

將Azure vWAN站點到站點VPN配置為安全防火牆

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[圖表](#)

[Azure和FTD之間的單DIA連結vWAN連線 \(Azure負載平衡/冗餘 \)](#)

[設定](#)

[第1階段：Azure vWAN/中心配置](#)

[步驟 1:建立vWAN](#)

[步驟 2:建立vWAN中心](#)

[第2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 vWAN Site VPN引數](#)

[步驟 3:下載Azure vWAN站點隧道配置](#)

[第3階段：FTD組態](#)

[步驟 1:分析Azure VPN配置](#)

[步驟 2:配置環回](#)

[步驟 3:配置階段1/階段2策略對象](#)

[步驟 4:配置到Azure的安全連線](#)

[步驟 5:驗證到Azure的初始連線](#)

[步驟 6:配置到Azure例項1終結點的第三個隧道](#)

[步驟 7:配置ECMP](#)

[步驟 8:配置到例項專用IP的靜態路由](#)

[步驟 9:設定BGP](#)

[步驟 10:設定BGP多重路徑](#)

[驗證](#)

[其他注意事項](#)

[AS-Path預置](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹到Cisco安全防火牆的Microsoft Azure虛擬WAN(vWAN)站點到站點VPN連線的配置。

必要條件

需求

思科建議瞭解以下主題：

- Microsoft Azure虛擬廣域網(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)

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

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

Microsoft Azure虛擬WAN(vWAN)將多個Azure網路、安全和路由功能結合到單個Hub結構之後。每個vWAN中心都可以託管一個Microsoft管理的站點到站點VPN網關，遠端裝置（如安全防火牆）使用該網關訪問Azure，而無需構建和維護網關基礎架構。

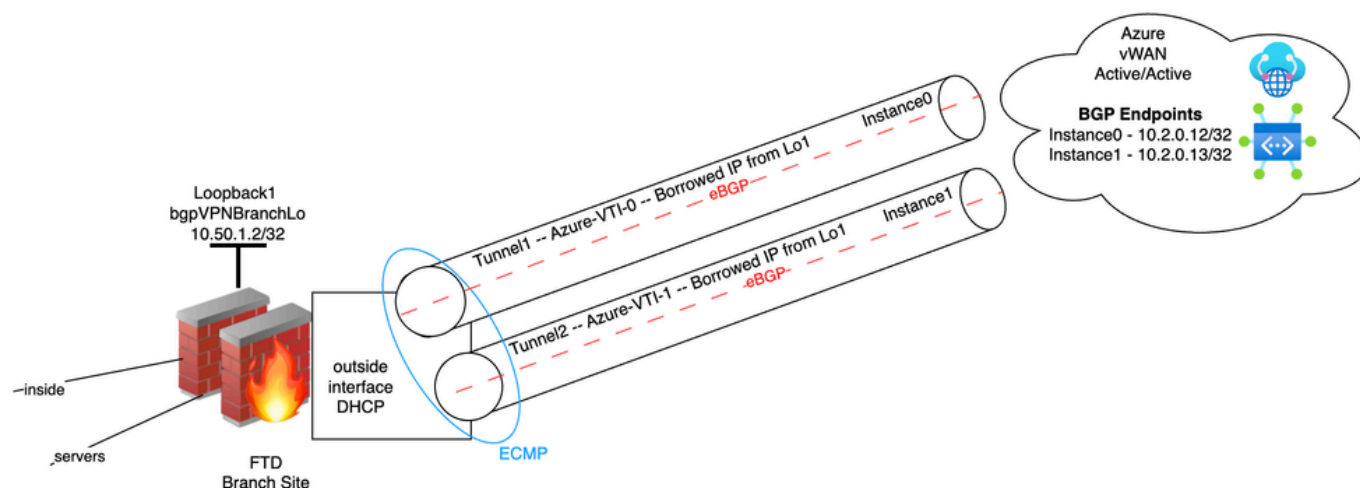
與傳統的雙端點IPsec VPN不同，Azure vWAN站點到站點VPN網關部署為一對活動 — 活動例項（Instance0和Instance1），每個例項都有自己的公共IP地址和邊界網關協定(BGP)對等地址。為了同時利用這兩個例項來實現冗餘和額外的吞吐量，分支FTD會建立通向每個例項的一個IP安全(IPsec)隧道，並使用BGP（而不是僅使用靜態路由）在例項可用或不可用時動態學習和撤銷路由。接著FTD上的等價多重路徑(ECMP)路由和BGP多重路徑會同時保持兩個通道處於使用中狀態，而不是將一個通道視為被動待機。

本文檔將設計分為三個階段：首先建立Azure vWAN集線器和VPN站點對象，下載生成的連線引數，然後使用這些相同的引數在FTD上配置匹配的虛擬隧道介面(VTI)、Internet金鑰交換版本2(IKEv2)/IPsec策略、靜態路由、ECMP和BGP對等（通過FMC）。

圖表

該圖顯示了本文所述的配置拓撲。單一直接網際網路存取(DIA)變體從FTD上的一個外部介面來源兩個Azure通道。

Azure和FTD之間的單DIA連結vWAN連線 (Azure負載平衡/冗餘)



設定

按順序完成這三個階段。在第1階段和第2階段中建立的Azure端對象會生成對等IP地址、BGP自治系統(AS)編號和預共用金鑰，然後在第3階段將這些金鑰應用於FTD。

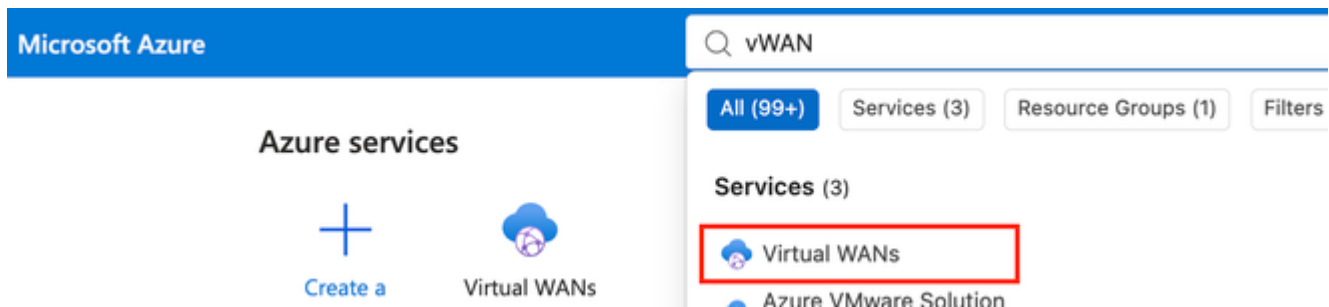
第1階段：Azure vWAN/中心配置



附註：本文檔中的配置步驟是高級步驟，並提供將FTD連線到Azure vWAN的必要步驟。請參閱Microsoft的Azure vWAN文檔以瞭解配置的重要性。請參閱[什麼是Azure虛擬WAN?](#)和更多文檔。

步驟 1:建立vWAN

a)在Azure搜尋框中搜尋vWAN，按一下虛擬WAN。



b)按一下+ Create。



c)為新的vWAN例項輸入Name，按一下Review + create，然後在嚮導的Review + Create頁上按一下Create。

Create WAN ...

Basics Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#) 

Project details

Subscription *

Resource group *

[Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >



附註：覆蓋影像中各個欄位中的值的空白用於發佈此文檔。

d)按一下轉至資源。



VirtualWanDeployment | Overview

Deployment



Delete



Cancel



Redeploy



Download



Refresh

Overview

Inputs

Outputs

Template



Your deployment is complete



Deployment name : VirtualWanDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

步驟 2: 建立vWAN中心

a) 導航至Connectivity > Hubs，然後點選+ New Hub。

CX-vWAN | Hubs

Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub	Hub status	Region
No results		

b)請參閱Azure文檔以瞭解有關進一步配置的更多上下文。請確保分配的Hub專用地址空間不會與任何內部地址空間重疊。配置名稱、Virtual Hub、Hub routing preference。按一下「Next:站點到站點>」。

Home > CX-vWAN | Hubs

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). [Learn more](#)

Project details

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

Subscription

Resource group

Virtual Hub Details

Region

Name

Hub private address space

Virtual hub capacity

Hub routing preference

Next steps

Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next : Site to site >](#)

c)有關所顯示欄位的資訊，請參閱Microsoft Azure vWAN Hub文檔。切換Yes以建立站點到站點 (VPN網關)。分配的預設BGP自治系統(AS)編號為65515，如Internet工程任務組(IETF)在請求註釋(RFC)6996中定義私有使用AS保留中所分配。



附註：記錄BGP AS以瞭解FMC上的未來配置步驟。

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

☒ Yes

☐ No

Copied

AS Number

65515

Gateway scale units

Routing preference

☒ Microsoft network ☐ Internet

Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

Next : Point to site >

按一下Review + create，或按一下Next:指向站點>以配置可選設定。

d)驗證摘要後，按一下Create。



附註：按照Azure狀態，建立中心需要30分鐘。

Create virtual hub ...

