

Configurar SD-WAN para VPN site a site sobre firewall seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de recurso](#)

[Topologias cobertas](#)

[HUB & Spoke \(ISP único\)](#)

[HUB duplo e spoke \(ISP único para HUB redundante via EBGP entre HUB secundário e spokes\)](#)

[HUB e spoke duplos \(ISP duplo para HUB e ISP redundantes via EBGP entre HUB e spokes secundários\)](#)

[Conclusão](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve cenários de implantação de VPN baseada em rota com roteamento de sobreposição de BGP usando o recurso SD-WAN no Firewall Seguro.

Pré-requisitos

Todos os hubs e spokes estão executando o software FTD 7.6 ou posterior e são gerenciados pelo mesmo FMC, que também está executando o software 7.6 ou posterior.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IKEv2
- VPN de rota
- Interfaces de túnel virtual (VTI)
- IPsec
- BGP

Componentes Utilizados

As informações neste documento são baseadas em:

- Cisco Secure Firewall Threat Defense 7.7.10

- Cisco Secure Firewall Management Center 7.7.10

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.

Informações de recurso

O Management Center simplifica a configuração de túneis VPN e o roteamento entre centrais (hubs) e filiais remotas (spokes) usando o novo assistente SD-WAN.

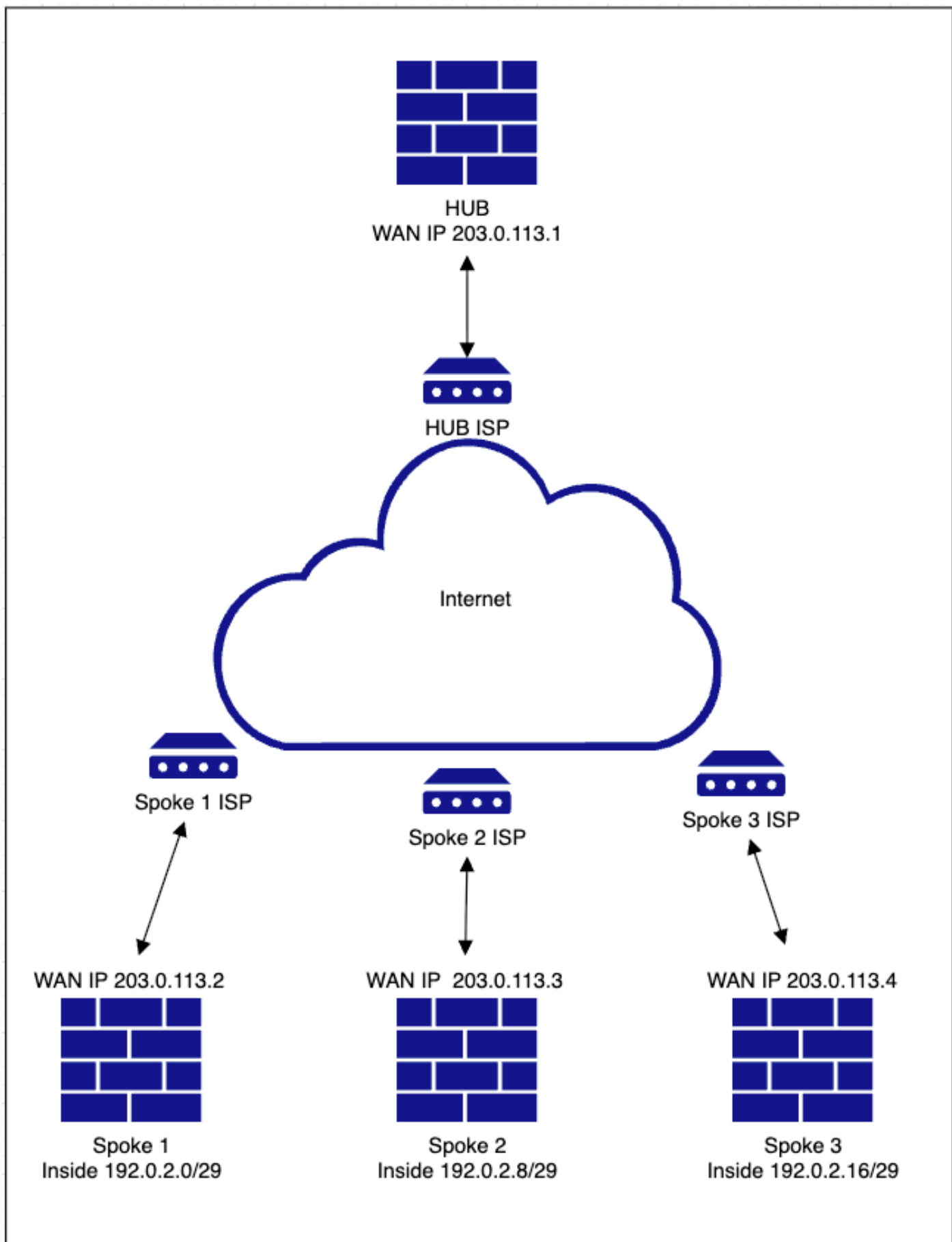
- Automatiza a configuração de VPN aproveitando DVTI (Dynamic Virtual Tunnel Interface) em hubs e SVTI (Static Virtual Tunnel Interface) em spokes, com roteamento de sobreposição habilitado através do BGP.
- Atribui automaticamente endereços IP SVTI para spokes e envia por push a configuração VTI completa, incluindo parâmetros de criptografia.
- Fornece configuração de roteamento fácil e em uma etapa dentro do mesmo assistente para ativar o BGP para roteamento de sobreposição.
- Permite o roteamento escalável e ideal, aproveitando o atributo de refletor de rota para BGP.
- Permite que vários spokes sejam adicionados simultaneamente com intervenção mínima do usuário.

Topologias cobertas

Neste artigo, várias topologias são cobertas para garantir que os usuários estejam cientes de vários cenários de implantação.

HUB & Spoke (ISP único)

Diagrama de Rede



Configurações

- Navegue até **Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create**.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin

Last Updated: 09:41 AM Refresh NAT Exemptions Add

Select... × Refresh

Create VPN Topology

Topology Name *
HUB-Spoke-VPN-Single-ISP

VPN Type

SD-WAN Topology New

Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☒ Hub and Spoke

[Prerequisites](#)

Route-Based VPN

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

SASE Topology

⚠️ SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

[Prerequisites](#)

[Refresh](#)

[Cancel](#) [Create](#)

· Adicione um hub e crie um DVTI na extremidade do hub. Como parte da configuração do DVTI, certifique-se de selecionar a interface de origem do túnel correta de acordo com a topologia.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

2 Spokes

3 Authentication

4 SD-WAN Settings

Next

Add Hub

Device * ftd1

Dynamic Virtual Tunnel Interface (DVTI) * VPN-OUT-1_dynamic_vti_1
Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.1)

Hub Gateway IP Address 203.0.113.1

Spoke Tunnel IP Address Pool * Select...

Cancel Add

Edit Virtual Tunnel Interface

General

Tunnel Type
☐ Static ☒ Dynamic

Name: * VPN-OUT-1_dynamic_vti_1

☒ Enabled

Description:

Security Zone: VPN-OUT-1

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Template ID: * 1 (1 - 10413)

Tunnel Source: GigabitEthernet0/0 (VPN-OUT-1) 203.0.113.1

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode: *
☒ IPv4 ☐ IPv6

IP Address: *
☐ Configure IP
☒ Borrow IP (IP unnumbered) Loopback1 (VPN-Loopback-IB...)

