

為通過安全防火牆的站點到站點VPN配置SD-WAN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[功能資訊](#)

[涵蓋的拓撲](#)

[中心輻射型 \(單ISP\)](#)

[雙中心輻射型 \(通過輔助中心輻射和輻射之間的EBGP為冗餘中心提供單一ISP\)](#)

[雙中心輻射型 \(雙ISP用於冗餘中心，ISP通過輔助中心輻射和輻射之間的EBGP\)](#)

[結論](#)

[相關資訊](#)

簡介

本檔案介紹使用安全防火牆上的SD-WAN功能的BGP重疊路由的基於路由的VPN部署方案。

必要條件

所有集線器和輻條均運行FTD 7.6或更高版本軟體，並通過同樣運行7.6或更高版本軟體的同一FMC進行管理。

需求

思科建議您瞭解以下主題：

- IKEv2
- 路由型VPN
- 虛擬通道介面(VTI)
- IPsec
- BGP

採用元件

本檔案中的資訊是根據：

- 思科安全防火牆威脅防禦7.7.10
- 思科安全防火牆管理中心7.7.10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

功能資訊

通過使用新的SD-WAN嚮導，管理中心簡化了VPN隧道的配置以及中央總部（集線器）和遠端分支站點（分支）之間的路由。

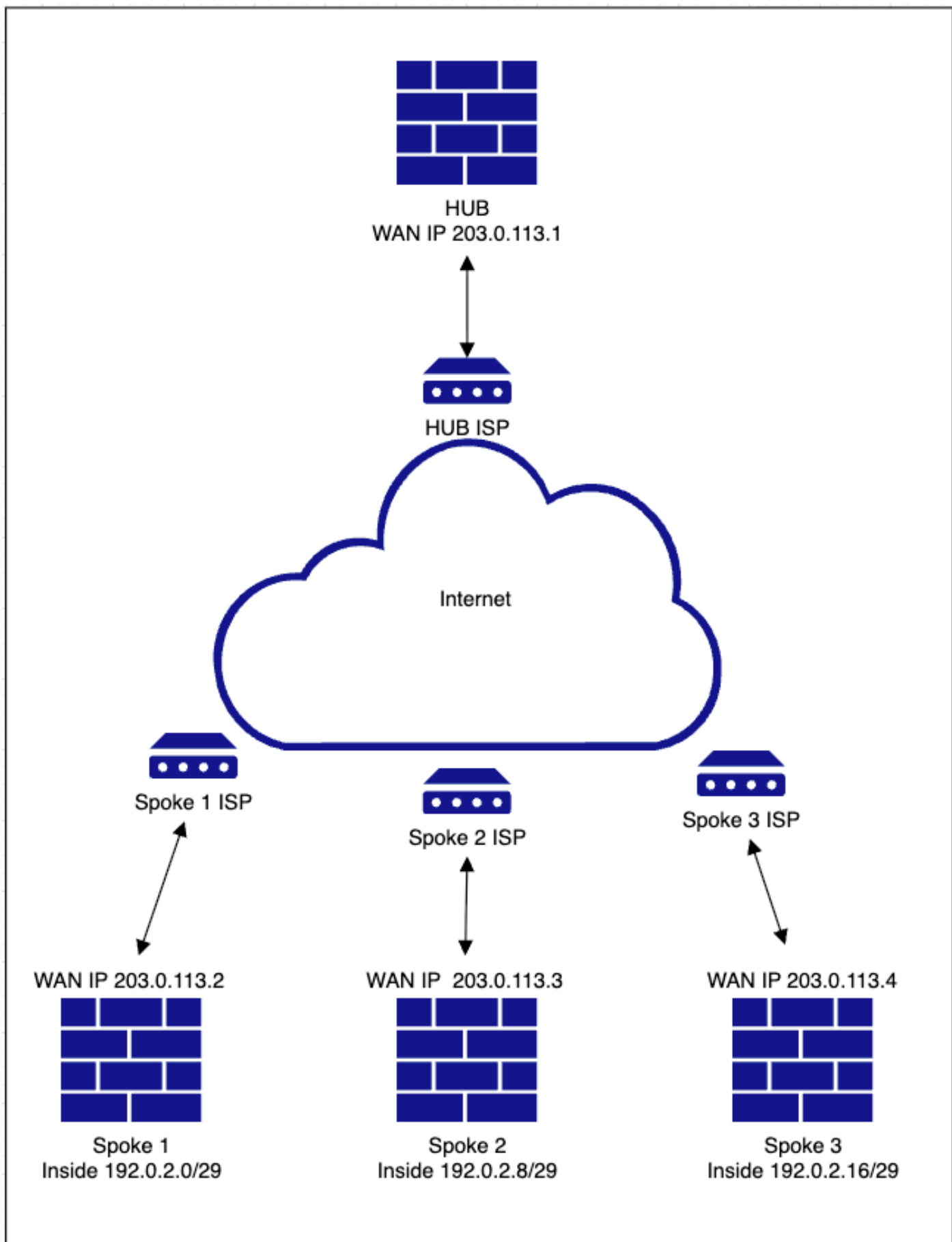
- 在集線器上利用DVTI（動態虛擬通道介面）在分支上利用SVTI（靜態虛擬通道介面），通過BGP啟用重疊路由，從而自動執行VPN配置。
- 自動為分支分配SVTI IP地址並推送完整的VTI配置，包括加密引數。
- 在同一嚮導內提供簡單的一步路由配置，以便為重疊路由啟用BGP。
- 利用BGP的路由反射器屬性，實現可擴展的最佳路由。
- 允許同時新增多個輪輻，只需最少的使用者干預。

