

Configuration de SD-WAN pour VPN site à site sur pare-feu sécurisé

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations sur les fonctionnalités](#)

[Topologies couvertes](#)

[HUB & Spoke \(FAI unique\)](#)

[Double HUB & Spoke \(ISP unique pour concentrateur redondant via EBGp entre concentrateur secondaire et satellites\)](#)

[Double concentrateur et satellite \(double FAI pour concentrateur redondant et FAI via EBGp entre concentrateur secondaire et satellites\)](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Ce document décrit les scénarios de déploiement VPN basés sur la route avec le routage de superposition BGP utilisant la fonctionnalité SD-WAN sur Secure Firewall.

Conditions préalables

Tous les concentrateurs et les rayons exécutent le logiciel FTD 7.6 ou version ultérieure et sont gérés via le même FMC, qui exécute également le logiciel 7.6 ou version ultérieure.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- VPN reposant sur des routes
- Interfaces de tunnel virtuel (VTI)
- IPsec
- BGP

Composants utilisés

Les informations contenues dans ce document sont basées sur :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations sur les fonctionnalités

Management Center simplifie la configuration des tunnels VPN et le routage entre le siège central (concentrateurs) et les sites distants (satellites) à l'aide du nouvel assistant SD-WAN.

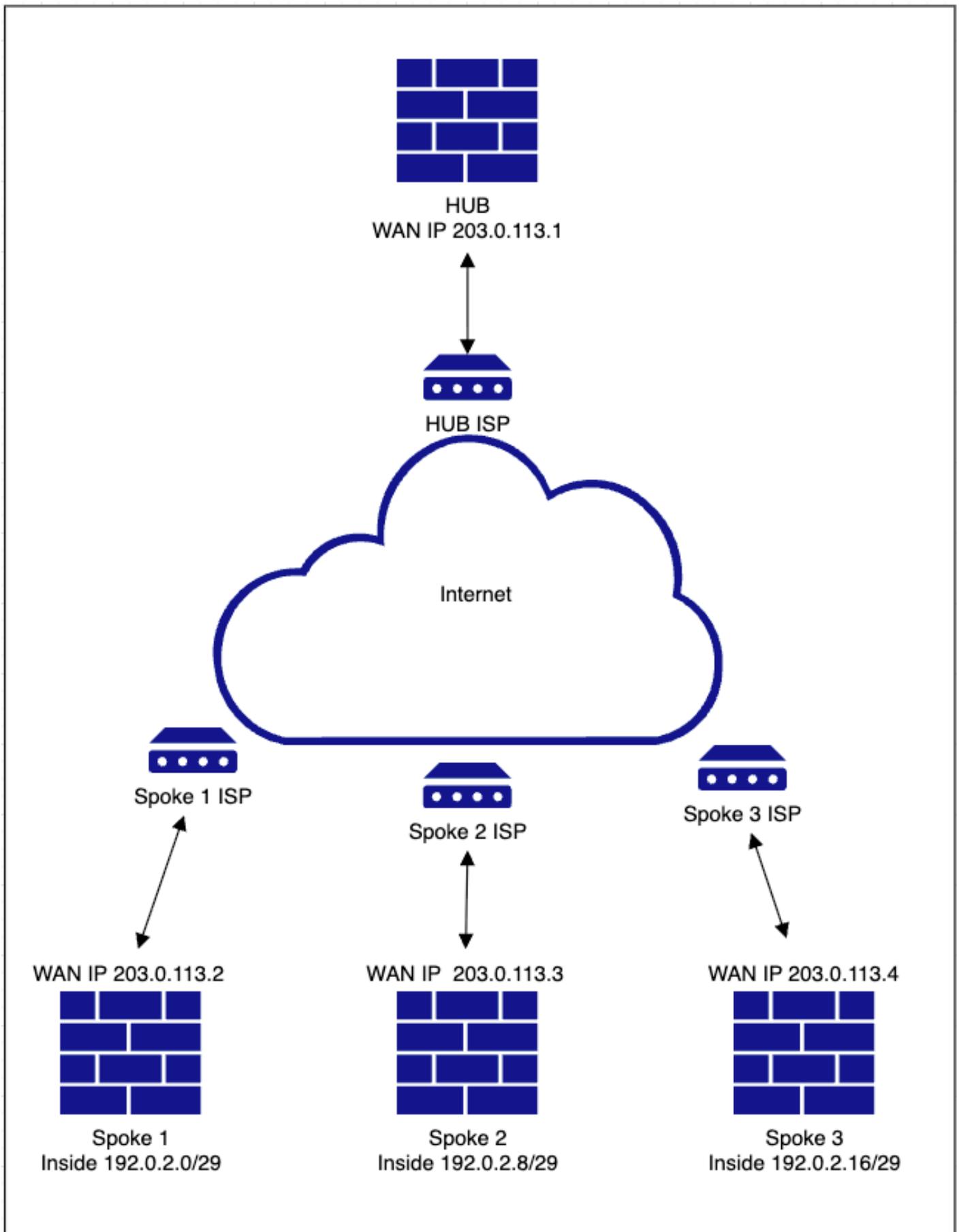
- Automatise la configuration VPN en exploitant DVTI (Dynamic Virtual Tunnel Interface) sur les concentrateurs et SVTI (Static Virtual Tunnel Interface) sur les rayons, avec routage de superposition activé via BGP.
- Attribue automatiquement des adresses IP SVTI pour les rayons et applique la configuration VTI complète, y compris les paramètres de chiffrement.
- Configuration simple et en une étape du routage dans le même assistant pour activer le routage de superposition BGP.
- Permet un routage évolutif et optimal en exploitant l'attribut route-reflector pour BGP.
- Permet l'ajout simultané de plusieurs rayons avec une intervention minimale de l'utilisateur.

Topologies couvertes

Dans cet article, plusieurs topologies sont abordées pour garantir que les utilisateurs connaissent les différents scénarios de déploiement.

