

Configuración de VPN sitio a sitio de Azure vWAN para Secure Firewall

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama](#)

[Conectividad vWAN de enlace DIA único entre Azure y FTD \(Azure Load-Balancing/Redundancy\)](#)

[Configurar](#)

[Fase 1: Configuración de Azure vWAN/Hub](#)

[Paso 1: Crear vWAN](#)

[Paso 2: Crear hub vWAN](#)

[Fase 2: Configuración del sitio VPN de Azure vWAN](#)

[Paso 1: Crear sitio VPN de Azure vWAN \(dispositivo FTD remoto\)](#)

[Paso 2: Configurar parámetros VPN de sitio de Azure vWAN](#)

[Paso 3: Descargar configuración de túnel de sitio de Azure vWAN](#)

[Fase 3: Configuración de FTD](#)

[Paso 1: Analizar configuración de VPN de Azure](#)

[Paso 2: Configurar loopback](#)

[Paso 3: Configuración de objetos de política de fase 1/fase 2](#)

[Paso 4: Configurar la conectividad segura a Azure](#)

[Paso 5: Verificar conectividad inicial con Azure](#)

[Paso 6: Configuración del segundo túnel al punto final Azure Instance1](#)

[Paso 7: Configuración de ECMP](#)

[Paso 8: Configuración de Rutas Estáticas para IP Privadas de Instancia](#)

[Paso 9: Configuración de BGP](#)

[Paso 10: Configuración de BGP Multi-Path](#)

[Verificación](#)

[Otras consideraciones](#)

[AS-Path Prepending](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de la conectividad VPN de sitio a sitio de Microsoft Azure Virtual WAN (vWAN) a Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure FTD versión 10.0
- Cisco Secure FMC Versión 10.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La WAN virtual (vWAN) de Microsoft Azure combina varias capacidades de red, seguridad y routing de Azure en una única construcción de concentrador. Cada vWAN Hub puede alojar un gateway VPN de sitio a sitio administrado por Microsoft que los dispositivos remotos, como Secure Firewall, utilizan para llegar a Azure sin tener que crear y mantener la infraestructura del gateway.

A diferencia de una VPN IPsec convencional de dos terminales, el gateway VPN sitio a sitio de Azure vWAN se implementa como un par de instancias activo-activo (Instance0 e Instance1), cada una con su propia dirección IP pública y dirección de iguales BGP (Border Gateway Protocol). Para aprovechar ambas instancias para obtener redundancia y rendimiento adicional, el FTD de sucursal establece un túnel de seguridad IP (IPsec) para cada instancia y utiliza BGP, en lugar de ruteo estático solo, para aprender dinámicamente y retirar rutas a medida que las

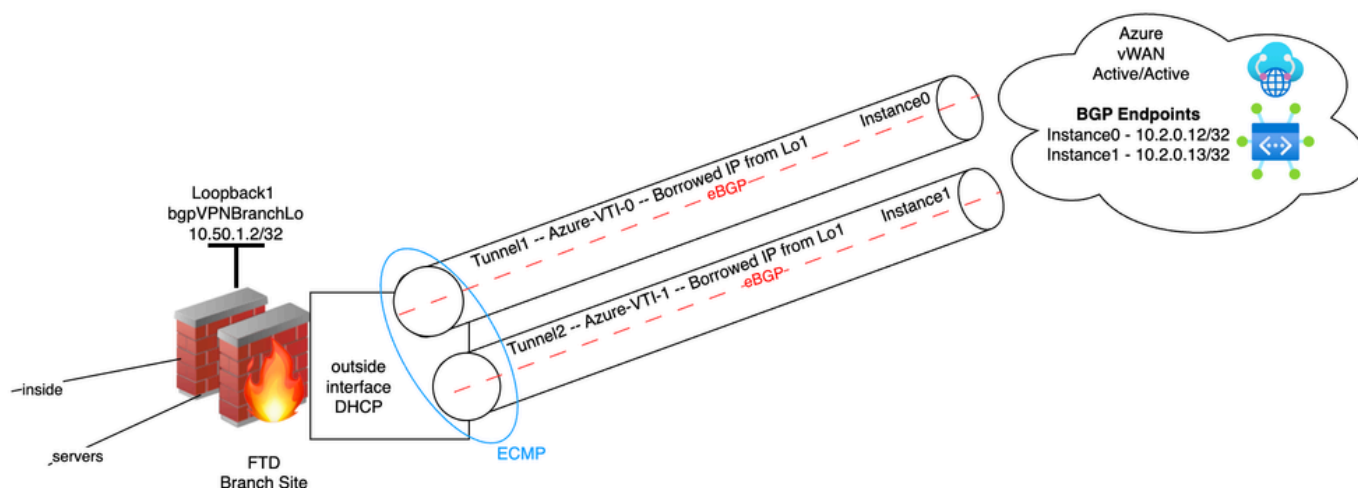
instancias estén disponibles o no estén disponibles. El routing de múltiples rutas de igual coste (ECMP) y las múltiples rutas BGP en el FTD mantienen ambos túneles activos al mismo tiempo, en lugar de tratar uno como un modo de espera pasivo.

Este documento configura ese diseño en tres fases: Los objetos de Azure vWAN Hub y VPN Site se crean en primer lugar, se descargan los parámetros de conexión resultantes y, a continuación, se utilizan esos mismos parámetros para configurar las interfaces de túnel virtual (VTI), las políticas IPsec, las rutas estáticas, ECMP y el modelo de iguales BGP que coincidan en el FTD a través de FMC.

Diagrama

El diagrama muestra la topología de la configuración descrita en este artículo. La única variante Direct Internet Access (DIA) origina ambos túneles de Azure desde una interfaz externa en el FTD.

Conectividad vWAN de enlace DIA único entre Azure y FTD (Azure Load-Balancing/Redundancy)



Configurar

Complete las tres fases en orden. Los objetos del lado de Azure creados en la Fase 1 y la Fase 2 producen las direcciones IP del peer, los números del Sistema Autónomo BGP (AS) y la clave previamente compartida que la Fase 3 aplica al FTD.

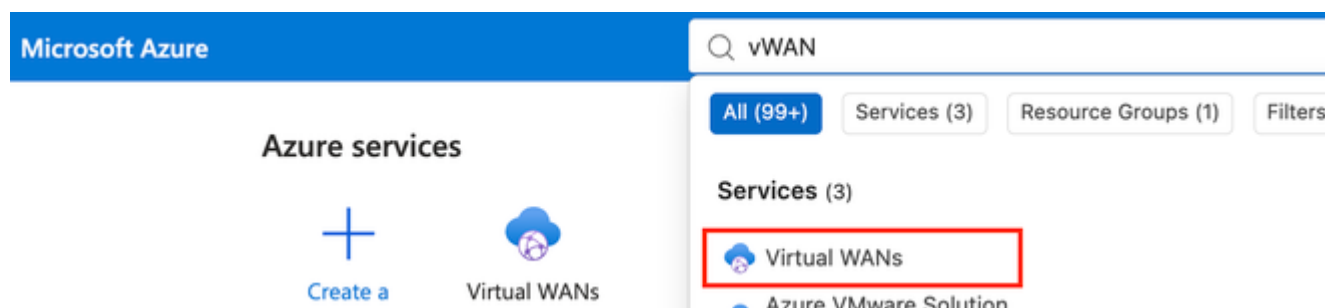
Fase 1: Configuración de Azure vWAN/Hub



Nota: Los pasos de configuración de este documento son de alto nivel y proporcionan los pasos necesarios para conectar el FTD a Azure vWAN. Consulte la documentación de Azure vWAN de Microsoft para comprender la importancia de las configuraciones. Vea [¿Qué es la WAN virtual de Azure?](#) y más documentación.

Paso 1: Crear vWAN

a) Busque vWAN en el cuadro de búsqueda de Azure, haga clic en Virtual WANs.



b) Haga clic en + Crear.



c) Introduzca un nombre para la nueva instancia de vWAN, haga clic en Revisar + crear y, a continuación, haga clic en Crear en la página Revisar + Crear del asistente.

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 >



Nota: El espacio en blanco que cubre los valores de varios campos de las imágenes es intencional para la publicación de este documento.

d) Haga clic en Ir al recurso.



