

Configurar a VPN Site a Site do Azure vWAN para o Firewall Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama](#)

[Conectividade de vWAN de Link DIA Único entre Azure e FTD \(Balanceamento de Carga/Redundância do Azure\)](#)

[Configurar](#)

[Fase 1: Configuração do vWAN/Hub do Azure](#)

[Passo 1: Criar vWAN](#)

[Passo 2: Criar Hub vWAN](#)

[Fase 2: Configuração do Site VPN vWAN do Azure](#)

[Passo 1: Criar Site VPN vWAN do Azure \(Dispositivo FTD Remoto\)](#)

[Passo 2: Configurar Parâmetros VPN do Site vWAN do Azure](#)

[Passo 3: Baixar Configuração do Túnel do Site vWAN do Azure](#)

[Fase 3: Configuração de FTD](#)

[Passo 1: Analisar Configuração de VPN do Azure](#)

[Passo 2: Configurar loopback](#)

[Passo 3: Configurar Objetos de Política da Fase 1/Fase 2](#)

[Passo 4: Configurar Conectividade Segura para o Azure](#)

[Passo 5: Verificar Conectividade Inicial com o Azure](#)

[Passo 6: Configurar o Segundo Túnel para o Ponto de Extremidade da Instância1 do Azure](#)

[Passo 7: Configurar ECMP](#)

[Passo 8: Configurar rotas estáticas para IPs privados de instância](#)

[Etapa 9: Configurar BGP](#)

[Etapa 10: Configurar o multipath de BGP](#)

[Verificar](#)

[Outras considerações](#)

[AS-Path Prepending](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração da conectividade VPN site a site da WAN Virtual do Microsoft Azure (vWAN) com o Cisco Secure Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Rede de Longa Distância Virtual (vWAN) do Microsoft Azure
- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure FTD Versão 10.0
- Cisco Secure FMC Versão 10.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A WAN Virtual do Microsoft Azure (vWAN) combina vários recursos de rede, segurança e roteamento do Azure por trás de uma única construção de Hub. Cada Hub vWAN pode hospedar um gateway VPN Site a Site gerenciado pela Microsoft que dispositivos remotos, como o Firewall Seguro, usam para acessar o Azure sem a necessidade de criar e manter a infraestrutura do gateway.

Diferentemente de uma VPN IPsec de dois pontos de extremidade convencional, o gateway VPN Site a Site da vWAN do Azure é implantado como um par de instâncias ativo-ativo (Instância0 e Instância1), cada uma com seu próprio endereço IP público e endereço de emparelhamento de protocolo de gateway de borda (BGP). Para aproveitar as duas instâncias de redundância e throughput adicional, o FTD de filial estabelece um túnel de segurança IP (IPsec) para cada instância e usa o BGP, em vez do roteamento estático sozinho, para aprender dinamicamente e retirar rotas quando as instâncias se tornam disponíveis ou indisponíveis. O roteamento Equal-

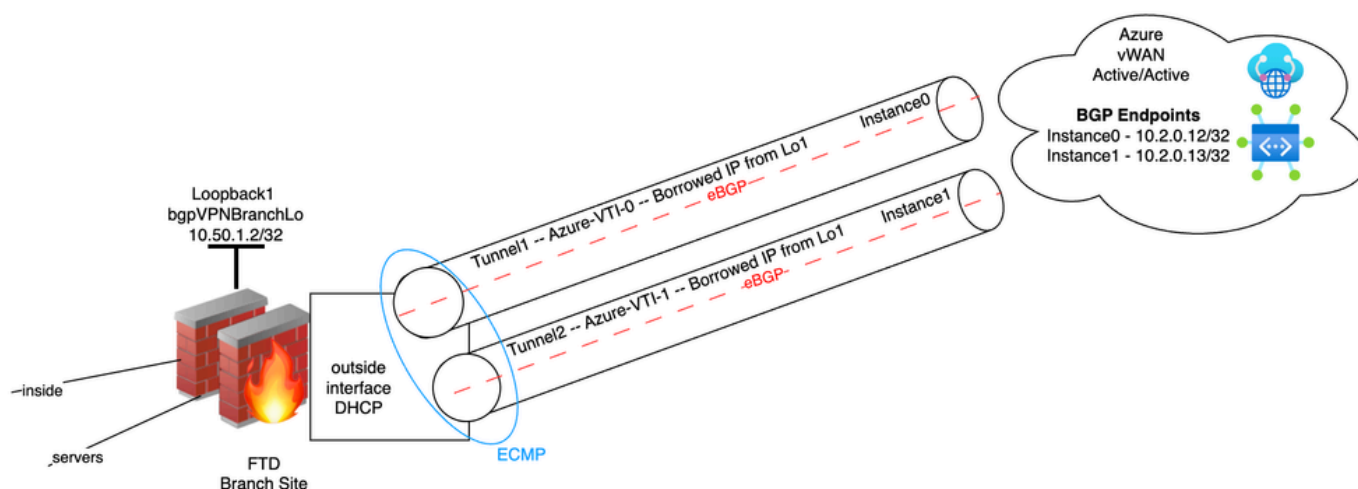
Cost Multi-Path (ECMP) e o multipath de BGP no FTD mantêm ambos os túneis ativos ao mesmo tempo, em vez de tratá-los como um standby passivo.

Este documento configura esse projeto em três fases: os objetos de Hub vWAN e Site VPN do Azure são criados primeiro, os parâmetros de conexão resultantes são baixados e esses mesmos parâmetros são usados para configurar interfaces de túnel virtual (VTIs) correspondentes, políticas Internet Key Exchange versão 2 (IKEv2)/IPsec, rotas estáticas, ECMP e peering BGP no FTD por meio do FMC.

Diagrama

O diagrama mostra a topologia da configuração descrita neste artigo. A única variante do Direct Internet Access (DIA) origina os túneis do Azure de uma interface externa no FTD.

Conectividade de vWAN de Link DIA Único entre Azure e FTD (Balanceamento de Carga/Redundância do Azure)



Configurar

Conclua as três fases na ordem. Os objetos do lado do Azure criados na Fase 1 e na Fase 2 produzem os endereços IP do peer, os números de Sistema Autônomo (AS) BGP e a chave pré-compartilhada que a Fase 3 aplica ao FTD.

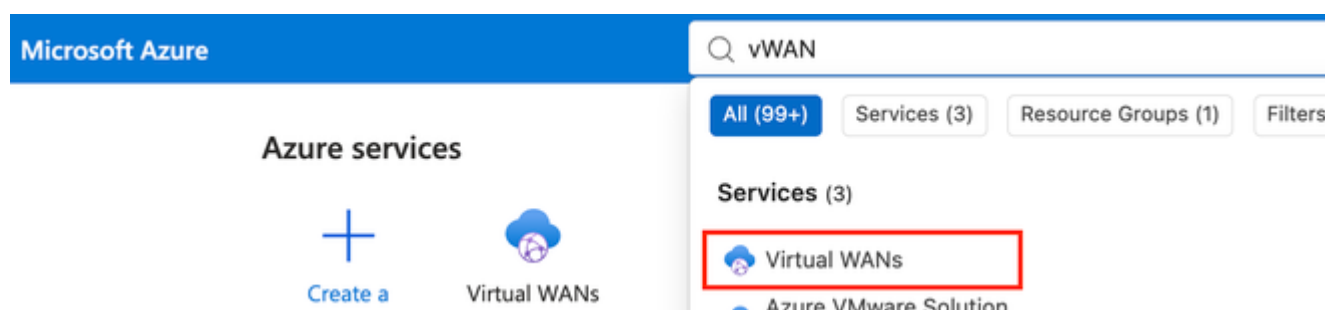
Fase 1: Configuração do vWAN/Hub do Azure



Note: As etapas de configuração neste documento são de alto nível e fornecem as etapas necessárias para conectar o FTD ao Azure vWAN. Consulte a documentação do Azure vWAN da Microsoft para entender o significado das configurações. Consulte [O que é a WAN Virtual do Azure?](#) e documentação adicional.

Passo 1: Criar vWAN

a) Procure vWAN na caixa de pesquisa do Azure e clique em WANs virtuais.



b) Clique em + Criar.



c) Insira um Nome para a nova instância da vWAN, clique em Revisar + criar e clique em Criar na página Revisar + Criar do assistente.

Create WAN ...

Basics Review + create

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

Project details

Subscription *

Resource group *
[Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >



Note: O espaço em branco que cobre valores em vários campos nas imagens é intencional para a publicação deste documento.

d) Clique em Ir para 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

Passo 2: Criar Hub vWAN

a) Navegue até Connectivity > Hubs e clique em + New Hub.



