

Configuración de SD-WAN para VPN de sitio a sitio a través de firewall seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Información sobre la Función](#)

[Topologías cubiertas](#)

[HUB y radio \(ISP único\)](#)

[HUB y radio duales \(ISP único para HUB redundante a través de EGBP entre HUB y radios secundarios\)](#)

[HUB y radio duales \(ISP duales para HUB redundante e ISP a través de EGBP entre HUB y radios secundarios\)](#)

[Conclusión](#)

[Información Relacionada](#)

Introducción

Este documento describe escenarios de implementación de VPN basada en rutas con ruteo de superposición BGP mediante la función SD-WAN en Secure Firewall.

Prerequisites

Todos los hubs y spokes ejecutan el software FTD 7.6 o posterior y se gestionan a través del mismo FMC, que también ejecuta el software 7.6 o posterior.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IKEv2
- VPN basada en ruta
- Interfaces de túnel virtual (VTI)
- IPsec
- BGP

Componentes Utilizados

La información de este documento se basa en:

- Cisco Secure Firewall Threat Defence 7.7.10
- Cisco Secure Firewall Management Center 7.7.10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información sobre la Función

Management Center simplifica la configuración de túneles VPN y el routing entre la sede central (hubs) y las sucursales remotas (spokes) mediante el nuevo asistente para SD-WAN.

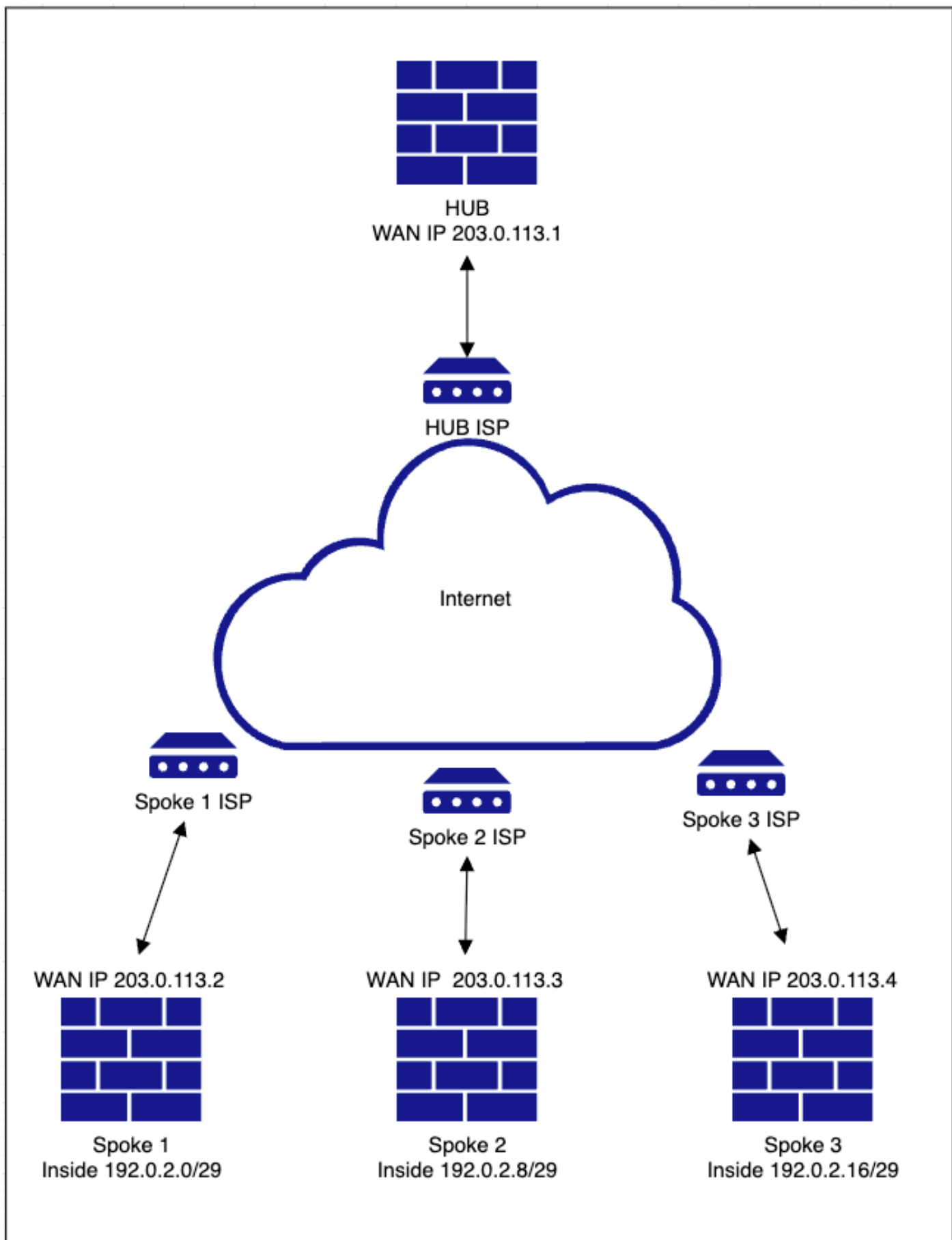
- Automatiza la configuración de VPN aprovechando el DVTI (Dynamic Virtual Tunnel Interface) en los hubs y el SVTI (Static Virtual Tunnel Interface) en los spokes, con el ruteo superpuesto habilitado a través de BGP.
- Asigna automáticamente direcciones IP SVTI para radios e introduce la configuración VTI completa, incluidos los parámetros criptográficos.
- Proporciona una configuración de ruteo sencilla de un paso dentro del mismo asistente para habilitar BGP para el ruteo superpuesto.
- Habilita el ruteo escalable y óptimo aprovechando el atributo de reflector de ruta para BGP.
- Permite agregar varios radios simultáneamente con la mínima intervención del usuario.