VPN Topology Usage

Cancel OK

- Crie um pool de endereços IP do Spoke Tunnel, clique em Salvar e em Adicionar. O pool de endereços IP é usado para atribuir endereços IP de túnel VTI aos spokes.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

Add Hub

Device * ⓘ

ftd1

Dynamic Virtual Tunnel Interface (DVTI) * ⓘ

VPN-OUT-1_dynamic_vti_1

Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.1)

Hub Gateway IP Address ⓘ

203.0.113.1

Spoke Tunnel IP Address Pool *

Select...

Cancel

Add

Add IPv4 Pool ⓘ

Name*

VPN-POOL-198.51.100.0

Description

IPv4 Address Range*

198.51.100.10-198.51.100.20

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

Mask*

255.255.255.0

☐ Allow Overrides

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

Cancel

Save

Cancel

Finish

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

Add Hub

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20

Next

2 Spokes ⓘ

Edit

3 Authentication Settings ⓘ

Edit

4 SD-WAN Settings

Edit

Cancel

Finish

- Clique em Avançar para continuar e adicionar os spokes. Você pode aproveitar qualquer opção de adição em massa se tiver nomes de interface/zona comuns ou adicionar spokes

individualmente.

The screenshot shows the FMC Site To Site configuration interface. The top navigation bar includes 'FMC Site To Site', 'Overview', 'Analysis', 'Policies', 'Devices' (selected), 'Objects', and 'Integration'. On the right, there are icons for 'Deploy', search, notifications (1), settings, help, and a user profile 'admin'. The main header displays 'HUB-Spoke-VPN-Single-ISP' and 'Hub and Spoke Route-Based (VTI) VPN Topology'. A vertical progress bar on the left indicates four steps: 1. Hubs (selected), 2. Spokes, 3. Authentication Settings, and 4. SD-WAN Settings. In the 'Hubs' step, a table lists configuration details: Device (ftd1), DVTI (VPN-OUT-1_dynamic_vti_1), Gateway IP Address (203.0.113.1), and Spoke Tunnel IP Address Pool (VPN-POOL-198.51.100.0). An 'Edit' link is present for the Hubs step. In the 'Spokes' step, there are three buttons: 'View Generated Tunnel Interfaces', 'Add Spokes (Bulk Addition)' (highlighted with a green box), and 'Add Spoke'. Below these buttons, a message states 'No spokes are configured. Add a spoke.' A 'Next' button is located between the 'Spokes' and 'Authentication Settings' steps. At the bottom right, there are 'Cancel' and 'Finish' buttons.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 1 ⚙️ ? admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs [Edit](#)

Device	ftd1	DVTI	VPN-OUT-1_dynamic_vti_1	Gateway IP Address	203.0.113.1	Spoke Tunnel IP Address Pool	VPN-POOL-198.51.100.0
--------	------	------	-------------------------	--------------------	-------------	------------------------------	-----------------------

2 Spokes [View Generated Tunnel Interfaces](#) **Add Spokes (Bulk Addition)** [Add Spoke](#)

No spokes are configured. Add a spoke.

[Next](#)

3 Authentication Settings [Edit](#)

4 SD-WAN Settings [Edit](#)

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

- Selecione os dispositivos e especifique um padrão de nomenclatura para a interface WAN/externa. Se os dispositivos compartilharem o mesmo nome de interface, o uso de iniciais será suficiente. Clique em Avançar e, se a validação for bem-sucedida, clique em Adicionar. Para adições em massa, você também pode usar o nome da região da mesma forma.

FMC
Site To Site

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Edit

Spokes (Bulk Addition) Add Spoke

Next

Edit

Edit

Cancel Finish

1 Add Devices

2 Validate Devices

Available Devices *

AddRemove

Selected Devices *

ftd2ftd3ftd4

Select VPN Interface Using *

☒ Interface Name Pattern

☐ Security Zone

Select...

+

CancelNext

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 1 2 3 4 admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs Edit

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

1 Add Devices

2 Validate Devices

✓ Device Name: ftd2, Interface Name: VPN-OUT-1

✓ Device Name: ftd3, Interface Name: VPN-OUT-1

✓ Device Name: ftd4, Interface Name: VPN-OUT-4

Spokes (Bulk Addition) Add Spoke

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Back Add

Cancel Finish

- Verifique os spokes e os detalhes da interface de sobreposição para garantir que as interfaces corretas estejam selecionadas e clique em Avançar.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Edit

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

[View Generated Tunnel Interfaces](#)[Add Spokes \(Bulk Addition\)](#)[Add Spoke](#)

Device	VPN Interface	Local Tunnel (IKE) Identity	
ftd2 Threat Defense	VPN-OUT-1 (GigabitEthernet0/0) IP Address:203.0.113.2	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd2	 
ftd3 Threat Defense	VPN-OUT-1 (GigabitEthernet0/0) IP Address:203.0.113.3	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd3	 
ftd4 Threat Defense	VPN-OUT-4 (GigabitEthernet0/0) IP Address:203.0.113.4	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd4	 

[Next](#)

<<

Viewing 1-3 of 3

>>

3 Authentication Settings

Edit

4 SD-WAN Settings

Edit

Cancel

[Finish](#)

- Você pode reter os parâmetros padrão para a configuração IPsec ou especificar cifras personalizadas conforme necessário. Clique em Avançar para continuar. Neste documento, você está usando os parâmetros padrão.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1

Hubs

Edit

2

Spokes

Edit

3

Authentication Settings

Authentication Type*

Pre-shared Automatic Key

Pre-shared Key Length*

24

The range is 1 to 127.

Next

Transform Sets (IPsec Proposals)*

AES-GCM

Show Details

IKEv2 Policies*

AES-GCM-NUL-STA-LATEST

Show Details

4

SD-WAN Settings

Edit

Cancel

Finish

- Finalmente, você pode configurar o roteamento de sobreposição dentro do mesmo assistente para essa topologia especificando os parâmetros BGP apropriados, como o número AS, o anúncio de interface interna e as tags de comunidade para filtragem de prefixo. A zona de segurança pode ajudar na filtragem de tráfego por meio de políticas de controle de acesso, enquanto você também pode criar um objeto para interfaces e usá-las na redistribuição de interfaces conectadas se o nome for diferente do nome interno ou não for simétrico entre os dispositivos na topologia.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1

Hubs

Edit

Device

ftd1

DVTI

VPN-OUT-1_dynamic_vti_1

Gateway IP Address

203.0.113.1

Spoke Tunnel IP Address Pool

VPN-POOL-198.51.100.32

2

Spokes

Edit

Device

ftd2

VPN Interface

VPN-OUT-1

Local Tunnel (IKE) Identity

Key ID: HUB-Spoke-VPN-Single-ISP_ftd2

ftd3

VPN-OUT-1

Key ID: HUB-Spoke-VPN-Single-ISP_ftd3

ftd4

VPN-OUT-4

Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3

Authentication Settings

Edit

Authentication

Pre-shared Automatic Key

Pre-shared Key Length

24

4

SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) 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

VPN-OUT-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 *

65500

Community Tag for Local Routes *

101010

☒ Redistribute Connected Interfaces

Default inside*

+

☒ 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 Avançar, em Concluir e, finalmente, em Implantar para concluir o processo.

