

# 配置雙ISP拓撲，在同一區域中配置兩個集線器和四個輻條

## 目錄

---

### [簡介](#)

### [必要條件](#)

[支援的軟體和硬體平台](#)

[需求](#)

[採用元件](#)

### [設定](#)

[網路圖表](#)

[步驟1.建立以WAN-1作為VPN介面的SD-WAN拓撲](#)

[步驟2.在主集線器上配置動態虛擬通道介面\(DVTI\)](#)

[步驟3.在輔助集線器上配置動態虛擬通道介面\(DVTI\)](#)

[步驟4.配置輻條](#)

[步驟5.配置身份驗證設定](#)

[步驟6.配置SD-WAN設定](#)

[步驟7.建立以WAN-2作為VPN介面的SD-WAN拓撲](#)

[步驟8.配置ECMP區域](#)

[步驟9.修改集線器上的BGP本地首選項](#)

### [驗證](#)

[驗證隧道狀態](#)

[驗證虛擬通道介面](#)

[驗證VPN流量的負載平衡](#)

[驗證雙ISP冗餘](#)

[驗證中心級冗餘](#)

---

## 簡介

本文檔介紹如何使用SD-WAN嚮導在同一區域配置具有兩個集線器和四個輻條的雙ISP拓撲。

## 必要條件

### 支援的軟體和硬體平台

經理	FTD	支援的平台
<ul style="list-style-type: none"><li>FMC &gt;= 7.6.0和FMC REST API</li><li>cdFMC &gt;= 7.6.0</li></ul>	<ul style="list-style-type: none"><li>集線器FTD &gt;= 7.6.0</li><li>分支FTD &gt;= 7.3.0</li></ul>	FMC >= 7.6.0可以管理的所有平台

- |             |  |  |
|-------------|--|--|
| • FDM — 不支援 |  |  |
|-------------|--|--|

## 需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦
- 思科安全防火牆管理中心
- 軟體定義WAN(SD-WAN)

## 採用元件

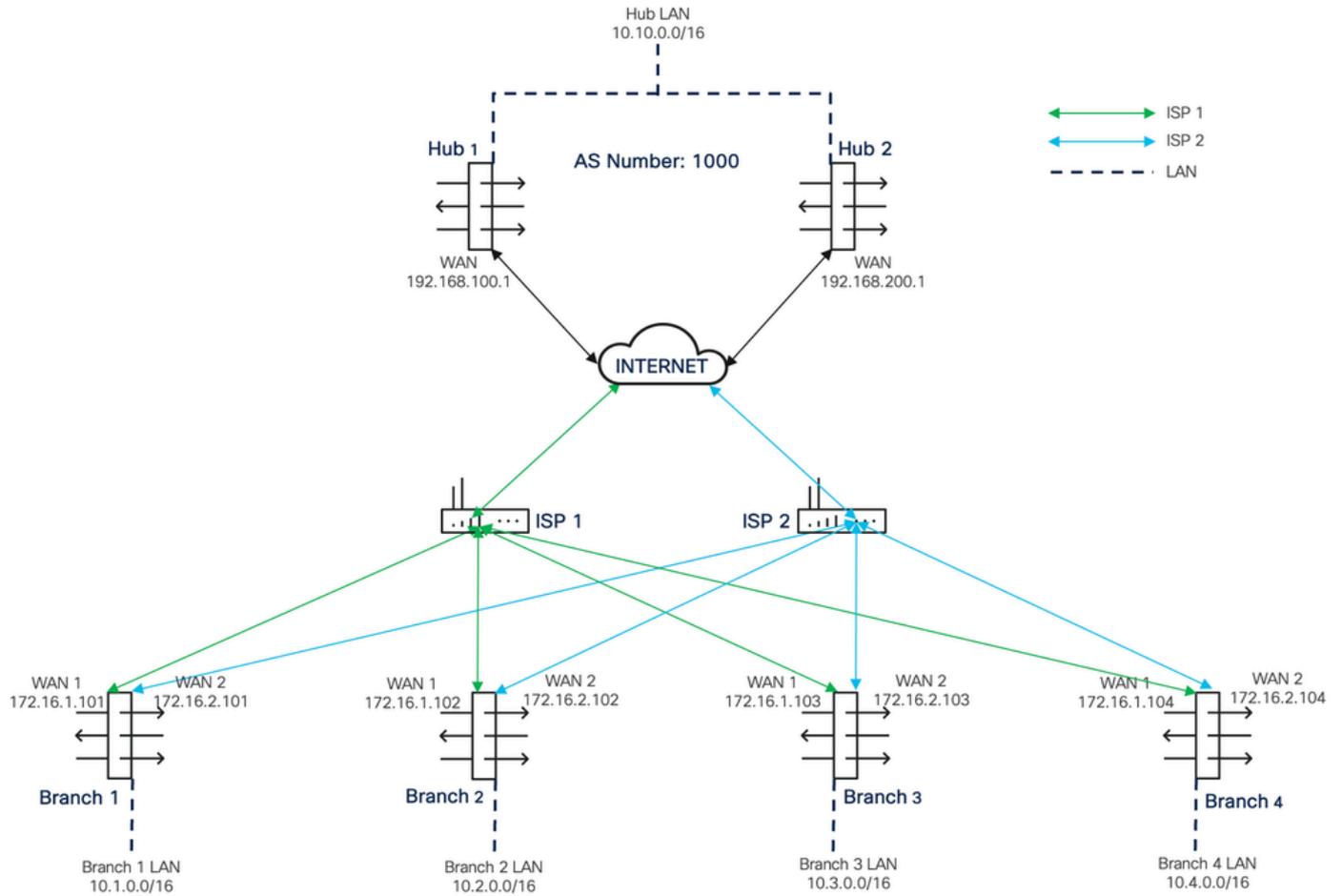
本文中的資訊係根據以下軟體和硬體版本：

- FTD版本7.6.0
- FMC 7.6.0版

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。

## 設定

### 網路圖表



Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

Deploy Search admin

View By: Group

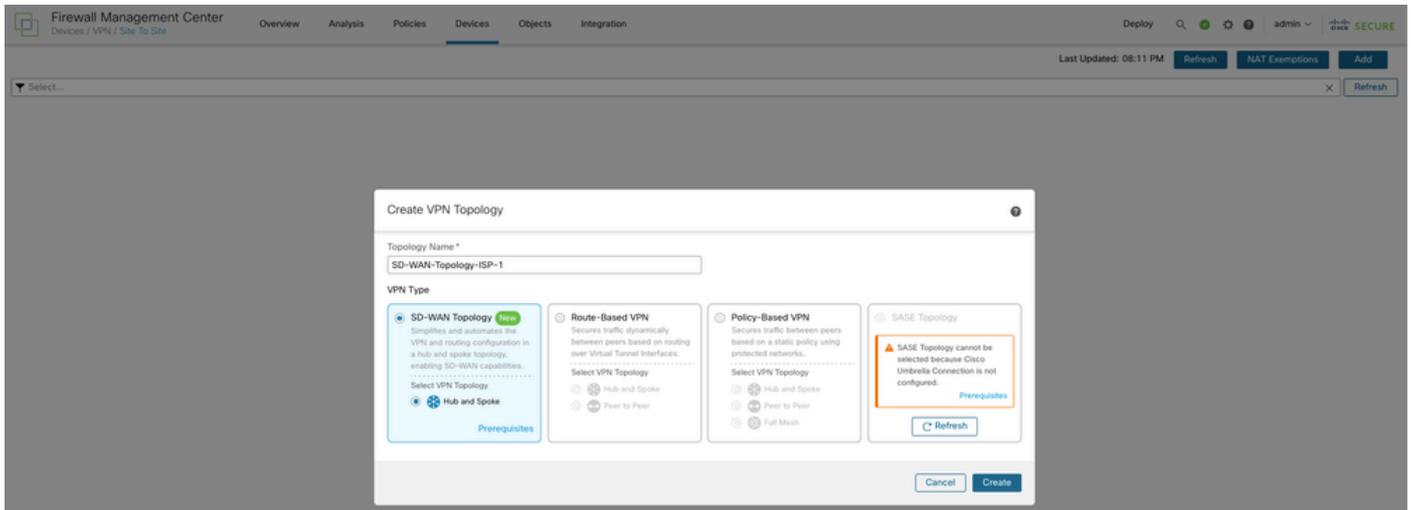
All (8) Error (0) Warning (0) Offline (0) Normal (8) Deployment Pending (0) Upgrade (0) Snort 3 (8)