涵蓋的拓撲

在本文中，涵蓋多個拓撲，以確保使用者瞭解各種部署方案。

中心輻射型（單ISP）

網路圖表



組態

- 導航到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](#)

·新增中心並在中心端建立DVTI。作為DVTI配置的一部分，請確保根據拓撲選擇正確的隧道源介面。

。

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

- 建立分支通道IP地址池，然後點選Save，然後Add。ip地址池用於將VTI隧道IP地址分配給分支。

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

3 Authentication Settings 📘

4 SD-WAN Settings

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

- 按一下下一步繼續並新增輻條。如果您有通用介面/區域名稱，則可以利用批次新增選項，也可以單獨新增分支。

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

2 Spokes ⓘ

View Generated Tunnel Interfaces

Add Spokes (Bulk Addition)

Add Spoke

No spokes are configured. Add a spoke.

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Cancel Finish

- 選擇裝置並指定WAN/外部介面的命名模式。如果裝置共用相同的介面名稱，使用首字母就足夠了。按一下Next，如果驗證成功，則按一下Add。對於批次新增，您也可以以相同的方式使用區域名稱。

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

Edit

Cancel

Finish

1 Add Devices

2 Validate Devices

Available Devices *

🔍 Search

Add

Remove

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

Interface Name Pattern

out

Security Zone

Select... +

Cancel

Next

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 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

Cancel Back Add

Next
3 Authentication Settings ⓘ
4 SD-WAN Settings

Spokes (Bulk Addition) Add Spoke Edit
Cancel Finish

- 驗證輻條和重疊介面詳細資訊以確保選擇了正確的介面，然後按一下下一步。

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](#)

- 您可以保留IPsec配置的預設引數，也可以根據需要指定自定義密碼。按一下下一步繼續。在本檔案中，您使用的是預設引數。

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

ftd2	VPN Interface	VPN-OUT-1	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- SHA-LATEST x ▾
[Show Details](#)Pre-shared Key Length *
24 The range is 1 to 127.[Next](#)

4 SD-WAN Settings

Edit

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

- 最後，您可以通過指定適當的BGP引數（如用於字首過濾的AS編號、內部介面通告和社群標籤），在此拓撲的同一嚮導內配置重疊路由。安全區域可以通過訪問控制策略幫助流量過濾，同時還可以為介面建立一個對象，並在所連線的介面重分配中使用它們（如果名稱不同於拓撲中的內部名稱或跨裝置不對稱）。

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

- Hubs** Edit

Device	DVTI	VPN-OUT-1_dynamic_vti_1	Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1			203.0.113.1	VPN-POOL-198.51.100.32
- Spokes** Edit

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

☒ **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.

