

在安全防火墙上配置Azure双ISP vWAN连接

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[图解](#)

[双直接互联网接入\(DIA\)链路 \(Azure + FTD负载均衡/冗余 \)](#)

[配置](#)

[第 1 阶段：Azure vWAN VPN站点配置](#)

[步骤 1：创建Azure vWAN VPN站点 \(远程FTD设备 \)](#)

[步骤 2：配置Azure APIPA网关参数](#)

[步骤 3：配置Azure vWAN Site VPN参数](#)

[步骤 4：在VPN站点链路实例上启用和激活自定义BGP APIPA](#)

[步骤 5：下载VPN站点配置文件](#)

[第 2 阶段：配置FTD以实现到Azure vWAN的双ISP连接](#)

[步骤 1：分析下载的VPN配置](#)

[步骤 2：配置链路BGP更新源环回接口](#)

[步骤 3：配置第1阶段/第2阶段策略对象](#)

[步骤 4：配置虚拟隧道接口\(VTI\)](#)

[步骤 5：调配IPsec VPN拓扑](#)

[步骤 6：验证VPN拓扑](#)

[步骤 7：配置ECMP](#)

[步骤 8::配置BGP](#)

[步骤 9：配置eBGP多路径](#)

[验证/故障排除](#)

简介

本文档介绍如何使用双WAN链路将Microsoft Azure虚拟广域网(vWAN)站点到站点VPN连接配置为安全防火墙。

先决条件

要求

建议掌握下列主题的相关知识：

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

确保这些组件最初均在Azure环境中配置：

- Microsoft Azure vWAN实例
- Microsoft Azure vWAN Hub

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全FTD版本10.0
- 思科安全FMC版本10.0
- Microsoft Azure vWAN

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

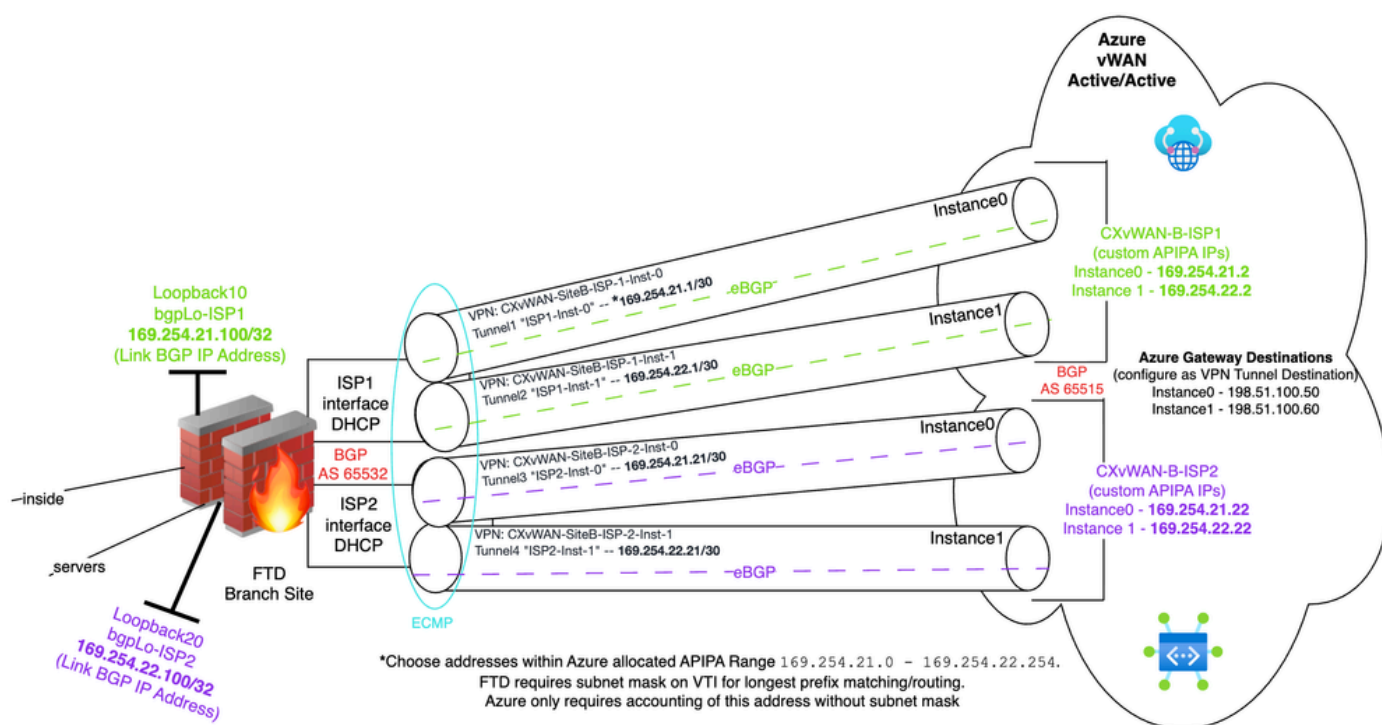
当分支机构FTD有两个面向Internet服务提供商(ISP)的外部接口时，每个接口都可以冗余主动连接到Azure vWAN，因此每个ISP链路都得以利用。Azure vWAN为每个站点链接创建两个IPsec隧道（一个到Azure Hub Instance0，一个到Instance1），因此每个ISP接口终止两个隧道。在两条ISP链路上，这将导致四条IPsec隧道在FTD上终止。

Azure实例在主用/主用模式下运行以实现负载均衡和冗余，因此FTD通过所有四个IPsec隧道的等价多路径(ECMP)配置反映这一点。使用自定义自动私有IP寻址(APIPA)地址，在四个隧道的每个隧道上建立具有不同专用自治系统编号(ASN)的外部边界网关协议(eBGP)邻居关系。这将启用BGP多路径功能，为每个Azure Hub Site Link实例对提供多个冗余路径。

图解

该图显示了本文所述的配置拓扑。双直接互联网访问(DIA)链路变体从FTD上的两个外部接口来源两个Azure隧道。

双直接互联网接入(DIA)链路 (Azure + FTD负载均衡/冗余)



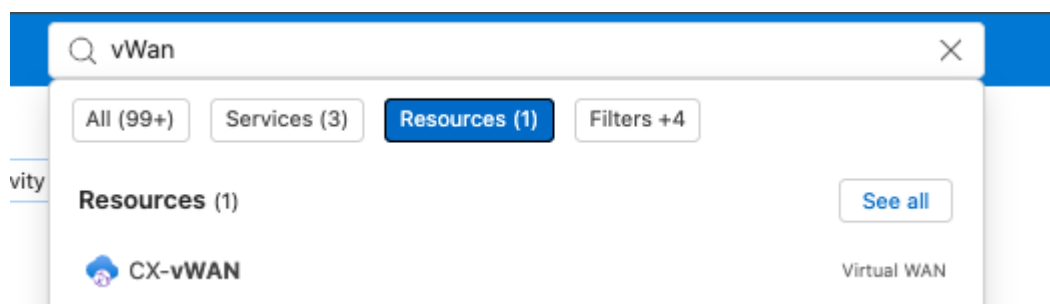
双直接Internet接入连接拓扑

配置

第 1 阶段：Azure vWAN VPN站点配置

步骤 1：创建Azure vWAN VPN站点 (远程FTD设备)

1)在Azure搜索字段中搜索vWAN，点击虚拟WAN以进入现有的Azure vWAN Hub。接下来，导航到连接>中心，然后点击现有的Azure vWAN中心。



虚拟广域网的搜索查询

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

选择现有的虚拟WAN集线器

2)单击Connectivity > VPN(Site to site) , 然后单击+ 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		

创建新的虚拟WAN站点



注意：覆盖图像中各个字段中的值的空白是用于发布本文档。

3)在必填字段中输入值。完成后，单击Next:Links >向前移动。

Create VPN site ...