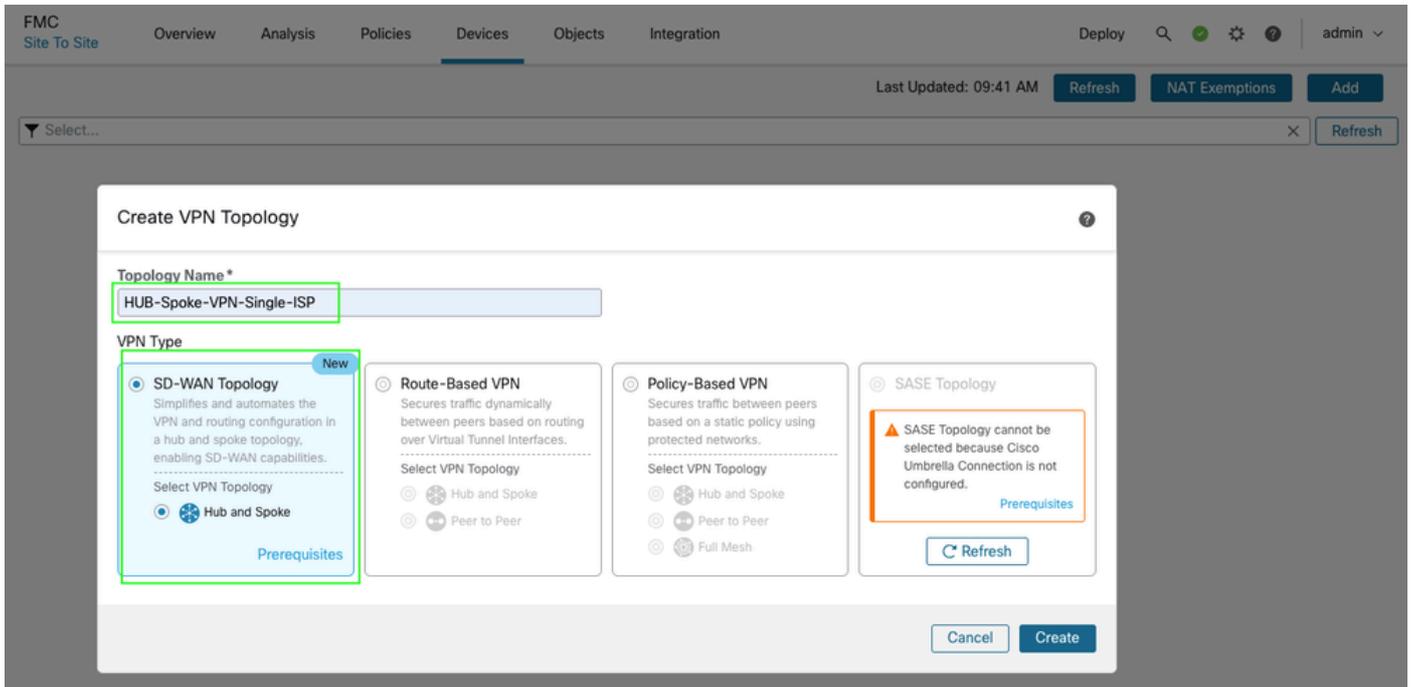
HUB & Spoke (FAI unique)

Diagramme du réseau



Configurations

- Accédez à **Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create**.



- Ajoutez un concentrateur et créez une interface DVTI à l'extrémité du concentrateur. Dans le cadre de la configuration DVTI, assurez-vous de sélectionner l'interface source de tunnel correcte conformément à la topologie.

The screenshot shows the FMC configuration interface for a HUB-Spoke-VPN-Single-ISP topology. The 'Add Hub' dialog is open, showing fields for Device (ftd1), Dynamic Virtual Tunnel Interface (DVTI) (VPN-OUT-1_dynamic_vti_1), Hub Gateway IP Address (203.0.113.1), and Spoke Tunnel IP Address Pool (Select...). The 'Edit Virtual Tunnel Interface' dialog is also open, showing the General tab with Tunnel Type set to Dynamic, Name (VPN-OUT-1_dynamic_vti_1), Enabled checked, Security Zone (VPN-OUT-1), Template ID (1), Tunnel Source (GigabitEthernet0/0 (VPN-OUT-1) with IP 203.0.113.1), IPsec Tunnel Mode (IPv4), and IP Address (Borrow IP (IP unnumbered) with Loopback1 (VPN-Loopback-IB...)).

- Créez un pool d'adresses IP de tunnel Spoke et cliquez sur Save puis sur Add. Le pool d'adresses IP est utilisé pour attribuer des adresses IP de tunnel VTI aux rayons.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy Search 11 Settings Help admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

Add Hub

Device *

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

Hub Gateway IP Address

Spoke Tunnel IP Address Pool *

Cancel **Add**

Add IPv4 Pool

Name*

Description

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

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 Search 11 Settings Help 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	<input type="text" value="Add Hub"/>

Next

2 Spokes [Edit](#)

3 Authentication Settings [Edit](#)

4 SD-WAN Settings [Edit](#)

Cancel **Finish**

- Cliquez sur Next pour continuer et ajouter les rayons. Vous pouvez utiliser l'option d'ajout en bloc si vous avez des noms d'interface/de zone communs ou ajouter des rayons

individuellement.

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	fd1	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.

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Finish

- Sélectionnez les périphériques et spécifiez un modèle d'attribution de noms pour l'interface WAN/externe. Si les périphériques partagent le même nom d'interface, l'utilisation d'initiales est suffisante. Cliquez sur Next, et si la validation est réussie, cliquez sur Add. Pour les ajouts en bloc, vous pouvez également utiliser le nom de la zone de la même manière.

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

Add Bulk Spokes

1 Add Devices 2 Validate Devices

Available Devices *

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

Interface Name Pattern ?

Security Zone ?