Topologías cubiertas

En este artículo, se tratan varias topologías para garantizar que los usuarios conocen los diversos escenarios de implementación.

HUB y radio (ISP único)

Diagrama de la red



Configuraciones

- Vaya a **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](#)

· Agregue un concentrador y cree un DVTI en el extremo del concentrador. Como parte de la configuración DVTI, asegúrese de seleccionar la interfaz de origen de túnel correcta según la topología.

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

- Cree un conjunto de direcciones IP de túnel radial y haga clic en Guardar y luego en Agregar. El conjunto de direcciones IP se utiliza para asignar direcciones IP de túnel VTI a los radios.

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

📘 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 📘

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	

Add Hub

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- Haga clic en Next para continuar y agregar los radios. Puede aprovechar cualquiera de las opciones de adición masiva si tiene nombres comunes de interfaz/zona o agrega radios

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 links for 'Deploy', a search icon, a notification icon with '13', a settings icon, a help icon, 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 sidebar on the left contains four steps: '1 Hubs' (selected), '2 Spokes', '3 Authentication Settings', and '4 SD-WAN Settings'. The 'Hubs' step has an 'Edit' link. The 'Spokes' step is active and shows a table with columns: 'Device', 'DVTI', 'VPN-OUT-1_dynamic_vti_1', 'Gateway IP Address', and 'Spoke Tunnel IP Address Pool'. The table contains one row: 'ftd1', 'DVTI', 'VPN-OUT-1_dynamic_vti_1', '203.0.113.1', and 'VPN-POOL-198.51.100.0'. Below the table, there are three buttons: 'View Generated Tunnel Interfaces', 'Add Spokes (Bulk Addition)' (highlighted with a green box), and 'Add Spoke'. A message states 'No spokes are configured. Add a spoke.' At the bottom left, there is a 'Next' button. At the bottom right, there are 'Cancel' and 'Finish' buttons.

FMC Site To Site Overview Analysis Policies Devices Objects Integration Deploy 🔍 13 ⚙️ ? 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 [Edit](#)
 - [View Generated Tunnel Interfaces](#) [Add Spokes \(Bulk Addition\)](#) [Add Spoke](#)
 - No spokes are configured. Add a spoke.
- 3 Authentication Settings [Edit](#)
- 4 SD-WAN Settings [Edit](#)

[Next](#)

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

- Seleccione los dispositivos y especifique un patrón de nomenclatura para la interfaz WAN/externa. Si los dispositivos comparten el mismo nombre de interfaz, basta con utilizar las iniciales. Haga clic en Next y, si la validación se realiza correctamente, haga clic en Add. Para las adiciones masivas, también puede utilizar el nombre de zona del mismo modo.

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

Next

3 Authentication Settings

4 SD-WAN Settings

Spokes (Bulk Addition)

Add Spoke

Edit

Edit

Cancel

Finish

1 Add Devices

2 Validate Devices

Available Devices *

Add

Remove

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

☒ Interface Name Pattern

☐ Security Zone

Select...

+

Cancel

Next

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 los spokes y los detalles de la interfaz de superposición para asegurarse de que se seleccionen las interfaces correctas y, a continuación, haga clic en Next.

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

- Puede conservar los parámetros predeterminados para la configuración de IPsec o especificar cifrados personalizados según sea necesario. Para continuar, haga clic en Next (Siguiente). En este documento, está utilizando los parámetros predeterminados.

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

[Edit](#)

Device	ftd2	VPN Interface	VPN-OUT-1	Local Tunnel (IKE) Identity	Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
	ftd3	VPN Interface	VPN-OUT-1		Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
	ftd4	VPN Interface	VPN-OUT-4		Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3 Authentication Settings

Authentication Type *

Pre-shared Automatic Key

Transform Sets (IPsec Proposals) *

AES-GCM x

[Show Details](#)

IKEv2 Policies *

AES-GCM-NUL-SSH-LATEST x

[Show Details](#)

Pre-shared Key Length *

24 The range is 1 to 127.

Next

4 SD-WAN Settings

[Edit](#)

Cancel

Finish

- Finalmente, puede configurar el ruteo superpuesto dentro del mismo asistente para esta topología especificando los parámetros BGP apropiados, como el número AS, el anuncio de interfaz interna y las etiquetas de comunidad para el filtrado de prefijos. La zona de seguridad puede ayudar en el filtrado del tráfico a través de las políticas de control de acceso, mientras que también puede crear un objeto para las interfaces y utilizarlas en la redistribución de interfaces conectadas si el nombre es diferente del interno o no es simétrico entre los dispositivos de la topología.