Basics Links Review + create

Project details

Subscription	
Resource group *	

Instance details

Region *	
Name *	Dual-ISP-Site
Device vendor *	Cisco

Private address space

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

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

Previous

Next : Links >

常规VPN站点配置设置

4)输入所需的链路信息。链路BGP地址和链路ASN是内部隧道BGP第3层目标地址以及在站点到站点隧道上形成邻居关系的分支端上的BGP AS编号。链路BGP地址是已配置的集线器私有地址空间子网外部的非重叠子网地址(/32),Azure将该子网安装为作为BGP邻居到达的/32路由。在FTD的后续部分中创建了两个环回接口,以代表每个双站点链路的链路BGP地址。链路IP地址/完全限定域名(FQDN)是流向分支站点的流量的外部报头第3层目标IP地址,这是调配IP安全(IPsec)/Internet密钥交换版本2(IKEv2)连接所必需的。完成后单击下一步:审阅+创建>。



注意:如果您使用范围从169.254.21.0到169.254.22.255的地址作为隧道地址,请确保查看特定Azure文档:[选择BGP APIPA地址。](#)

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 >

配置站点链路参数

5)确认信息符合预期后，单击Create。

Create VPN site ...

 Validation passed

- basics
- links
- Review + create**

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

Basics

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

Links

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

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

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

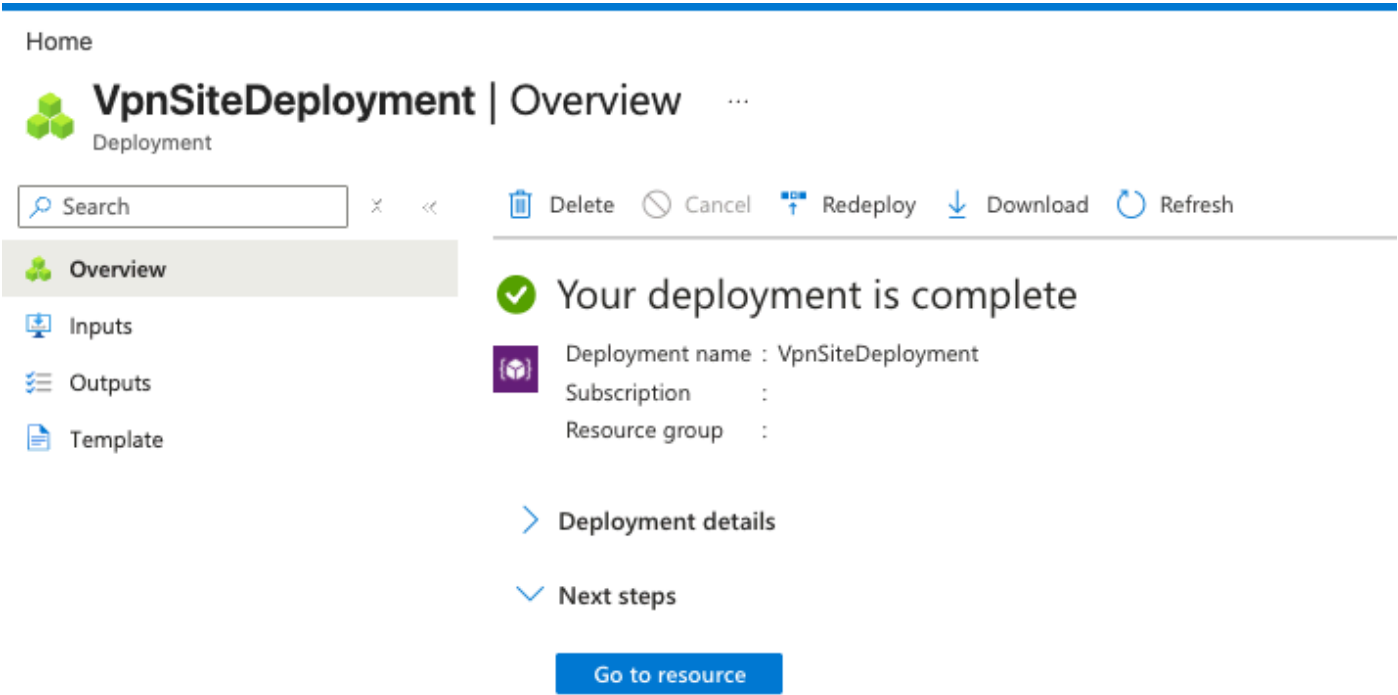
Create

Previous

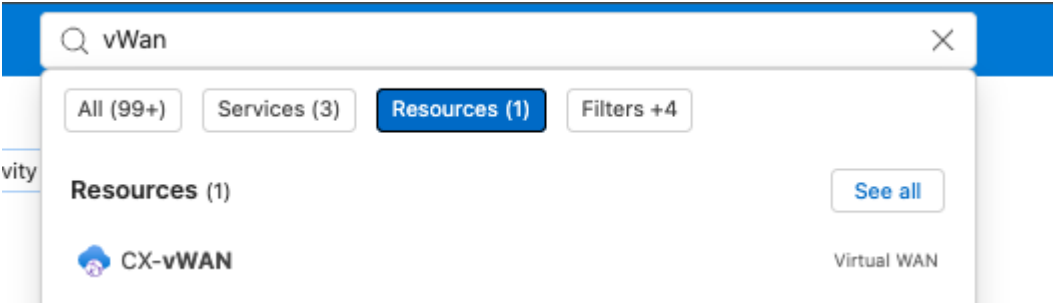
Next

查看和创建新的VPN站点

6)VPN站点的部署完成后，导航回vWAN Hub配置。



虚拟广域网站点部署进度



虚拟广域网的搜索查询

步骤 2：配置Azure APIPA网关参数

Azure需要对169.254.0.0/16 IPv4地址空间内的自动私有IP寻址(APIPA)地址进行额外配置。

1)通过Connectivity > Hubs进入现有中心。

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

导航至虚拟WAN集线器连接

2)再次导航到Connectivity > VPN(Site to site)，然后点击Gateway Configuration超链接。

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 ⓘ

Access Gateway Configuration超链接

3)侧面板显示为编辑VPN网关。在VPN网关实例0和VPN网关实例1下，输入两个唯一的自定义BGP IP地址，这两个地址充当通过IPsec隧道的BGP邻居关系的每个实例的邻居IP。如果选择在此拓扑中使用APIPA编址，则必须执行此操作。在标记为对等体地址的字段中，输入要用于从FTD访问Azure实例的BGP邻居IP。如果正在使用APIPA寻址，Azure不会尝试使用FTD建立BGP，因此FTD会尝试使用Azure在每个隧道上建立eBGP邻居。