Collapsible All Download Device List Report

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

## 步驟1. 建立以WAN-1作為VPN介面的SD-WAN拓撲

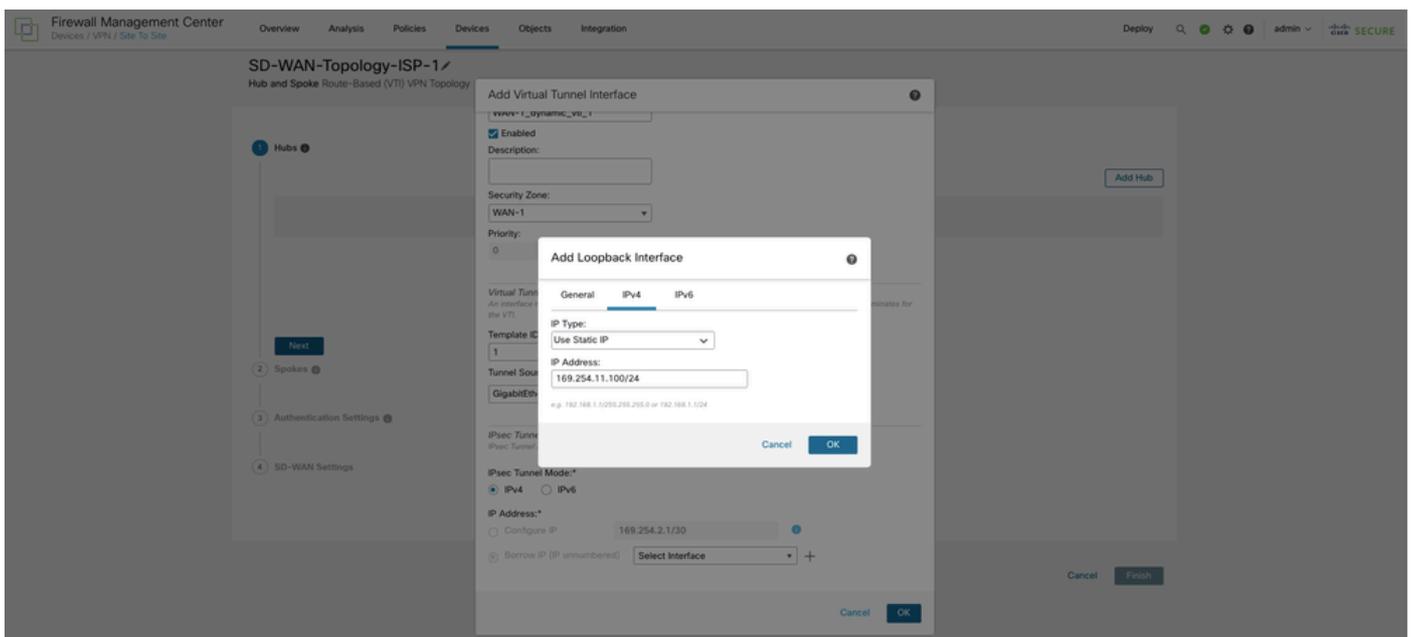
導航到Devices > VPN > Site To Site。選擇Add，然後在Topology Name欄位中輸入第一個以WAN-1作為VPN介面的拓撲的合適名稱。選擇SD-WAN Topology，然後選擇Create。



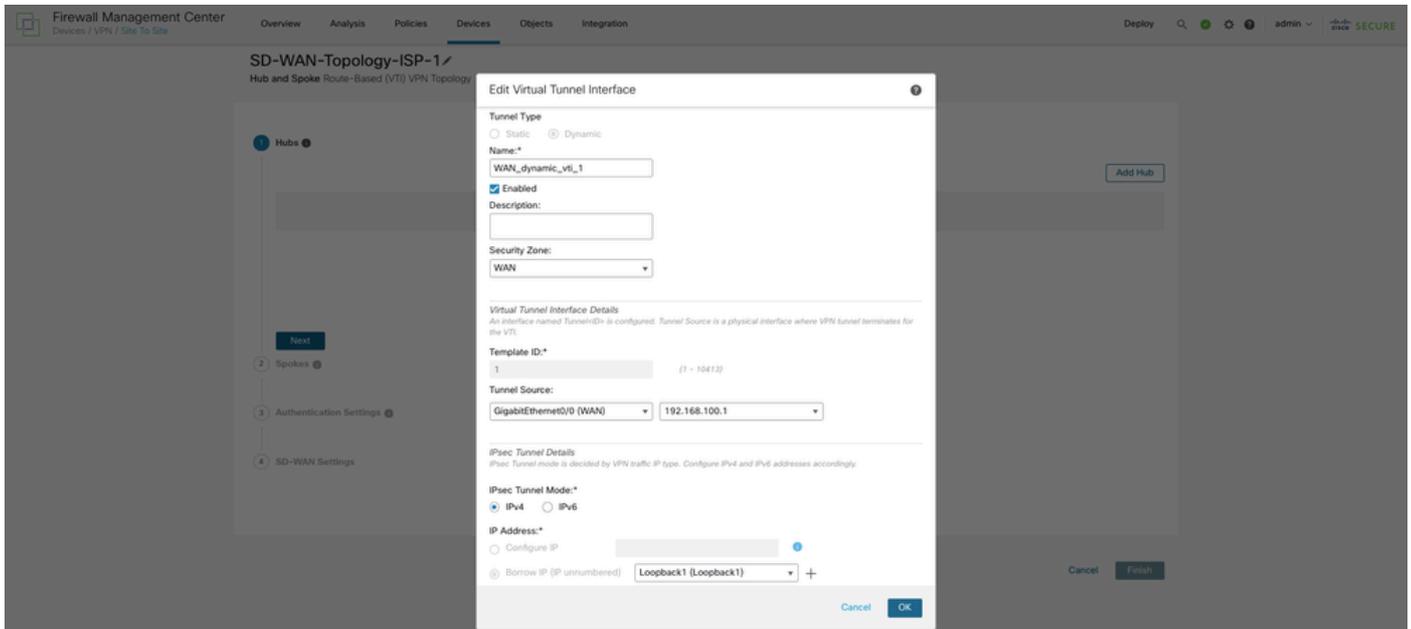
## 步驟2.在主中心上配置動態虛擬通道介面(DVTI)

選擇Add Hub，然後從Device下拉選單中選擇主集線器。選擇Dynamic Virtual Tunnel Interface(DVTI)旁邊的+圖示。配置名稱、安全區域和模板ID並分配WAN-1作為DVTI的通道源介面

o



從Border IP下拉選單中選擇一個物理或環回介面。在當前拓撲中，DVTI繼承環回介面IP地址。選擇OK。



選擇地址池，或選擇Spoke Tunnel IP Address Pool旁邊的+圖示以建立新的地址池。新增輻條時，嚮導會自動生成分支隧道介面，並從此IP地址池將IP地址分配給這些分支介面。