Select... ▾ +

3 Authentication Settings Edit

4 SD-WAN Settings Edit

The screenshot displays the 'Add Bulk Spokes' dialog box in the FMC interface. The dialog is divided into two steps: 'Add Devices' (step 1) and 'Validate Devices' (step 2). The 'Add Devices' step is currently active and shows a list of three devices with green checkmarks, indicating successful validation:

- ✓ Device Name: ftd2, Interface Name: VPN-OUT-1
- ✓ Device Name: ftd3, Interface Name: VPN-OUT-1
- ✓ Device Name: ftd4, Interface Name: VPN-OUT-4

The background shows the 'Spokes' configuration page for a 'HUB-Spoke-VPN-Single-ISP' topology. A table lists existing spokes:

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

Buttons for 'Add Bulk Spokes (Bulk Addition)', 'Add Spoke', 'Next', 'Cancel', 'Back', 'Add', 'Cancel', and 'Finish' are visible.

- Vérifiez les détails de l'interface de rayons et de superposition pour vous assurer que les interfaces correctes sont sélectionnées, puis cliquez sur 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](#)

- Vous pouvez conserver les paramètres par défaut de la configuration IPsec ou spécifier des chiffrements personnalisés, le cas échéant. Cliquez sur Next pour continuer. Dans ce document, vous utilisez les paramètres par défaut.

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

3 Authentication Settings Edit

Authentication Type*
Pre-shared Automatic Key ▼

Pre-shared Key Length*
 The range is 1 to 127.

Transform Sets (IPsec Proposals)*
AES-GCM x ▼ Show Details

IKEv2 Policies*
AES-GCM-NULL-SHA-LATEST x ▼ Show Details

4 SD-WAN Settings Edit

- Enfin, vous pouvez configurer le routage de superposition dans le même assistant pour cette topologie en spécifiant les paramètres BGP appropriés, tels que le numéro de système autonome, l'annonce d'interface interne et les balises de communauté pour le filtrage de préfixe. La zone de sécurité peut aider au filtrage du trafic via des politiques de contrôle d'accès, tandis que vous pouvez également créer un objet pour les interfaces et les utiliser dans la redistribution des interfaces connectées si le nom est différent de celui qui est à l'intérieur ou n'est pas symétrique entre les périphériques dans la topologie.

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 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 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 (S/VTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)
 - Spoke Tunnel Interface Security Zone**
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

- Cliquez sur Next, puis sur Finish, et enfin sur Deploy pour terminer le processus.

Vérification

- Vous pouvez vérifier l'état du tunnel en naviguant vers Devices > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select...

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEx1	IKEx2
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_dynam... (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_dynam... (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_dynam... (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

- Vous pouvez vérifier des détails supplémentaires en naviguant vers Overview > Dashboards

> Site to Site VPN.

The screenshot shows the 'Site to Site VPN' overview dashboard in the Firewall Management Center. On the left, there is a 'Tunnel Summary' section with a green donut chart indicating '100% Active' and '3 connections'. Below it is a 'Topology' section with a legend and a table showing 0 red, 0 orange, and 3 green status indicators for 'HUB-Spoke-VPN-Single-...'. The main area features a table with columns: Node A, Node B, Topology, Status, and Last Updated. The table lists three active tunnels.

Node A	Node B	Topology	Status	Last Updated
fd1 (VPN IP: 203.0.113.1)	fd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15

- Pour plus d'informations, sélectionnez le tunnel et cliquez sur View Full Information.

This screenshot is similar to the first one, but the first row of the table is highlighted in grey. A small icon with a magnifying glass is visible over the first row, and a tooltip 'View full information' is shown above it.

This screenshot shows the 'View Full Information' panel for the selected tunnel. The table from the previous screenshot is visible in the background. The details panel on the right shows the tunnel configuration for 'A: fd1' and 'B: fd2'. It includes fields for Topology, Status, Node A, Node B, Node A IP, Node B IP, Node A VPN Interface Name, Node B VPN Interface Name, and Last Updated.

Node A	Node B	Topology	Status	Last Updated
fd1 (VPN IP: 203.0.113.1)	fd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15

A: fd1 ↔ B: fd2	
Topology:	HUB-Spoke-VPN-Single-ISP
Status:	Active
Node A:	fd1
Node B:	fd2
Node A IP:	203.0.113.1
Node B IP:	203.0.113.2
Node A VPN Interface Name:	VPN-OUT-1
Node B VPN Interface Name:	VPN-OUT-1
Last Updated:	2025-09-09 06:06:15

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 (203.0.113.1/30)	Node B (203.0.113.2/30)
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

- Le résultat est affiché directement à partir de l'interface de ligne de commande FTD et peut être actualisé pour afficher des compteurs mis à jour et des informations importantes, telles que les détails de l'index des paramètres de sécurité (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)
<pre> 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 f #pre-frag successes: 0, #pre-frag failures: 0, #fragments creat #PMTUS sent: 0, #PMTUS rcvd: 0, #decapsulated frgs needing read #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_vt sa timing: remaining key lifetime (sec): 24309 </pre>	<pre> 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 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 f #pre-frag successes: 0, #pre-frag failures: 0, #fragments creat #PMTUS sent: 0, #PMTUS rcvd: 0, #decapsulated frgs needing read #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- sa timing: remaining key lifetime (sec): 24308 </pre>

Close Refresh

- L'interface de ligne de commande FTD peut également être utilisée pour vérifier les informations de routage et l'état d'appairage BGP.

Côté concentrateur

<#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

Côté Rayon

La même vérification peut également être effectuée sur les périphériques en étoile. Voici un exemple de l'un des rayons.