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-198.51.100.32

Edit

2 Spokes

Device

ftd2

VPN Interface

VPN-OUT-1

Local Tunnel (IKE) Identity

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

Device

ftd3

VPN Interface

VPN-OUT-1

Local Tunnel (IKE) Identity

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

Device

ftd4

VPN Interface

VPN-OUT-4

Local Tunnel (IKE) Identity

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

- Haga clic en Next, luego en Finish y, por último, en Deploy para completar el proceso.

Verificación

- Puede verificar el estado del túnel navegando hasta 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...

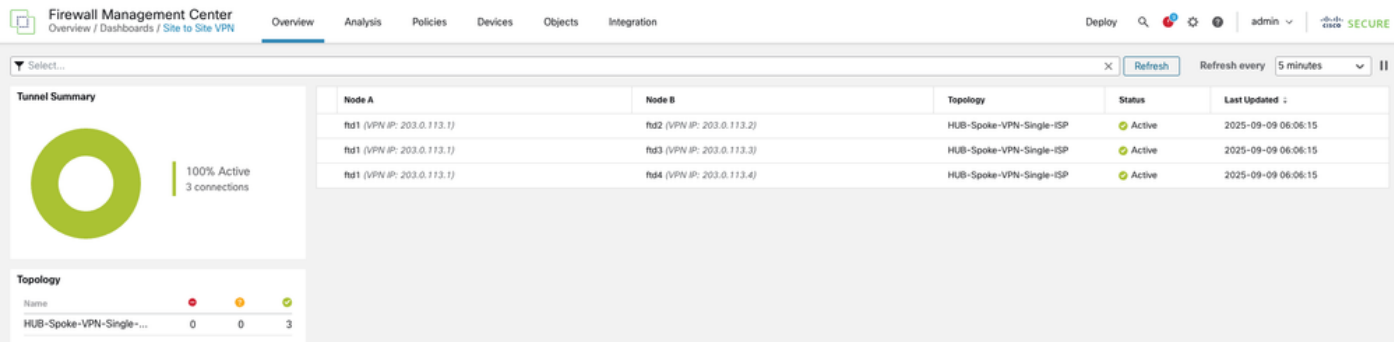
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	Tunnels	✓	

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

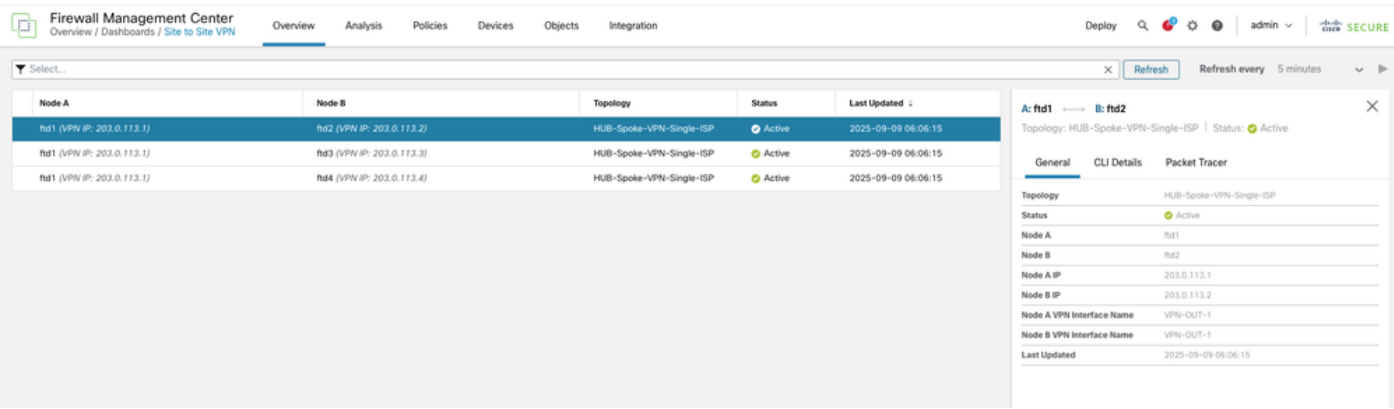
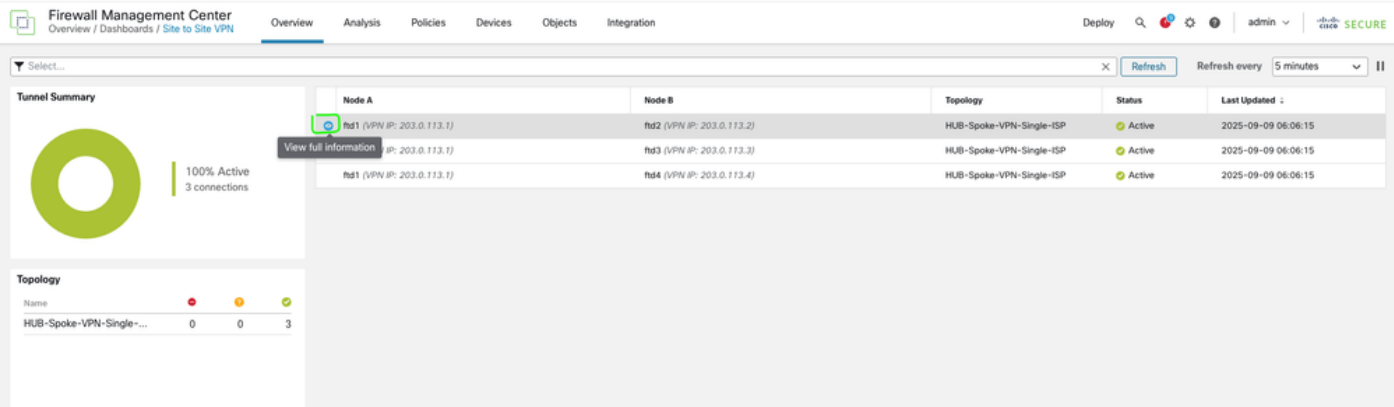
Viewing 1-3 of 3