## Add IPv4 Pool



Name\*

Spoke-Pool-Hub-1-ISP-1

Description

IPv4 Address Range\*

169.254.11.101-169.254.11.150

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

Mask\*

255.255.255.0

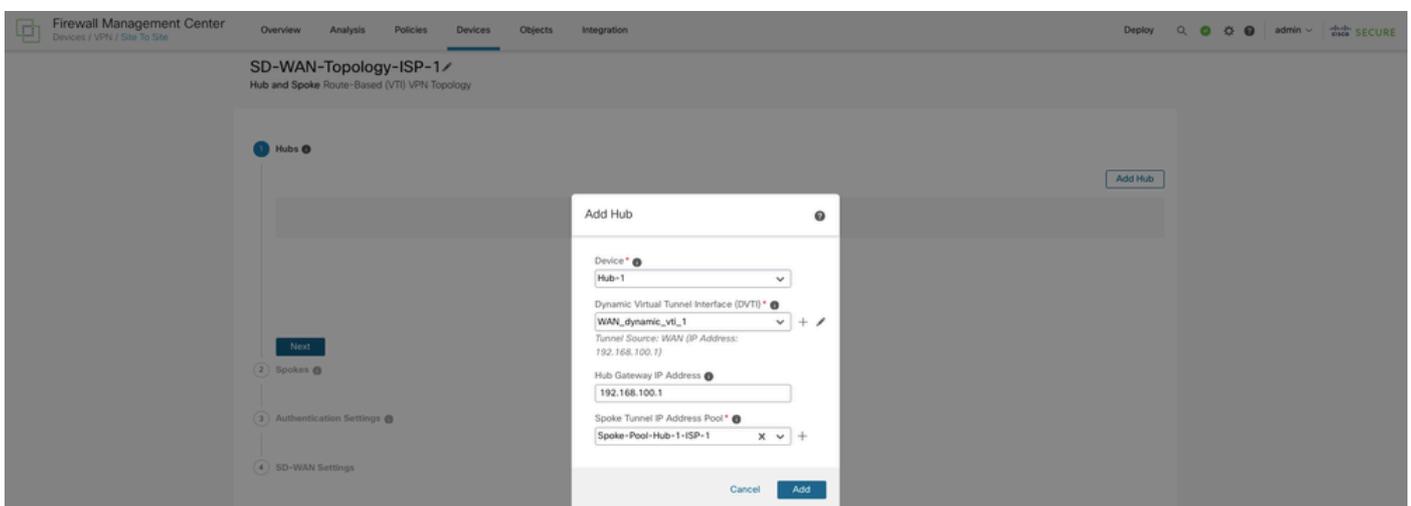
Allow Overrides

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

Cancel

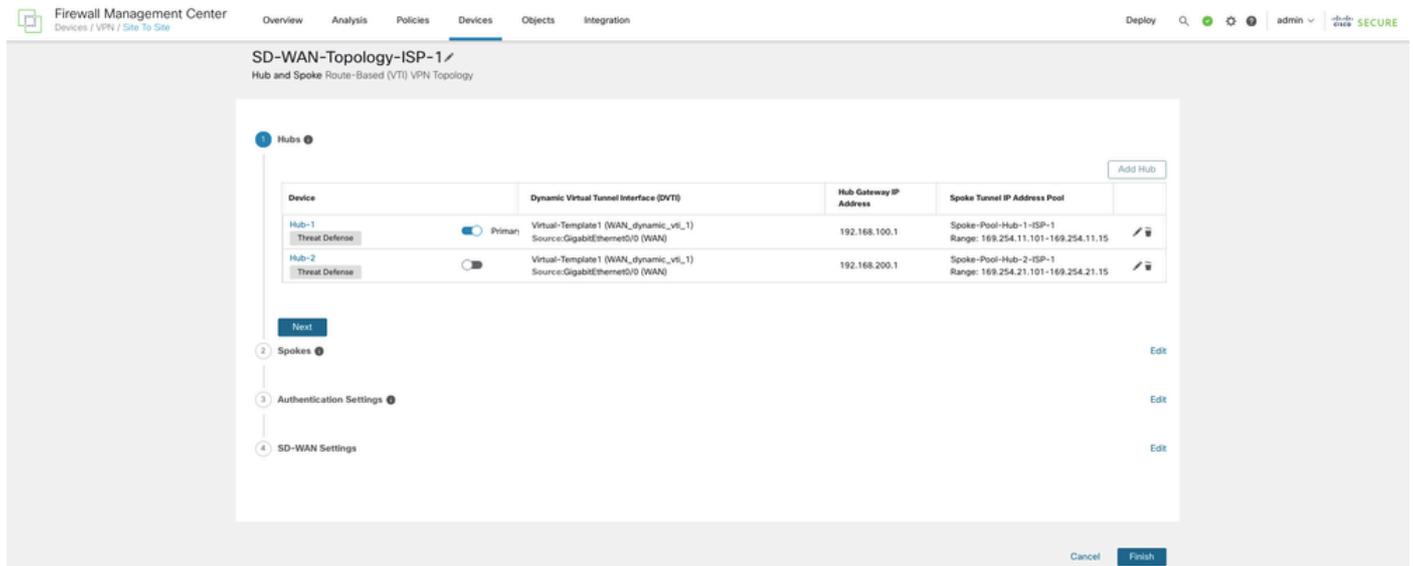
Save

主集線器配置完成後，選擇Add將主集線器儲存在拓撲中。



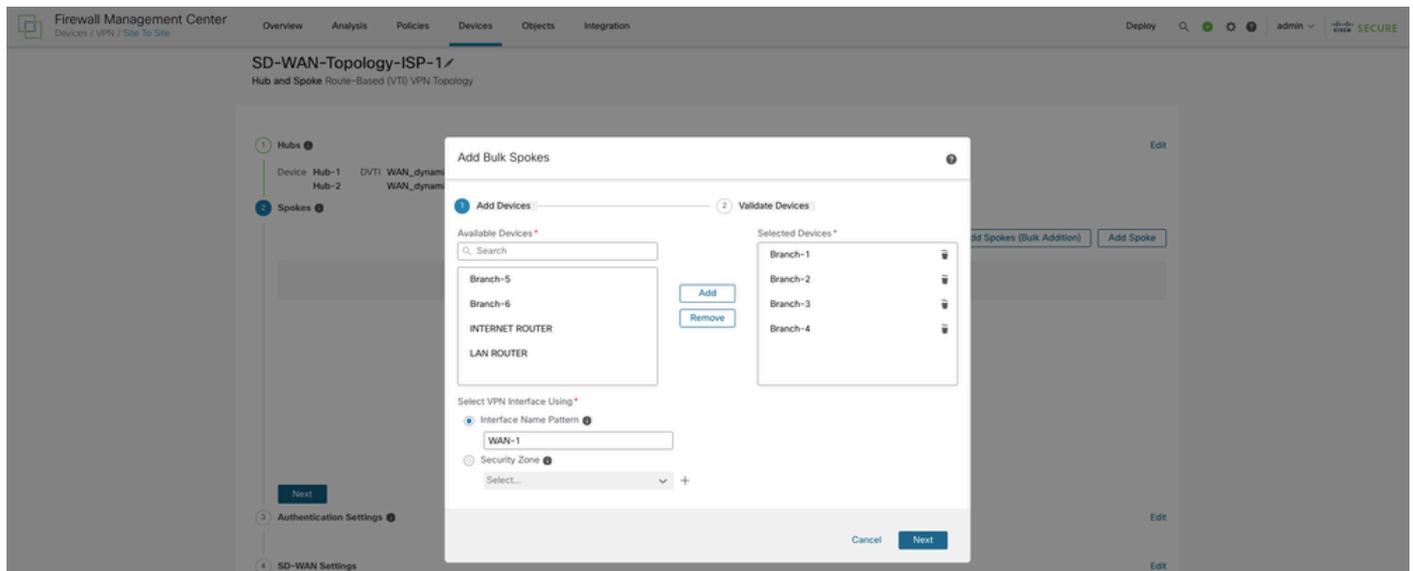
### 步驟3.在輔助集線器上配置動態虛擬通道介面(DVTI)