CX-vWAN | Hubs



Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub	Hub status	Region
No results		

b) Consulte a documentação do Azure para obter mais contexto sobre configurações adicionais. Verifique se o espaço de endereço privado do Hub alocado não se sobrepõe a nenhum dos seus espaços de endereço interno. Configure Name, Virtual Hub, preferência de roteamento de hub. Clique em Next: Site a site >.

Home > CX-vWAN | Hubs

Create virtual hub

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

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

Project details

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

Subscription

Resource group

Virtual Hub Details

Region

Name

Hub private address space

Virtual hub capacity

Hub routing preference

Review + create Previous Next: Site to site >

Creating a hub with a gateway will take 30 minutes.

c) Consulte a documentação do Microsoft Azure vWAN Hub para obter informações sobre os campos apresentados. Alterne Sim para criar um site a site (Gateway VPN). O número padrão de Sistema Autônomo (AS) BGP alocado é 65515, conforme alocado pela Internet Engineering Task Force (IETF) em Request For Comments (RFC) 6996 definindo Private Use AS Reservation.



Note: Registre o AS do BGP para etapas futuras de configuração no 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 >

Clique em Revisar + criar ou clique em Avançar : Aponte para site > para definir as configurações opcionais.

d) Depois que o resumo for verificado, clique em Create.



Note: Como o Azure afirma, a criação do hub leva 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) Quando a implantação estiver concluída, procure o nome original do recurso vWAN. Para restringir ainda mais sua pesquisa, clique em Recursos.

VirtualHubDeployment | Overview ...

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

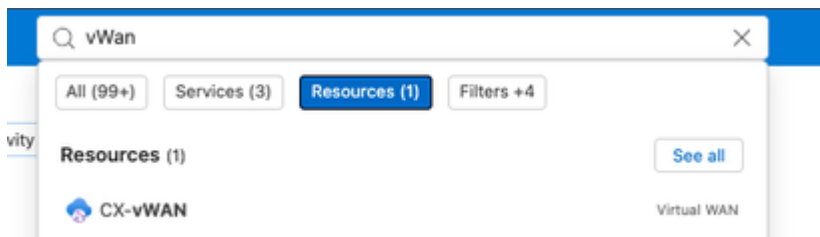
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

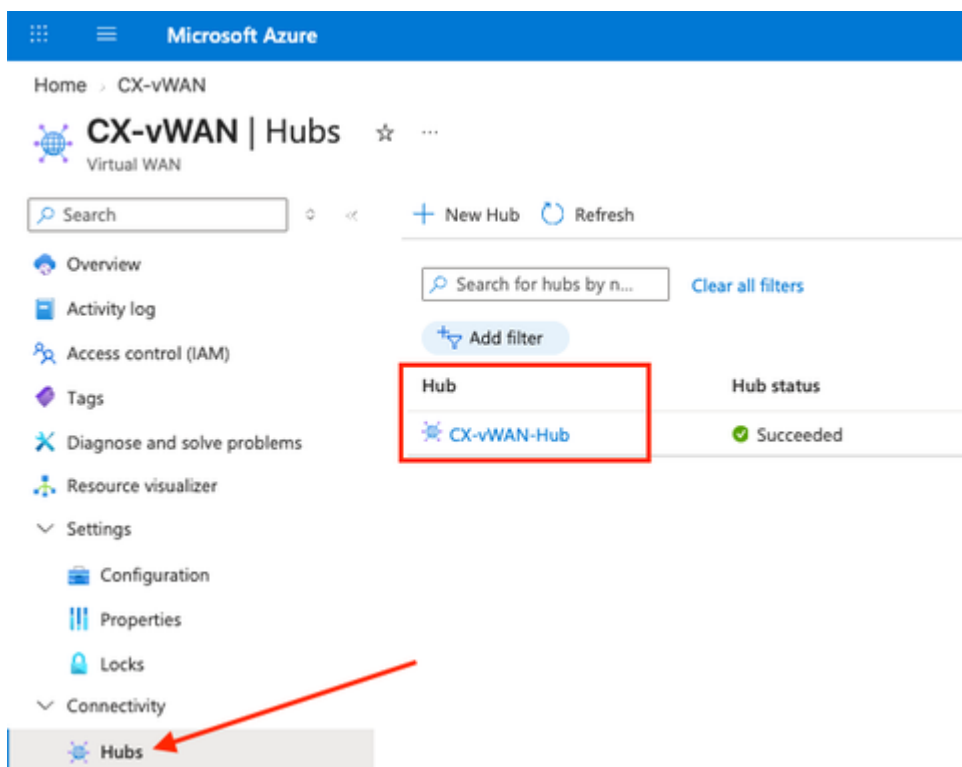
[Go to resource](#)



Fase 2: Configuração do Site VPN vWAN do Azure

Passo 1: Criar Site VPN vWAN do Azure (Dispositivo FTD Remoto)

a) Entre no hub criado via Connectivity > Hubs e clique no hub criado nas etapas anteriores.



b) Clique em Connectivity > VPN (Site to site) e clique em + Create new VPN site.

Microsoft Azure

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

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ⓘ

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

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

Site name	Location	Cloud
No results		

c) Insira os valores nos campos obrigatórios. Ao terminar, clique em Avançar: Links > para avançar.

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) Insira as informações de link necessárias. Os campos Link BGP Address e Link ASN refletem o endereço de destino do BGP da camada 3 do túnel interno e o número BGP AS no site da filial com o qual a vizinhança com o Azure é formada nos túneis site a site. O Endereço BGP de Link é um endereço de sub-rede sem sobreposição (/32) fora da sub-rede de espaço de endereço privado de Hub previamente configurada, que o Azure instala como uma rota /32 para acessar como um vizinho BGP. O endereço IP/FQDN do link é o endereço IP destino de Camada 3 do cabeçalho externo do tráfego que vai para o local da filial necessário para provisionar a conectividade IPsec/IKEv2.



Note: Se você estiver usando endereços que variam de 169.254.21.0 a 169.254.22.255 para endereços de túnel, certifique-se de revisar [Como configurar o BGP para o Gateway VPN do Azure](#) 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) Depois de confirmar que as configurações estão corretas, clique em 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) Quando a implantação do site VPN for concluída, navegue de volta para a configuração do 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](#)

Q vWan

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

Resources (1) [See all](#)

 **CX-vWAN** Virtual WAN

Passo 2: Configurar Parâmetros VPN do Site vWAN do Azure

a) Entre no hub criado via Connectivity > Hubs e clique no hub criado nas etapas 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) Navegue mais uma vez para Connectivity > VPN (Site to site) e clique no X para limpar a Associação de Hub: Filtragem conectada para exibir sites 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

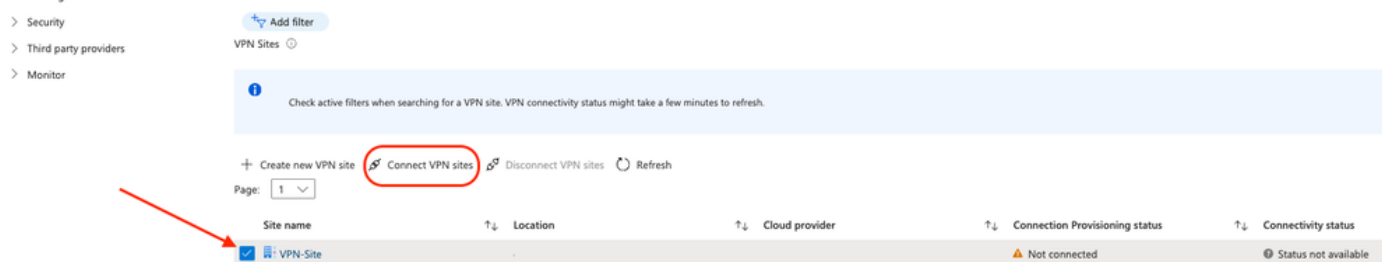
Search this page Clear all filters

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) Marque a caixa ao lado do site VPN configurado anteriormente e clique em Connect VPN sites, que se torna habilitado depois que o site é selecionado.



d) O painel da gaveta lateral Conectar locais é exibido. Insira uma chave pré-compartilhada (PSK) e defina as configurações desejadas de IKEv2 fase 1 e IPsec fase 2. Quando você escolhe Custom na lista suspensa IPsec, os valores são preenchidos automaticamente; observe esses valores, pois eles devem corresponder no FTD. Você também deve escolher se o PFS (Perfect Forward Secrecy) é desejado. Como este é um túnel baseado em rota, defina as configurações de acordo. Depois de concluir, clique em Connect para salvar a configuração.