总数为2个链路x2个隐式隧道；每个ISP链路一条通向Instance0和Instance1的隧道；总计为四个IPsec隧道，其中Azure和两个FTD ISP接口之间具有BGP邻居关系。

这些地址必须是唯一的，在本演示中，分配给每个隧道的/30子网中的第二个和最后一个主机地址将在FTD上配置以供使用。配置后，单击Edit。



注意：如果您使用范围从169.254.21.0到169.254.22.255的地址作为隧道地址，请确保查看特定Azure文档：[选择BGP APIPA地址](#)

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

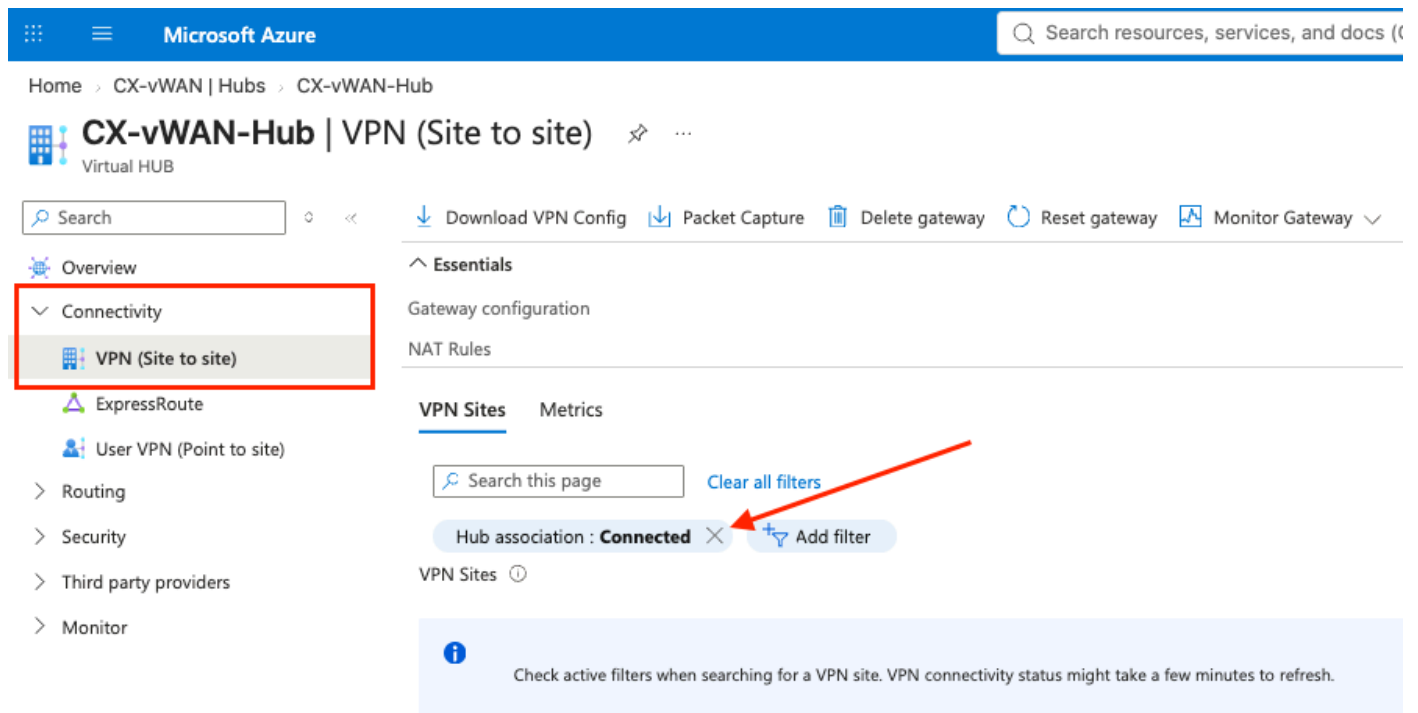
编辑VPN网关自定义BGP IP地址



注意：正如Azure所指出的，更新此内容可能需要30分钟或更长时间。

步骤 3：配置Azure vWAN Site VPN参数

1)在Azure vWAN Hub配置中的Connectivity > VPN(Site to site)页面上，单击X以清除Hub关联：已连接过滤以查看断开的VPN站点。



清除集线器关联连接过滤器

2)选中最近调配的VPN站点旁边的复选框，然后点击连接VPN站点。

 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**

连接VPN站点操作

3)配置所需的预共享密钥(PSK),并通过点击Custom切换选项配置所需的IPsec参数。在后续步骤中,这些IPSec参数必须与FMC/FTD配置匹配。要保存,请点击连接。



注意: FTD/FMC版本6.7删除了Diffie-Hellman(DH)组24支持。

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

配置预共享密钥和IPsec参数

4)确认VPN站点调配已成功完成。

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

确认VPN站点调配状态

步骤 4：在VPN站点链路实例上启用和激活自定义BGP APIPA

1)刷新VPN (站点到站点) 页，并确认连接调配状态列指示其成功，这使您可以单击省略号，并允许您单击编辑VPN连接到此中心下拉菜单项。

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

Page: 1

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

验证连接成功并编辑VPN连接

2)单击以配置Link Connection 1(ISP1)，然后再次输入适用的Pre-Shared Key(PSK)，并确保单击Custom BGP IP Address旁边的Enable开关，并映射将成为FTD生成的BGP IP报头的内部隧道目标IP地址字段值的/30子网的剩余主机地址。

实质上，ISP1 VTI Tunnel1到Azure Instance0的地址分配为169.254.21.1/30，终止于FTD的第二个ISP1 VTI Tunnel2为实例1分配了IP 169.254.22.1/30。

单击“下一步”:Link Connection 2>进入ISP 2链路参数。



注意：您可能需要重新输入您的PSK，并重新点击Azure下拉菜单中的已调整的PFS组选项。

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)重复上述步骤，并应用Link Connection 2(ISP2 link)下的适用参数。完成后，点击创建。