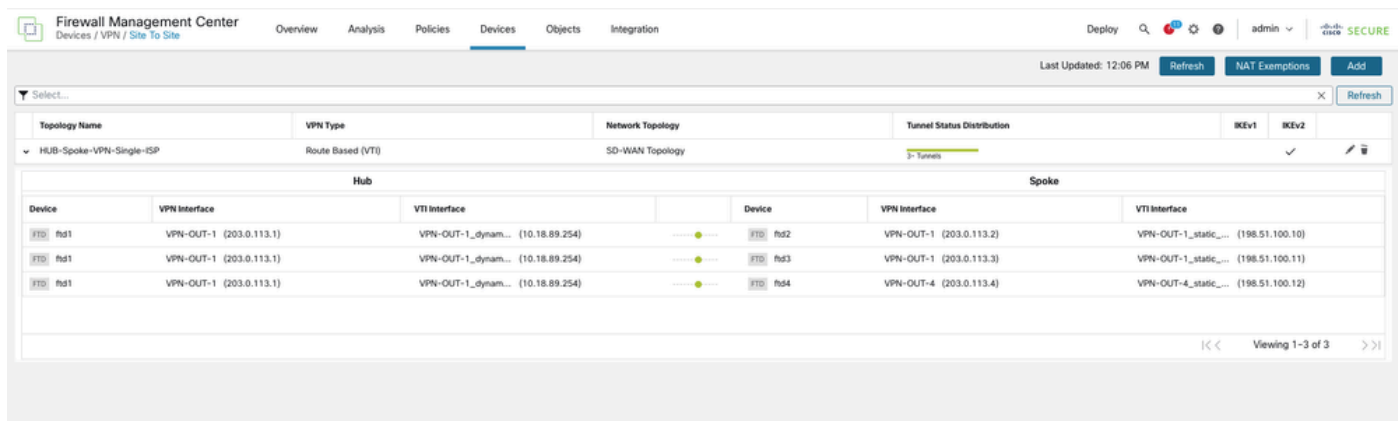
Next You have unsaved changes

Cancel Finish

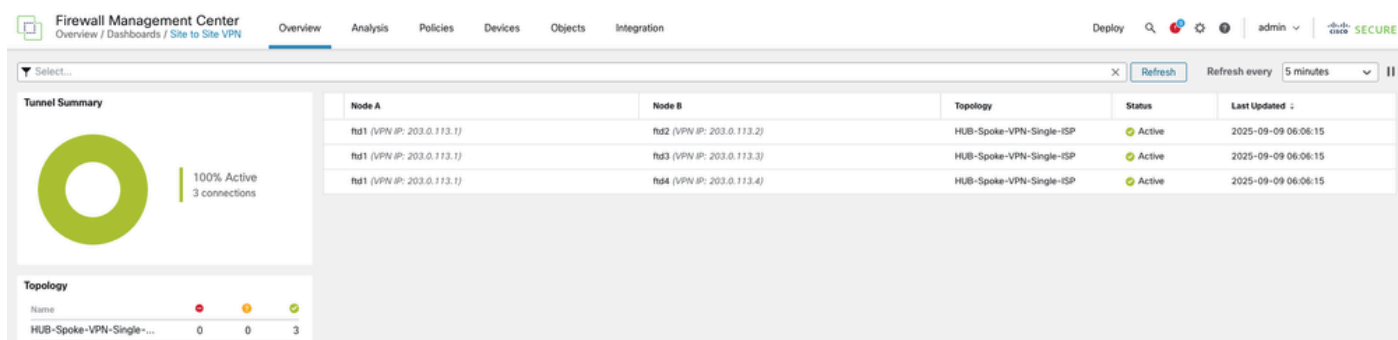
- 按一下「Next」，然後「Finish」，最後按一下「Deploy」完成整個程式。