Note: Consulte [Políticas IPsec Padrão vs. Personalizadas do Azure vWAN](#) para obter mais informações.

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) São exibidas informações indicando que o gateway está sendo atualizado, juntamente com o tempo estimado para conclusão.

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

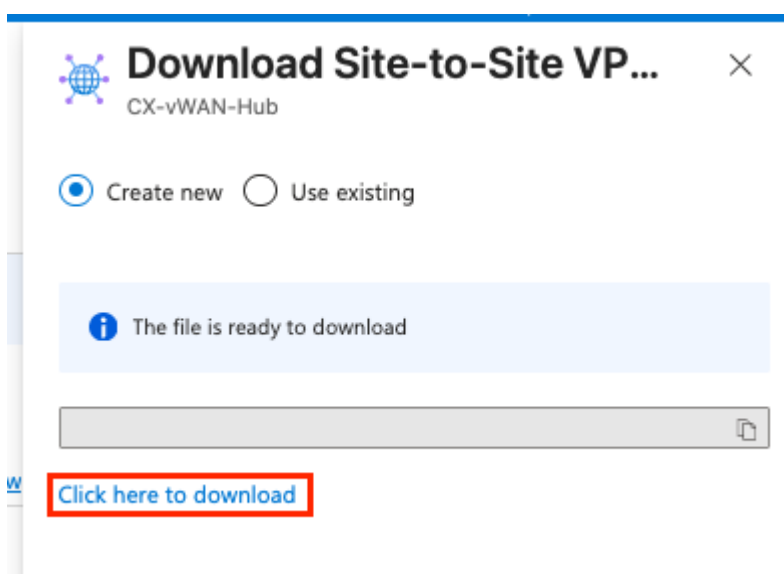
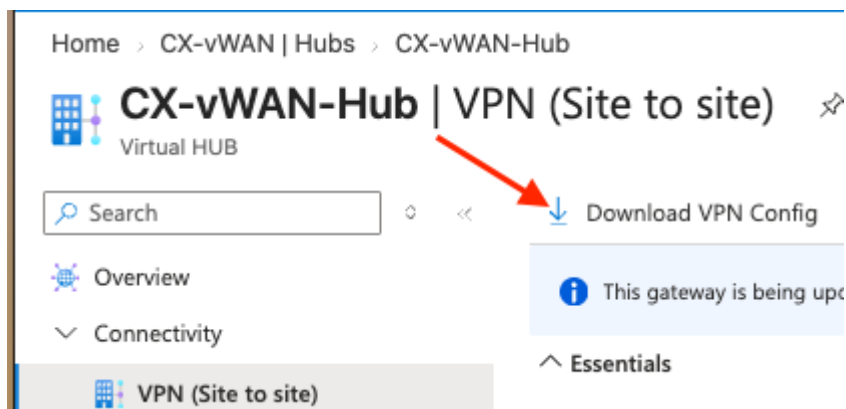
Connectivity



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

Passo 3: Baixar Configuração do Túnel do Site vWAN do Azure

a) Enquanto o gateway está sendo atualizado, você pode baixar a configuração da VPN.



Com o site VPN criado e seus parâmetros de conexão (endereços de peer, números AS BGP e PSK) baixados, os mesmos valores são usados para configurar os elementos correspondentes no FTD na Fase 3.

Fase 3: Configuração de FTD

Passo 1: Analisar Configuração de VPN do Azure

a) Abra o arquivo de configuração VPN baixado do Azure. Ele se parece com a saída condensada mostrada e fornece informações úteis:



Note: Para maior focagem, vários objetos irrelevantes e pares de chave/valor são

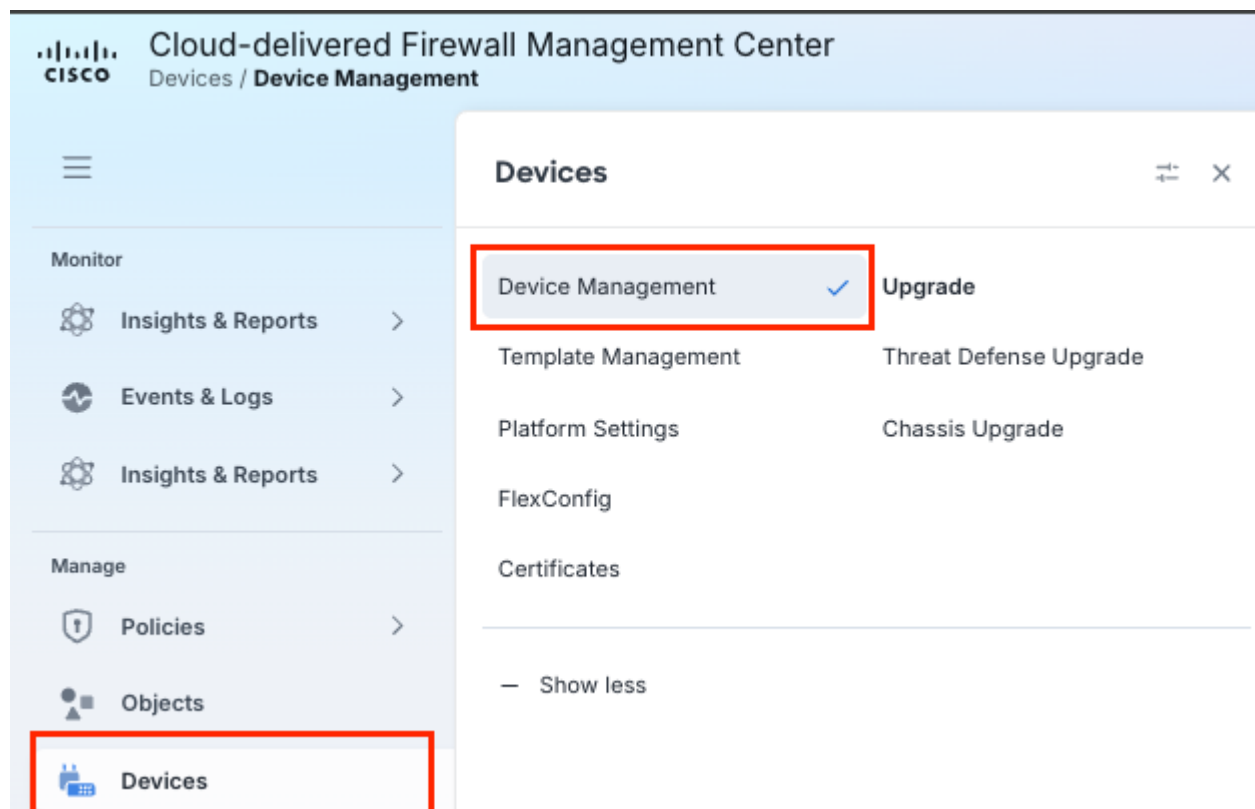
removidos por serem breves.

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

Passo 2: Configurar loopback

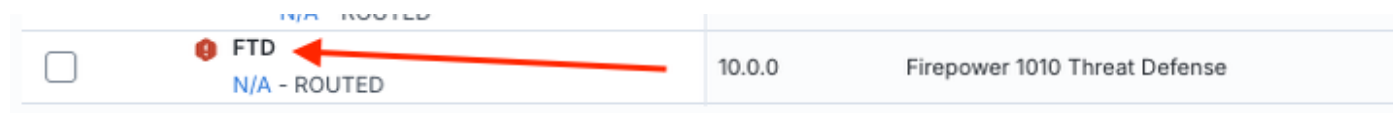
Cada VTI configurado posteriormente precisa de uma origem de túnel estável, de modo que uma interface de loopback seja configurada primeiro e compartilhada entre os dois VTIs.

a) Navegue até Devices > Device Management.

