

Configure Azure vWAN Site-to-Site VPN to Secure Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Diagram](#)

[Single DIA Link vWAN Connectivity Between Azure and FTD \(Azure Load-Balancing/Redundancy\)](#)

[Configure](#)

[Phase 1: Azure vWAN/Hub Configuration](#)

[Step 1: Create vWAN](#)

[Step 2: Create vWAN Hub](#)

[Phase 2: Azure vWAN VPN Site Configuration](#)

[Step 1: Create Azure vWAN VPN Site \(Remote FTD Device\)](#)

[Step 2: Configure Azure vWAN Site VPN Parameters](#)

[Step 3: Download Azure vWAN Site Tunnel Configuration](#)

[Phase 3: FTD Configuration](#)

[Step 1: Analyze Azure VPN Configuration](#)

[Step 2: Configure Loopback](#)

[Step 3: Configure Phase 1/Phase 2 Policy Objects](#)

[Step 4: Configure Secure Connectivity to Azure](#)

[Step 5: Verify Initial Connectivity to Azure](#)

[Step 6: Configure Second Tunnel to Azure Instance1 Endpoint](#)

[Step 7: Configure ECMP](#)

[Step 8: Configure Static Routes to Instance Private IPs](#)

[Step 9: Configure BGP](#)

[Step 10: Configure BGP Multi-path](#)

[Verify](#)

[Other Considerations](#)

[AS-Path Prepending](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the configuration of Microsoft Azure Virtual WAN (vWAN) site-to-site VPN connectivity to Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Microsoft Azure Virtual Wide Area Network (vWAN)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure FTD Version 10.0
- Cisco Secure FMC Version 10.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Microsoft Azure Virtual WAN (vWAN) combines several Azure networking, security, and routing capabilities behind a single Hub construct. Each vWAN Hub can host a Microsoft-managed Site-to-Site VPN gateway that remote devices, such as Secure Firewall, use to reach into Azure without the having to build and maintain the gateway infrastructure.

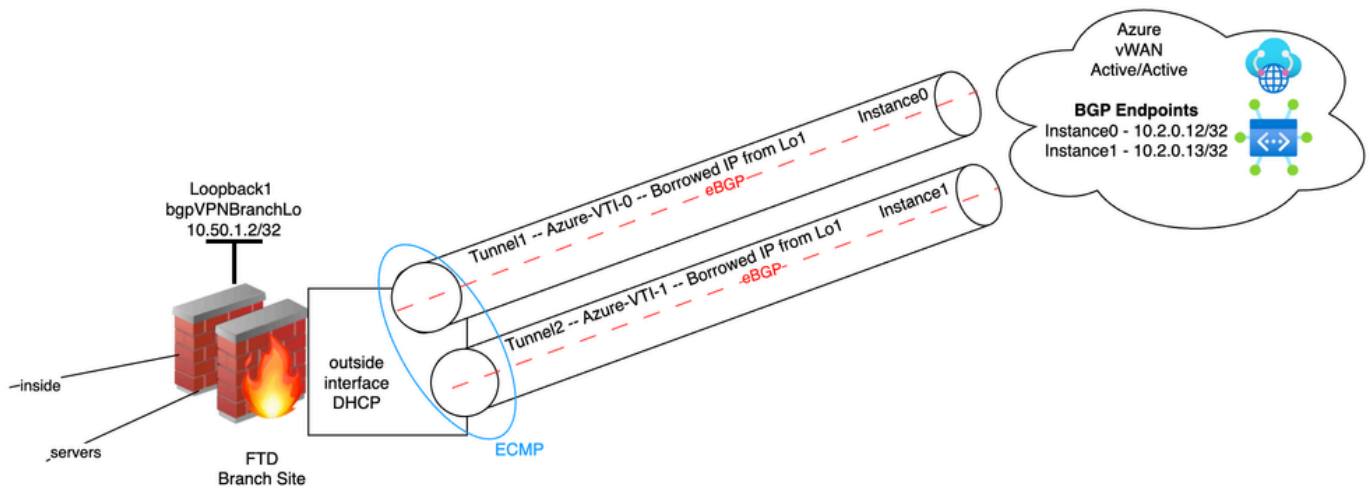
Unlike a conventional two-endpoint IPsec VPN, the Azure vWAN Site-to-Site VPN gateway deploys as an active-active pair of instances (Instance0 and Instance1), each with their own public IP address and Border Gateway Protocol (BGP) peering address. To take advantage of both instances for redundancy and additional throughput, the branch FTD establishes one IP security (IPsec) tunnel to each instance and uses BGP, rather than static routing alone, to dynamically learn and withdraw routes as instances become available or unavailable. Equal-Cost Multi-Path (ECMP) routing and BGP multipath on the FTD then keep both tunnels active at the same time, instead of treating one as a passive standby.

This document configures that design in three phases: the Azure vWAN Hub and VPN Site objects are created first, the resulting connection parameters are downloaded, and those same parameters are then used to configure matching Virtual Tunnel Interfaces (VTIs), Internet Key Exchange Version 2 (IKEv2)/IPsec policies, static routes, ECMP, and BGP peering on the FTD through FMC.

Diagram

The diagram shows the topology of the configuration described in this article. The single Direct Internet Access (DIA) variant sources both Azure tunnels from one outside interface on the FTD.

Single DIA Link vWAN Connectivity Between Azure and FTD (Azure Load-Balancing/Redundancy)



Configure

Complete the three phases in order. The Azure-side objects created in Phase 1 and Phase 2 produce the peer IP addresses, BGP Autonomous System (AS) numbers, and pre-shared key that Phase 3 then applies to the FTD.

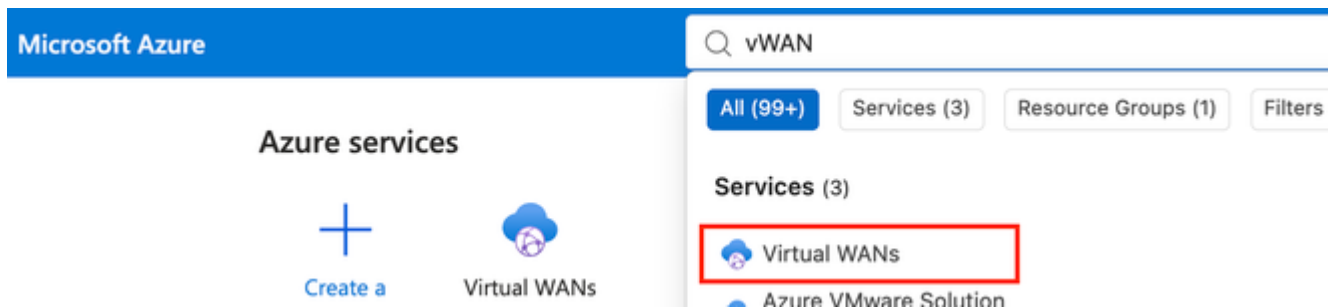
Phase 1: Azure vWAN/Hub Configuration



Note: The configuration steps in this document are high level and provide the necessary steps to connect the FTD to Azure vWAN. Refer to Azure vWAN documentation from Microsoft to understand the significance of the configurations. See [What is Azure Virtual WAN?](#) and further documentation.