 Validation passedBasics Site to site Point to site ExpressRoute Tags **Review + create**

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

Basics

Region
Name CX-vWAN-Hub
Hub private address space 10.2.0.0/16
Virtual hub capacity
Hub routing preference

Site to site

Site to site (VPN gateway) Enabled
AS Number 65515
Gateway scale units

Point to site

Point to site (VPN gateway)

ExpressRoute

ExpressRoute gateway

Tanz

 Creating a hub with a gateway will take 30 minutes.**Create**

Previous

Next

[Download a template for automation](#)

e)部署完成後，搜尋原始vWAN資源名稱。若要進一步縮小搜尋範圍，請按一下「Resources」。

 VirtualHubDeployment | Overview ...

Deployment

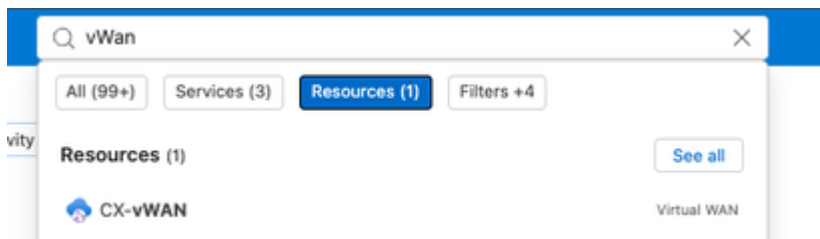
   Delete  Cancel  Redeploy  Download  Refresh Overview Inputs Outputs Template **Your deployment is complete**

 Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

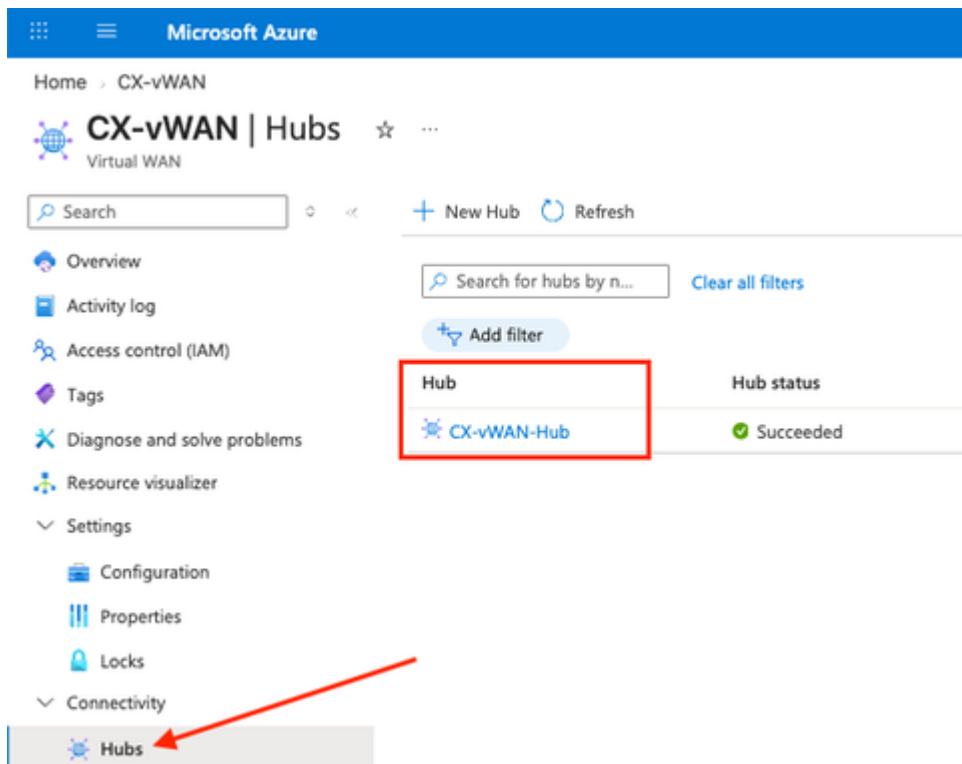
[Go to resource](#)



第2階段：Azure vWAN VPN站點配置

步驟 1: 建立Azure vWAN VPN站點 (遠端FTD裝置)

a) 通過連線>集線器進入已建立的集線器，然後點選在前面步驟中建立的集線器。



b) 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		

c)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 *	VPN-Site
Device vendor *	Cisco

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 >

d)輸入所需的連結資訊。Link BGP Address和Link ASN欄位反映了在通過站點到站點隧道與 Azure建立鄰居關係的分支站點上的內部隧道BGP第3層目標地址和BGP AS編號。鏈路BGP地址是位於先前配置的集線器私有地址空間子網之外的非重疊子網地址(/32),Azure將該子網安裝為作為BGP鄰居到達的/32路由。鏈路IP地址/FQDN是流向分支站點的流量的外部報頭第3層目標IP地址,這是調配IPsec/IKEv2連線所必需的。



附註：如果您使用範圍從169.254.21.0到169.254.22.255的地址作為隧道地址，請確保檢視 [How to configure BGP for Azure VPN Gateway](#)以滿足特定要求。

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	
single-dia-link ✓	1000 ✓	provider ✓	✓	10.50.1.2 ✓	65500 ✓	...

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

Previous

Next : Review + create >

e)確認設定正確後，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

Name VPN-Site

Device vendor Cisco

Private address space

Links

Link name	single-dia-link
Link provider name	provider
Link speed	1000
Link IP address / FQDN	
Link ASN	65500
Link BGP address	169.254.10.2

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

Create

Previous

Next

f)完成VPN站點的部署後，導航回vWAN Hub配置。

Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

Go to resource

Search vWan

All (99+) Services (3) Resources (1) Filters +4

Resources (1)

See all

CX-vWAN Virtual WAN

步驟 2:配置Azure vWAN Site VPN引數

a)通過連線>集線器進入已建立的集線器，然後點選在前面步驟中建立的集線器。

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

b)再次導航到Connectivity > VPN(Site to site)，然後點選X以清除Hub Association:已連線的篩選以檢視斷開連線的站點。

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

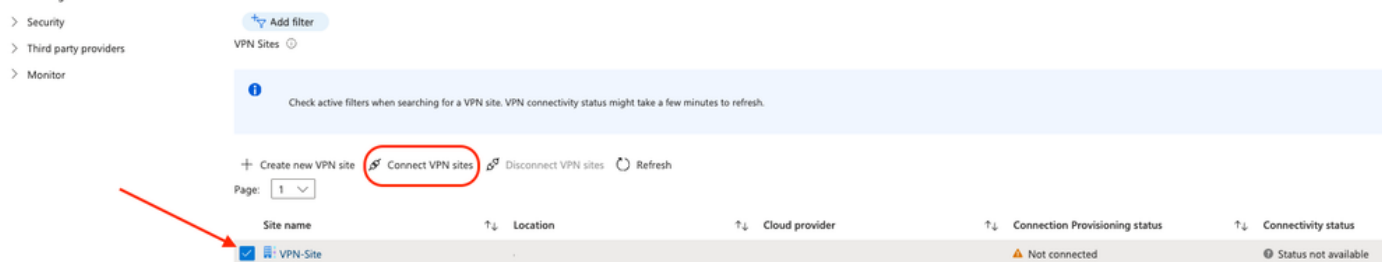
Search this page Clear all filters

Hub association : **Connected** X Add filter

VPN Sites ⓘ

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

c)選中先前配置的VPN站點旁邊的框，然後按一下Connect VPN sites，該選項在選擇站點後變為啟用。



d)出現「Connect sites (連線站點)」側抽屜面板。輸入預共用金鑰(PSK)並配置所需的第1階段IKEv2和第2階段IPsec設定。從IPsec下拉選單中選擇Custom時，值將自動填充；請注意這些值，因為它們必須在FTD上相符。您還必須選擇是否需要完全向前保密(PFS)。由於這是基於路由的隧道，請相應地配置設定。完成後，按一下Connect儲存配置。