Verificação

- Você pode verificar o status do túnel navegando para Devices > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ SECURE

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select...

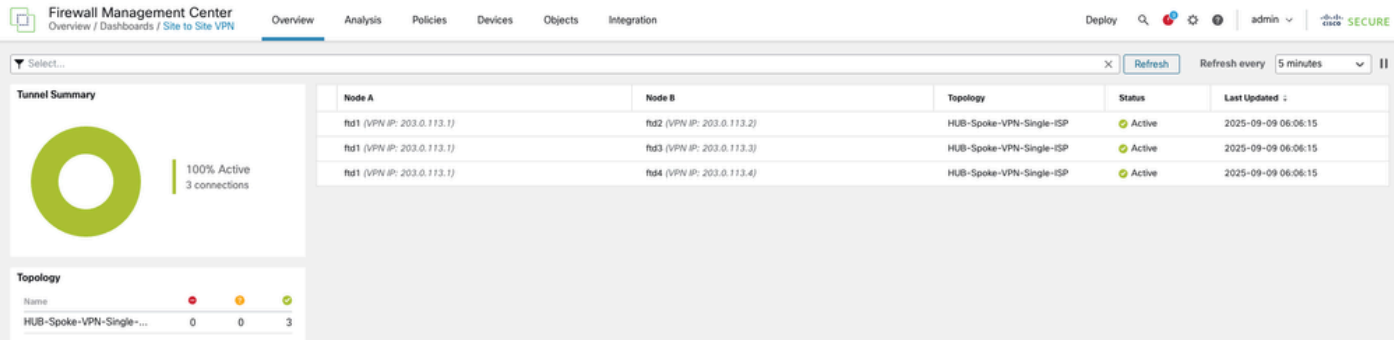
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	Tunnels	✓	

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_static... (198.51.100.10)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.11)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.12)

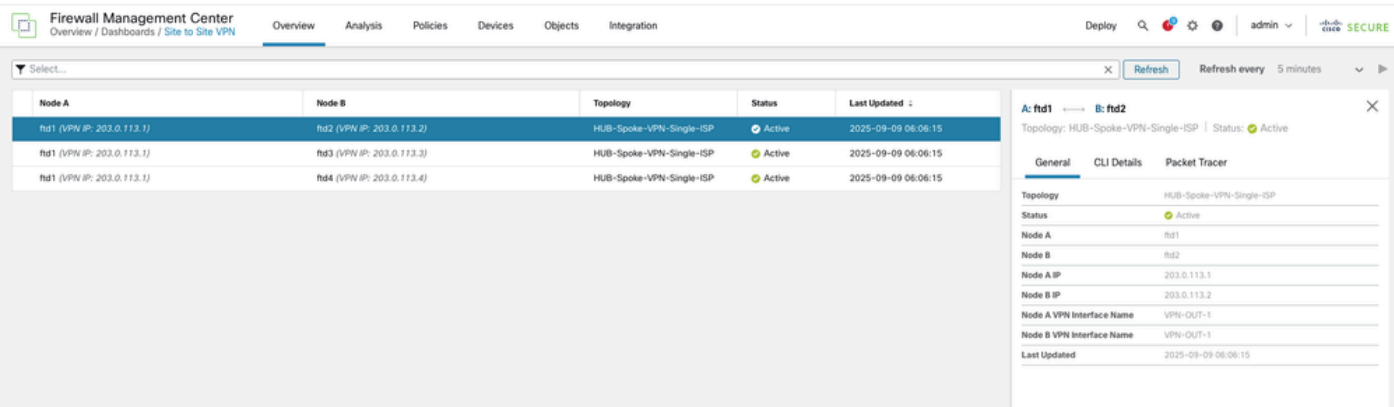
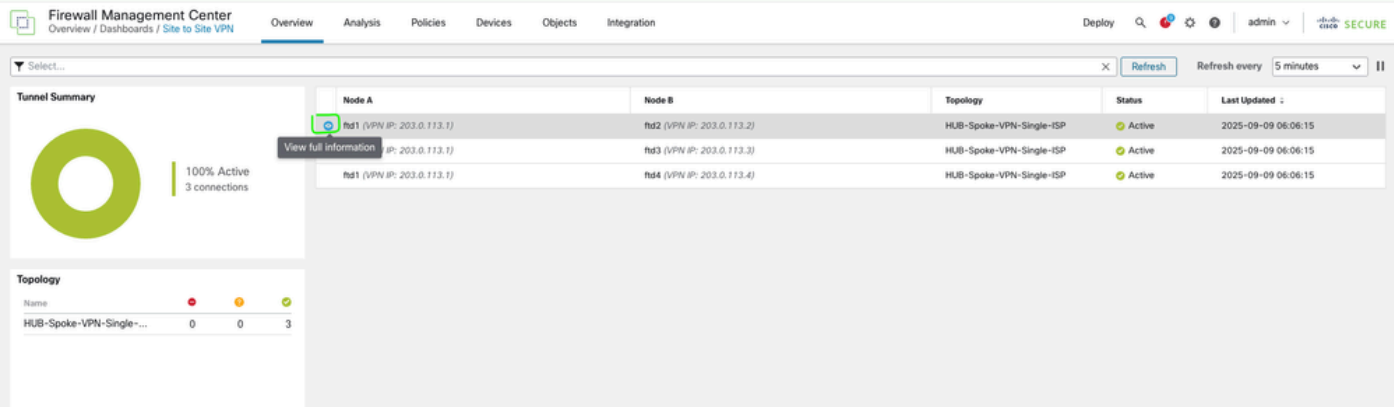
Viewing 1-3 of 3

- Detalhes adicionais podem ser verificados navegando até Overview > Dashboards > Site to

Site VPN.



- Para obter mais informações, selecione o túnel e clique em View Full Information.



Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Select...

Node A	Node B	Topology	Status	Last Updated
ftd1 (VPN IP: 203.0.113.1)	ftd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15

Refresh Refresh every 5 minutes

A: ftd1 ↔ B: ftd2
Topology: HUB-Spoke-VPN-Single-ISP | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (203.0.113.1/500)	Node B (203.0.113.2/500)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)

IPsec Security Associations (1)

```

0.0.0.0/0.0.0.0/0
0.0.0.0/0.0.0.0/0

ftd1 (VPN Interface IP: 203.0.113.1)
show crypto ipsec sa peer 203.0.113.2
peer address: 203.0.113.2
interface: VPN-OUT-1_dynamic_vti_1_va9
Crypto map tag: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map, seq num: 1, local addr: 203.0.113.1

Protected vrf (jvrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 203.0.113.2

#pkts encaps: 155, #pkts encrypt: 155, #pkts digest: 155
#pkts decaps: 154, #pkts decrypt: 154, #pkts verify: 154
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 155, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#pkts not offload decrypted: 154

ftd2 (VPN Interface IP: 203.0.113.2)
show crypto ipsec sa peer 203.0.113.1
peer address: 203.0.113.1
interface: VPN-OUT-1_static_vti_1
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 203.0.113.2

Protected vrf (jvrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 203.0.113.1

```

Viewing 1-3 of 3

- A saída é mostrada diretamente da CLI do FTD e pode ser atualizada para exibir contadores atualizados e informações importantes, como detalhes do Índice de Parâmetros de Segurança (SPI).