- Para verificar detalles adicionales, acceda a Descripción general > Paneles > VPN de sitio a

sitio.



- Para obtener más información, seleccione el túnel y haga clic en Ver información completa.



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)
remote ident (addr/mask/prot/port): (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)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
current_peer: 203.0.113.1

```

Viewing 1-3 of 3

- El resultado se muestra directamente desde la CLI de FTD y se puede actualizar para mostrar contadores actualizados e información importante, como los detalles del índice de parámetros de seguridad (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) 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 Protected vrf (ivrf): 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 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.1/500, remote crypto endpt.: 203.0.113.2/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 3EE69843 current inbound spi : D113FBF4 inbound esp sas: spi: 0xD113FBF4 (3507747828) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 9, crypto-map: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map sa timing: remaining key lifetime (sec): 24309	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 ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) Protected vrf (ivrf): 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 #pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154 #pkts decaps: 155, #pkts decrypt: 155, #pkts verify: 155 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 154, #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: 155 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.2/500, remote crypto endpt.: 203.0.113.1/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: D113FBF4 current inbound spi : 3EE69843 inbound esp sas: spi: 0x3EE69843 (1055299651) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (sec): 24308

Close Refresh

- La CLI de FTD también se puede utilizar para verificar la información de ruteo y el estado de peering de BGP.

En el lado del 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

Lado de radio