附註：如需詳細資訊，請參閱[預設與自訂IPsec原則Azure vWAN](#)。

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 *

DHGroup24

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



VPN-Site

eastus

Connect

e)顯示表明正在更新網關的資訊，以及預計的完成時間。

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

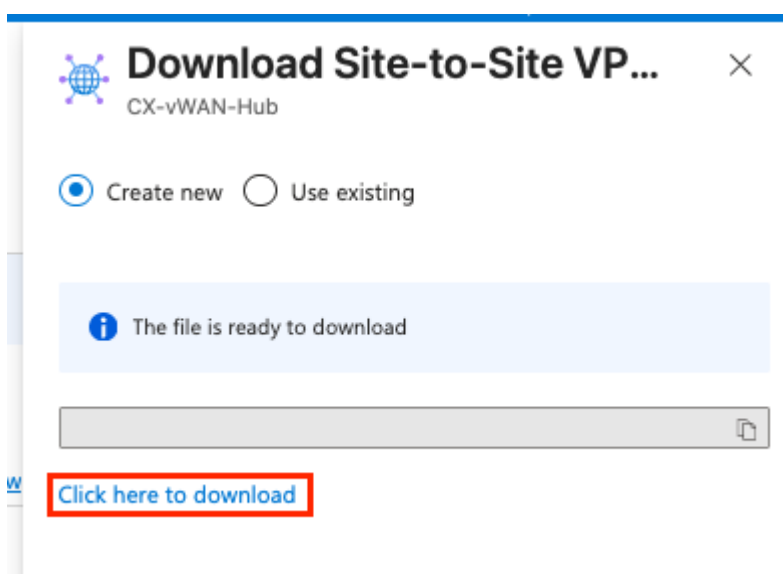
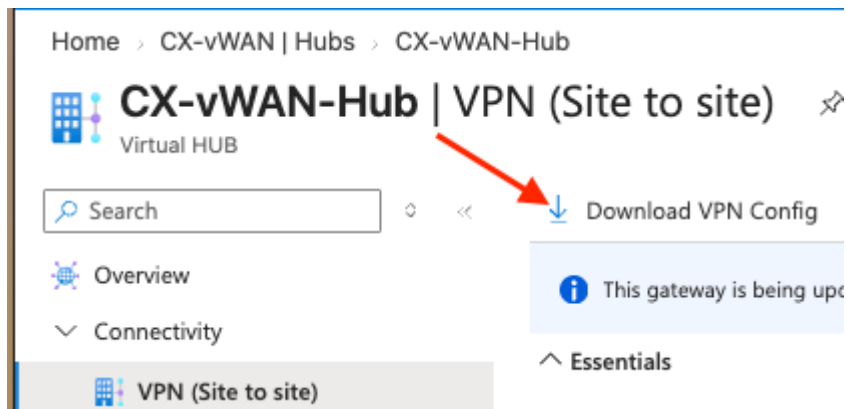
Connectivity



This gateway is being updated. It may take upto 30 minutes for the update

步驟 3:下載Azure vWAN站點隧道配置

a)更新網關時，可以下載VPN配置。



建立VPN站點並下載其連線引數（對等體位址、BGP AS編號和PSK）後，在第3階段中使用相同的值在FTD上設定匹配的元素。

第3階段：FTD組態

步驟 1:分析Azure VPN配置

a)從Azure開啟下載的VPN配置檔案。它看起來與圖中所示的壓縮輸出相似，並提供有用的資訊：



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。

```
[
  {
    "configurationVersion": {
      "LastUpdatedTime": "

    ",
    "Version": "

    ",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "Region": "

      "
    },
    "gatewayConfiguration": {
      "IpAddresses": {
        "Instance0": "57.x.x.x",
        "Instance1": "52.x.x.x"
      },
      "BgpSetting": {
        "Asn": 65515,
        "BgpPeeringAddresses": {
          "Instance0": "10.2.0.12",
          "Instance1": "10.2.0.13"
        }
      }
    },
    "connectionConfiguration": {
      "IsBgpEnabled": true,
      "PSK": "

    ",
    "IPsecParameters": {
      "IpsecEncryption": "GCMAES256",
      "IpsecIntegrity": "GCMAES256",
      "IkeEncryption": "GCMAES256",
      "IkeIntegrity": "SHA384",
      "PfsGroup": "None",
      "DhGroup": "DHGroup14",
      "SADataSizeInKilobytes": 0,
      "SALifeTimeInSeconds": 27000
    }
  }
]

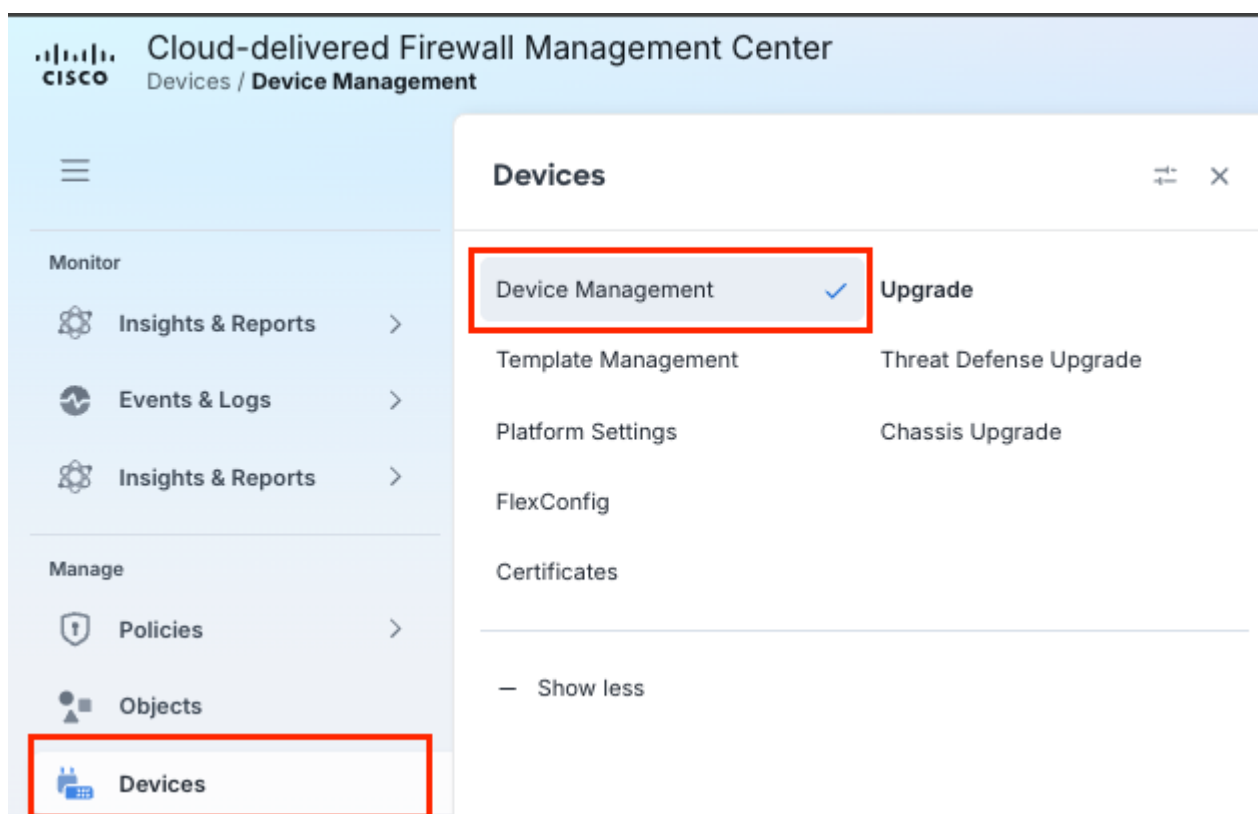
```

}
]