<#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

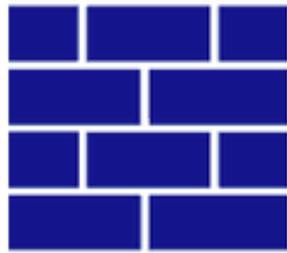
B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

<<<<<< spoke 3 inside network

Double HUB & Spoke (ISP unique pour concentrateur redondant via EBGP entre concentrateur secondaire et satellites)

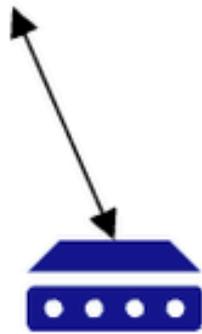
Diagramme du réseau

AS65500



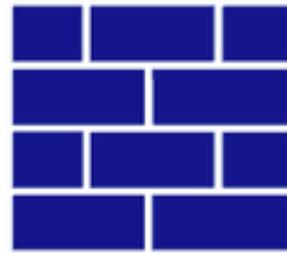
HUB 1

WAN IP 203.0.113.1



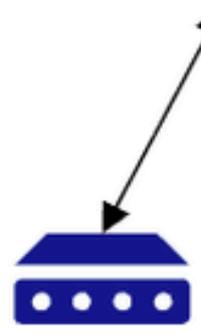
HUB 1 ISP

AS65510

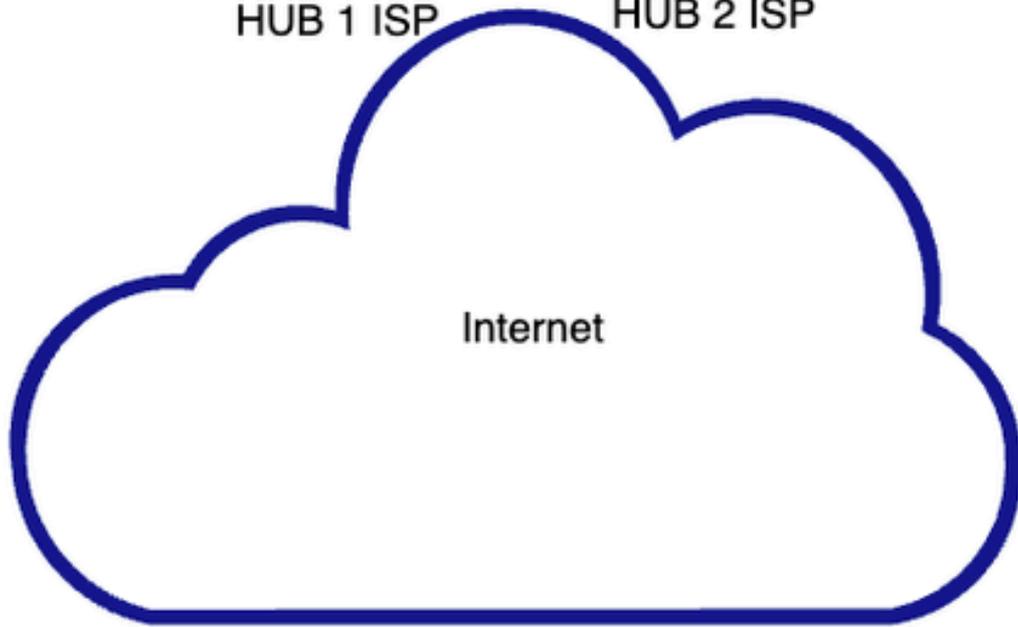


HUB 2

WAN IP 203.0.113.2



HUB 2 ISP



Internet



Spoke 1 ISP



Spoke 2 ISP

WAN IP 203.0.113.3



WAN IP 203.0.113.4



Après avoir ajouté le premier concentrateur, ajoutez le second en suivant les mêmes étapes que pour le concentrateur 1.

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: 198.51.100.10-198.51.1

- Créez l'interface DVTI (Dynamic Virtual Tunnel Interface).

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
 Static Dynamic

Name:*
VPN-OUT-1_dynamic_vti_1

Enabled

Description:

Security Zone:

Priority:
0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named TunnelID* 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) 203.0.113.2

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) Select Interface

Add Loopback Interface

General IPv4 IPv6

Name:
VPN-OUT-LOOPBACK

Enabled

Loopback ID:*
1 (1-1024)

Description

- Un nouveau pool d'adresses IP est requis pour les tunnels VTI du HUB 2 côté satellite. Créez et configurez le nouveau pool, puis enregistrez les modifications.

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

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

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 ✓ **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 <input checked="" type="checkbox"/> Primar	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 <input type="checkbox"/>	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 VPN Interface VPN-OUT-1 Local Tunnel (IKE) Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
ftd4 VPN-OUT-4 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

- Pour configurer l'appairage eBGP entre le deuxième concentrateur et les rayons, modifiez les paramètres SD-WAN à l'étape finale. Activez l'option Secondary HUB is in a different Autonomous System et spécifiez le numéro de système autonome (AS) pour le HUB secondaire. IBGP peut également être utilisé s'il n'y a aucune limitation à l'utilisation d'un numéro de système autonome différent sur votre environnement en laissant l'option Secondary HUB is in a different Autonomous System décochée. Cela permet d'envoyer la même balise de communauté et le même numéro de système autonome pour le concentrateur secondaire également. L'article se concentre sur eBGP pour la configuration

actuelle.

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

- Hubs** Edit
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** Edit
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** Edit
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** (highlighted in green)
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.

