

# 在安全防火牆上配置Azure Dual ISP vWAN連線

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[圖表](#)

[雙直接網際網路接入\(DIA\)鏈路 \( Azure + FTD負載平衡/冗餘 \)](#)

[設定](#)

[第1階段：Azure vWAN VPN站點配置](#)

[步驟 1:建立Azure vWAN VPN站點 \(遠端FTD裝置\)](#)

[步驟 2:配置Azure APIPA網關引數](#)

[步驟 3:配置Azure vWAN Site VPN引數](#)

[步驟 4:在VPN站點連結例項上啟用和啟用自定義BGP APIPA](#)

[步驟 5:下載VPN站點配置檔案](#)

[第2階段：配置FTD以實現到Azure vWAN的雙ISP連線](#)

[步驟 1:分析下載的VPN配置](#)

[步驟 2:配置鏈路BGP更新源環回介面](#)

[步驟 3:配置階段1/階段2策略對象](#)

[步驟 4:設定虛擬通道介面\(VTI\)](#)

[步驟 5:設定IPsec VPN拓撲](#)

[步驟 6:驗證VPN拓撲](#)

[步驟 7:配置ECMP](#)

[步驟 8:設定BGP](#)

[步驟 9:設定eBGP多重路徑](#)

[驗證/疑難排解](#)

---

## 簡介

本文檔介紹如何使用雙WAN連結配置到安全防火牆的Microsoft Azure虛擬WAN(vWAN)站點到站點VPN連線。

## 必要條件

### 需求

思科建議瞭解以下主題：

- Microsoft Azure 虛擬WAN(vWAN)
- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)

確保這些元件最初都在Azure環境中配置：

- Microsoft Azure vWAN例項
- Microsoft Azure vWAN中心

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全FTD版本10.0
- Cisco安全FMC版本10.0
- Microsoft Azure vWAN

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。

## 背景資訊

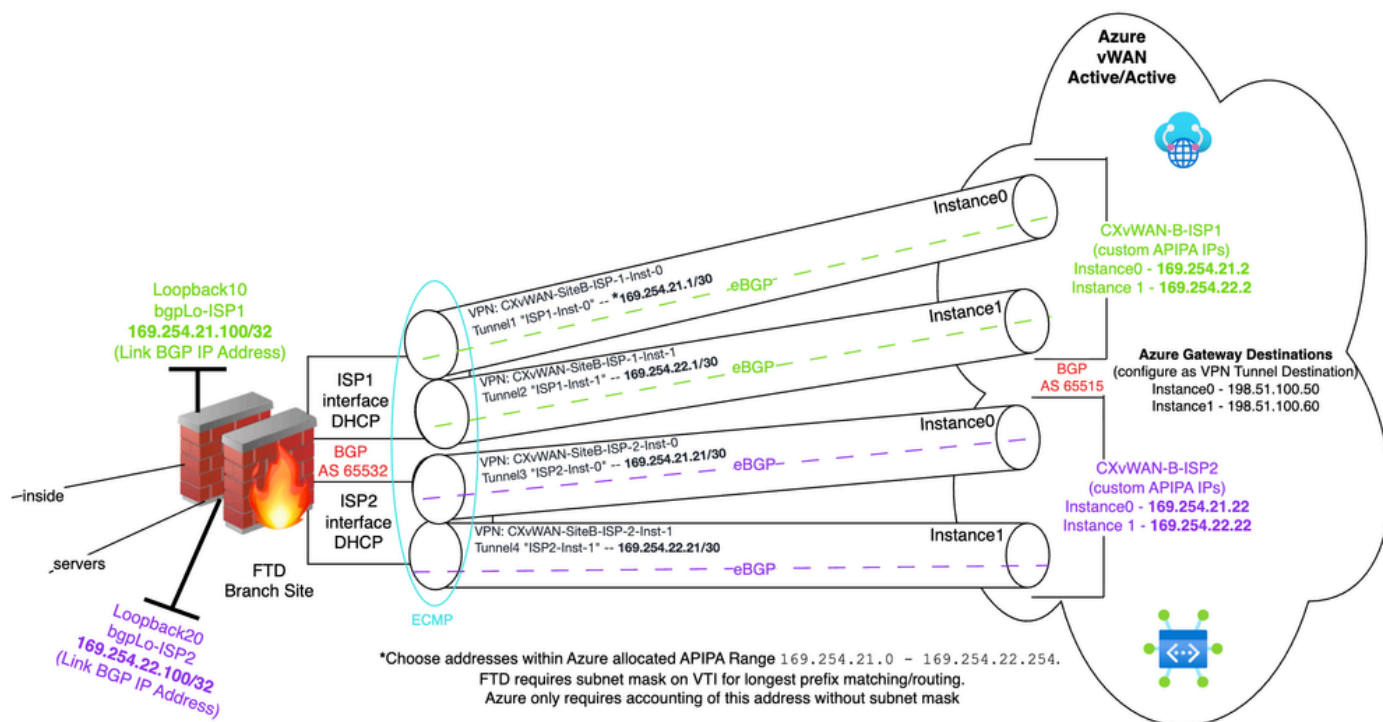
當分支FTD有兩個面向Internet服務提供商(ISP)的外部介面時，每個介面都可以冗餘主動連線到Azure vWAN，因此每個ISP鏈路都得到了利用。Azure vWAN為每個站點連結建立兩個IPsec隧道（一個到Azure Hub Instance0，一個到Instance1），因此每個ISP介面終止兩個隧道。透過兩條ISP連結，這會導致四條IPsec通道在FTD上終止。

Azure例項在Active/Active模式下運行以實現負載平衡和冗餘，因此FTD通過跨所有四個IPsec隧道的等價多路徑(ECMP)配置反映這一點。使用自定義自動私有IP定址(APIPA)地址，在四個通道中的每一個上建立具有不同專用自治系統編號(ASN)的外部邊界網關協定(eBGP)鄰居關係。這將啟用BGP多重路徑功能，為每個Azure Hub Site Link例項對提供多個冗餘路徑。

## 圖表

該圖顯示了本文所述的配置拓撲。雙重直接網際網路存取(DIA)連結變體從FTD上的兩個外部介面來源兩個Azure通道。

## 雙直接網際網路接入(DIA)鏈路 ( Azure + FTD負載平衡/冗餘 )



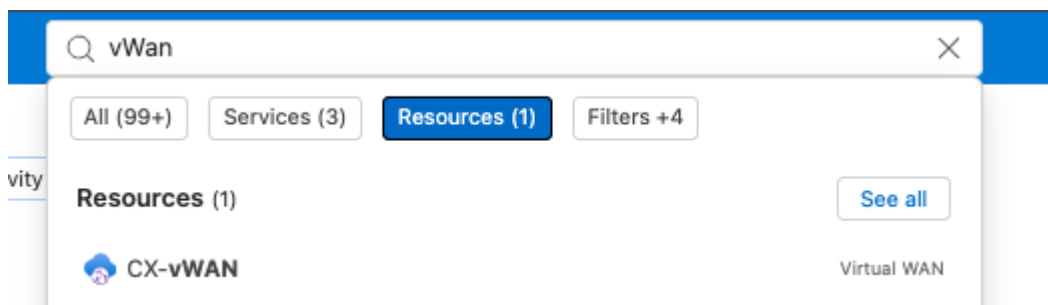
雙直接Internet接入連線拓撲

## 設定

### 第1階段：Azure vWAN VPN站點配置

#### 步驟 1:建立Azure vWAN VPN站點 ( 遠端FTD裝置 )

1)在Azure搜尋欄位中搜尋vWAN，按一下Virtual WAN以進入現有的Azure vWAN Hub。接下來，導航到連線>中心，然後按一下現有的Azure vWAN中心。



虛擬WAN搜尋查詢

Microsoft Azure

Home > CX-vWAN

## CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Search for hubs by n... Clear all filters

Add filter

| Hub         | Hub status |
|-------------|------------|
| CX-vWAN-Hub | Succeeded  |

選擇現有的虛擬WAN中心

2)按一下Connectivity > VPN(Site to site) , 然後按一下+ Create new VPN site

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

### CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ⓘ

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

| Site name  | Location | Cloud |
|------------|----------|-------|
| No results |          |       |

建立新的虛擬WAN站點



附註：覆蓋影像中各個欄位中的值的空白用於發佈此文檔。

3)在必填欄位中輸入值。完成後，按一下下一步：連結>以向前移動。

## Create VPN site ...

Basics Links Review + create

### Project details

Subscription

Resource group \*

### Instance details

Region \*

Name \*

Device vendor \*

Private address space

At least one address space is required if BGP isn't configured. To configure BGP, please go to Links tab.

