

Configurar a Conectividade vWAN do ISP Duplo do Azure no Firewall Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama](#)

[Links Dual Direct Internet Access \(DIA\) \(Balanceamento de Carga/Redundância Azure + FTD\)](#)

[Configurar](#)

[Fase 1: Configuração do Site VPN vWAN do Azure](#)

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

[Passo 2: Configurar Parâmetros de Gateway APIPA do Azure](#)

[Passo 3: Configurar Parâmetros VPN do Site vWAN do Azure](#)

[Passo 4: Habilitar e Ativar o BGP APIPA Personalizado em Instâncias de Link de Site VPN](#)

[Passo 5: Fazer download do arquivo de configuração do site VPN](#)

[Fase 2: Configurar FTD para Conectividade ISP Dupla com vWAN do Azure](#)

[Passo 1: Analisar a configuração de VPN baixada](#)

[Passo 2: Configurar interfaces de loopback de origem de atualização de BGP de link](#)

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

[Passo 4: Configurar interfaces de túnel virtual \(VTI\)](#)

[Passo 5: Provisionar Topologias VPN IPsec](#)

[Passo 6: Validar Topologias VPN](#)

[Passo 7: Configurar ECMP](#)

[Passo 8: Configurar BGP](#)

[Etapa 9: Configurar o multipath de eBGP](#)

[Verificar/solucionar problemas](#)

Introdução

Este documento descreve como configurar a Conectividade VPN Site a Site da WAN Virtual (vWAN) do Microsoft Azure para o Firewall Seguro usando links WAN duplos.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- WAN Virtual do Microsoft Azure (vWAN)
- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Verifique se esses componentes foram configurados inicialmente no ambiente do Azure:

- Instância do Microsoft Azure vWAN
- Hub vWAN do Microsoft Azure

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
- vWAN do Microsoft Azure

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

Quando o FTD da filial tem duas interfaces externas voltadas para o Provedor de Serviços de Internet (ISP), cada uma pode se conectar de forma redundante e ativa ao vWAN do Azure, para que cada link do ISP seja utilizado. O Azure vWAN cria dois túneis IPsec por Link de Site — um para a Instância0 do Hub do Azure e um para a Instância1 — de modo que cada interface do ISP termine dois túneis. Em ambos os links ISP, isso resulta em quatro túneis IPsec terminando no FTD.

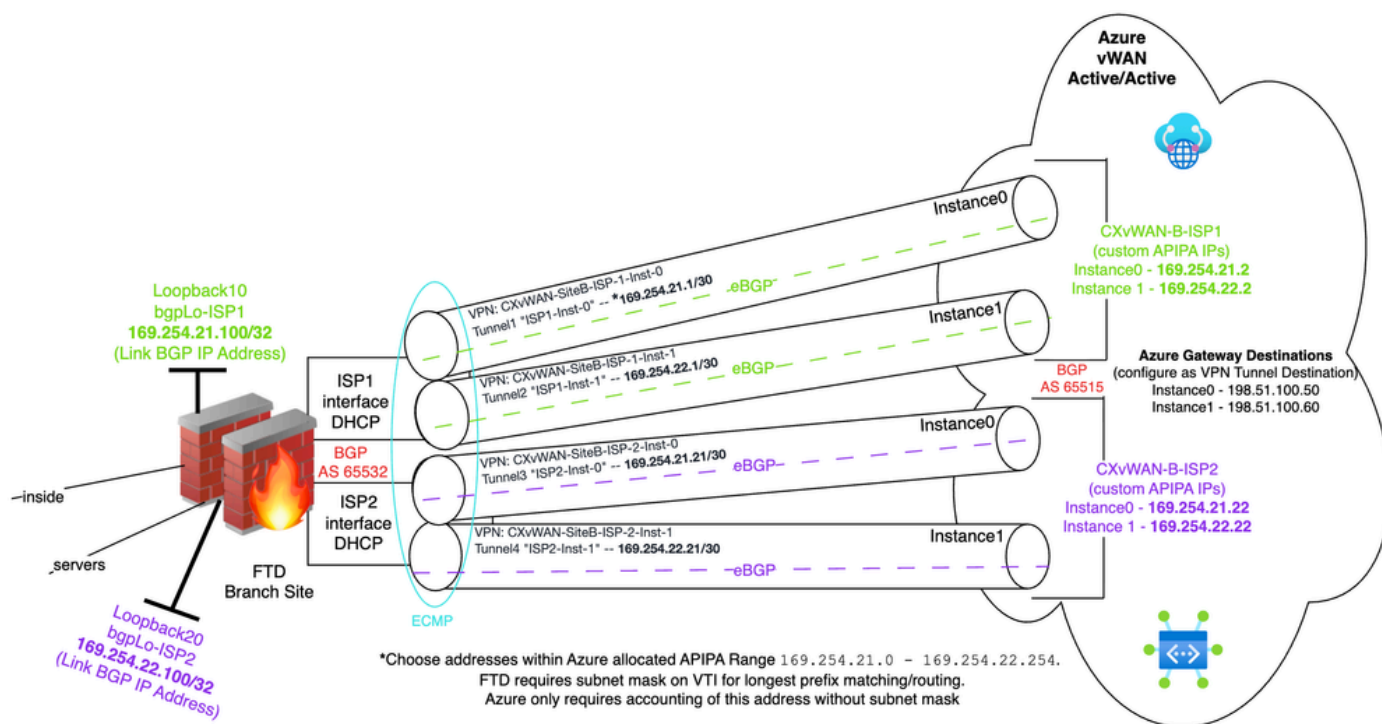
As Instâncias do Azure operam no modo Ativo/Ativo para balanceamento de carga e redundância, portanto, o FTD reflete isso através da configuração do Equal-Cost Multi-Pathing (ECMP) em todos os quatro túneis IPsec. Usando endereços IP privados automáticos (APIPA - Automatic Private IP Addressing) personalizados, as vizinhanças de protocolo de gateway de borda externo (eBGP - Border Gateway Protocol) com números de sistemas autônomos privados (ASNs -

Private Autonomous System Numbers) distintos são estabelecidas sobre cada um dos quatro túneis. Isso habilita a funcionalidade de vários caminhos BGP, fornecendo vários caminhos redundantes para cada par de Instâncias de Link de Site de Hub do Azure.

Diagrama

O diagrama mostra a topologia da configuração descrita neste artigo. A variante de link de Acesso Direto à Internet (DIA) dupla origina os túneis do Azure de duas interfaces externas no FTD.

Links Dual Direct Internet Access (DIA) (Balanceamento de Carga/Redundância Azure + FTD)



