

将Azure vWAN Site-to-Site VPN配置为安全防火墙

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[图解](#)

[Azure和FTD之间的单DIA链路vWAN连接 \(Azure负载均衡/冗余 \)](#)

[配置](#)

[第 1 阶段：Azure vWAN/集线器配置](#)

[步骤 1：创建vWan](#)

[步骤 2：创建vWAN中心](#)

[第 2 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 vWAN Site VPN参数](#)

[步骤 3：下载Azure vWAN Site隧道配置](#)

[第 3 阶段:FTD配置](#)

[步骤 1：分析Azure VPN配置](#)

[步骤 2：配置环回](#)

[步骤 3：配置第1阶段/第2阶段策略对象](#)

[步骤 4：配置到Azure的安全连接](#)

[步骤 5：验证到Azure的初始连接](#)

[步骤 6：配置到Azure Instance1终结点的第二个隧道](#)

[步骤 7：配置ECMP](#)

[步骤 8::配置实例专用IP的静态路由](#)

[步骤 9：配置BGP](#)

[步骤 10：配置BGP多路径](#)

[验证](#)

[其他注意事项](#)

[AS路径预置](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何配置Microsoft Azure虚拟广域网(vWAN)站点到站点VPN与思科安全防火墙的连接。

先决条件

要求

建议掌握下列主题的相关知识：

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

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

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

Microsoft Azure Virtual WAN(vWAN)将多个Azure网络、安全和路由功能结合到单个集线器结构之后。每个vWAN Hub可以托管Microsoft管理的站点到站点VPN网关，远程设备（如安全防火墙）使用该网关访问Azure，而无需构建和维护网关基础设施。

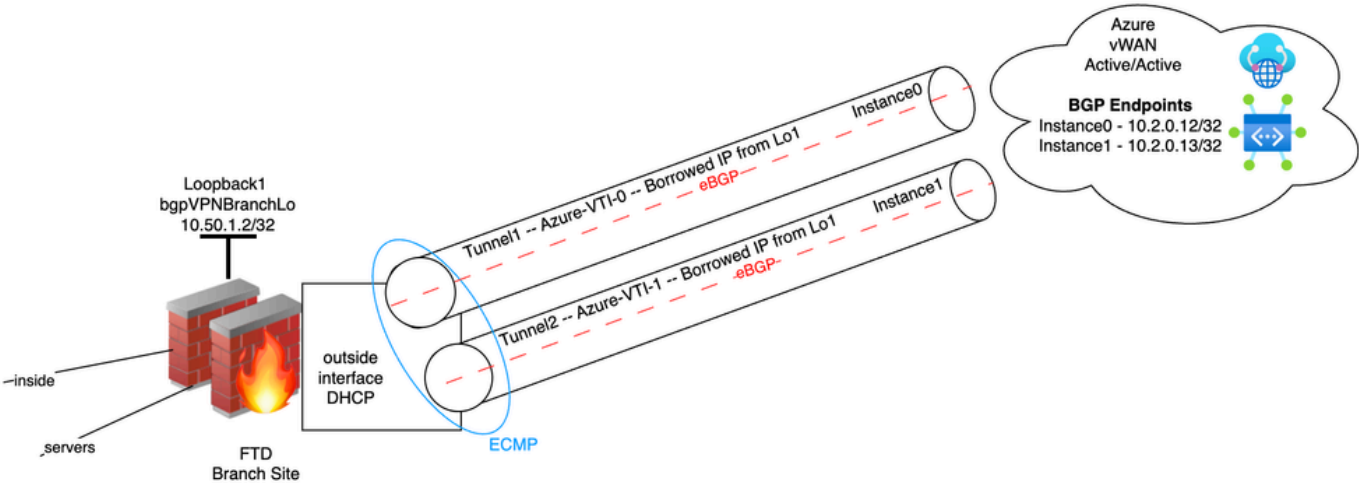
与传统双端点IPsec VPN不同，Azure vWAN Site-to-Site VPN网关部署为一对主动 — 主动实例（Instance0和Instance1），每个实例都有自己的公共IP地址和边界网关协议(BGP)对等地址。为了利用这两个实例实现冗余和额外吞吐量，分支FTD会为每个实例建立一个IP安全(IPsec)隧道，并使用BGP（而不是仅使用静态路由）在实例可用或不可用时动态学习和撤消路由。然后，FTD上的等价多路径(ECMP)路由和BGP多路径将两个隧道同时保持活动状态，而不是将一个隧道视为被动备用。

本文档将设计分为三个阶段：首先创建Azure vWAN Hub和VPN Site对象，然后下载生成的连接参数，然后使用这些相同的参数在FTD上配置匹配的虚拟隧道接口(VTI)、互联网密钥交换版本2(IKEv2)/IPsec策略、静态路由、ECMP和BGP对等（通过FMC）。

图解

该图显示了本文所述的配置拓扑。单个直接互联网访问(DIA)变体从FTD上的一个外部接口来源两个 Azure隧道。

Azure和FTD之间的单DIA链路vWAN连接 (Azure负载平衡/冗余)



配置

按顺序完成这三个阶段。在第1阶段和第2阶段中创建的Azure端对象会生成对等体IP地址、BGP自治系统(AS)编号和预共享密钥，然后在第3阶段将其应用到FTD。

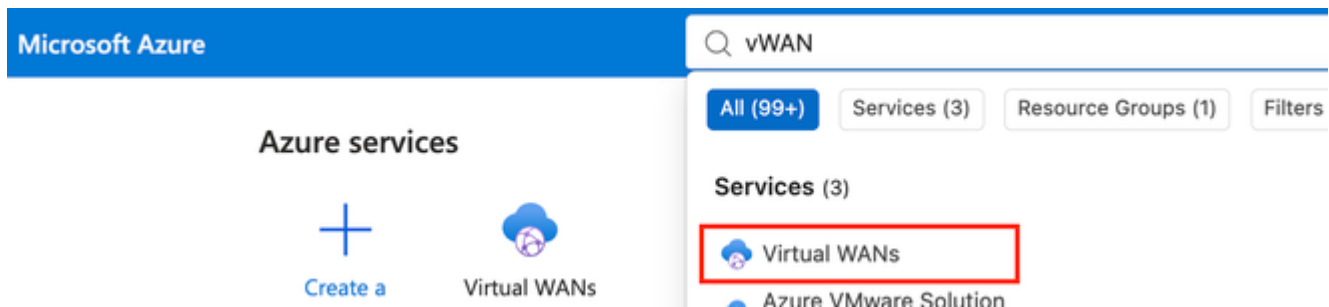
第 1 阶段：Azure vWAN/集线器配置



注意：本文档中的配置步骤是高级配置步骤，提供了将FTD连接到Azure vWAN的必要步骤。请参阅Microsoft的Azure vWAN文档，了解配置的重要性。请参阅[什么是Azure虚拟WAN?](#)和更多文档。

步骤 1：创建vWan

a)在Azure搜索框中搜索vWAN，然后点击虚拟WAN。



b)单击+ Create。



c)为新的vWAN实例输入Name，单击Review + create，然后在向导内的Review + Create页面上单击Create。

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 *
CX-vWAN

Type ⓘ

Review + create

Previous

Next : Review + create >



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。

d)点击转至资源。



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

步骤 2：创建vWAN中心

a)导航到连接>集线器，然后单击+新集线器。



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)请参阅Azure文档以获取有关进一步配置的更多上下文。请确保分配的Hub私有地址空间不会与任何内部地址空间重叠。配置Name、Virtual Hub和Hub routing preference。单击“下一步”:站点到站点>。

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

CX-vWAN-Hub

10.2.0.0/16

Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

Next : Site to site >

c)有关所显示字段的信息，请进一步参阅Microsoft Azure vWAN Hub文档。切换Yes以创建站点到站点 (VPN网关)。 分配的默认BGP自治系统(AS)编号为65515，由Internet工程任务组(IETF)在定义专用使用AS预留的请求注释(RFC)6996中分配。



注意：记录BGP AS以在FMC上执行后续配置步骤。

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 >

单击Review + create，或单击Next:指向站点>以配置可选设置。

d)验证摘要后，单击Create。



注意：按照Azure状态，创建中心需要30分钟。

Create virtual hub ...