驗證

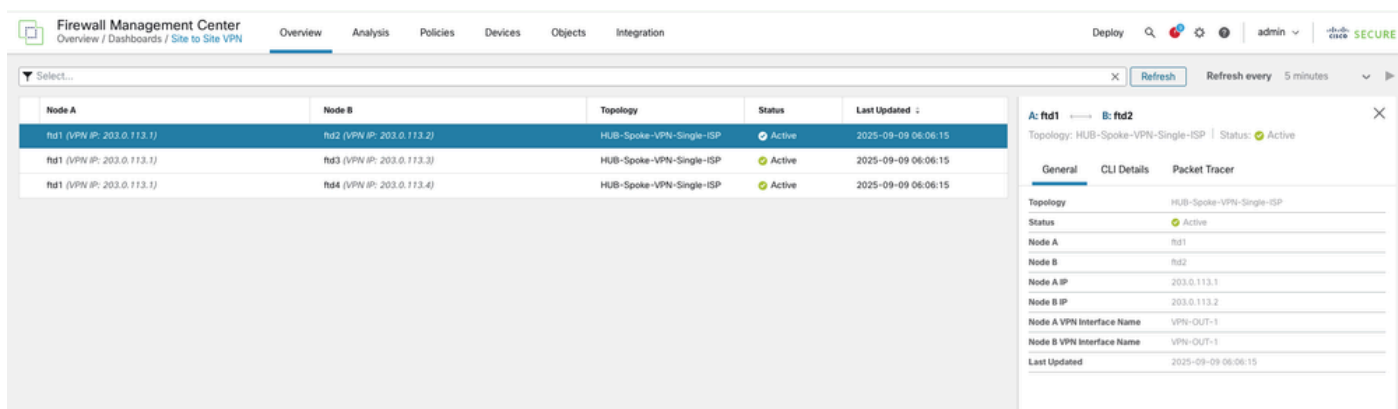
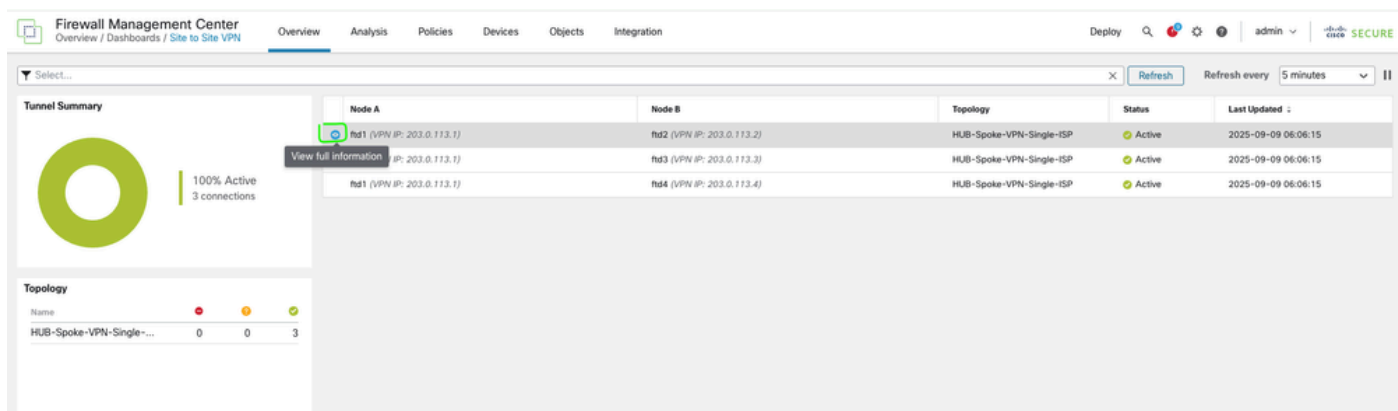
- 您可以通過導航到Devices > VPN > Site to Site來驗證隧道狀態。



- 可通過導航到概述>控制面板>站點到站點VPN來驗證其他詳細資訊。



- 如需進一步的深入分析，請選擇通道，然後點選檢視完整資訊。



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

- 輸出直接從FTD CLI顯示，並可以刷新以顯示更新的計數器和重要資訊，例如安全引數索引 (SPI)詳細資訊。

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: 100 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