Topologia de conectividade de acesso duplo direto à Internet

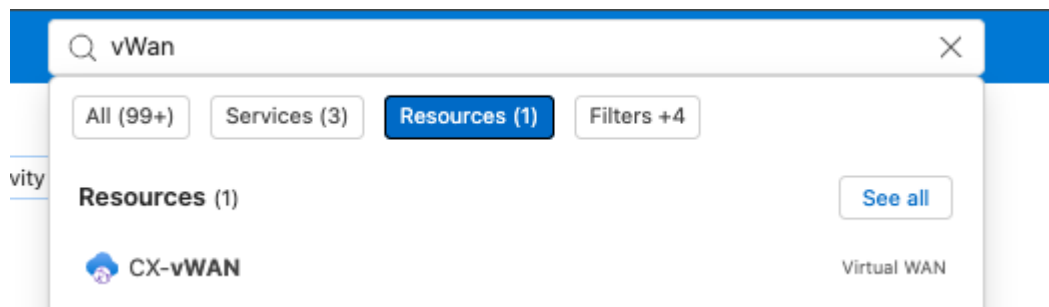
Configurar

Fase 1: Configuração do Site VPN vWAN do Azure

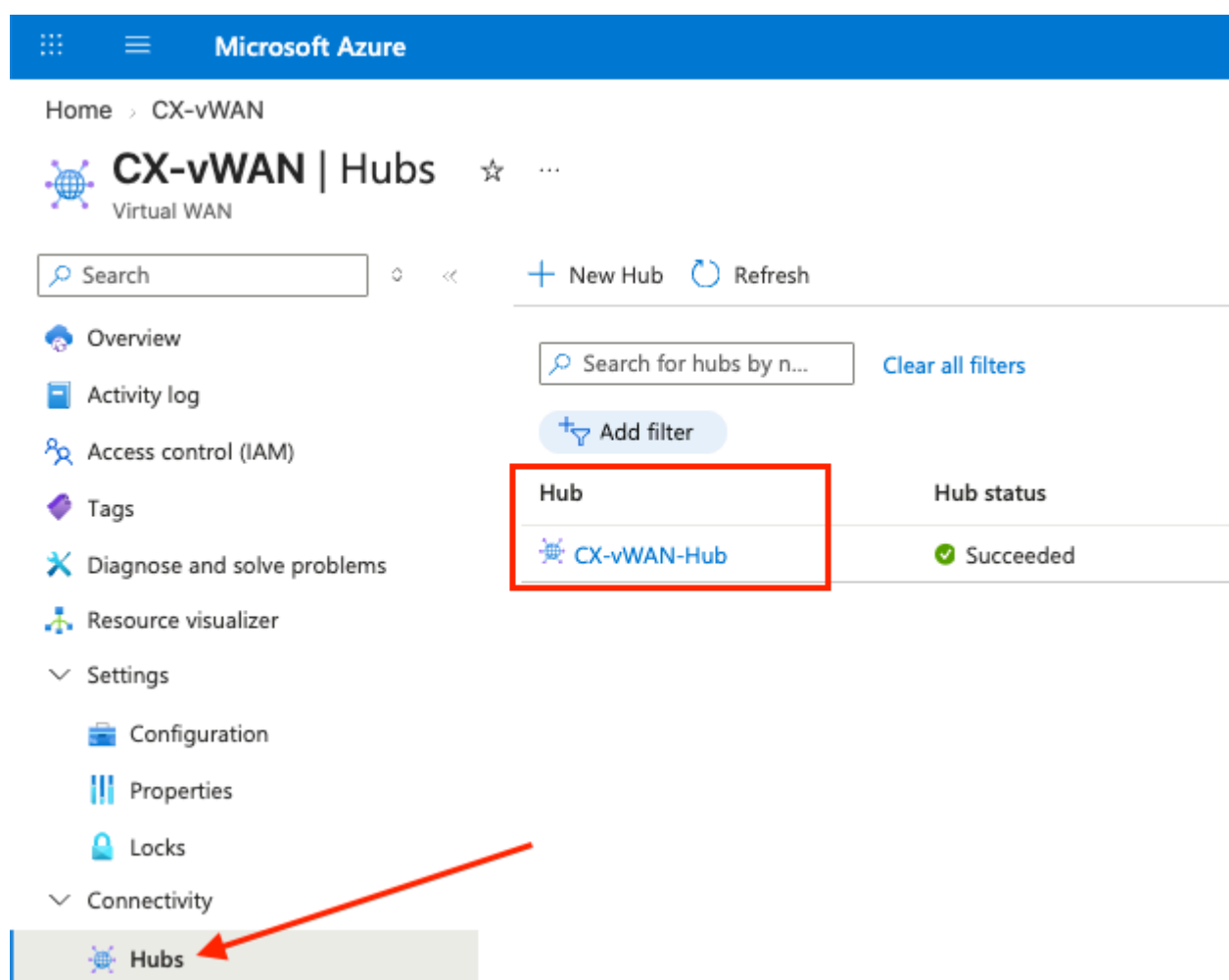
Passo 1: Criar Site VPN vWAN do Azure (Dispositivo FTD Remoto)

1) Procure vWAN no campo de pesquisa do Azure, clique em WANs virtuais para entrar no Hub

vWAN do Azure existente. Em seguida, navegue para Conectividade > Hubs e clique no Hub vWAN do Azure existente.



Pesquisar consulta por WAN virtual



Selecionar Hub WAN virtual existente

2) 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		

Criar novo local de WAN virtual



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

3) Informe 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 *	Dual-ISP-Site ✓
Device vendor *	Cisco ✓
Private address space	

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

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

Previous

Next : Links >

Configurações gerais do site VPN

4) Insira as informações de link necessárias. O Endereço BGP de Enlace e o ASN de Enlace são o endereço de destino BGP da Camada 3 do túnel interno e o número BGP AS no lado da filial com o qual a vizinhança é formada nos túneis de site para 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 configurada, que o Azure instala como uma rota /32 para acessar como um vizinho BGP. Duas interfaces de loopback são criadas em seções posteriores no FTD para representar o endereço BGP de link para cada um dos links de site duplo. O endereço IP do link/FQDN (Fully Qualified Domain Name) é o endereço IP de destino do cabeçalho externo da Camada 3 do tráfego que vai para o local da filial necessário para provisionar a conectividade IPsec (IP Security)/IKEv2 (Internet Key Exchange version 2). Vá para a próxima etapa quando terminar clicando em Avançar : Revisar + criar >.



Note: Certifique-se de revisar a documentação específica do Azure se estiver usando endereços que variam de 169.254.21.0 a 169.254.22.255 para endereços de túnel:

Escolhendo endereços APIPA BGP.

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

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

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

Previous

Next : Review + create >

Configurar Parâmetros de Link de Site

5) Depois que as informações forem confirmadas como pretendidas, clique em Criar.

Create VPN site ...

 Validation passed

basics links Review + create

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

Basics

Region	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	
Links	

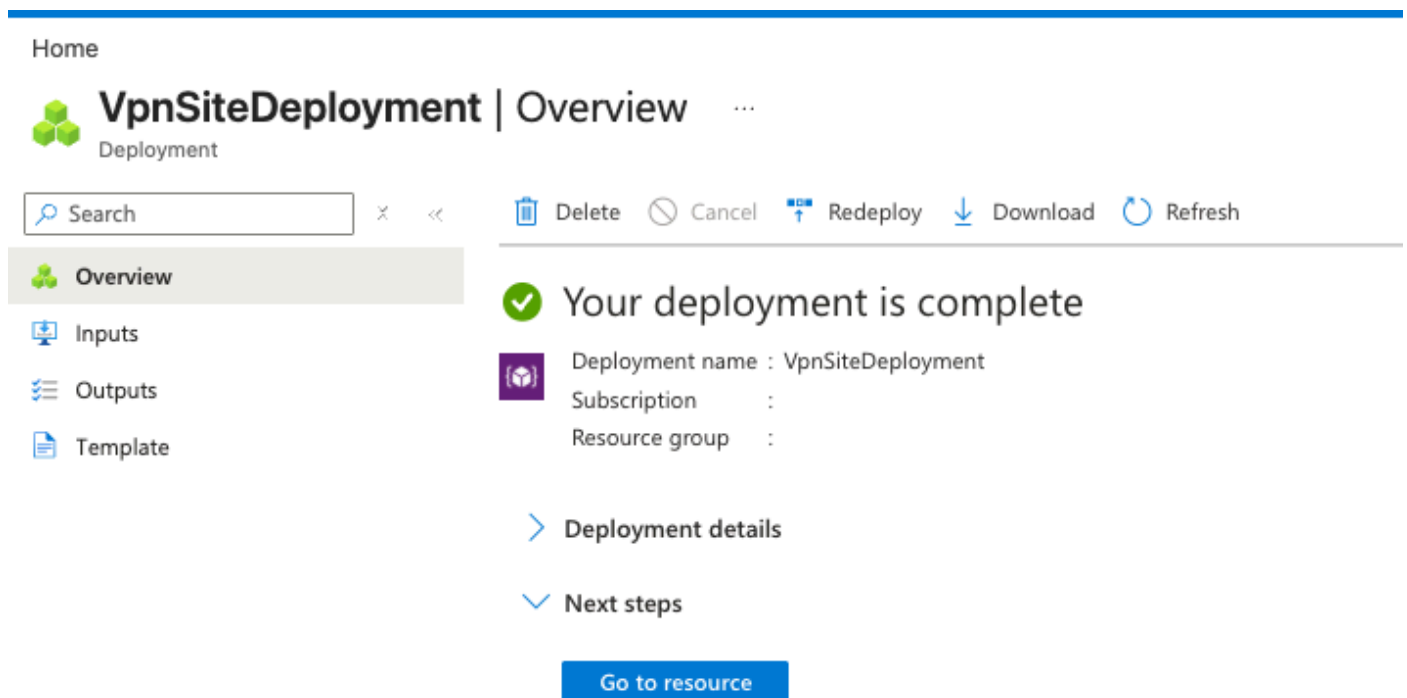
Link name	ISP-1-Link
Link provider name	ISP1
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.21.100