Tunnel Details	
Summary	
Node A (203.0.113.1/500)	Node B (203.0.113.2/500)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)
IPsec Security Associations (1)	
0.0.0.0/0.0.0.0/0/0	0.0.0.0/0.0.0.0/0/0
ftd1 (VPN Interface IP: 203.0.113.1)	ftd2 (VPN Interface IP: 203.0.113.2)
show crypto ipsec sa peer 203.0.113.2 peer address: 203.0.113.2 interface: VPN-OUT-1_dynamic_vti_1_va9 Crypto map tag: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map, seq num: 100	show crypto ipsec sa peer 203.0.113.1 peer address: 203.0.113.1 interface: VPN-OUT-1_static_vti_1 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, loc
Protected vrf (ivrf): Global	Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)	local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)	remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 203.0.113.2	current_peer: 203.0.113.1
#pkts encaps: 155, #pkts encrypt: 155, #pkts digest: 155	#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 154, #pkts decrypt: 154, #pkts verify: 154	#pkts decaps: 155, #pkts decrypt: 155, #pkts verify: 155
#pkts compressed: 0, #pkts decompressed: 0	#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 155, #pkts comp failed: 0, #pkts decomp t	#pkts not compressed: 154, #pkts comp failed: 0, #pkts decomp t
#pre-frag successes: 0, #pre-frag failures: 0, #fragments creat	#pre-frag successes: 0, #pre-frag failures: 0, #fragments creat
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reas	#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reas
#TFC rcvd: 0, #TFC sent: 0	#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0	#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#pkts not offload decrypted: 154	#pkts not offload decrypted: 155
#send errors: 0, #recv errors: 0	#send errors: 0, #recv errors: 0
local crypto endpt.: 203.0.113.1/500, remote crypto endpt.: 203	local crypto endpt.: 203.0.113.2/500, remote crypto endpt.: 203
path mtu 1500, ipsec overhead 55(36), media mtu 1500	path mtu 1500, ipsec overhead 55(36), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df	PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled	ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 3EE69843	current outbound spi: D113FBF4
current inbound spi : D113FBF4	current inbound spi : 3EE69843
inbound esp sas:	inbound esp sas:
spi: 0xD113FBF4 (3507747828)	spi: 0x3EE69843 (1055299651)
SA State: active	SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression	transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings =(L2L, Tunnel, IKEv2, VTI, }	in use settings =(L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 9, crypto-map: VPN-OUT-1_dynamic_vti_1_vt	slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-
sa timing: remaining key lifetime (sec): 24309	sa timing: remaining key lifetime (sec): 24308

Close Refresh

- A CLI do FTD também pode ser usada para verificar informações de roteamento e o status de peering do BGP.

No HUB

<#root>

HUB1# show bgp summary

```
BGP router identifier 198.51.100.3, local AS number 65500
BGP table version is 7, main routing table version 7
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
```

1/1 BGP path/bestpath attribute entries using 208 bytes of memory
 1 BGP community entries using 24 bytes of memory
 1 BGP route-map cache entries using 64 bytes of memory
 0 BGP filter-list cache entries using 0 bytes of memory
 BGP using 856 total bytes of memory
 BGP activity 2/0 prefixes, 4/2 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.10	4	65500	4	6	7	0	0	00:00:45	0

<<<< spoke 1 bgp peering

198.51.100.11	4	65500	5	5	7	0	0	00:00:44	1
---------------	---	-------	---	---	---	---	---	----------	---

<<<< spoke 2 bgp peering

198.51.100.12	4	65500	5	5	7	0	0	00:00:52	1
---------------	---	-------	---	---	---	---	---	----------	---

<<<< spoke 3 bgp peering

<#root>

HUB1# show route bgp

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

B 192.0.2.0 255.255.255.248 [200/1] via 198.51.100.10, 00:00:18

<<<<<<< spoke 1 inside network

B 192.0.2.8 255.255.255.248 [200/1] via 198.51.100.11, 00:08:08

<<<<<<< spoke 2 inside network

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.12, 00:08:16

<<<<<<< spoke 3 inside network

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.10 routes

<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.0/29	198.51.100.10	1	100	0	?

<<<<<<<< routes received from spoke 1

Total number of prefixes 1

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.11 routes

<<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.11	1	100	0	?

<<<<<<<< routes received from spoke 2

Total number of prefixes 1

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.12 routes

<<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.16/29	198.51.100.12	1	100	0	?

<<<<<<<< routes received from spoke 3

Total number of prefixes 1

No lado do raio

A mesma verificação também pode ser executada nos dispositivos spoke. Aqui está um exemplo de um dos spokes.

<#root>

Spoke1# show bgp summary

BGP router identifier 198.51.100.4, local AS number 65500
BGP table version is 12, main routing table version 12
3 network entries using 600 bytes of memory
3 path entries using 240 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
2 BGP rrinfo entries using 80 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1360 total bytes of memory
BGP activity 5/2 prefixes, 7/4 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.1	4	65500	12	11	12	0	0	00:07:11	2

<<<<<<<< BGP peering with HUB

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 routes

BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.1	1	100	0	?

<<<<<<< route received from HUB for spoke 2

*>i192.0.2.16/29	198.51.100.1	1	100	0	?
------------------	--------------	---	-----	---	---

<<<<<<< route received from HUB for spoke 3

Total number of prefixes 2

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 advertised-routes

BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.0.2.0/29	0.0.0.0	0		32768	?