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

Paso 2: Crear hub vWAN

a) Navegue hasta Conectividad > Hubs y haga clic en + Nuevo 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) Consulte la documentación de Azure para obtener más contexto sobre la configuración adicional. Asegúrese de que el espacio de dirección privada del Hub asignado no se superponga a ninguno de los espacios de dirección interna. Configure Name, Virtual Hub, Hub routing preference. Haga clic en Next (Siguiente): De sitio a sitio >.

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 (vpsite). [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) Consulte la documentación del Microsoft Azure vWAN Hub para obtener información sobre los campos presentados. Active Yes para crear una puerta de enlace de sitio a sitio (VPN Gateway). El número de sistema autónomo (AS) BGP predeterminado asignado es 65515, según lo asignado por el Grupo de trabajo de ingeniería de Internet (IETF) en la solicitud de comentarios (RFC) 6996 que define la reserva AS de uso privado.



Nota: Registre el AS BGP para los pasos de configuración futuros en el 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 >

Haga clic en Review + create, o haga clic en Next : Señale sitio > para configurar los parámetros opcionales.

d) Una vez verificado el resumen, haga clic en Create.



Nota: Como indica Azure, la creación del hub tarda 30 minutos.

Create virtual hub ...

✓ Validation passed

Basics 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

Tags

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

Create

Previous

Next

[Download a template for automation](#)

e) Una vez finalizada la implementación, busque el nombre original del recurso vWAN. Para restringir aún más la búsqueda, haga clic en Recursos.

VirtualHubDeployment | Overview ...

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

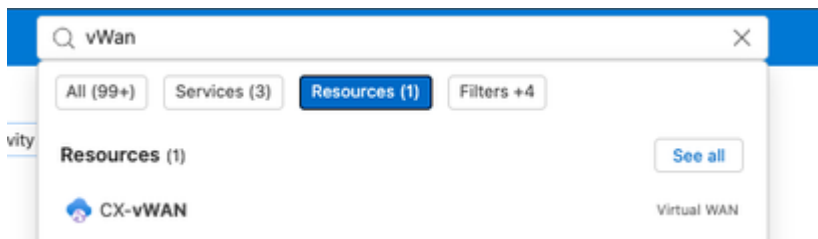
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

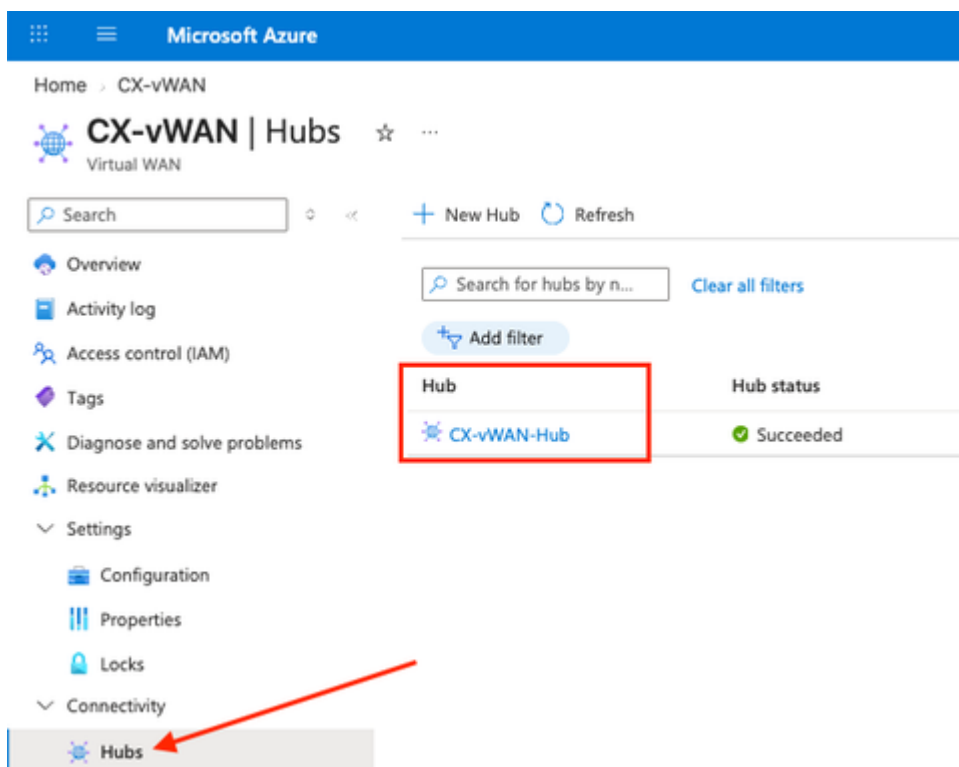
[Go to resource](#)



Fase 2: Configuración del sitio VPN de Azure vWAN

Paso 1: Crear sitio VPN de Azure vWAN (dispositivo FTD remoto)

a) Entre en el hub creado a través de Conectividad > Hubs y haga clic en el hub creado en pasos anteriores.



b) Haga clic en Conectividad > VPN (de sitio a sitio) y haga clic en + Crear nuevo sitio VPN.

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) Introduzca los valores en los campos obligatorios. Cuando haya terminado, haga clic en Siguiente: Enlaces > para avanzar.

Create VPN site ...

Basics Links Review + create

Project details

Subscription

Resource group *

Instance details

Region *

Name *

Device vendor *

Private address space

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

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

Previous

Next : Links >

d) Introduzca la información de enlace necesaria. Los campos Link BGP Address (Dirección BGP de enlace) y Link ASN (Dirección ASN de enlace) reflejan la dirección de destino BGP de capa 3 del túnel interior y el número de AS BGP en el sitio de sucursal con el que se forma la vecindad con Azure en los túneles de sitio a sitio. La dirección BGP de vínculo es una dirección de subred no superpuesta (/32) fuera de la subred del espacio de direcciones privadas del concentrador previamente configurada, que Azure instala como ruta /32 para alcanzar como vecino BGP. La dirección IP/FQDN del enlace es la dirección IP de destino de capa 3 del encabezado externo del tráfico que va al sitio de la sucursal necesario para aprovisionar la conectividad IPsec/IKEv2.



Nota: Si utiliza direcciones que van desde 169.254.21.0 a 169.254.22.255 para direcciones de túnel, asegúrese de revisar [Cómo configurar BGP para Azure VPN Gateway](#) para requisitos específicos.

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) Después de confirmar que los parámetros son correctos, haga clic en 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) Una vez finalizada la implementación del sitio VPN, vuelva a la configuración del vWAN Hub.

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

Paso 2: Configurar parámetros VPN de sitio de Azure vWAN

a) Entre en el hub creado a través de Conectividad > Hubs y haga clic en el hub creado en pasos anteriores.

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) Vaya de nuevo a Conectividad > VPN (de sitio a sitio) y haga clic en la X para borrar la Asociación del hub: Filtrado conectado para ver los sitios desconectados.

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

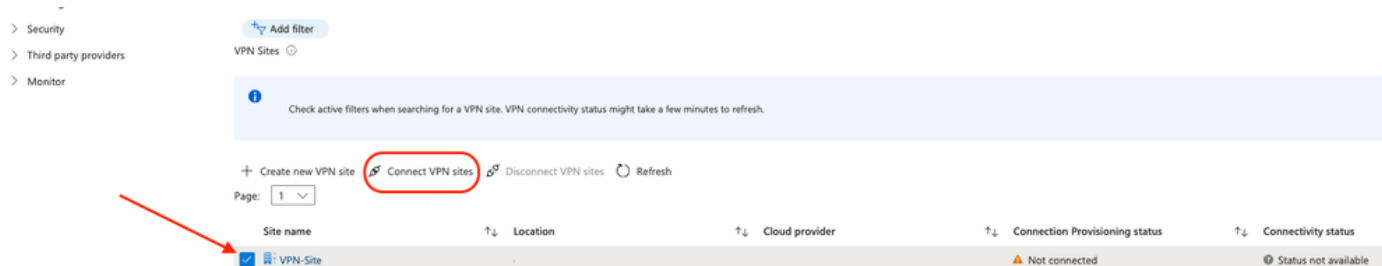
Search this page Clear all filters

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) Active la casilla situada junto al sitio VPN configurado anteriormente y, a continuación, haga clic en Connect VPN sites (Conectar sitios VPN), que se activará una vez que se haya seleccionado el sitio.



d) Aparecerá el panel de la sección Sitios de conexión. Ingrese una clave previamente compartida (PSK) y configure los valores deseados de Fase 1 IKEv2 y Fase 2 IPsec. Cuando elige Custom de la lista desplegable IPsec, los valores se rellenan automáticamente; anote estos valores, ya que deben coincidir en el FTD. También debe elegir si desea utilizar Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS). Dado que se trata de un túnel basado en rutas, configure los parámetros en consecuencia. Una vez completada, haga clic en Connect para guardar la configuración.