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

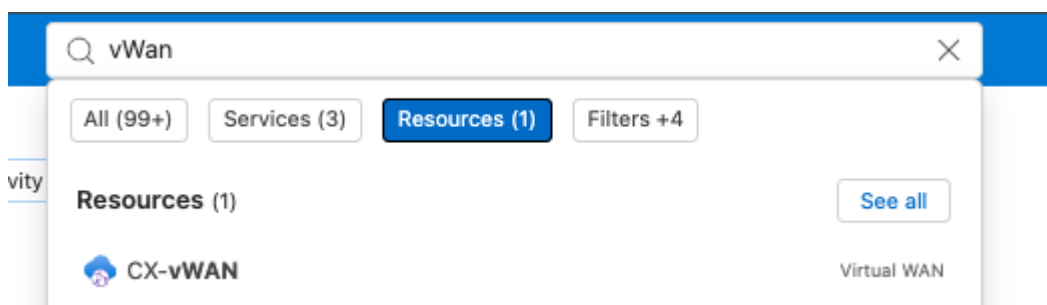
 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Revisar e criar um novo site VPN

6) Quando a implantação do site VPN for concluída, navegue de volta para a configuração do vWAN Hub.



Progresso da Implantação do Local da WAN Virtual



Pesquisar consulta por WAN virtual

Passo 2: Configurar Parâmetros de Gateway APIPA do Azure

O Azure requer configuração extra para endereços APIPA (Automatic Private IP Addressing) dentro do espaço de endereço 169.254.0.0/16 IPv4.

1) Entre no hub existente via Connectivity > Hubs.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Navegue até a conectividade do Virtual WAN Hub

2) Navegue mais uma vez para Connectivity > VPN (Site to site) e clique no hiperlink Gateway Configuration.

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

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

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

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites 1

Hiperlink de configuração do gateway de acesso

3) Um painel lateral aparece para Edit VPN Gateway. Em VPN Gateway Instance0 e VPN Gateway Instance1, insira dois endereços IP BGP personalizados exclusivos que atuem como IPs vizinhos a cada instância para vizinhos BGP sobre túneis IPsec. Isso é necessário se você optar por usar o endereçamento APIPA dentro dessa topologia. No campo rotulado Endereço de Par, insira o IP do vizinho BGP a ser usado para acessar as Instâncias do Azure a partir do FTD. O Azure não tentará o estabelecimento do BGP com o FTD se o endereçamento APIPA estiver em uso, portanto o FTD tentará o estabelecimento do vizinho eBGP sobre cada túnel com o Azure.

O total sai para 2 enlaces x 2 túneis implícitos; um túnel para Instance0 e Instance1 por link do ISP; o total chega a quatro túneis IPsec com vizinhanças BGP entre o Azure e as duas interfaces FTD ISP.

Esses endereços devem ser exclusivos e, nesta demonstração, o segundo e último endereço de host nas sub-redes /30 atribuídas a cada túnel deve ser configurado no FTD para uso. Depois de configurado, clique em Editar.



Note: Certifique-se de revisar a documentação específica do Azure se estiver usando endereços que variam de 169.254.21.0 a 169.254.22.255 para endereços de túnel:
[Escolhendo endereços BGP APIPA](#)

Edit VPN Gateway



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

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ



Microsoft network



Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address



VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



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

Edit

Cancel

Editar endereços IP BGP personalizados do gateway VPN



Note: Como o Azure observa, isso pode levar até 30 minutos ou mais para ser atualizado.

Passo 3: Configurar Parâmetros VPN do Site vWAN do Azure

1) Na página Conectividade > VPN (Site a site) na configuração do Hub vWAN do Azure e clique no X para limpar a Associação de Hub: Filtragem conectada para exibir sites VPN desconectados.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > CX-vWAN | Hubs > CX-vWAN-Hub. The main heading is 'CX-vWAN-Hub | VPN (Site to site)'. Below this, there's a search bar and a row of action buttons: Download VPN Config, Packet Capture, Delete gateway, Reset gateway, and Monitor Gateway. The left sidebar contains a navigation menu with 'Overview', 'Connectivity' (highlighted with a red box), 'ExpressRoute', 'User VPN (Point to site)', 'Routing', 'Security', 'Third party providers', and 'Monitor'. Under 'Connectivity', 'VPN (Site to site)' is also highlighted. The main content area shows the 'VPN Sites' tab. It includes a search bar labeled 'Search this page' and a 'Clear all filters' link. Below this, there's a filter bar with the text 'Hub association : Connected' and a red 'X' icon next to it, which is pointed to by a red arrow. There's also an 'Add filter' button. At the bottom, there's a message box with an information icon and the text: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Limpar Filtros de Conexão de Associação de Hub

2) Marque a caixa de seleção ao lado do site VPN provisionado recentemente e clique em Connect VPN Site.

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

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

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

VPN Sites Metrics

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



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

+ Create new VPN site

 **Connect VPN sites**

 Disconnect VPN sites

 Refresh

Page:

Site name

↑↓ Location

☒  **Dual-ISP-Site**

Ação Conectar Local VPN

3) Configure a chave pré-compartilhada (PSK) desejada e configure os parâmetros IPsec desejados clicando na opção de alternância Personalizar. Esses parâmetros de IPsec devem corresponder à configuração do FMC/FTD nas etapas posteriores. Para salvar, clique em Conectar.



Note: O suporte ao Diffie-Hellman (DH) Group 24 foi removido na versão 6.7 do FTD/FMC.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

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

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

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

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

Connect

Configurar parâmetros de chave pré-compartilhada e IPsec

4) Confirme se o provisionamento do site VPN foi concluído com êxito.

Notifications



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

[Dismiss all](#)



Successfully created VPN connection



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

a few seconds ago

Confirmar Status de Provisionamento do Site VPN

Passo 4: Habilitar e Ativar o BGP APIPA Personalizado em Instâncias de Link de Site VPN

1) Atualize a página VPN (Site to site) e confirme se a coluna Status de fornecimento de conexão indica seu sucesso, o que permite clicar nas reticências e clicar no item de menu suspenso Editar conexão VPN para este hub .

The screenshot shows a table of VPN connections. The table has columns: Site name, Location, Cloud provider, Connection Provisioning status, and Connectivity status. The first row shows a connection named 'Dual-ISP-Site' with location 'eastus' and a status of 'Succeeded'. A red box highlights the 'Succeeded' status. To the right of the table, a dropdown menu is open, showing three options: 'Edit VPN connection to this hub', 'Delete VPN connection to this hub', and 'Download VPN site configuration file'. A red arrow points to the dropdown menu.