現在，重複步驟1和2，再次選擇Add Hub以配置拓撲中以WAN-1作為VPN介面的輔助集線器。選擇Next。

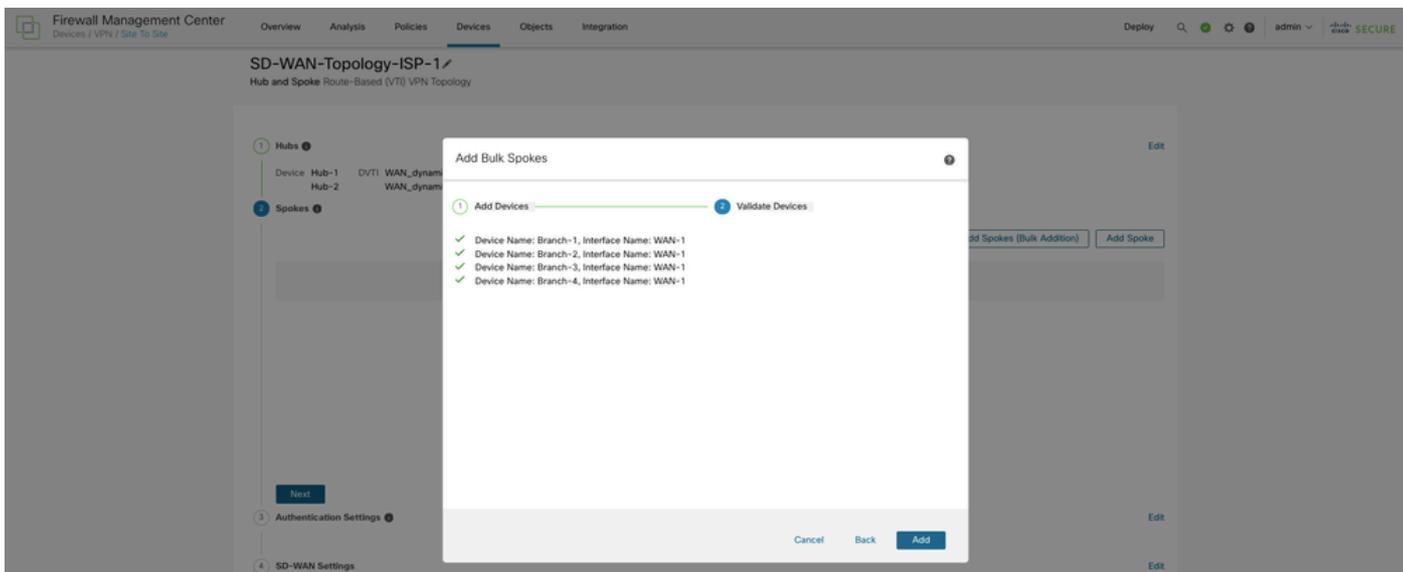


### 步驟4.配置輻條

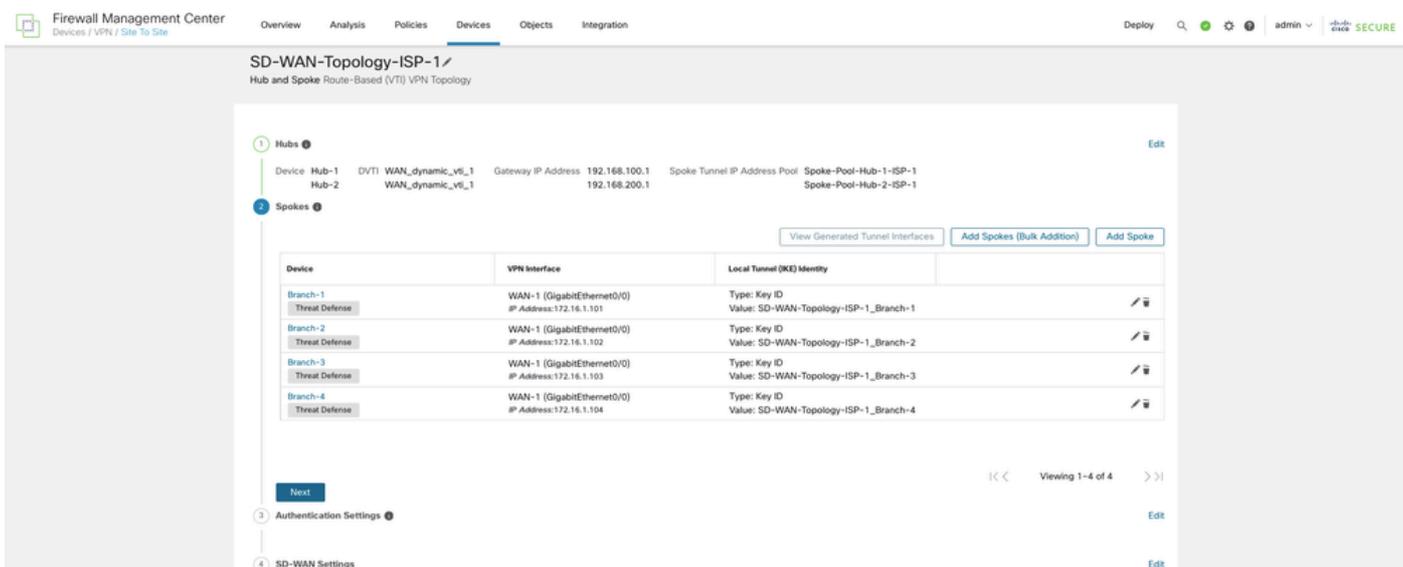
選擇Add Spoke以新增單個分支裝置，或按一下Add Spoke(Bulk Addition)將多個分支新增到拓撲中。當前拓撲使用後一個選項將多個分支FTD新增到拓撲中。在「新增批次輻條」對話方塊中，選擇要作為輻條新增的必要FTD。在所有輻條上選擇一個與WAN-1的邏輯名稱相匹配的通用介面名稱模式，或者選擇與WAN-1相關聯的安全區域。



