

Configure Azure Dual ISP vWAN Connectivity on Secure Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Diagram](#)

[Dual Direct Internet Access \(DIA\) Links \(Azure + FTD Load-Balancing/Redundancy\)](#)

[Configure](#)

[Phase 1: Azure vWAN VPN Site Configuration](#)

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

[Step 2: Configure Azure APIPA Gateway Parameters](#)

[Step 3: Configure Azure vWAN Site VPN Parameters](#)

[Step 4: Enable and Activate Custom BGP APIPA on VPN Site Link Instances](#)

[Step 5: Download VPN Site Configuration File](#)

[Phase 2: Configure FTD for Dual ISP Connectivity to Azure vWAN](#)

[Step 1: Analyze the Downloaded VPN Configuration](#)

[Step 2: Configure Link BGP Update Source Loopback Interfaces](#)

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

[Step 4: Configure Virtual Tunnel Interfaces \(VTI\)](#)

[Step 5: Provision IPsec VPN Topologies](#)

[Step 6: Validate VPN Topologies](#)

[Step 7: Configure ECMP](#)

[Step 8: Configure BGP](#)

[Step 9: Configure eBGP Multipath](#)

[Verify/Troubleshoot](#)

Introduction

This document describes how to configure Microsoft Azure Virtual WAN (vWAN) Site-to-Site VPN Connectivity to Secure Firewall using dual WAN links.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

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

Ensure that these components both initially configured in the Azure environment:

- Microsoft Azure vWAN Instance
- Microsoft Azure vWAN Hub

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
- Microsoft Azure vWAN

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

When the branch FTD has two Internet Service Provider (ISP)-facing outside interfaces, each one can connect redundantly and actively to Azure vWAN, so each ISP link is utilized. Azure vWAN creates two IPsec tunnels per Site Link — one to Azure Hub Instance0 and one to Instance1 — so each ISP interface terminates two tunnels. Across both ISP links, this results in four IPsec tunnels terminating on the FTD.

Azure Instances operate in Active/Active mode for load balancing and redundancy, so the FTD reflects this through Equal-Cost Multi-Pathing (ECMP) configuration across all four IPsec tunnels. Using custom Automatic Private IP Addressing (APIPA) addresses, external Border Gateway Protocol (eBGP) neighborships with distinct Private Autonomous System Numbers (ASNs) are established over each of the four tunnels. This enables BGP multipath functionality, providing multiple redundant paths to each Azure Hub Site Link pair of Instances.

Diagram

The diagram shows the topology of the configuration described in this article. The dual Direct Internet

Search Query For Virtual WAN

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

Select Existing Virtual WAN Hub

2) 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		

Create New Virtual WAN Site



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

3) 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 *	Dual-ISP-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.

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

Previous

Next : Links >

General VPN Site Configuration Settings

4) Enter the **required link information**. The Link BGP Address and the Link ASN are the inner-tunnel BGP Layer 3 destination address and BGP AS number on the branch side that the neighborship is formed with over the site-to-site tunnels. The Link BGP Address is a non-overlapping subnet address (/32) outside of the configured Hub private address space subnet, which Azure installs as a /32 route to reach as a BGP neighbor. Two loopback interfaces are created in later sections on the FTD to represent the Link BGP Address for each of the dual site links. The Link IP address/Fully Qualified Domain Name (FQDN) is the outer-header Layer 3 destination IP address of traffic going to the branch site necessary to provision IP Security (IPsec)/Internet Key Exchange version 2 (IKEv2) connectivity. Proceed to the next step when finished by clicking **Next : Review + create >**.



Note: Ensure to review specific Azure documentation if you are using addresses ranging from 169.254.21.0 to 169.254.22.255 for tunnel addresses: [Choosing BGP APIPA addresses.](#)

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

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

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

Previous

Next : Review + create >

Configure Site Link Parameters

5) Once the information is confirmed as intended, 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	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	

Links

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

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

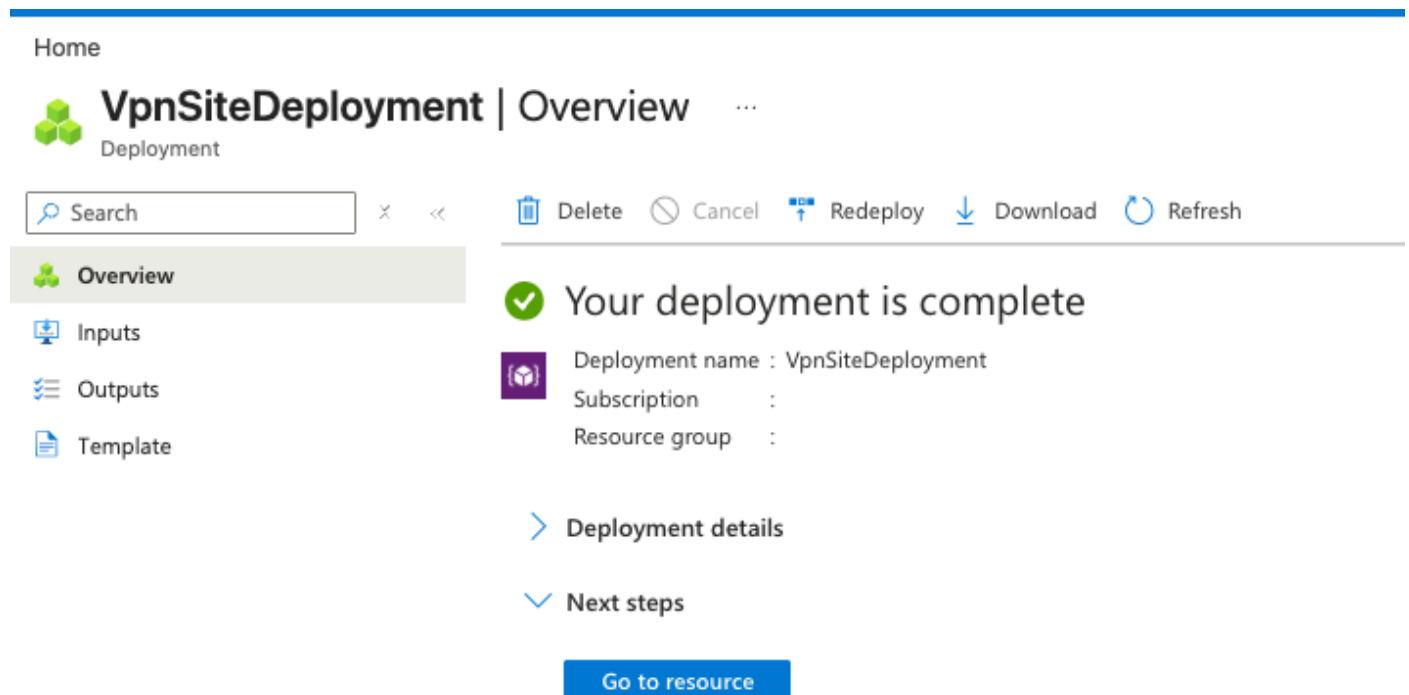
 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Create