<<<<<<< route advertised by this spoke into BGP

Total number of prefixes 1

<#root>

Spoke1# show route bgp

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

B 192.0.2.8 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

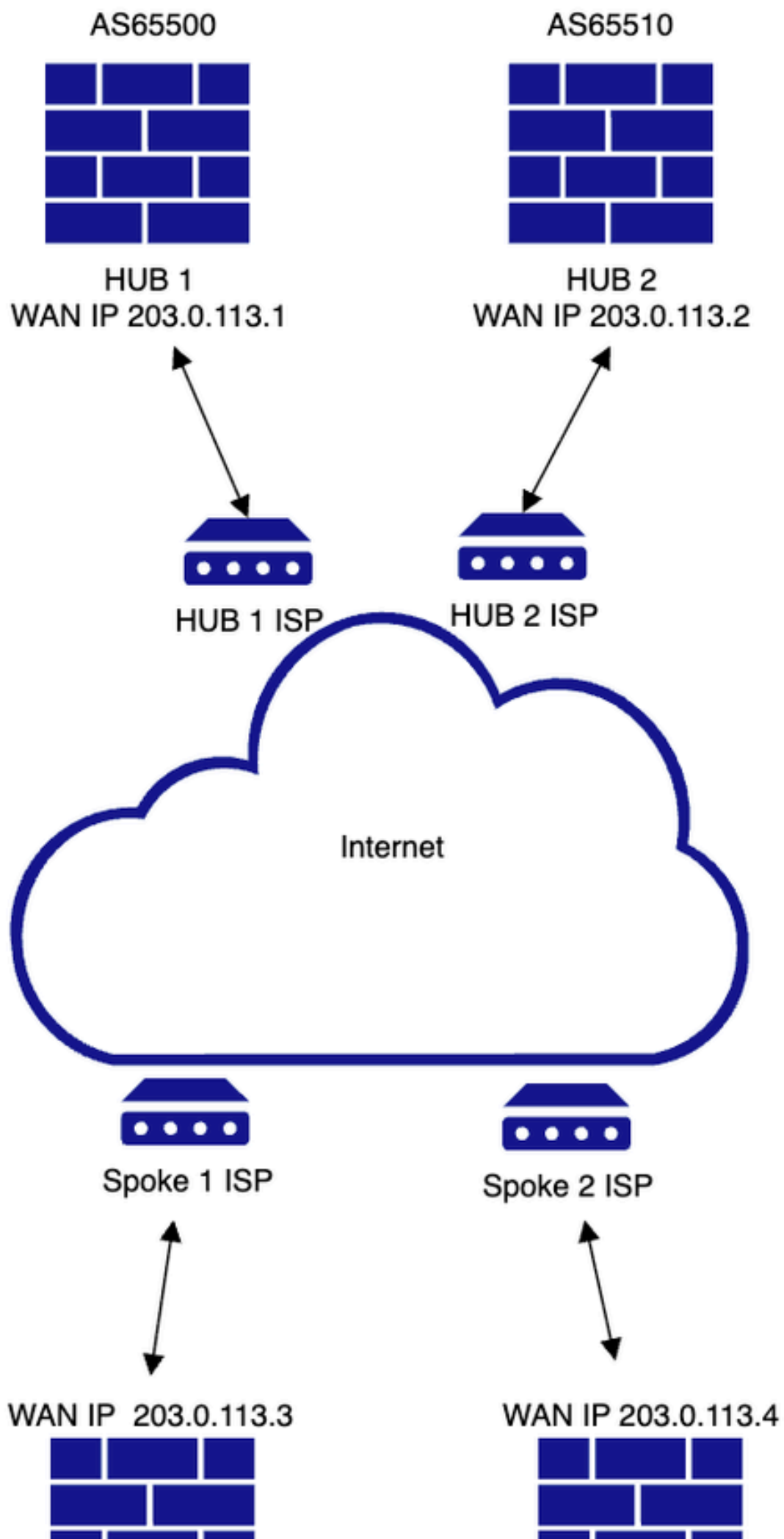
<<<<<< spoke 2 inside network

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

<<<<<< spoke 3 inside network

HUB duplo e spoke (ISP único para HUB redundante via EBGP entre HUB secundário e spokes)

Diagrama de Rede



Após adicionar o primeiro HUB, continue adicionando o segundo HUB usando as mesmas etapas anteriormente usadas para o HUB1.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 3 ⚙️ ? admin ▾

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.11

Next

- Continue para criar a Dynamic Virtual Tunnel Interface (DVTI).

Firewall Management Center Devices / VPN / Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 3 ⚙️ ? admin ▾

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Add Virtual Tunnel Interface

Add Loopback Interface

- Um novo pool de endereços IP é necessário para túneis VTI do HUB 2 no lado do spoke. Crie e configure o novo pool e salve as alterações.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⌂ admin ✓ cisco SECURE

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20

Next

2 Spokes

Device ftd3 ftd4 VPN Interface VPN-OUT-1 VPN-OUT-4 Local Tunnel (IKE Identity)

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

4 SD-WAN Settings

BGP on Overlay Enabled
Hubs and spokes are configured with internal BGP and AS number 65500.

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
VPN-OUT-1_dynamic_vti_1
Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.2)

Hub Gateway IP Address
203.0.113.2

Spoke Tunnel IP Address Pool *
VPN-POOL-198.51.100.32

Cancel Add

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⌂ admin ✓ cisco SECURE

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20
ftd2 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.2	VPN-POOL-198.51.100.32 Range: 198.51.100.40-198.51.100.50

Next

2 Spokes

Device ftd3 ftd4 VPN Interface VPN-OUT-1 VPN-OUT-4 Local Tunnel (IKE Identity)

Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

4 SD-WAN Settings

BGP on Overlay Enabled
Hubs and spokes are configured with internal BGP and AS number 65500.

Cancel Finish

- Para configurar o peering eBGP entre o segundo HUB e os spokes, modifique as configurações de SD-WAN na etapa final. Habilite a opção O HUB secundário está em um sistema autônomo diferente e especifique o número do sistema autônomo (AS) para o HUB secundário. O IBGP também pode ser usado se não houver limitação de usar um número AS diferente em seu ambiente, deixando a opção O HUB secundário está em um sistema autônomo diferente desmarcada. Isso envia a mesma marca de comunidade e número AS para o HUB secundário também. O artigo concentra-se no eBGP para a configuração atual.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin ▾ **SECURE**

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs
2 Spokes
3 Authentication Settings
4 SD-WAN Settings

Device ftd1 ftd2
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1 203.0.113.2
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0 VPN-POOL-198.51.100.32

Device ftd3 ftd4
VPN Interface VPN-OUT-1 VPN-OUT-4
Local Tunnel (IKE) Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd3 Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) 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

VPN-OUT-1 x v +

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 * 65500 Community Tag for Local Routes * 101010

☒ Redistribute Connected Interfaces

Default inside* v +

☒ Secondary Hub is in different Autonomous System

Autonomous System Number * 65510 Community Tag for Learned Routes * 010101

☒ 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.