- FTD CLI也可用於檢查路由資訊和BGP對等狀態。

在HUB端

<#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

在輻條側

也可以在輻條裝置上執行相同的驗證。下面是一個輻條上的示例。

<#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

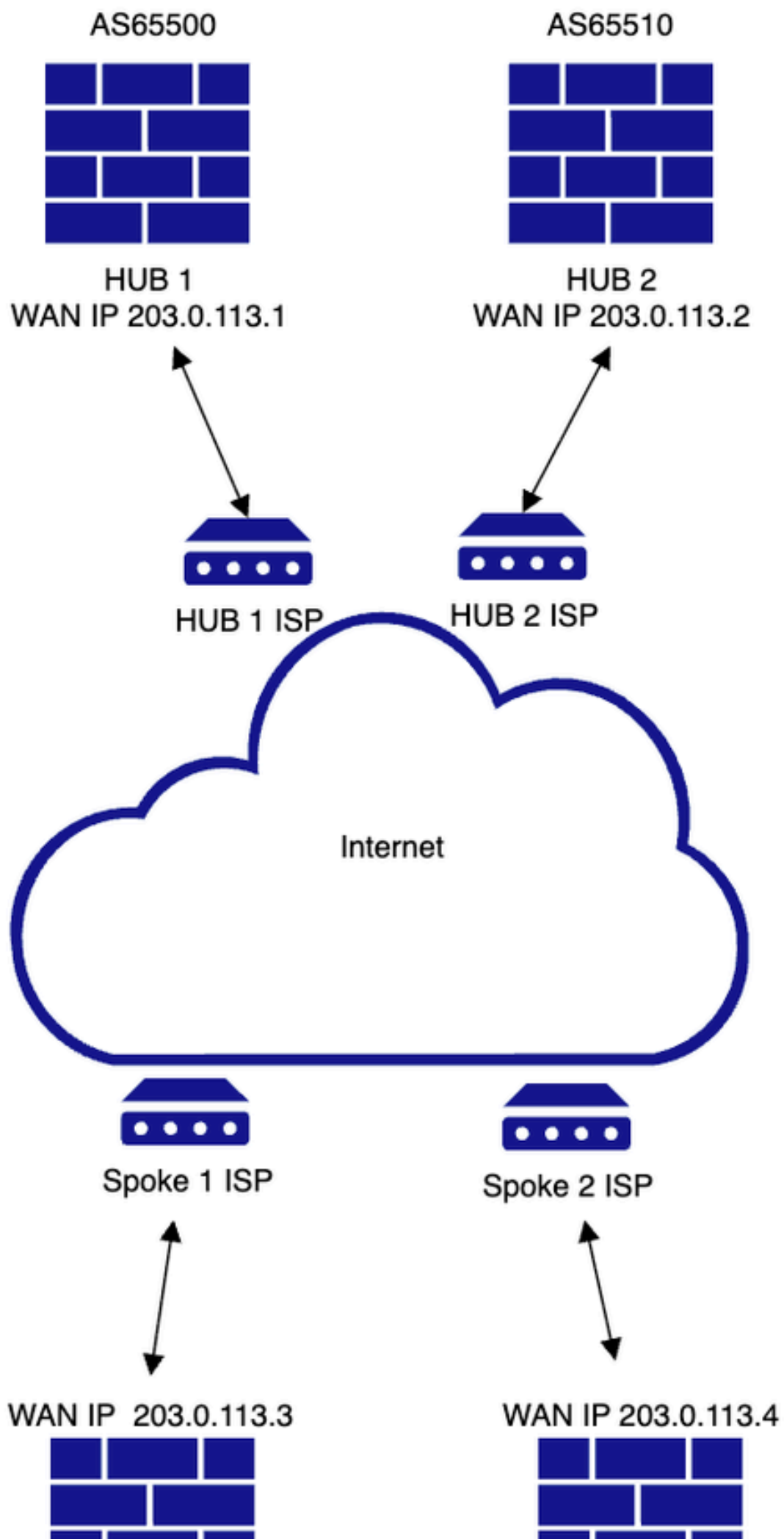
<<<<<<< spoke 2 inside network

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

<<<<<<< spoke 3 inside network

雙中心輻射型 (通過輔助中心輻射和輻射之間的EBGP為冗餘中心提供單一ISP)

網路圖表



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。