步驟 2:配置環回

以後配置的每個VTI都需要穩定的隧道源，因此首先配置環回介面並在兩個VTI之間共用。

a)導航至Devices > Device Management。

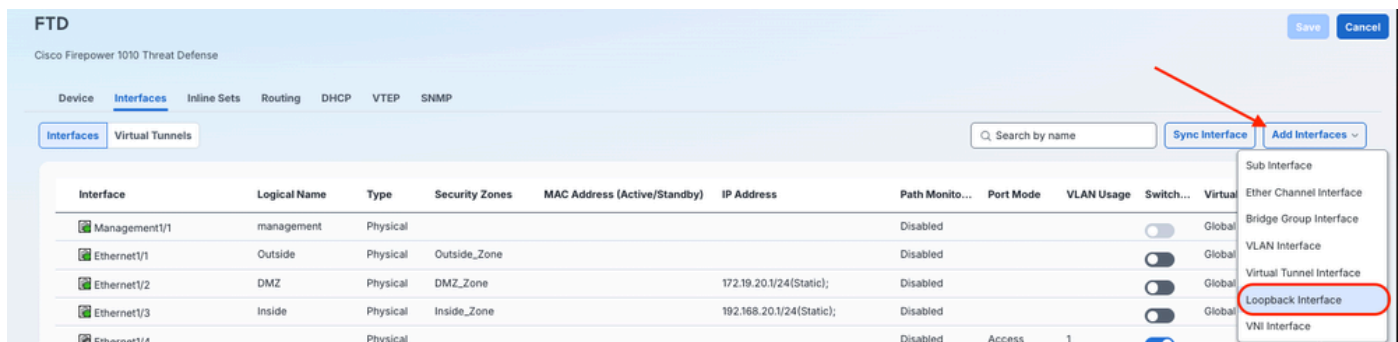


附註：本實驗使用雲交付的防火牆管理中心(cdFMC);但是，內部FMC的步驟保持不變。

b)選擇要配置為分支/站點VPN裝置的FTD。



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



d)必要時為環回介面提供Name、Loopback ID和Description。按一下「IPv4」。

e)確保IP Type定義為Use Static IP，輸入Link BGP Address (如第2階段第1d步中所配置)。您可以引用之前在下載的VPN配置JSON中定義的值，位於 `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



附註：使用/32掩碼並在RFC 1918 address-space中定義地址。

Add Loopback Interface

General **IPv4** IPv6

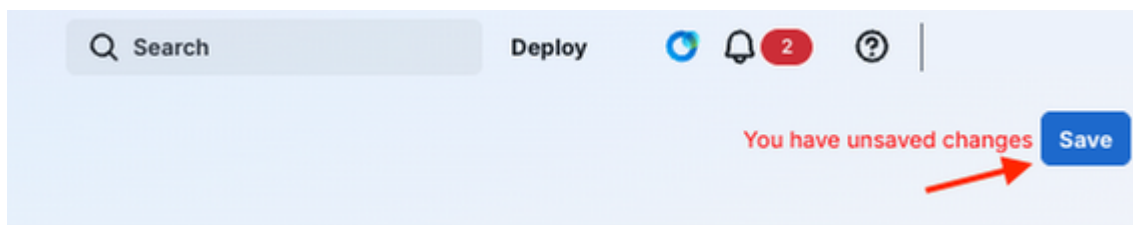
IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel **OK**

f)按一下Save



步驟 3:配置階段1/階段2策略對象

a)要在FMC上配置要應用於FTD VPN拓撲的匹配IKEv2/IPsec配置，請導航至Manage > Objects，在左側選單向下滾動至VPN，然後展開子選單。在選單中選擇IKEv2 Policy，然後按一下Add IKEv2 Policy，配置IKEv2第1階段策略。

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

IKEv2 Policy

Secure Client Customization

Secure Client File

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	
AES-GCM-NUL- SHA	☐ ☐
AES-GCM-NUL- SHA-LATEST	☐ ☐
AES- SHA - SHA	☐ ☐
AES- SHA - SHA-LATEST	☐ ☐
DES- SHA - SHA	☐ ☐
DES- SHA - SHA-LATEST	☐ ☐
Umbrella-AES-GCM-256	☐ ☐

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

b)為新的IKEv2策略輸入名稱，選擇Priority和/或Lifetime。請確保通道兩端的原則與Integrity、Encryption、PRF和Diffie-Hellman(DH)群相符。選擇要與Azure配置匹配的對齊的演算法/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:*
Azure_IKEv2

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)
3600

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

Selected Algorithms

SHA256

Cancel Save

c)配置完成後，按一下Save。

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
21

Add

Selected Groups

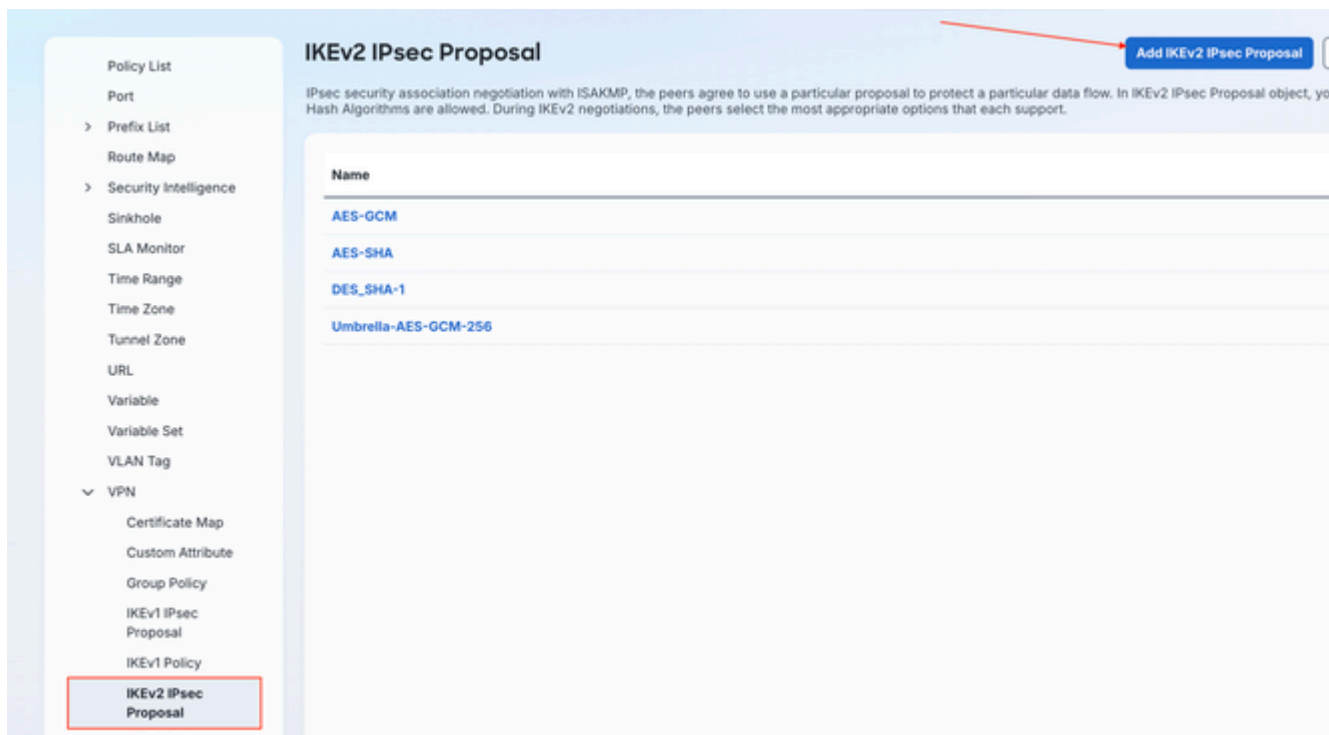
14



Cancel

Save

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



e)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」。



附註：您可以在下載的配置檔案中引用這些值，網址為
`vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256