Step 1: Create vWAN

a) Search for **vWAN** in the Azure search box, click **Virtual WANs**.



b) Click + **Create**.



c) Enter a **Name** for the new vWAN instance, click **Review + create**, and click **Create** on the **Review + Create** page within the wizard.

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 >



Note: White space covering values in various fields in the images is intentional for the publishing of this document.

d) Click **Go to resource**.



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

Step 2: Create vWAN Hub

a) Navigate to **Connectivity** > **Hubs** and click + **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) Refer to Azure documentation for further context on further configuration. Ensure that your **Hub private address space** allocated does not overlap any of your internal address spaces. Configure **Name**, **Virtual Hub**, **Hub routing preference**. Click **Next : Site to site >**.

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 * ⓘ

Review + create Previous Next : Site to site >

Creating a hub with a gateway will take 30 minutes.

c) Further refer to Microsoft Azure vWAN Hub documentation for information on the fields presented. Toggle **Yes** to create a **Site to site (VPN Gateway)**. The default BGP Autonomous System (AS) number allocated is **65515**, as allocated by the Internet Engineering Task Force (IETF) in Request For Comments (RFC) 6996 defining *Private Use AS Reservation*.



Note: Take record of the BGP AS for future configuration steps on the FMC.

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 >

Click **Review + create**, or click **Next : Point to site >** to configure optional settings.

d) Once the summary is verified, click **Create**.



Note: As Azure states, creating the hub takes 30 minutes.

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

Tanc

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

Previous

Next

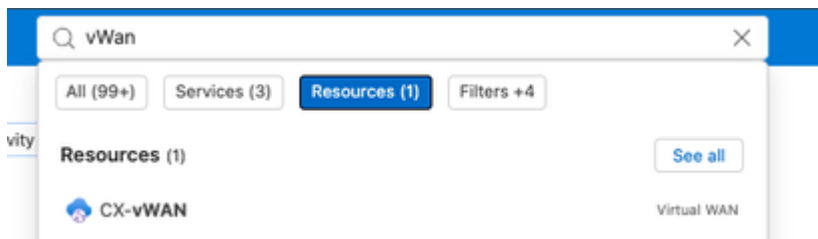
[Download a template for automation](#)

e) Once deployment is complete, search for your original vWAN resource name. To further narrow down your search, click **Resources**.

 VirtualHubDeployment | Overview ...    Delete  Cancel  Redeploy  Download  Refresh Overview Inputs Outputs Template Your deployment is complete

 Deployment name : VirtualHubDeployment
Subscription :
Resource group :

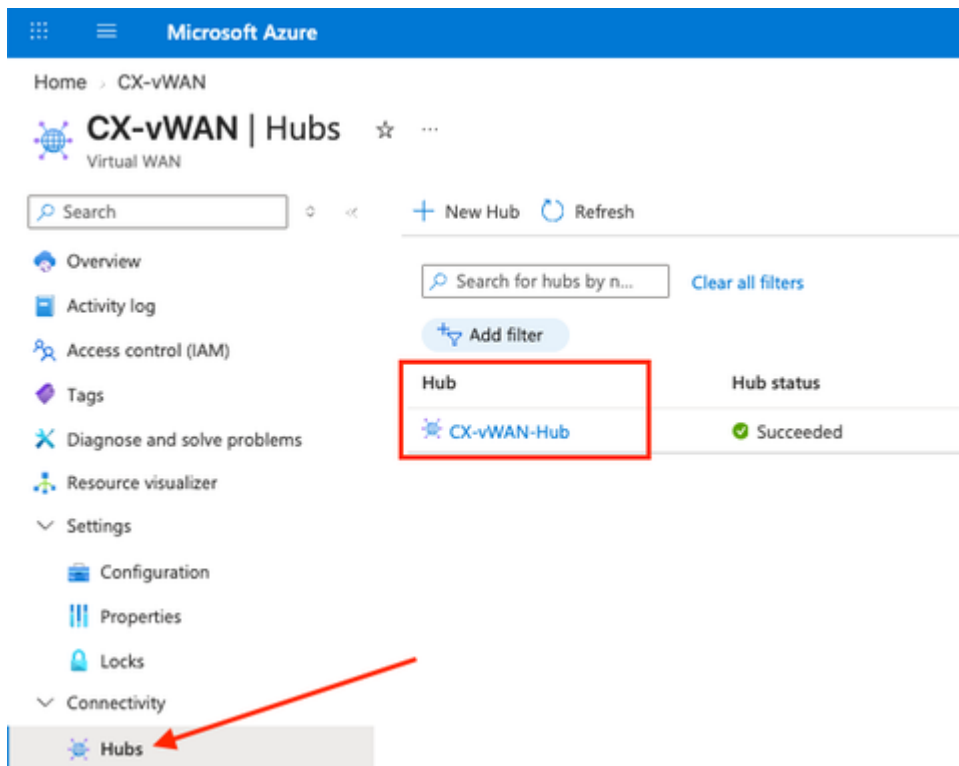
[Deployment details](#)[Next steps](#)[Go to resource](#)



Phase 2: Azure vWAN VPN Site Configuration

Step 1: Create Azure vWAN VPN Site (Remote FTD Device)

a) Enter into the created hub via **Connectivity > Hubs** and click the **hub** created in previous steps.



b) Click **Connectivity > VPN (Site to site)** and click + **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) Enter the **values** in the required fields. When done, click **Next: Links >** to move forward.

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) Enter the **required link information**. The Link BGP Address and the Link ASN fields reflect the inner-tunnel BGP Layer 3 destination address and BGP AS number on the branch site the neighborship with Azure is formed with over the site-to-site tunnels. The Link BGP Address is a non-overlapping subnet address (/32) outside of the previously configured Hub private address space subnet, which Azure installs as a /32 route to reach as a BGP neighbor. The Link IP address/FQDN is the outer-header Layer 3 destination IP address of traffic going to the branch site necessary to provision IPsec/IKEv2 connectivity.



Note: If you are using addresses ranging from 169.254.21.0 to 169.254.22.255 for tunnel addresses, ensure that you review [How to configure BGP for Azure VPN Gateway](#) for specific requirements.