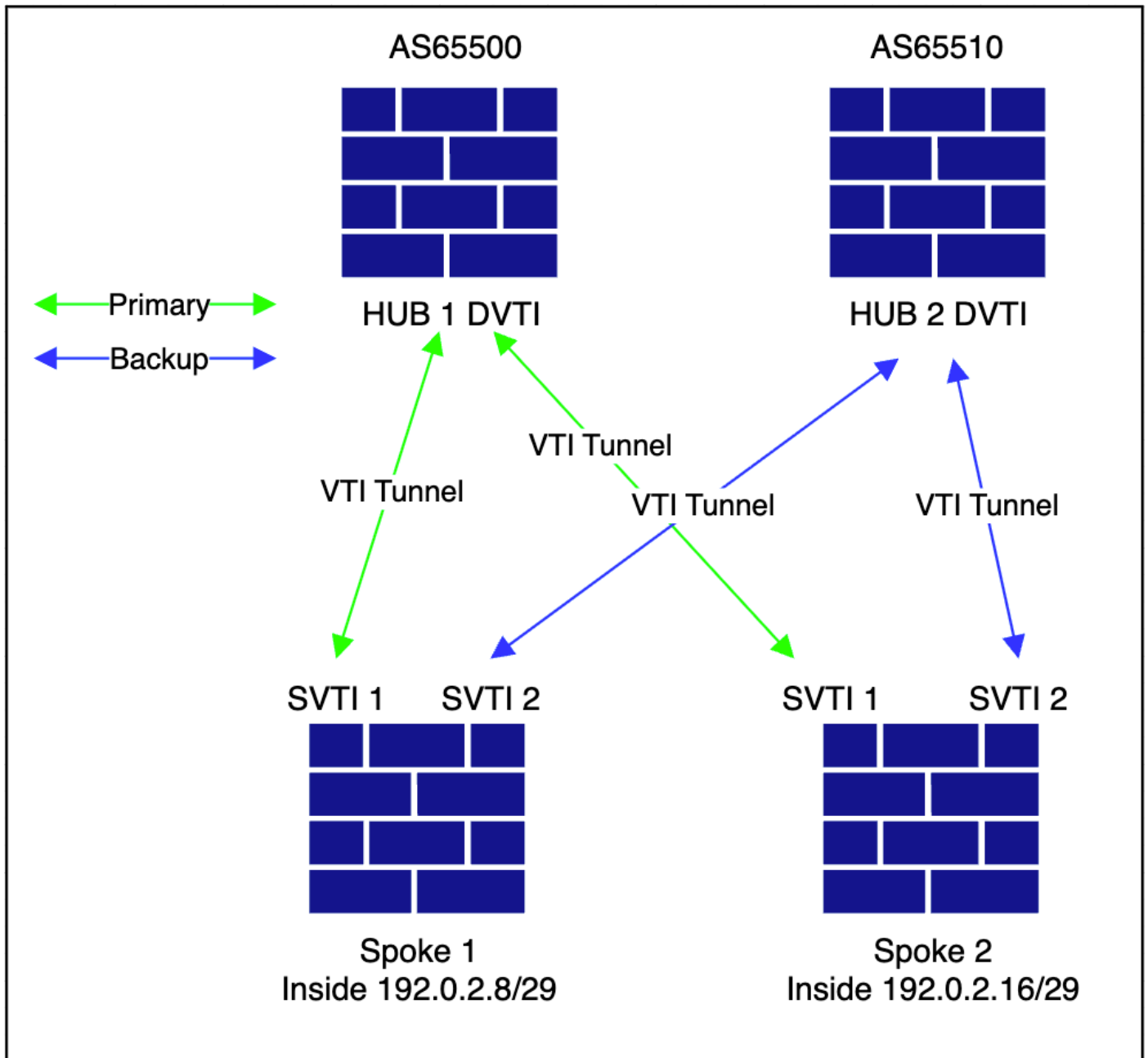
Next You have unsaved changes

Cancel Finish

Certifique-se de que o número do sistema autônomo (AS) e a marca de comunidade sejam exclusivos nesta configuração.

Verificação

Este diagrama ilustra a topologia de sobreposição.



- No FMC, navegue até Devices > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ **SECURE**

Last Updated: 02:20 PM Refresh NAT Exemptions Add

Select... X Refresh

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
Dual-HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	4 Tunnels	✓	

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.11)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynam... (198.51.100.2)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.40)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynam... (198.51.100.2)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.41)

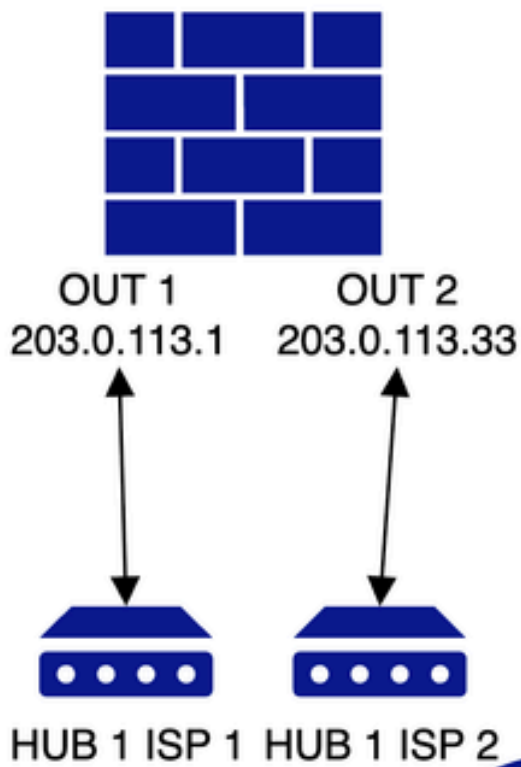
<< Viewing 1-4 of 4 >>

- Todas as outras etapas permanecem inalteradas.

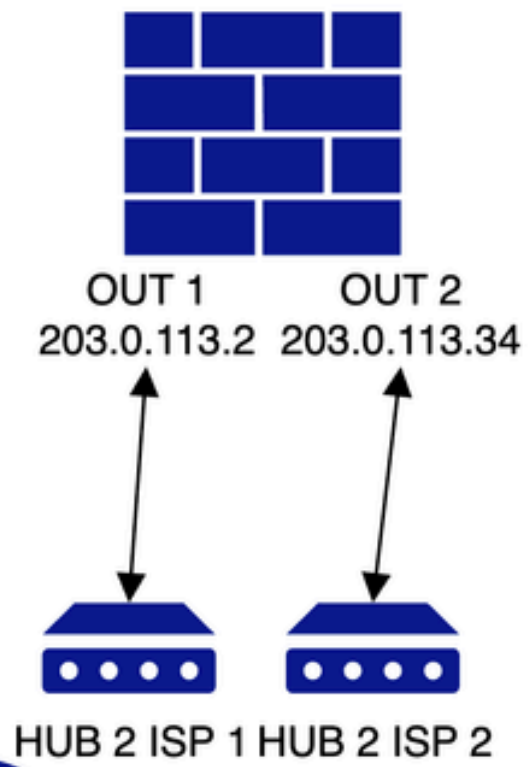
HUB e spoke duplos (ISP duplo para HUB e ISP redundantes via EBGP entre HUB e spokes secundários)

Diagrama de Rede

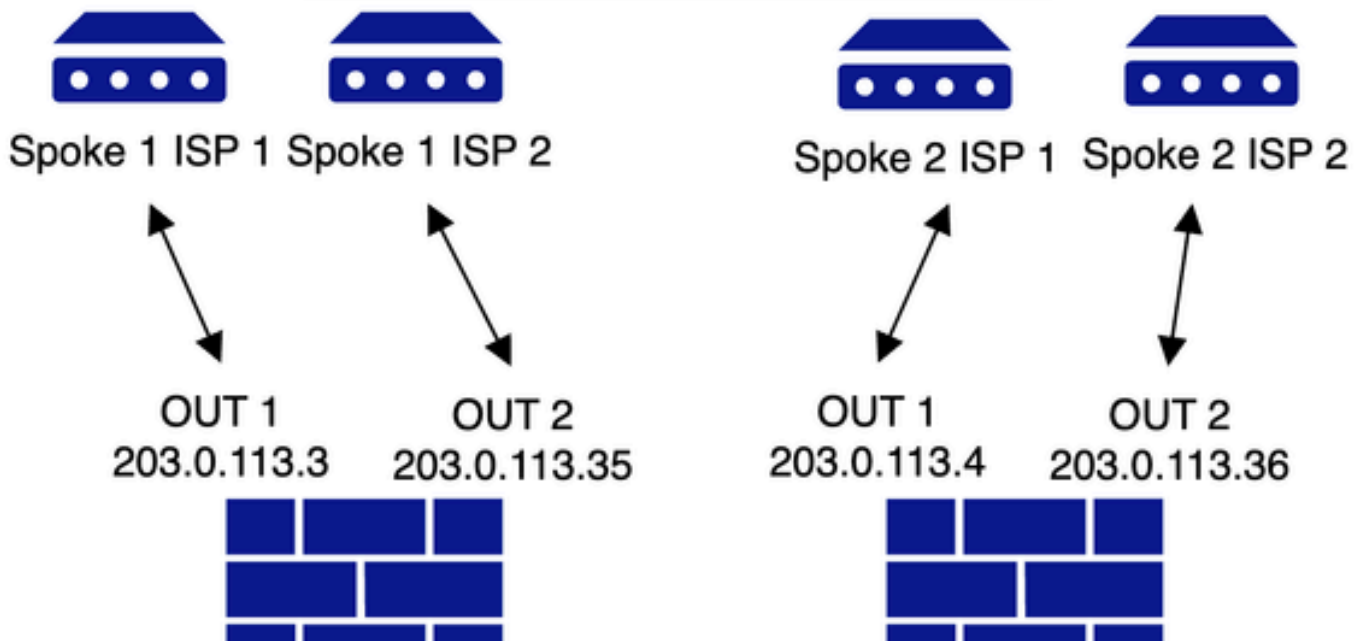
AS65500



AS65510



Internet



A implantação para esta topologia é ignorada usando o primeiro ISP, pois isso é abordado na topologia anterior.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
Dual-HUB-Spoke-VPN-Dual-ISP-1	Route Based (VTI)	SD-WAN Topology	4 - Tunnels	✓	
Hub					
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic_... (198.51.100.1)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static_... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic_... (198.51.100.1)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static_... (198.51.100.11)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynamic_... (198.51.100.2)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static_... (198.51.100.40)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynamic_... (198.51.100.2)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static_... (198.51.100.41)