 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Links >

常規VPN站點配置設定

4)輸入所需的連結資訊。鏈路BGP地址和鏈路ASN是內部隧道BGP第3層目標地址和在通過站點到站點隧道形成鄰居的分支端上的BGP AS編號。鏈路BGP地址是已配置的中心專用地址空間子網外部的非重疊子網地址(/32),Azure將該子網安裝為作為BGP鄰居到達的/32路由。在FTD的稍後部分中建立了兩個回送介面，以代表每個雙站台連結的連結BGP位址。連結IP地址/完全限定域名(FQDN)是流向分支站點的流量的外部標頭第3層目標IP地址，該地址是設定IP安全(IPsec)/Internet金鑰交換版本2(IKEv2)連線所必需的。按一下「下一步：審閱+建立>」。



附註：如果正在使用範圍從169.254.21.0到169.254.22.255的隧道地址，請確保檢視特定的Azure文檔：[選擇BGP APIPA地址。](#)

# Create VPN site ...

Basics Links Review + create

Link Details ⓘ

| Link name  | Link speed | Link provider name | Link IP address / FQDN | Link BGP address | Link ASN |     |
|------------|------------|--------------------|------------------------|------------------|----------|-----|
| ISP-1-Link | 1000       | ISP1               |                        | 169.254.21.100   | 65532    | ... |
| ISP-2-Link | 1000       | ISP2               |                        | 169.254.22.100   | 65532    | ... |

**i** You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous    Next : Review + create >

配置站點連結引數

5)確認資訊符合預期後，按一下Create。

# Create VPN site ...

 Validation passed

- basics
- links
- Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

## Basics

|                       |               |
|-----------------------|---------------|
| Region                | East US       |
| Name                  | Dual-ISP-Site |
| Device vendor         | Cisco         |
| Private address space |               |

Links

|                        |                |
|------------------------|----------------|
| Link name              | ISP-1-Link     |
| Link provider name     | ISP1           |
| Link speed             | 1000           |
| Link IP address / FQDN |                |
| Link ASN               | 65532          |
| Link BGP address       | 169.254.21.100 |

|                        |                |
|------------------------|----------------|
| Link name              | ISP-2-Link     |
| Link provider name     | ISP2           |
| Link speed             | 1000           |
| Link IP address / FQDN |                |
| Link ASN               | 65532          |
| Link BGP address       | 169.254.22.100 |

 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

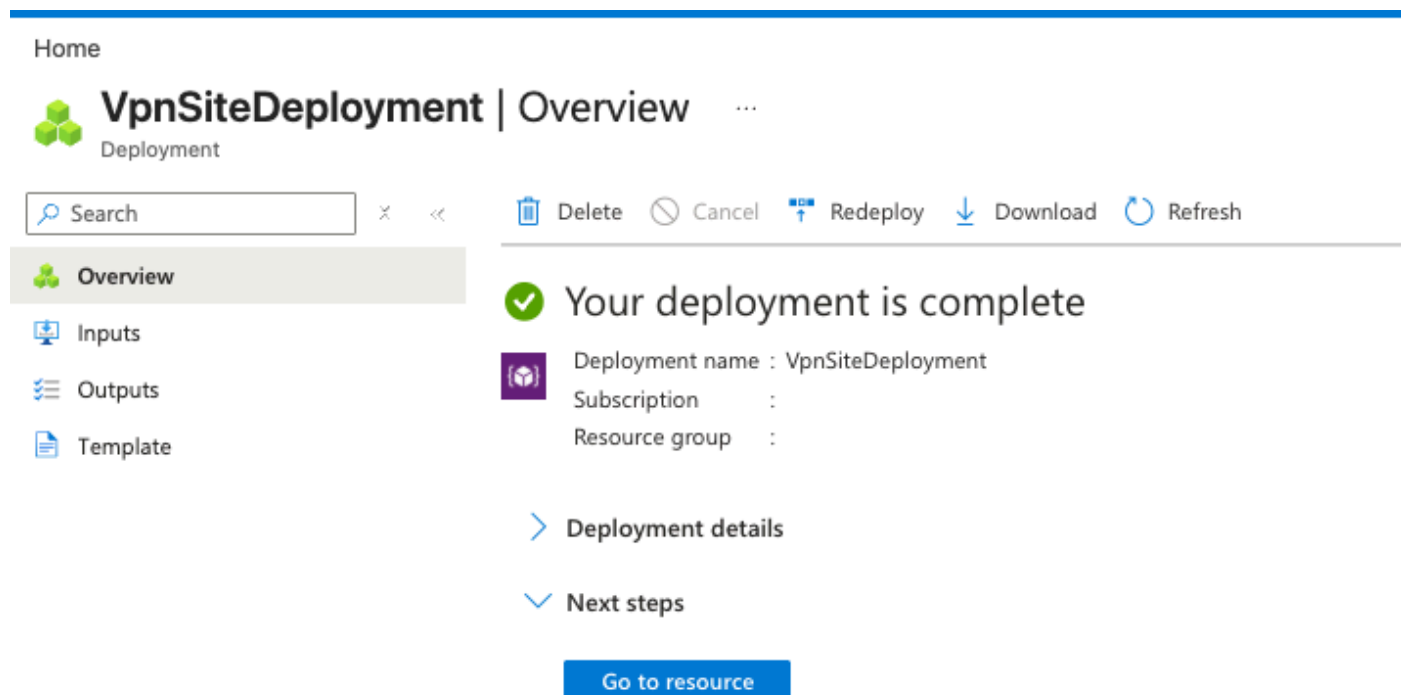
Create

Previous

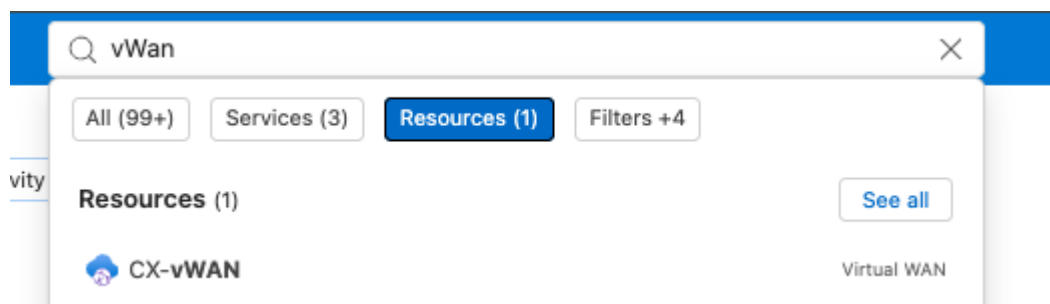
Next

檢視和建立新的VPN站點

6)完成VPN站點的部署後，導航回vWAN Hub配置。



虛擬WAN站點部署進度



虛擬WAN搜尋查詢

## 步驟 2:配置Azure APIPA網關引數

Azure需要對169.254.0.0/16 IPv4地址空間內的自動私有IP定址(APIPA)地址進行額外配置。

1)通過Connectivity > Hub進入現有中心。

Microsoft Azure

Home > CX-vWAN

## CX-vWAN | Hubs

Virtual WAN

Search [ ] < << + New Hub Refresh

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Resource visualizer  
Settings  
Configuration  
Properties  
Locks  
Connectivity  
**Hubs**

Search for hubs by n... Clear all filters

+ Add filter

| Hub         | Hub status |
|-------------|------------|
| CX-vWAN-Hub | Succeeded  |

導航到虛擬WAN中心連線

2)再次導航到Connectivity > VPN(Site to site)，然後點選Gateway Configuration超鏈接。

## CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search [ ] × < << Download VPN Config Packet Capture Delete gateway Rese

Overview  
Connectivity  
**VPN (Site to site)**  
ExpressRoute  
User VPN (Point to site)  
Routing  
Connection Policies  
Route Map

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** × + Add filter

VPN Sites ⓘ

Access Gateway Configuration超連結

3)側面板顯示編輯VPN網關。在VPN網關例項0和VPN網關例項1下，輸入兩個唯一的自定義BGP IP地址，這兩個地址充當通過IPsec隧道的BGP鄰居的每個例項的鄰居IP。如果您選擇在此拓撲中使用APIPA編址，這是必要的。在標有Peer Address 的欄位中，輸入BGP鄰居IP，以使用從FTD到達Azure例項。如果正在使用APIPA定址，Azure不會嘗試使用FTD建立BGP，因此FTD會嘗試使用Azure在每個隧道上建立eBGP鄰居。

總共有2個連結x2個隱含通道；每個ISP鏈路上一條通往Instance0和Instance1的隧道；總計有四個IPsec隧道，在Azure和兩個FTD ISP介面之間具有BGP鄰居關係。

這些地址必須是唯一的，在本演示中，分配給每個隧道的/30子網中的第二個和最後一個主機地址將在FTD上配置以供使用。配置後，按一下Edit。



附註：如果正在使用範圍從169.254.21.0到169.254.22.255的隧道地址，請確保檢視特定的Azure文檔：[選擇BGP APIPA地址](#)

---

## Edit VPN Gateway



A Site to site (VPN gateway) enables you to connect VPN sites to a hub.