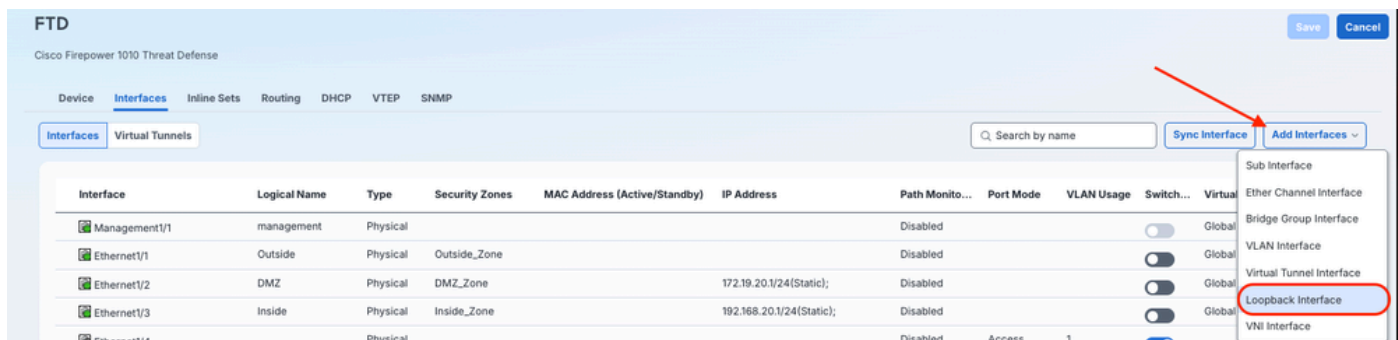


Note: Este laboratório usa o Centro de Gerenciamento de Firewall (cdFMC - Firewall Management Center) fornecido em nuvem; no entanto, as etapas continuam a ser as mesmas para o CVP local.

b) Selecione o FTD que você está configurando como o dispositivo VPN de filial/site.



c) Clique no menu suspenso Add Interfaces e clique em Loopback Interface.



d) Dê à Interface de Loopback seu Nome, ID de Loopback e Descrição, se necessário. Clique em IPv4.

e) Certifique-se de que o Tipo de IP esteja definido como Usar IP estático, insira o Endereço BGP de link conforme configurado na Fase 2, etapa 1d. Você pode consultar o valor previamente definido no JSON de configuração de VPN baixado em `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Note: Defina o endereço com uma máscara /32 e dentro do espaço de endereço RFC 1918.

Add Loopback Interface

General **IPv4** IPv6

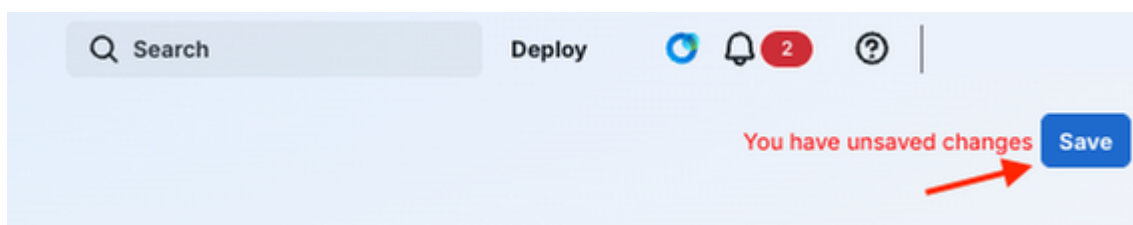
IP Type:
Use Static IP

IP Address:
10.50.1.2/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

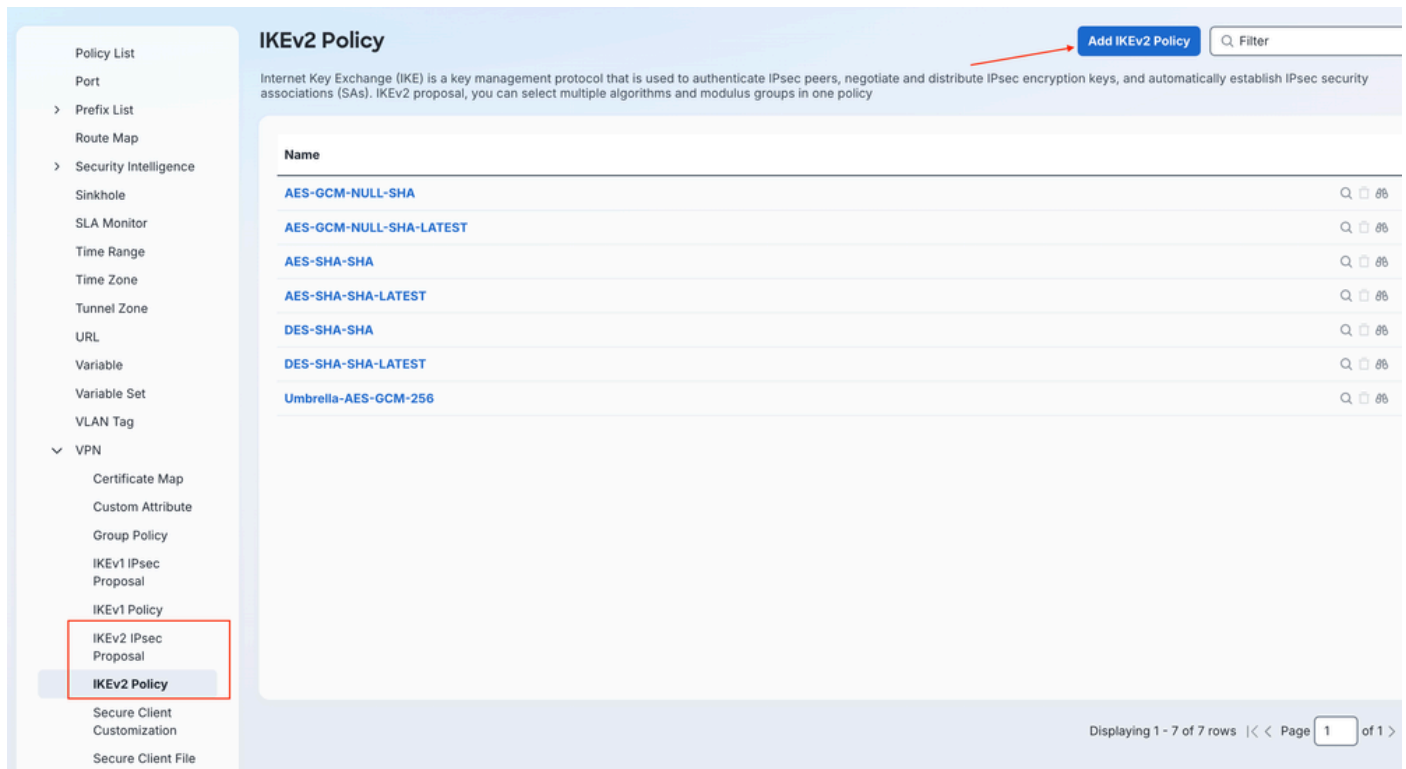
Cancel OK

f) Clique em Save



Passo 3: Configurar Objetos de Política da Fase 1/Fase 2

a) Para configurar a configuração de IKEv2/IPsec correspondente no FMC para aplicação nas topologias de VPN FTD, navegue para Manage > Objects, role para baixo no menu esquerdo até VPN e expanda o submenu. Configure a Política da Fase 1 de IKEv2 escolhendo Política de IKEv2 no menu e clicando em Adicionar Política de IKEv2.



IKEv2 Policy

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

[Add IKEv2 Policy](#)

Name		
AES-GCM-NUL-SHA		⋮
AES-GCM-NUL-SHA-LATEST		⋮
AES-SHA-SHA		⋮
AES-SHA-SHA-LATEST		⋮
DES-SHA-SHA		⋮
DES-SHA-SHA-LATEST		⋮
Umbrella-AES-GCM-256		⋮

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

b) Insira um nome para a nova Política IKEv2, escolha Prioridade e/ou Tempo de vida. Assegure-se de que a política corresponda em ambas as extremidades do túnel em relação a Integridade, Criptografia, PRF, e Grupo Diffie-Hellman (DH). Escolha os elementos Algoritmo/Grupo alinhados para corresponder à configuração do Azure e clique em Adicionar.



Note: Você pode fazer referência a esses valores exatos no arquivo de configuração baixado em `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
-
- SHA384
- NULL

Selected Algorithms

- SHA256

c) Quando a configuração estiver concluída, clique em 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 os parâmetros da Fase 2/IPsec no submenu IKEv2 IPsec Proposal e clique em Add IKEv2 IPsec Proposal.