- Em seguida, prossiga para adicionar a segunda topologia criando duas interfaces DVTI adicionais por HUB, cada uma utilizando a interface subjacente para ISP 2 (VPN-OUT-2).

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy

Dual-HUB-Spoke-VPN-Dual-ISP-2
Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Device * ftd1

Dynamic Virtual Tunnel Interface (DVTI) * Select... +

Hub Gateway IP Address

Cancel Add

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
Static Dynamic

Name: * VPN-OUT-1_dynamic_vti_2

Enabled

Description:

Security Zone:

Priority: 0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Template ID: * 2 (1 - 10413)

Tunnel Source: GigabitEthernet0/1 (VPN-OUT-2) 203.0.113.33

Ipssec Tunnel Details
Ipssec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

Ipssec Tunnel Mode: * IPv4 IPv6

IP Address: *
Configure IP 169.254.2.1/30
Borrow IP (IP unnumbered) Loopback2 (VPN-2-LOOPBACK...) +

Cancel OK

- Um pool adicional de endereços IP da VPN é provisionado especificamente para endereços da Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) spoke.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Add Hub

Device* ⓘ

ftd1

Dynamic Virtual Tunnel Interface (DVTI)* ⓘ

VPN-OUT-1_dynamic_vti_2

Tunnel Source: VPN-OUT-2 (IP Address: 203.0.113.33)

Hub Gateway IP Address ⓘ

203.0.113.33

Spoke Tunnel IP Address Pool*

VPN-POOL-198.51.100.70

Cancel Add

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool	
ftd1 Threat Defense	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source: GigabitEthernet0/1 (VPN-OUT-2)	203.0.113.33	VPN-POOL-198.51.100.70 Range: 198.51.100.70-198.51.100.80	Add Hub

Spokes ⓘ

Authentication Settings ⓘ

SD-WAN Settings

Edit Edit Edit

Cancel Finish

- Para adicionar um hub secundário, repita o processo criando o DVTI 2 usando a interface ISP secundária (VPN-OUT-2) e configure um pool IP adicional para endereços VTI de extremidade de spoke.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)
ftd1	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source:GigabitEthernet0/1 (VPN-OUT-2)

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
Select... +

Hub Gateway IP Address

Cancel Add

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☐ Static ☒ Dynamic

Name:*
VPN-OUT-1_dynamic_vti_2

☒ Enabled

Description:

Security Zone:
VPN-OUT-2

Priority:
0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Template ID:*
2 (1 - 10413)

Tunnel Source:
GigabitEthernet0/1 (VPN-OUT-2) 203.0.113.34

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☐ Configure IP 169.254.2.1/30 ⓘ
☒ Borrow IP (IP unnumbered) Loopback2 (VPN-2-LOOPBACK) +

Cancel OK

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source:GigabitEthernet0/1 (VPN-OUT-2)	203.0.113.34	VPN-POOL-198.51.100.70 Range: 198.51.100.70-198.51.100.80

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Next

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
VPN-OUT-1_dynamic_vti_2 +

Tunnel Source: VPN-OUT-2 (IP Address: 203.0.113.34)

Hub Gateway IP Address
203.0.113.34

Spoke Tunnel IP Address Pool*
VPN-POOL-198.51.100.100 x +

Cancel Add

Cancel Finish

- Ao adicionar um spoke, certifique-se de que a interface de WAN/base correta esteja especificada para os túneis VTI. Essa topologia está usando a interface secundária do ISP

VPN-OUT-2.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 ftd2 DVTI VPN-OUT-1_dynamic_vti_2 VPN-OUT-1_dynamic_vti_2 Gateway IP Address 203.0.113.33 203.0.113.34 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70 VPN-POOL-198.51.100.100

2 Spokes

Next

3 Authentication Settings

4 SD-WAN Settings

Add Bulk Spokes

1 Add Devices

2 Validate Devices

✓ Device Name: ftd3, Interface Name: VPN-OUT-2

✓ Device Name: ftd4, Interface Name: VPN-OUT-2

Cancel

Back

Add

Spokes (Bulk Addition)

Add Spoke

Cancel

Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 ftd2 DVTI VPN-OUT-1_dynamic_vti_2 VPN-OUT-1_dynamic_vti_2 Gateway IP Address 203.0.113.33 203.0.113.34 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70 VPN-POOL-198.51.100.100

2 Spokes

View Generated Tunnel Interfaces

Add Spokes (Bulk Addition)

Add Spoke

Device	VPN Interface	Local Tunnel (IKE) Identity
ftd3 Threat Defense	VPN-OUT-2 (GigabitEthernet0/1) IP Address:203.0.113.35	Type: Key ID Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd3
ftd4 Threat Defense	VPN-OUT-2 (GigabitEthernet0/1) IP Address:203.0.113.36	Type: Key ID Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd4

Next

3 Authentication Settings

4 SD-WAN Settings

Cancel

Finish

Viewing 1-2 of 2

- Ao configurar o roteamento, certifique-se de que as tags de comunidade e os números de AS para ambos os HUBs nessa topologia sejam consistentes com aqueles usados na topologia anterior do ISP1. A topologia está usando diferentes zonas de segurança, mas as configurações restantes, como números de AS para HUBs primários e secundários, juntamente com marcas de comunidade, são as mesmas. Isso é obrigatório para que a interface do usuário conclua a validação da topologia.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ
Device ftd1
Device ftd2
DVTI VPN-OUT-1_dynamic_vti_2
DVTI VPN-OUT-1_dynamic_vti_2
Gateway IP Address 203.0.113.33
Gateway IP Address 203.0.113.34
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.100

Edit

2 Spokes ⓘ
Device ftd3
Device ftd4
VPN Interface VPN-OUT-2
VPN Interface VPN-OUT-2
Local Tunnel (IKE) Identity Key ID: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd3
Local Tunnel (IKE) Identity Key ID: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd4

Edit

3 Authentication Settings ⓘ
Authentication Pre-shared Automatic Key
Pre-shared Key Length 24

Edit

4 SD-WAN Settings
Spoke Tunnel Interface Auto Generation
Static Virtual Tunnel Interfaces (SVTIs) 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 ⓘ
VPN-OUT-2 X +
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 * ⓘ 65500
Community Tag for Local Routes * ⓘ 101010
☒ Redistribute Connected Interfaces ⓘ
Default Inside* +
☒ Secondary Hub is in different Autonomous System ⓘ
Autonomous System Number * ⓘ 65510
Community Tag for Learned Routes * ⓘ 010101
☒ 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.