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) After you confirm that the settings are correct, click **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) Once deployment of the VPN site completes, navigate back to the **vWAN Hub configuration**.

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

Step 2: Configure Azure vWAN Site VPN Parameters

a) Enter into the created hub via **Connectivity > Hubs** and click the **hub** created in previous steps.

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) Navigate once again to **Connectivity > VPN (Site to site)** and click the **X** to clear the **Hub Association: Connected** filtering to view disconnected sites.

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

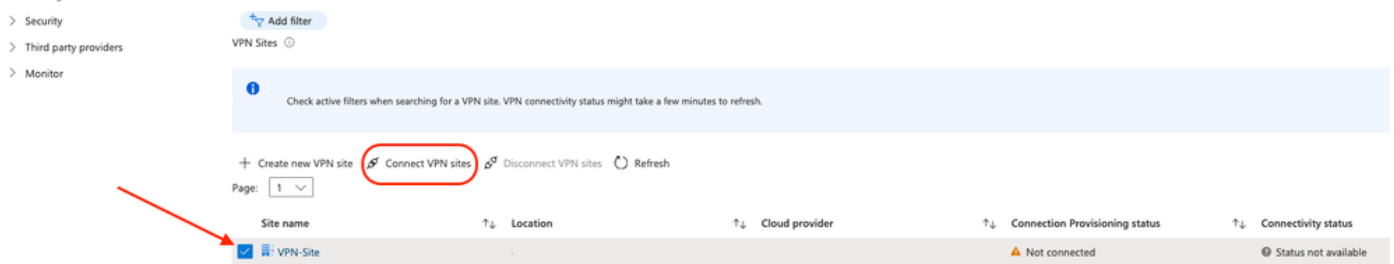
Search this page Clear all filters

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) Check the **box** next to the previously configured VPN site, and then click **Connect VPN sites**, which becomes enabled after the site is selected.



d) The Connect sites side drawer panel appears. Enter a **Pre-shared key (PSK)** and configure the desired **Phase 1 IKEv2** and **Phase 2 IPsec** settings. When you choose **Custom** from the **IPsec** drop-down list, the values populate automatically; note these values, as they must match on the FTD. You must also choose whether Perfect Forward Secrecy (PFS) is desired. Because this is a route-based tunnel, configure the settings accordingly. Once complete, click **Connect** to save the configuration.



Note: See [Default vs. Custom IPsec Policies Azure vWAN](#) for further information.

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) Information is displayed stating that the gateway is being updated, along with the estimated time to completion.

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

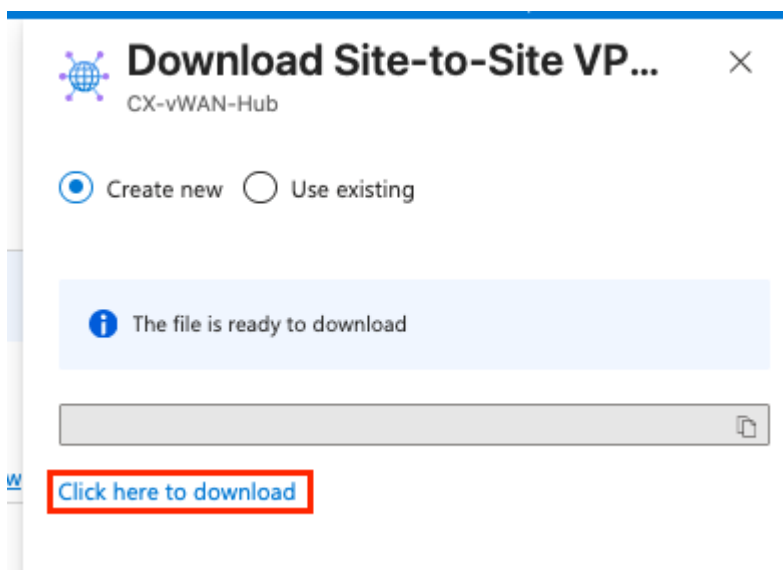
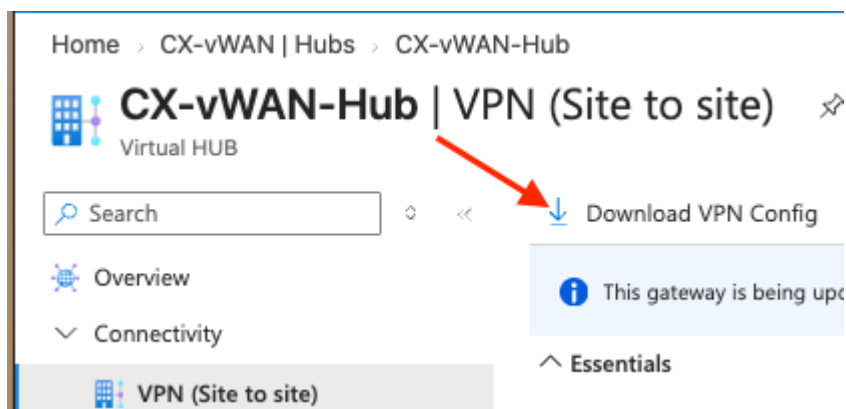
Connectivity



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

Step 3: Download Azure vWAN Site Tunnel Configuration

a) While the gateway is being updated, you can download the **VPN configuration**.



With the VPN Site created and its connection parameters (peer addresses, BGP AS numbers, and PSK) downloaded, the same values are used to configure the matching elements on the FTD in Phase 3.

Phase 3: FTD Configuration

Step 1: Analyze Azure VPN Configuration

a) Open the downloaded **VPN configuration** file from Azure. It looks similar to the condensed output shown and provides helpful information:



Note: For enhanced focus, several irrelevant objects and key/value pairs are pruned for brevity.

```
[
  {
    "configurationVersion": {
      "LastUpdateTime": "<Last Update Time>",
      "Version": "<Version UUID>"
    },
    "vpnSiteConfiguration": {
      "Name": "VPN-Site",
      "IPAddress": "<FTD public IP address>",
      "BgpSetting": {
        "Asn": 65500,
        "BgpPeeringAddress": "10.50.1.2"
      },
      "LinkName": "single-dia-link"
    },
    "vpnSiteConnections": [
      {
        "hubConfiguration": {
          "AddressSpace": "10.2.0.0/16",
          "Region": "<Azure 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": "<IPSec PSK>",
          "IPsecParameters": {
            "IpsecEncryption": "GCMAES256",
            "IpsecIntegrity": "GCMAES256",
            "IkeEncryption": "GCMAES256",
            "IkeIntegrity": "SHA384",
            "PfsGroup": "None",
            "DhGroup": "DHGroup14",
            "SADataSizeInKilobytes": 0,
            "SALifeTimeInSeconds": 27000
          }
        }
      }
    ]
  }
]
```

Step 2: Configure Loopback

Each VTI configured later needs a stable tunnel source, so a loopback interface is configured first and shared between both VTIs.

a) Navigate to **Devices > Device Management**.