The screenshot shows the Cisco IOS XE configuration interface. On the left is a navigation menu with categories like Policy List, Port, Prefix List, Route Map, Security Intelligence, Sinkhole, SLA Monitor, Time Range, Time Zone, Tunnel Zone, URL, Variable, Variable Set, VLAN Tag, and VPN. The VPN category is expanded, showing sub-items: Certificate Map, Custom Attribute, Group Policy, IKEv1 IPsec Proposal, IKEv1 Policy, and **IKEv2 IPsec Proposal** (highlighted with a red box). The main content area is titled "IKEv2 IPsec Proposal" and contains a description: "IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can specify the encryption and authentication algorithms. During IKEv2 negotiations, the peers select the most appropriate options that each support." Below the description is a table with the header "Name" and four entries: [AES-GCM](#), [AES-SHA](#), [DES_SHA-1](#), and [Umbrella-AES-GCM-256](#). In the top right corner, there is a blue button labeled "Add IKEv2 IPsec Proposal" with a red arrow pointing to it.

e) Nomeie a Proposta IKEv2 IPsec e certifique-se de que as mesmas configurações sejam alinhadas. Quando terminar, clique em Salvar.



Note: Você pode fazer referência a esses valores no arquivo de configuração baixado em `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

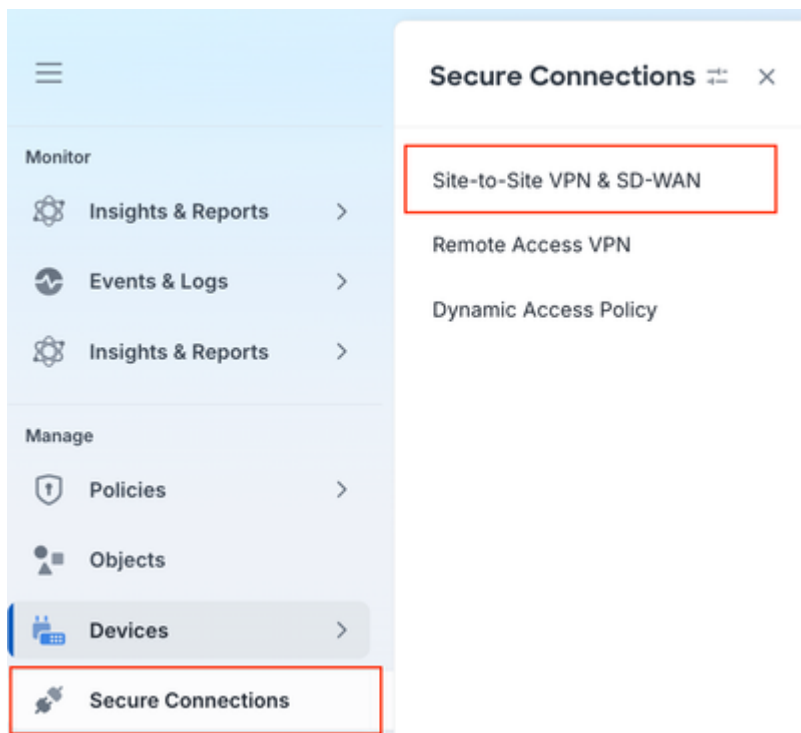


Cancel

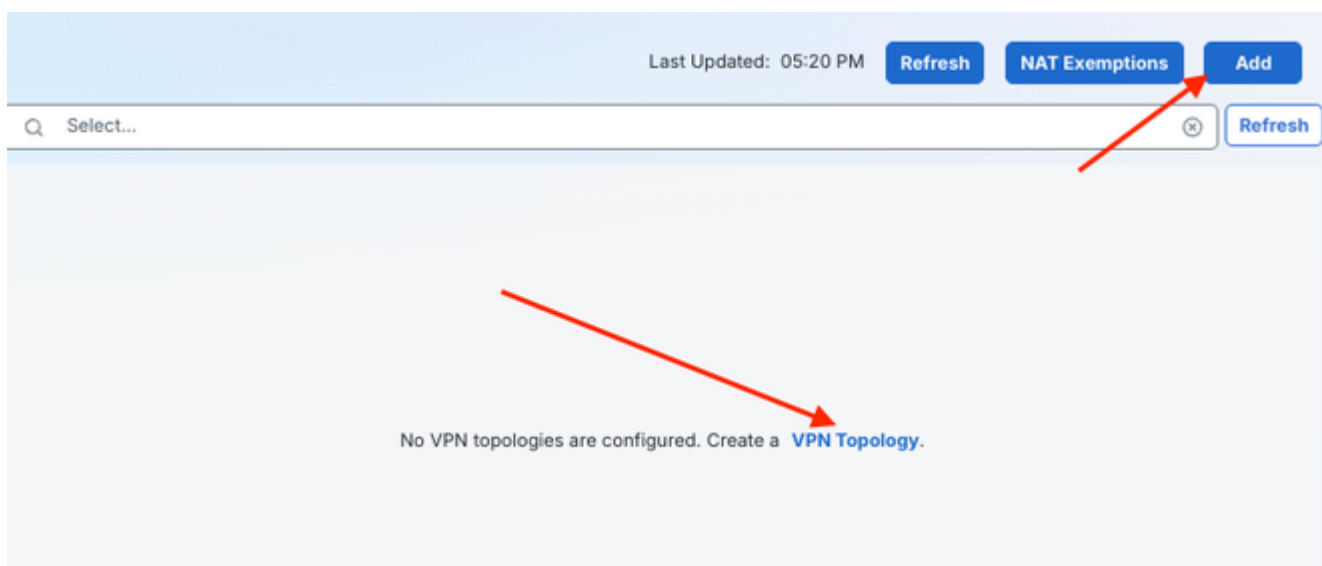
Save

Passo 4: Configurar Conectividade Segura para o Azure

a) Navegue até Manage > Secure Connections > Site-to-Site VPN & SD-WAN.



b) Clique no hiperlink de configuração inicial da Topologia VPN no meio ou clique em Adicionar.



c) Insira um nome de topologia para o primeiro túnel para a Instância0 do Azure, clique no botão de opção VPN Baseada em Rota e clique no tipo de topologia VPN Ponto a Ponto. Depois de concluído, clique em Criar.

Create VPN Topology

Topology name *

Azure-VTI-Instance0

VPN Type

☐ SD-WAN Topology

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

Select VPN Topology

☐ Hub and Spoke

Prerequisites

☒ **Route-Based VPN**

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

Select VPN Topology

☐ Hub and Spoke

☒ **Peer to Peer**

☐ Policy-Based VPN

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

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

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

[Prerequisites](#)

[Refresh](#)

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

d) Para o Node A, clique na lista suspensa Device e escolha o nome do par HA FTD/FTD gerenciado no qual a configuração está sendo implantada. Para o Nó B, como é a extremidade remota da conexão na topologia que termina nas instâncias vWAN do Azure, escolha Extranet na lista suspensa Dispositivo. Em seguida, para o Nó A, clique no ícone + ao lado da lista suspensa Interface de túnel virtual (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) Dê um Nome ao primeiro VTI e verifique se ele está Habilitado. Atribua uma zona de segurança nova ou existente ao VTI, atribua a origem do túnel e escolha o endereço IP na lista suspensa adjacente.

The screenshot shows the 'Add Virtual Tunnel Interface' configuration page. It includes a 'Tunnel Type' section with 'Static' selected. The 'Name' field is 'Azure-VTI-0'. The 'Enabled' checkbox is checked. The 'Description' field is empty. The 'Security Zone' dropdown is set to '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: the first is set to 'Ethernet1/1 (Outside)' and the second is set to 'Dynamic'. Red arrows point to the 'Name', 'Security Zone', 'Tunnel ID', and the first 'Tunnel Source' dropdown.

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) Em seguida, verifique se o botão de opção Borrow IP (IP unnumbered) está selecionado e escolha o mesmo loopback na lista suspensa à direita. Clique em OK depois de concluir.

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)

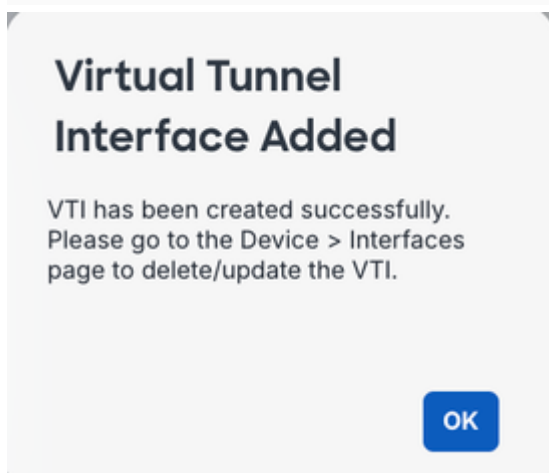
Tunnel Source:*

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



g) Depois que o VTI for configurado e aplicado, preencha manualmente o endereço IP origem do túnel (ele será preenchido automaticamente se o endereço da interface pai for preenchido a partir do DHCP) e verifique se o nome do dispositivo Node B está configurado, bem como o endereço IP do ponto final da instância. Depois de concluir, clique na guia IKE.