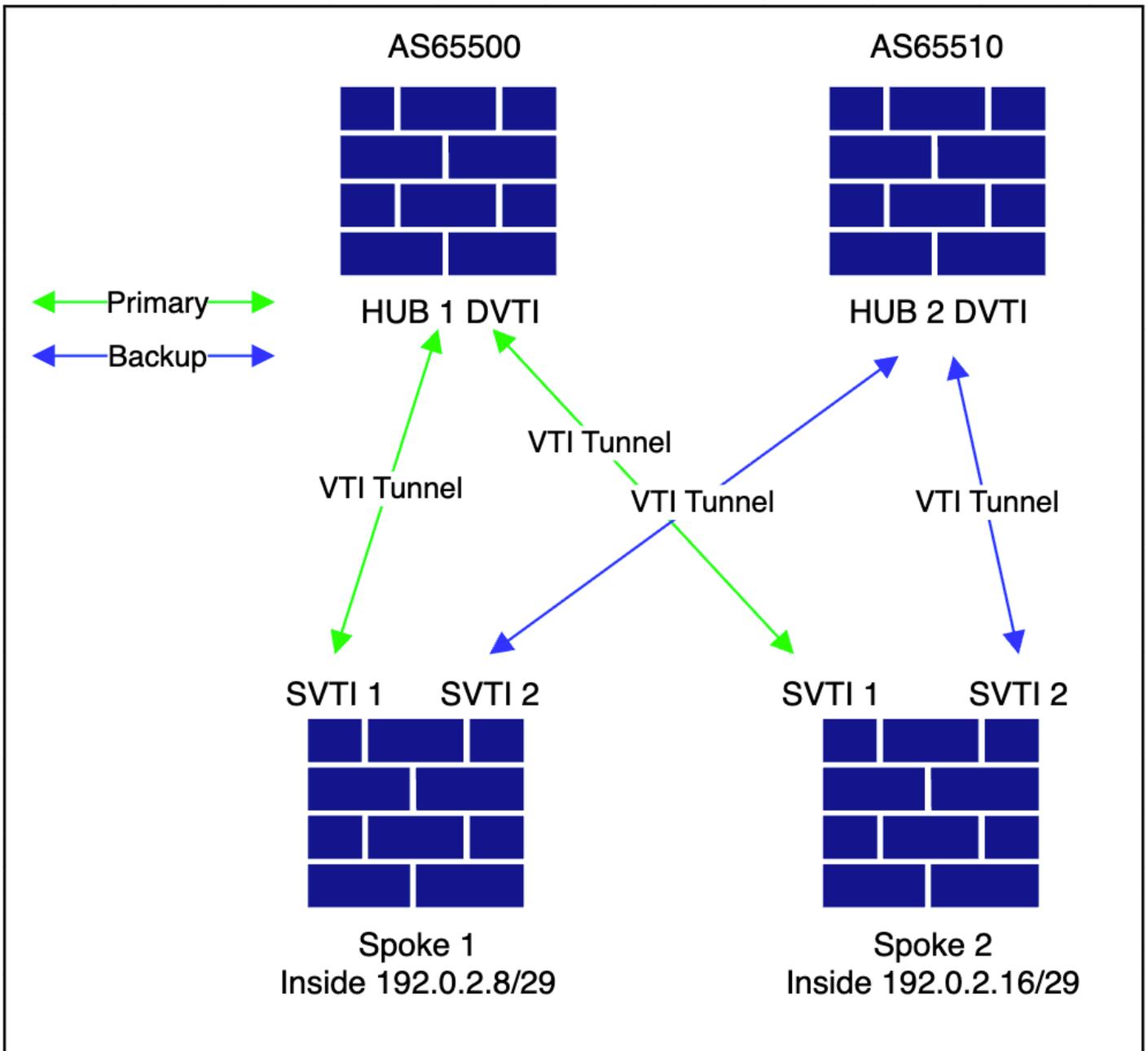
Next You have unsaved changes

Cancel **Finish**

Assurez-vous que le numéro de système autonome (AS) et l'étiquette de communauté sont uniques dans cette configuration.

Vérification

Ce schéma illustre la topologie de superposition.



- Dans le FMC, accédez à Devices > VPN > Site to Site.

Firewall Management Center
 Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