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 * ⓘ

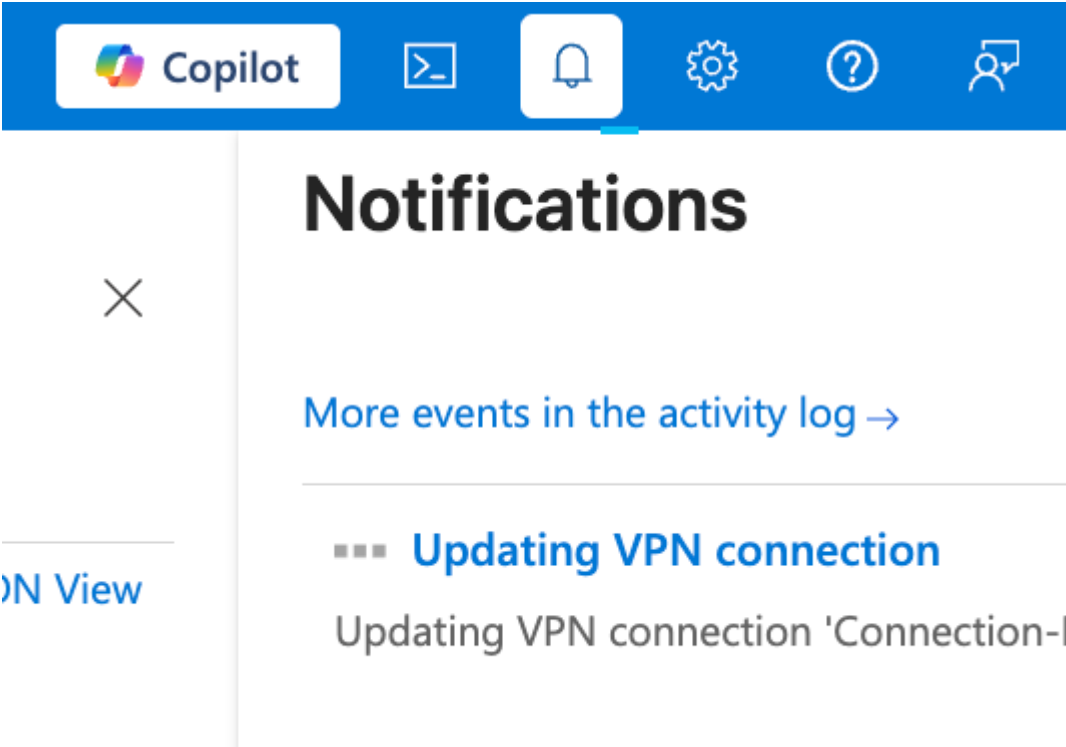
Create

Previous

Next

配置链路连接两个自定义BGP设置

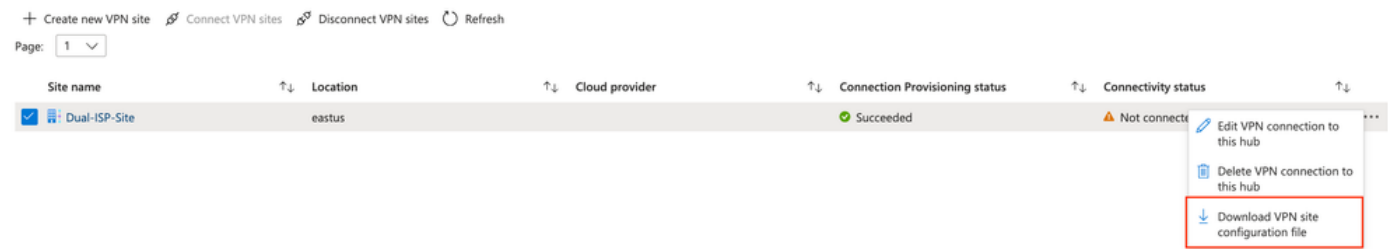
4)Azure UI中的通知显示更新任务开始。



Azure更新任务开始通知

步骤 5：下载VPN站点配置文件

1)在Azure中的同一VPN（站点到站点）页中，选择已配置VPN站点最右侧的省略号图标，然后选择下载VPN站点配置文件选项。



下载VPN站点配置文件选项

2)单击Click here to download超链接。



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



下载VPN站点配置文件

第 2 阶段：配置FTD以实现到Azure vWAN的双ISP连接

步骤 1：分析下载的VPN配置

1)打开已下载的配置文件，并出现类似的JavaScript Object Notation(JSON)输出。输出显示文件中写入的两个对象之一。此信息为FTD配置提供了有用的环境。



注意：为了增强焦点，多个无关对象和密钥/值对被修剪以简洁。



注意：下载文件中的ISP-Link-1 JSON对象顺序颠倒。代码输出中的省略号表示ISP-2-Link对象及其适用的配置。

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

```

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

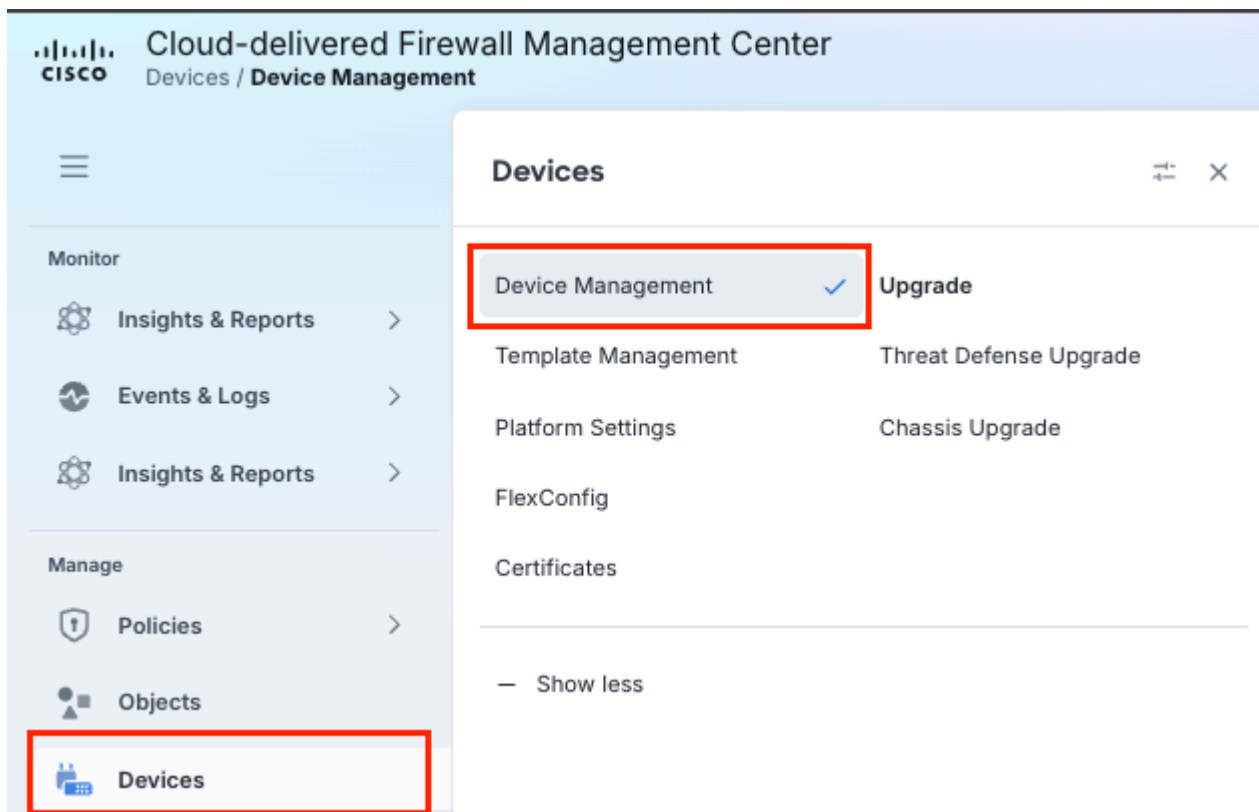
```