Note: Você pode referenciar o valor do Endereço IP do ponto final Instance0 no arquivo de configuração baixado em `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) Role para baixo até IKEv2 Settings e verifique se Authentication Type está definido como Pre-shared Manual Key, e insira a PSK configurada no Azure nas etapas anteriores. Configure as Políticas da Fase 1 do IKEv2 clicando no ícone do lápis para editar as políticas disponíveis do IKEv2.



Note: Note: Você pode fazer referência à chave pré-compartilhada no arquivo de configuração baixado em `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) Adicione a política IKEv2 fase 1 configurada inicialmente na etapa 3.

IKEv2 Policy



Available IKEv2 Policy 



 Search

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

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

j) Selezione a guida 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 a Proposta IKEv2 IPsec em Transform Sets clicando no ícone do lápis.

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) Clique no ícone da lixeira para remover o conjunto de transformação padrão AES-GCM e adicione a proposta personalizada do conjunto de transformação Azure_IPsec/IPsec IKEv2 criada na segunda metade da Etapa 3. Clique em OK.

IKEv2 IPsec Proposal



Available Transform Sets  +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec 

Cancel

OK

m) Role para baixo e insira 27000 para a duração do tempo de vida correspondente aos parâmetros do Azure. Habilite o grupo PFS, se aplicável. Click Save.



Note: Você pode fazer referência ao valor do tempo de vida no arquivo de configuração baixado em `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) Implante as alterações.

Search Deploy

Search Device Advanced Deploy **Deploy All**

☐ FTD

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

o) Quando a implantação terminar, verifique em Manage > Secure Connections > Site-to-Site VPN & SD-WAN em Tunnel Status Distribution; a conectividade bem-sucedida reflete Verde (ativado).

Last Updated: 11:11 PM Refresh NAT Exemptions Add					
Q Select... Refresh					
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✎ ✕

Com o primeiro túnel implantado, confirme se ele se estabelece com êxito nas camadas IKE/IPsec e BGP antes de configurar o segundo túnel para redundância.

Passo 5: Verificar Conectividade Inicial com o Azure

a) Use SSH no FTD e insira `system support diagnostic-cli`, digite `en` e pressione Enter, pois não há senha na CLI do FTD somente leitura.

```
<#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) Verifique o status do túnel das fases 1 e 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) Execute capturas para verificar os pacotes do Protocolo de Controle de Transmissão (TCP) BGP recebidos do Azure no túnel e o tráfego da Network Address Translation - Traversal (NAT-T) User Datagram Protocol (UDP) porta 4500/UDP porta 500 na captura externa do IP público do Túnel do Azure da Instância-0.