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

- Edit VPN connection to this hub
- Delete VPN connection to this hub
- Download VPN site configuration file

Validar Êxito da Conexão e Editar Conexão VPN

2) Clique para configurar Link Connection 1 (ISP1) e insira novamente a Pre-Shared Key (PSK) aplicável, e certifique-se de clicar na opção Enable ao lado de Custom BGP IP Address, e mapeie qual seria o endereço de host restante das sub-redes /30 que serão os valores do campo de endereço IP de destino do túnel interno do cabeçalho IP BGP gerado pelos FTDs.

Em essência, o ISP1 VTI Tunnel1 para a Instância0 do Azure tem uma atribuição de endereço de 169.254.21.1/30, e o segundo ISP1 VTI Tunnel2 que termina no FTD tem um IP de 169.254.22.1/30 atribuído para a Instância1.

Clique em Next: Link Connection 2> para continuar com os parâmetros de link do ISP 2.



Note: É possível que você precise inserir novamente sua PSK e clicar novamente na opção Grupo PFS alinhado no menu suspenso no Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK)

.....

Connection Mode

Default Initiator Only Responder Only

Border gateway protocol

Disable Enable

Custom BGP IP Addresses

Disable Enable

Custom BGP IP Address

Instance 0

169.254.21.2

Instance 1

169.254.22.2

Use Azure Private IP Address

Yes No

Protocol

IKEv2 IKEv1

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

Use policy based traffic selector

Enable Disable

IPsec

Default Custom

SA Lifetime in seconds

27000

IKE Phase 1

Encryption

GCMAES256

Integrity/PRF

SHA384

DH Group

DHGroup14

IKE Phase 2(ipsec)

IPsec Encryption

GCMAES256

IPsec Integrity

GCMAES256

PFS Group

NONE

DPD timeout in seconds

45

Review + create

Previous

Next : Link connection 2 >

3) Repita as etapas anteriores e aplique os parâmetros aplicáveis em Link Connection 2 (link ISP2). Após a conclusão, clique em Criar.

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection **Enable** Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

Connection Mode ⓘ **Default** Initiator Only Responder Only

Border gateway protocol ⓘ Disable **Enable**

Custom BGP IP Addresses ⓘ Disable **Enable**

Custom BGP IP Address

Instance 0 ⓘ ▼

Instance 1 ⓘ ▼

Use Azure Private IP Address ⓘ Yes **No**

Protocol IKEv2 **IKEv1**

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

Use policy based traffic selector ⓘ Enable **Disable**

IPsec ⓘ Default **Custom**

SA Lifetime in seconds * ⓘ

IKE Phase 1 ⓘ Encryption * Integrity/PRF * DH Group *

GCMAES256 ▼	SHA384 ▼	DHGroup14 ▼
-------------	----------	-------------

IKE Phase 2(ipsec) ⓘ IPsec Encryption * IPsec Integrity * PFS Group *

GCMAES256 ▼	GCMAES256 ▼	NONE ▼
-------------	-------------	--------

DPD timeout in seconds * ⓘ

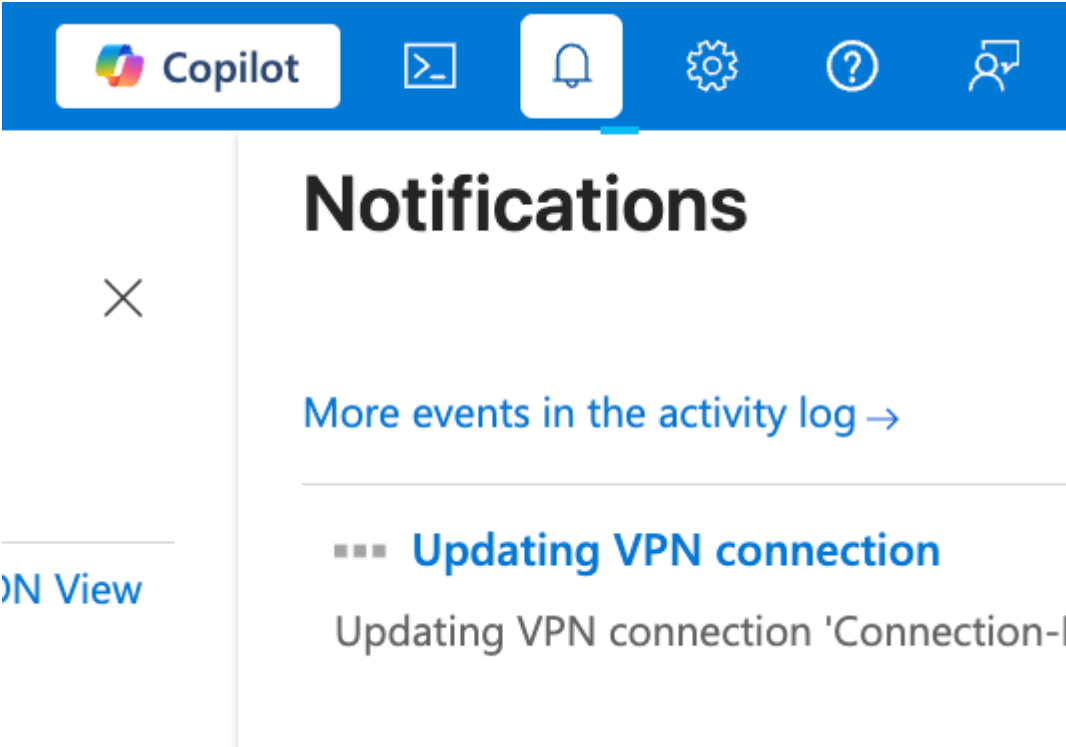
Create

Previous

Next

Configurar conexão de link Duas configurações de BGP personalizadas

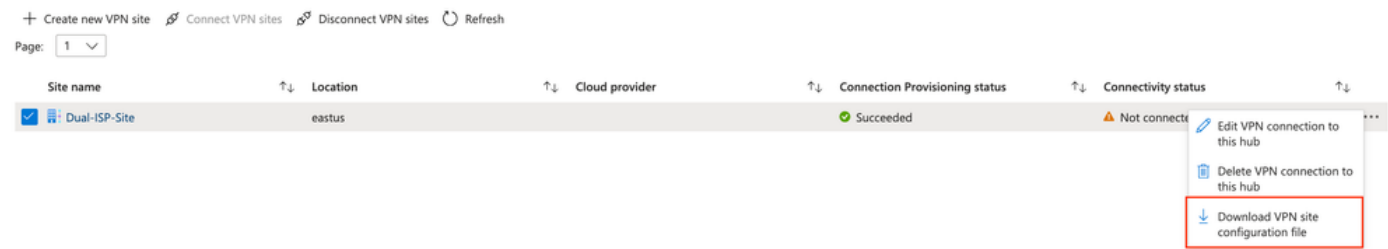
4) As notificações na interface do usuário do Azure mostram o início da tarefa de atualização.



Notificação de Início da Tarefa de Atualização do Azure

Passo 5: Fazer download do arquivo de configuração do site VPN

1) Na mesma página VPN (Site a Site) no Azure, escolha o ícone de reticências na extrema direita do site VPN configurado e escolha a opção Baixar arquivo de configuração do site VPN .



Opção Baixar Arquivo de Configuração de Site VPN

2) Clique no hiperlink Click here to download (Clique aqui para baixar).



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



Fazer download do arquivo de configuração do site VPN

Fase 2: Configurar FTD para Conectividade ISP Dupla com vWAN do Azure

Passo 1: Analisar a configuração de VPN baixada

1) Abra o arquivo de configuração baixado e uma saída JavaScript Object Notation (JSON) semelhante será exibida. A saída mostra um dos dois objetos gravados no arquivo. Essas informações fornecem um contexto útil para a configuração do FTD.