完成这些步骤时，请保留此输出作为参考。

步骤 2：配置链路BGP更新源环回接口

FTD BGP进程下的BGP邻居配置条目（在FTD的后续步骤中配置）需要代表Azure站点链路配置中对应链路BGP IP地址的稳定源。

1)导航到Devices > Device Management。



导航到Firepower管理中心的设备管理



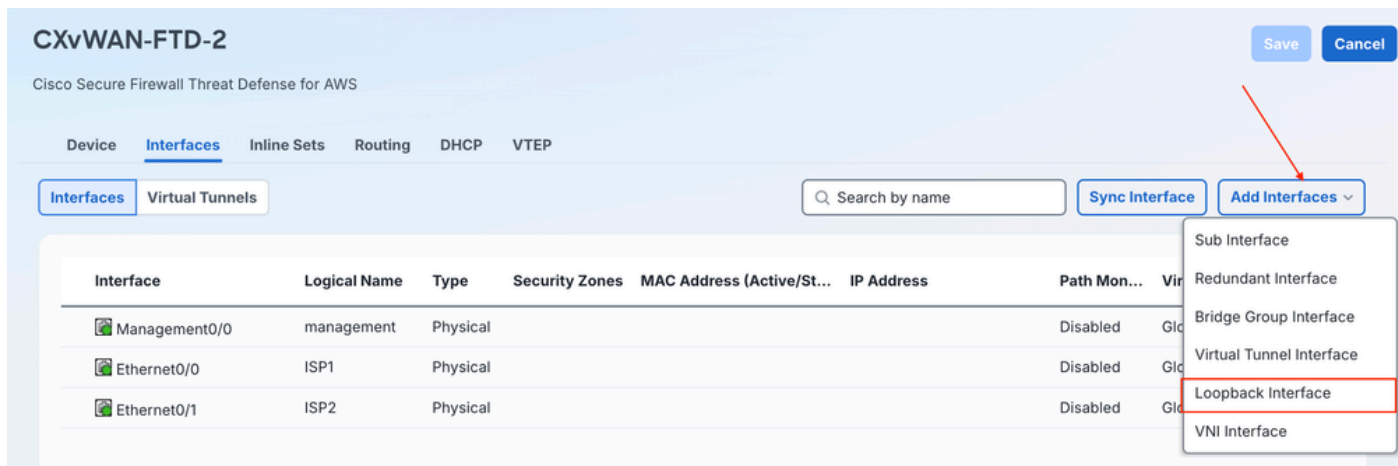
注意：本实验使用云交付的防火墙管理中心(cdFMC);但是，内部FMC的步骤保持不变。

2) 点击要配置为具有双ISP连接的分支机构/站点VPN设备的FTD。

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

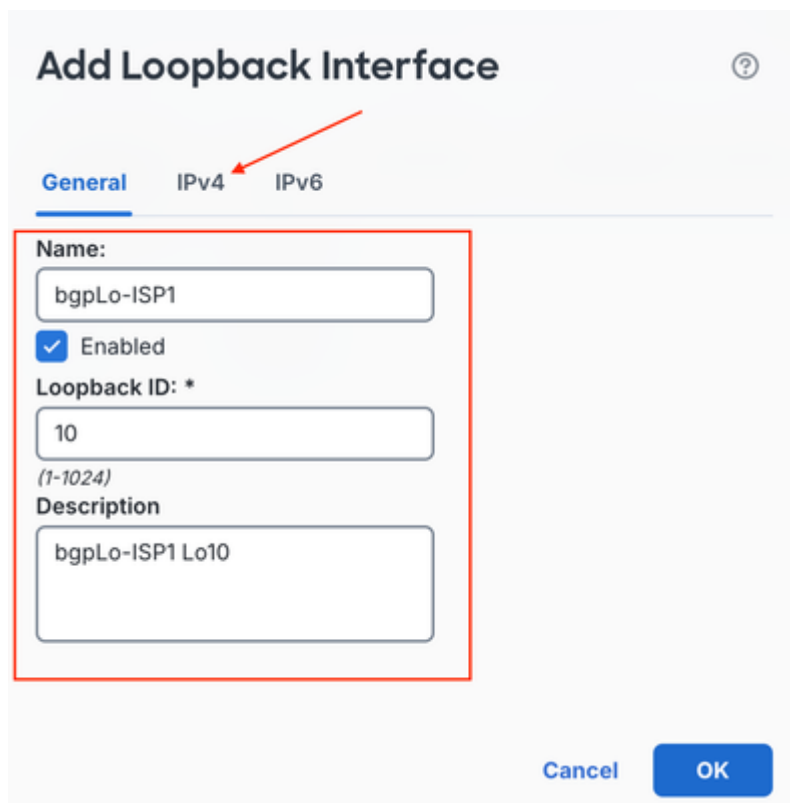
选择用于配置部署的FTD

3) 单击Add Interfaces下拉菜单，然后单击Loopback Interface。



向设备添加环回接口

4)输入环回接口的Name，确保选中Enabled复选框，并输入Loopback ID。如果需要，请输入Description。完成后，单击IPv4选项卡。



Add Loopback Interface ⓘ

General **IPv4** IPv6

Name:
bgpLo-ISP1

☒ Enabled

Loopback ID: *
10
(1-1024)

Description
bgpLo-ISP1 Lo10

Cancel **OK**

配置环回接口信息和IPv4地址

5)输入环回IP地址作为之前步骤中为Azure中的ISP1站点链路配置的链路BGP IP地址。此IP用作ISP1上FTD和Azure实例之间配置的邻居关系上的BGP更新源。



注意：您可以引用之前在vpnSiteConfiguration.BgpSetting.BgpPeeringAddress for ISP1下载的VPN配置JSON中定义的值

Add Loopback Interface

?

General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

169.254.21.100/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

输入环回IPv4地址并点击OK

6)在此序列中为ISP2 BGP环回配置重复子步骤c-e。

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

创建第一个和第二个环回接口

7)保存配置。

You have unsaved changes

Save

Cancel

保存更改

步骤 3：配置第1阶段/第2阶段策略对象

1)要在FMC和FTD VPN拓扑上配置匹配的IKEv2/IPsec配置，请导航到Manage > Objects，在导航菜单中滚动到VPN，然后展开子菜单。通过选择菜单中的IKEv2 Policy并点击Add IKEv2 Policy来配置IKEv2第1阶段策略。

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 1 of 1 >

创建新的IKEv2策略对象

2)输入新IKEv2策略的名称，选择Priority和/或Lifetime。确保有关完整性、加密、伪随机函数 (PRF)和DH组的隧道两端策略匹配。选择要与Azure配置匹配的算法/组元素，然后单击Add。



注意：您可以在下载的配置文件中（位于 `vpnSiteConnections[0].connectionConfiguration.IPsecParameters` ）引用这些精确值

New IKEv2 Policy

Name:*

Description:

Priority:*

Lifetime: seconds (120-2147483647)

Available Algorithms

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

MD5

SHA

SHA512

SHA256

SHA384

NULL

[Add](#)

Selected Algorithms

SHA256

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

创建IKEv2策略

3)完成配置后，点击保存。

Edit IKEv2 Policy

Name:*

Azure_IKEv2

Description:

Priority:*

(1-65535)

5

Lifetime:

seconds (120-2147483647)

3600

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

1

2

5

14

15

16

19

20

Add

Selected Groups

14

Cancel

Save

保存IKEv2策略

4)在IKEv2 IPsec Proposal子菜单中配置阶段2/IPsec参数，然后单击Add IKEv2 IPsec Proposal。

Policy List

Port

> Prefix List

Route Map

> Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

URL

Variable

Variable Set

VLAN Tag

VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 IPsec Proposal

Add IKEv2 IPsec Proposal

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can configure the encryption and integrity algorithms and their priority. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Name