 Validation passedBasics 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

Tanz

 Creating a hub with a gateway will take 30 minutes.[Create](#) [Previous](#) [Next](#) [Download a template for automation](#)

e)部署完成后，搜索原始vWAN资源名称。要进一步缩小搜索范围，请单击Resources。

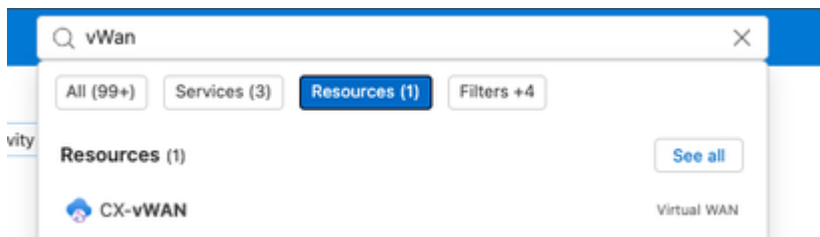
 VirtualHubDeployment | Overview ...

Deployment

    Redeploy  Download  Refresh Overview Inputs Outputs Template Your deployment is complete

 Deployment name : VirtualHubDeployment
Subscription :
Resource group :

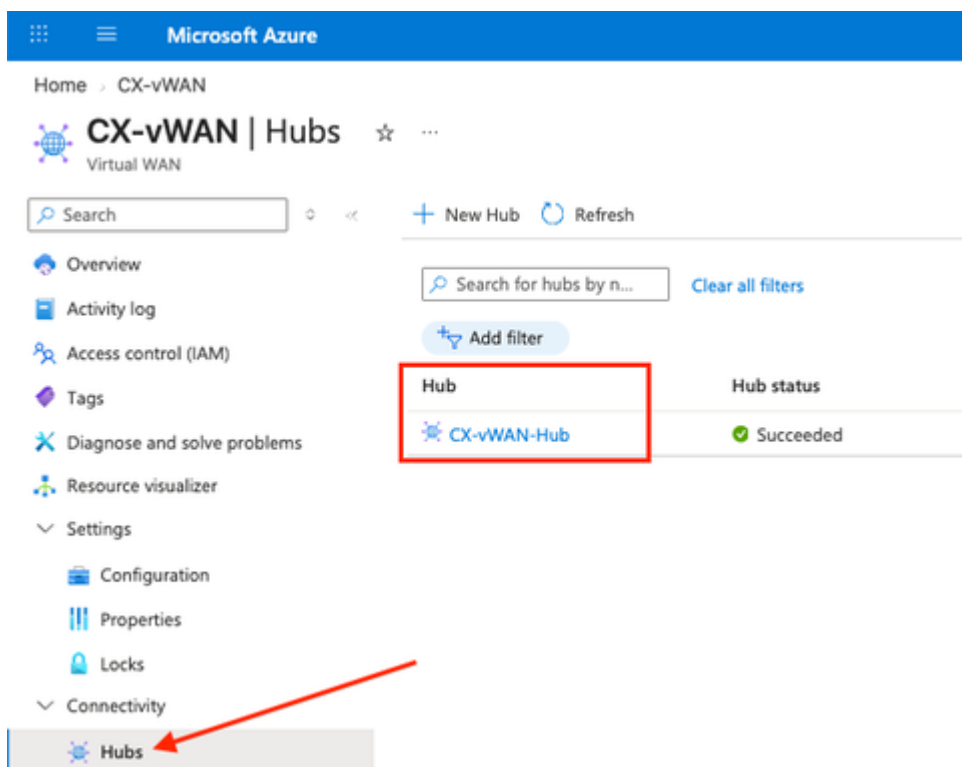
[Deployment details](#)[Next steps](#)[Go to resource](#)



第 2 阶段：Azure vWAN VPN站点配置

步骤 1：创建Azure vWAN VPN站点 (远程FTD设备)

a)通过Connectivity > Hub进入已创建的集线器，然后单击在之前步骤中创建的集线器。



b)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		

c)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 *

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)输入所需的链路信息。“链路BGP地址”和“链路ASN”字段反映了在分支站点上的内部隧道BGP第3层目标地址和BGP AS编号，与Azure的邻居关系是通过站点到站点隧道形成的。链路BGP地址是位于先前配置的集线器私有地址空间子网之外的非重叠子网地址(/32),Azure将其安装为作为/32路由以作为BGP邻居到达。链路IP地址/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IPsec/IKEv2连接所必需的。



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[How to configure BGP for Azure VPN Gateway](#)以满足特定要求。

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 ✓	...

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

Previous

Next : Review + create >

e)确认设置正确后，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

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)VPN站点的部署完成后，导航回vWAN Hub配置。

Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

[Go to resource](#)

Search vWan

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

Resources (1) [See all](#)

 **CX-vWAN** Virtual WAN

步骤 2：配置Azure vWAN Site VPN参数

a)通过Connectivity > Hub进入已创建的集线器，然后单击在之前步骤中创建的集线器。

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)再次导航到Connectivity > VPN(Site to site)，然后点击X以清除Hub Association:已连接过滤以查看断开连接的站点。

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

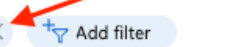
VPN Sites Metrics

Search this page Clear all filters

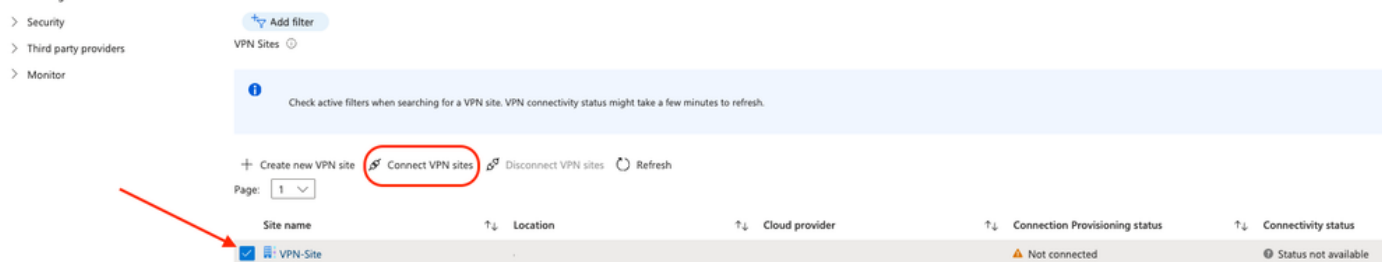
Hub association : **Connected** X Add filter