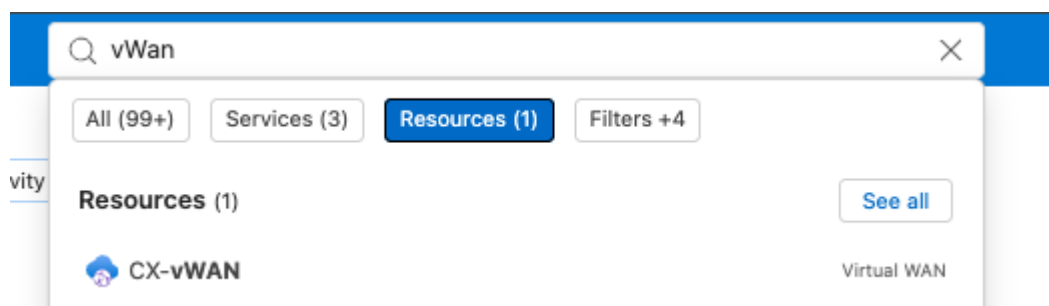
Previous

Next

6) Once deployment of the VPN site completes, navigate back to the **vWAN Hub configuration**.



Virtual WAN Site Deployment Progress



Search Query For Virtual WAN

Step 2: Configure Azure APIPA Gateway Parameters

Azure requires extra configuration for Automatic Private IP Addressing (APIPA) addresses within the 169.254.0.0/16 IPv4 address space.

1) Enter the existing hub via **Connectivity > Hubs**.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Navigate To Virtual WAN Hub Connectivity

2) Navigate once again to **Connectivity > VPN (Site to site)** and click the **Gateway Configuration** hyperlink.

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

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

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

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites 1

Access Gateway Configuration Hyperlink

3) A side panel appears to **Edit VPN Gateway**. Under VPN Gateway Instance0 and VPN Gateway Instance1, enter two **unique custom BGP IP addresses** that acts as neighbor IPs to each instance for BGP neighborships over the IPsec tunnels. This is necessary if you choose to use APIPA addressing within this topology. In the field labeled **Peer Address**, enter the **BGP neighbor IP** to use to reach the Azure Instances from the FTD. Azure does not attempt BGP establishment with the FTD if APIPA addressing is in use, hence the FTD attempts eBGP neighbor establishment over each tunnel with Azure.

The total comes out to 2 links x 2 implicit tunnels; one tunnel to Instance0 and Instance1 per ISP link; the total comes to four IPsec tunnels with BGP neighborships between Azure and the two FTD ISP interfaces.

These addresses must be unique, and in this demonstration, the second and final host address in the /30 subnets assigned to each tunnel is to be configured on the FTD for use. Once configured, click **Edit**.



Note: Ensure to review specific Azure documentation if you are using addresses ranging from 169.254.21.0 to 169.254.22.255 for tunnel addresses: [Choosing BGP APIPA addresses](#)

Edit VPN Gateway



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

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ

☒ Microsoft network ☐ Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



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

Edit

Cancel

Edit VPN Gateway Custom BGP IP Addresses



Note: As Azure notes, it is possible for this to take up to 30 minutes or more to update.

Step 3: Configure Azure vWAN Site VPN Parameters

1) On the **Connectivity > VPN (Site to site)** page within the Azure vWAN Hub configuration, and click the **X** to clear the **Hub Association: Connected** filtering to view disconnected VPN sites.

The screenshot shows the Azure vWAN Hub configuration page. The left sidebar has a red box around the 'Connectivity' section, which includes 'VPN (Site to site)'. The main content area shows the 'VPN Sites' tab with a search bar and a filter for 'Hub association: Connected'. A red arrow points to the 'X' icon next to the filter, indicating it should be clicked to clear the filter. Below the filter, there is a message: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Clear Hub Association Connection Filters

2) Check the check box next to the **recently provisioned VPN Site**, and click **Connect VPN Site**.

 Search

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

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

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

VPN Sites Metrics

 Search this page

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



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

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

Page: 1 ▼

Site name

↑↓ Location

  **Dual-ISP-Site**

Connect VPN Site Action

3) Configure the desired **Pre-Shared key (PSK)**, and configure desired **IPsec parameters** by clicking the **Custom** toggle option. These IPsec parameters must match on the FMC/FTD configuration in later steps. To save, click **Connect**.



Note: Diffie-Hellman (DH) Group 24 support was removed in FTD/FMC version 6.7.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

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

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

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

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

Connect

Configure Pre Shared Key And IPsec Parameters

4) Confirm VPN site provisioning completed successfully.

Notifications



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

[Dismiss all](#)



Successfully created VPN connection



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

a few seconds ago

Confirm VPN Site Provisioning Status

Step 4: Enable and Activate Custom BGP APIPA on VPN Site Link Instances

1) Refresh the **VPN (Site to site)** page and confirm the **Connection Provision status** column indicates its success, which enables you to click on the **ellipsis** and allows you to click the **Edit VPN connection to this hub** drop-down menu item.

Table with 5 columns: Site name, Location, Cloud provider, Connection Provisioning status, Connectivity status.

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

Validate Connection Success And Edit VPN Connection

2) Click to configure **Link Connection 1** (ISP1) and enter the applicable **Pre-Shared Key (PSK)** again, and ensure that you click the **Enable** toggle next to the **Custom BGP IP Address**, and map what would be the remaining host address of the /30 subnets that are going to be the inner-tunnel destination IP address field values of the BGP IP header generated by the FTDs.

In essence, ISP1 VTI Tunnel1 to Azure Instance0 has an address assignment of 169.254.21.1/30, and the second ISP1 VTI Tunnel2 terminating on the FTD has an IP of 169.254.22.1/30 assigned for Instance1.

Click **Next: Link Connection 2>** to proceed to ISP 2 link parameters.



Note: It is possible that you need to re-enter your PSK and re-click the aligned PFS Group option in the drop-down menu in Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

.....