AES-GCM

AES-SHA

DES_SHA-1

Umbrella-AES-GCM-256

创建IKEv2 IPsec提议

5)命名IKEv2 IPsec Proposal并确保相同的设置保持一致。完成后，单击Save。

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



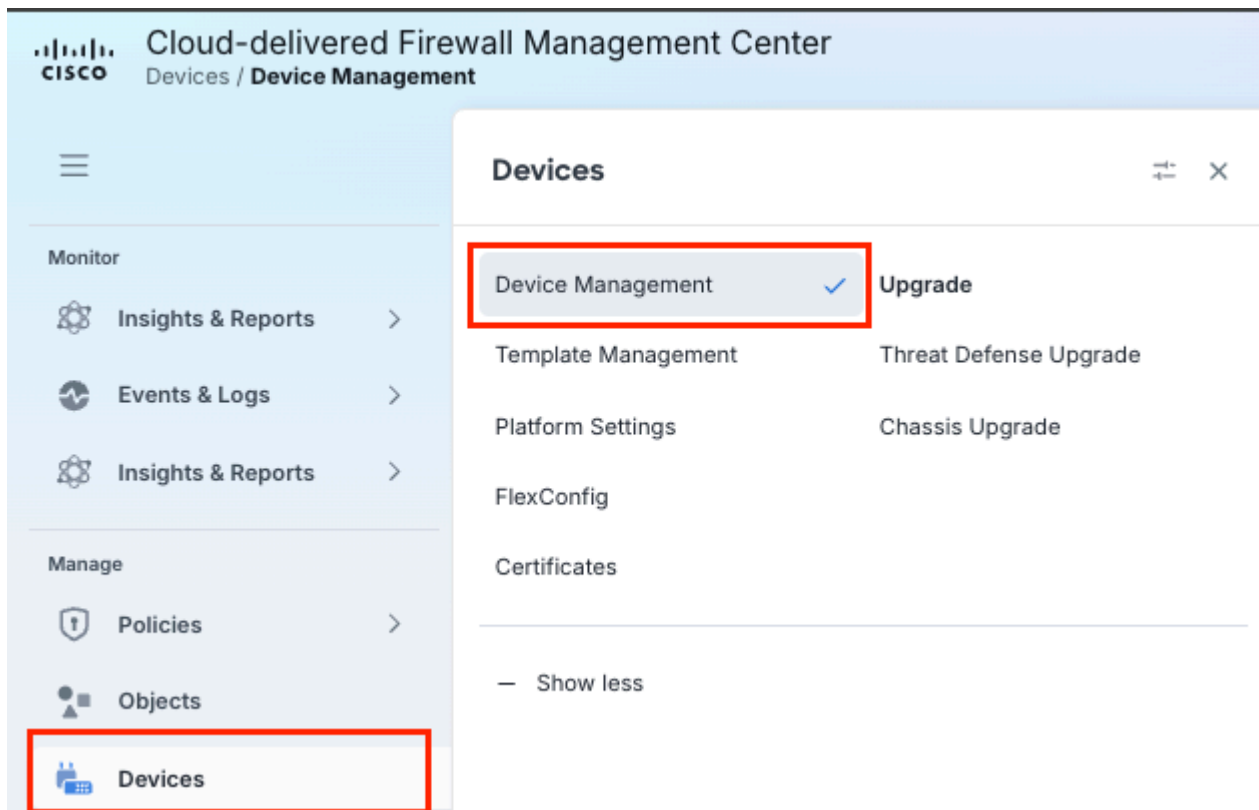
Cancel

Save

命名IKEv2 IPsec建议并点击Save

步骤 4：配置虚拟隧道接口(VTI)

1)导航到Devices > Device Management。



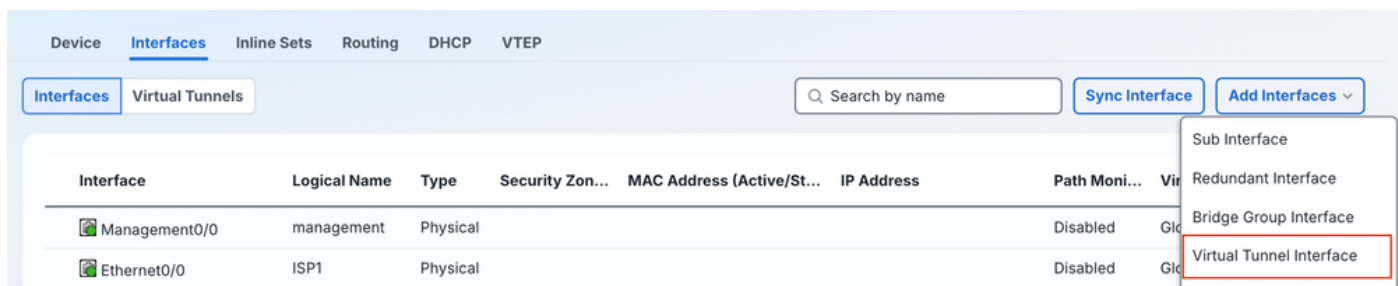
导航到Firepower管理中心的设备管理

2) 点击要配置为具有双ISP连接的分支机构/站点VPN设备的FTD。

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

选择用于配置部署的FTD

3) 单击Add Interfaces下拉菜单，然后选择Virtual Tunnel Interface(VTI)。



创建虚拟通道接口

4) 输入隧道信息。确保选中Enabled复选框，输入Name (如果需要，还应输入Description)，并选择可选的Security Zone。调整正确的面向ISP的父接口，以在VTI下配置VTI，并为该VTI的内部隧道IPsec连接配置适当的IP地址。完成后单击OK。