選擇下一步，以便嚮導驗證輻條是否具有指定模式或安全區域的介面。

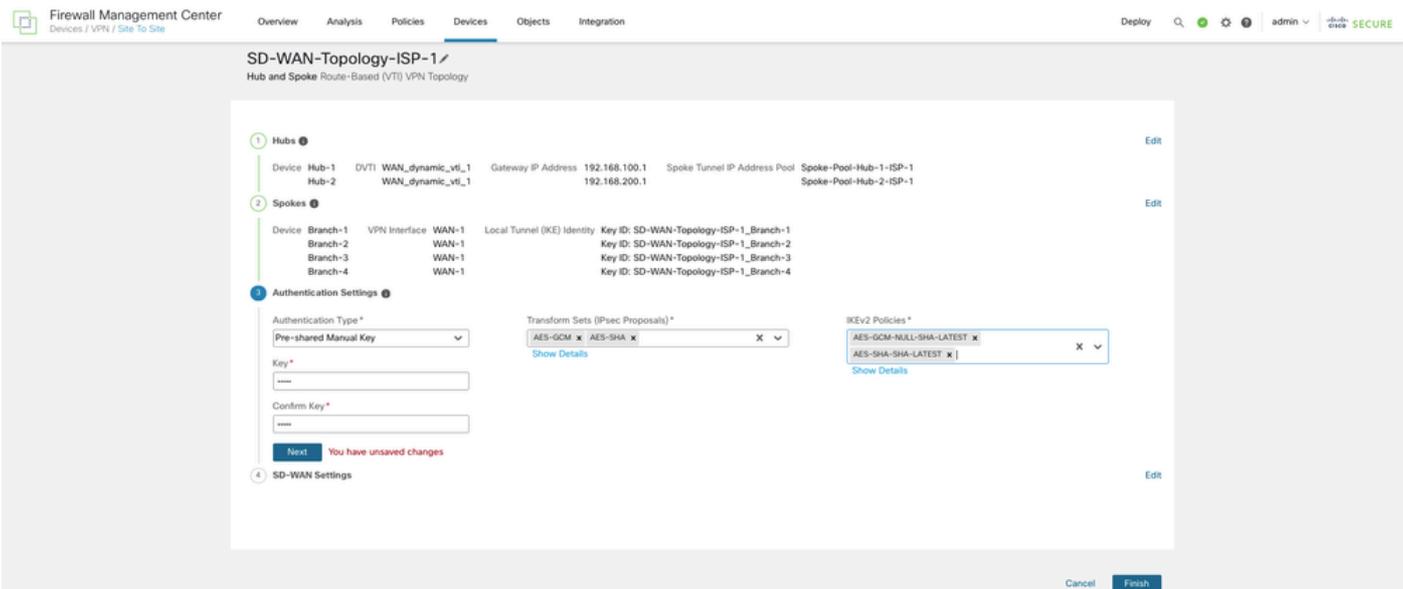


選擇Add，嚮導將自動選擇中心DVTI作為每個分支的隧道源IP地址。



## 步驟5. 配置身份驗證設定

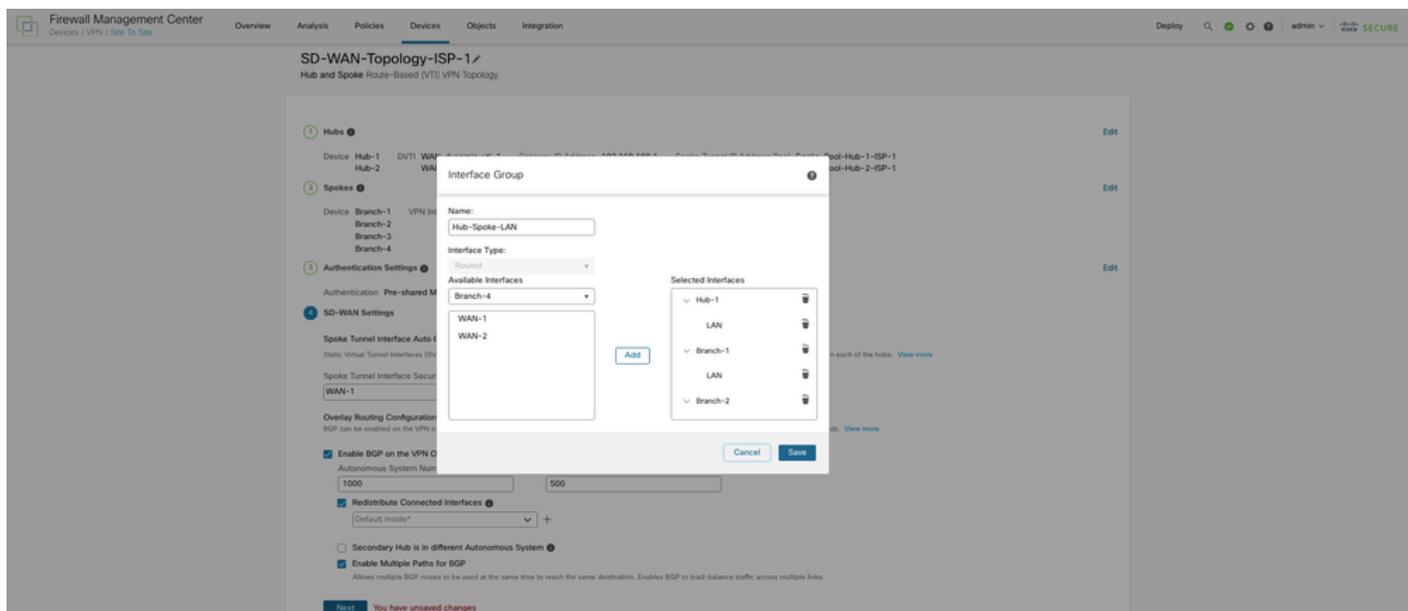
選擇Next以配置Authentication Settings。對於裝置身份驗證，您可以在Authentication Type下拉選單中選擇手動預共用金鑰、自動生成的預共用金鑰或證書。從Transform Sets和IKEv2 Policies下拉選單中選擇一個或多個演算法。



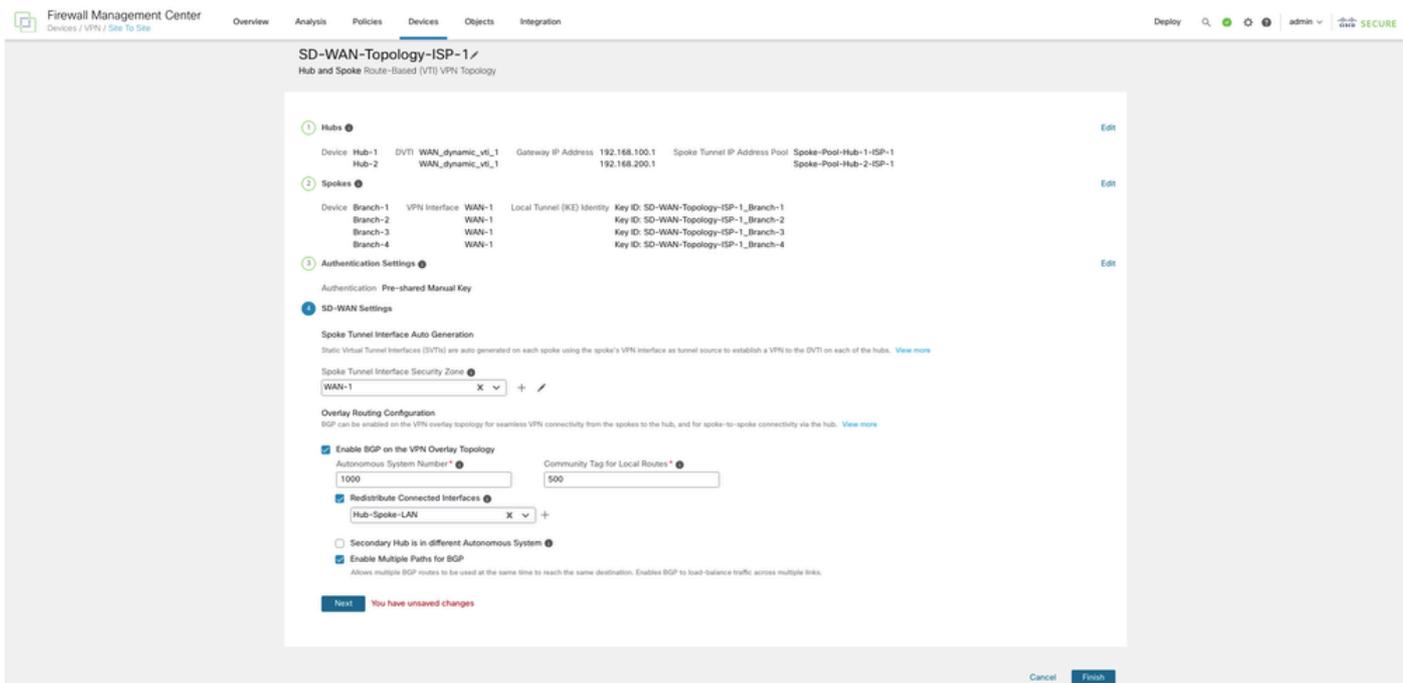
## 步驟6.配置SD-WAN設定

選擇Next配置SD-WAN設定。此步驟涉及分支隧道介面的自動生成以及重疊網路的BGP配置。在「分支通道介面安全區域」下拉選單中，選擇安全區域，或選擇+以建立安全區域，嚮導會自動將分支的自動生成的靜態虛擬通道介面(SVTI)新增到安全區域。