Note: Para maior focagem, vários objetos irrelevantes e pares de chave/valor são removidos por serem breves.



Note: A ordem do objeto JSON ISP-Link-1 no arquivo baixado é revertida. As reticências na saída do código representam o objeto ISP-2-Link com sua configuração aplicável.

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


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

Navegue Até Device Management No Firepower Management Center



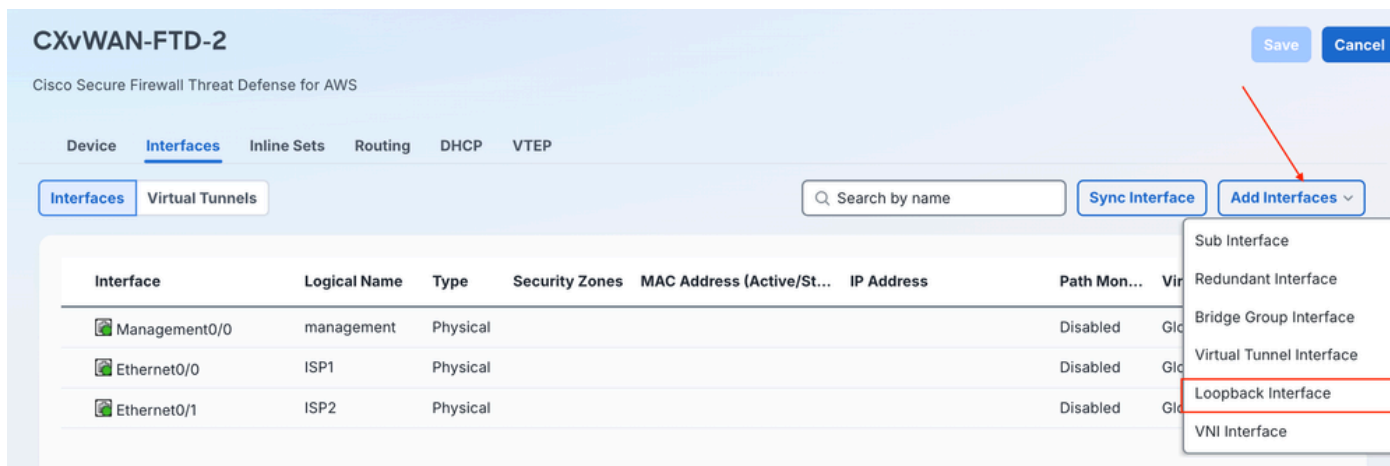
Note: Este laboratório usa o Centro de Gerenciamento de Firewall (cdFMC - Firewall Management Center) fornecido em nuvem; no entanto, as etapas continuam a ser as mesmas para o CVP local.

2) Clique no FTD que você está configurando como o dispositivo VPN de filial/site com conectividade ISP dupla.

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

Selecionar O FTD Para Implantação Da Configuração

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



Adicionar Interface De Loopback Ao Dispositivo

4) Insira um Nome da interface de loopback, certifique-se de marcar a caixa de seleção Habilitado e insira um ID de loopback. Insira uma Descrição se desejar. Depois de concluir, clique na guia IPv4.

Configurar Informações de Interface de Loopback e Endereço IPv4

5) Insira o endereço IP de loopback para ser o endereço IP do BGP do link configurado em etapas anteriores para o link do site do ISP1 no Azure. Esse IP é usado como a fonte de atualização do BGP nas vizinhanças configuradas entre as Instâncias do FTD e do Azure sobre ISP1.



Note: Você pode referenciar o valor previamente definido no JSON de configuração de VPN baixado em `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress` para ISP1

Add Loopback Interface ?

General **IPv4** IPv6

IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

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

Insira O Endereço IPv4 De Loopback E Pressione OK

6) Repita as subetapas c-e nesta sequência para a configuração de loopback de BGP do ISP2.

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

Criar A Primeira E A Segunda Interfaces De Loopback

7) Salve sua configuração.

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

Salvar alterações

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

1) Para configurar a correspondência da configuração de IKEv2/IPsec no FMC para as topologias de VPN FTD, navegue para Manage > Objects, role no menu de navegação para 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 >

Criar novo objeto de política IKEv2

2) Insira um nome para a nova Política IKEv2, escolha Prioridade e/ou Tempo de vida. Certifique-se de que a política corresponda em ambas as extremidades do túnel em relação a Integridade, Criptografia, Função Pseudo-Aleatória (PRF - Pseudo Random Function) e Grupo DH. Escolha quais elementos de Algoritmo/Grupo devem 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

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

SHA256

Cancel Save

Criar política IKEv2

3) Quando a configuração estiver concluída, clique em Save (Salvar).

Edit IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

1
2
5
14
15
16
19
20

Add

14

Cancel Save

Salvar política IKEv2

4) Configure os parâmetros da Fase 2/IPsec no submenu IKEv2 IPsec Proposal e clique em Add IKEv2 IPsec Proposal.

The screenshot shows the Fortinet FortiGate web interface. On the left sidebar, the 'IKEv2 IPsec Proposal' option is highlighted with a red rectangle. The main content area is titled 'IKEv2 IPsec Proposal' and includes a brief description of IPsec security association negotiation. A blue button labeled 'Add IKEv2 IPsec Proposal' is located in the top right corner. Below the description, there is a table listing existing proposals:

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

Criar Proposta IKEv2 IPsec

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

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



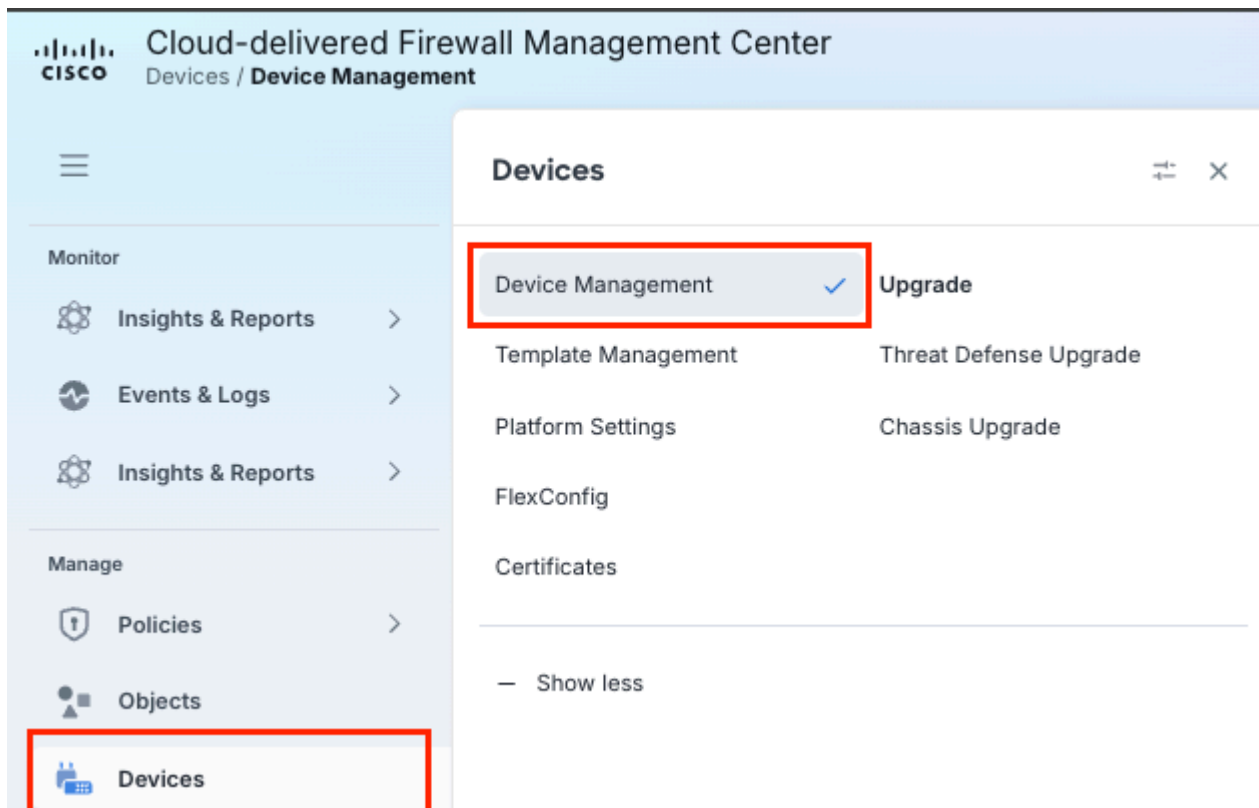
Cancel

Save

Nomeie Proposta IKEv2 IPsec E Clique em Salvar

Passo 4: Configurar interfaces de túnel virtual (VTI)

1) Navegue até Devices > Device Management.