Last Updated: 02:20 PM Refresh NAT Exemptions Add

Select... Refresh

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

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

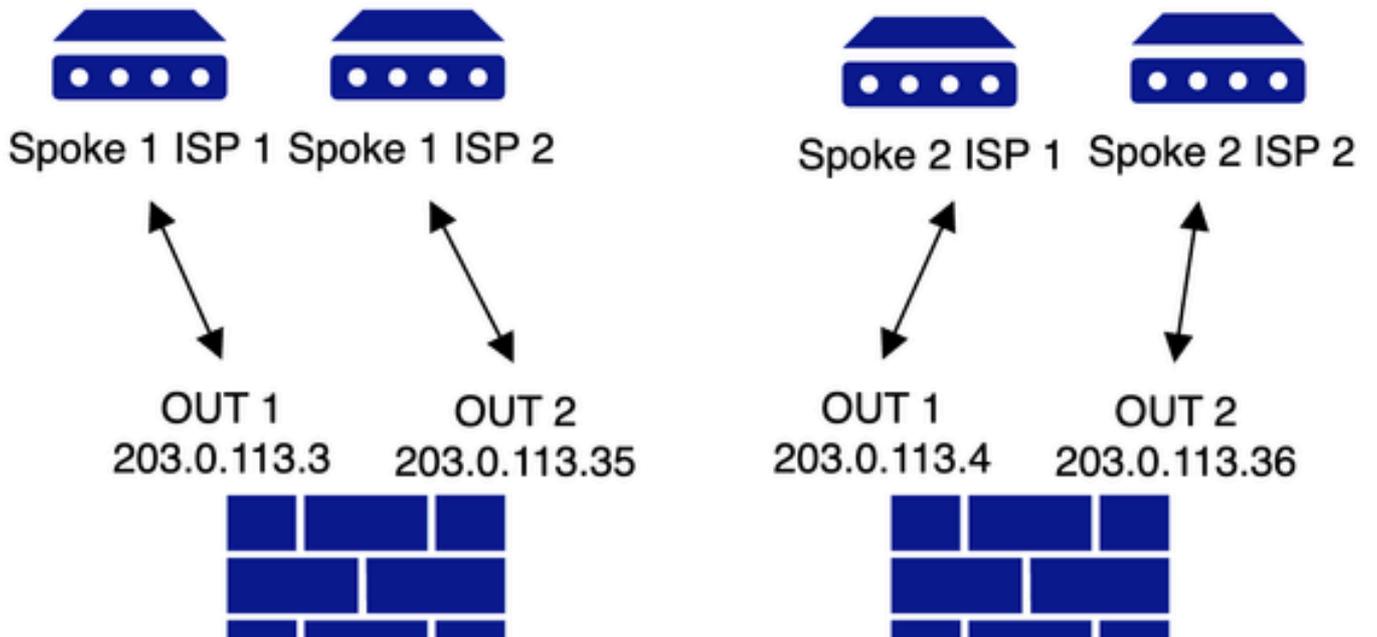
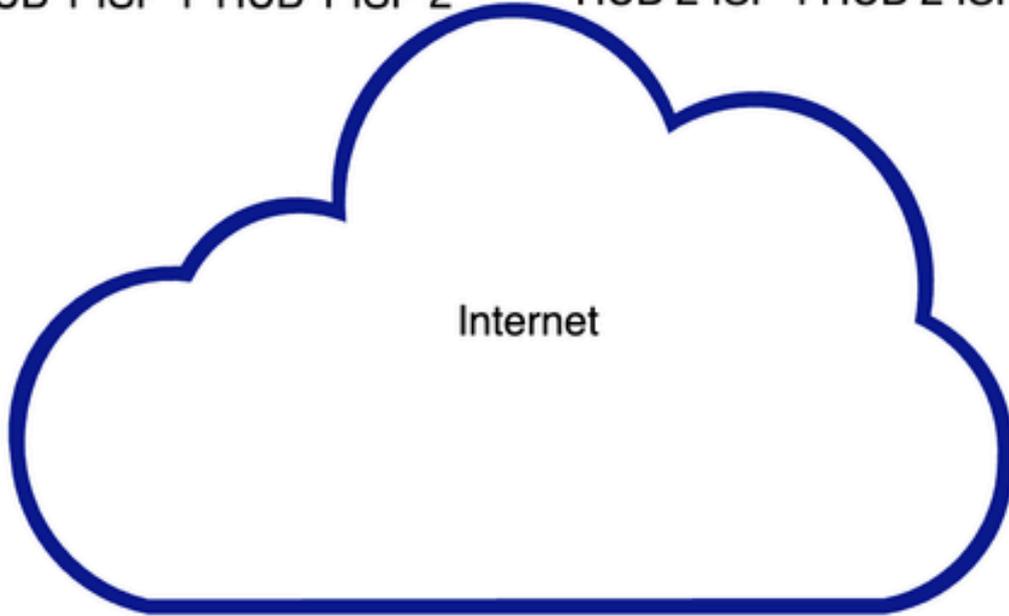
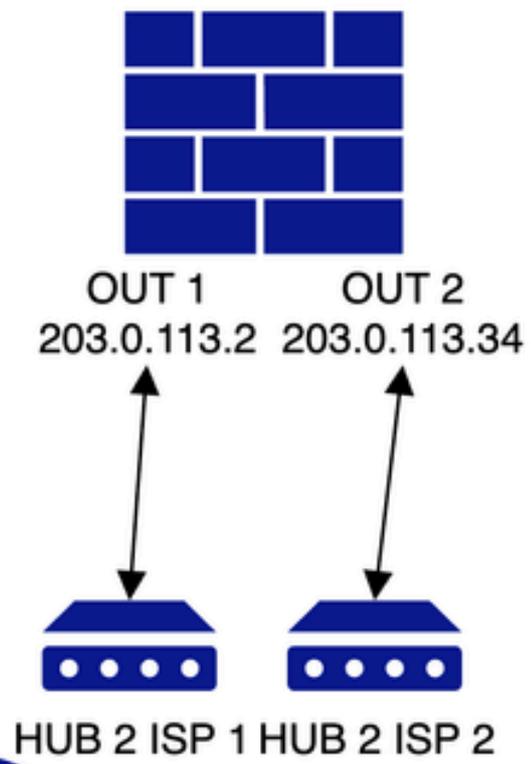
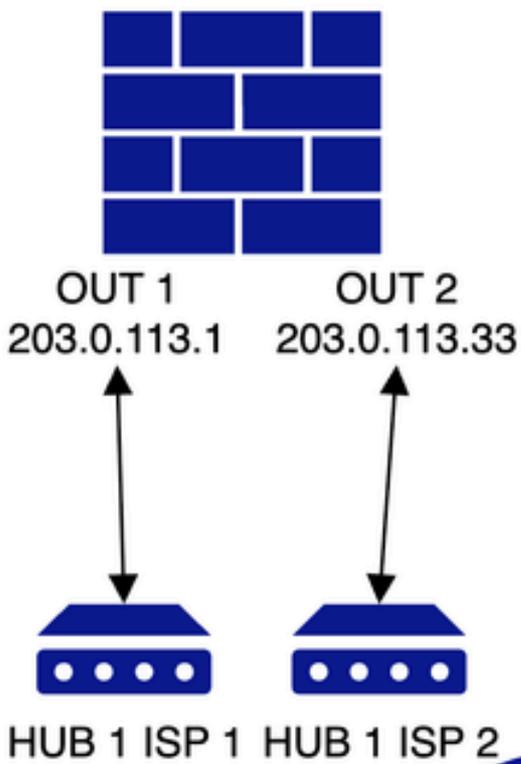
- Toutes les autres étapes restent inchangées.

Double concentrateur et satellite (double FAI pour concentrateur redondant et FAI via EBGP entre concentrateur secondaire et satellites)