選中在VPN重疊拓撲上啟用BGP覈取方塊以自動執行重疊隧道介面之間的BGP配置。在Autonomous System Number欄位中，輸入自治系統(AS)編號。勾選「Redistribute Connected Interfaces」覈取方塊並從下拉式清單中選擇一個介面組，或選擇「+」，使用集線器的已連線LAN介面和輻條建立一個介面組，以便在重疊拓撲中進行BGP路由重分發。



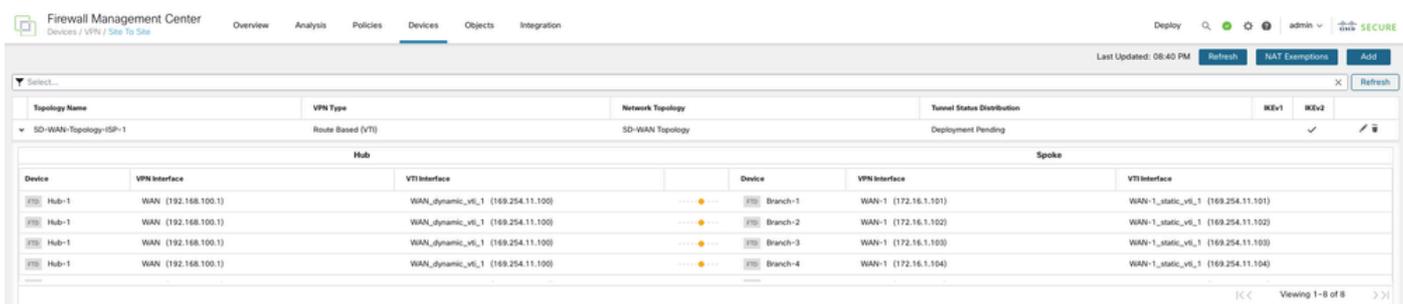
在Community Tag for Local Routes欄位中，輸入BGP社群屬性以標籤連線的和重新分配的本地路由。此屬性支援輕鬆路由過濾。如果不同AS中有輔助集線器，請選中Secondary Hub is in the Different Autonomous System復選框。最後，勾選Enable Multiple Paths for BGP 覈取方塊以啟用BGP以負載均衡多個鏈路上的流量。



按一下Finish儲存並驗證SD-WAN拓撲。

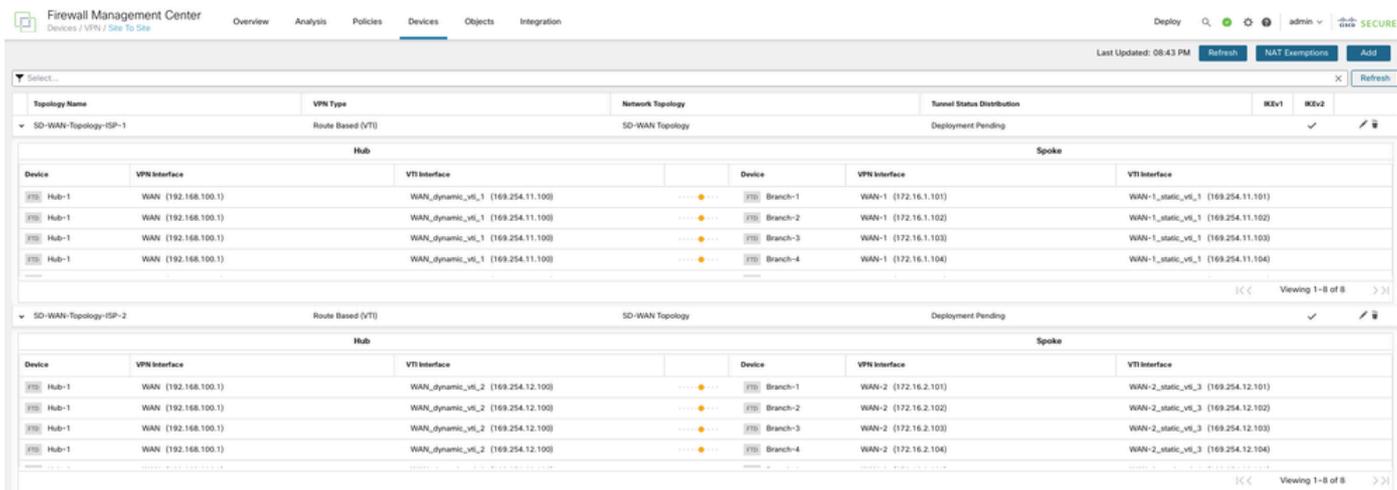


您可以在Devices > Site-to-site VPN下檢視拓撲。第一個SD-WAN拓撲中的隧道總數為8。



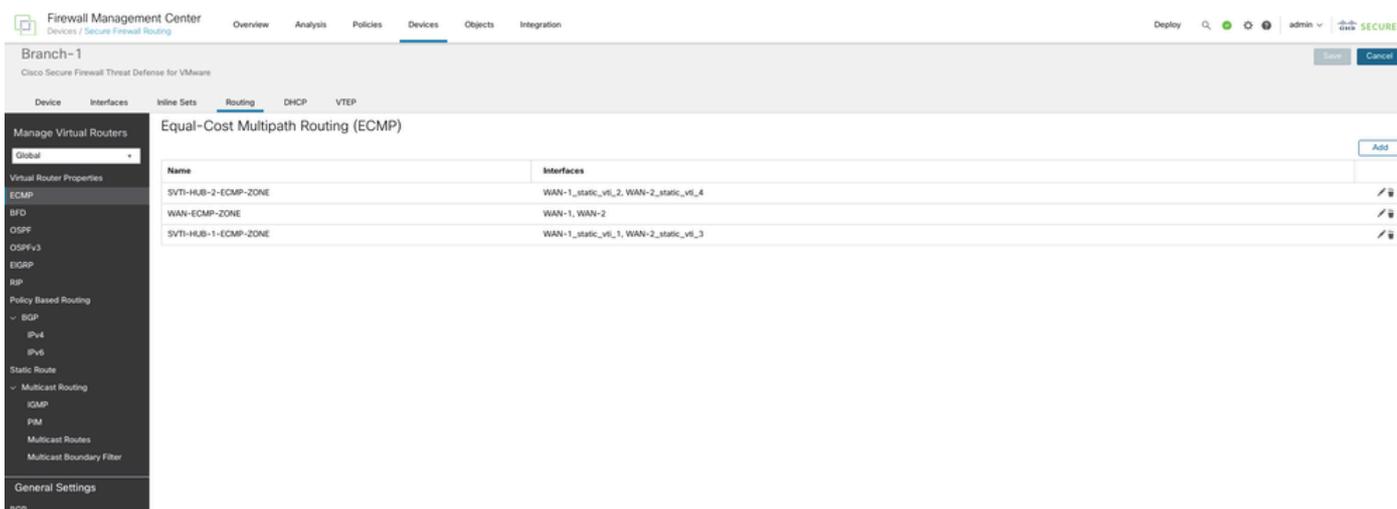
步驟7.建立以WAN-2作為VPN介面的SD-WAN拓撲

重複步驟1至6，配置以WAN-2作為VPN介面的SD-WAN拓撲。第二個SD-WAN拓撲中的隧道總數為8。最終的拓撲必須如下圖所示。



## 步驟8.配置ECMP區域

在每個分支上，導航到Routing > ECMP，並為連線到主集線器和輔助集線器的WAN介面和SVTI配置ECMP (等價多路徑) 區域，如下所示。這樣可以提供鏈路冗餘並啟用VPN流量的負載均衡。