Connection Mode ⓘ

Default Initiator Only Responder Only

Border gateway protocol ⓘ

Disable **Enable**

Custom BGP IP Addresses ⓘ

Disable **Enable**

Custom BGP IP Address

Instance 0 ⓘ

169.254.21.2

Instance 1 ⓘ

169.254.22.2

Use Azure Private IP Address ⓘ

Yes **No**

Protocol

IKEv2 **IKEv1**

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

Use policy based traffic selector ⓘ

Enable **Disable**

IPsec ⓘ

Default **Custom**

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

DPD timeout in seconds * ⓘ

45

Review + create

Previous

Next : Link connection 2 >

3) Repeat the previous steps and **apply the applicable parameters** under **Link Connection 2** (ISP2 link). Upon completion, click **Create**.

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

.....

Connection Mode ⓘ

Default Initiator Only Responder Only

Border gateway protocol ⓘ

Disable **Enable**

Custom BGP IP Addresses ⓘ

Disable **Enable**

Custom BGP IP Address

Instance 0 ⓘ

169.254.21.22

Instance 1 ⓘ

169.254.22.22

Use Azure Private IP Address ⓘ

Yes **No**

Protocol

IKEv2 IKEv1

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

Use policy based traffic selector ⓘ

Enable **Disable**

IPsec ⓘ

Default **Custom**

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

DPD timeout in seconds * ⓘ

45

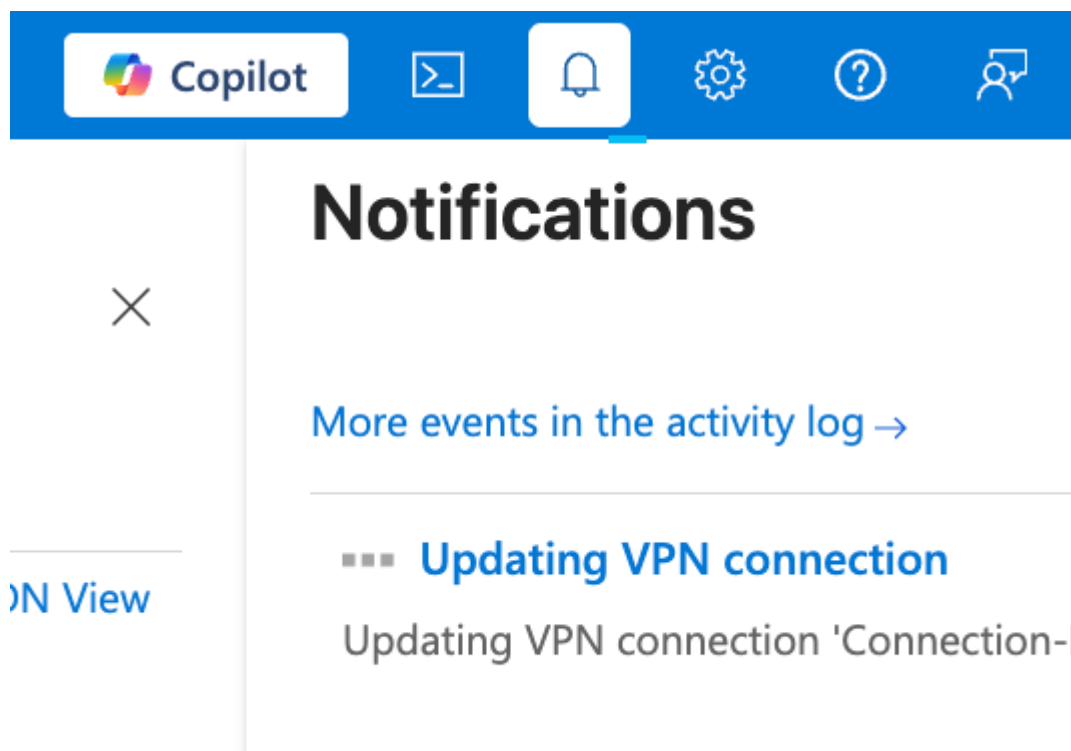
Create

Previous

Next

Configure Link Connection Two Custom BGP Settings

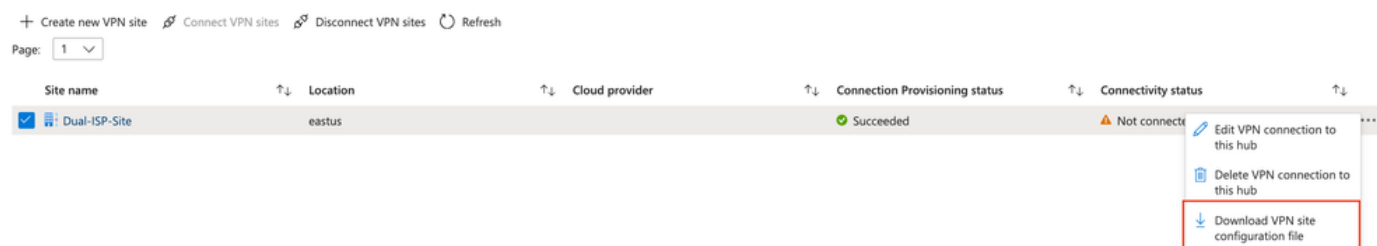
4) Notifications in Azure UI show the update task commencing.



Azure Update Task Commencement Notification

Step 5: Download VPN Site Configuration File

1) In the same **VPN (Site to site)** page in Azure, choose the **ellipsis icon** on the far right of the configured VPN site and choose the **Download VPN site configuration file** option.



Download VPN Site Configuration File Option

2) Click the **Click here to download** hyperlink.



Download Site-to-Site VP...



Dual-ISP-Site



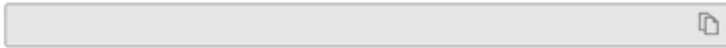
Create new



Use existing



The file is ready to download



[Click here to download](#)



Download VPN Site Configuration File

Phase 2: Configure FTD for Dual ISP Connectivity to Azure vWAN

Step 1: Analyze the Downloaded VPN Configuration

1) Open the **downloaded configuration file** and a similar JavaScript Object Notation (JSON) output appears. The output shows one of the two objects written in the file. This information provides helpful context for FTD configuration.



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



Note: ISP-Link-1 JSON object ordering in the downloaded file is reversed. Ellipsis in the code output represents the ISP-2-Link object with its applicable configuration.

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

```

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

```

Keep this output as reference as you complete the steps.