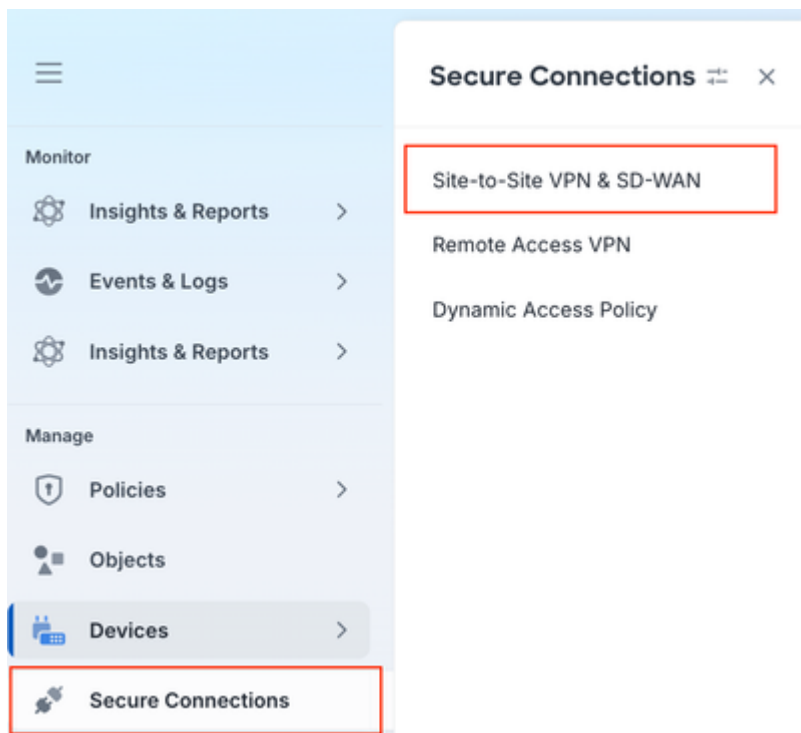


Cancel

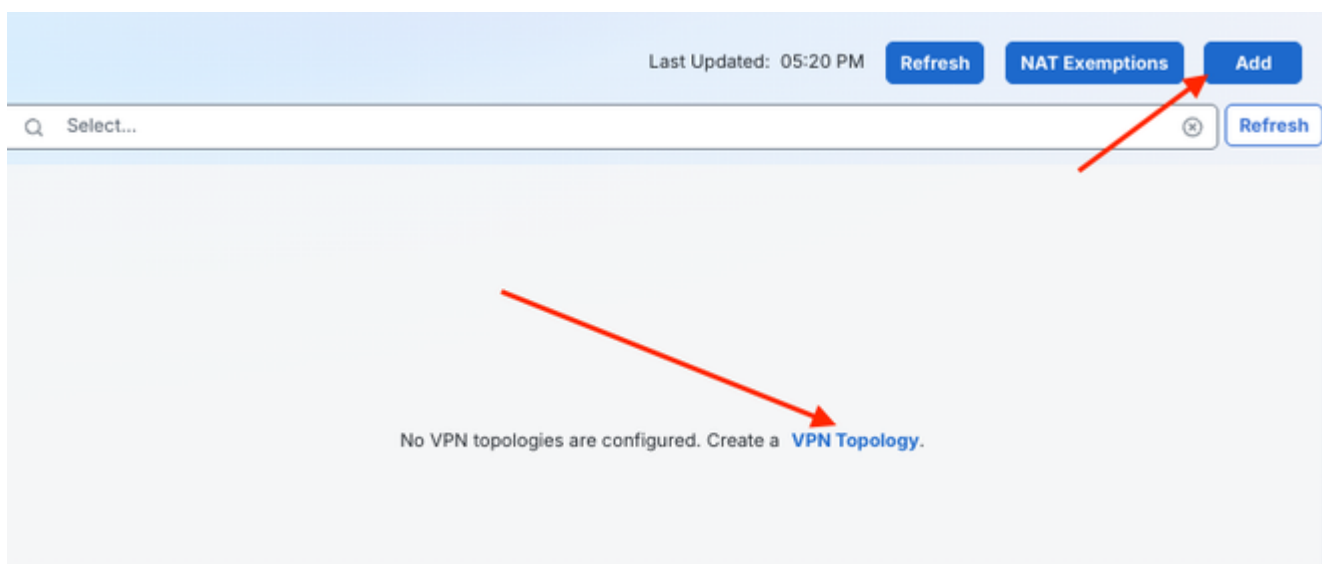
Save

步驟 4:配置到Azure的安全連線

a)導航至管理>安全連線>站點到站點VPN和SD-WAN。



b) 按一下中間的初始VPN拓撲配置超連結，或按一下Add。



c) 為通向Azure例項0的第一個隧道輸入拓撲名稱，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 *

Azure-VTI-Instance0

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](#)

d)對於節點A，點選Device下拉選單，並選擇將配置部署到的託管FTD/FTD HA對的名稱。對於節點B，由於它是在Azure vWAN例項上終止的拓撲中的連線的遠端端，因此請從Device下拉選單中選擇Extranet。接下來，對於節點A，按一下Virtual Tunnel Interface(VTI)下拉選單旁的+圖示。

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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

Device:*

FTD

Virtual Tunnel Interface:*

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

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

e)為第一個VTI指定名稱，並確保其處於啟用狀態。為VTI分配新的或現有的安全區域，分配隧道源

，並從相鄰下拉選單中選擇IP地址。

Add Virtual Tunnel Interface ?

Tunnel Type
☒ Static ☐ Dynamic

Name:*

☒ Enabled

Description:

Security Zone:

Priority:
 (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:*
 (0 - 10413)

Tunnel Source:*

f) 接下來，確保選中Border IP(IP unnumbered)單選按鈕，然後從右側下拉選單中選擇相同的loopback。完成後按一下OK。

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:*
 (0 - 10413)

Tunnel Source:*

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) +



g)配置並應用VTI後，手動填充隧道源IP地址（如果從DHCP填充父介面地址，則自動填充），並確保配置了Node B裝置名稱以及例項Endpoint IP地址。完成後，按一下IKE頁籤。



附註：您可以在以下位置下載的配置檔案中引用Instance0 Endpoint IP Address值
： `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

☐ 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

Device:*
FTD

Virtual Tunnel Interface:*
Azure-VTI-0 +

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

Tunnel Source IP Address:* ⓘ

☐ Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional

Node B

Device:*
Extranet

Device Name*:
Azure-Instance-0

Endpoint IP Address*:

Cancel Save

h) 向下滾動到IKEv2 Settings，並確保Authentication Type設定為Pre-shared Manual Key，然後輸入先前步驟中在Azure中配置的PSK。通過按一下鉛筆圖示來編輯可用的IKEv2策略來配置IKEv2第1階段策略。



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

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) 新增最初在步驟3中配置的IKEv2第1階段策略。

IKEv2 Policy



Available IKEv2 Policy 



Selected IKEv2 Policy

 Search

AES-GCM-NULL-SHA
AES-GCM-NULL-SHA-LAT...
AES-SHA-SHA
AES-SHA-SHA-LATEST
Azure_IKEv2
DES-SHA-SHA
DES-SHA-SHA-LATEST

Add

Azure_IKEv2 

Cancel

OK

j)選擇IPsec選項卡。

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Azure_IKEv2

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐

Enforce hex-based pre-shared key only

k)按一下Transform Sets(轉換集)下的IKEv2 IPsec Proposal(鉛筆圖示)編輯IKEv2 IPsec Proposal。

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ 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

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

l)按一下trash bin 圖示刪除預設AES-GCM轉換集，然後新增在步驟3的後半部分建立的自定義 Azure_IPsec轉換集/IKEv2 IPsec提議。按一下確定。

IKEv2 IPsec Proposal



Available Transform Sets  +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec 

Cancel

OK

m)向下滾動並輸入27000作為與Azure引數匹配的生存期。啟用PFS Group (如果適用)。按一下「Save」。



附註：您可以在以下位置下載的配置檔案中引用生存期值

： `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

☐ 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

Lifetime Duration*: 27000 Seconds (Range 120-2147483647)

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

> ESPv3 Settings

Cancel Save

n)部署更改。

Search Deploy

Search Device Advanced Deploy Deploy All

FTD In Progress... (83%) Applying updated policy configurat

o)部署完成後，請檢查隧道狀態分佈下的管理>安全連線>站點到站點VPN和SD-WAN;成功的連線呈綠色 (向上)。

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✓

部署第一個隧道後，在配置第二個隧道進行冗餘之前，請確認它已在IKE/IPsec和BGP層成功建立。

步驟 5:驗證到Azure的初始連線

a)SSH進入FTD，然後輸入system support diagnostic-cli、輸入en，然後按Enter鍵，因為唯讀FTD CLI上沒有密碼。

```
<#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>
```

```
en
```

```
Password:
```

```
ftd#
```

b)檢查階段1/階段2隧道狀態。

```
<#root>
```

```
ftd#
```

```
show crypto isakmp sa | i Status:
```

```
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show crypto ipsec sa | i State|spi
```

```
current outbound spi: 5E83023A
```

```
current inbound spi : 62BC7C9E
```

```
spi: 0x62BC7C9E (0x00010B45)
```

```
SA State: active
```

```
spi: 0x5E83023A (0x0002029B)
```

```
SA State: active
```

```
ftd#
```

c)執行擷取，以檢查在通道中從Azure接收的BGP傳輸控制協定(TCP)封包，以及從Instance-0Azure通道公用IP的外部擷取上的網路位址轉譯 — 遍歷(NAT-T)使用者資料包協定(UDP)連線埠4500/UDP連線埠500流量。

```
<#root>
```

```
ftd#
```

```
capture out-instance-0 trace interface Outside match ip host
```

```
any
```

```
ftd#
```

```
capture tun-vti-0 interface Azure-VTI-0 trace match ip host
```

```
any
```

```
ftd#
```

```
show cap tun-vti-0
```

```
3 packets captured
```

```
1: 03:23:43.510074      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240
```

```
2: 03:23:44.511204      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240
```

```
3: 03:23:46.512211      10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240
```

```
ftd#
```