VPN Sites ⓘ

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



c)选中之前配置的VPN站点旁边的框，然后单击Connect VPN sites，该功能在选择站点后变为启用状态。



d)出现“连接站点”侧抽屉面板。输入预共享密钥(PSK)并配置所需的第1阶段IKEv2和第2阶段IPsec设置。从IPsec下拉列表中选择Custom时，值会自动填充；请注意这些值，因为它们必须在FTD上匹配。您还必须选择是否需要Perfect Forward Secrecy(PFS)。由于这是基于路由的隧道，请相应地配置设置。完成后，单击Connect保存配置。



注意：有关详细信息，请参阅[默认与自定义IPsec策略Azure vWAN](#)。

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)显示表明网关正在更新的信息以及预计的完成时间。

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

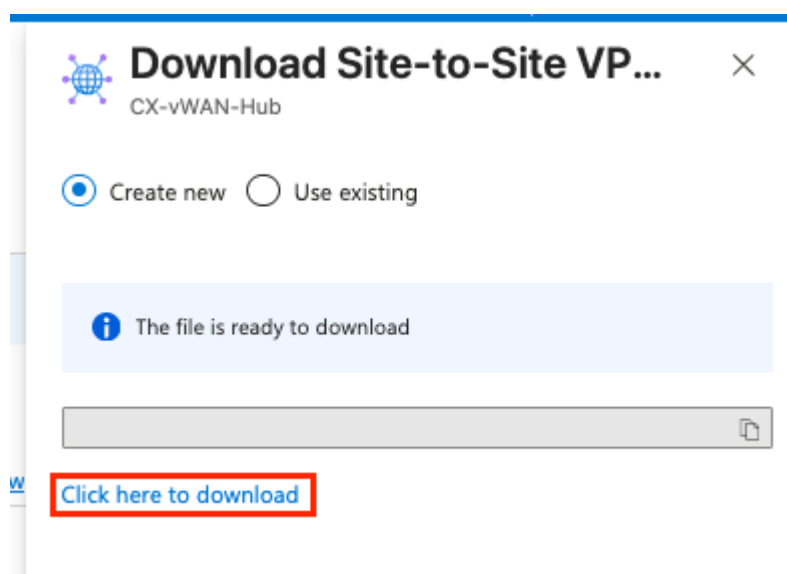
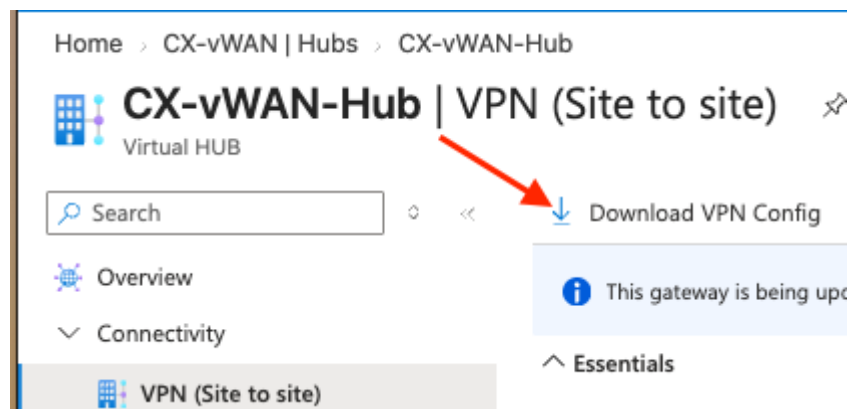
Connectivity



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

步骤 3 : 下载Azure vWAN Site隧道配置

a)更新网关时，可以下载VPN配置。



创建VPN站点并下载其连接参数（对等体地址、BGP AS编号和PSK）后，在第3阶段使用相同的值在FTD上配置匹配元素。

第 3 阶段:FTD配置

步骤 1：分析Azure VPN配置

a)从Azure打开下载的VPN配置文件。它看起来与所示的压缩输出类似，并提供有用的信息：



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。

```

[
  {
    "configurationVersion": {
      "LastUpdatedTime": "

    },
    "Version": "

    ",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "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": "

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

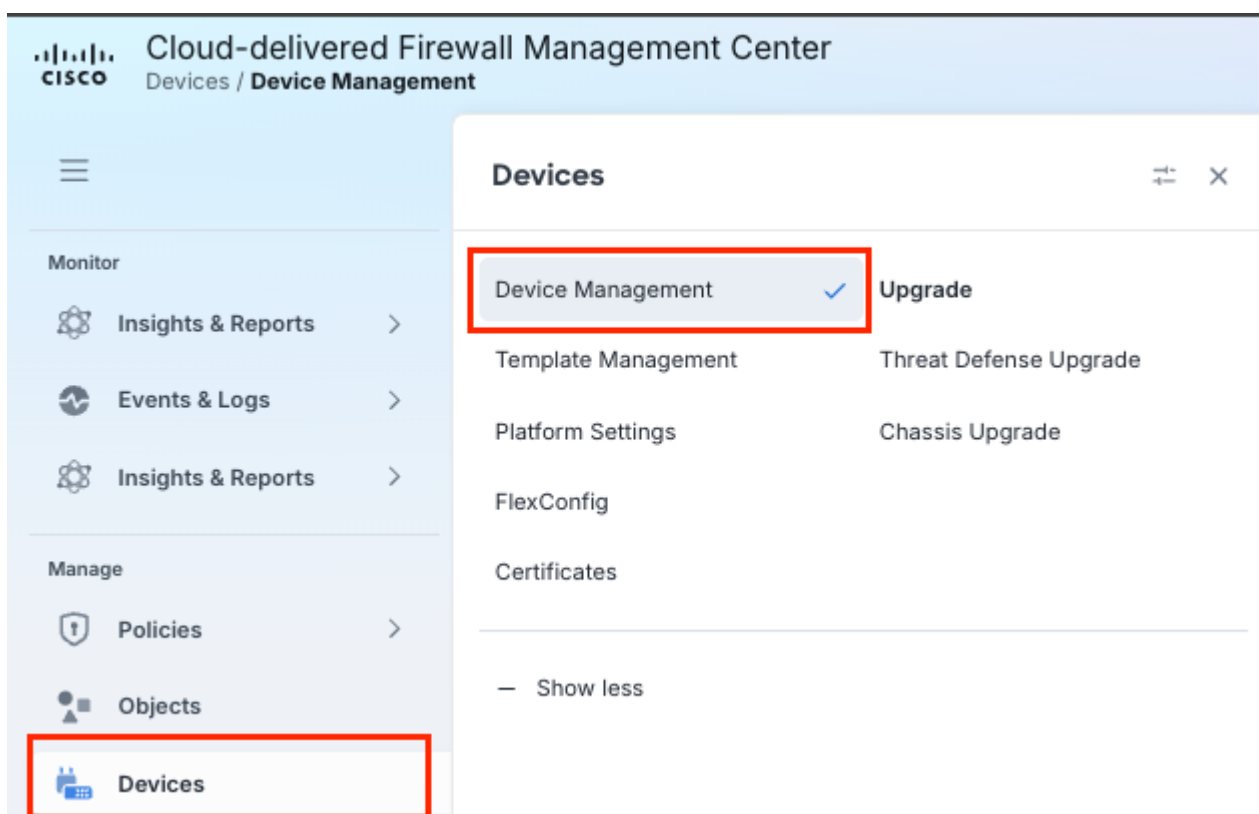
```