Step 2: Configure Link BGP Update Source Loopback Interfaces

BGP neighbor configuration entries under the FTD BGP process (configured in later steps on the FTD) need a stable source representing the corresponding Link BGP IP Address in Azure Site Link configuration.

1) 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

Navigate To Device Management On Firepower Management Center



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

2) Click on the **FTD** you are configuring as the branch/site VPN device with dual ISP connectivity.

N/A - ROUTED		
☐	✓ CXvWAN-FTD-2 N/A - ROUTED	10.0.0

Select The FTD For Configuration Deployment

3) Click the **Add Interfaces** drop-down menu, and click **Loopback Interface**.

CXvWAN-FTD-2
Cisco Secure Firewall Threat Defense for AWS

Device **Interfaces** Inline Sets Routing DHCP VTEP

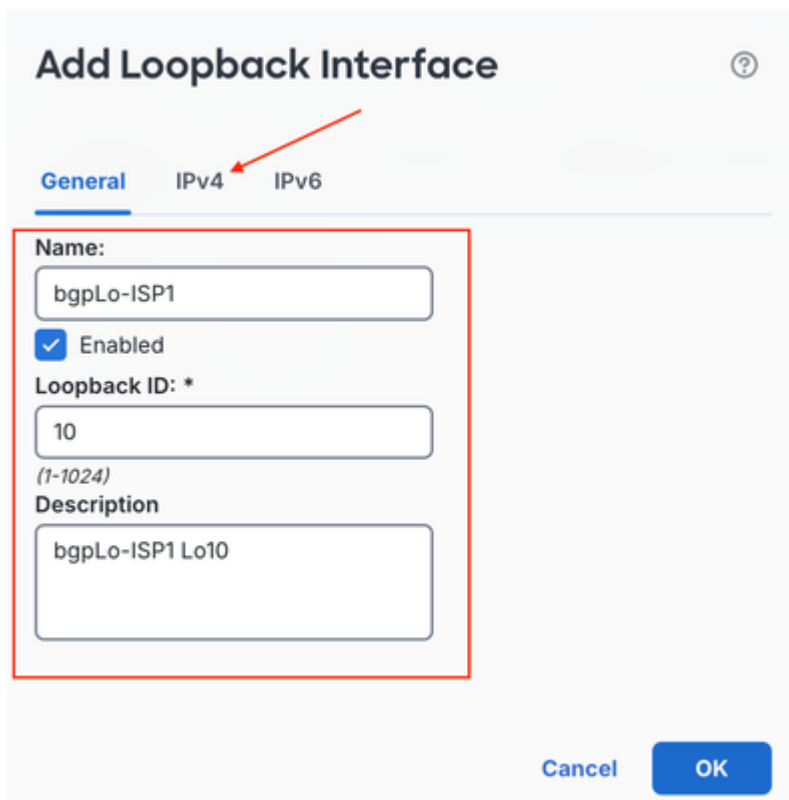
Interfaces Virtual Tunnels

Search by name Sync Interface Add Interfaces

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

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

4) Enter a **Name** of the loopback interface, ensure to check the **Enabled** check box, and enter a **Loopback ID**. Enter a **Description** if desired. Once complete, click the **IPv4** tab.



The screenshot shows the 'Add Loopback Interface' dialog box with the 'General' tab selected. A red box highlights the configuration fields: 'Name' (bgpLo-ISP1), 'Enabled' (checked), 'Loopback ID' (10), and 'Description' (bgpLo-ISP1 Lo10). A red arrow points to the 'IPv4' tab.

5) Enter the loopback **IP address** to be the Link BGP IP address configured in earlier steps for the ISP1 site link in Azure. This IP is used as the BGP update source on the neighborships configured between the FTD and Azure Instances over ISP1.



Note: You can reference the value previously defined in the downloaded VPN config JSON under `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress` for ISP1

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](#)

Enter Loopback IPv4 Address And Hit OK

6) Repeat sub-steps c-e in this sequence for the ISP2 BGP Loopback configuration.

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

Create First And Second Loopback Interfaces

7) **Save** your configuration.

You have unsaved changes [Save](#) [Cancel](#)

Save Changes

Step 3: Configure Phase 1/Phase 2 Policy Objects

1) To configure matching IKEv2/IPsec configuration on the FMC to FTD VPN topologies, navigate to **Manage > Objects**, scroll in the navigation 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**.

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

Filter

Name	
AES-GCM-NULL-SHA	Q ☐ ⚙
AES-GCM-NULL-SHA-LATEST	Q ☐ ⚙
AES-SHA-SHA	Q ☐ ⚙
AES-SHA-SHA-LATEST	Q ☐ ⚙
DES-SHA-SHA	Q ☐ ⚙
DES-SHA-SHA-LATEST	Q ☐ ⚙
Umbrella-AES-GCM-256	Q ☐ ⚙

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

Create New IKEv2 Policy Object

2) Enter a **name** for the new **IKEv2 Policy**, choose **Priority** and/or **Lifetime**. Ensure the policy matches on both ends of the tunnel regarding **Integrity, Encryption, Pseudo Random Function (PRF), and DH Group**. Choose which **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:*

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

Selected Algorithms

Add

SHA256

Cancel

Save

3) Once configuration is done, click **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

Add

Selected Groups

14

Cancel Save

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

IKEv2 IPsec Proposal

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

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

Add IKEv2 IPsec Proposal

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

Edit IKEv2 IPsec Proposal

Name:*
Azure_IPsec

Description:

ESP Hash
ESP Encryption

Available Algorithms
AES-GCM-256
AES-256
AES-GCM-192
AES-192
AES-GCM
AES
3DES
DES