AS Number ⓘ

65515



Gateway scale units \* ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ

☒ Microsoft network ☐ Internet

### VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

### VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



Updating a hub can take 30 minutes or more. [Learn more.](#)

Edit

Cancel

編輯VPN網關自定義BGP IP地址



附註：正如Azure所指出，更新此操作可能需要30分鐘或更長時間。

### 步驟 3: 配置Azure vWAN Site VPN引數

1) 在Azure vWAN Hub配置的Connectivity > VPN ( 站點到站點 ) 頁面上，按一下X以清除Hub關聯：連線過濾以檢視斷開的VPN站點。

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > CX-vWAN | Hubs > CX-vWAN-Hub. The main heading is 'CX-vWAN-Hub | VPN (Site to site)'. Below this, there's a search bar and a set of action buttons: 'Download VPN Config', 'Packet Capture', 'Delete gateway', 'Reset gateway', and 'Monitor Gateway'. The left sidebar contains a navigation menu with 'Overview', 'Connectivity', 'ExpressRoute', 'User VPN (Point to site)', 'Routing', 'Security', 'Third party providers', and 'Monitor'. The 'Connectivity' section is expanded, and 'VPN (Site to site)' is selected. The main content area shows the 'VPN Sites' tab. It includes a search bar labeled 'Search this page' and a 'Clear all filters' link. Below the search bar, there's a filter bar with the text 'Hub association : Connected' and a red 'X' icon next to it. A red arrow points to this 'X' icon. There's also an 'Add filter' button. At the bottom, there's a message box that says: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

清除集線器關聯連線過濾器

2) 選中最近調配的VPN站點旁邊的覈取方塊，然後點選連線VPN站點。

 Search

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

**VPN Sites** Metrics

 Search this page

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



Check active filters when searching for a VPN site. VPN connectivity status might take a few mi

+ Create new VPN site

 **Connect VPN sites**

 Disconnect VPN sites

 Refresh

Page: 1 ▼

Site name

↑↓ Location

☒  **Dual-ISP-Site**

連線VPN站點操作

3)配置所需的預共用金鑰(PSK),並通過按一下Custom切換選項配置所需的IPsec引數。在後續步驟中, FMC/FTD配置上的這些IPSec引數必須匹配。要儲存,請按一下連線。



附註: FTD/FMC 6.7版已移除Diffie-Hellman(DH)群組24支援。

# Connect sites

Virtual HUB



## Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

**i** When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

SA Lifetime in seconds \* ⓘ

27000

IKE Phase 1 ⓘ

Encryption \*

GCMAES256

Integrity/PRF \*

SHA384

DH Group \*

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption \*

GCMAES256

IPsec Integrity \*

GCMAES256

PFS Group \*

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

These sites will be connected to the [CX-vWAN-Hub] hub.

| Site name                                                                                         | ↑↓ | Region | ↑↓ |
|---------------------------------------------------------------------------------------------------|----|--------|----|
|  Dual-ISP-Site |    | eastus |    |

Connect

配置預共用金鑰和IPsec引數

4)確認VPN站點設定已成功完成。

# Notifications



[More events in the activity log →](#)

[Dismiss all](#)



## Successfully created VPN connection



Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

確認VPN站點調配狀態

步驟 4:在VPN站點連結例項上啟用和啟用自定義BGP APIPA

1)刷新「VPN ( 站點到站點 )」頁，並確認「Connection Provision status」列指示其成功，這允許您按一下省略號，並允許您按一下Edit VPN connection to this hub下拉選單項。

+ Create new VPN site   Connect VPN sites   Disconnect VPN sites   Refresh

Page: 1

| Site name     | Location | Cloud provider | Connection Provisioning status | Connectivity status |  |
|---------------|----------|----------------|--------------------------------|---------------------|--|
| Dual-ISP-Site | eastus   |                | Succeeded                      | Not connected       |  |

驗證連線成功並編輯VPN連線

2)按一下以配置Link Connection 1(ISP1)並再次輸入適用的Pre-Shared Key(PSK)，確保您按一下Custom BGP IP Address旁邊的Enable切換按鈕，並對映將成為FTD生成的BGP IP報頭的內部隧道目標IP地址欄位值的/30子網的剩餘主機地址。

實質上，ISP1 VTI Tunnel1到Azure Instance0的地址分配為169.254.21.1/30，在FTD上終止的第二個ISP1 VTI Tunnel2為例項1分配了IP為169.254.22.1/30。

按一下「Next:Link Connection 2>繼續ISP 2鏈路引數。



---

附註：您可能需要重新輸入您的PSK，並重新按一下Azure下拉選單中的對齊PFS組選項。

---

# Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

.....

Connection Mode ⓘ

Default Initiator Only Responder Only

Border gateway protocol ⓘ

Disable Enable

Custom BGP IP Addresses ⓘ

Disable Enable

## Custom BGP IP Address

Instance 0 ⓘ

169.254.21.2

Instance 1 ⓘ

169.254.22.2

Use Azure Private IP Address ⓘ

Yes No

Protocol

IKEv2 IKEv1

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ

Enable Disable

IPsec ⓘ

Default Custom

SA Lifetime in seconds \* ⓘ

27000

IKE Phase 1 ⓘ

Encryption \*

GCMAES256

Integrity/PRF \*

SHA384

DH Group \*

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption \*

GCMAES256

IPsec Integrity \*

GCMAES256

PFS Group \*

NONE

DPD timeout in seconds \* ⓘ

45

Review + create

Previous

Next : Link connection 2 >

配置一個自定義BGP設定的鏈路連線

3)重複前面的步驟，並應用Link Connection 2(ISP2 link)下的適用引數。完成後，按一下Create。

# Edit VPN connection

Basics   Link connection 1   Link connection 2

Link name: ISP-2-Link

Link connection   **Enable**   Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ  

Connection Mode ⓘ   **Default**   Initiator Only   Responder Only

Border gateway protocol ⓘ   Disable   **Enable**

Custom BGP IP Addresses ⓘ   Disable   **Enable**

## Custom BGP IP Address

Instance 0 ⓘ    ▼

Instance 1 ⓘ    ▼

Use Azure Private IP Address ⓘ   Yes   **No**

Protocol   IKEv2   **IKEv1**

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ   Enable   **Disable**

IPsec ⓘ   Default   **Custom**

SA Lifetime in seconds \* ⓘ  

IKE Phase 1 ⓘ   Encryption \*   Integrity/PRF \*   DH Group \*

|             |          |             |
|-------------|----------|-------------|
| GCMAES256 ▼ | SHA384 ▼ | DHGroup14 ▼ |
|-------------|----------|-------------|

IKE Phase 2(ipsec) ⓘ   IPsec Encryption \*   IPsec Integrity \*   PFS Group \*

|             |             |        |
|-------------|-------------|--------|
| GCMAES256 ▼ | GCMAES256 ▼ | NONE ▼ |
|-------------|-------------|--------|

DPD timeout in seconds \* ⓘ  

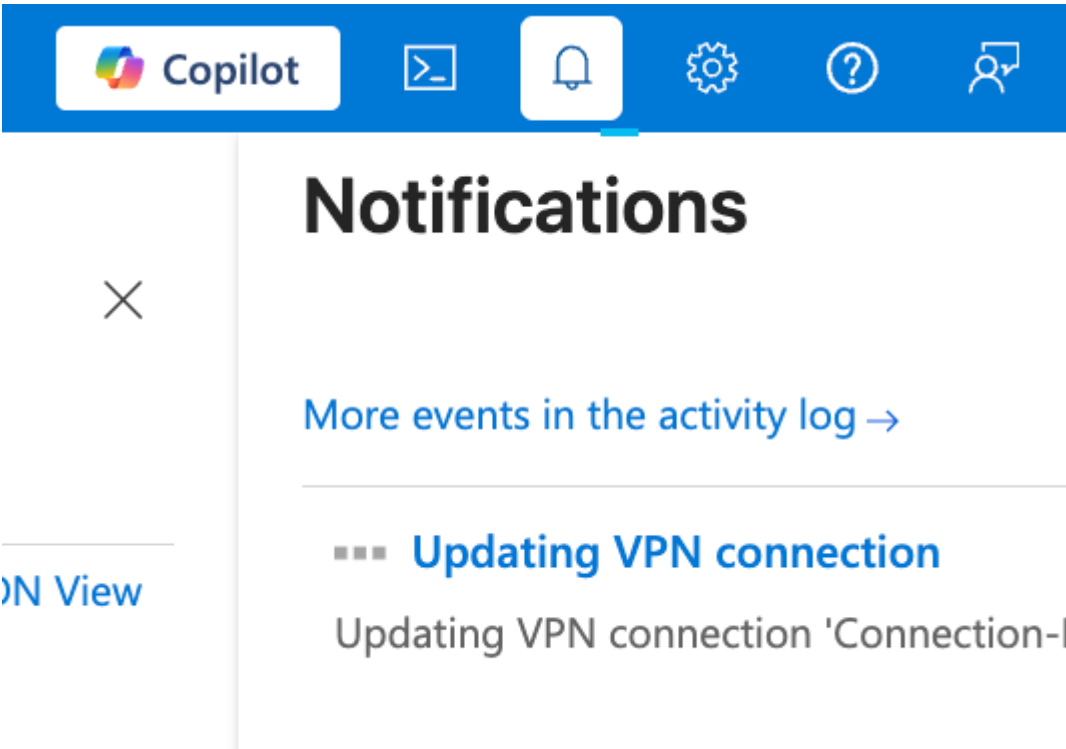
**Create**

Previous

Next

配置鏈路連線兩個自定義BGP設定

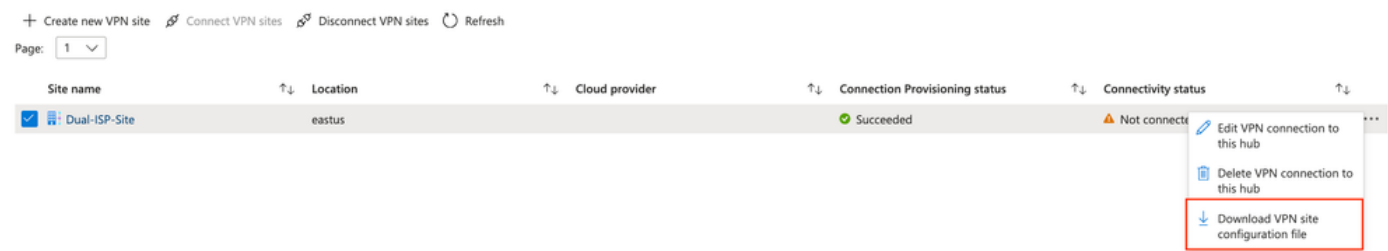
4)Azure UI中的通知顯示更新任務開始。



Azure更新任務開始通知

步驟 5:下載VPN站點配置檔案

1)在Azure中的同一VPN（站點到站點）頁面中，選擇已配置VPN站點最右邊的省略號圖示，然後選擇下載VPN站點配置檔案選項。



下載VPN站點配置檔案選項

2)按一下Click here to download hyperlink。



## Download Site-to-Site VP...



Dual-ISP-Site



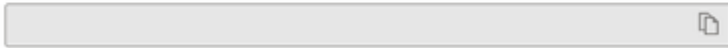
Create new



Use existing



The file is ready to download



[Click here to download](#)