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



Note: This lab uses cloud-delivered Firewall Management Center (cdFMC); however, the steps remain the same for on-prem FMC.

b) Select the **FTD** you are configuring as the branch/site VPN device.

☐	FTD N/A - ROUTED	10.0.0	Firepower 1010 Threat Defense
--------------------------	----------------------------	--------	-------------------------------

c) Click the **Add Interfaces** dropdown menu, and click **Loopback Interface**.

FTD
Cisco Firepower 1010 Threat Defense

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

Interfaces Virtual Tunnels

Search by name Sync Interface **Add Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monito...	Port Mode	VLAN Usage	Switch...	Virtual
Management1/1	management	Physical				Disabled				Global
Ethernet1/1	Outside	Physical	Outside_Zone			Disabled				Global
Ethernet1/2	DMZ	Physical	DMZ_Zone		172.19.20.1/24(Static);	Disabled				Global
Ethernet1/3	Inside	Physical	Inside_Zone		192.168.20.1/24(Static);	Disabled				Global
Ethernet1/4		Physical				Disabled	Access	1		Global

Sub Interface
Ether Channel Interface
Bridge Group Interface
VLAN Interface
Virtual Tunnel Interface
Loopback Interface
VNI Interface

d) Give the Loopback Interface its **Name**, **Loopback ID**, and **Description** if necessary. Click **IPv4**.

Add Loopback Interface ?

General **IPv4** IPv6

Name:

☒ Enabled

Loopback ID: *

(1-1024)

Description

[Cancel](#) [OK](#)

e) Ensure that the **IP Type** is defined as **Use Static IP**, enter the **Link BGP Address** as configured in Phase 2, step 1d. You can refer to the value previously defined in the downloaded VPN config JSON under `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Note: Define the address with a /32 mask and within RFC 1918 address-space.

Add Loopback Interface ?

General **IPv4** IPv6

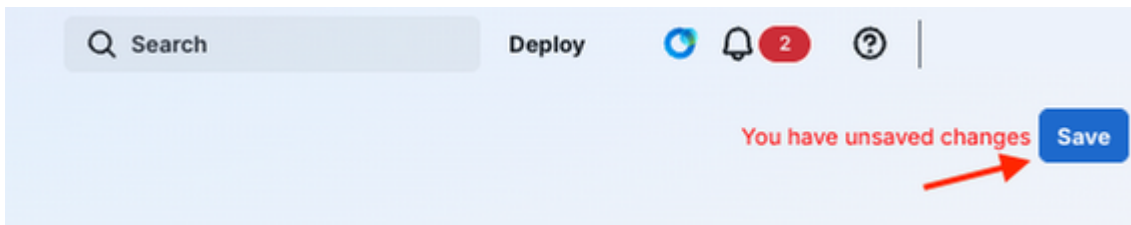
IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

[Cancel](#) [OK](#)

f) Click **Save**



Step 3: Configure Phase 1/Phase 2 Policy Objects

a) To configure matching IKEv2/IPsec configuration on the FMC to apply in the FTD VPN topologies, navigate to **Manage > Objects**, scroll down on the left menu to **VPN**, and expand the sub menu. Configure the **IKEv2 Phase 1 Policy** by choosing **IKEv2 Policy** in the menu and clicking **Add IKEv2 Policy**.

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

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) Enter a **name** for the new **IKEv2 Policy**, choose **Priority** and/or **Lifetime**. Ensure that the policy matches on both ends of the tunnel regarding **Integrity, Encryption, PRF, and Diffie-Hellman (DH) Group**. Choose the **aligned Algorithm/Group** elements to match with the Azure configuration, and click **Add**.



Note: You can reference these exact values within the downloaded configuration file at `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

New IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

Selected Algorithms

SHA256 

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

c) Once configuration is done, click **Save**.

Edit IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

1

2

5

14

15

16

19

20

...

Add

14

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

d) Configure **Phase 2/IPsec parameters** in the **IKEv2 IPsec Proposal** sub-menu and click **Add IKEv2 IPsec Proposal**.

The screenshot shows the Palo Alto Networks configuration interface. On the left is a navigation pane with a tree structure. Under the 'VPN' category, 'IKEv2 IPsec Proposal' is highlighted with a red rectangle. The main content area is titled 'IKEv2 IPsec Proposal' and contains a description: '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 specify the encryption and authentication algorithms. During IKEv2 negotiations, the peers select the most appropriate options that each support.' Below the description is a table with the following entries:

Name
AES-GCM
AES-SHA
DES_SHA-1
Umbrella-AES-GCM-256

In the top right corner of the main area, there is a blue button labeled 'Add IKEv2 IPsec Proposal' with a red arrow pointing to it from the top right edge of the screenshot.

e) Name the **IKEv2 IPsec Proposal** and ensure that the same settings align. Once done, click **Save**.



Note: You can reference these values within your downloaded configuration file at `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