Diagramme du réseau

AS65500

AS65510



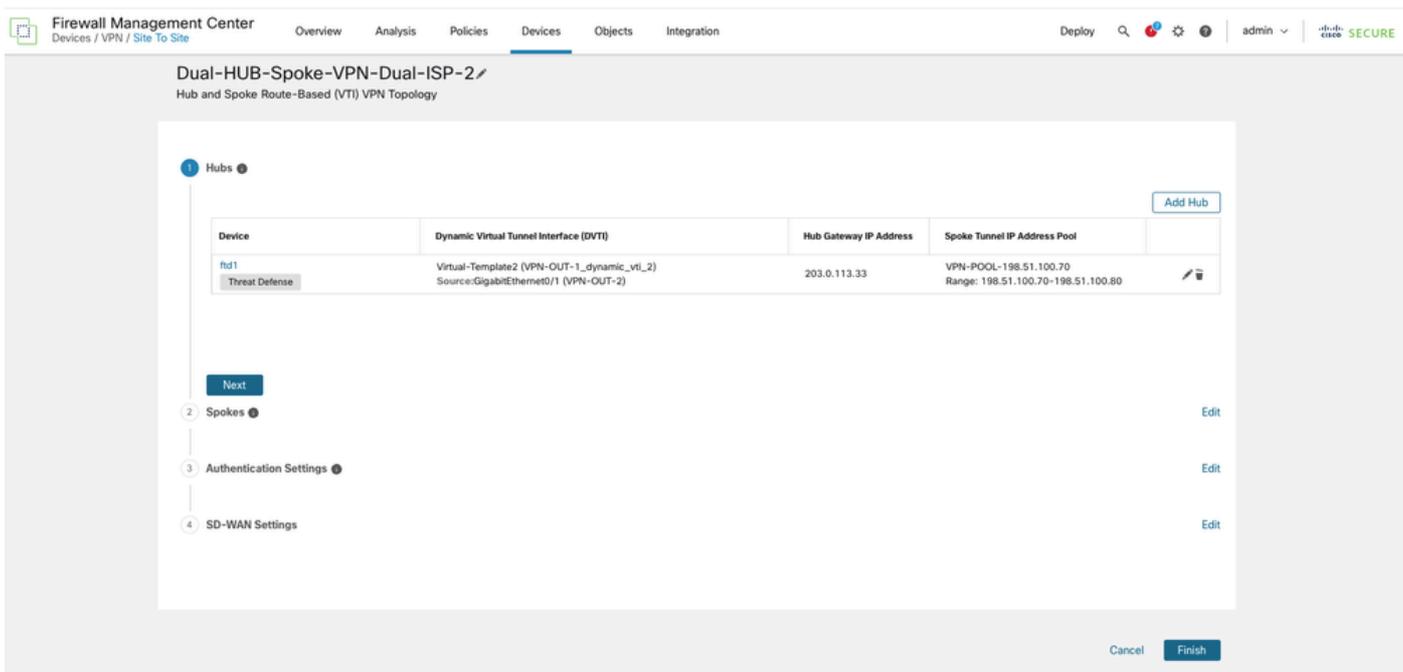
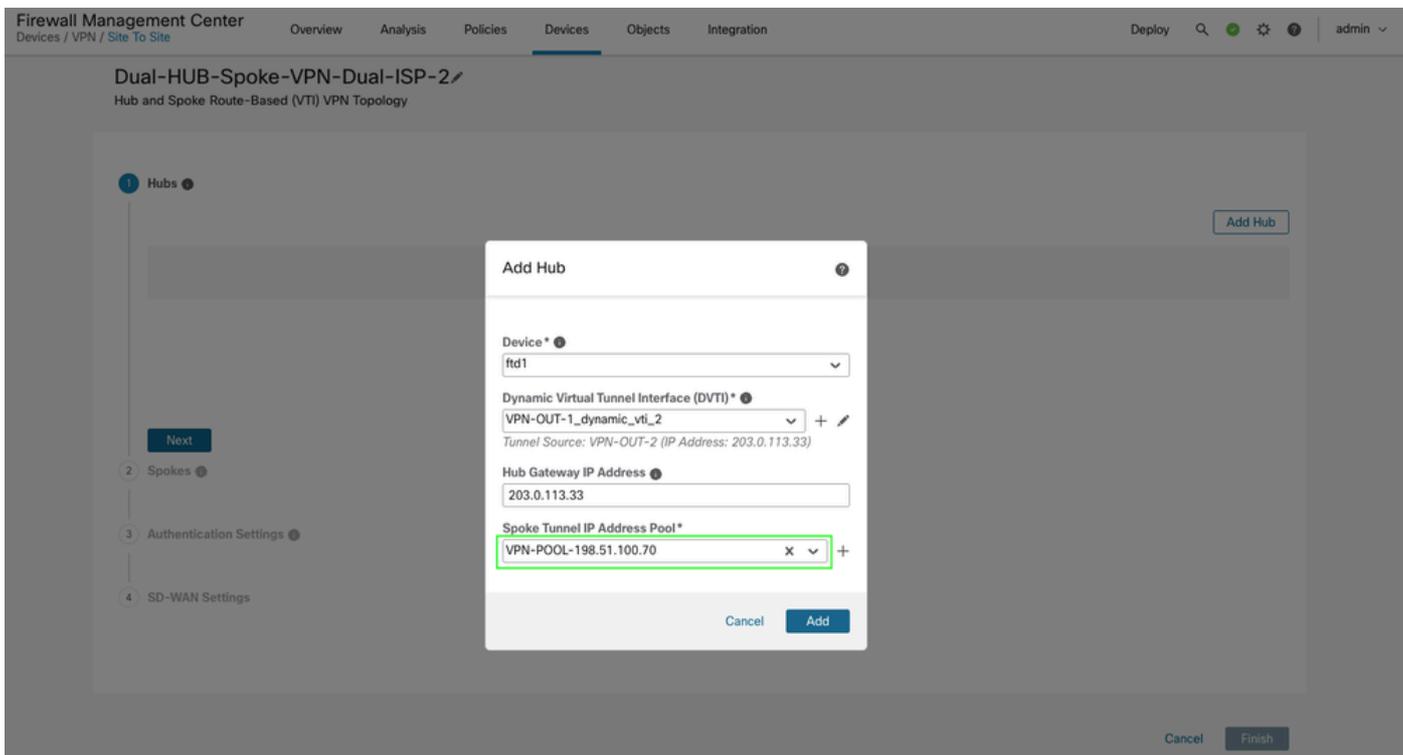
Le déploiement de cette topologie est ignoré à l'aide du premier FAI, car il est traité dans la topologie précédente.

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)	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)

- Ensuite, ajoutez la deuxième topologie en créant deux interfaces DVTI supplémentaires par concentrateur, chacune utilisant l'interface sous-jacente pour ISP 2 (VPN-OUT-2).

The screenshot shows the Firewall Management Center interface for configuring a Virtual Tunnel Interface (VTI). The 'Add Virtual Tunnel Interface' dialog is open, showing the 'General' tab. The 'Tunnel Type' is set to 'Dynamic'. The 'Name' is 'VPN-OUT-1_dynamic_vti_2'. The 'Enabled' checkbox is checked. The 'Security Zone' is set to 'GigabitEthernet0/1 (VPN-OUT-2)'. The 'Priority' is 0. The 'Virtual Tunnel Interface Details' section shows 'Template ID' as 2 and 'Tunnel Source' as 'GigabitEthernet0/1 (VPN-OUT-2)' with IP address '203.0.113.33'. The 'IPsec Tunnel Details' section shows 'IPsec Tunnel Mode' as 'IPv4' and 'IP Address' as 'Borrow IP (IP unnumbered)' with 'Loopback2 (VPN-2-LOOPBACK...)' selected.