下載VPN站點配置檔案

## 第2階段：配置FTD以實現到Azure vWAN的雙ISP連線

### 步驟 1:分析下載的VPN配置

1)開啟下載的配置檔案，將顯示類似的JavaScript Object Notation(JSON)輸出。輸出將顯示寫入檔案中的兩個對象之一。此資訊為FTD設定提供有用背景。



附註：為了增強焦點，為了簡潔起見，會修剪若干無關對象和鍵/值對。



附註：下載檔案中的ISP-Link-1 JSON對象順序顛倒。代碼輸出中的省略號表示ISP-2-Link對象及其適用的配置。

```
...
{
  "configurationVersion": {
    "LastUpdatedTime": "2026-09-25T20:20:26.7658453Z",
    "Version": "15221e61-4e2c-42f5-b9e4-96d674f5a9a3"
  },
  "vpnSiteConfiguration": {
    "Name": "Dual-ISP-Site",
    "IPAddress": "FTD_ISP1_WAN_IP",
    "BgpSetting": {
      "Asn": 65532,
      "BgpPeeringAddress": "169.254.21.100",
      "PeerWeight": 32768
    }
  }
}
```

```

    },
    "LinkName": "ISP-1-Link"
  },
  "vpnSiteConnections": [
    {
      "gatewayConfiguration": {
        "IpAddresses": {
          "Instance0": "Inst0IP",
          "Instance1": "Inst1IP"
        },
        "BgpSetting": {
          "Asn": 65515,
          "CustomBgpPeeringAddresses": {
            "Instance0": [
              "169.254.21.22",
              "169.254.21.2"
            ],
            "Instance1": [
              "169.254.22.22",
              "169.254.22.2"
            ]
          }
        },
        "connectionConfiguration": {
          "IsBgpEnabled": true,
          "PSK": "PSK",
          "IPsecParameters": {
            "IpsecEncryption": "GCMAES256",
            "IpsecIntegrity": "GCMAES256",
            "IkeEncryption": "GCMAES256",
            "IkeIntegrity": "SHA384",
            "PfsGroup": "None",
            "DhGroup": "DHGroup14",
            "SALifeTimeInSeconds": 27000
          }
        }
      }
    }
  ]
}
]

```

完成這些步驟時，保留此輸出作為參考。

## 步驟 2: 配置鏈路BGP更新源環回介面

FTD BGP流程下的BGP鄰居組態專案（在FTD的後續步驟中設定）需要代表Azure站點連結設定中對應連結BGP IP位址的穩定來源。

1) 導航到Devices > Device Management。

**Cloud-delivered Firewall Management Center**  
Devices / Device Management

**Devices**

- Device Management ✓ Upgrade
- Template Management Threat Defense Upgrade
- Platform Settings Chassis Upgrade
- FlexConfig
- Certificates

— Show less

**Monitor**

- Insights & Reports >
- Events & Logs >
- Insights & Reports >

**Manage**

- Policies >
- Objects
- Devices**

導航到Firepower管理中心上的裝置管理



附註：本實驗使用雲交付的防火牆管理中心(cdFMC);但是，內部現場故障修復管理模組的步驟保持不變。

2)點選要配置為具有雙ISP連線的分支/站點VPN裝置的FTD。

|                          |                                                                         |        |
|--------------------------|-------------------------------------------------------------------------|--------|
| N/A - ROUTED             |                                                                         |        |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> <b>CXvWAN-FTD-2</b><br>N/A - ROUTED | 10.0.0 |

選擇用於配置部署的FTD

3)按一下Add Interfaces下拉選單，然後按一下Loopback Interface。

**CXvWAN-FTD-2** Save Cancel

Cisco Secure Firewall Threat Defense for AWS

Device **Interfaces** Inline Sets Routing DHCP VTEP

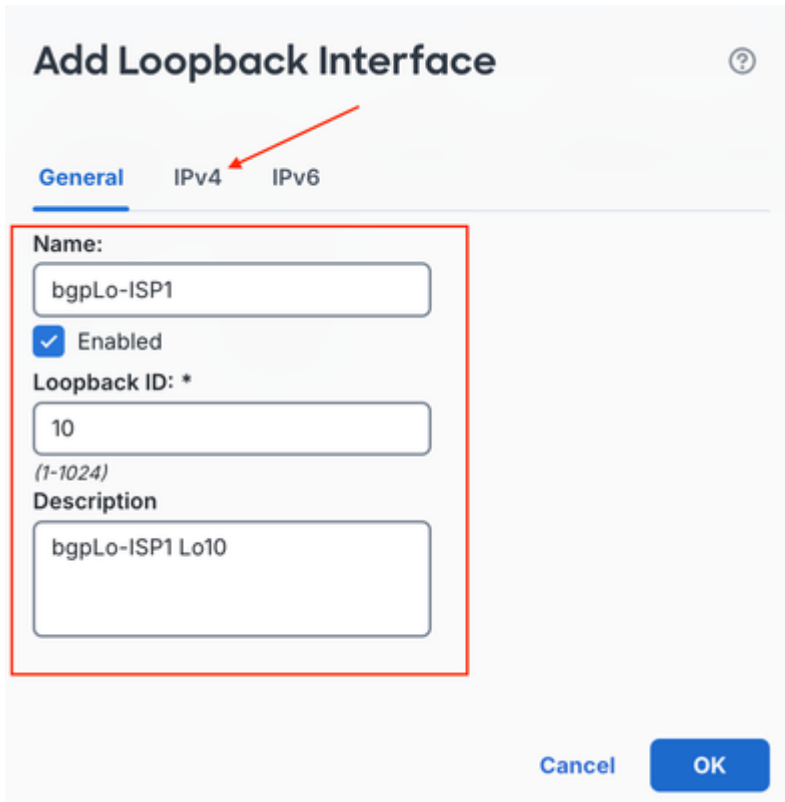
Interfaces Virtual Tunnels  Sync Interface Add Interfaces ▾

| Interface     | Logical Name | Type     | Security Zones | MAC Address (Active/St... | IP Address | Path Mon... | Vir |
|---------------|--------------|----------|----------------|---------------------------|------------|-------------|-----|
| Management0/0 | management   | Physical |                |                           |            | Disabled    | Glo |
| Ethernet0/0   | ISP1         | Physical |                |                           |            | Disabled    | Glo |
| Ethernet0/1   | ISP2         | Physical |                |                           |            | Disabled    | Glo |

- Sub Interface
- Redundant Interface
- Bridge Group Interface
- Virtual Tunnel Interface
- Loopback Interface**
- VNI Interface

向裝置新增環回介面

4)輸入環回介面的名稱，確保選中Enabled釐取方塊，然後輸入Loopback ID。如果需要，請輸入Description。完成後，按一下IPv4 頁籤。



**Add Loopback Interface** ⓘ

**General** IPv4 IPv6

Name:  
bgpLo-ISP1

☒ Enabled

Loopback ID: \*  
10  
(1-1024)

Description  
bgpLo-ISP1 Lo10

Cancel OK

配置環回介面資訊和IPv4地址

5)輸入環回IP地址，該地址是先前步驟中為Azure中的ISP1站點連結配置的鏈路BGP IP地址。此IP用作ISP1上FTD和Azure例項之間配置的鄰居關係上的BGP更新源。



附註：您可以引用之前在ISP1的vpnSiteConfiguration.BgpSetting.BgpPeeringAddress下下載的VPN配置JSON中定義的值

## Add Loopback Interface ?

General **IPv4** IPv6

IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

輸入環回IPv4地址並按Ok

6)在此序列中為ISP2 BGP環回配置重複子步驟c-e。

|            |            |          |                            |          |        |  |
|------------|------------|----------|----------------------------|----------|--------|--|
| Loopback10 | bgpLo-ISP1 | Loopb... | 169.254.21.100/32(Static); | Disabled | Global |  |
| Loopback20 | bgpLo-ISP2 | Loopb... | 169.254.22.100/32(Static); | Disabled | Global |  |

建立第一個和第二個環回介面

7)儲存組態。

**You have unsaved changes**

儲存更改

步驟 3:配置階段1/階段2策略對象

1)要在FMC和FTD VPN拓撲上配置匹配的IKEv2/IPsec配置，請導航至Manage > Objects，在導航選單中滾動至VPN，然後展開子選單。通過在選單中選擇IKEv2 Policy並按一下Add IKEv2 Policy來配置IKEv2第1階段策略。

**IKEv2 Policy**

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

[Add IKEv2 Policy](#)

| Name                                             |                                           |
|--------------------------------------------------|-------------------------------------------|
| <a href="#">AES-GCM-NUL-<b>SHA</b></a>           | <input type="text"/> <input type="text"/> |
| <a href="#">AES-GCM-NUL-<b>SHA-LATEST</b></a>    | <input type="text"/> <input type="text"/> |
| <a href="#">AES-<b>SHA</b>-<b>SHA</b></a>        | <input type="text"/> <input type="text"/> |
| <a href="#">AES-<b>SHA</b>-<b>SHA-LATEST</b></a> | <input type="text"/> <input type="text"/> |
| <a href="#">DES-<b>SHA</b>-<b>SHA</b></a>        | <input type="text"/> <input type="text"/> |
| <a href="#">DES-<b>SHA</b>-<b>SHA-LATEST</b></a> | <input type="text"/> <input type="text"/> |
| <a href="#">Umbrella-AES-GCM-256</a>             | <input type="text"/> <input type="text"/> |