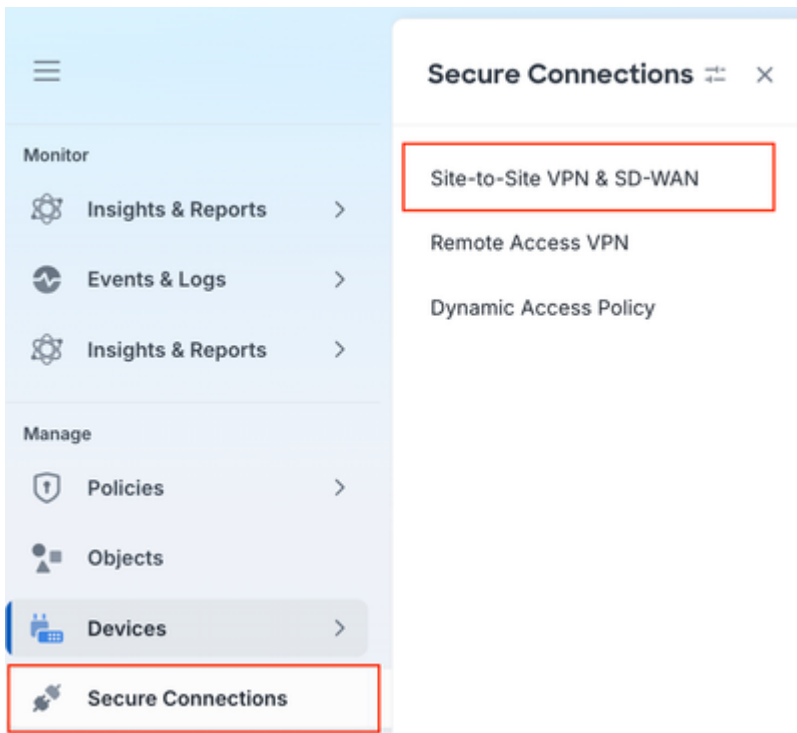


Cancel

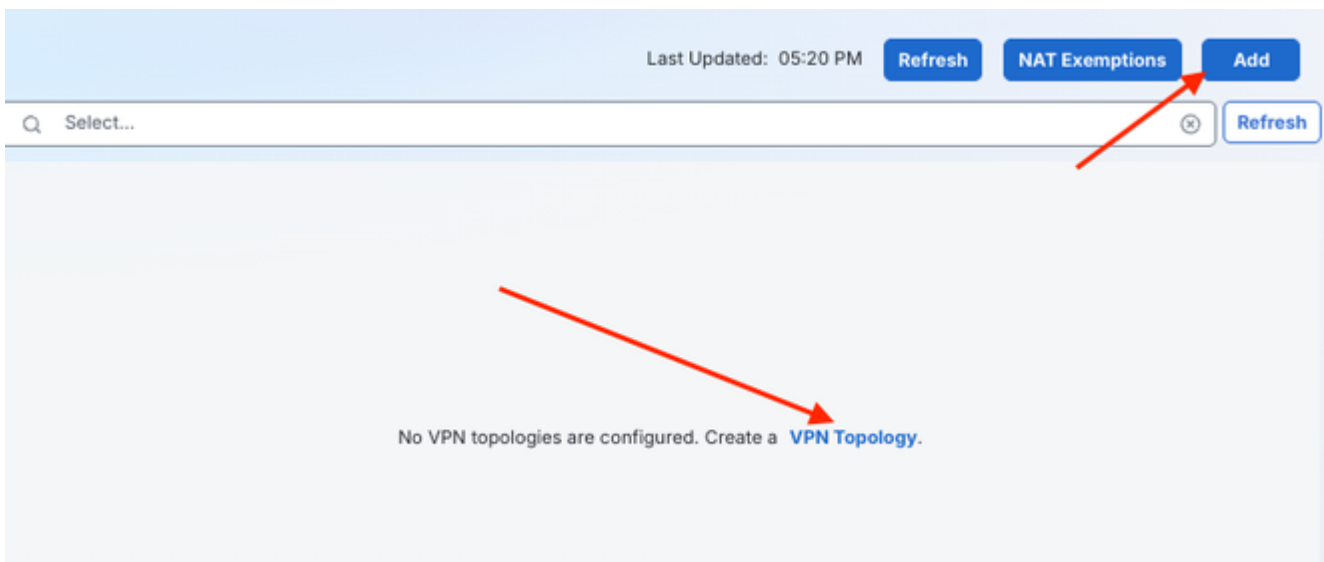
Save

Step 4: Configure Secure Connectivity to Azure

a) Navigate to **Manage > Secure Connections > Site-to-Site VPN & SD-WAN**.



b) Click either the initial **VPN Topology** configuration hyperlink in the middle, or click **Add**.



c) Enter a **Topology name** for the first tunnel to Azure Instance0, click the **Route-Based VPN** radio button, and click the **Peer to Peer** VPN topology type. Once completed, click **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

Warning: SASE topology cannot be selected because Secure Access and Umbrella are not configured.

Prerequisites

Refresh

Cancel Create

d) For **Node A**, click the **Device** drop-down list and choose the name of the managed FTD/FTD HA-Pair that the configuration is being deployed to. For **Node B**, because it is the remote end of the connection in the topology terminating on Azure vWAN instances, choose **Extranet** from the **Device** drop-down list. Next, for **Node A**, click the + icon adjacent to the **Virtual Tunnel Interface (VTI)** drop-down list.

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)

Tunnel Source IP is Private Edit VTI

Send Local Identity to Peers

> Advanced Settings

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

Cancel Save

e) Give the first VTI a **Name**, and ensure that it is **Enabled**. Assign a new or existing **Security Zone** to the

VTI, assign the **Tunnel Source**, and choose the **IP address** from the adjacent drop-down list.

Add Virtual Tunnel Interface ?

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Azure-VTI-0

☒ Enabled

Description:

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:*
Ethernet1/1 (Outside) Dynamic

The screenshot shows the 'Add Virtual Tunnel Interface' configuration page. Red arrows point to the 'Name' field (containing 'Azure-VTI-0'), the 'Security Zone' dropdown (containing 'Azure-Spoke-Zone'), the 'Tunnel ID' field (containing '1'), the 'Tunnel Source' dropdown (containing 'Ethernet1/1 (Outside)'), and the 'Dynamic' radio button in the 'Tunnel Source' section.

f) Next, ensure that the **Borrow IP (IP unnumbered)** radio button is selected, then choose the same **loopback** from the right drop-down list. Click **OK** once complete.

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

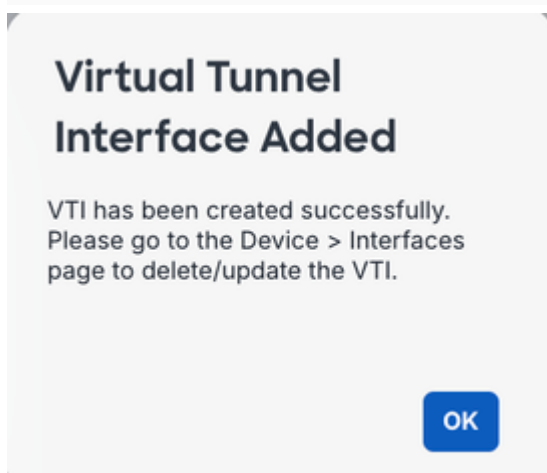
Tunnel ID:*
 (0 - 10413)

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) Once the VTI is configured and applied, manually populate the **Tunnel Source IP Address** (it populates automatically if parent interface address is populated from DHCP), and ensure that the **Node B** device name is configured, as well as the Instance **Endpoint IP Address**. Once complete, click the **IKE** tab.



Note: You can reference Instance0 Endpoint IP Address value in the downloaded configuration file at `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

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](#)

h) Scroll down to **IKEv2 Settings** and ensure that the **Authentication Type** is set to **Pre-shared Manual Key**, and enter the **PSK** configured in Azure in previous steps. Configure the **IKEv2 Phase 1 Policies** by clicking the **pencil icon** to edit available IKEv2 policies.