Add

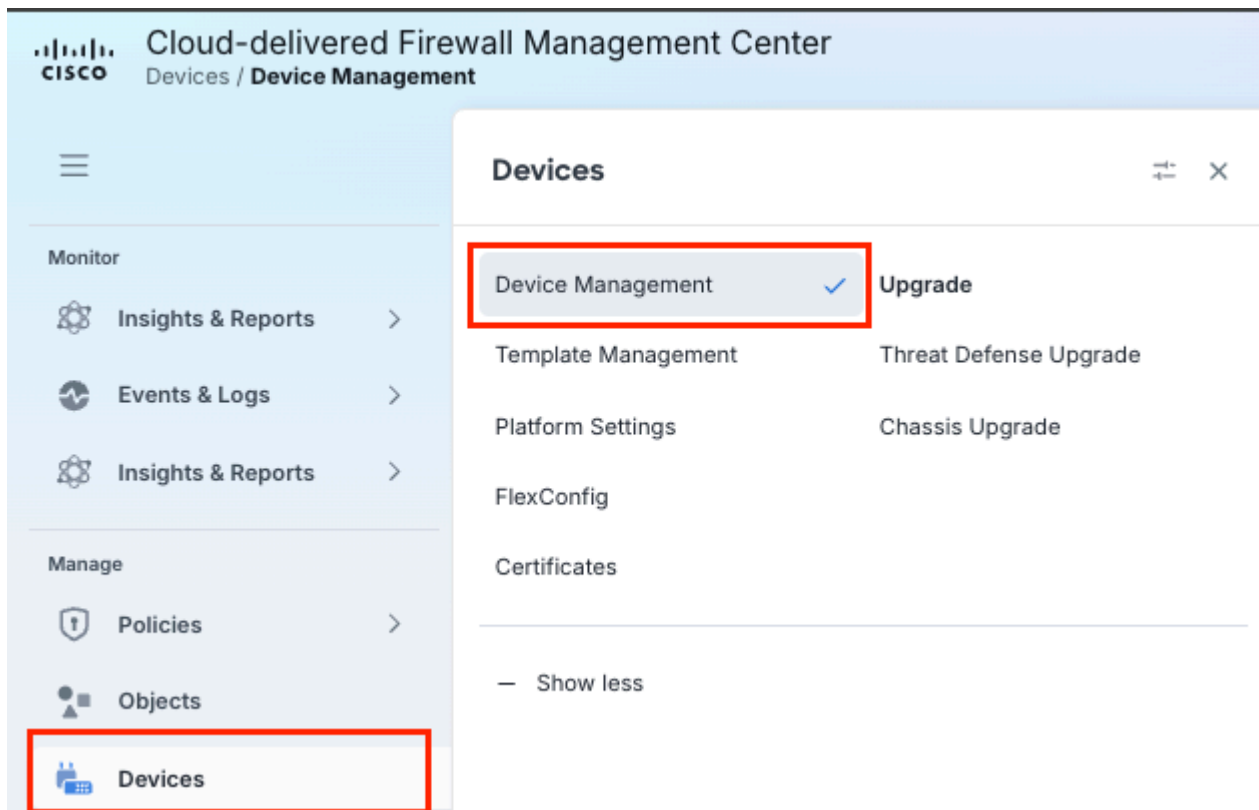
Selected Algorithms
AES-GCM-256

Cancel Save

Name IKEv2 IPsec Proposal And Click Save

Step 4: Configure Virtual Tunnel Interfaces (VTI)

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



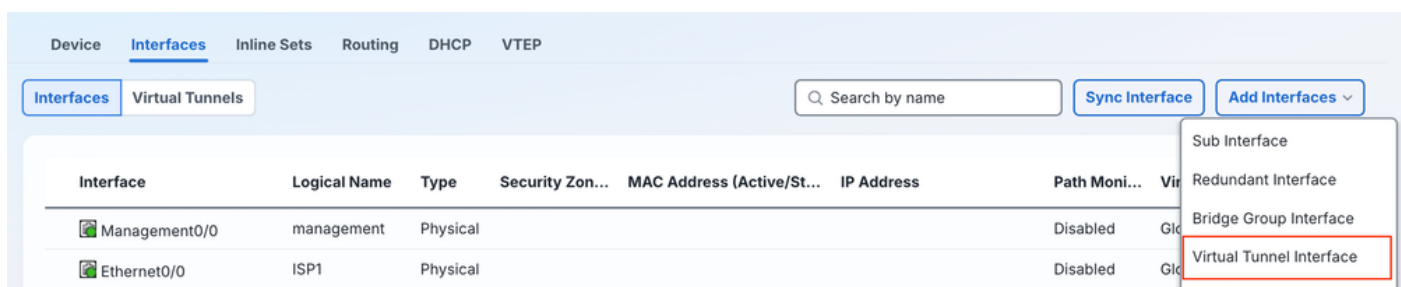
Navigate To Device Management On Firepower Management Center

- 2) Click the **FTD** you are configuring as the branch/site VPN device with dual ISP connectivity.

	✓ CXvWAN-FTD-2 N/A - ROUTED	10.0.0
---	---	-------------------

Select The FTD For Configuration Deployment

- 3) Click the **Add Interfaces** drop-down menu and choose **Virtual Tunnel Interface (VTI)**.



Create Virtual Tunnel Interface

- 4) Enter the **tunnel information**. Ensure the **Enabled** check box is checked, **Name** is entered (**Description** as well, if desired), and optional **Security Zone** is chosen. Align the correct parent ISP-facing interface to configure the VTI under, and configure the appropriate **IP address** for the inner-tunnel IPsec connectivity for the VTI. Hit **OK** when complete.



Tip: Reference diagram shows further context on potential VPN configuration for Azure dual-

WAN connectivity with FTD.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

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

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



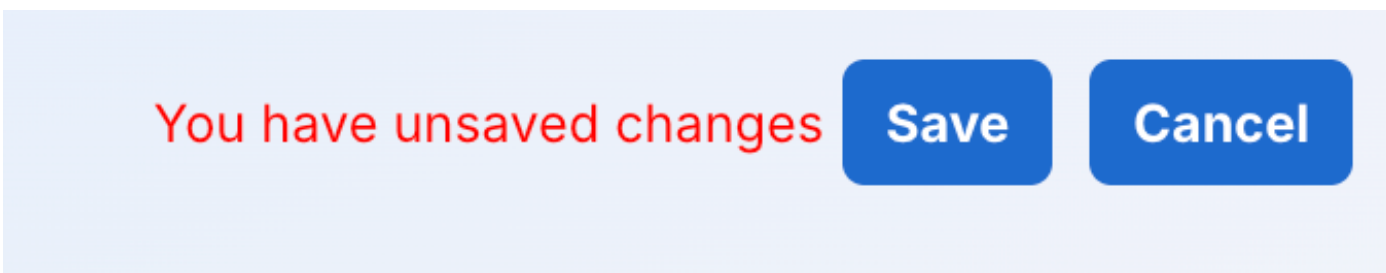
Cancel

OK

5) Configure **3 additional VTIs** across parent ISP1 and ISP2 Interfaces.