確認與Instance0的連線後，為Instance1重複相同的VTI和VPN拓撲配置，以便兩個Azure網關例項

均可訪問。

步驟 6: 配置到 Azure 例項 1 終結點的第二個隧道

a) 從同一環回建立第二個 VTI (Azure-VTI-1) (步驟 3 b-f) 。

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:*
 (0 - 10413)

Tunnel Source:*

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)

VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b) 配置第二例項 VPN 拓撲 (步驟 4 g-n) 。



附註：您可以在以下位置下載的配置檔案中引用 Instance1 Endpoint IP Address 值：
： `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

c)部署配置更改，並檢查通道狀態。

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	
> Azure-VTI-Instance1	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	

d)簽入Azure，Instance0和Instance1都獲得Connected。

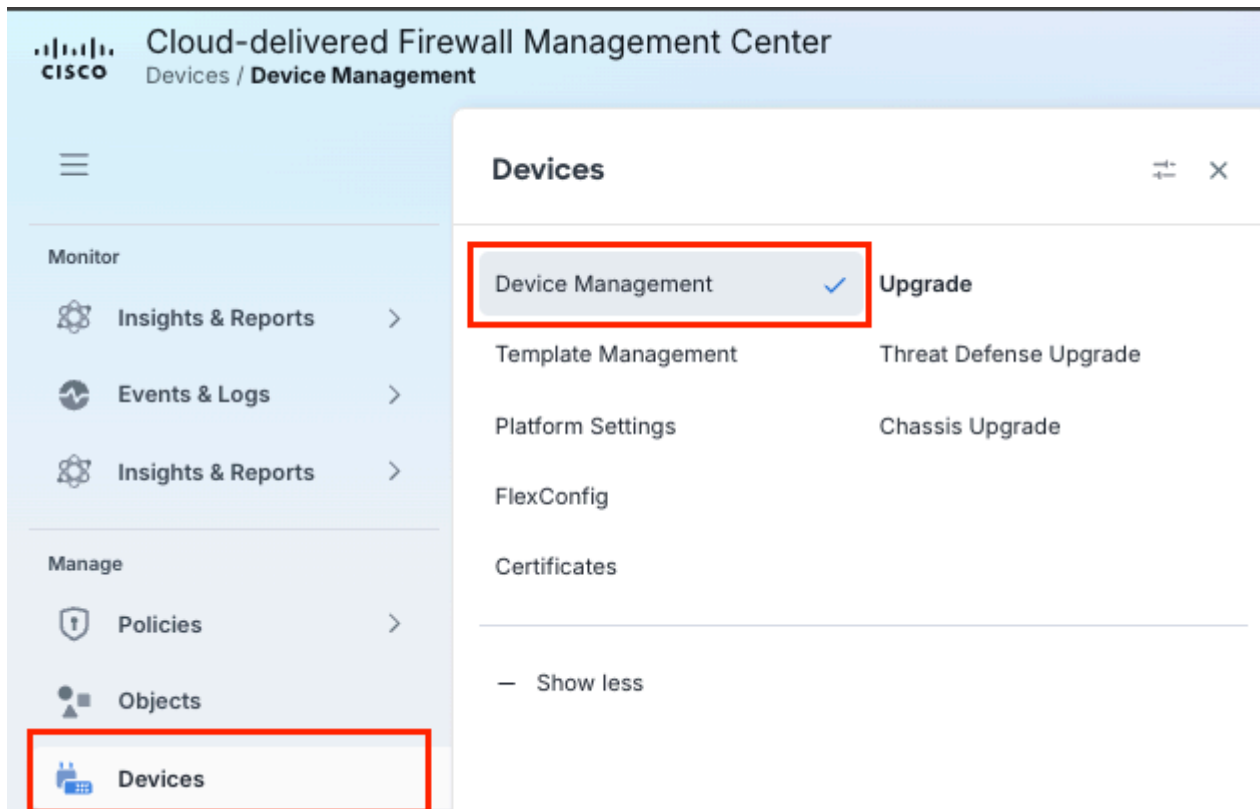
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

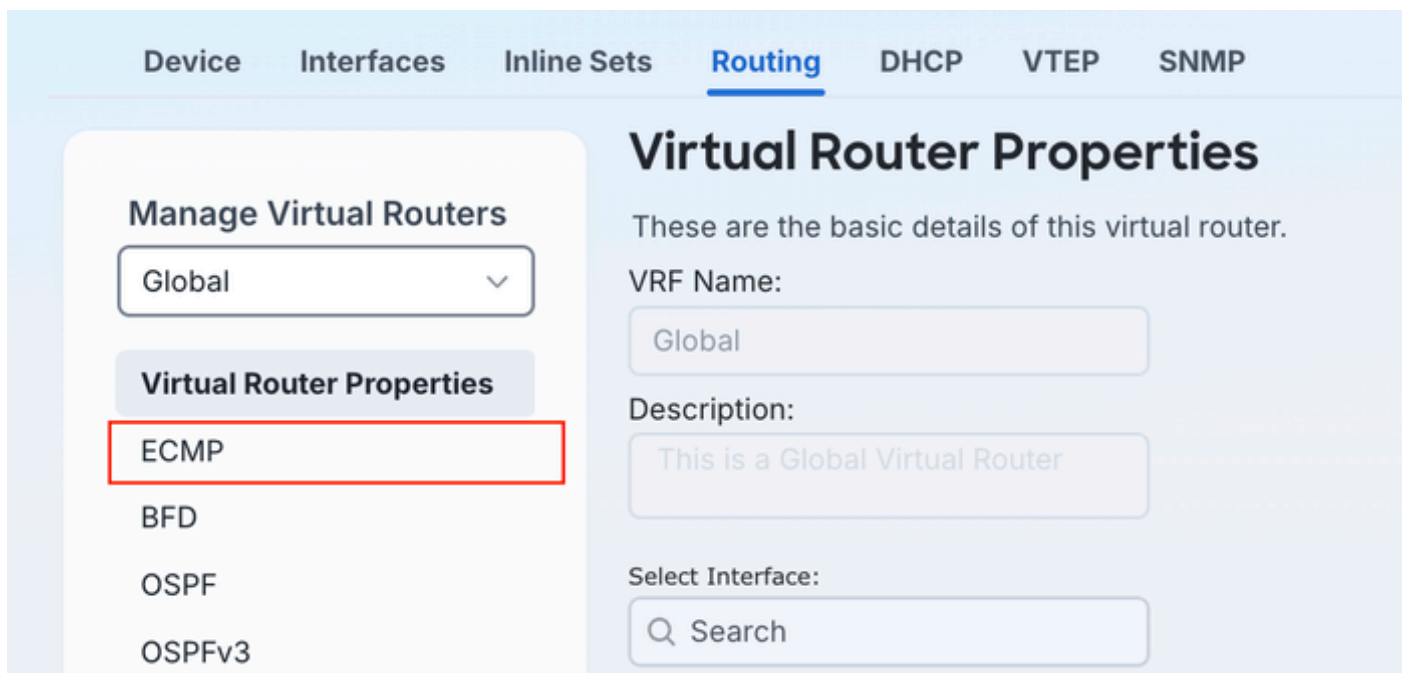
當兩個通道都處於作用中時，FTD需要ECMP路由，如此一來，流量就可以同時使用兩個路徑，而不是將第二個通道視為被動待命。