Note: Note: You can reference the pre-shared key in the downloaded configuration file at `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

i) Add the **IKEv2 Phase 1 policy** configured initially in Step 3.

IKEv2 Policy



Available IKEv2 Policy  +

 Search

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

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

j) Select the **IPsec** tab.

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) Edit the **IKEv2 IPsec Proposal** under **Transform Sets** by clicking the **pencil icon**.

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

1) Click the **trash bin** icon to remove the default **AES-GCM** transform set, and add the custom **Azure_IPsec** transform set/IKEv2 IPsec Proposal created in the second half of Step 3. Click **OK**.

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) Scroll down and enter **27000** for the lifetime duration matching Azure parameters. Enable **PFS Group** if applicable. Click **Save**.



Note: You can reference the lifetime value in the downloaded configuration file at `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) Deploy the changes.

Search Deploy

Search Device Advanced Deploy Deploy All

☐ FTD

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

o) Once deployment concludes, check under **Manage > Secure Connections > Site-to-Site VPN & SD-WAN** under **Tunnel Status Distribution**; successful connectivity reflects **Green (Up)**.

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

With the first tunnel deployed, confirm that it establishes successfully at both the IKE/IPsec and BGP layers before configuring the second tunnel for redundancy.

Step 5: Verify Initial Connectivity to Azure

a) SSH into the FTD and enter `system support diagnostic-cli`, type `en`, and press **Enter**, as there is no password on the read-only FTD CLI.

```
<#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) Check phase 1/phase 2 tunnel status.

```
<#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) Perform captures to check for BGP Transmission Control Protocol (TCP) packets received from Azure in the tunnel and either **Network Address Translation - Traversal (NAT-T) User Datagram Protocol (UDP) port 4500/UDP port 500** traffic on the outside capture from the public IP of **Instance-0** Azure Tunnel.

```
<#root>
```

```
ftd#
```

```
capture out-instance-0 trace interface Outside match ip host <Azure-instance0-IP> any
```

```
ftd#
```

```
capture tun-vti-0 interface Azure-VTI-0 trace match ip host <Link BGP IP> 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 <ms
2: 03:23:44.511204      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240 <ms
3: 03:23:46.512211      10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240 <mss
```

```
ftd#
```

With connectivity to Instance0 confirmed, repeat the same VTI and VPN topology configuration for Instance1 so that both Azure gateway instances are reachable.

Step 6: Configure Second Tunnel to Azure Instance1 Endpoint

a) Create Second VTI (**Azure-VTI-1**) borrowing from same loopback (Step 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:*
2 (0 - 10413)

Tunnel Source:*
Ethernet1/1 (Outside) 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
☒ Borrow IP (IP unnumbered) Loopback1 (bgpVPNBranchLo)

VPN Topology Usage
Azure-VTI-Instance1 (Tunnel Destination IP -

b) Configure **second instance VPN topology** (Step 4 g-n).



Note: You can reference Instance1 Endpoint IP Address value in the downloaded configuration file at `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 [i](#)

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

c) Deploy **configuration changes**, and check the **tunnel status**.

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

d) Checking in Azure, both Instance0 and Instance1 yield Connected.

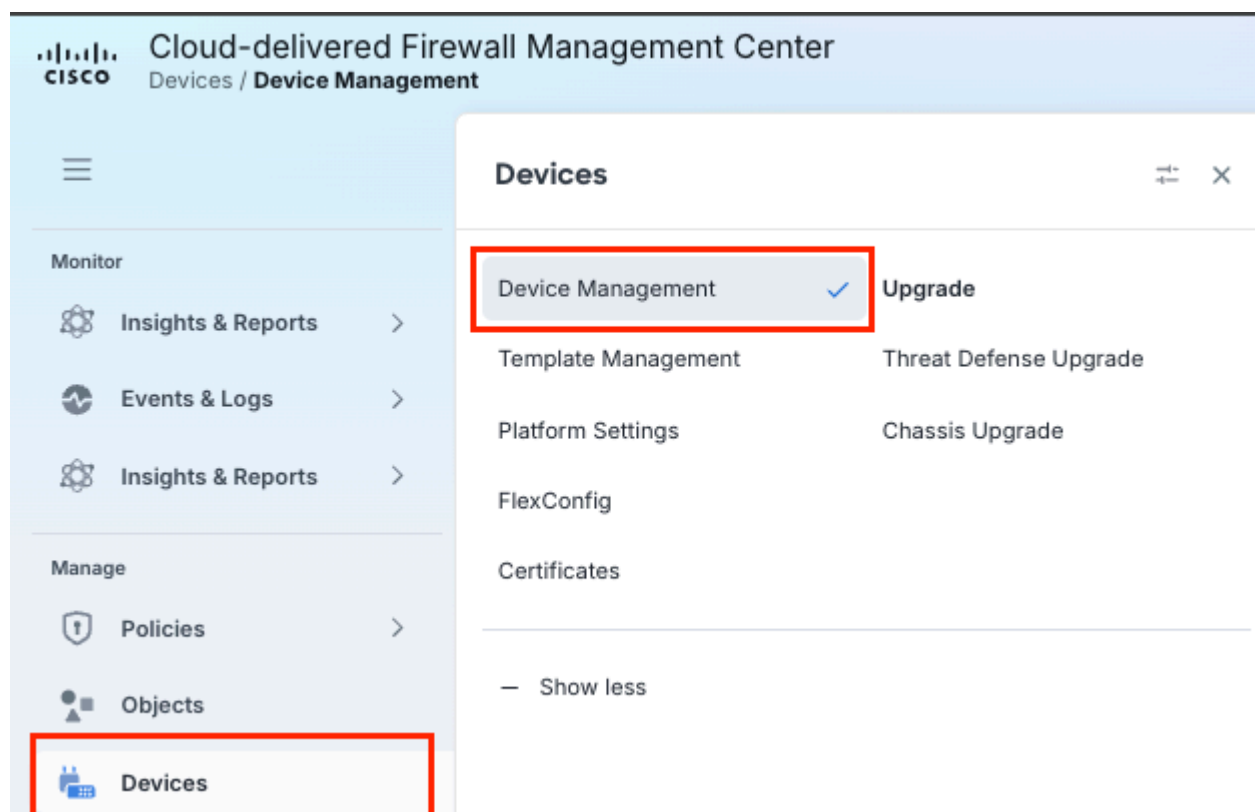
Links

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

With both tunnels active, the FTD needs ECMP routing so that traffic can use both paths at the same time, instead of treating the second tunnel as a passive standby.