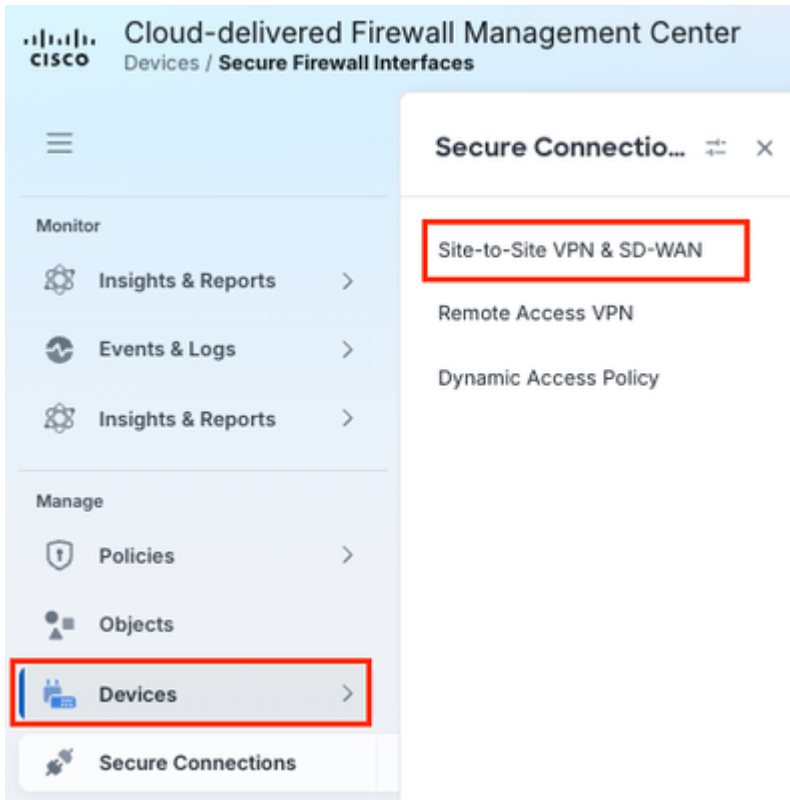
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
Ethernet0/0	ISP1	Physical				Disabled	Global
Tunnel1	ISP1-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.1/30(Static);	Disabled	Global
Tunnel2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

f) Ensure to click **Save** to save your changes.



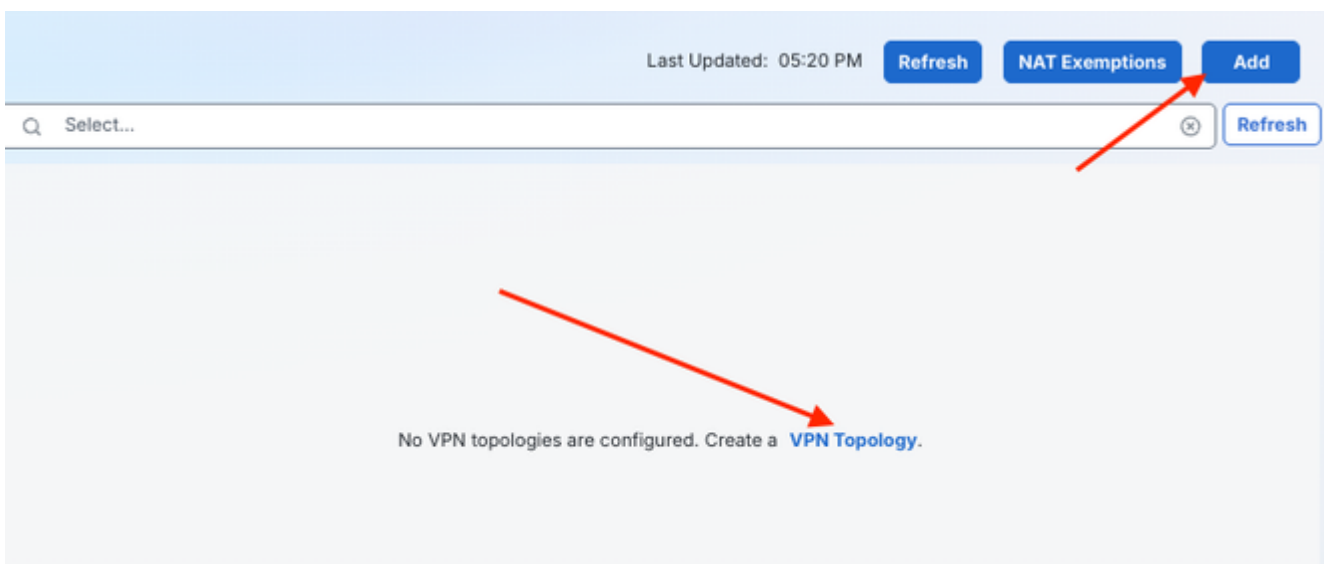
Step 5: Provision IPsec VPN Topologies

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



Manage Site To Site VPN And SD-WAN Connections

2) Click either the initial **VPN Topology** configuration hyperlink in the middle of the initial output, or click the **Add** button.



Add New VPN Topology Configuration

3) Enter a **Topology name** for the first tunnel over ISP1 link 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 *
 CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

☐ SD-WAN Topology New

Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ Hub and Spoke

[Prerequisites](#)

☒ **Route-Based VPN**

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ Peer to Peer

☐ Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

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

[Prerequisites](#)

[Refresh](#)

[Cancel](#) [Create](#)

Configure Route Based VPN Topology Type

4) First, choose the **Node A** device and under the **Device** drop-down list signifying the FTD terminating the VPN tunnels from Azure. After the wizard fetches the available VTIs from the device, select the **VTI** appropriate to the parent interface and instance you are configuring from the drop-down menu. From the **Node B Device menu**, choose the Azure side to be the **Extranet** node in the VPN topology configuration. Ensure that you configure a **friendly name** for Node B, as well as ensuring to enter the appropriate **Endpoint IP Address**. Once complete, click the **IKE** tab to implement Phase 1 tunnel configuration.



Note: You can reference Instance **Endpoint IP Address** values in the downloaded configuration file at `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` and `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Node B

Device:*

CXvWAN-FTD-2

Virtual Tunnel Interface:*

ISP1-Inst-0 (IP: 169.254.21.1)



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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

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

Additional



Device:*

Extranet

Device Name:*

Azure-ISP1-Link-Inst0

Endpoint IP Address:*

Cancel

Save

Define Node A And Node B Topology Endpoints

5) Scroll in the navigation menu to **IKEv2 Settings** and click the **pencil icon** to edit the policies to the recently configured IKEv2 Policy. Next, choose the **Pre-shared Manual Key** option from the **Authentication Type** drop-down menu, and enter the PSK previously configured in Azure. Once complete, click the **IPsec** tab to configure Phase 2 IPsec tunnel parameters.