```
<#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#
```

Com a conectividade com a Instance0 confirmada, repita a mesma configuração de topologia de VTI e VPN para a Instance1 de modo que ambas as instâncias de gateway do Azure estejam acessíveis.

Passo 6: Configurar o Segundo Túnel para o Ponto de Extremidade da Instância1 do Azure

a) Crie o Segundo VTI (Azure-VTI-1) tomando emprestado do mesmo loopback (Etapa 3 b-f).

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

Tunnel ID:*
 (0 - 10413)

Tunnel Source:*

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

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☐ Configure IP
☒ Borrow IP (IP unnumbered)

VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b) Configure a topologia de VPN de segunda instância (Etapa 4 g-n).



Note: Você pode referenciar o valor do Endereço IP do ponto final Instance1 no arquivo de configuração baixado em `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) Implante alterações de configuração e verifique o status do 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) Fazendo check-in no Azure, Instance0 e Instance1 produzem Connected.

Links

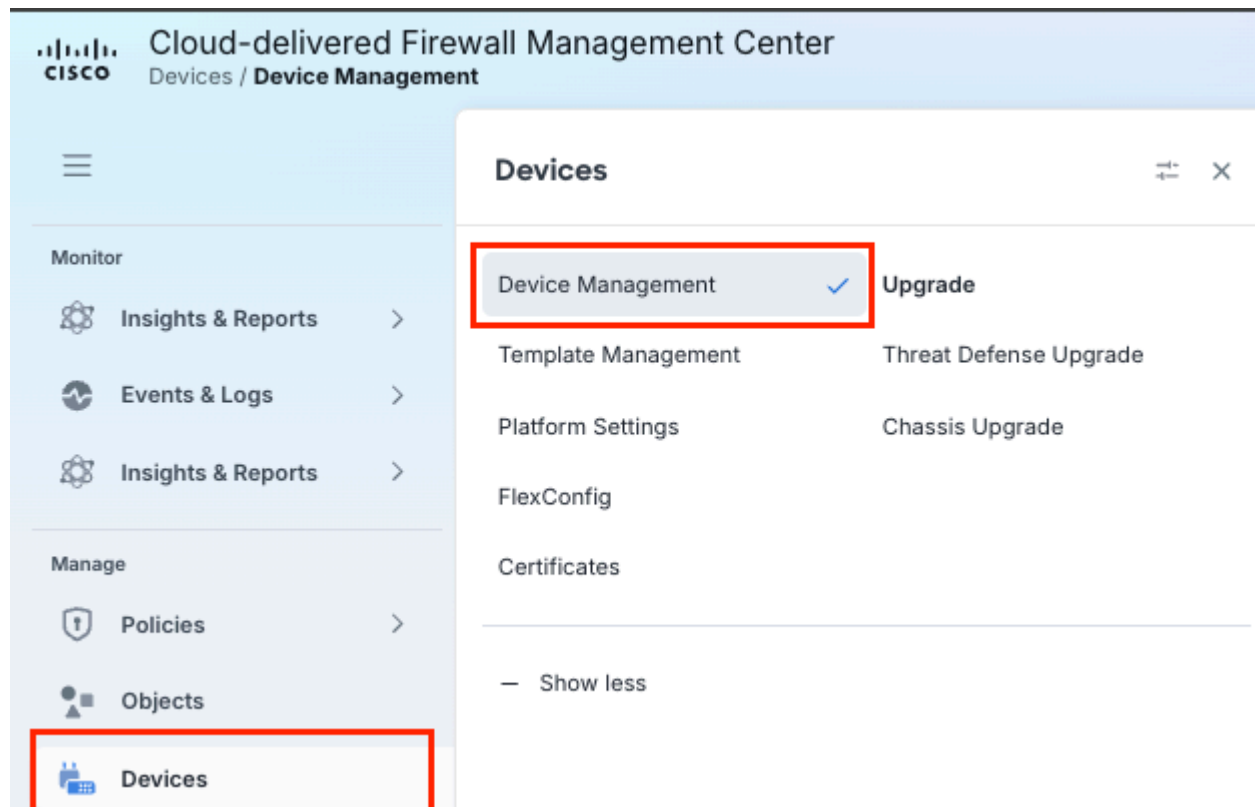
☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Com ambos os túneis ativos, o FTD precisa do roteamento ECMP para que o tráfego possa usar ambos os caminhos ao mesmo tempo, em vez de tratar o segundo túnel como um standby

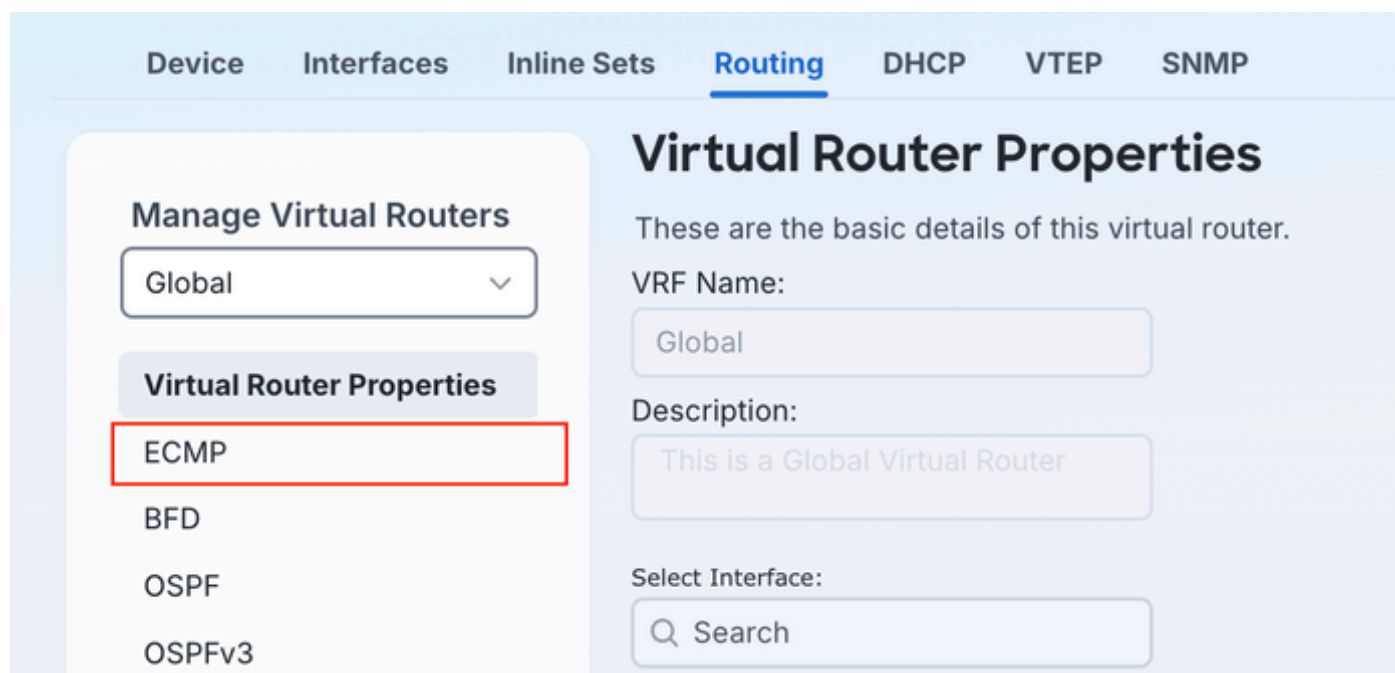
passivo.

Passo 7: Configurar ECMP

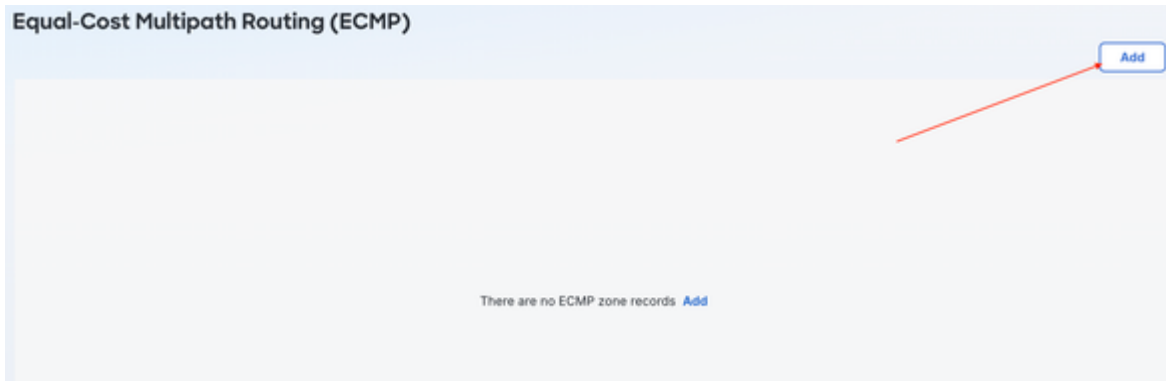
a) Navegue para Manage > Devices > Device Management e selecione o FTD configurado com VPNs para o Azure.



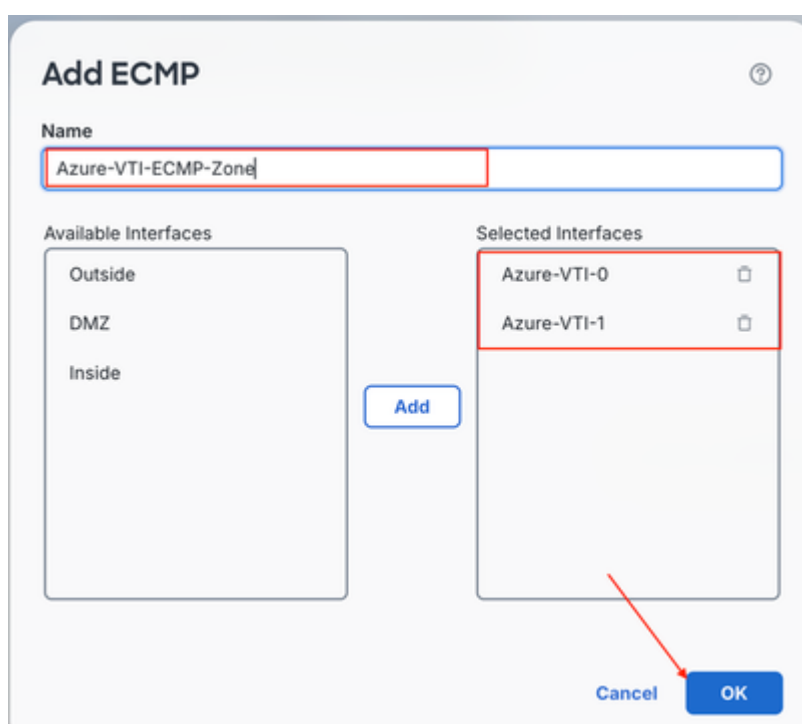
b) Clique na guia Routing e escolha ECMP.



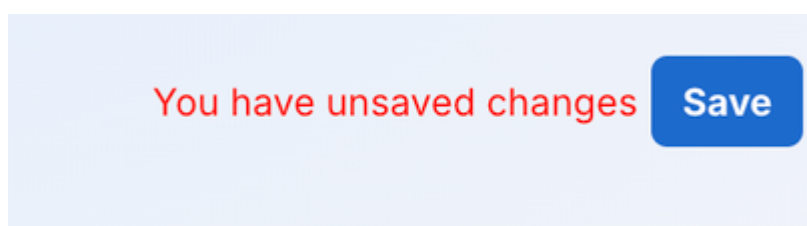
c) Clique em Add para criar uma nova zona ECMP.



d) Alterne para realçar os VTIs clicando em ambos os VTIs no painel Interfaces disponíveis e clique em Adicionar para aplicar os VTIs à Zona ECMP nomeada.



e) Depois de confirmar que as configurações estão corretas, clique em Save.



Passo 8: Configurar rotas estáticas para IPs privados de instância

O BGP requer rotas para se conectar com êxito aos vizinhos e, como os pontos finais não estão diretamente conectados, nenhuma rota é preenchida por padrão. O ECMP permite que você configure rotas estáticas com a mesma métrica (Distância Administrativa) para o mesmo destino, de modo que ambas as rotas sejam instaladas na Base de Informações de Roteamento (RIB) e usadas simultaneamente.

a) Navegue até Manage > Devices > Device Management e escolha o dispositivo FTD aplicável.

CISCO Cloud-delivered Firewall Management Center
Devices / Device Management

Monitor

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

Manage

- Policies >
- Objects
- Devices**

Devices

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

— Show less



b) Navegue até Roteamento > Rota estática.

FTD

Cisco Firepower 1010 Threat Defense

Monitor

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

Manage

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

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

Manage Virtual Routers

Global

Virtual Router Properties

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

Network ▲ Inte

IPv4 Routes

IPv6 Routes

c) Clique em + Add Route.

+ Add Route

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

d) Adicione rotas para ambos os endereços IP da Instância criando a primeira rota para o VTI da Instância0 e adicione o objeto de rede de destino para ele clicando no sinal + ao lado de Available Network. Em seguida, clique no objeto de rede da lista e clique no botão Add para adicioná-lo como o destino da rota estática. Certifique-se de escolher o IP da Instância0 e ele esteja definido como o Gateway. Depois de concluir, clique em OK.



Note: Esses valores de rede de destino da rota estática estão sob `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` e

vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1 no arquivo de configuração baixado.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*:

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

Available Network +

Selected Network

Azure-Instance0-BGP_Peer

Azure-Instance1-BGP_Peer

Ensure that egress virtualrouter has route to that destination

Gateway: +

Metric: (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e) Repita as etapas c-d para adicionar a segunda rota estática através do VTI da Instância 1. Certifique-se de clicar em Salvar para salvar suas alterações.

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						

As rotas estáticas só alcançam os endereços de peering BGP; O próprio BGP ainda deve ser habilitado e correspondido para que o Azure e o FTD troquem rotas dinamicamente de/para redes maiores entre si.

Etapa 9: Configurar BGP

a) Ative o BGP Process 65500 no FTD em Routing > General Settings > BGP. Marque a caixa de seleção Enable BGP e insira o número AS configurado anteriormente na Fase 2, Etapa 1. Navegue ao lado de Routing > BGP > IPv4.

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id
Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

b) Habilite o roteamento BGP IPv4 para 65500 de processo/AS marcando a caixa de seleção adjacente Habilitar IPv4 e clique em Vizinho para configurar vizinhos 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) Clique em + Adicionar.

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) Insira as informações de peering de BGP da Instance0, faça referência ao BGP AS anotado do hub vWAN e digite-o como o AS Remoto do Vizinho, e adicione uma descrição se desejar. Clique em Advanced (Avançado).



Importante: Certifique-se de alterar a Origem de Atualização do BGP para fazer referência ao pai de Loopback de ambas as interfaces VTI no FTD.

Add Neighbor

IP Address*
10.2.0.12

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

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

BFD Fallover
none

Update Source:
bgpVPNBranchLo

Description
Instance0 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

e) Dentro do menu Advanced da configuração do Vizinho do BGP no FTD, você pode alterar o número de saltos TTL do eBGP padrão de 1 salto para um número variável. Os pontos de extremidade do BGP do Azure não estão diretamente conectados pelo túnel na infraestrutura do Azure, e tende a haver mais saltos para o ponto de extremidade do que o TTL do eBGP padrão de 1 permite.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Repita as mesmas etapas para o Peer BGP da Instância1 do 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

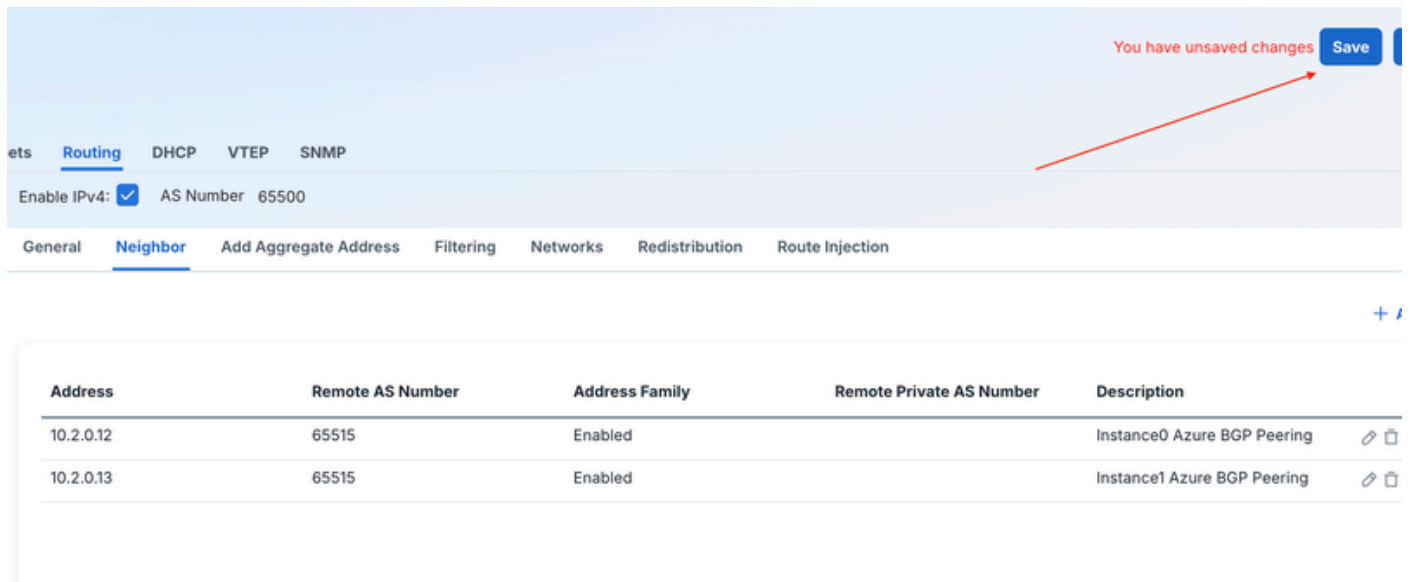
Filtering Routes Routes Timers **Advanced** Migration

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops
50
(1-255)

g) Certifique-se de Salvar as alterações depois de concluí-las.



Por padrão, o BGP instala apenas um único melhor caminho na tabela de roteamento, mesmo que o ECMP disponibilize ambas as rotas estáticas. O multipath de BGP deve ser habilitado separadamente para que ambos os caminhos aprendidos sejam instalados e usados ao mesmo tempo.

Etapa 10: Configurar o multipath de BGP

a) Navegue até Routing > BGP > IPv4, clique na guia General e clique no ícone de lápis adjacente a Forward Packets Over Multiple Paths.

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

Enable IPv4: ☒ AS Number 65500

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

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

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

b) Altere o valor padrão do campo Número de caminhos de 1 para 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Certifique-se de salvar e implantar as alterações.

Verificar

Após a conclusão da implantação, confirme se o BGP forma adjacências com ambas as instâncias do Azure. Posteriormente, confirme se as rotas foram aprendidas em ambos os túneis e se o tráfego usa ambos os VTIs, usando o mesmo acesso de diagnóstico CLI estabelecido na Fase 3, Etapa 5.

Navegue até `system support diagnostic-cli` em FTD CLI.

a) Uma vez implantado, espera-se que os vizinhos BGP apareçam e os prefixos sejam recebidos.