提示：参考图表显示有关使用FTD进行Azure双WAN连接的潜在VPN配置的更多情景。

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)在父ISP1和ISP2接口上配置3个附加VTI。

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

配置其他虚拟隧道接口

f)确保单击Save以保存更改。

You have unsaved changes

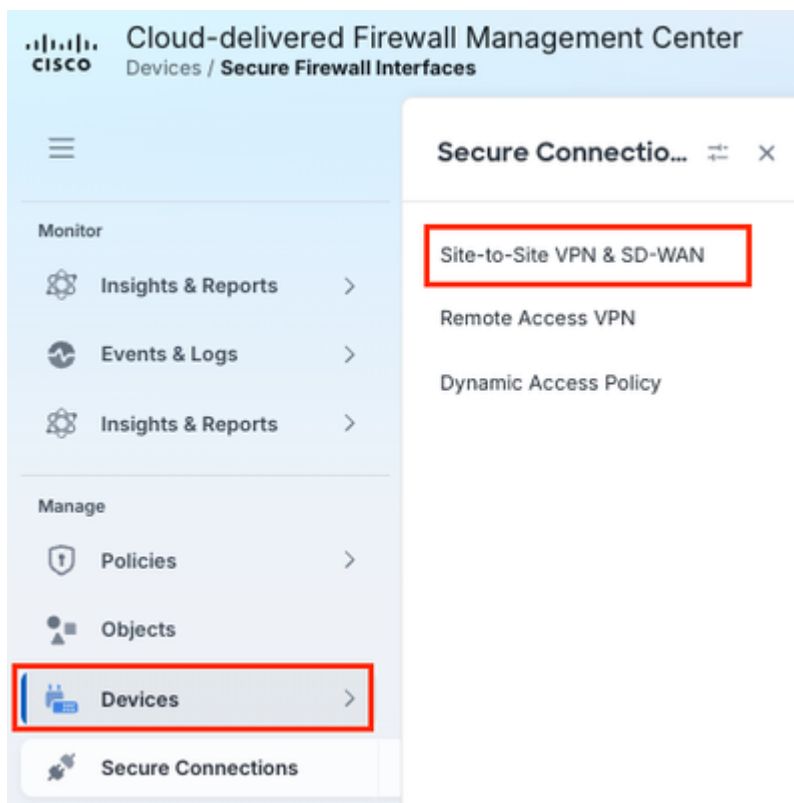
Save

Cancel

保存更改

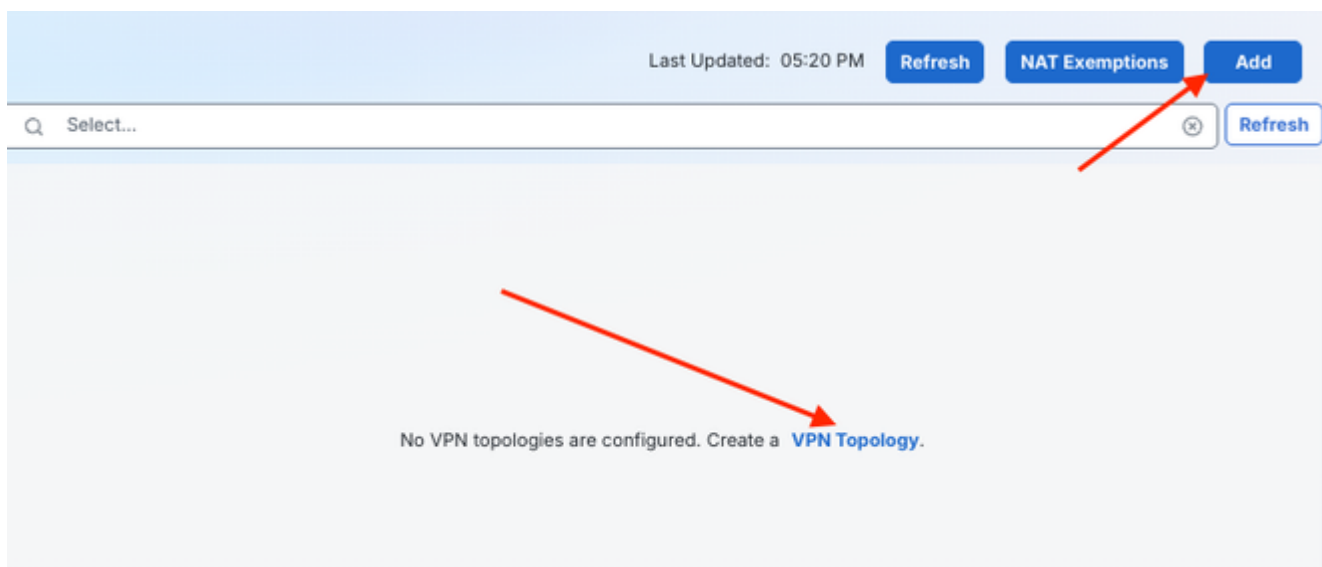
步骤 5：调配IPsec VPN拓扑

1)导航到管理>安全连接>站点到站点VPN和SD-WAN。



管理站点到站点VPN和SD-WAN连接

2)单击初始输出中间的初始VPN Topology configuration超链接，或单击Add按钮。



添加新的VPN拓扑配置

3)为通向Azure实例0的ISP1链路路上的第一个隧道输入Topology name。单击Route-Based VPN单选按钮，然后单击Peer to Peer VPN拓扑类型。完成后，单击Create。

Create VPN Topology ?

Topology name *
CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

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

Select VPN Topology

☐ Hub and Spoke

Prerequisites

Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ Peer to Peer

Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

SASE Topology

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

Prerequisites

[Refresh](#)

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

配置基于路由的VPN拓扑类型

4)首先，选择Node A设备，并在Device下拉列表下表示从Azure终止VPN隧道的FTD。在向导从设备获取可用的VTI后，从下拉菜单中选择适合您配置的父接口和实例的VTI。从Node B Device菜单中，选择Azure端作为VPN拓扑配置中的Extranet节点。请确保为节点B配置友好名称，并确保输入适当的Endpoint IP Address。完成后，单击IKE选项卡实施第1阶段隧道配置。



注意：可以在vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0和vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1的下载配置文件中引用Instance Endpoint IP Address值

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](#)

定义节点A和节点B拓扑终端

5)在导航菜单中滚动到IKEv2 Settings，然后单击铅笔图标将策略编辑到最近配置的IKEv2 Policy。然后，从身份验证类型下拉菜单中选择预共享手动密钥选项，并输入以前在Azure中配置的PSK。完成后，单击IPsec选项卡以配置第2阶段IPsec隧道参数。



注意：您可以在下载的配置文件中（位于 `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`）引用预共享密钥

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

编辑IKEv2设置和身份验证密钥

6)点击IKEv2 IPsec Proposal Transform Set旁的铅笔图标，并选择之前配置的IPsec策略参数。确保更改Lifetime Duration值以匹配Azure vWAN VPN设置。确认配置信息后，单击Save。



注意：您可以在下载的配置文件中的Lifetime值引用
`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

配置IPsec建议生命周期持续时间

7)重复步骤5中的上述子步骤，创建跨ISP1实例1、ISP2实例0和ISP2实例1的其他Azure隧道。

> 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	✓	✎	🗑

创建其他站点到站点VPN拓扑

步骤 6：验证VPN拓扑

进入system support diagnostic-cli，键入en，然后点击enter（只读CLI）。

1)检查IKE第1阶段隧道连接。

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

2)检查IPsec第2阶段的连通性。

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



注意：当查看IPsec安全关联(SA)输出和pkts decaps和pkts decrypt计数器正在递增，但pkts encaps和pkts encrypt未递增时，此场景中预期会出现这种情况。Azure正在尝试通过中心专用IP空间地址形成BGP邻居关系，如果邻居终端使用APIPA BGP编址，则Azure不会启动协商。使用自定义APIPA时，连接到Azure的设备有责任启动BGP协商。