## 步驟9.修改集線器上的BGP本地首選項

在輔助集線器上導航到Routing > General Settings > BGP。選擇Enable BGP，設定AS編號，並在Best Path Selection下設定預設本機優先選項值，使其低於在主集線器上設定的值。選擇Save。這可確保通向主集線器的路由優先於通往輔助集線器的路由。當主集線器關閉時，通往輔助集線器的路由將接管該路由。

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🔄 🏠 admin 🔒 **SECURE**

Hub-2  
Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP  
BFD  
OSPF  
OSPFv3  
EGRP  
RIP

Policy Based Routing

BGP

IPv4  
IPv6

Static Route

Multicast Routing

IGMP  
PIM  
Multicast Routes  
Multicast Boundary Filter

General Settings

BGP

Enable BGP:

AS Number\*  
1000  
(1-4294967295 or 1-0-65535,65535)

Override BGP general settings router-id address:

Router Id  
Automatic

IP Address\*

**General**

Scanning Interval: 60

Number of AS numbers in AS\_PATH attribute of received routes: None

Log Neighbor Changes: Yes

Use TCP path MTU discovery: Yes

Reset session upon fallover: Yes

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

Use dot notation for AS number: No

Aggregate Timer: 30

**Best Path Selection**

Default local preference: 90

Allow comparing MED from different neighbors: No

Compare Router ID for identical EBGp paths: No

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

Treat missing MED as the best preferred path: No

**Neighbor Timers**

Keepalive Interval: 60

Hold time: 180

Min hold time: 0

**Next Hop**

Address tracking: Yes

Delay interval: 5

**Graceful Restart (Use in fallover or spanned cluster mode)**

Graceful Restart: No

Restart time: 120

Statepath time: 300

將配置部署到所有裝置。

## 驗證

### 驗證隧道狀態

要驗證SD-WAN拓撲的VPN隧道是否已啟動，請選擇Device > VPN > Site-to-Site。

Firewall Management Center  
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🔄 🏠 admin 🔒 **SECURE**

Last Updated: 09:21 PM Refresh NAT Exemptions Add

Select...

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKv1	IKv2
SD-WAN-Topology-ISP-1	Route Based (VTI)	SD-WAN Topology	8 Tunnels	✓	✓

**Hub**

Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)

**Spoke**

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

Viewing 1-8 of 8

**SD-WAN-Topology-ISP-2**

Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)

**Spoke**

Device	VPN Interface	VTI Interface
Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_1 (169.254.12.101)
Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_1 (169.254.12.102)
Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_1 (169.254.12.103)
Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_1 (169.254.12.104)

Viewing 1-8 of 8

要檢視SD-WAN VPN隧道的詳細資訊，請選擇Overview > Dashboards > Site-to-site VPN。

Firewall Management Center  
Overview / Dashboards / Site To Site VPN

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🔄 🏠 admin 🔒 **SECURE**

Select...

Refresh Refresh every 5 minutes

**Tunnel Summary**

100% Active  
16 connections

**Topology**

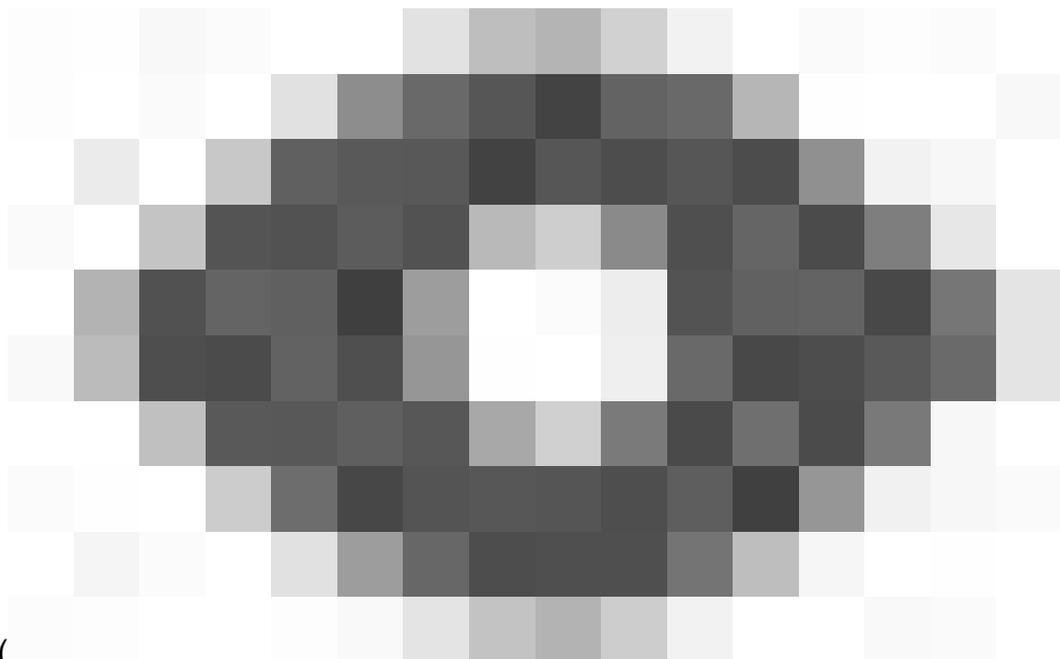
Name	Active	Down	Disabled
SD-WAN-Topology-ISP-1	0	0	8
SD-WAN-Topology-ISP-2	0	0	8

Node A	Node B	Topology	Status	Last Updated :
Branch-4 (VPN IP: 172.16.1.104)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-4 (VPN IP: 172.16.2.104)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:17:16
Branch-1 (VPN IP: 172.16.1.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-3 (VPN IP: 172.16.2.103)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:17:16
Branch-3 (VPN IP: 172.16.1.103)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-2 (VPN IP: 172.16.2.102)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:17:21
Branch-2 (VPN IP: 172.16.1.102)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:21
Branch-1 (VPN IP: 172.16.1.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-2 (VPN IP: 172.16.1.102)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-3 (VPN IP: 172.16.1.103)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27

Viewing 1-16 of 16

要檢視每個VPN隧道的詳細資訊，請執行以下操作：

1. 將滑鼠懸停在隧道上。



2. 選擇檢視完整資訊( )圖示。系統將顯示一個包含通道詳細資訊和更多操作的窗格。
3. 選擇側窗格中的CLI Details頁籤以檢視show命令和IPsec安全關聯的詳細資訊。

A: Branch-1 ↔ B: Hub-1



Topology: SD-WAN-Topology-ISP-2 | Status: ✔ Active

General CLI Details Packet Tracer

Refresh Maximize view

### Summary

Node A (172.16.2.101/500) ⓘ		Node B (192.168.100.1/500) ⓘ	
<b>Transmitted:</b>	8.46 KB (8664 B)	<b>Transmitted:</b>	5.98 KB (6123 B)
<b>Received:</b>	27.73 KB (28400 B)	<b>Received:</b>	7.68 KB (7868 B)