```
<#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) Verifique se as rotas recebidas do Azure são mostradas como rotas de vários caminhos.

```
<#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 a contagem de pacotes 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 as rotas estáticas para vizinhos 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) Confirme as 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 a configuração do 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 tabela de roteamento.

<#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
```

Outras considerações

A configuração básica neste documento pressupõe uma única interface externa e um único ISP no FTD da filial. Essas considerações estendem esse projeto.

AS-Path Prepending

Se você precisar influenciar qual dos dois túneis o Azure ou o FTD prefere como primário, em vez de compartilhar a carga igualmente através de multipath de ECMP e BGP, coloque o número AS local uma ou mais vezes adicionais no vizinho de BGP a ser tratado como secundário. O vizinho com o caminho AS mais longo e prefixado é priorizado durante a seleção do melhor caminho BGP padrão, sem a necessidade de remover esse vizinho da zona ECMP inteiramente.

Troubleshooting

- O túnel da Fase 1/Fase 2 não é ativado: Confirme se a chave pré-compartilhada e os parâmetros de política IKEv2/IPsec (criptografia, integridade, PRF, grupo DH e tempo de vida) correspondem exatamente entre a proposta de política IKEv2/IPsec do FMC e os valores no arquivo de configuração de VPN do Azure baixado. Use `show crypto isakmp sa` e `show crypto ipsec sa`, como mostrado na Fase 3, Etapa 5.
- O túnel está ativo, mas os vizinhos BGP não formam `update-source: ebgp-multihop`. Verifique se o BGP está definido como a interface de loopback, não o VTI em si, e se ele está configurado com um valor alto o suficiente para acessar o endereço de peering do BGP do Azure, que não está diretamente conectado ao FTD.
- O BGP se forma, mas apenas um túnel transporta tráfego: Confirme se ambos os VTIs são membros da mesma zona ECMP, se as rotas estáticas para ambos os endereços BGP da instância do Azure estão instaladas com a mesma distância administrativa e se o multipath de BGP está configurado para dois caminhos, conforme descrito na Fase 3, Etapa 10.
- Sem tráfego de retorno ou roteamento assimétrico para o Azure: Como o Azure vWAN anuncia o espaço de endereço de hub em ambos os túneis, certifique-se de que o ECMP não esteja desabilitado em nenhum outro lugar na configuração de roteamento e verifique os mapas de rotas ou o roteamento baseado em políticas que possam fixar o tráfego em um único caminho.
- O BGP está ativo e as rotas estão instaladas, mas o tráfego parece estar bloqueado: Verifique se você tem as regras de controle de acesso configuradas com a zona de segurança atribuída aos VTIs, permitindo que o tráfego entre e saia.

Informações Relacionadas

- [O que é a WAN Virtual do Azure?](#)
- [Como configurar o BGP para o Gateway VPN do Azure](#)
- [Diretivas IPsec Padrão vs. Personalizadas vWAN do Azure](#)

- [Solucionar problemas de BGP para o Gateway VPN do Azure](#)
- [Sobre os gateways VPN do modo ativo-ativo](#)
- [Tutorial: Criar uma conexão site a site usando a WAN Virtual do Azure](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.