3)检查第2层的连通性。

```
show arp
```

4)检查IP路由。

```
show route
```

5)在ISP1和ISP2接口上执行捕获。

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

6)Azure验证 — 导航到vWAN Hub > Connectivity。 > VPN Sites > 选择配置的站点。

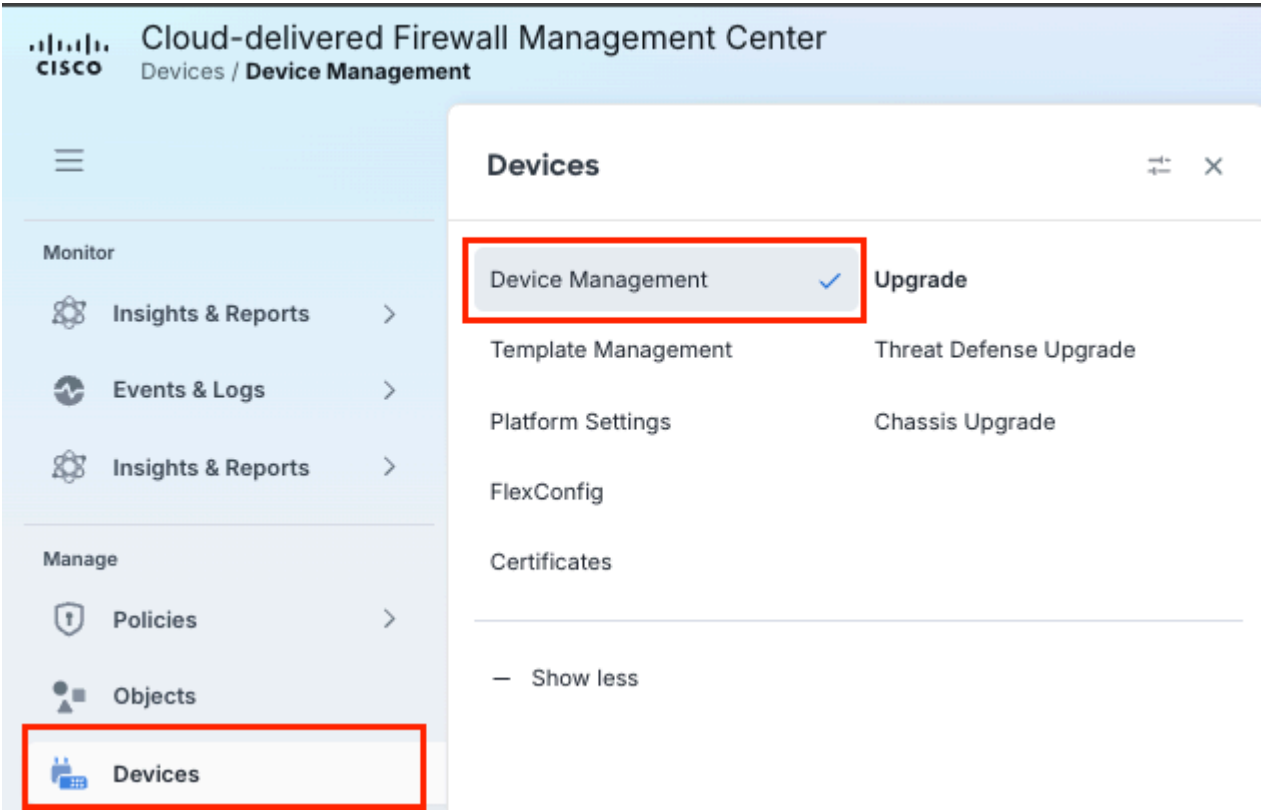
Links

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

Azure链接连接验证

步骤 7：配置ECMP

1)导航到Manage > Devices > Device Management，然后点击FTD。



导航到Firepower管理中心的设备管理

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

选择用于配置部署的FTD

2)单击Routing选项卡，然后选择ECMP。

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

SNMP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

等价多路径配置设置

3)单击Add。

Equal-Cost Multipath Routing (ECMP)

Add

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

添加等价多路径配置设置

4)为ECMP区域命名，点击可用的VTI接口，然后点击添加按钮将其应用到所选接口列，然后单击确定。

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

为等价多路径区域选择接口

5)确保保存更改。

You have unsaved changes

Save

Cancel

保存更改

步骤 8::配置BGP

1)在Routing > General Settings > BGP下启用FTD上的BGP进程。选中Enable BGP复选框，并输入之前在第1阶段第1d中配置的AS编号。导航到Routing > BGP > IPv4。

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

在General Settings下启用边界网关协议进程

2)确保选中BGP进程的Enable IPv4复选框，然后单击Neighbor以在Azure中配置BGP邻居。

Manage Virtual Routers

Global

Enable IPv4: ☒

AS Number 65532

General

Neighbor

Add Aggregate Address

启用IPv4边界网关协议进程

3)单击+ Add。

+ Add

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

添加新的边界网关协议邻居

4)输入ISP1 Instance0 BGP对等信息，参考来自vWAN集线器的注意BGP AS，然后将其输入为Neighbor Remote AS，如果需要，还可以添加Description。单击 Advanced。



注意：确保选择BGP Update Source以引用映射到Azure中配置的ISP1链路的FTD上VTI接口的环回。

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

配置边界网关协议对等信息

5)在FTD上的BGP Neighbor配置的Advanced菜单中，您可以将Time To Live(TTL)跳数从eBGP默认的1跳更改为变量数。Azure BGP终结点未通过隧道直接连接到Azure基础设施，并且与终结点的跃点数往往比1的默认eBGP TTL允许的跃点数多。Click OK.

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

高级边界网关协议邻居设置

6)重复子步骤3-5，为ISP1实例1配置Tunnel2。

7)重复子步骤3-5两次，以配置ISP2 Instance0/Instance1 BGP对等信息。



注意：确保选择引用映射到Azure中配置的ISP2链路的FTD上VTI接口的环回的对齐BGP Update Source。

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

ISP2实例1 BGP邻居配置

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

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

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

- ☐ Enable Authentication
- Enable Encryption

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

10

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

Cancel

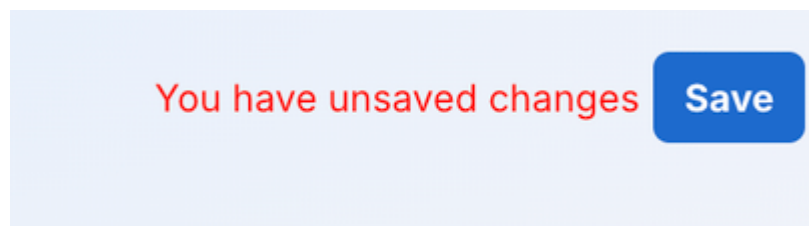
OK

ISP 2实例2 BGP邻居配置

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		

结束BGP邻居结果配置

完成后，单击Save。



保存更改

默认情况下，BGP在路由表中仅安装一个最佳路径，即使ECMP在通往Azure的所有VTI之间都进行了配置。必须单独启用BGP多路径，以便同时安装和使用BGP多路径。

步骤 9：配置eBGP多路径

1)导航到Routing > BGP > IPv4，单击General选项卡，然后单击Forward Packets Over Multiple Paths旁的铅笔图标。

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 IPv4: ☒ AS Number 65532

GeneralNeighborAdd Aggregate AddressFilteringNetworksRedistributionRou

Setting

Learned Route Map

Administrative Route Distances

External20

Internal200

Local200

Routes and Synchronization

Generate default routesNo

Summarize subnet routes into network level routesNo

Advertise inactive routesYes

Synchronize between BGP and IGP systemsNo

Redistribute IBGP into IGPNo

(Use filtering to limit the number of prefixes that are redistributed)

Forward Packets Over Multiple Paths

Number of Paths1

IBGP number of paths1

在多路径上转发数据包设置

2)将Number of Paths字段的默认值从1更改为4。单击OK。

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

更改多路径转发数据包设置

3)确保Save并部署更改。

验证/故障排除

部署完成后，请确认FTD BGP进程在各自隧道上与两个Azure实例建立邻居邻接关系，并且路由已获取、接口已打开，并且协议连接已返回连接表中。

导航至system support diagnostic-cliFTD CLI上，如第2阶段第7步所述。

1)部署后，BGP邻居将进入工作状态并接收前缀。

<#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)检查从Azure接收的路由是否显示为多路径路由。

```
<#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)检查路由表填充。

```
<#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)检查BGP会话的连接表。

<#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
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。