Nota: Consulte [Políticas IPsec predeterminadas frente a políticas IPsec personalizadas para Azure vWAN](#) para obtener más información.

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) Se muestra información que indica que el gateway se está actualizando, junto con el tiempo estimado hasta su finalización.

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

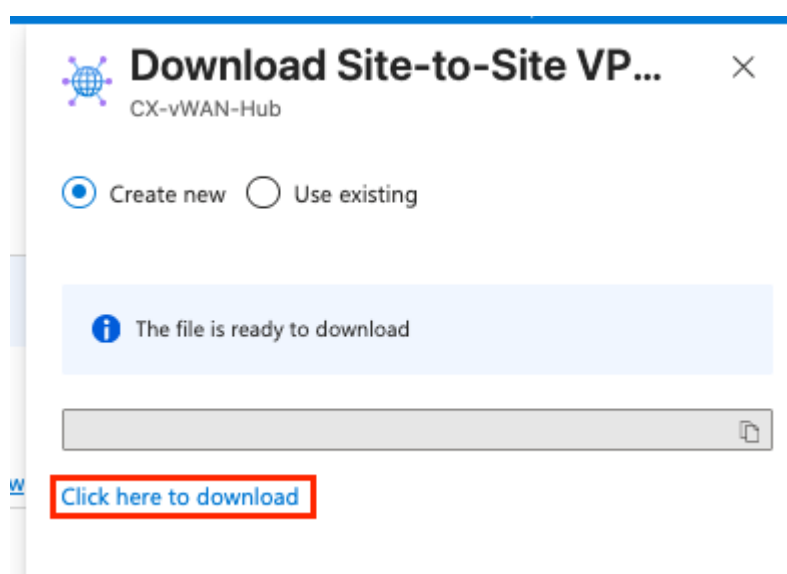
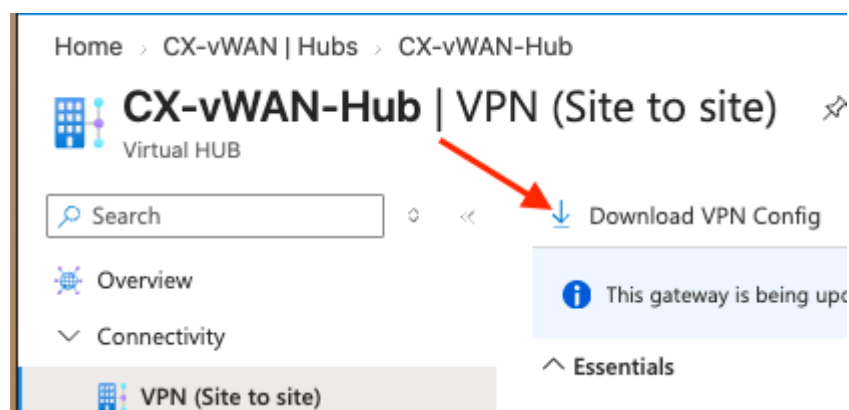
Connectivity



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

Paso 3: Descargar configuración de túnel de sitio de Azure vWAN

a) Mientras se actualiza el gateway, puede descargar la configuración VPN.



Con el sitio VPN creado y sus parámetros de conexión (direcciones de peer, números AS BGP y PSK) descargados, se utilizan los mismos valores para configurar los elementos coincidentes en el FTD en la fase 3.

Fase 3: Configuración de FTD

Paso 1: Analizar configuración de VPN de Azure

a) Abra el archivo de configuración VPN descargado desde Azure. Es similar a la salida condensada que se muestra y proporciona información útil:



Nota: Para mejorar el enfoque, varios objetos irrelevantes y pares clave/valor se recortan

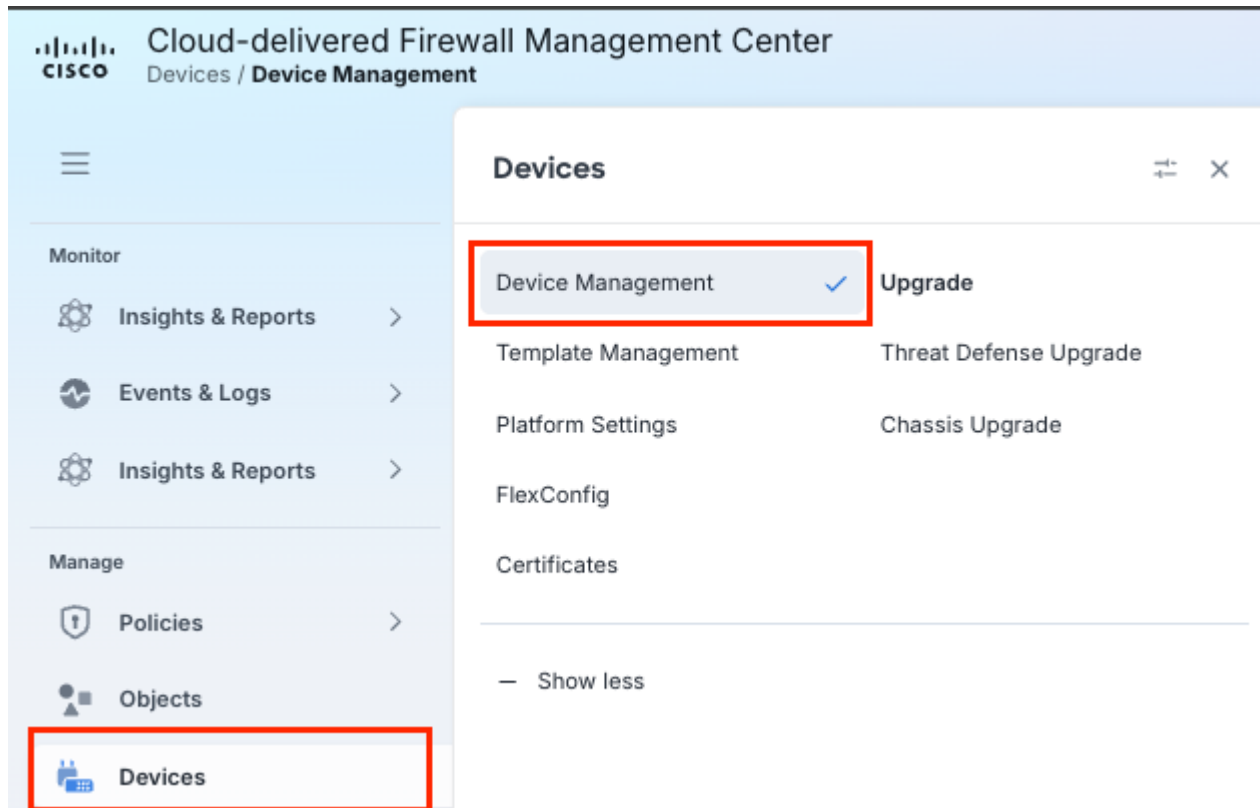
para obtener brevedad.

```
[
{
  "configurationVersion": {
    "LastUpdatedTime": "<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": {
          "IpssecEncryption": "GCMAES256",
          "IpssecIntegrity": "GCMAES256",
          "IkeEncryption": "GCMAES256",
          "IkeIntegrity": "SHA384",
          "PfsGroup": "None",
          "DhGroup": "DHGroup14",
          "SADataSizeInKilobytes": 0,
          "SALifeTimeInSeconds": 27000
        }
      }
    }
  ]
}
]
```

Paso 2: Configurar loopback

Cada VTI configurada posteriormente necesita un origen de túnel estable, por lo que una interfaz de loopback se configura primero y se comparte entre ambas VTI.

a) Vaya a Devices > Device Management.