La misma verificación se puede realizar también en los dispositivos spoke. Aquí hay un ejemplo de uno de los 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

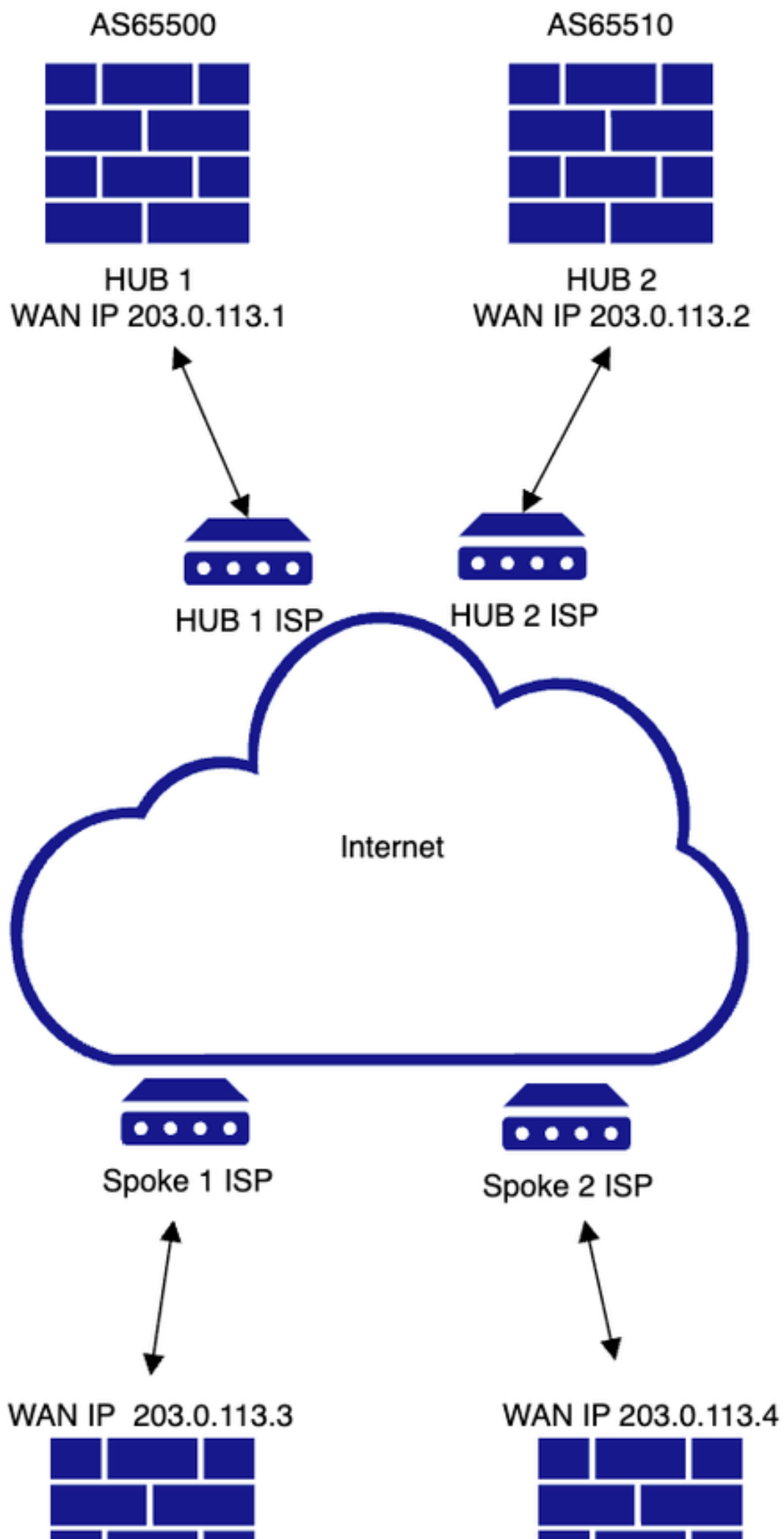
<<<<<< spoke 2 inside network

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

<<<<<< spoke 3 inside network

HUB y radio duales (ISP único para HUB redundante a través de EBGP entre HUB y radios secundarios)

Diagrama de la red



Después de agregar el primer HUB, continúe agregando el segundo HUB siguiendo los mismos pasos utilizados anteriormente para 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

- Proceda a crear la interfaz de túnel virtual dinámico (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

- Se requiere un nuevo conjunto de direcciones IP para los túneles VTI HUB 2 en el lado spoke. Cree y configure el nuevo grupo y guarde los cambios.

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 el peering eBGP entre el segundo HUB y los radios, modifique la configuración de SD-WAN en el paso final. Habilite la opción Secondary HUB is in a different Autonomous System y especifique el número de sistema autónomo (AS) para el HUB secundario. IBGP también se puede utilizar si no existe ninguna limitación de uso de números AS diferentes en su entorno dejando la opción Secondary HUB is in a different Autonomous System sin marcar. Esto también envía la misma etiqueta de comunidad y el mismo número AS para el HUB secundario. El artículo se centra en eBGP para la configuración actual.

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

- Hubs**
 - 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
- 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
- Authentication Settings**
 - 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
 - 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.

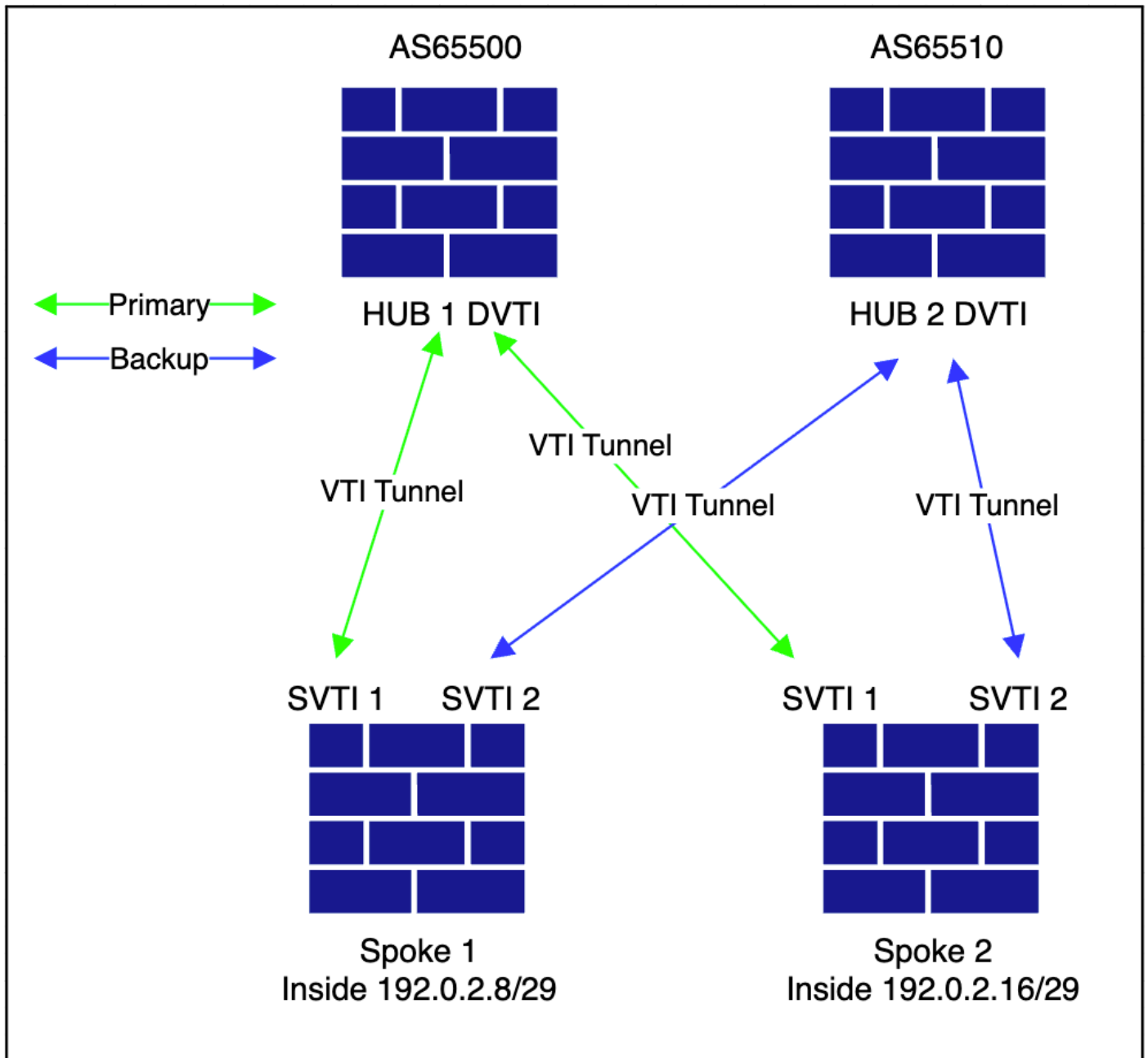
[Next](#) You have unsaved changes

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

Asegúrese de que el número del sistema autónomo (AS) y la etiqueta de comunidad sean únicos en esta configuración.

Verificación

Este diagrama ilustra la topología de superposición.



- En el FMC, navegue hasta 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)