Step 7: Configure ECMP

a) Navigate to **Manage > Devices > Device Management** and select the **FTD** configured with VPNs to Azure.



b) Click the **Routing** tab and choose **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

c) Click **Add** to create a new ECMP Zone.

Equal-Cost Multipath Routing (ECMP)

Add

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

d) Toggle to **highlight the VTIs** by clicking both VTIs in the **Available Interfaces** panel and click **Add** to apply the VTIs to the named ECMP Zone.

Add ECMP

Name

Azure-VTI-ECMP-Zone

Available Interfaces

Outside

DMZ

Inside

Add

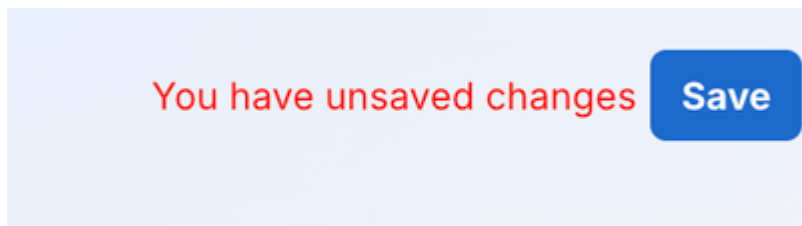
Selected Interfaces

Azure-VTI-0

Azure-VTI-1

Cancel OK

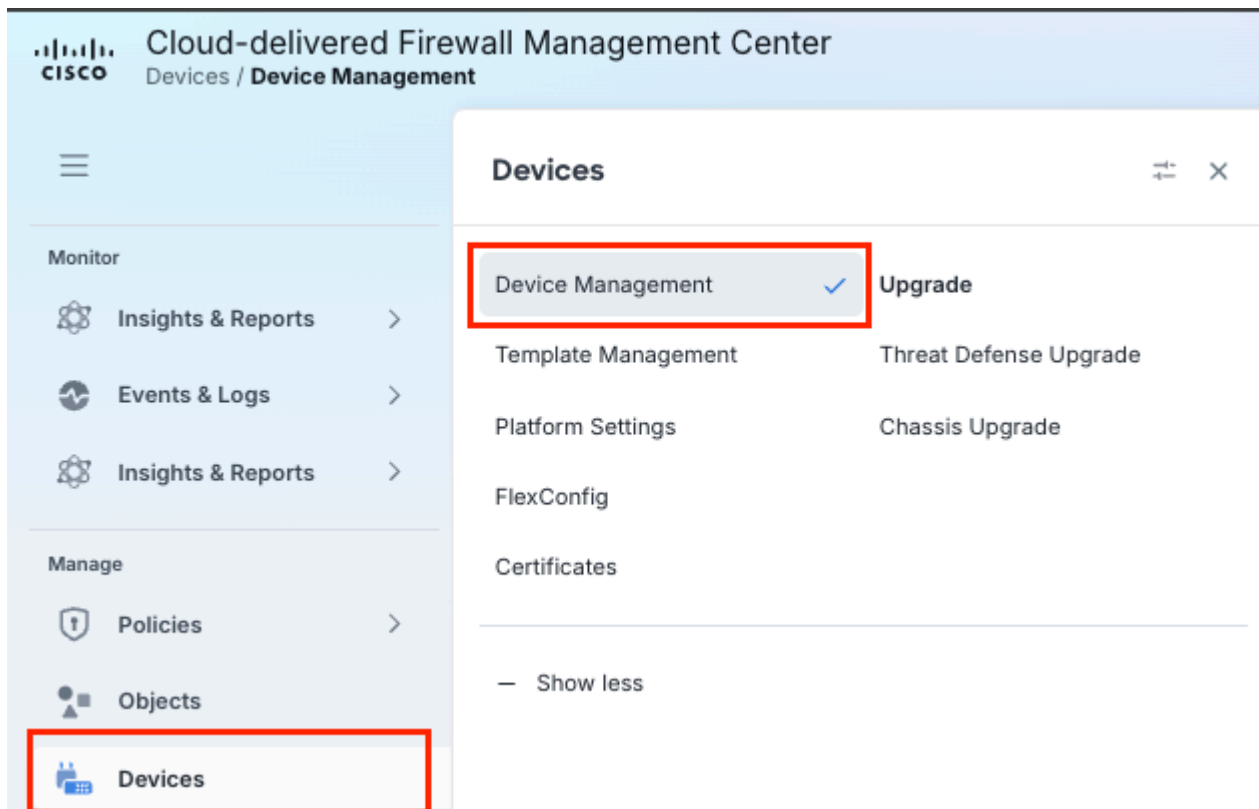
e) After you confirm that the settings are correct, click **Save**.



Step 8: Configure Static Routes to Instance Private IPs

BGP requires routes to successfully connect to neighbors, and because the endpoints are not directly connected, no routes are populated by default. ECMP allows you to configure static routes with the same metric (Administrative Distance) to the same destination, so that both routes are installed in the Routing Information Base (RIB) and used simultaneously.

a) Navigate to **Manage > Devices > Device Management** and choose the applicable **FTD device**.



b) Navigate to **Routing > Static Route**.

c) Click + **Add Route**.

d) Add routes for both Instance IP addresses by creating the first route to your **Instance0** VTI, and add the destination network object for it by clicking the + next to **Available Network**. Then, click the **network object** from the list and click the **Add** button to add it as the destination of the static route. Ensure that you choose the **Instance0** IP and it is set as the **Gateway**. Once complete, click **OK**.



Note: These static route destination network values are under `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` and `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` in the downloaded configuration file.

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

Selected Network

Azure-Instance0-BGP_Peer

Azure-Instance1-BGP_Peer

Add

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) Repeat steps c-d to add the second static route via the **Instance1** VTI. Ensure that you click **Save** to save your changes.

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						

Static routes only reach the BGP peering addresses; BGP itself must still be enabled and peered so that Azure and the FTD exchange routes dynamically to/from each others greater networks.

Step 9: Configure BGP

a) Enable BGP Process 65500 on FTD under **Routing > General Settings > BGP**. Check the **Enable BGP** check box, and enter the **AS number** configured earlier in Phase 2, Step 1. Navigate next to **Routing > BGP > IPv4**.

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) Enable IPv4 BGP routing for process/AS 65500 by checking the adjacent **Enable IPv4** check box, and click **Neighbor** to configure BGP neighbors.

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) Click + **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) Enter the **Instance0 BGP peering information**, reference the noted **BGP AS** from the vWAN hub and enter it as the **Neighbor Remote AS**, and add a **description** if desired. Click **Advanced**.



Important: Ensure that you change the BGP **Update Source** to reference the Loopback parent of both VTI interfaces on the FTD.