}
]

步骤 2：配置环回

以后配置的每个VTI都需要稳定的隧道源，因此首先配置环回接口并在两个VTI之间共享。

a)导航到Devices > Device Management。

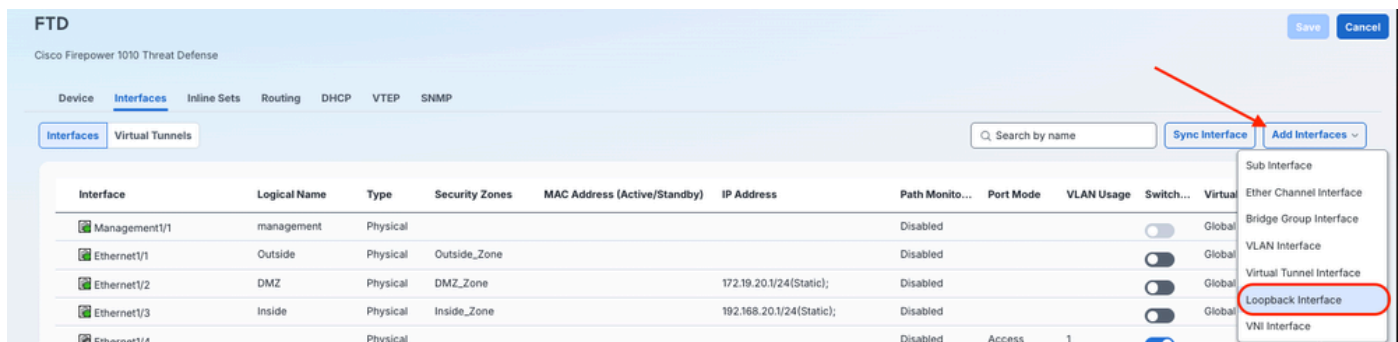


注意：本实验使用云交付的防火墙管理中心(cdFMC);但是，内部FMC的步骤保持不变。

b)选择要配置为分支/站点VPN设备的FTD。



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



d)必要时为环回接口指定Name、Loopback ID和Description。单击IPv4。

Add Loopback Interface

General **IPv4** IPv6

Name:

☒ Enabled

Loopback ID: *

(1-1024)

Description:

Cancel **OK**

e)确保IP Type定义为Use Static IP，输入Link BGP Address，如第2阶段第1d步中所配置。您可以参考之前在下载VPN配置JSON中定义的值 `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



注意：使用/32掩码并在RFC 1918 address-space中定义地址。

Add Loopback Interface

General **IPv4** IPv6

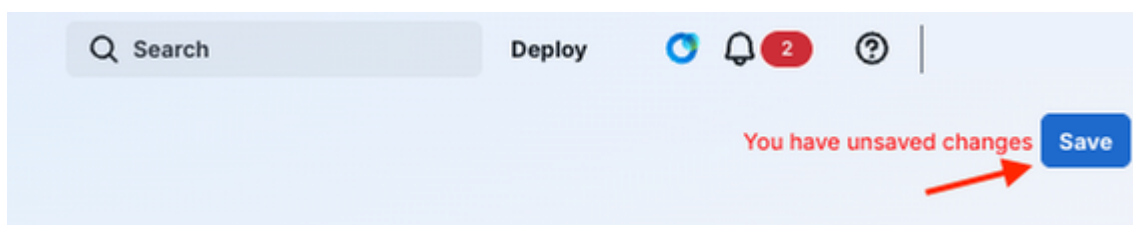
IP Type:
Use Static IP

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) 点击保存



步骤 3：配置第1阶段/第2阶段策略对象

a) 要在FMC上配置要应用于FTD VPN拓扑的匹配IKEv2/IPsec配置，请导航到Manage > Objects，在左侧菜单上向下滚动到VPN，然后展开子菜单。在菜单中选择IKEv2 Policy，然后单击Add IKEv2 Policy，配置IKEv2 Phase 1 Policy。

IKEv2 Policy

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

Add IKEv2 Policy Filter

Name	
AES-GCM-NUL- SHA	Q ☰
AES-GCM-NUL- SHA-LATEST	Q ☰
AES- SHA -SHA	Q ☰
AES- SHA -SHA-LATEST	Q ☰
DES- SHA -SHA	Q ☰
DES- SHA -SHA-LATEST	Q ☰
Umbrella-AES-GCM-256	Q ☰

Policy List
Port
> Prefix List
Route Map
> Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute
Group Policy
IKEv1 IPsec Proposal
IKEv1 Policy
IKEv2 IPsec Proposal
IKEv2 Policy
Secure Client Customization
Secure Client File

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

b)输入新IKEv2策略的名称，选择Priority和/或Lifetime。确保与Integrity、Encryption、PRF和Diffie-Hellman(DH)组相关的隧道两端策略匹配。选择要与Azure配置匹配的对齐的算法/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:*
Azure_IKEv2

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)
3600

Available Algorithms

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

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

Selected Algorithms

SHA256

Cancel Save

c)完成配置后，单击Save。

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

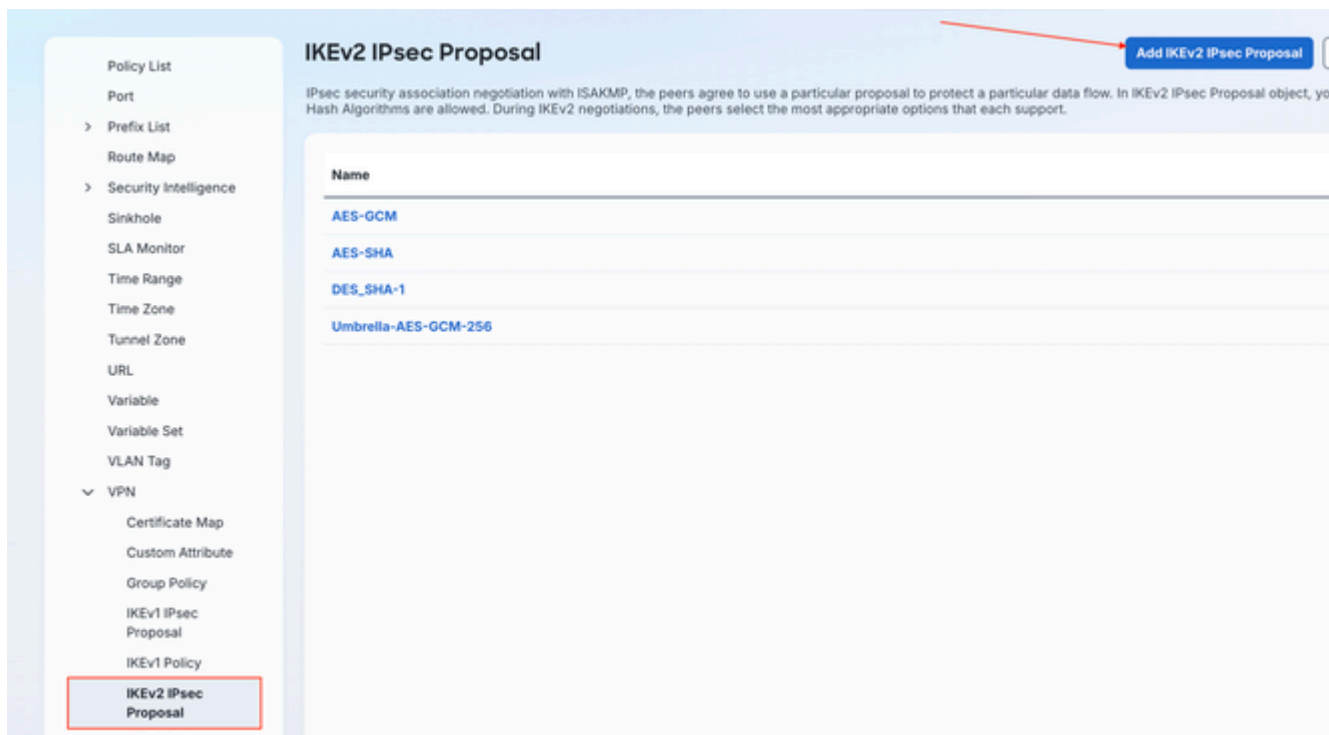
...