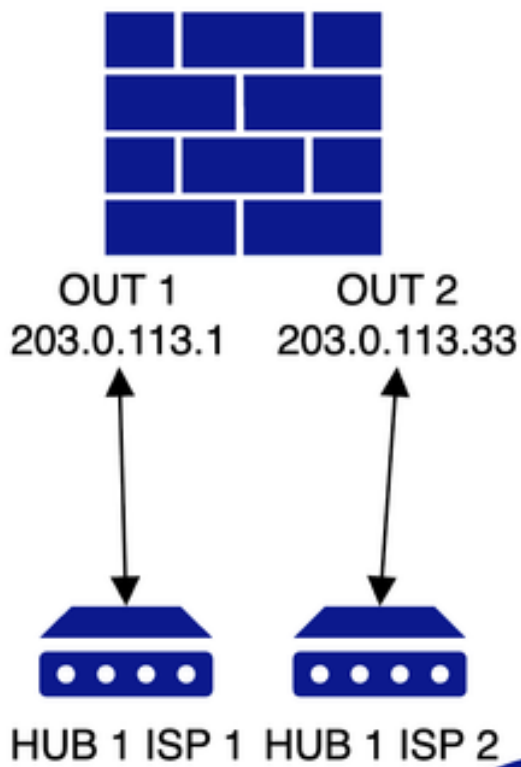
<< Viewing 1-4 of 4 >>

- Los demás pasos no se modifican.

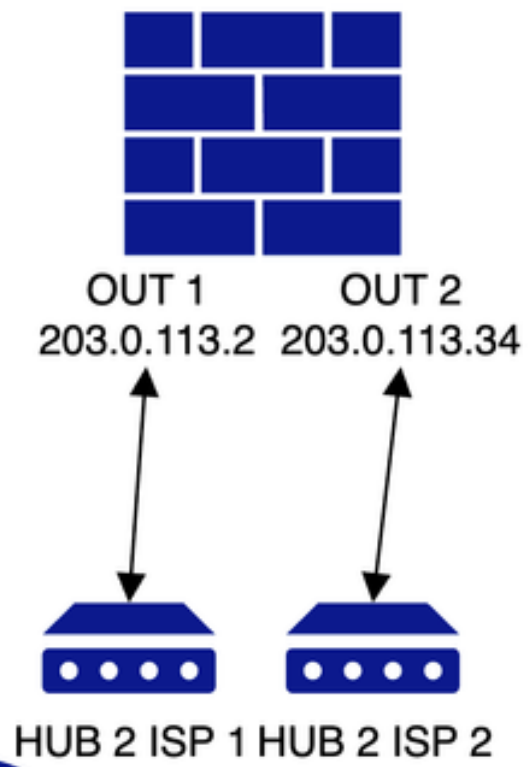
HUB y radio duales (ISP duales para HUB redundante e ISP a través de EBGp entre HUB y radios secundarios)

Diagrama de la red

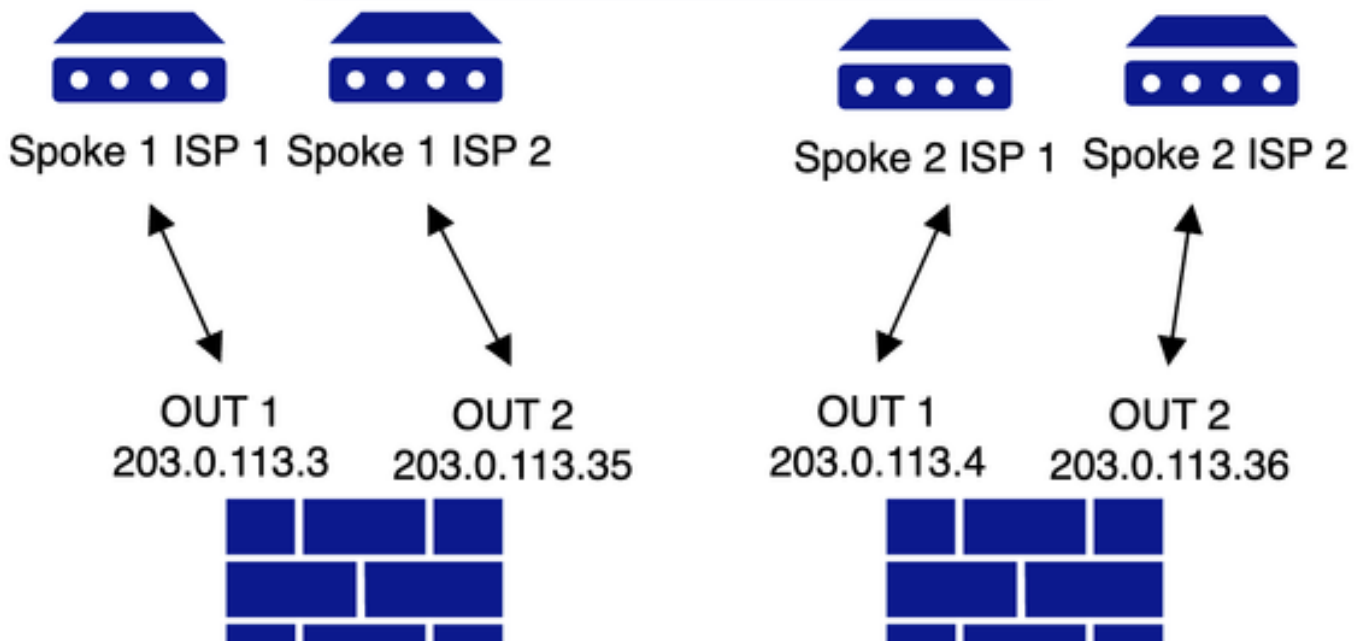
AS65500



AS65510



Internet



La implementación de esta topología se omite utilizando el primer ISP, ya que está cubierto en la topología 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)

- A continuación, agregue la segunda topología creando dos interfaces DVTI adicionales por HUB, cada una de las cuales utiliza la interfaz subyacente para ISP 2 (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

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

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

- Se proporciona un grupo de direcciones IP VPN adicional específicamente para las direcciones de la interfaz de túnel virtual (VTI) 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

Cancel Add

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

Edit

Edit

Edit

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

Cancel Finish

- Para agregar un hub secundario, repita el proceso creando DVTI 2 mediante la interfaz ISP secundaria (VPN-OUT-2) y configure un grupo de IP adicional para direcciones VTI de extremo de radio.

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

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

- Al agregar un spoke, asegúrese de que se especifica la interfaz subyacente/WAN correcta para los túneles VTI. Esta topología utiliza la interfaz ISP secundaria 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

Edit

2 Spokes

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

Next

3 Authentication Settings

Edit

4 SD-WAN Settings

Edit

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

Edit

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

Edit

4 SD-WAN Settings

Edit

Cancel Finish

- Al configurar el ruteo, asegúrese de que las etiquetas de comunidad y los números AS para