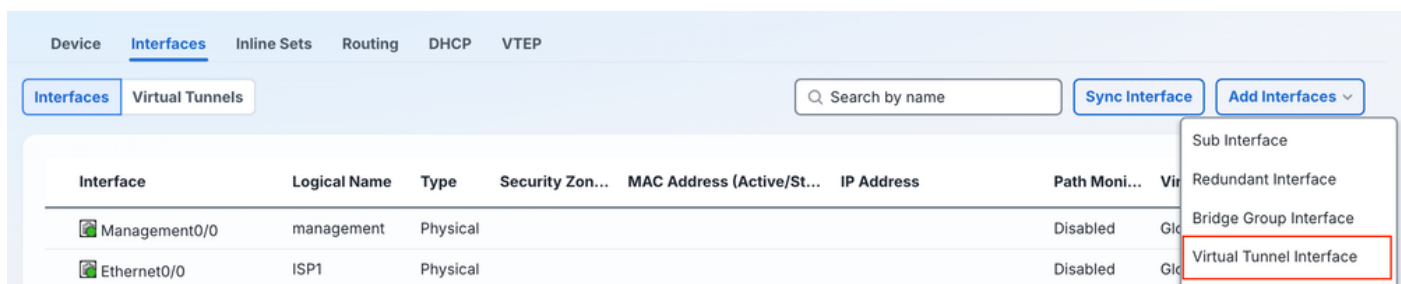
Navegue Até Device Management No Firepower Management Center

2) Clique no FTD que você está configurando como o dispositivo VPN de filial/site com conectividade ISP dupla.

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

Selecionar O FTD Para Implantação Da Configuração

3) Clique no menu suspenso Add Interfaces e selecione Virtual Tunnel Interface (VTI).



Criar interface de túnel virtual

4) Insira as informações do túnel. Verifique se a caixa de seleção Enabled está marcada, se Name foi inserido (Description também, se desejado) e se Security Zone opcional foi escolhido. Alinhe a interface correta voltada para o ISP pai para configurar o VTI e configure o endereço IP apropriado para a conectividade IPsec de túnel interno do VTI. Pressione OK quando terminar.



Tip: O diagrama de referência mostra mais contexto sobre a configuração de VPN potencial para conectividade de WAN dupla do Azure com FTD.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

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

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



Cancel

OK

5) Configure 3 VTIs adicionais em interfaces ISP1 e ISP2 pai.

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

Configurar interfaces adicionais de túnel virtual

f) Certifique-se de clicar em Save para salvar suas alterações.

You have unsaved changes

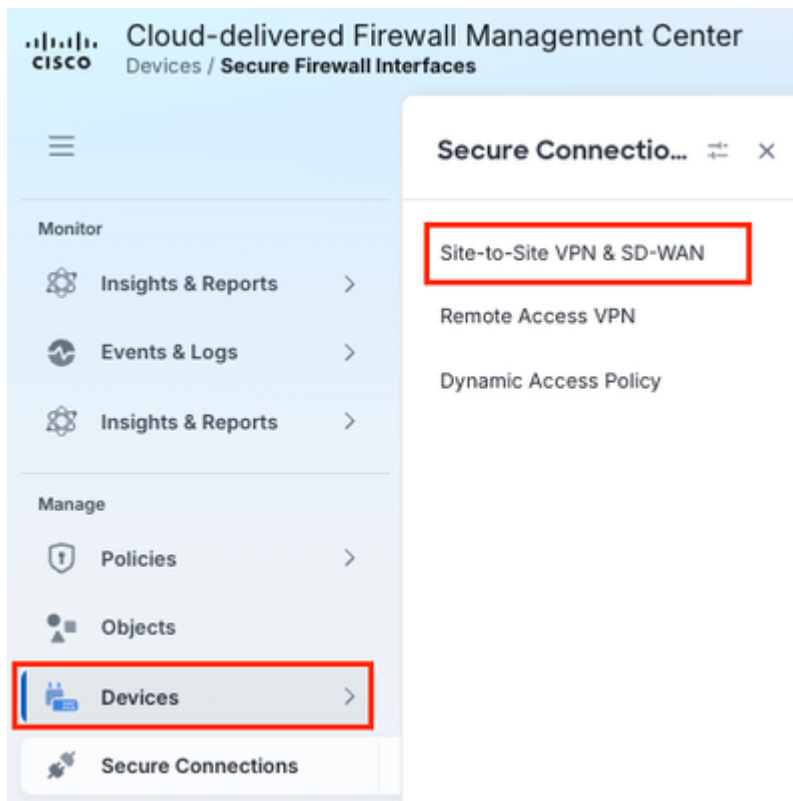
Save

Cancel

Salvar alterações

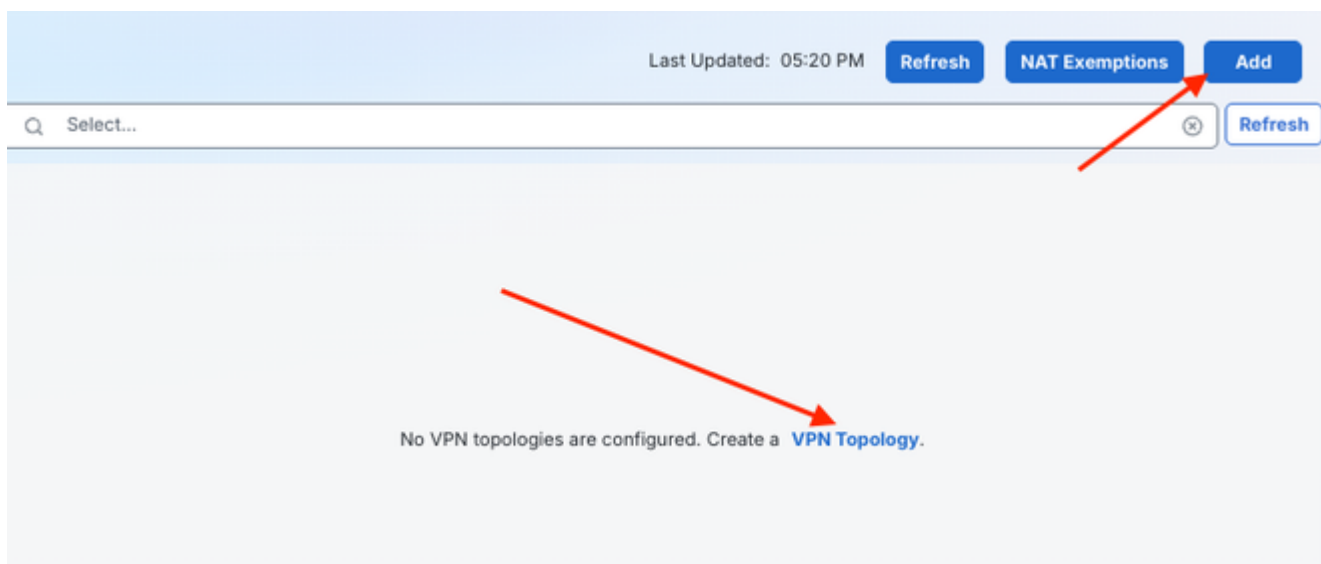
Passo 5: Provisionar Topologias VPN IPsec

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



Gerenciar conexões VPN Site a Site e SD-WAN

2) Clique no hiperlink de configuração inicial da Topologia VPN no meio da saída inicial ou clique no botão Add .