Displaying 1 - 7 of 7 rows | < < Page 1 of 1 >

建立新的IKEv2策略對象

2)為新的IKEv2策略輸入名稱，選擇Priority和/或Lifetime。確保通道兩端的策略與完整性、加密、偽隨機函式(PRF)和DH組相匹配。選擇要與Azure配置匹配的演算法/組元素，然後按一下Add。



附註：您可以在vpnSiteConnections[0].connectionConfiguration.IPsecParameters下載的配置檔案中引用這些精確值

**New IKEv2 Policy**

Name:\*

Description:

Priority:\*

Lifetime:  seconds (120-2147483647)

Available Algorithms

|                       |        |                                    |                             |
|-----------------------|--------|------------------------------------|-----------------------------|
| Integrity Algorithms  | MD5    | <input type="button" value="Add"/> | Selected Algorithms         |
| Encryption Algorithms | SHA    |                                    | SHA256 <input type="text"/> |
| PRF Algorithms        | SHA512 |                                    |                             |
| Diffie-Hellman Group  | SHA256 |                                    |                             |
|                       | SHA384 |                                    |                             |
|                       | NULL   |                                    |                             |

建立IKEv2策略

3)配置完成後，按一下Save(儲存)。

**Edit IKEv2 Policy**

Name:\*  
Azure\_IKEv2

Description:

Priority:\* (1-65535)  
5

Lifetime: seconds (120-2147483647)  
3600

Available Groups

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

1  
2  
5  
14  
15  
16  
19  
20

Add

Selected Groups

14

Cancel Save

儲存IKEv2策略

4)在IKEv2 IPsec Proposal子選單中配置Phase 2/IPsec引數，然後按一下Add IKEv2 IPsec Proposal。

**IKEv2 IPsec Proposal**

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can configure the Phase 2 algorithms. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Name

- AES-GCM
- AES-SHA
- DES\_SHA-1
- Umbrella-AES-GCM-256

Add IKEv2 IPsec Proposal

Policy List  
Port  
> Prefix List  
Route Map  
> Security Intelligence  
Sinkhole  
SLA Monitor  
Time Range  
Time Zone  
Tunnel Zone  
URL  
Variable  
Variable Set  
VLAN Tag  
VPN  
Certificate Map  
Custom Attribute  
Group Policy  
IKEv1 IPsec Proposal  
IKEv1 Policy  
IKEv2 IPsec Proposal

建立IKEv2 IPsec方案

5)命名IKEv2 IPsec建議並確保相同的設定保持一致。完成後，按一下「Save」。

## Edit IKEv2 IPsec Proposal

Name:\*  
Azure\_IPsec

Description:

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

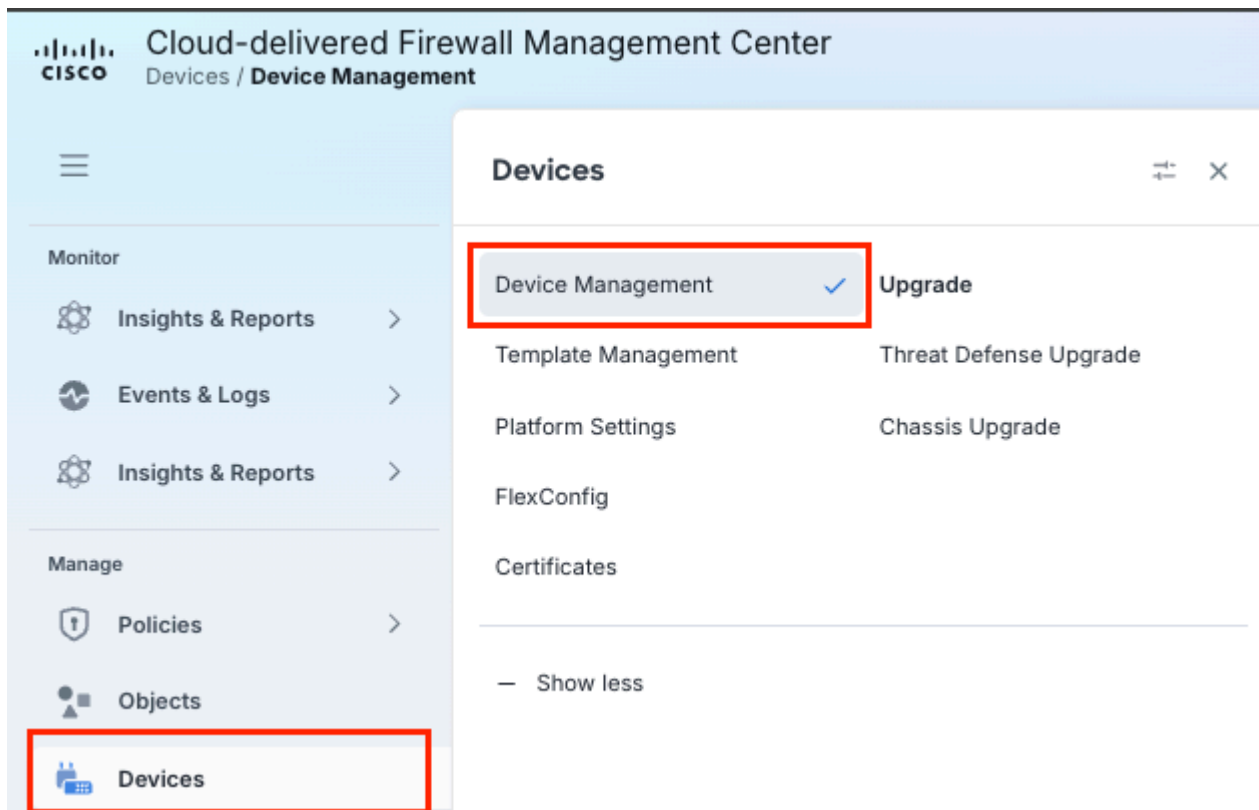
AES-GCM-256

Cancel Save

為IKEv2 IPsec建議命名，然後按一下儲存

#### 步驟 4:設定虛擬通道介面(VTI)

1)導航到Devices > Device Management。



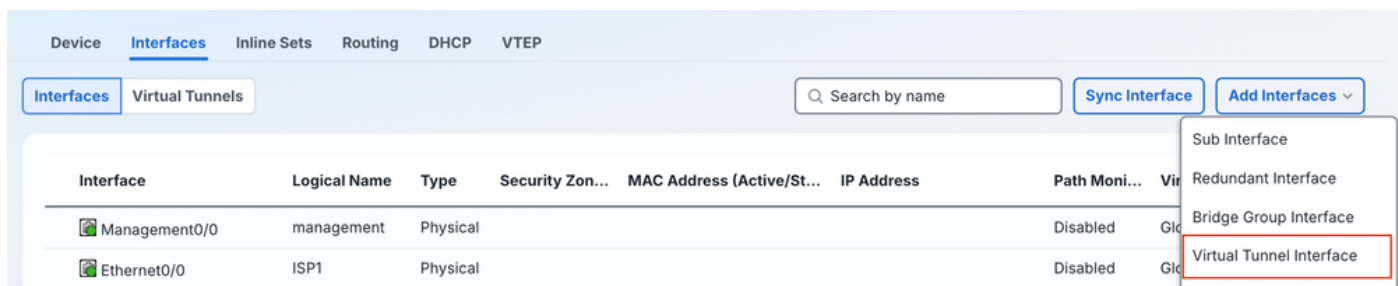
導航到Firepower管理中心上的裝置管理

2)點選要配置為具有雙ISP連線的分支/站點VPN裝置的FTD。

|                                                                                     |                                                                                                                         |  |        |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|--|--------|
| N/A - ROUTED                                                                        |                                                                                                                         |  |        |
|  |  <b>CXvWAN-FTD-2</b><br>N/A - ROUTED |  | 10.0.0 |

選擇用於配置部署的FTD

3)按一下Add Interfaces下拉選單，然後選擇Virtual Tunnel Interface(VTI)。



建立虛擬通道介面

4)輸入通道資訊。確保選中Enabled覆取方塊，輸入Name(如果需要，還應輸入Description)，並選擇可選Security Zone。調整正確的面向ISP的父介面，以在VTI下配置VTI，並為該VTI的內部隧道IPsec連線配置適當的IP地址。完成時按下OK。



提示：參考圖顯示有關使用FTD的Azure雙WAN連線的潛在VPN配置的更多上下文。

# Add Virtual Tunnel Interface



## Tunnel Type

☒ Static ☐ Dynamic

Name:\*

ISP1-Inst-0

☒ Enabled

Description:

For "CXvWAN-SiteB-ISP-1-Inst-0" VPN topology

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

## Virtual Tunnel Interface Details

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

Tunnel ID:\*

1

(0 - 10413)

Tunnel Source:\*

Ethernet0/0 (ISP1)