ambos HUB en esta topología sean consistentes con los utilizados en la topología ISP1 anterior. La topología utiliza diferentes zonas de seguridad, pero las configuraciones restantes, como los números AS para los HUB principales y secundarios, junto con las etiquetas de comunidad, son las mismas. Esto es obligatorio para que la interfaz de usuario complete la validación de la topología.

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

Edit

2 Spokes

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

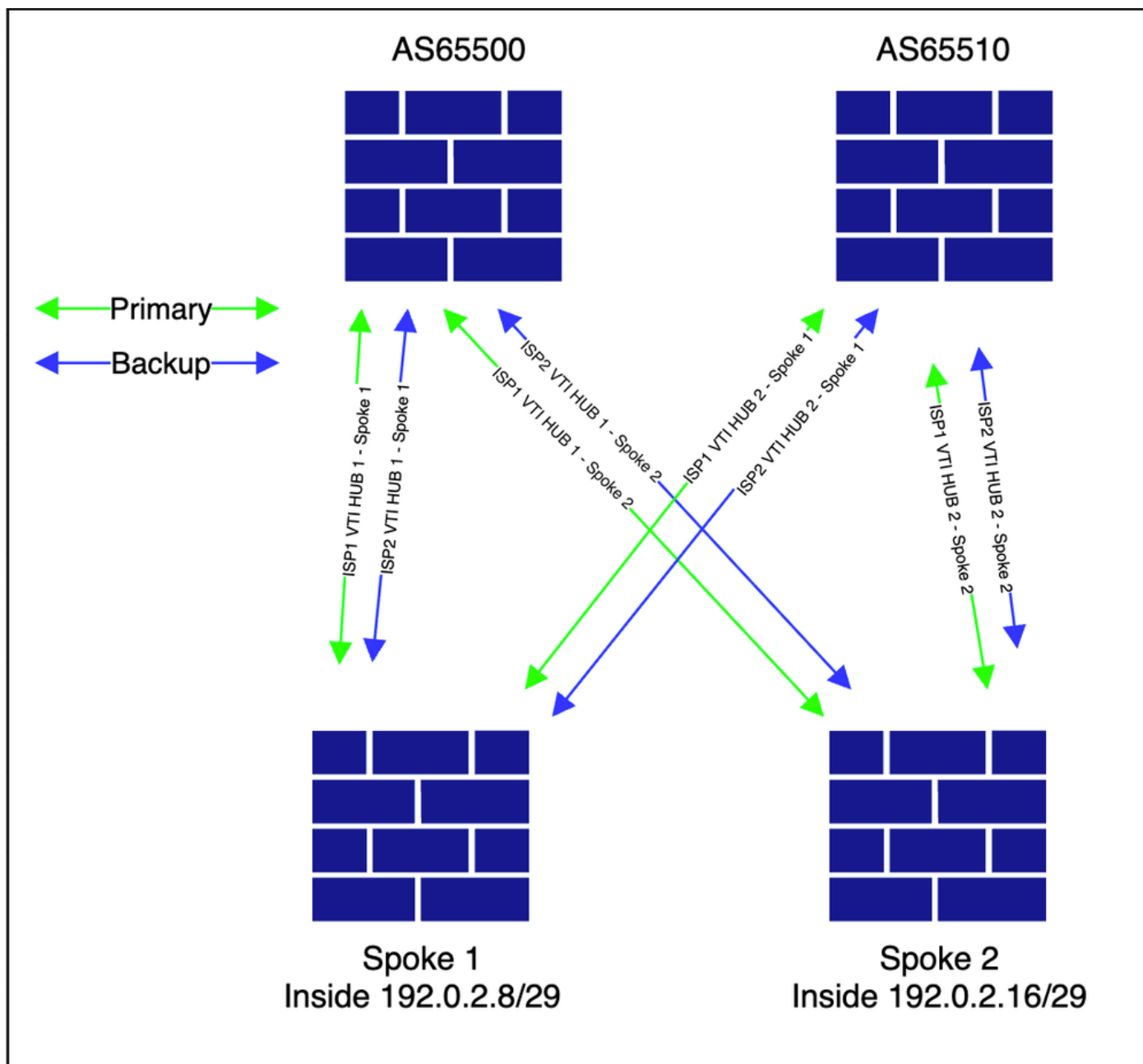
Cancel

Finish

- El resto de la configuración permanece sin cambios. Finalice el asistente y continúe con la implementación.

Verificación

- La topología aparece como se muestra.



- Navegue hasta Devices > VPN > Site to Site para ver la topología.

Firewall Management Center

[Devices / VPN / Site To Site](#)

[Overview](#)
[Analysis](#)
[Policies](#)
[Devices](#)
[Objects](#)
[Integration](#)

[Deploy](#)
[Refresh](#)
[NAT Exemptions](#)
[Add](#)

Last Updated: 03:26 PM

Select...

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

Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	HUB 1 ISP 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)		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)		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)	HUB 2 ISP 1	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static_... (198.51.100.41)

Viewing 1-4 of 4

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

Route Based (VTI)

SD-WAN Topology

4- Tunnels

Hub

Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-2 (203.0.113.33)	HUB 1 ISP 2	FTD ftd3	VPN-OUT-2 (203.0.113.35)	VPN-OUT-2_static_... (198.51.100.70)
FTD ftd1	VPN-OUT-2 (203.0.113.33)		FTD ftd4	VPN-OUT-2 (203.0.113.36)	VPN-OUT-2_static_... (198.51.100.71)
FTD ftd2	VPN-OUT-2 (203.0.113.34)		FTD ftd3	VPN-OUT-2 (203.0.113.35)	VPN-OUT-2_static_... (198.51.100.100)
FTD ftd2	VPN-OUT-2 (203.0.113.34)	HUB 2 ISP 2	FTD ftd4	VPN-OUT-2 (203.0.113.36)	VPN-OUT-2_static_... (198.51.100.101)

Viewing 1-4 of 4

Esta configuración da como resultado cuatro pares BGP por dispositivo, y cada radio tiene las rutas apropiadas para alcanzar otros radios. Por ejemplo, puede recuperar la salida de uno de los radios.

Para radio 1

<#root>

Spoke1#show bgp summary