Adicionar nova configuração de topologia de VPN

3) Insira um nome de Topologia para o primeiro túnel no link ISP1 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 *

CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

New

☐ 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](#)

Configurar Tipo de Topologia VPN Baseada em Rota

4) Primeiro, escolha o dispositivo Node A e na lista suspensa Device significando o FTD que termina os túneis VPN do Azure. Depois que o assistente buscar os VTIs disponíveis no dispositivo, selecione o VTI apropriado para a interface pai e a instância que você está configurando no menu suspenso. No menu Dispositivo do Nó B, escolha o lado do Azure para ser o nó Extranet na configuração da topologia de VPN. Certifique-se de configurar um nome amigável para o Nó B, bem como de garantir a inserção do Endereço IP do Ponto de Extremidade apropriado. Depois de concluir, clique na guia IKE para implementar a configuração do túnel da Fase 1.



Note: Você pode fazer referência a valores de Endereço IP do Ponto de Extremidade da Instância no arquivo de configuração baixado em
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` e
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Node B

Device:*
CXvWAN-FTD-2

Virtual Tunnel Interface:*
ISP1-Inst-0 (IP: 169.254.21.1) +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Device:*
Extranet

Device Name*:
Azure-ISP1-Link-Inst0

Endpoint IP Address*:

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

Definir Endpoints De Topologia Do Nó A E Do Nó B

5) Role no menu de navegação para IKEv2 Settings e clique no ícone do lápis para editar as políticas para a Política IKEv2 configurada recentemente. Em seguida, escolha a opção Pre-shared Manual Key no menu suspenso Authentication Type e insira a PSK configurada anteriormente no Azure. Depois de concluir, clique na guia IPsec para configurar os parâmetros de túnel IPsec da fase 2.



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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Azure_IKEv2

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

Editar configurações de IKEv2 e chave de autenticação

6) Clique no ícone de lápis ao lado do Conjunto de transformação de proposta IKEv2 IPsec e escolha os parâmetros de política IPsec configurados anteriormente. Certifique-se de alterar o valor de Duração da Vida para corresponder às configurações de VPN vWAN do Azure. Depois que as informações configuradas forem confirmadas, clique em Salvar.



Note: Você pode fazer referência ao valor Lifetime no arquivo de configuração baixado em
`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Azure_IPsec

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*:

27000

 Seconds (Range 120-2147483647)

Lifetime Size:

Unlimited

 Kbytes (Range 10-2147483647)

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

Configurar Duração da Vida Útil da Proposta IPsec

7) Repita as subetapas anteriores na Etapa 5 para criar os outros Túneis do Azure através da Instância1 do ISP1, Instância0 do ISP2 e Instância1 do ISP2.

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

Criar topologias VPN site a site adicionais

Passo 6: Validar Topologias VPN

Entre no system support diagnostic-cli, digite en e pressione enter (CLI somente leitura).

1) Verifique a conectividade do túnel da fase 1 do IKE.

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

2) Verifique a conectividade da fase 2 do IPsec.

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



Note: Ao visualizar a saída de Associações de Segurança (SA - Security Associations) de IPsec e decapitações de pacotes e contadores de descriptografia de pacotes estão aumentando, mas os encapsulamentos de pacotes e criptografias de pacotes não estão, isso é esperado neste cenário. O Azure está tentando formar vizinhanças BGP sobre os endereços de Espaço IP Privado de Hub, e o Azure não inicia a negociação se a extremidade vizinha usar o endereçamento BGP APIPA. É responsabilidade do dispositivo que se conecta ao Azure iniciar a negociação BGP quando o APIPA personalizado é usado.

3) Verifique a conectividade da camada 2.

```
show arp
```

4) Verifique o IP Routing.

```
show route
```

5) Execute Capture nas interfaces ISP1 e ISP2.

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

6) Verificação do Azure - Navegue até Hub vWAN > Conectividade.> Sites VPN > Escolha o site

configurado.

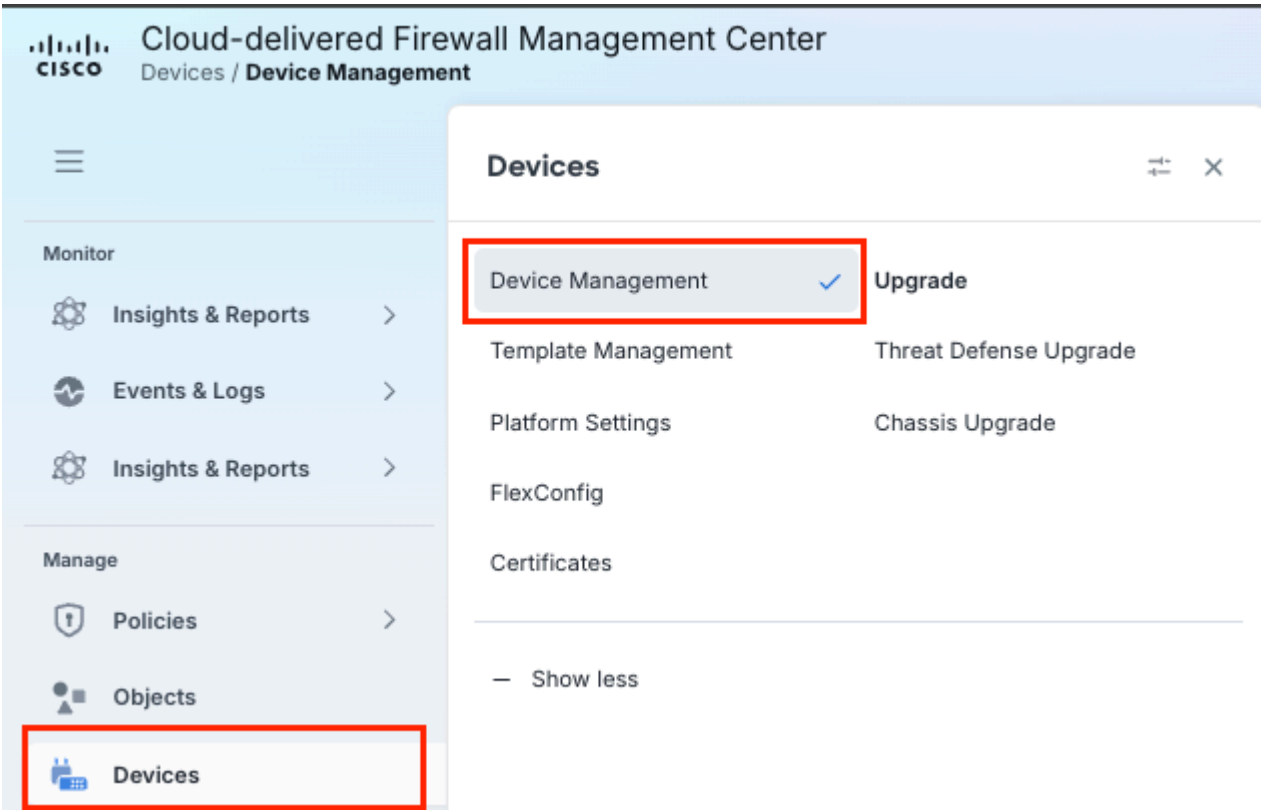
Links

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

Verificação de Conectividade do Link do Azure

Passo 7: Configurar ECMP

1) Navegue até Manage > Devices > Device Management e clique no FTD.