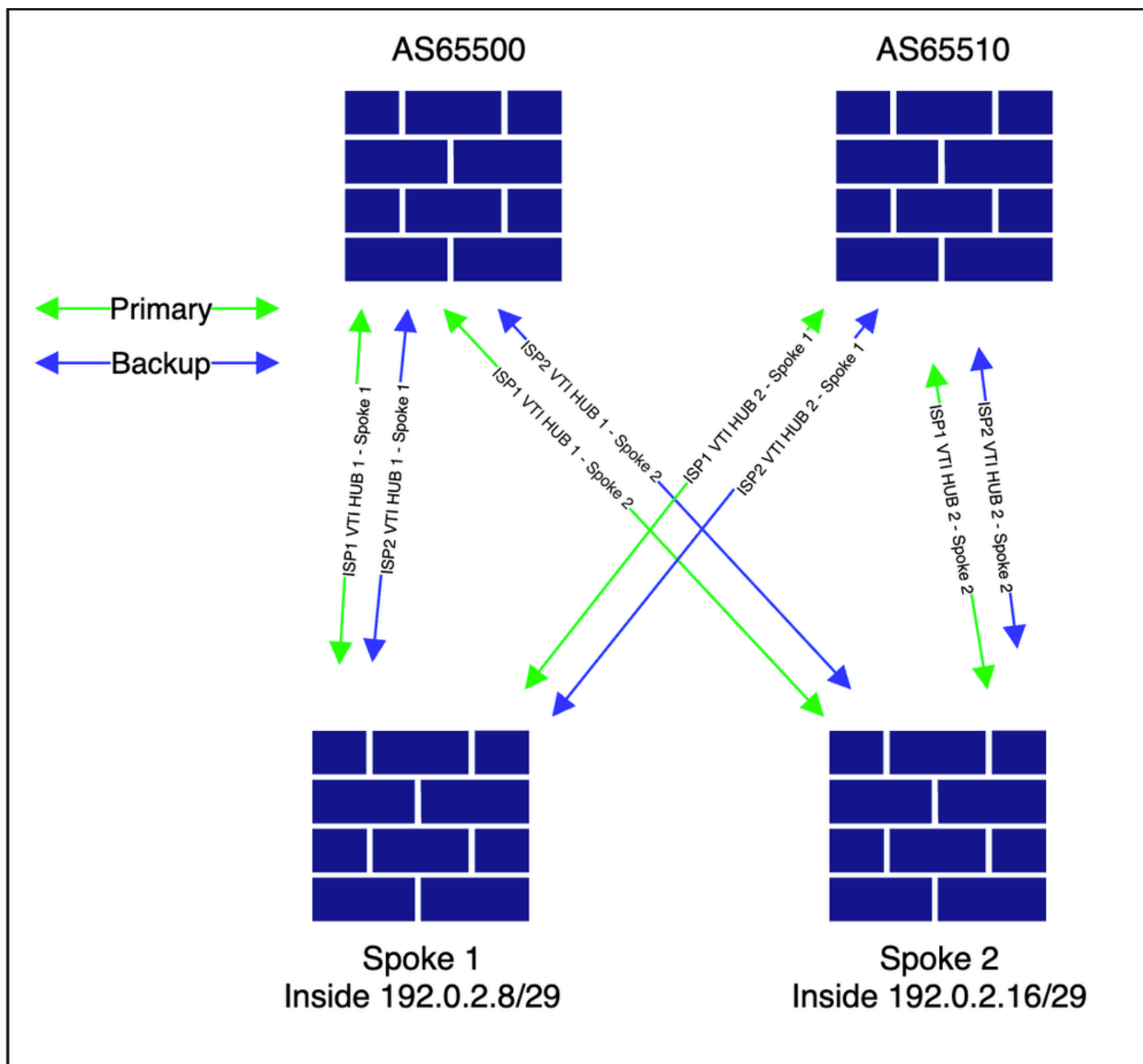
Next You have unsaved changes

Cancel Finish

- Todas as outras configurações permanecem inalteradas. Conclua o assistente e continue com a implantação.

Verificação

- A topologia é exibida conforme mostrado.



- Navegue até Devices > VPN > Site to Site para visualizar a topologia.

198.51.100.4 4 65510 183 183 4 0 0 03:16:30 2

<<<<<<<< HUB 2 ISP 2 VTI

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.1 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.16/29	198.51.100.1	1	100	0	?

<<<<<<< spoke 2 network received via HUB 1 ISP 1 tunnel

Total number of prefixes 1

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.3 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*mi192.0.2.16/29	198.51.100.3	1	100	0	?

<<<<<<< spoke 2 network received via HUB 1 ISP 2 tunnel

Total number of prefixes 1

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.2 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.2	100		0	65510 65510 ?

<<<<<<< inside network receieved cause we advertised it to HUB 1 from ISP 2 topology

* 192.0.2.16/29	198.51.100.2	100		0	65510 65510 ?
-----------------	--------------	-----	--	---	---------------

<<<<<<< spoke 2 network received via HUB 2 ISP 1 tunnel but not preferred

Total number of prefixes 2

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.4 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.4	100		0	65510 65510 ?

<<<<<<< inside network received cause we advertised it to HUB 2 from ISP 1 topology

* 192.0.2.16/29	198.51.100.4	100		0	65510 65510 ?
-----------------	--------------	-----	--	---	---------------

<<<<<<< spoke 2 network received via HUB 2 ISP 2 tunnel but not preferred

Total number of prefixes 2

A tabela de roteamento é exibida como mostrado, confirmando que o tráfego tem balanceamento de carga entre os dois links no lado do spoke.

<#root>

Spoke1#show route bgp

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

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.3, 03:23:53

<<<<< multipath for spoke 2 inside network

[200/1] via 198.51.100.1, 03:23:53

<<<<< multipath for spoke 2 inside network

<#root>

Spoke1#show bgp 192.0.2.16

BGP routing table entry for 192.0.2.16/29, version 4

Paths: (4 available, best #4, table default)

Multipath: eBGP iBGP

Advertised to update-groups:

2 4

65510 65510

198.51.100.4 from 198.51.100.4 (198.51.100.4)

<<<< HUB2 ISP2 next-hop

Origin incomplete, metric 100, localpref 100, valid, external

Community: 10101

Local

198.51.100.3 from 198.51.100.3 (198.51.100.3)

<<<< HUB1 ISP2 next-hop

Origin incomplete, metric 1, localpref 100, valid, internal, multipath

Community: 10101

Originator: 203.0.113.36, Cluster list: 198.51.100.3

65510 65510

198.51.100.2 from 198.51.100.2 (198.51.100.4)

<<<< HUB2 ISP1 next-hop

Origin incomplete, metric 100, localpref 100, valid, external

Community: 10101

Local

198.51.100.1 from 198.51.100.1 (198.51.100.3)

<<<< HUB1 ISP1 next-hop

Origin incomplete, metric 1, localpref 100, valid, internal, multipath, best

Community: 10101

Originator: 203.0.113.36, Cluster list: 198.51.100.3

Conclusão

A finalidade deste artigo é explicar vários cenários de implantação que podem ser facilmente implementados usando um único assistente de configuração.

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o TAC. É necessário um contrato de suporte válido: [Cisco Worldwide Support Contacts](#).
- Você também pode visitar a Cisco VPN Community [aqui](#).

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.