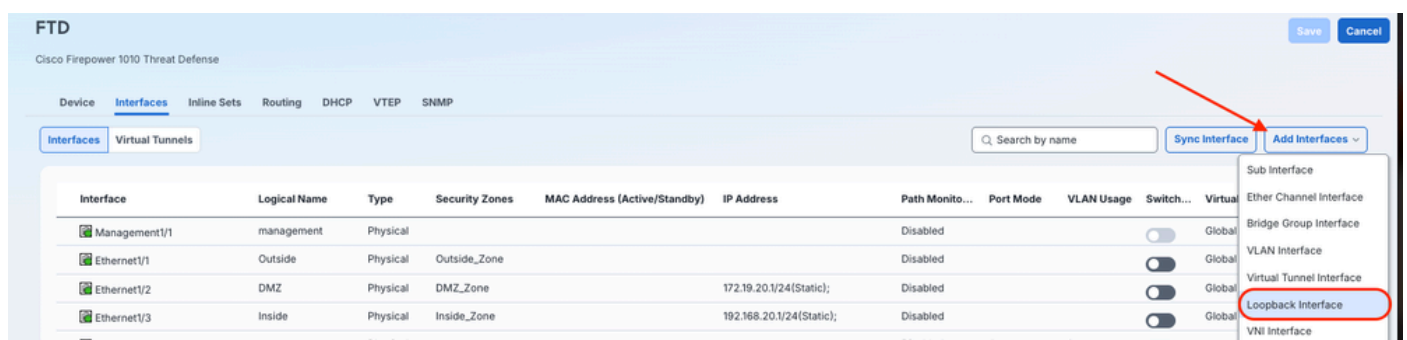


Nota: Este laboratorio utiliza el centro de gestión de firewall (cdFMC) proporcionado en la nube; sin embargo, los pasos siguen siendo los mismos para el FMC in situ.

b) Seleccione el FTD que está configurando como dispositivo VPN de sucursal/sitio.



c) Haga clic en el menú desplegable Add Interfaces, y haga clic en Loopback Interface.



d) Proporcione a la Interfaz de Loopback su Nombre, ID de Loopback y Descripción si es necesario. Haga clic en IPv4.

Add Loopback Interface

General **IPv4** IPv6

Name:
bgpVPNBranchLo

☒ Enabled

Loopback ID: *
1
(1-1024)

Description
Branch Loopback for BGP neighboring and VPN termination from Azure

Cancel OK

e) Asegúrese de que el Tipo de IP esté definido como Usar IP Estática, ingrese la Dirección BGP de Link según lo configurado en la Fase 2, paso 1d. Puede hacer referencia al valor definido previamente en la configuración JSON de VPN descargada

en `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Nota: Defina la dirección con una máscara /32 y dentro del espacio de dirección RFC 1918.

Add Loopback Interface

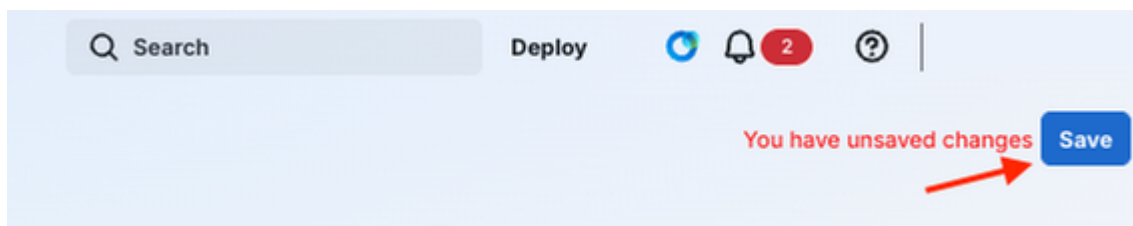
General **IPv4** IPv6

IP Type:
Use Static IP

IP Address:
10.50.1.2/32
e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

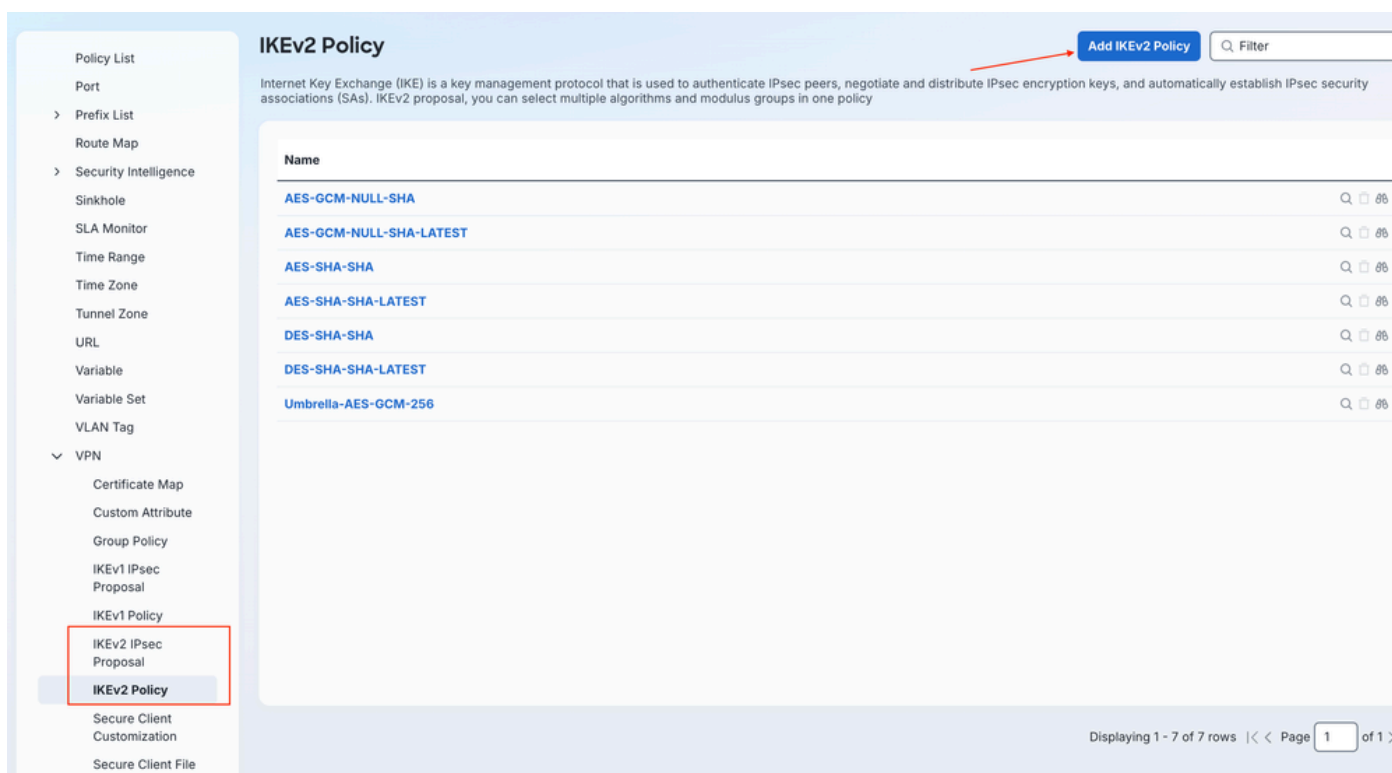
Cancel OK

f) Haga clic en Guardar



Paso 3: Configuración de objetos de política de fase 1/fase 2

a) Para configurar una configuración IKEv2/IPsec coincidente en el FMC para aplicarla en las topologías VPN FTD, navegue hasta Manage > Objects, desplácese hacia abajo en el menú de la izquierda hasta VPN y expanda el submenú. Configure la política de fase 1 de IKEv2 eligiendo IKEv2 Policy en el menú y haciendo clic en Add IKEv2 Policy.



b) Introduzca un nombre para la nueva política IKEv2, seleccione Prioridad y/o Duración. Asegúrese de que la política coincida en ambos extremos del túnel con respecto a Integrity, Encryption, PRF, y Diffie-Hellman (DH) Group. Elija los elementos Algoritmo/Grupo alineados que coincidan con la configuración de Azure y haga clic en Agregar.