Dynamic

## 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

169.254.21.1/30



Cancel

OK

5)在父ISP1和ISP2介面上配置3個附加VTI。

| Interface     | Logical Name | Type     | Security Zones   | MAC Address (Active/Standby) | IP Address                 | Path Monitoring | Virtual Router |
|---------------|--------------|----------|------------------|------------------------------|----------------------------|-----------------|----------------|
| Management0/0 | management   | Physical |                  |                              |                            | Disabled        | Global         |
| Ethernet0/0   | ISP1         | Physical |                  |                              |                            | Disabled        | Global         |
| Tunnel1       | ISP1-Inst-0  | VTI      | Azure-Spoke-Zone |                              | 169.254.21.1/30(Static);   | Disabled        | Global         |
| Tunnel2       | ISP1-Inst-1  | VTI      | Azure-Spoke-Zone |                              | 169.254.22.1/30(Static);   | Disabled        | Global         |
| Ethernet0/1   | ISP2         | Physical |                  |                              |                            | Disabled        | Global         |
| Tunnel3       | ISP2-Inst-0  | VTI      | Azure-Spoke-Zone |                              | 169.254.21.21/30(Static);  | Disabled        | Global         |
| Tunnel4       | ISP2-Inst-1  | VTI      | Azure-Spoke-Zone |                              | 169.254.22.21/30(Static);  | Disabled        | Global         |
| Loopback10    | bgpLo-ISP1   | Loopback |                  |                              | 169.254.21.100/32(Static); | Disabled        | Global         |
| Loopback20    | bgpLo-ISP2   | Loopback |                  |                              | 169.254.22.100/32(Static); | Disabled        | Global         |

配置其他虛擬通道介面

f)確保按一下Save以儲存更改。

You have unsaved changes

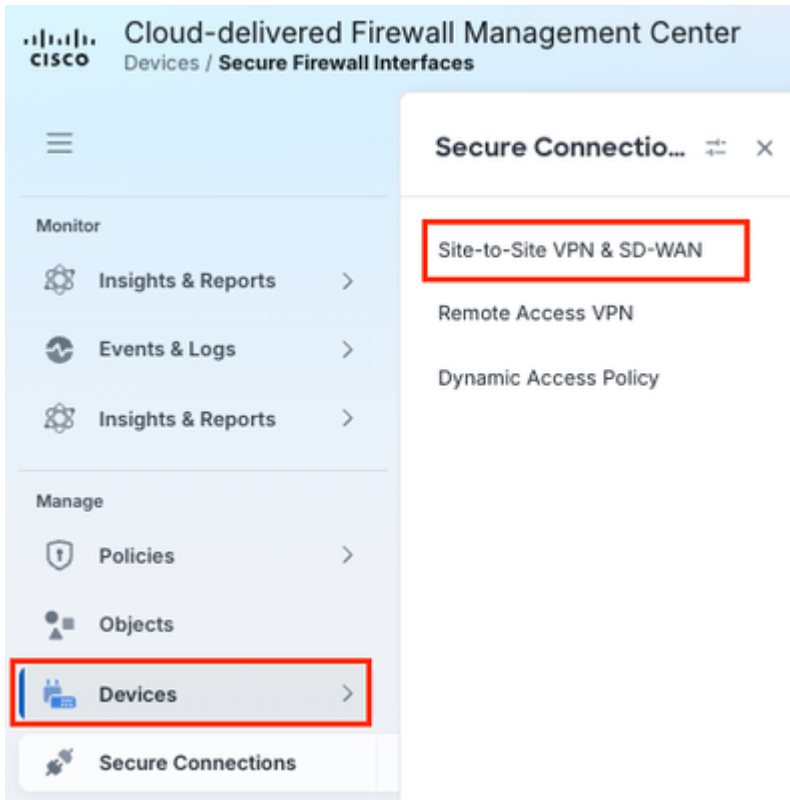
Save

Cancel

儲存更改

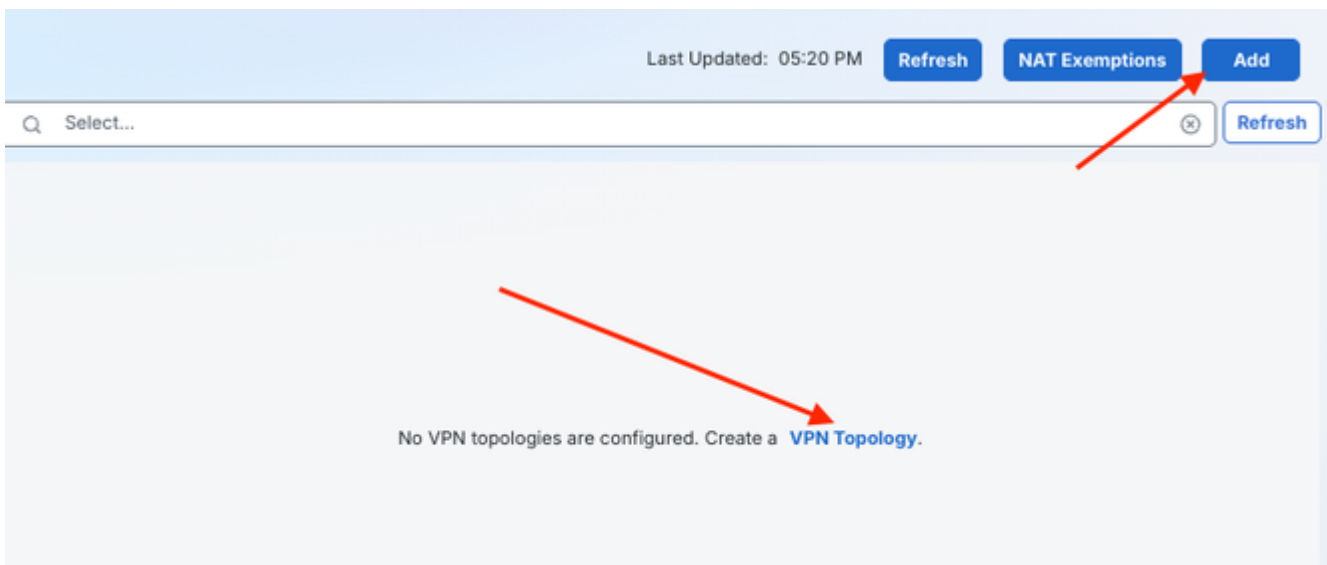
步驟 5:設定IPsec VPN拓撲

1)導航至管理>安全連線>站點到站點VPN和SD-WAN。



管理站點到站點VPN和SD-WAN連線

2)按一下初始輸出中間的初始VPN Topology配置超連結，或按一下Add按鈕。



新增新的VPN拓撲配置

3)為指向Azure例項0的ISP1的第一個隧道連結輸入拓撲名稱。按一下Route-Based VPN單選按鈕，然後按一下Peer to Peer VPN拓撲型別。完成後，按一下「Create」。

## Create VPN Topology

**Topology name \***  
CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

**SD-WAN Topology**  
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 Secure Access and Umbrella are not configured.

Prerequisites

Refresh

Cancel Create

配置基於路由的VPN拓撲型別

4) 首先，選擇Node A裝置，然後在Device下拉選單下方，該清單表示從Azure終止VPN隧道的FTD。嚮導從裝置獲取可用的VTI後，從下拉選單中選擇與正在配置的父介面和例項相匹配的VTI。從Node B Device選單中，選擇Azure端作為VPN拓撲配置中的Extranet節點。請確保為節點B配置友好名稱，並確保輸入適當的終結點IP地址。完成後，按一下IKE頁籤實施第1階段隧道配置。



附註：您可以在vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0和vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1的下載配置檔案中引用Instance Endpoint IP Address值

## Edit VPN Topology

Topology Name:\*  
CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:  
**Point to Point** Hub and Spoke Full Mesh

IKE Version:\* ☐ IKEv1 ☒ IKEv2

**Endpoints** IKE IPsec Advanced

**Node A**

**Node B**

Device:\*  
CXvWAN-FTD-2

Virtual Tunnel Interface:\*  
ISP1-Inst-0 (IP: 169.254.21.1) +

Tunnel Source IP is Dynamic (DHCP) [Edit VTI](#)

Tunnel Source IP Address:\*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Device:\*  
Extranet

Device Name\*:  
Azure-ISP1-Link-Inst0

Endpoint IP Address\*:

[Cancel](#) [Save](#)

定義節點A和節點B拓撲端點

5)在導航選單中滾動到IKEv2設定，然後按一下鉛筆圖示，將策略編輯到最近配置的IKEv2策略。接下來，從身份驗證型別下拉選單中選擇預共用手動金鑰選項，然後輸入以前在Azure中配置的PSK。完成後，按一下IPsec頁籤以配置第2階段IPsec隧道引數。



附註：您可以在下載的配置檔案中(位於 `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`)引用預共用金鑰

## Edit VPN Topology

Topology Name:\*  
CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:  
**Point to Point** Hub and Spoke Full Mesh

IKE Version:\* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

### IKEv2 Settings

Policies:\* Azure\_IKEv2

Authentication Type: Pre-shared Manual Key

Key:\* .....

Confirm Key:\* .....