步驟 7:配置ECMP

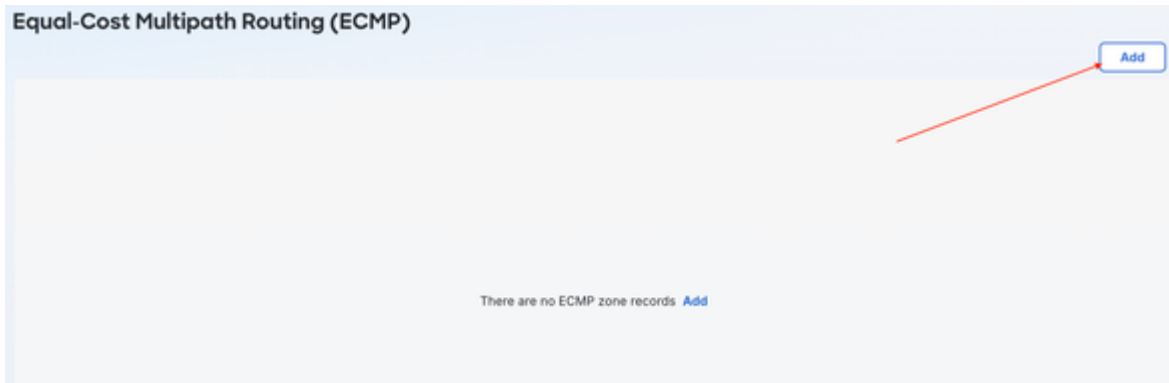
a)導航到Manage > Devices > Device Management，然後選擇為Azure配置VPN的FTD。



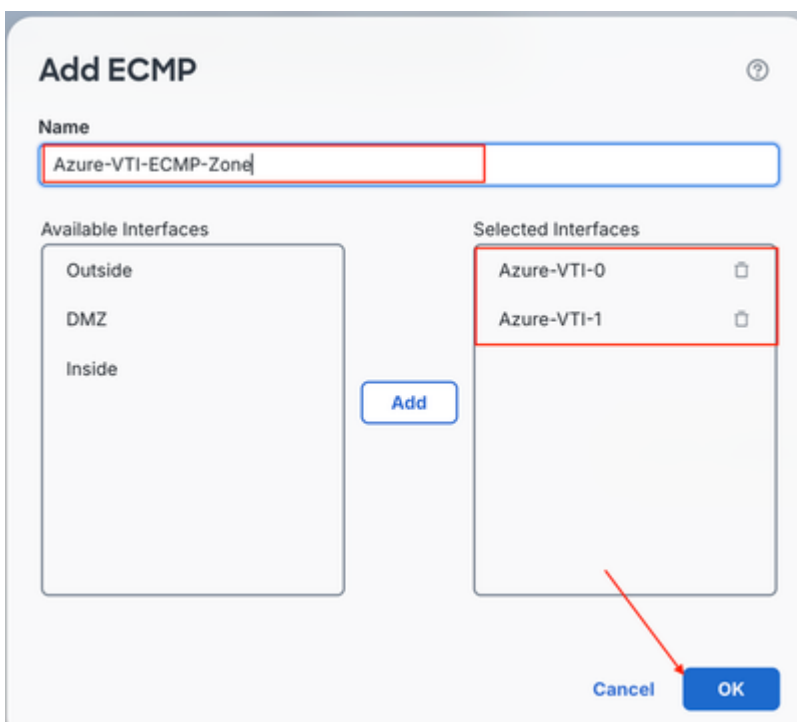
b)按一下Routing頁籤，然後選擇ECMP。



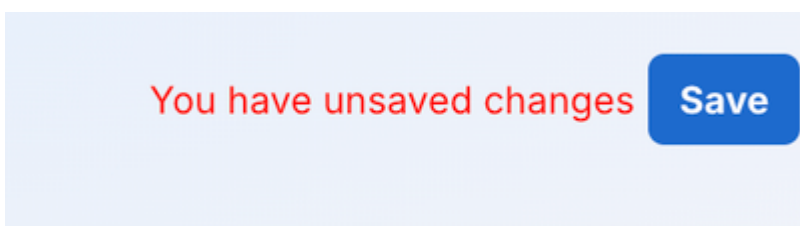
c)按一下Add以建立新的ECMP區域。



d)在Available Interfaces面板中按一下兩個VTI並單擊Add以將VTI應用於指定的ECMP區域，從而切換以突出顯示VTI。



e)確認設定正確後，按一下Save。



步驟 8:配置到例項專用IP的靜態路由

BGP需要路由才能成功連線到鄰居，並且由於端點不是直接連線的，因此預設情況下不會填充任何路由。ECMP允許您使用相同的度量（管理距離）配置到達同一目標的靜態路由，以便這兩個路由都安裝在路由資訊庫(RIB)中並同時使用。

a)導覽至Manage > Devices > Device Management，然後選擇適用的FTD裝置。

CISCO

Cloud-delivered Firewall Management Center

Devices / Device Management

Monitor

Insights & Reports

>

Events & Logs

>

Insights & Reports

>

Manage

Policies

>

Objects

>

Devices

>

Devices

Device Management

✓

Upgrade

Template Management

Threat Defense Upgrade

Platform Settings

Chassis Upgrade

FlexConfig

Certificates

Show less

b)導航到Routing > Static Route。

FTD

Cisco Firepower 1010 Threat Defense

Monitor

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

Manage

- Policies >
- Objects
- Devices >**
- Secure Connections >
- Integrations >
- Troubleshooting >
- Administration >

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

Manage Virtual Routers

Global

Virtual Router Properties

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

Network ▲ Inte

IPv4 Routes

IPv6 Routes

c)按一下+ Add Route。

+ Add Route

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

d)通過建立指向Instance0 VTI的第一條路由為兩個例項IP地址新增路由，並通過按一下「可用網路」旁邊的+為IP地址新增目標網路對象。然後，按一下清單中的網路對象並按一下「新增」按鈕，將其新增為靜態路由的目標。請確保選擇Instance0 IP並將其設定為Gateway。完成後，按一下OK。



附註：這些靜態路由目標網路值位於下 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` 載的 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` 配置檔案下方，位於下載的配置檔案中

。

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*
 Azure-VTI-0

(Interface starting with this icon  signifies it is available for route leak)

Available Network

Search: a

- Azure-Instance0-BGP_Peer
- Azure-Instance1-BGP_Peer

Add

Selected Network

- Azure-Instance0-BGP_Peer

Azure-Instance0-BGP_Peer
10.2.0.12

Ensure that egress virtualrouter has route to that destination

Gateway
 Azure-Instance0-BGP_Peer

Metric:
 1
 (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e)重複步驟c-d，通過Instance1 VTI新增第二條靜態路由。確保按一下Save以儲存更改。

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Azure-Instance1-BGP_Peer	Azure-VTI-1	Global	Azure-Instance1-BGP_Peer (10.2.0.13)	false	1	 
Azure-Instance0-BGP_Peer	Azure-VTI-0	Global	Azure-Instance0-BGP_Peer (10.2.0.12)	false	1	 
IPv6 Routes						

靜態路由僅到達BGP對等地址；BGP本身仍然必須啟用和共用，以便Azure和FTD可以動態地相互交換路由到更大的網路，或從其他網路交換路由。

步驟 9:設定BGP

a)在Routing > General Settings > BGP下，在FTD上啟用BGP Process 65500。選中Enable BGP覈取方塊，然後輸入先前在第2階段第1步中配置的AS編號。導航到Routing > BGP > IPv4旁。

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

SNMP

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*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

b)選中相鄰的Enable IPv4竅取方塊，為進程/AS 65500啟用IPv4 BGP路由，然後按一下Neighbor配置BGP鄰居。

FTD
Cisco Firepower 1010 Threat Defense

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

Enable IPv4: ☒ AS Number 65500

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3

General **Neighbor** Add Aggregate Address Filtering Networks Redis

Setting
Learned Route Map

c)按一下+ Add。

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

+ Add

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
No records to display				

d)輸入Instance0 BGP對等資訊，從vWAN集線器引用指定的BGP AS，然後輸入它作為Neighbor Remote AS，如果需要，新增description。按一下「Advanced」。



重要：確保變更BGP更新來源以參考FTD上兩個VTI介面的回送父項。

Add Neighbor

IP Address*
10.2.0.12

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
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e)在FTD上的BGP Neighbor設定的Advanced功能表中，可以將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。

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f)對Azure例項1 BGP對等項重複相同步驟。

Add Neighbor ?