Nota: Puede hacer referencia a estos valores exactos dentro del archivo de configuración descargado en 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

Available Algorithms

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

Selected Algorithms

SHA256 

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

c) Una vez finalizada la configuración, haga clic en 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

d) Configure los parámetros de Fase 2/IPSec en el submenú Propuesta IPSec IKEv2 y haga clic en Agregar propuesta IPSec IKEv2.

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 specify the encryption and authentication algorithms. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Add IKEv2 IPsec Proposal

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

e) Asigne un nombre a la propuesta IPsec de IKEv2 y asegúrese de que coinciden los mismos parámetros. Una vez hecho esto, haga clic en Guardar.



Nota: Puede hacer referencia a estos valores en el archivo de configuración descargado en `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

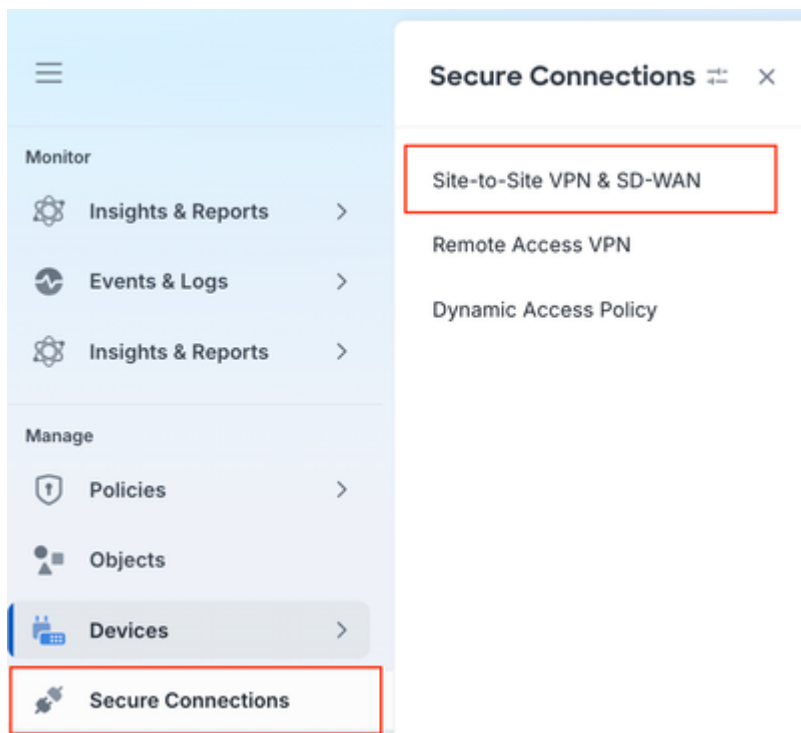


Cancel

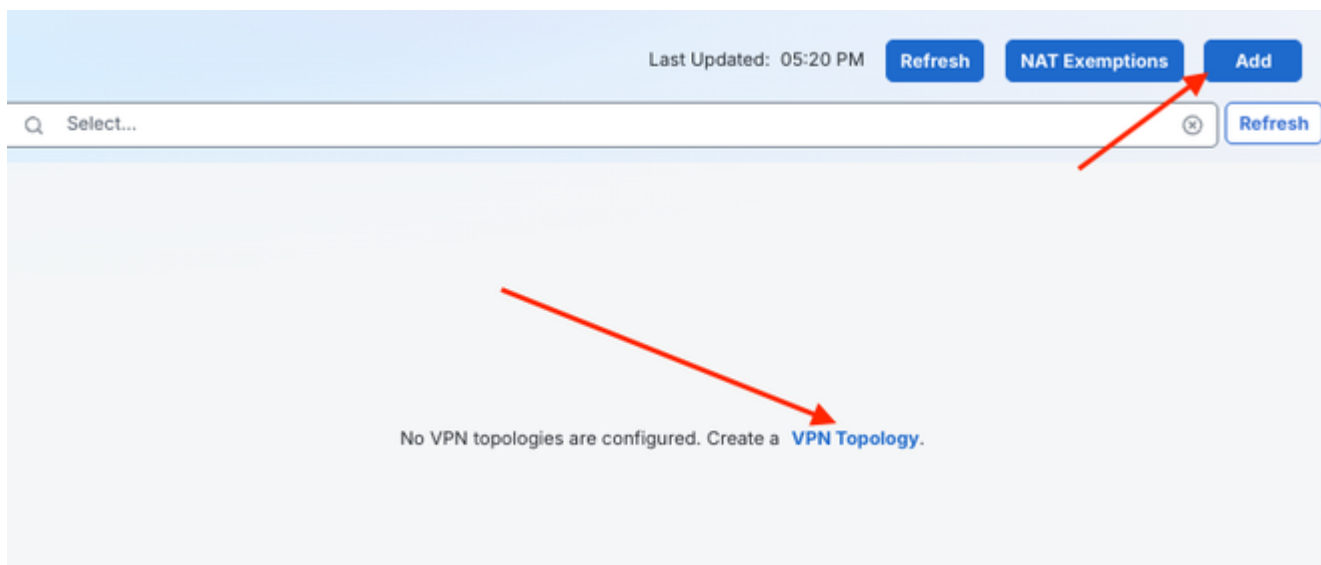
Save

Paso 4: Configurar la conectividad segura a Azure

a) Vaya a Administrar > Conexiones seguras > VPN de sitio a sitio y SD-WAN.



b) Haga clic en el hipervínculo de configuración inicial de VPN Topology en el centro, o haga clic en Add.



c) Ingrese un nombre de topología para el primer túnel a Azure Instance0, haga clic en el botón de radio Route-Based VPN y haga clic en el tipo de topología Peer to Peer VPN. Una vez completado, haga clic en Create.

Create VPN Topology

Topology name *

Azure-VTI-Instance0

VPN Type

☐ SD-WAN Topology

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

Select VPN Topology

☐ Hub and Spoke

Prerequisites

☒ **Route-Based VPN**

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

Select VPN Topology

☐ Hub and Spoke

☒ **Peer to Peer**

☐ Policy-Based VPN

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

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

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

[Prerequisites](#)

[Refresh](#)

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

d) Para el Nodo A, haga clic en la lista desplegable Device y elija el nombre del par HA FTD/FTD administrado en el que se está implementando la configuración. Para el Nodo B, debido a que es el extremo remoto de la conexión en la topología que termina en las instancias vWAN de Azure, elija Extranet en la lista desplegable Device. A continuación, para el Nodo A, haga clic en el icono + junto a la lista desplegable Virtual Tunnel Interface (VTI).

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:*

+

☐ Tunnel Source IP is Private [Edit VTI](#)

☐ Send Local Identity to Peers

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

[> Advanced Settings](#)

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

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

e) Asigne un nombre al primer VTI y asegúrese de que esté habilitado. Asigne una zona de seguridad nueva o existente al VTI, asigne el origen del túnel y elija la dirección IP en la lista desplegable adyacente.

The screenshot shows the 'Add Virtual Tunnel Interface' configuration page. It includes a header with a question mark icon. The 'Tunnel Type' section has 'Static' selected. The 'Name' field is 'Azure-VTI-0'. The 'Enabled' checkbox is checked. The 'Description' field is empty. The 'Security Zone' dropdown is 'Azure-Spoke-Zone'. The 'Priority' field is '0'. The 'Propagate Security Group Tag' checkbox is checked. Below this is a section titled 'Virtual Tunnel Interface Details' with a descriptive paragraph. The 'Tunnel ID' field is '1'. The 'Tunnel Source' section has two dropdowns: 'Ethernet1/1 (Outside)' and 'Dynamic'. Red arrows point to the 'Name' field, 'Security Zone' dropdown, 'Tunnel ID' field, and the 'Dynamic' dropdown in the 'Tunnel Source' section.

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

f) A continuación, asegúrese de que el botón de opción Préstamo de IP (IP sin numerar) está seleccionado, y luego elija el mismo loopback de la lista desplegable derecha. Haga clic en Aceptar una vez completado.