```
BGP router identifier 203.0.113.35, local AS number 65500
BGP table version is 4, main routing table version 4
2 network entries using 400 bytes of memory
7 path entries using 560 bytes of memory
1 multipath network entries and 2 multipath paths
3/2 BGP path/bestpath attribute entries using 624 bytes of memory
1 BGP rrinfo entries using 40 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
2 BGP community entries using 48 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 1712 total bytes of memory
BGP activity 2/0 prefixes, 7/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	Tb1Ver	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.1	4	65500	229	226	4	0	0	04:07:22	1

<<<<<<<<< HUB 1 ISP 1 VTI

198.51.100.2	4	65510 226	230	4	0	0 04:06:36	2
--------------	---	-----------	-----	---	---	------------	---

<<<<<<<<< HUB 2 ISP 1 VTI

```
198.51.100.3      4      65500 182      183      4      0      0 03:16:45 1
```

<<<<<<<<< HUB 1 ISP 2 VTI

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

La tabla de ruteo aparece como se muestra, lo que confirma que el tráfico está balanceado por carga entre ambos links en el lado 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

Conclusión

El objetivo de este artículo es explicar diversos escenarios de implementación que se pueden implementar fácilmente mediante un único asistente de configuración.

Información Relacionada

- Para obtener ayuda adicional, póngase en contacto con el TAC. Se necesita un contrato de asistencia válido: [Contactos de asistencia globales de Cisco](#).
- También puede visitar la Comunidad VPN de Cisco [aquí](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).