☐ Enforce hex-based pre-shared key only

Cancel Save

編輯IKEv2設定和身份驗證金鑰

6)按一下IKEv2 IPsec Proposal Transform Set旁的鉛筆圖示，然後選擇以前配置的IPsec策略引數。確保更改Lifetime Duration值以匹配Azure vWAN VPN設定。確認配置資訊後，按一下Save。



附註：您可以在下載的配置檔案中在  
vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds中  
引用Lifetime值

## Edit VPN Topology

Topology Name:\*  
CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:  
**Point to Point** Hub and Spoke Full Mesh

IKE Version:\* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals\*

tunnel\_aes256\_sha

Azure\_IPsec

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group: 

▼

Lifetime Duration\*: 

27000

 Seconds (Range 120-2147483647)

Lifetime Size: 

Unlimited

 Kbytes (Range 10-2147483647)

Cancel

Save

配置IPsec建議生命週期持續時間

7)重複步驟5中的上述子步驟，建立跨ISP1例項1、ISP2例項0和ISP2例項1的其他Azure隧道。

|                             |                   |                |                    |   |  |  |
|-----------------------------|-------------------|----------------|--------------------|---|--|--|
| > CXvWAN-SiteB-ISP-1-Inst-0 | Route Based (VTI) | Point-to-Point | Deployment Pending | ✓ |  |  |
| > CXvWAN-SiteB-ISP-1-Inst-1 | Route Based (VTI) | Point-to-Point | Deployment Pending | ✓ |  |  |
| > CXvWAN-SiteB-ISP-2-Inst-0 | Route Based (VTI) | Point-to-Point | Deployment Pending | ✓ |  |  |
| > CXvWAN-SiteB-ISP-2-Inst-1 | Route Based (VTI) | Point-to-Point | 0- Tunnels         | ✓ |  |  |

建立其他站點到站點VPN拓撲

## 步驟 6:驗證VPN拓撲

進入system support diagnostic-cli，鍵入en，然後按下enter（只讀CLI）。

1)檢查IKE第1階段隧道連線。

```
`show crypto isakmp sa | i UP|READY`
```

## 2)檢查IPsec第2階段的連通性。

```
show crypto ipsec sa | i int|current_peer|pkts
```



附註：當檢視IPsec安全關聯(SA)輸出和pkts decaps和pkts decrypt計數器正在遞增，但pkts encaps和pkts encrypt未遞增時，這種情況是預期的。Azure正在嘗試通過中心專用IP空間地址形成BGP鄰居，如果鄰居終端使用APIPA BGP定址，則Azure不會啟動協商。使用自定義APIPA時，連線到Azure的裝置有責任啟動BGP協商。

---

## 3)檢查第2層連通性。

```
show arp
```

## 4)檢查IP Routing。

```
show route
```

## 5)在ISP1和ISP2介面上執行捕獲。

```
capture isp1 interface ISP1 match udp any any eq 500
capture isp1 interface ISP1 match udp any any eq 4500
capture isp1 interface ISP1 match esp any any
...
show cap
show cap isp1
show cap isp2
```

## 6)Azure驗證 — 導航到vWAN中心>連線。> VPN站點>選擇配置的站點。

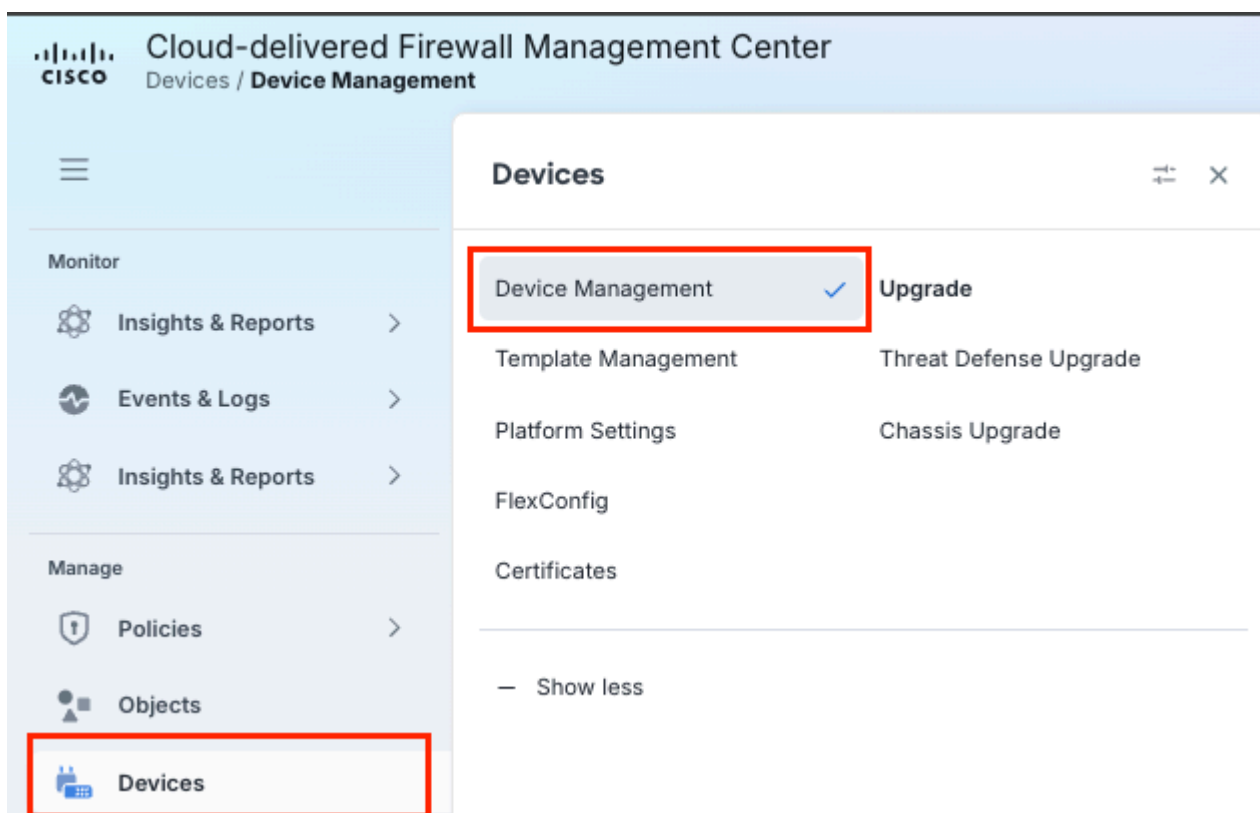
## Links

| <input type="checkbox"/> Link name  | ↑↓ Link provider name | ↑↓ Connectivity status                     | ↑↓ Hub name |
|-------------------------------------|-----------------------|--------------------------------------------|-------------|
| <input type="checkbox"/> ISP-1-Link | ISP1                  | Instance0: Connected, Instance1: Connected | CX-vWAN-Hub |
| <input type="checkbox"/> ISP-2-Link | ISP2                  | Instance0: Connected, Instance1: Connected | CX-vWAN-Hub |

Azure連結連線驗證

## 步驟 7:配置ECMP

1)導覽至Manage > Devices > Device Management，然後按一下FTD。



導航到Firepower管理中心上的裝置管理

|                          |                                                                  |        |
|--------------------------|------------------------------------------------------------------|--------|
| N/A - ROUTED             |                                                                  |        |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> CXvWAN-FTD-2<br>N/A - ROUTED | 10.0.0 |

選擇用於配置部署的FTD

2)按一下Routing頁籤，然後選擇ECMP。

Device Interfaces Inline Sets **Routing** DHCP VTEP SNMP

## Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

**Virtual Router Properties**

**ECMP**

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

等價多路徑配置設定

3)按一下Add。

### Equal-Cost Multipath Routing (ECMP)

Add

There are no ECMP zone records [Add](#)

新增等價多路徑配置設定

4)為ECMP區域命名，然後按一下可用的VTI介面，然後按一下Add按鈕將其應用到Selected Interfaces列，然後按一下OK。

# Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

為等價多路徑區域選擇介面

5)確保儲存更改。

You have unsaved changes

Save

Cancel

儲存更改

步驟 8:設定BGP

1)在FTDRouting > General Settings > BGP下啟用BGP程式。選中Enable BGP覈取方塊，然後輸入先前在第1階段第1d步中配置的AS編號。導覽至Routing > BGP > IPv4。

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

## Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

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\*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address\*

## General

Scanning Interval

Number of AS numbers in AS\_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

## Best Path Selection

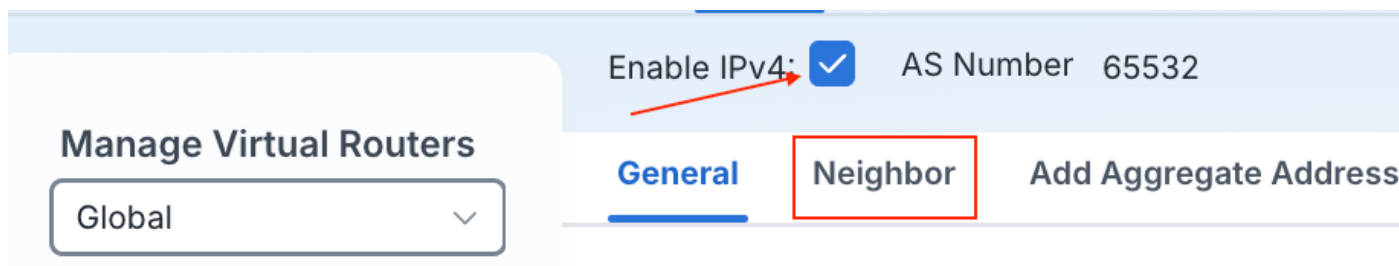
Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

在General Settings下啟用邊界網關協定進程

2)確保選中BGP進程的Enable IPv4覈取方塊，然後按一下Neighbor在Azure中配置BGP鄰居。



Manage Virtual Routers

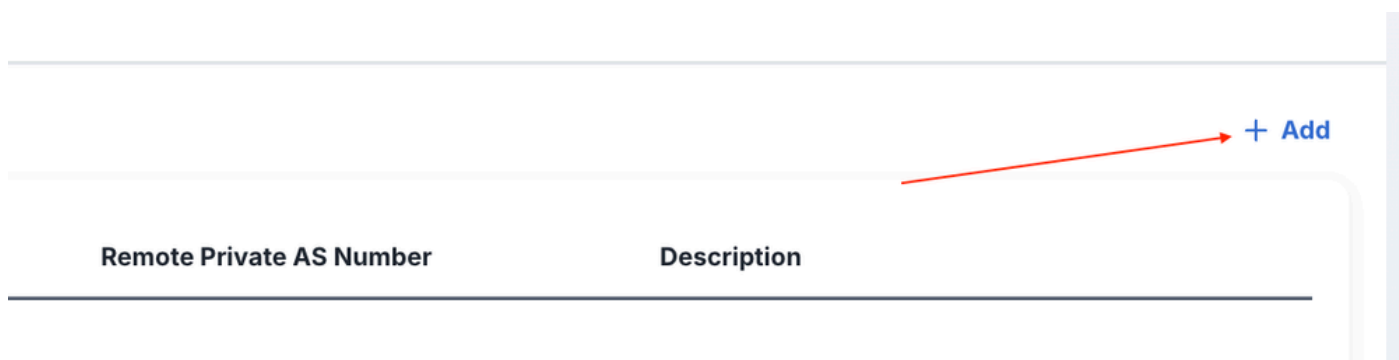
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