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)

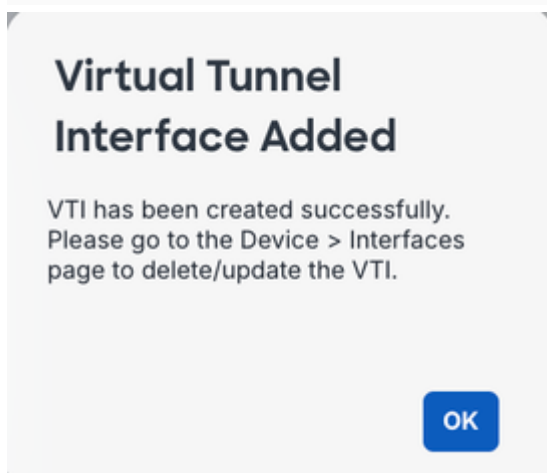
Tunnel Source:*

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) Loopback1 (bgpVPNBranchLo) ▾ +

Cancel OK



g) Una vez configurado y aplicado el VTI, rellene manualmente la dirección IP de origen del túnel (se rellena automáticamente si la dirección de la interfaz principal se rellena desde DHCP) y asegúrese de que se configura el nombre del dispositivo Nodo B, así como la dirección IP del punto final de la instancia. Una vez completada, haga clic en la pestaña IKE.



Nota: Puede hacer referencia al valor de la dirección IP del terminal Instance0 en el archivo de configuración descargado

en `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) Desplácese hasta IKEv2 Settings y asegúrese de que el Authentication Type esté configurado en Pre-shared Manual Key, e ingrese el PSK configurado en Azure en los pasos anteriores. Configure las políticas de IKEv2 Phase 1 haciendo clic en el icono del lápiz para editar las políticas IKEv2 disponibles.



Nota: Nota: Puede hacer referencia a la clave previamente compartida en el archivo de configuración descargado en `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

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

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) Agregue la política IKEv2 Phase 1 configurada inicialmente en el Paso 3.

IKEv2 Policy



Available IKEv2 Policy



Search

AES-GCM-NUL-
AES-GCM-NUL-
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) Seleccione la pestaña IPsec.

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) Edite la Propuesta IPsec de IKEv2 en Conjuntos de transformación haciendo clic en el icono del lápiz.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

l) Haga clic en el icono papelera para quitar el conjunto de transformación predeterminado AES-GCM y agregar el conjunto de transformación personalizado Azure_IPsec/IKEv2 IPsec Propuesta creada en la segunda mitad del paso 3. Haga clic en Aceptar.

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) Desplácese hacia abajo e ingrese 27000 para la duración que coincide con los parámetros de Azure. Habilite PFS Group si corresponde. Click Save.



Nota: Puede hacer referencia al valor de duración en el archivo de configuración descargado en `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) Implementar los cambios.

Search Deploy

Search Device Advanced Deploy **Deploy All**

☐ FTD

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

o) Una vez finalizada la implementación, verifique Manage > Secure Connections > Site-to-Site VPN & SD-WAN bajo Tunnel Status Distribution; conectividad satisfactoria refleja Green (Up).

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

Con el primer túnel implementado, confirme que se establece correctamente en las capas IKE/IPsec y BGP antes de configurar el segundo túnel para redundancia.

Paso 5: Verificar conectividad inicial con Azure

a) Introduzca SSH en el FTD e introduzca `system support diagnostic-cli`, escriba `en` y pulse Intro, ya que no hay contraseña en la CLI de FTD de solo lectura.

```
<#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) Comprobar el estado del túnel de fase 1/fase 2.

```
<#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) Realice capturas para verificar si hay paquetes del Protocolo de control de transmisión BGP (TCP) recibidos de Azure en el túnel y el puerto 4500/UDP puerto 500 del protocolo de datagrama de usuario NAT-T (Traducción de direcciones de red - Traversal) en la captura externa de la IP pública del túnel Instance-0 Azure.

```
<#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#
```

Con la conectividad a Instance0 confirmada, repita la misma configuración de topología VTI y VPN para Instance1 para que ambas instancias de gateway de Azure sean accesibles.

Paso 6: Configuración del segundo túnel al punto final Azure Instance1

a) Crear un segundo préstamo de VTI (Azure-VTI-1) a partir del mismo bucle invertido (paso 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) Configuración de la topología VPN de segunda instancia (Paso 4 g-n).



Nota: Puede hacer referencia al valor de la dirección IP del terminal Instance1 en el archivo de configuración descargado

en `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

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

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

c) Implemente cambios de configuración y compruebe el estado del túnel.

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

d) Incorporación de Azure, tanto Instance0 como Instance1 producen Connected.

Links

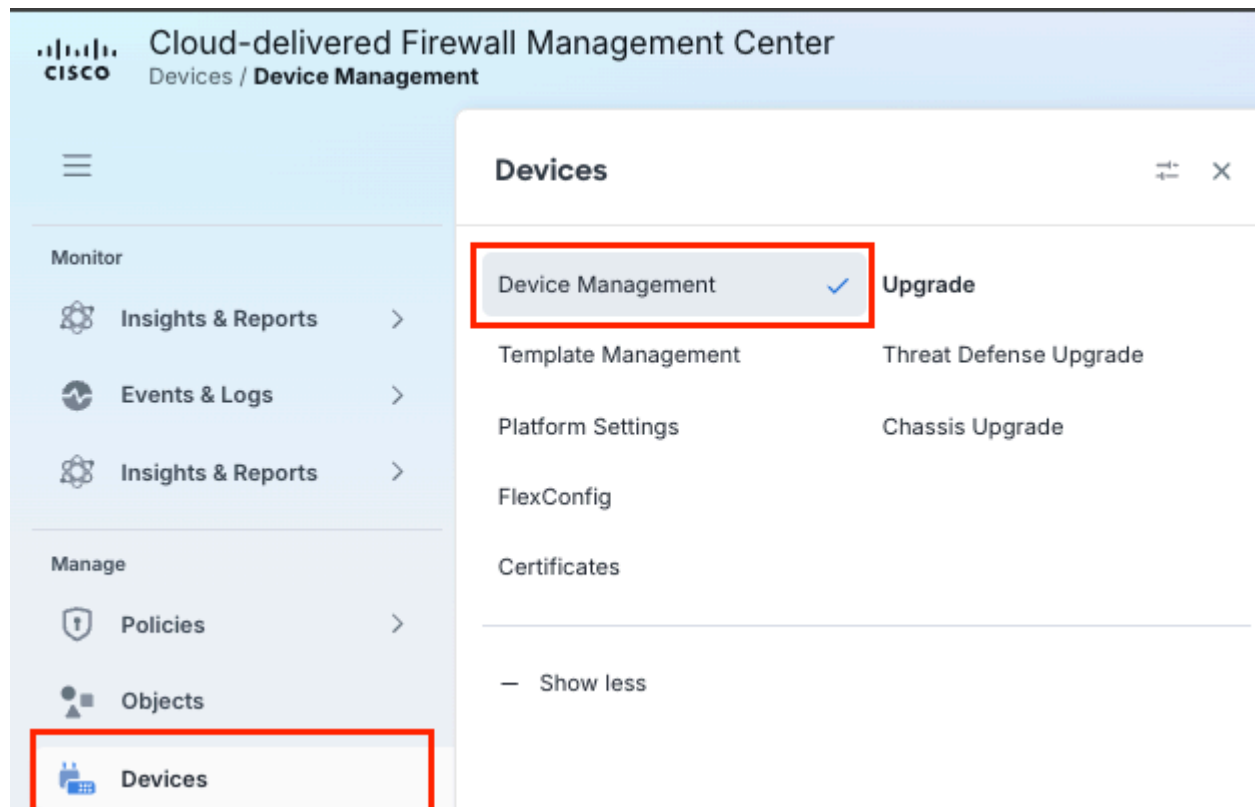
☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Con ambos túneles activos, el FTD necesita un routing ECMP para que el tráfico pueda utilizar ambas rutas al mismo tiempo, en lugar de tratar el segundo túnel como un modo de espera

