-1			Active 2024-12-07 10:17:27			
Branch-1 (VPN IP: 172.16.2.101)			Hub-3 (VPN IP: 192.168.100.1)			SD-WAN-Topology-ISP-2			Inactive 2024-12-08 08:29:41			
Branch-1 (VPN IP: 172.16.2.101)			Hub-2 (VPN IP: 192.168.200.1)			SD-WAN-Topology-ISP-2			Inactive 2024-12-08 08:29:41			

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

Firewall Management Center

Analysis / Unified Events

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy🔍🔒🔑🛡️admin🔒🔑🛡️SECURE

EventsTroubleshooting

🔍 Source IP: 10.1.0.100 x 📌 Destination IP: 10.10.0.100 x

🕒 16 📊 📉 📈 📉 📈 15 events

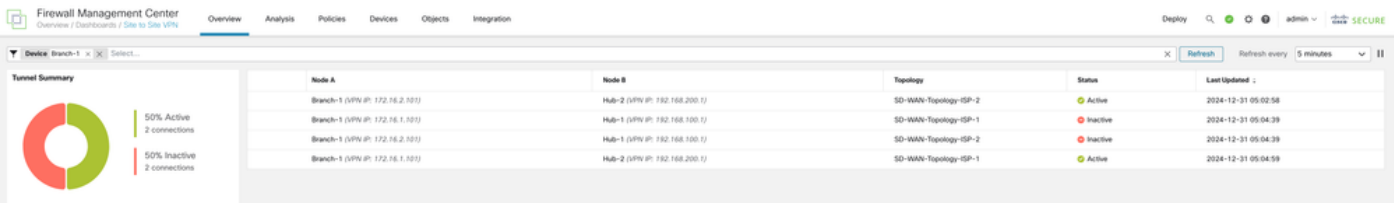
🔄 Refresh

📅 2024-12-08 08:09:59 21m 5s 🟢 Live

Time	Event Type	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Device	Decrypt Peer	Egress Interface	Encrypt Peer	VPN Action
2024-12-08 08:30:33	% Connection	10.1.0.100	10.10.0.100	32800 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-1_static_v6_1	192.168.100.1	Encrypt
2024-12-08 08:30:32	% Connection	10.1.0.100	10.10.0.100	32800 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN		Decrypt
2024-12-08 08:30:28	% Connection	10.1.0.100	10.10.0.100	32794 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-1_static_v6_1	192.168.100.1	Encrypt
2024-12-08 08:30:27	% Connection	10.1.0.100	10.10.0.100	32794 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN		Decrypt

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:

```
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 169.254.22.100, 00:09:02
[200/1] via 169.254.21.100, 00:09:02
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, 00:11:13, WAN-1
D 192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 00:11:13, WAN-2
D 192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
[90/1024] via 172.16.1.1, 00:11:13, WAN-1
D 192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
[90/1024] via 172.16.1.1, 00:11:13, WAN-1
```

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

The screenshot shows the Firewall Management Center interface with the 'Unified Events' tab selected. The table displays the following events:

Time	Event Type	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Device	Decrypt Peer	Egress Interface	Encrypt Peer	VPN Action
2024-12-31 05:27:10	% Connection	10.1.0.100	10.10.0.100	37096 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-1_static_vti_2	192.168.200.1	Encrypt
2024-12-31 05:27:10	% Connection	10.1.0.100	10.10.0.100	37096 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-2	172.16.1.101	LAN		Decrypt
2024-12-31 05:27:07	% Connection	10.1.0.100	10.10.0.100	53570 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-2_static_vti_4	192.168.200.1	Encrypt
2024-12-31 05:27:07	% Connection	10.1.0.100	10.10.0.100	53570 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-2	172.16.2.101	LAN		Decrypt

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.