### IPsec Security Associations (2)

0.0.0.0/0.0.0.0/0/0 ⓘ		0.0.0.0/0.0.0.0/0/0 ⓘ	
<b>Settings:</b>	L2L,Tunnel,IKEv2,...	<b>Settings:</b>	L2L,Tunnel,IKEv2,VTI
<b>Encaps/Encrypt:</b>	140 / 140 pkts	<b>Encaps/Encrypt:</b>	92 / 92 pkts
<b>Dcaps/Decrypt:</b>	232 / 232 pkts	<b>Dcaps/Decrypt:</b>	96 / 96 pkts
<b>Remaining Lifetime for SPI ID: 0x5B2983A9</b>			
<b>Outbound:</b>	3.69 GB (3962871000 B) 12:47:26 (26246 sec)	<b>Inbound:</b>	3.65 GB (3916794000 B) 12:50:26 (26426 sec)
<b>Remaining Lifetime for SPI ID: 0x0F4EA9C0</b>			
<b>Inbound:</b>	3.99 GB (4285416000 B) 12:47:26 (26246 sec)	<b>Outbound:</b>	3.69 GB (3962874000 B) 12:50:26 (26426 sec)
0.0.0.0/0.0.0.0/0/0 ⓘ			
<b>Settings:</b>	L2L,Tunnel,IKEv2,...	Info is not available for Extranet device	
<b>Encaps/Encrypt:</b>	96 / 96 pkts		
<b>Dcaps/Decrypt:</b>	92 / 92 pkts		
<b>Remaining Lifetime for SPI ID: 0x1DEFCEB21</b>			
<b>Outbound:</b>	4.03 GB (4331514000 B) 12:50:25 (26425 sec)	<b>Inbound:</b>	No data
<b>Remaining Lifetime for SPI ID: 0x53B1AE47</b>			
<b>Inbound:</b>	3.65 GB (3916794000 B) 12:50:25 (26425 sec)	<b>Outbound:</b>	No data

Branch-1 (VPN Interface IP: 172.16.2.101)

show crypto ipsec sa peer 192.168.100.1 ⓘ

WAN-2\_static\_vti\_3 — 通過ISP 2將伺服器連線到集線器1

WAN-1\_static\_vti\_2 — 通過ISP 1將伺服器連線到集線器2

WAN-2\_static\_vti\_4 — 通過ISP 2將伺服器連線到集線器2

## 驗證VPN流量的負載平衡

隧道狀態可以在Site to Site VPN控制面板中看到。理想情況下，所有隧道都必須處於活動狀態：



首選到主集線器的路由。Branch 1上的show route命令表明，VPN流量在ISP 1和ISP 2上的兩個SVTI之間負載均衡，可到達主集線器：

```
CLI Troubleshoot
> Command: show route
Execute Refresh Copy
Device: Branch-1
> show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C    10.1.0.0 255.255.0.0 is directly connected, LAN
L    10.1.0.1 255.255.255.255 is directly connected, LAN
B    10.10.0.0 255.255.0.0 [200/1] via 169.254.12.100, 01:41:02
    [200/1] via 169.254.11.100, 01:41:02
C    169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V    169.254.11.100 255.255.255.255
    connected by VPN (advertised), WAN-1_static_vti_1
L    169.254.11.101 255.255.255.255
    is directly connected, WAN-1_static_vti_1
C    169.254.12.0 255.255.255.0 is directly connected, WAN-2_static_vti_3
V    169.254.12.100 255.255.255.255
    connected by VPN (advertised), WAN-2_static_vti_3
L    169.254.12.101 255.255.255.255
    is directly connected, WAN-2_static_vti_3
C    169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V    169.254.21.100 255.255.255.255
    connected by VPN (advertised), WAN-1_static_vti_2
L    169.254.21.101 255.255.255.255
    is directly connected, WAN-1_static_vti_2
C    169.254.22.0 255.255.255.0 is directly connected, WAN-2_static_vti_4
V    169.254.22.100 255.255.255.255
    connected by VPN (advertised), WAN-2_static_vti_4
L    169.254.22.101 255.255.255.255
    is directly connected, WAN-2_static_vti_4
C    172.16.1.0 255.255.255.0 is directly connected, WAN-1
L    172.16.1.101 255.255.255.255 is directly connected, WAN-1
C    172.16.2.0 255.255.255.0 is directly connected, WAN-2
L    172.16.2.101 255.255.255.255 is directly connected, WAN-2
D    192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 02:03:26, WAN-1
D    192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 02:03:26, WAN-2
D    192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
    [90/1024] via 172.16.1.1, 02:03:26, WAN-1
D    192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
    [90/1024] via 172.16.1.1, 02:03:26, WAN-1
```

在Unified Events中可以看到為實際VPN流量所採用的輸出介面：

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

## 驗證雙ISP冗餘

當ISP-2關閉時，隧道狀態表示通過ISP-1的隧道處於活動狀態：

Node A	Node B	Topology	Status	Last Updated
Branch-1 (VPN IP: 172.16.1.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-1 (VPN IP: 172.16.1.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-1 (VPN IP: 172.16.2.101)	Hub-3 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-2	Inactive	2024-12-08 08:29:41
Branch-1 (VPN IP: 172.16.2.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Inactive	2024-12-08 08:29:41

首選到主集線器的路由。Branch 1上的show route命令表示VPN流量通過ISP-1上的SVTI路由到主集線器：

```

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

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C    10.1.0.0 255.255.0.0 is directly connected, LAN
I    10.1.0.1 255.255.255.255 is directly connected, LAN
B    10.10.0.0 255.255.0.0 [200/1] via 169.254.11.100, 00:04:02
C    169.254.11.0 255.255.255.0 is directly connected, WAN-1 static vti 1
V    169.254.11.100 255.255.255.255
      connected by VPN (advertised), WAN-1_static_vti_1
L    169.254.11.101 255.255.255.255
      is directly connected, WAN-1_static_vti_1
C    169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V    169.254.21.100 255.255.255.255
      connected by VPN (advertised), WAN-1_static_vti_2
L    169.254.21.101 255.255.255.255
      is directly connected, WAN-1_static_vti_2
C    172.16.1.0 255.255.255.0 is directly connected, WAN-1
L    172.16.1.101 255.255.255.255 is directly connected, WAN-1
D    172.16.2.0 255.255.255.0 [90/1280] via 172.16.1.1, 00:04:03, WAN-1
D    192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 22:12:57, WAN-1
D    192.168.2.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D    192.168.100.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D    192.168.200.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1

```

在Unified Events中可以看到為實際VPN流量所採用的輸出介面：

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

## 驗證中心級冗餘

當主集線器關閉時，通道狀態表示通往輔助集線器的通道處於活動狀態：



由於主集線器已關閉，因此首選到輔助集線器的路由。Branch 1上的show route命令表示在ISP 1和ISP 2上的兩個SVTI之間將VPN流量負載均衡到輔助中心：

CLI Troubleshoot

>\_ Command:  Execute Refresh Copy | Device:

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C    10.1.0.0 255.255.0.0 is directly connected, LAN
L    10.1.0.1 255.255.255.255 is directly connected, LAN
B    10.10.0.0 255.255.0.0 [200/1] via 169.254.22.100, 00:09:02
    [200/1] via 169.254.21.100, 00:09:02
C    169.254.21.0 255.255.255.0 is directly connected, WAN-1 static vti 2
V    169.254.21.100 255.255.255.255
    connected by VPN (advertised), WAN-1_static_vti_2
L    169.254.21.101 255.255.255.255
    is directly connected, WAN-1_static_vti_2
C    169.254.22.0 255.255.255.0 is directly connected, WAN-2 static vti 4
V    169.254.22.100 255.255.255.255
    connected by VPN (advertised), WAN-2_static_vti_4
L    169.254.22.101 255.255.255.255
    is directly connected, WAN-2_static_vti_4
C    172.16.1.0 255.255.255.0 is directly connected, WAN-1
L    172.16.1.101 255.255.255.255 is directly connected, WAN-1
C    172.16.2.0 255.255.255.0 is directly connected, WAN-2
L    172.16.2.101 255.255.255.255 is directly connected, WAN-2
D    192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 00:11:13, WAN-1
D    192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 00:11:13, WAN-2
D    192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
    [90/1024] via 172.16.1.1, 00:11:13, WAN-1
D    192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
    [90/1024] via 172.16.1.1, 00:11:13, WAN-1
    
```

Close

在Unified Events中可以看到為實際VPN流量所採用的輸出介面：

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

## 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）。