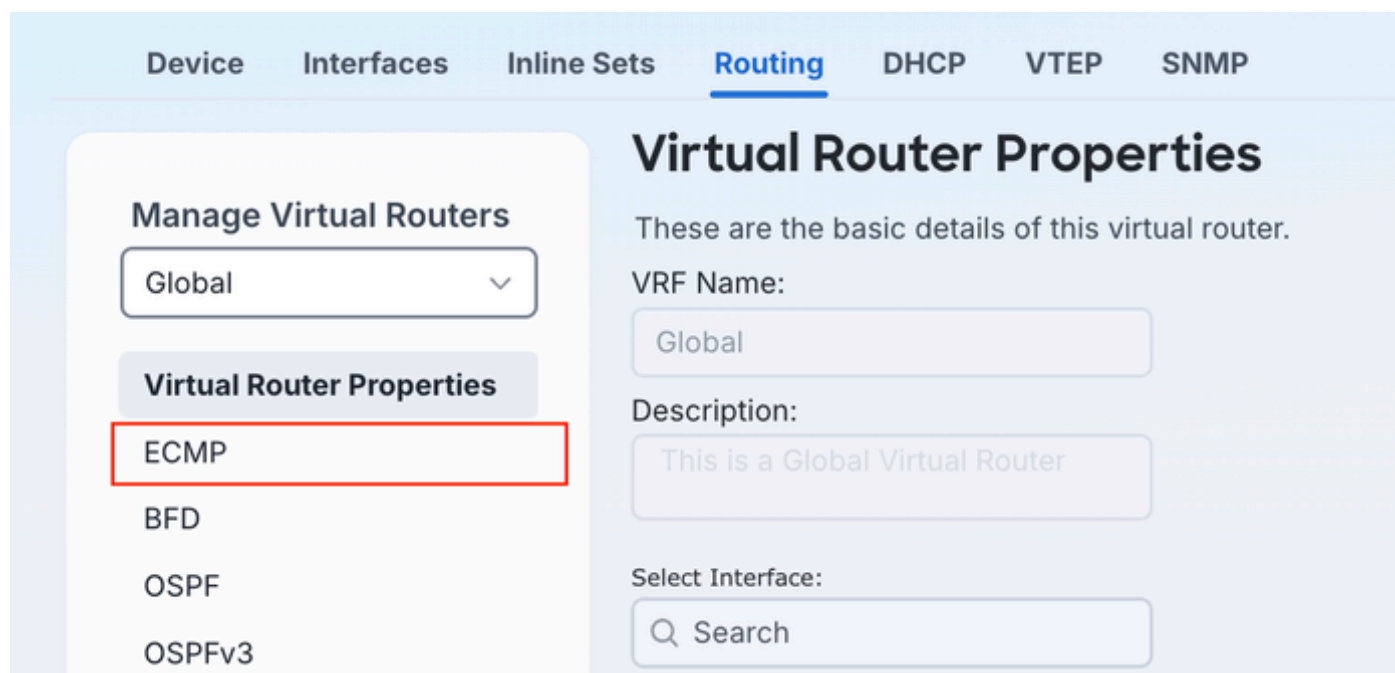
pasivo.

Paso 7: Configuración de ECMP

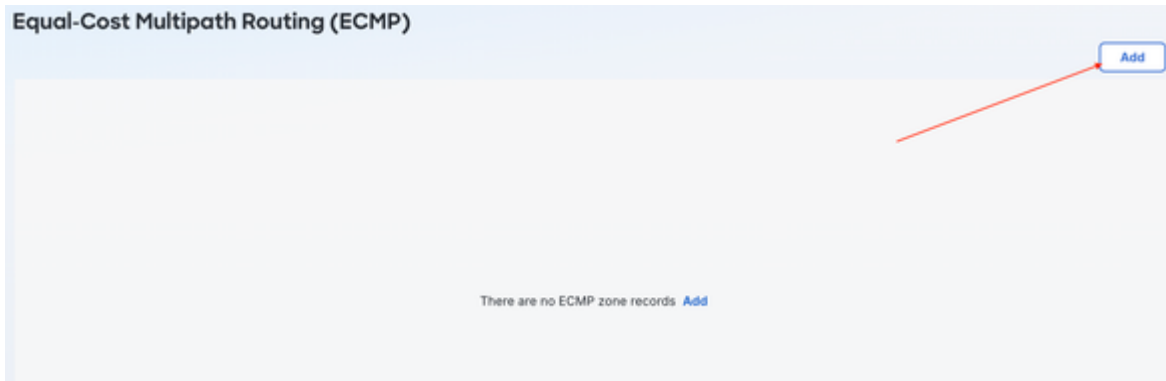
a) Navegue hasta Manage > Devices > Device Management y seleccione el FTD configurado con VPNs a Azure.



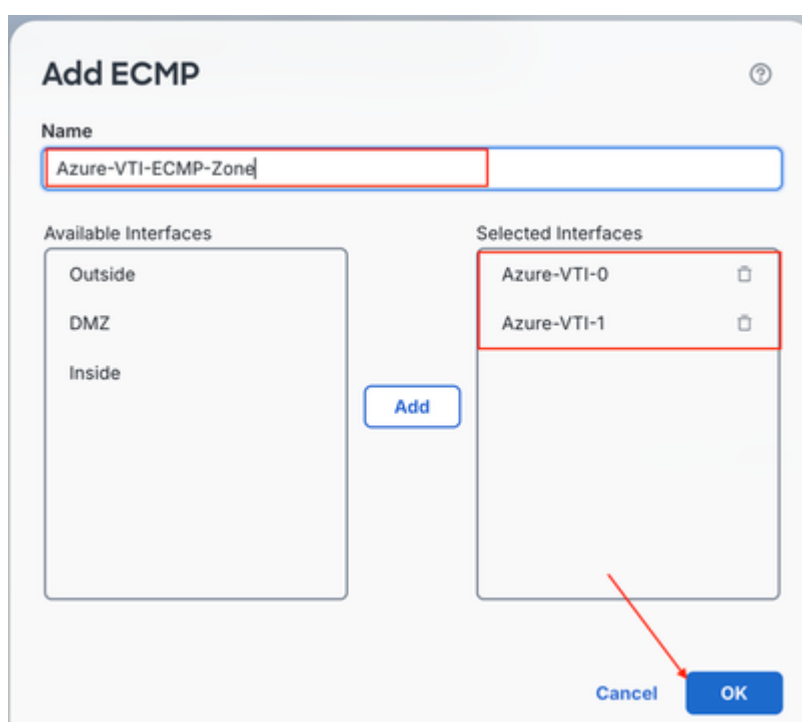
b) Haga clic en la pestaña Routing y elija ECMP.



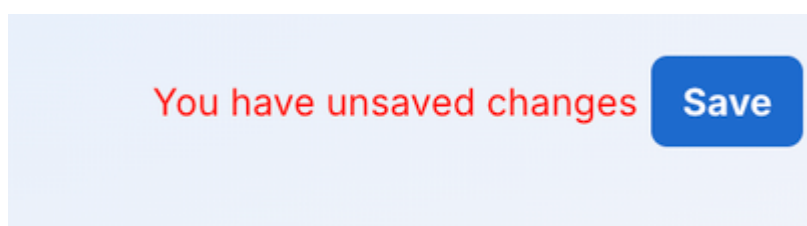
c) Haga clic en Agregar para crear una nueva zona ECMP.



d) Alterne para resaltar las VTIs haciendo clic en ambas VTIs en el panel Interfaces disponibles y haga clic en Agregar para aplicar las VTIs a la zona ECMP nombrada.



e) Después de confirmar que los parámetros son correctos, haga clic en Save.



Paso 8: Configuración de Rutas Estáticas para IP Privadas de Instancia

BGP requiere que las rutas se conecten correctamente a los vecinos y, como los terminales no están conectados directamente, no se rellena ninguna ruta de forma predeterminada. ECMP permite configurar rutas estáticas con la misma métrica (distancia administrativa) al mismo destino, de modo que ambas rutas se instalen en la Base de información de routing (RIB) y se utilicen simultáneamente.

a) Navegue hasta Manage > Devices > Device Management y elija el dispositivo FTD aplicable.