Add

14

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

d)在IKEv2 IPsec Proposal子菜单中配置Phase 2/IPsec参数，然后单击Add IKEv2 IPsec Proposal。



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



注意：您可以在下载的配置文件中引用这些值，网址为
： `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

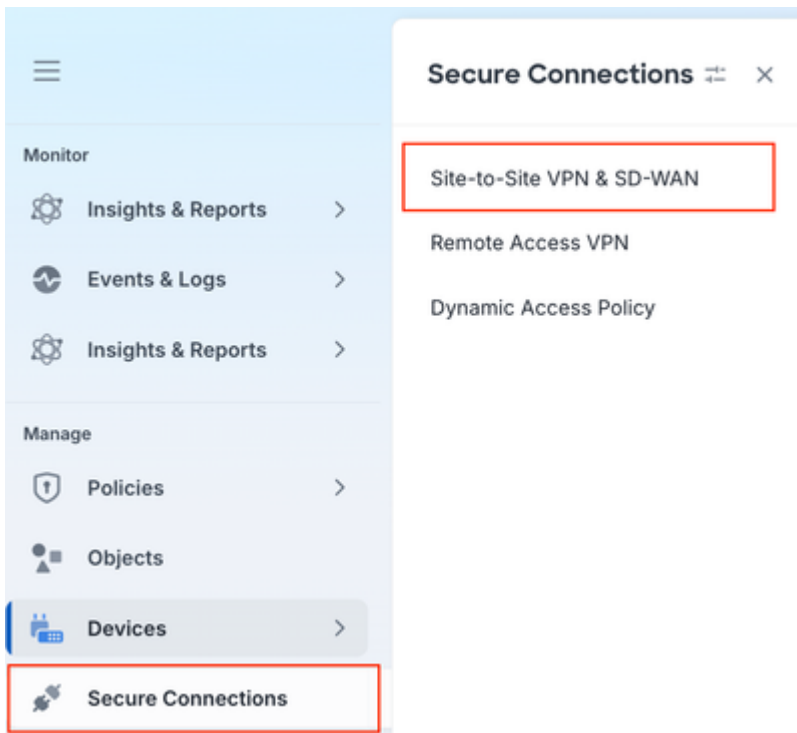


Cancel

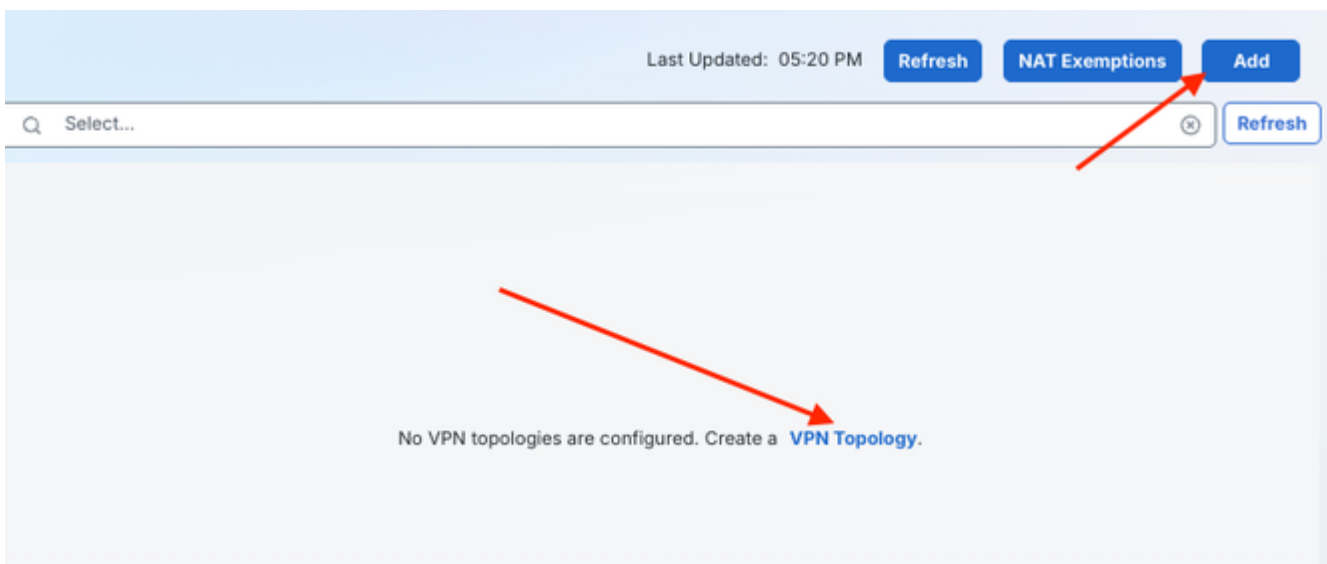
Save

步骤 4：配置到Azure的安全连接

a)导航到管理>安全连接>站点到站点VPN和SD-WAN。



b) 点击中间的初始VPN拓扑配置超链接，或者点击添加。



c) 为通向Azure Instance0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 *

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)对于Node A，点击Device下拉列表，并选择部署配置的托管FTD/FTD HA-Pair的名称。对于节点B，因为它是在Azure vWAN实例上终止的拓扑中的连接的远程端，所以从Device下拉列表中选择Extranet。接下来，对于Node A，点击虚拟隧道接口(VTI)下拉列表旁的+图标。

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:*

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

Cancel Save

e)为第一个VTI命名Name，并确保其为Enabled。将新的或现有的Security Zone分配给VTI，分配

Tunnel Source，并从相邻下拉列表中选择IP address。

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) 下一步，确保选中Bordering IP(IP unnumbered)单选按钮，然后从右侧下拉列表选择相同的loopback。完成后，单击OK。