Note: You can reference the pre-shared key in the downloaded configuration file at `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology

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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Azure_IKEv2 

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

Edit IKEv2 Settings And Authentication Key

6) Click the **pencil icon** adjacent to the **IKEv2 IPsec Proposal Transform Set**, and choose the previously configured **IPsec policy parameters**. Ensure to change the **Lifetime Duration** value to match Azure vWAN VPN settings. Once configured information is confirmed, 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:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals* 

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)



Configure IPsec Proposal Lifetime Duration

7) Repeat the previous sub-steps within Step 5 to create the other Azure Tunnels across ISP1 Instance1, ISP2 Instance0, and ISP2 Instance1.

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

Create Additional Site To Site VPN Topologies

Step 6: Validate VPN Topologies

Enter into **system support diagnostic-cli**, type **en** and hit enter (read-only CLI).

1) Check IKE Phase 1 Tunnel connectivity.

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

2) Check IPsec Phase 2 connectivity.

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



Note: When viewing IPsec Security Associations (SA) output and pkts decaps and pkts decrypt counters are incrementing, but pkts encaps and pkts encrypt are not, this is expected in this scenario. Azure is trying to form BGP neighborships over the Hub Private IP Space addresses, and Azure does not initiate negotiation if the neighboring end uses APIPA BGP addressing. It is the responsibility of the device connecting to Azure to initiate BGP negotiation when custom APIPA is used.

3) Check Layer 2 Connectivity.

```
show arp
```

4) Check IP Routing.

```
show route
```

5) Perform Capture on ISP1 and ISP2 interfaces.

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

6) Azure Verification - Navigate to **vWAN Hub > Connectivity.> VPN Sites > Choose the site configured.**

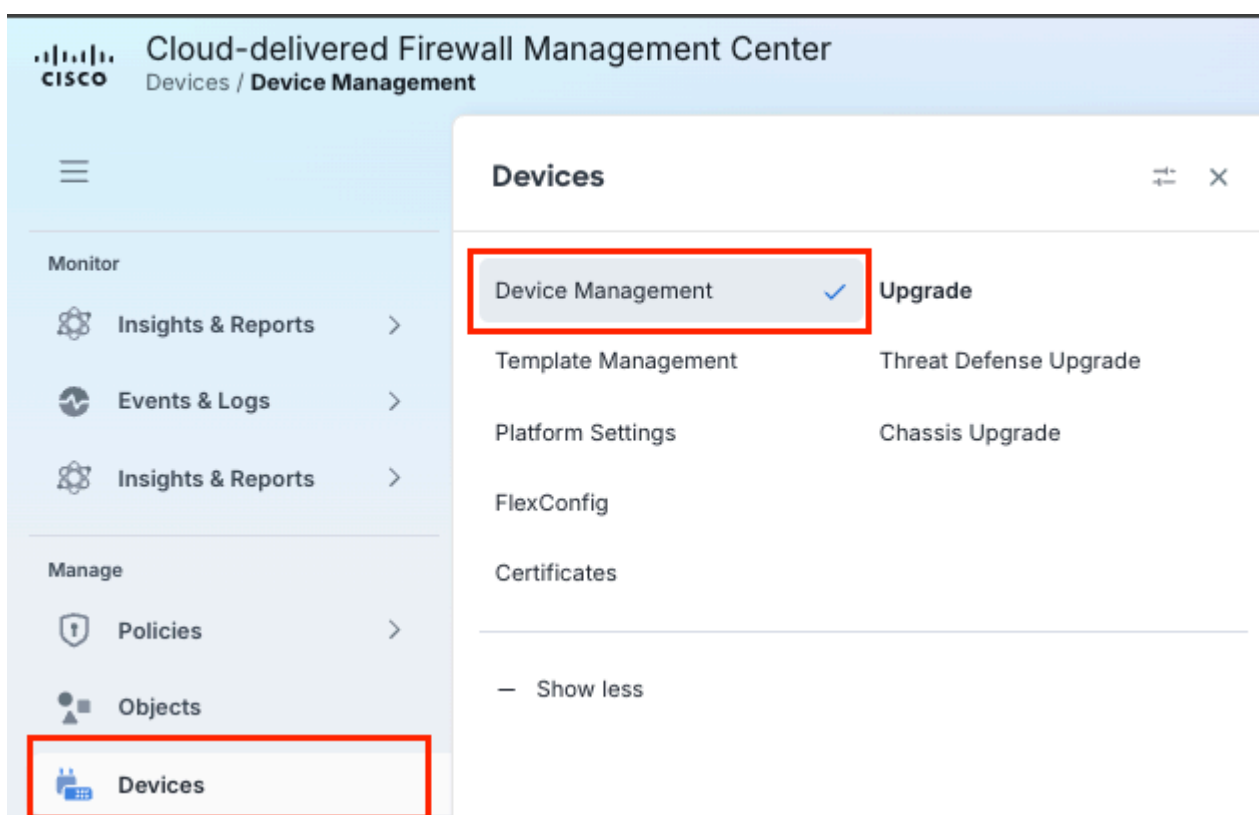
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ ISP-1-Link	ISP1	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub
☐ ISP-2-Link	ISP2	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Azure Link Connectivity Verification

Step 7: Configure ECMP

1) Navigate to **Manage > Devices > Device Management** and click the **FTD**.



Navigate To Device Management On Firepower Management Center

N/A - ROUTED		
☐	☒ CXvWAN-FTD-2 N/A - ROUTED	10.0.0

Select The FTD For Configuration Deployment

2) 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

Equal Cost Multi Path Configuration Settings

3) Click **Add**.

Equal-Cost Multipath Routing (ECMP)

Add

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

Add Equal Cost Multi Path Configuration Settings

4) Name the **ECMP Zone**, and click the available **VTI Interfaces**, then click the **Add** button to apply them to the **Selected Interfaces** column and click **OK**.

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

Select Interfaces For Equal Cost Multi Path Zone

5) Ensure to **Save** your changes.