IP Address*

10.2.0.13

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

BFD Fallover

none

Update Source:

bgpVPNBranchLo

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description

Instance1 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

☒ Allow connections with neighbor that is not directly connected

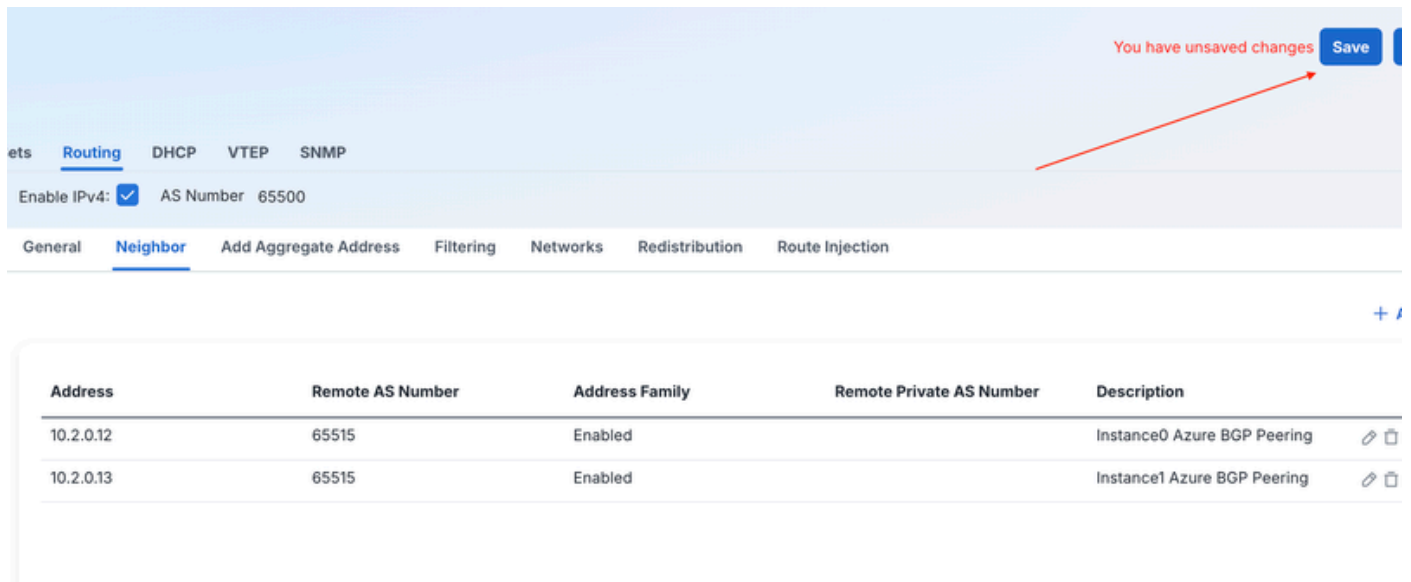
☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

g)確保在完成之後儲存更改。



預設情況下，BGP只在路由表中安裝一條最佳路徑，即使ECMP使兩條靜態路由都可用。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 10:設定BGP多重路徑

a)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。

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

Enable IPv4: ☒ AS Number 65500

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 Rout

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 (Use filtering to limit the number of prefixes that are redistributed)	No

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

b)將Number of Paths欄位的預設值從1更改為2。

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c)確保Save並部署更改。

驗證

部署完成後，請確認BGP與兩個Azure例項形成鄰接關係。隨後，使用第3階段第5步中建立的相同診斷CLI訪問，確認路由通過兩個隧道獲知，且流量使用兩個VTI。

在FTDsystem support diagnostic-cli CLI上導覽至。

a)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#
```

```
show bgp summary
```

```
BGP router identifier 10.50.1.2, local AS number 65500
```

```
BGP table version is 5, main routing table version 5
```

```
2 network entries using 400 bytes of memory
```

```
4 path entries using 320 bytes of memory
```

```
2 multipath network entries and 4 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 952 total bytes of memory
```

```
BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.2.0.12	4	65515	5	3	5	0	0	00:01:02	2
10.2.0.13	4	65515	3	4	5	0	0	00:00:55	2

```
ftd#
```

b)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 7, local router ID is 10.50.1.2
```

```
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	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i
*m 172.27.0.0	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i

```
ftd#
```

c) 檢查VTI資料包計數。

<#root>

ftd#

show interface Tunnel1 | i packets

```
118 packets input, 31385 bytes
134 packets output, 8780 bytes
0 packets dropped
```

ftd#

show interface Tunnel2 | i packets

```
127 packets input, 33629 bytes
230 packets output, 15119 bytes
0 packets dropped
```

ftd#

d) 確認BGP鄰居關係的靜態路由。

<#root>

ftd#

show running-config route

```
route Azure-VTI-0 10.2.0.12 255.255.255.255 10.2.0.12 1
route Azure-VTI-1 10.2.0.13 255.255.255.255 10.2.0.13 1
ftd#
```

e) 確認ECMP區域。

<#root>

ftd#

show zone

```
Zone: Azure-VTI-ECMP-Zone ecmp
  Security-level: 0
  Zone member(s): 2
    Azure-VTI-1          Tunnel2
    Azure-VTI-0          Tunnel1
```

ftd#

f) 確認BGP配置。

<#root>

ftd#

show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.2.0.12 remote-as 65515
    neighbor 10.2.0.12 description Instance0 Azure BGP Peering
    neighbor 10.2.0.12 ebgp-multihop 50
    neighbor 10.2.0.12 transport path-mtu-discovery disable
    neighbor 10.2.0.12 update-source bgpVPNBranchLo
    neighbor 10.2.0.12 activate
    neighbor 10.2.0.13 remote-as 65515
    neighbor 10.2.0.13 description Instance1 Azure BGP Peering
    neighbor 10.2.0.13 ebgp-multihop 50
    neighbor 10.2.0.13 transport path-mtu-discovery disable
    neighbor 10.2.0.13 update-source bgpVPNBranchLo
    neighbor 10.2.0.13 activate
  no auto-summary
  no synchronization
  exit-address-family
ftd#
```

g)確認路由表。

<#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 10.0.0.1 to network 0.0.0.0

```
B          10.2.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
          [20/0] via 10.2.0.12, 15:50:50
B          172.27.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
          [20/0] via 10.2.0.12, 15:50:50
```

其他注意事項

本檔案中的基本組態假設分支FTD有一個外部介面和一個ISP。這些考慮擴展了設計。

AS-Path預置

如果您需要影響Azure或FTD首選哪兩個隧道作為主隧道，而不是通過ECMP和BGP多重路徑等量共用負載，則在BGP鄰居上增加一個或多個本地AS號作為輔助隧道。在標準BGP最佳路徑選取期間，具有更長且預先AS路徑的鄰居會取消優先順序，而無需從ECMP區域完全移除該鄰居。

疑難排解

- 階段1/階段2通道無法啟動：確認預共用金鑰和IKEv2/IPsec策略引數（加密、完整性、PRF、DH組和生存期）在FMC IKEv2策略/IPsec建議與下載的Azure VPN配置檔案中的值之間完全匹配。使用`show crypto isakmp sa`和`show crypto ipsec sa`，如第3階段第5步中所示。
- 通道已啟動，但BGP鄰居未形成 `update-source`：確認BGP已設定為回送介面，而不是VTI本身，且已設定值高`ebgp-multihop`，足以到達Azure BGP對等位址（不是直接連線到FTD）。
- BGP形式，但只有一個通道傳輸流量：確認兩個VTI屬於同一個ECMP區域，以相同的管理距離安裝到兩個Azure例項BGP地址的靜態路由，並且為兩個路徑配置BGP多路徑，如第3階段第10步中所述。
- 沒有返回流量，或者到Azure的非對稱路由：因為Azure vWAN通過兩個隧道通告中心地址空間，所以請確保在路由配置的其他位置未禁用ECMP，並檢查路由對映或可以將流量固定到單一路徑的基於策略的路由。
- BGP已啟用且路由已安裝，但流量似乎遭封鎖：確保您配置了訪問控制規則，安全區域分配給VTI，允許流量進入和輸出。

相關資訊

- [什麼是Azure虛擬WAN？](#)
- [如何為Azure VPN網關配置BGP](#)
- [預設與自定義IPsec策略Azure vWAN](#)
- [對Azure VPN網關的BGP問題進行故障排除](#)
- [關於主用 — 主用模式VPN網關](#)
- [教程：使用Azure虛擬WAN建立站點到站點連線](#)

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）。