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

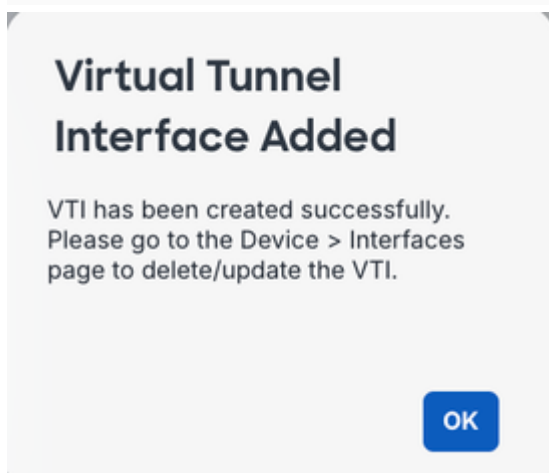
Tunnel ID:*
 (0 - 10413)

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)



g)配置并应用VTI后，手动填充隧道源IP地址（如果从DHCP填充父接口地址，则自动填充），并确保配置了Node B设备名称以及Instance Endpoint IP Address。完成后，单击IKE选项卡。



注意：您可以在以下位置下载的配置文件中引用Instance0终端IP地址值：
： `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

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:*
Azure-VTI-0 +

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:*
Extranet

Device Name*:
Azure-Instance-0

Endpoint IP Address*:

Cancel Save

h)向下滚动到IKEv2 Settings，并确保Authentication Type设置为Pre-shared Manual Key，然后输入之前步骤中在Azure中配置的PSK。通过点击铅笔图标以编辑可用的IKEv2策略，配置IKEv2第1阶段策略。



注意：注意：您可以在以下位置下载的配置文件中引用预共享密钥：

```
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

i) 添加最初在步骤3中配置的IKEv2第1阶段策略。

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)选择IPsec选项卡。

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)单击Transform Sets下的IKEv2 IPsec Proposal，方法是点击铅笔图标。

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)单击trash bin图标以删除默认AES-GCM转换集，并添加在第3步的后半部分创建的自定义Azure_IPsec转换集/IKEv2 IPsec提议。单击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)向下滚动并输入27000作为与Azure参数匹配的生存期。启用PFS组（如果适用）。Click Save.



注意：您可以在以下位置下载的配置文件中引用生命周期值
： `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)部署更改。

Search

Deploy

Search Device

Advanced Deploy

Deploy All

☐ FTD

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

o)部署完成后，在Tunnel Status Distribution下选中Manage > Secure Connections > Site-to-Site VPN & SD-WAN;成功的连接显示为绿色（向上）。

Last Updated: 11:11 PM

Refresh

NAT Exemptions

Add

Select...

Refresh

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

部署第一个隧道后，在配置第二个隧道以实现冗余之前，请确认它已在IKE/IPsec和BGP层成功建立。

步骤 5：验证到Azure的初始连接

a)通过SSH进入FTD，然后输入system support diagnostic-cli、键入en，然后按Enter，因为只读FTD CLI上没有密码。

```
<#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)检查阶段1/阶段2隧道状态。

```
<#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)执行捕获以检查隧道中从Azure接收的BGP传输控制协议(TCP)数据包，以及来自Instance-0Azure隧道的公共IP的外部捕获上的Network Address Translation - Traversal(NAT-T)User Datagram Protocol(UDP)port 4500/UDP port 500 traffic。

```
<#root>
```

```
ftd#
```

```
capture out-instance-0 trace interface Outside match ip host
```

```
any
```

```
ftd#
```

```
capture tun-vti-0 interface Azure-VTI-0 trace match ip host
```

```
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
```

```
2: 03:23:44.511204      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240
```

```
3: 03:23:46.512211      10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240
```