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

Update Source:
bgpVPNBranchLo

Description
Instance0 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

e) Within the **Advanced** menu of BGP **Neighbor** configuration on FTD, you can change the number of **TTL hops** from eBGP default of 1 hop to a variable number. Azure BGP endpoints are not directly

connected over the tunnel into Azure infrastructure, and there tend to be more hops to the endpoint than the default eBGP TTL of 1 permits.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Repeat same steps for Azure Instance1 BGP Peer.

Add Neighbor ?

IP Address*

10.2.0.13

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

Instance1 Azure BGP Peering

Update Source:

bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

☒ Allow connections with neighbor that is not directly connected

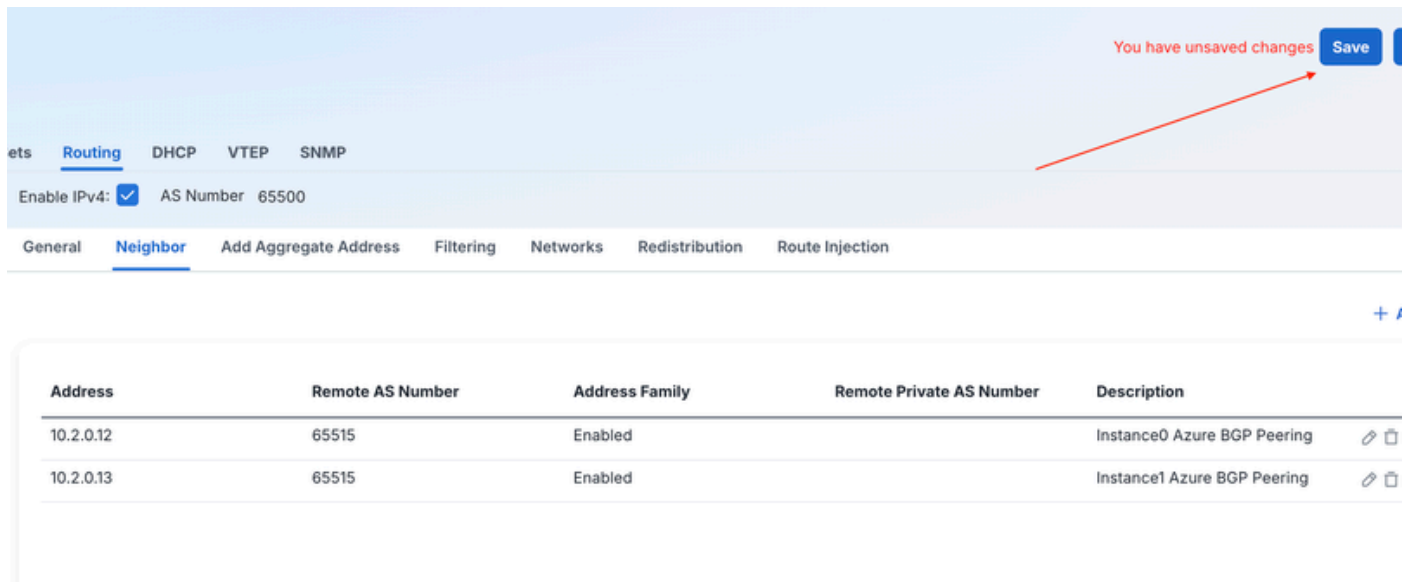
☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

g) Ensure that you **Save** changes once complete.



By default, BGP installs only a single best path in the routing table, even though ECMP makes both static routes available. BGP multipath must be enabled separately so that both learned paths are installed and used at the same time.

Step 10: Configure BGP Multi-path

a) Navigate to **Routing > BGP > IPv4**, click the **General** tab, and click the **pencil icon** adjacent to **Forward Packets Over Multiple Paths**.

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) Change the **Number of Paths** field default value from 1 to 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Ensure that you **Save** and deploy the changes.

Verify

After the deployment completes, confirm that BGP forms adjacencies with both Azure instances. Subsequently confirm that routes are learned over both tunnels, and that traffic uses both VTIs, using the same diagnostic CLI access established in Phase 3, Step 5.

Navigate to `system support diagnostic-cli` on FTD CLI.

a) Once deployed, BGP neighbors are expected to come up and prefixes are received.

```
<#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) Check that routes received from Azure show as multipath routes.

```
<#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) Check the VTI packet count.

<#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) Confirm static routes for BGP neighborships.

<#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) Confirm ECMP Zones.

<#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) Confirm BGP configuration.

<#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) Confirm Routing Table.

```
<#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
```

Other Considerations

The base configuration in this document assumes a single outside interface and a single ISP at the branch FTD. These considerations extend that design.

AS-Path Prepending

If you need to influence which of the two tunnels Azure or the FTD prefers as primary, rather than sharing load equally through ECMP and BGP multipath, prepend the local AS number one or more additional times on the BGP neighbor to be treated as secondary. The neighbor with the longer, prepended AS path is deprioritized during standard BGP best-path selection, without needing to remove that neighbor from the ECMP zone entirely.

Troubleshoot

- Phase 1/Phase 2 tunnel does not come up: Confirm that the pre-shared key and the IKEv2/IPsec policy parameters (encryption, integrity, PRF, DH group, and lifetime) match exactly between the FMC IKEv2 policy/IPsec proposal and the values in the downloaded Azure VPN configuration file. Use `show crypto isakmp sa` and `show crypto ipsec sa`, as shown in Phase 3, Step 5.
- Tunnel is up, but BGP neighbors do not form **update-source**: Verify that the BGP is set to the loopback interface, not the VTI itself, and that `ebgp-multihop` is configured with a value high enough to reach the Azure BGP peering address, which is not directly connected to the FTD.
- BGP forms, but only one tunnel carries traffic: Confirm that both VTIs are members of the same ECMP zone, that static routes to both Azure instance BGP addresses are installed with the same administrative distance, and that BGP multipath is configured for two paths, as described in Phase 3, Step 10.
- No return traffic, or asymmetric routing to Azure: Because Azure vWAN advertises the hub address space over both tunnels, ensure that ECMP is not disabled elsewhere in the routing configuration, and check for route maps or policy-based routing that could pin traffic to a single path.
- BGP is up and routes are installed, but traffic appears to be blocked: Ensure that you have Access Control rules configured with the Security Zone assigned to the VTIs allowing traffic to ingress and egress.

Related Information

- [What is Azure Virtual WAN?](#)
- [How to configure BGP for Azure VPN Gateway](#)
- [Default vs. Custom IPsec Policies Azure vWAN](#)
- [Troubleshoot BGP issues for Azure VPN Gateway](#)
- [About active-active mode VPN gateways](#)
- [Tutorial: Create a site-to-site connection using Azure Virtual WAN](#)