You have unsaved changes

Save

Cancel

Save Changes

Step 8: Configure BGP

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

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

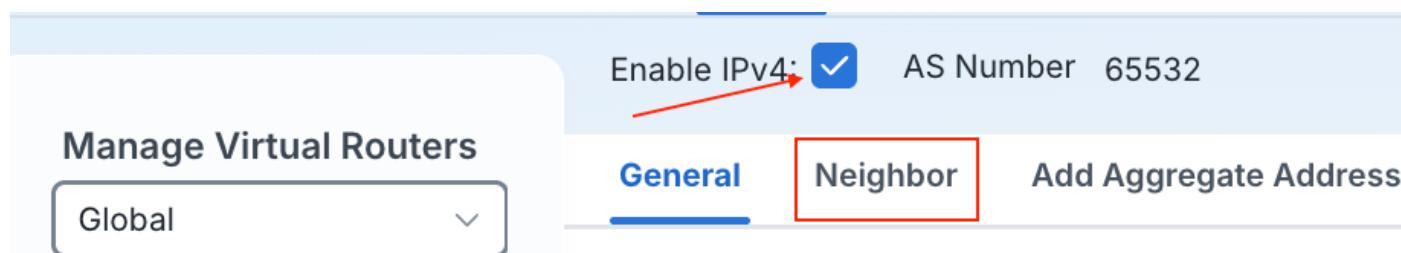
Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

2) Ensure to check the **Enable IPv4** checkbox for the BGP process, and click **Neighbor** to configure BGP neighbors in Azure.



Manage Virtual Routers

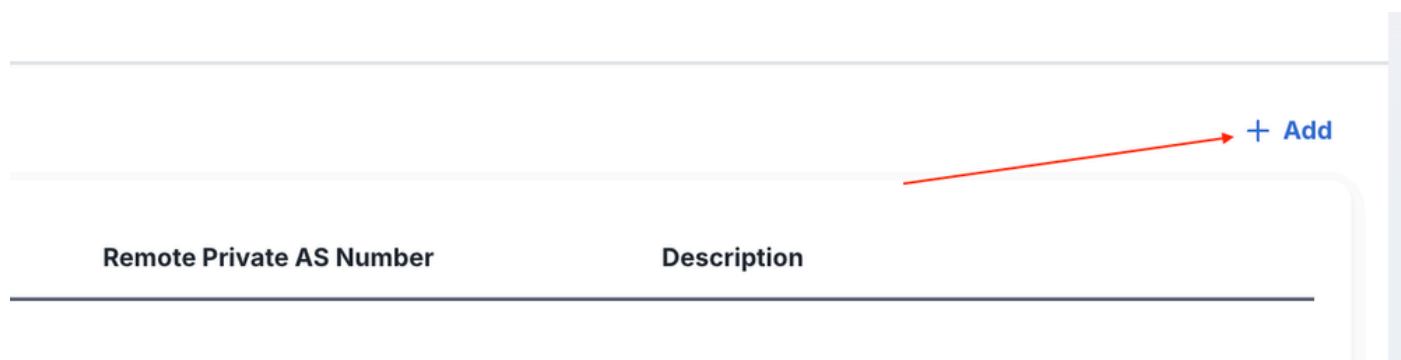
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

Enable IPv4 Border Gateway Protocol Process

3) Click + **Add**.



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

+ Add

Add New Border Gateway Protocol Neighbor

4) Enter the **ISP1 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**.



Note: Ensure that you choose the BGP **Update Source** to reference the Loopback for VTI interfaces on the FTD mapped to the ISP1 Link configured in Azure.

Add Neighbor

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Configure Border Gateway Protocol Peering Information

5) Within the **Advanced** menu of BGP **Neighbor** configuration on FTD, you can change the number of **Time To Live (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. Click **OK**.

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Advanced Border Gateway Protocol Neighbor Settings

6) Repeat sub-steps 3-5 to configure Tunnel2 for ISP1 Instance1.

7) Repeat sub-steps 3-5 twice to configure the **ISP2 Instance0/Instance1 BGP peering information.**



Note: Ensure that you choose the aligned BGP **Update Source** referencing the Loopback for VTI interfaces on the FTD mapped to the ISP2 Link configured in Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

ISP2 Instance 1 BGP Neighbor Configuration

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

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

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

- ☐ Enable Authentication
- Enable Encryption

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

10

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

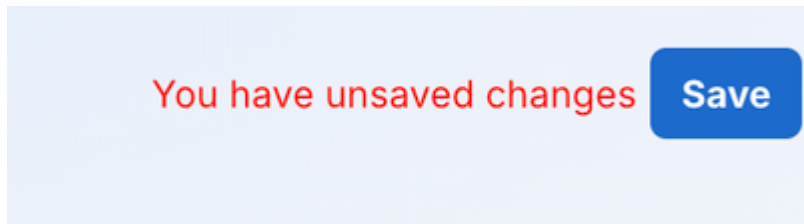
Cancel

OK

ISP 2 Instance 2 BGP Neighbor Configuration

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

Once complete, click **Save**.



Save Changes

By default, BGP installs only a single best path in the routing table, even though ECMP is configured across all VTIs to Azure. BGP multipath must be enabled separately so that both learned paths are installed and used at the same time.

Step 9: Configure eBGP Multipath

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

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

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

General Settings

BGP

General

Neighbor Add Aggregate Address Filtering Networks Redistribution Routes

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

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

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

Forward Packets Over Multiple Paths Setting

2) Change the **Number of Paths** field default value from **1** to **4**. Click **OK**.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Change Forward Packets Over Multiple Paths Setting

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

Verify/Troubleshoot

After the deployment completes, confirm that the FTD BGP process establishes neighbor adjacencies with both Azure instances on the respective tunnels, and that routes are learned, interfaces are up, and protocol connections are returned in the connection table.

Navigate to `system support diagnostic-cli` on FTD CLI as done in Phase 2, Step 7.

1) 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#
```

```
ftd#
```

```
show bgp summary
```

```
BGP router identifier 169.254.22.100, local AS number 65532
```

```
BGP table version is 29, main routing table version 29
```

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

```
8 path entries using 640 bytes of memory
```

2 multipath network entries and 8 multipath paths
 1/1 BGP path/bestpath attribute entries using 208 bytes of memory
 1 BGP AS-PATH entries using 24 bytes of memory
 0 BGP route-map cache entries using 0 bytes of memory
 0 BGP filter-list cache entries using 0 bytes of memory
 BGP using 1272 total bytes of memory
 BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

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

2) Check that routes received from Azure show as **multipath routes**.

<#root>

ftd#

show bgp

BGP table version is 29, local router ID is 169.254.22.100
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i
*m 172.27.0.0	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i

3) Check **routing table population**.

<#root>

ftd#

show route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, + - replicated route
 SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 172.31.3.33 to network 0.0.0.0

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

4) Check connection table for BGP sessions.

<#root>

ftd#

show conn all | include TCP|179

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