```
ftd#
```

确认与Instance0的连接后，为Instance1重复相同的VTI和VPN拓扑配置，以使两个Azure网关实例

均可访问。

步骤 6：配置到Azure Instance1终结点的第二个隧道

a)创建从同一环回借用的第二个VTI(Azure-VTI-1)（第3b-f步）。

Virtual Tunnel Interface Details

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

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

Ethernet1/1 (Outside)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4

☐ IPv6

IP Address:*

☐ Configure IP

i

☒ Borrow IP (IP unnumbered)

Loopback1 (bgpVPNBranchLo)

+

VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b)配置第二个实例VPN拓扑（步骤4 g-n）。



注意：您可以在以下位置下载的配置文件中引用Instance1 Endpoint IP Address值：
： 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)部署配置更改，并检查隧道状态。

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)签入Azure，Instance0和Instance1都获得Connected。

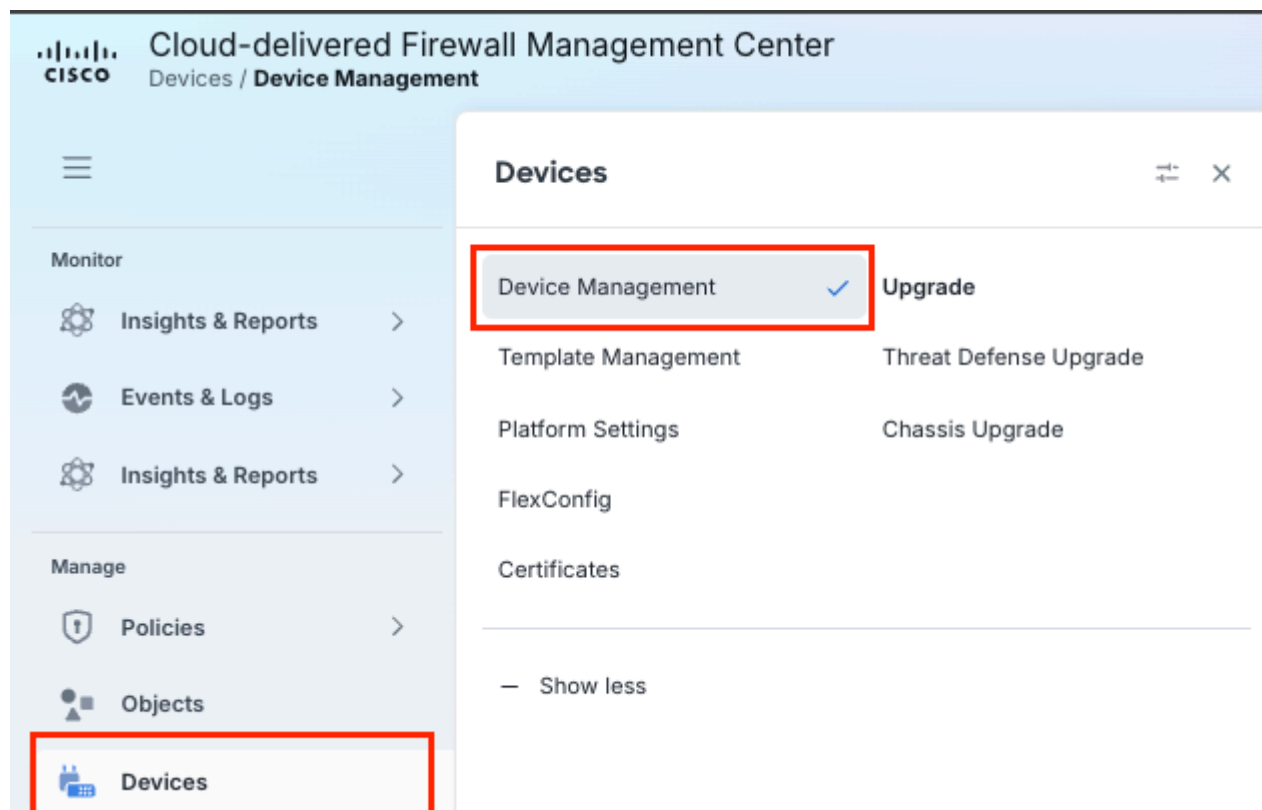
Links

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

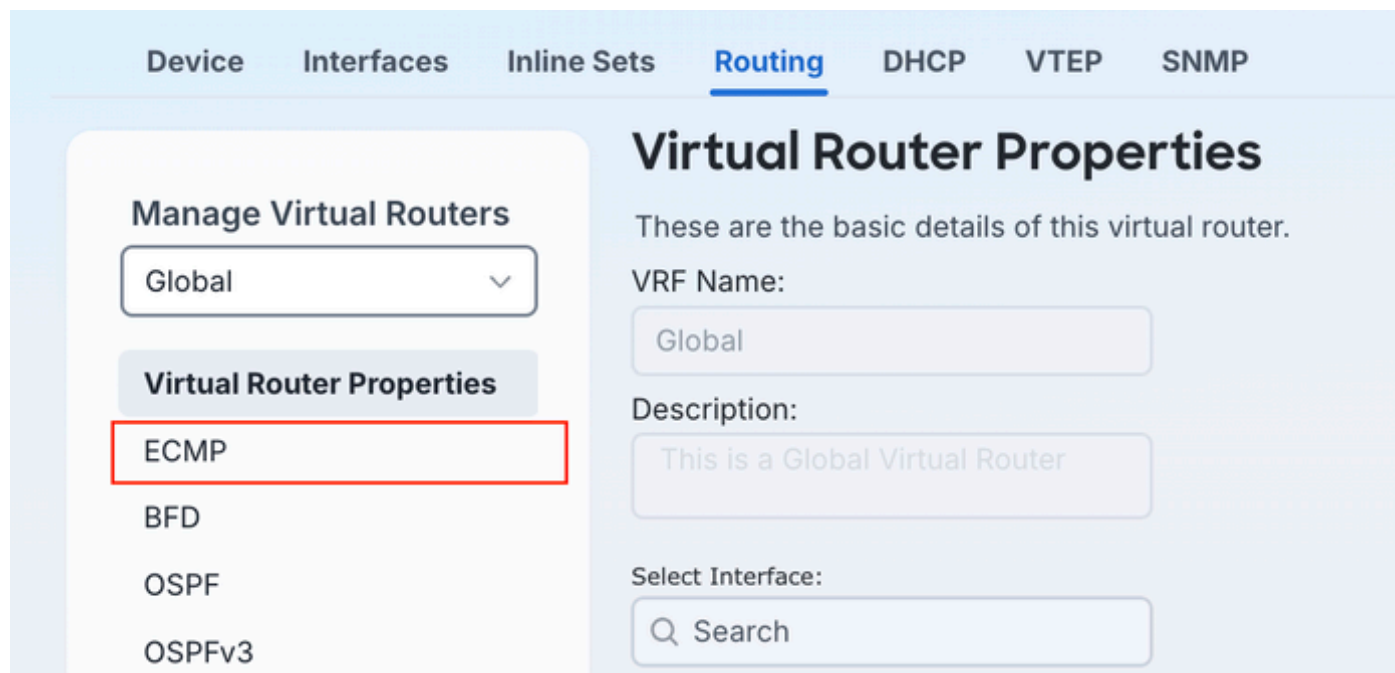
当两个隧道都处于活动状态时，FTD需要ECMP路由，以便流量可以同时使用两个路径，而不是将第二个隧道视为被动备用。

步骤 7：配置ECMP

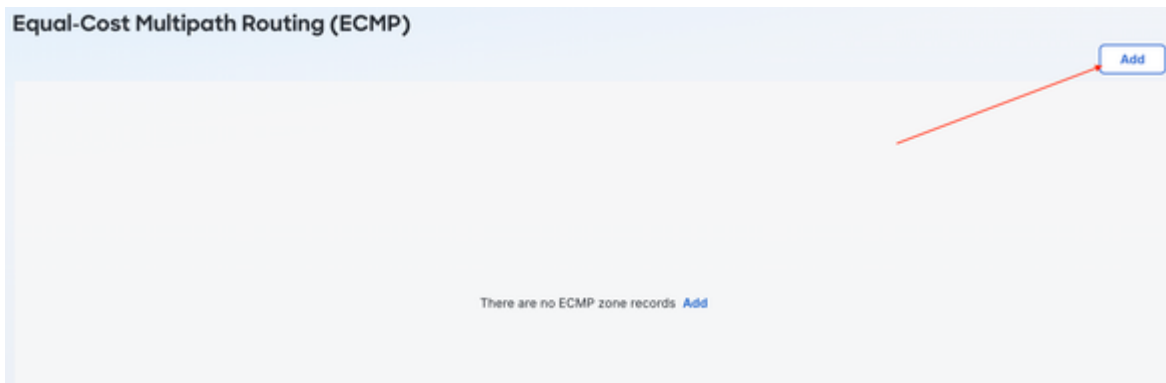
a)导航到Manage > Devices > Device Management，然后选择FTD，将VPN配置为Azure。



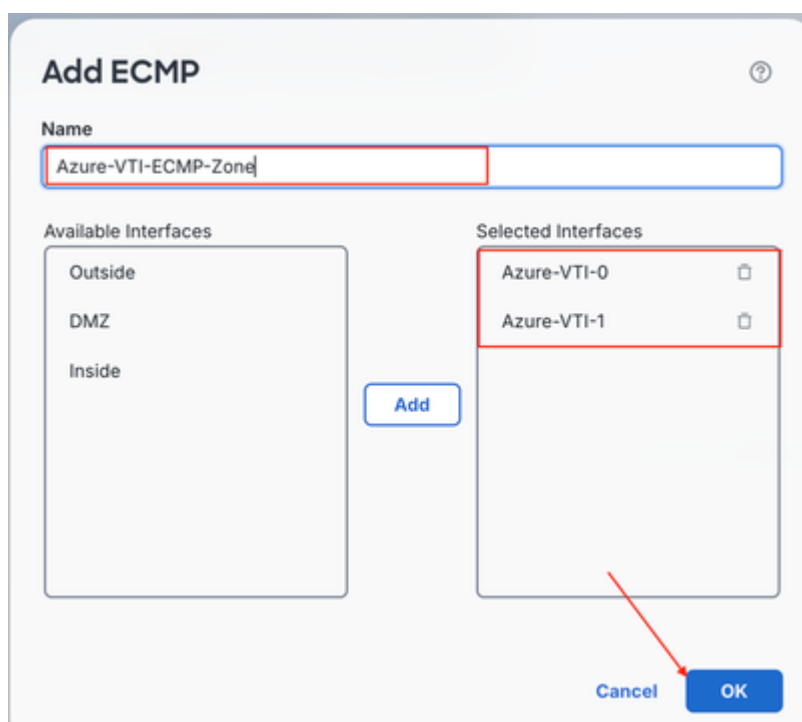
b)单击Routing选项卡并选择ECMP。



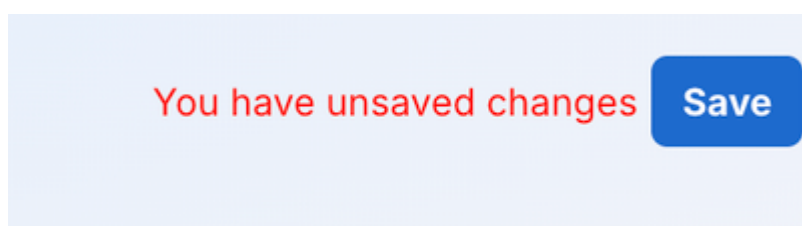
c)单击Add以创建新的ECMP区域。



d)通过在Available Interfaces面板中点击两个VTI，然后点击Add将VTI应用于指定的ECMP区域，切换以突出显示VTI。



e)确认设置正确后，单击Save。



步骤 8::配置实例专用IP的静态路由

BGP需要路由才能成功连接到邻居，并且由于终端不是直接连接的，因此默认情况下不会填充任何路由。ECMP允许您使用相同度量（管理距离）配置到相同目标的静态路由，以便两个路由都安装在路由信息库(RIB)中并同时使用。

a)导航到Manage > Devices > Device Management，然后选择适用的FTD设备。

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)导航到路由>静态路由。

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

c)单击+ Add Route。

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

d)通过创建指向Instance0 VTI的第一条路由，为两个实例IP地址添加路由，并通过单击“可用网络”旁边的+为其添加目标网络对象。然后，从列表中单击网络对象，然后单击“添加”按钮，将其添加为静态路由的目标。请确保选择Instance0 IP并将其设置为Gateway。完成后，单击OK。



注意：这些静态路由目标网络值位于下 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` 载的配 `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` 置文件下方，并位于下载的配置文件中。

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*
 Azure-VTI-0

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

Available Network

Search: a

- Azure-Instance0-BGP_Peer
- Azure-Instance1-BGP_Peer

Add

Selected Network

- Azure-Instance0-BGP_Peer

Azure-Instance0-BGP_Peer
10.2.0.12

Ensure that egress virtualrouter has route to that destination

Gateway
 Azure-Instance0-BGP_Peer

Metric:
 1