The screenshot shows the Cisco Firepower 1010 Threat Defense interface. The top navigation bar includes 'Device', 'Interfaces', 'Inline Sets', 'Routing' (highlighted with a red arrow), 'DHCP', 'VTEP', and 'SI'. The left sidebar has 'Monitor' and 'Manage' sections. Under 'Manage', 'Devices' is highlighted. The 'Manage Virtual Routers' sidebar is open, showing a list of routing options: 'Global', 'Virtual Router Properties', 'ECMP', 'BFD', 'OSPF', 'OSPFv3', 'EIGRP', 'RIP', 'Policy Based Routing', 'BGP' (expanded to show 'IPv4' and 'IPv6'), 'Static Route' (highlighted with a red box), 'Multicast Routing', and 'IGMP'. The main content area shows 'Network' and 'Interface' tabs, with 'IPv4 Routes' and 'IPv6 Routes' listed under 'Network'.

c) Haga clic en + Add Route.

The screenshot shows the 'Routing' tab in the Cisco Firepower 1010 Threat Defense interface. The 'Add Route' button is highlighted with a red arrow in the top right corner. Below the button, there is a table with columns: 'Network', 'Interface', 'Leaked from Virtual Router', 'Gateway', 'Tunneled', 'Metric', and 'Tracked'. The table is currently empty, with 'IPv4 Routes' and 'IPv6 Routes' listed as expandable sections.

d) Agregue rutas para ambas direcciones IP de instancia creando la primera ruta a su VTI de Instance0 y agregue el objeto de red de destino haciendo clic en el signo + junto a Red disponible. A continuación, haga clic en el objeto de red de la lista y haga clic en el botón Agregar para agregarlo como destino de la ruta estática. Asegúrese de que selecciona la dirección IP de Instance0 y que está establecida como la puerta de enlace. Una vez finalizado, haga clic en Aceptar.



Nota: Estos valores de red de destino de ruta estática se encuentran

bajo `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` y `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` en el archivo de configuración descargado.

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 +

Azure-Instance0-BGP_Peer
Azure-Instance1-BGP_Peer

Add

Selected Network

Azure-Instance0-BGP_Peer
10.2.0.12

Ensure that egress virtualrouter has route to that destination

Gateway: Azure-Instance0-BGP_Peer +

Metric: 1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking: +

Cancel OK

e) Repita los pasos c-d para agregar la segunda ruta estática a través de Instance1 VTI. Asegúrese de hacer clic en Guardar para guardar los cambios.

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						

Las rutas estáticas sólo alcanzan las direcciones de peering BGP; El propio BGP debe seguir habilitado y emparejado para que Azure y el FTD intercambien rutas dinámicamente hacia/desde redes más grandes.

Paso 9: Configuración de BGP

a) Habilite el Proceso BGP 65500 en FTD bajo Routing > General Settings > BGP. Marque la casilla de verificación Enable BGP e ingrese el número AS configurado anteriormente en la Fase 2, Paso 1. Navegue junto a 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

BGPEnable 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) Habilite el ruteo BGP IPv4 para el proceso/AS 65500 marcando la casilla de verificación adyacente Enable IPv4, y haga clic en Neighbor para configurar los vecinos BGP.

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) Haga clic en + Agregar.

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) Ingrese la información de peering BGP Instance0, haga referencia al BGP AS indicado del hub vWAN e ingréselo como el AS remoto vecino, y agregue una descripción si lo desea. Haga clic en Advanced.



Importante: Asegúrese de cambiar el BGP Update Source para hacer referencia al padre Loopback de ambas interfaces VTI en el 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

Description
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e) Dentro del menú Advanced de la configuración BGP Neighbor en FTD, puede cambiar el número de saltos TTL de eBGP predeterminado de 1 salto a un número variable. Los extremos BGP de Azure no están conectados directamente a través del túnel a la infraestructura de Azure y suele haber más saltos al extremo que los que permite el TTL de eBGP predeterminado de 1.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Repita los mismos pasos para el par BGP Instancia1 de Azure.

Add Neighbor ?

IP Address*
10.2.0.13

Remote AS*
65515
(1-4294967295 or 1.0-65535.65535)

BFD Fallover
none

Update Source:
bgpVPNBranchLo

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description
Instance1 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops
50
(1-255)

g) Asegúrese de que guarda los cambios una vez que los haya completado.

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) Cambie el valor predeterminado del campo Número de trayectorias de 1 a 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Asegúrese de que guarda e implementa los cambios.

Verificación

Una vez completada la implementación, confirme que BGP forma adyacencias con ambas instancias de Azure. Posteriormente, confirme que las rutas se aprenden a través de ambos túneles y que el tráfico utiliza ambas VTI, utilizando el mismo acceso CLI de diagnóstico establecido en la Fase 3, Paso 5.

Desplácese hasta `system support diagnostic-cli` en la CLI de FTD.

a) Una vez implementado, se espera que los vecinos BGP aparezcan y se reciban los prefijos.

```
<#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) Compruebe que las rutas recibidas de Azure se muestran como rutas de múltiples rutas.

```
<#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) Verifique el conteo de paquetes VTI.

```
<#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) Confirme las rutas estáticas para las vecindades BGP.

```
<#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) Confirmar zonas ECMP.

```
<#root>
```

```
ftd#
```

```
show zone
```

```
Zone: Azure-VTI-ECMP-Zone ecmp
  Security-level: 0
  Zone member(s): 2
    Azure-VTI-1      Tunne12
    Azure-VTI-0      Tunne11
```

```
ftd#
```

f) Confirme la configuración de BGP.

```
<#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) Confirmar tabla de enrutamiento.

```
<#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
```

Otras consideraciones

La configuración básica de este documento supone una única interfaz externa y un único ISP en el FTD de la sucursal. Estas consideraciones amplían ese diseño.

AS-Path Prepending

Si necesita influenciar cuál de los dos túneles prefiere Azure o FTD como primario, en lugar de compartir la carga de manera equitativa a través de ECMP y múltiples trayectorias BGP, anteponga el número AS local una o más veces más en el vecino BGP para ser tratado como secundario. El vecino con la trayectoria AS más larga y antepuesta pierde la prioridad durante la selección de la mejor trayectoria BGP estándar, sin necesidad de quitar ese vecino de la zona ECMP completamente.

Troubleshoot

- El túnel de fase 1/fase 2 no se activa: Confirme que la clave previamente compartida y los parámetros de la directiva IKEv2/IPsec (cifrado, integridad, PRF, grupo DH y duración) coincidan exactamente entre la directiva FMC IKEv2/propuesta IPsec y los valores del archivo de configuración VPN de Azure descargado. Utilice `show crypto isakmp sa` y `show crypto ipsec sa`, como se muestra en la fase 3, paso 5.
- El túnel está activo, pero los vecinos BGP no forman `update-source`: Verifique que BGP esté configurado en la interfaz de loopback, no en el VTI mismo, y que `ebgp-multihop` esté configurado con un valor lo suficientemente alto como para alcanzar la dirección de peering BGP de Azure, que no está conectada directamente con el FTD.
- Se forma BGP, pero sólo un túnel transporta tráfico: Confirme que ambas VTI sean miembros de la misma zona ECMP, que las rutas estáticas a ambas direcciones BGP de instancia de Azure estén instaladas con la misma distancia administrativa y que la ruta múltiple BGP esté configurada para dos rutas, como se describe en la Fase 3, Paso 10.
- No hay tráfico de retorno o routing asimétrico a Azure: Dado que Azure vWAN anuncia el espacio de la dirección del hub en ambos túneles, asegúrese de que ECMP no esté deshabilitado en ninguna parte de la configuración de routing y compruebe si hay mapas de ruta o routing basado en políticas que puedan anclar el tráfico a una única ruta.
- BGP está activo y las rutas están instaladas, pero el tráfico parece estar bloqueado: Asegúrese de que tiene reglas de control de acceso configuradas con la zona de seguridad asignada a las VTI que permiten la entrada y salida del tráfico.

Información Relacionada

- [¿Qué es la WAN virtual de Azure?](#)
- [Cómo configurar BGP para Azure VPN Gateway](#)
- [Políticas IPsec predeterminadas frente a políticas IPsec personalizadas Azure vWAN](#)

- [Solucionar problemas de BGP para Azure VPN Gateway](#)
- [Acerca de los gateways VPN de modo activo-activo](#)
- [Tutorial: Crear una conexión de sitio a sitio mediante la WAN virtual de Azure](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).