Navegue Até Device Management No Firepower Management Center

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

Selecionar O FTD Para Implantação Da Configuração

2) Clique na guia Routing e escolha ECMP.

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

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

Definições de Configuração de Vários Caminhos com Custo Igual

3) Clique em Adicionar.

Equal-Cost Multipath Routing (ECMP)

Add

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

Adicionar Configurações de Vários Caminhos de Custo Igual

4) Nomeie a Zona ECMP, clique nas Interfaces VTI disponíveis e clique no botão Adicionar para aplicá-las à coluna Interfaces selecionadas e clique em OK.

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

Selecionar Interfaces Para Zona De Múltiplos Caminhos De Custo Igual

5) Certifique-se de salvar suas alterações.

You have unsaved changes

Save

Cancel

Salvar alterações

Passo 8: Configurar BGP

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

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

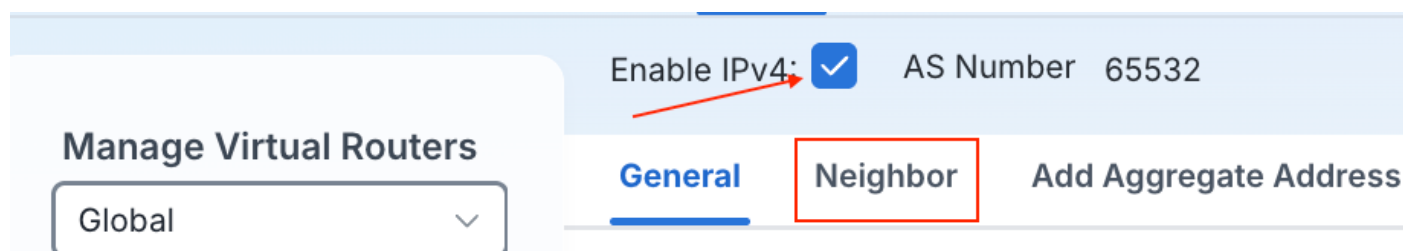
Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBG

2) Certifique-se de marcar a caixa de seleção Habilitar IPv4 para o processo BGP e clique em Vizinho para configurar vizinhos BGP no Azure.



Manage Virtual Routers

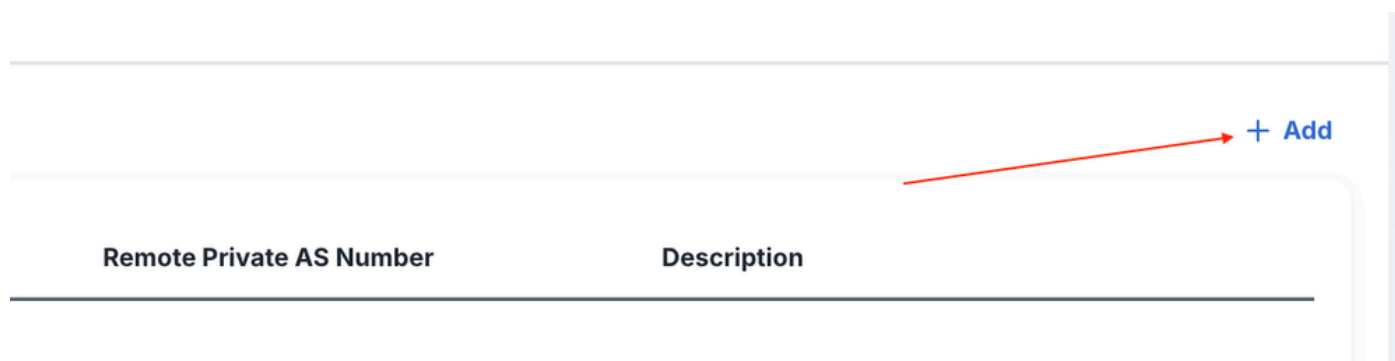
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

Habilitar Processo de Protocolo de Gateway de Borda IPv4

3) Clique em + Adicionar.



+ Add

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

Adicionar novo vizinho de protocolo BGP

4) Insira as informações de emparelhamento BGP da Instância0 do ISP1, faça referência ao AS BGP anotado do hub vWAN e insira-o como AS Remoto do Vizinho e adicione uma Descrição, se desejar. Clique em Advanced (Avançado).



Note: Certifique-se de escolher a Origem da Atualização do BGP para referenciar o Loopback para interfaces VTI no FTD mapeado para o Link ISP1 configurado no Azure.

Add Neighbor ?

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Configurar Informações de Emparelhamento do Protocolo Border Gateway

5) Dentro do menu Advanced da configuração do vizinho BGP no FTD, você pode alterar o número de saltos Time To Live (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. Click OK.

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Configurações Avançadas de Vizinhos do Border Gateway Protocol

6) Repita as subetapas 3-5 para configurar Tunnel2 para a Instância 1 do ISP1.

7) Repita as subetapas 3-5 duas vezes para configurar as informações de peering de BGP da Instância0/Instância1 do ISP2.



Note: Certifique-se de escolher a Origem de Atualização BGP alinhada referenciando o Loopback para interfaces VTI no FTD mapeado para o Link ISP2 configurado no Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

Configuração de Vizinho BGP da Instância 1 do ISP2

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

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

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes Routes Timers **Advanced** Migration

- ☐ Enable Authentication
- Enable Encryption
- 0
- Password
-
- Confirm Password
-
- ☐ Send Community attribute to this neighbor
- ☐ Use itself as next hop for this neighbor
- ☐ Disable Connection Verification
- ☒ Allow connections with neighbor that is not directly connected
- ☐ Limited number of TTL hops to neighbor
- TTL Hops
- 10
- (1-255)
- ☐ Use TCP path MTU discovery
- TCP Transport Mode
-

Cancel OK

Configuração de Vizinhos BGP da Instância 2 do ISP

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

Depois de concluir, clique em Salvar.

You have unsaved changes

Save

Salvar alterações

Por padrão, o BGP instala apenas um único melhor caminho na tabela de roteamento, mesmo que o ECMP esteja configurado em todos os VTIs para o Azure. O multipath de BGP deve ser habilitado separadamente para que ambos os caminhos aprendidos sejam instalados e usados ao mesmo tempo.

Etapa 9: Configurar o multipath de eBGP

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

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

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

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

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

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

Configuração Encaminhar pacotes por vários caminhos

2) Altere o valor padrão do campo Número de caminhos de 1 para 4. Clique em OK.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Configuração de encaminhamento de pacotes por vários caminhos

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

Verificar/solucionar problemas

Após a conclusão da implantação, confirme se o processo BGP de FTD estabelece adjacências de vizinhos com ambas as instâncias do Azure nos respectivos túneis e se as rotas são aprendidas, as interfaces estão ativas e as conexões de protocolo são retornadas na tabela de conexão.

Navegue para `system support diagnostic-cli` na CLI FTD conforme feito na Fase 2, Etapa 7.

1) 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#
```

```
ftd#
```

```
show bgp summary
```

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

```

BGP table version is 29, main routing table version 29
2 network entries using 400 bytes of memory
8 path entries using 640 bytes of memory
2 multipath network entries and 8 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1272 total bytes of memory
BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

```

```

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

```

2) Verifique se as rotas recebidas do Azure são mostradas como rotas de vários caminhos.

```
<#root>
```

```
ftd#
```

```
show bgp
```

```

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

```

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

3) Verifique o preenchimento da 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 172.31.3.33 to network 0.0.0.0

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

4) Verifique a tabela de conexão para sessões BGP.

<#root>

ftd#

show conn all | include TCP|179

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

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.