- Un pool d'adresses IP VPN supplémentaire est configuré spécifiquement pour les adresses VTI (Virtual Tunnel Interface) en étoile.



- Pour ajouter un concentrateur secondaire, répétez le processus en créant DVTI 2 à l'aide de l'interface ISP secondaire (VPN-OUT-2) et configurez un pool d'adresses IP supplémentaires pour les adresses VTI en étoile.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy

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

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

Next

Finish

- Lors de l'ajout d'un rayon, assurez-vous que l'interface sous-jacente / WAN correcte est spécifiée pour les tunnels VTI. Cette topologie utilise l'interface VPN-OUT-2 de l'ISP

secondaire.

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

2 Spokes

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

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

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

Cancel Finish

Viewing 1-2 of 2

- Lors de la configuration du routage, assurez-vous que les balises de communauté et les numéros de système autonome des deux concentrateurs de cette topologie sont cohérents avec ceux utilisés dans la topologie précédente du routeur ISP1. La topologie utilise différentes zones de sécurité, mais les configurations restantes, telles que les numéros de système autonome pour les concentrateurs principal et secondaire, ainsi que les balises de communauté sont identiques. Cette opération est obligatoire pour que l'interface utilisateur puisse valider la topologie.

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

- Hubs**

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

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

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.

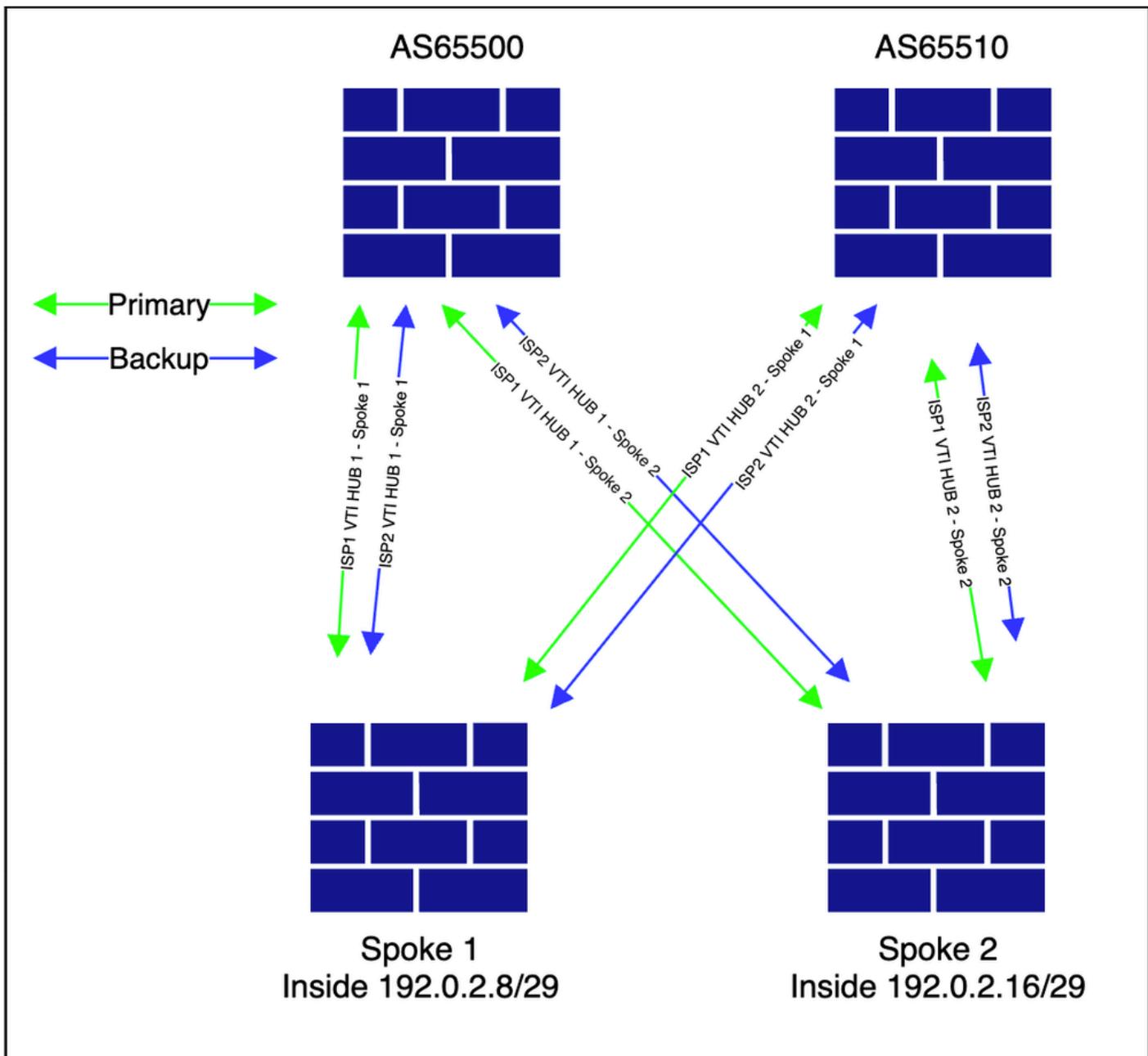
Next You have unsaved changes

Cancel **Finish**

- Tous les autres paramètres restent inchangés. Terminez l'Assistant et poursuivez le déploiement.

Vérification

- La topologie apparaît comme illustré.



- Accédez à Devices > VPN > Site to Site pour afficher la topologie.


```
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 received 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 table de routage apparaît comme indiqué, ce qui confirme que la charge du trafic est équilibrée entre les deux liaisons côté satellite.

<#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
```

Conclusion

L'objectif de cet article est d'expliquer divers scénarios de déploiement qui peuvent être facilement mis en oeuvre à l'aide d'un seul assistant de configuration.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis :[Contacts d'assistance internationale Cisco](#).
- Vous pouvez également visiter la communauté VPN Cisco [ici](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.