啟用IPv4邊界網關協定進程

3)按一下+ Add。



| Remote Private AS Number | Description |
|--------------------------|-------------|
|--------------------------|-------------|

+ Add

新增新的邊界網關協定鄰居

4)輸入ISP1 Instance0 BGP對等資訊，從vWAN集線器引用指定的BGP AS並輸入它作為Neighbor Remote AS，然後根據需要新增Description。按一下「Advanced」。



附註：請確保選擇BGP Update Source以引用對映到Azure中配置的ISP1鏈路的FTD上VTI介面的環回。

## Add Neighbor

IP Address\*

169.254.21.2

Remote AS\*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Update Source:

bgpLo-ISP1

Description

Filtering Routes

Routes

Timers

Advanced

Migration

配置邊界網關協定對等資訊

5)在FTD上設定BGP Neighbor的Advanced功能表中，可以將Time To Live(TTL)躍點數從eBGP預設的1躍點變更為可變數字。Azure BGP終結點未通過隧道直接連線到Azure基礎架構，並且終結點的躍點數往往多於預設eBGP TTL ( 1個許可證 ) 的躍點。按一下「OK」( 確定 )。

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

高級邊界網關協定鄰居設定

6)重複子步驟3-5，為ISP1例項1配置Tunnel2。

7)重複兩次子步驟3-5以配置ISP2 Instance0/Instance1 BGP對等資訊。



附註：確保選擇引用對映到Azure中配置的ISP2鏈路的FTD上VTI介面的環回的對齊BGP Update Source。

## Add Neighbor



IP Address\*

169.254.21.22

Remote AS\*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

**Advanced**

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

ISP2例項1 BGP鄰居配置

# Add Neighbor



IP Address\*

169.254.22.22

Remote AS\*

65515

(1-4294967295 or 1.0-65535.65535)

- ☒ Enabled address
- ☐ AS Override
- ☐ Shutdown administratively
- ☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

- ☐ Enable Authentication
- Enable Encryption

0
- Password
- Confirm Password
- ☐ Send Community attribute to this neighbor
- ☐ Use itself as next hop for this neighbor
- ☐ Disable Connection Verification
- ☒ Allow connections with neighbor that is not directly connected
- ☐ Limited number of TTL hops to neighbor
- TTL Hops

10

(1-255)
- ☐ Use TCP path MTU discovery
- TCP Transport Mode

Cancel

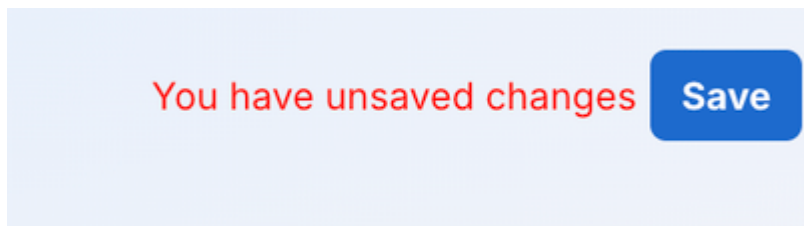
OK

ISP 2例項2 BGP鄰居配置

| Address       | Remote AS Number | Address Family | Remote Private AS Number | Description |
|---------------|------------------|----------------|--------------------------|-------------|
| 169.254.21.2  | 65515            | Enabled        |                          |             |
| 169.254.22.2  | 65515            | Enabled        |                          |             |
| 169.254.21.22 | 65515            | Enabled        |                          |             |
| 169.254.22.22 | 65515            | Enabled        |                          |             |

結束BGP鄰居結果配置

完成後，按一下「Save」。



儲存更改

預設情況下，BGP在路由表中僅安裝一條最佳路徑，即使ECMP在通往Azure的所有VTI上配置也是如此。必須分別啟用BGP多重路徑，才能同時安裝和使用獲知的路徑。

#### 步驟 9: 設定eBGP多重路徑

1) 導覽至Routing > BGP > IPv4，按一下General 索引標籤，然後按一下Forward Packets Over Multiple Paths旁的鉛筆圖示。

Enable IPv4: ☒ AS Number 65532

**Manage Virtual Routers**

Global

Virtual Router Properties

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP**
- IPv4
- IPv6
- Static Route
- Multicast Routing
  - IGMP
  - PIM
  - Multicast Routes
  - Multicast Boundary Filter

**General Settings**

BGP

**General** Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

**Setting**

Learned Route Map

**Administrative Route Distances**

|          |     |
|----------|-----|
| External | 20  |
| Internal | 200 |
| Local    | 200 |

**Routes and Synchronization**

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| Generate default routes                                                | No  |
| Summarize subnet routes into network level routes                      | No  |
| Advertise inactive routes                                              | Yes |
| Synchronize between BGP and IGP systems                                | No  |
| Redistribute IBGP into IGP                                             | No  |
| (Use filtering to limit the number of prefixes that are redistributed) |     |

**Forward Packets Over Multiple Paths**

|                      |   |
|----------------------|---|
| Number of Paths      | 1 |
| IBGP number of paths | 1 |

Forward Packets Over Multiple Paths設定

2)將「Number of Paths」欄位的預設值從1變更為4。單擊OK。

## Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

更改通過多個路徑轉發資料包設定

3)確保Save並部署更改。

## 驗證/疑難排解

部署完成後，請確認FTD BGP進程在各自的隧道上與兩個Azure例項建立鄰居鄰接關係，並確認路由已獲知、介面已啟動，並且協定連線已返回連線表中。

導覽至system support diagnostic-cliFTD CLI，如同第2階段第7步所述。

1)部署後，BGP鄰居應啟動並接收字首。

<#root>

>

**system support diagnostic-cli**

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.

ftd#

ftd#

ftd#

**show bgp summary**

BGP router identifier 169.254.22.100, local AS number 65532  
BGP table version is 29, main routing table version 29  
2 network entries using 400 bytes of memory  
8 path entries using 640 bytes of memory

```

2 multipath network entries and 8 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH 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 1272 total bytes of memory
BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

```

```

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.21.2 4 65515 20 17 29 0 0 00:13:14 2
169.254.22.2 4 65515 20 20 29 0 0 00:13:22 2
169.254.21.22 4 65515 19 21 29 0 0 00:13:19 2
169.254.22.22 4 65515 20 19 29 0 0 00:13:17 2
ftd#

```

2)檢查從Azure接收的路由是否顯示為多路徑路由。

```
<#root>
```

```
ftd#
```

```
show bgp
```

```

BGP table version is 29, local router ID is 169.254.22.100
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    |
|----------------|---------------|--------|--------|--------|---------|
| *m 10.2.0.0/16 | 169.254.21.2  |        |        | 0      | 65515 i |
| *m             | 169.254.22.22 |        |        | 0      | 65515 i |
| *m             | 169.254.21.22 |        |        | 0      | 65515 i |
| *>             | 169.254.22.2  |        |        | 0      | 65515 i |
| *m 172.27.0.0  | 169.254.21.2  |        |        | 0      | 65515 i |
| *m             | 169.254.22.22 |        |        | 0      | 65515 i |
| *m             | 169.254.21.22 |        |        | 0      | 65515 i |
| *>             | 169.254.22.2  |        |        | 0      | 65515 i |

3)檢查路由表填充。

```
<#root>
```

```
ftd#
```

```
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 172.31.3.33 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
B      172.27.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
```

4)檢查BGP會話的連線表。

<#root>

ftd#

**show conn all | include TCP|179**

```
TCP ISP2-Inst-0 169.254.21.22:179 bgpLo-ISP2 169.254.22.100:1603, idle 0:00:10, bytes 1517, flags UIO
TCP ISP2-Inst-1 169.254.22.22:179 bgpLo-ISP2 169.254.22.100:41883, idle 0:00:01, bytes 1486, flags UIO
TCP ISP1-Inst-1 169.254.22.2:179 bgpLo-ISP1 169.254.21.100:3804, idle 0:00:53, bytes 1467, flags UIO
TCP ISP1-Inst-0 169.254.21.2:179 bgpLo-ISP1 169.254.21.100:61287, idle 0:00:04, bytes 1331, flags UIO
TCP bgpLo-ISP1 169.254.22.2:179 NP Identity Ifc 169.254.21.100:3804, idle 0:00:53, bytes 751, flags U
TCP bgpLo-ISP2 169.254.21.22:179 NP Identity Ifc 169.254.22.100:1603, idle 0:00:10, bytes 844, flags U
TCP bgpLo-ISP2 169.254.22.22:179 NP Identity Ifc 169.254.22.100:41883, idle 0:00:01, bytes 751, flags U
TCP bgpLo-ISP1 169.254.21.2:179 NP Identity Ifc 169.254.21.100:61287, idle 0:00:04, bytes 639, flags U
```

## 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）。