 (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e)重复步骤c-d，通过Instance1 VTI添加第二条静态路由。确保单击Save保存更改。

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						

静态路由仅到达BGP对等地址；BGP本身仍然必须启用和对，以便Azure和FTD能够动态地相互交换路由到更大的网络，或从其他更大的网络交换路由。

步骤 9：配置BGP

a)在Routing > General Settings > BGP下，在FTD上启用BGP进程65500。选中Enable BGP复选框，并输入之前在第2阶段第1步中配置的AS编号。导航到Routing > BGP > IPv4旁。

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

SNMP

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

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)通过选中相邻的Enable IPv4复选框，为进程/AS 65500启用IPv4 BGP路由，然后单击Neighbor以配置BGP邻居。

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)单击+ Add。

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)输入Instance0 BGP对等信息，从vWAN集线器引用指定的BGP AS，然后将其输入为Neighbor Remote AS，如果需要，请添加说明。单击 Advanced。



重要信息：确保更改BGP更新源以引用FTD上两个VTI接口的环回父接口。

Add Neighbor

IP Address*
10.2.0.12

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

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

BFD Fallover
none

Description
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e)在FTD上的BGP Neighbor配置的Advanced菜单中，您可以将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。

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

f)对Azure Instance1 BGP对等体重复相同的步骤。

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

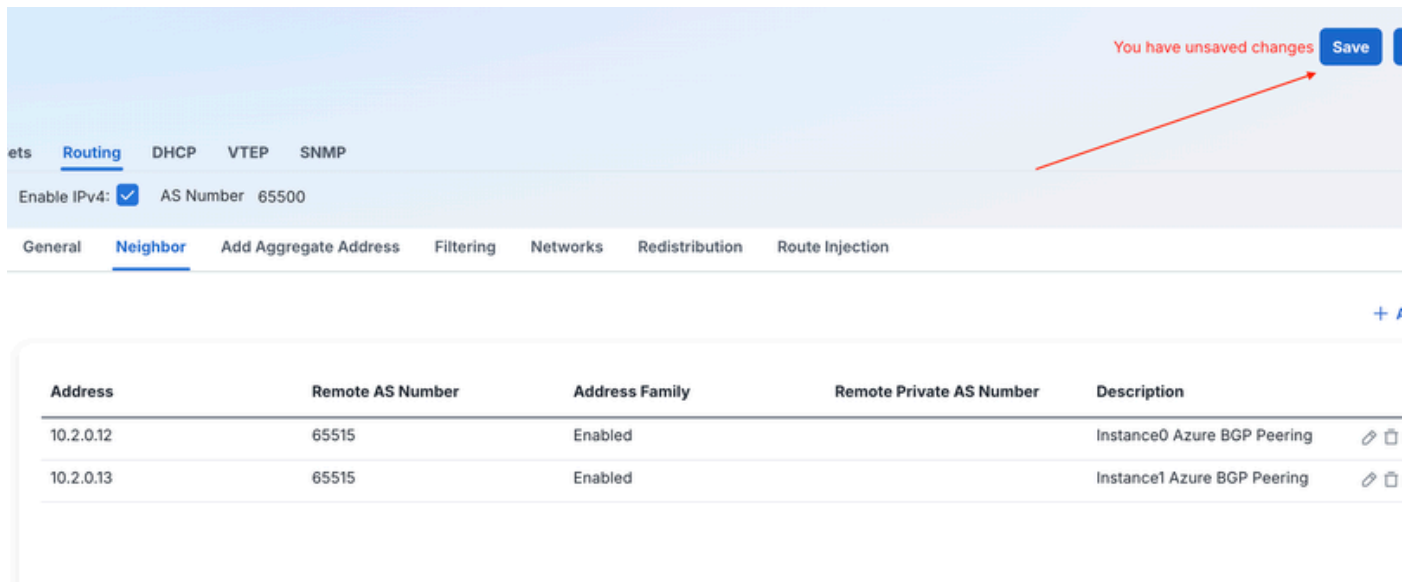
☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

g)确保在完成后保存更改。



默认情况下，BGP在路由表中只安装一个最佳路径，即使ECMP使两个静态路由都可用。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 10：配置BGP多路径

a)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。

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)将Number of Paths字段的默认值从1更改为2。

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c)确保Save并部署更改。

验证

部署完成后，确认BGP与两个Azure实例形成邻接关系。随后，使用第3阶段第5步中建立的相同诊断CLI访问，确认路由通过两个隧道获知，流量使用两个VTI。

在FTD CLI上导航至system support diagnostic-cli。

a)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#
```

```
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)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 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)检查VTI数据包计数。

<#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)确认BGP邻居的静态路由。

<#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)确认ECMP区域。

<#root>

ftd#

show zone

```
Zone: Azure-VTI-ECMP-Zone ecmp
  Security-level: 0
  Zone member(s): 2
    Azure-VTI-1          Tunnel2
    Azure-VTI-0          Tunnel1
```

ftd#

f)确认BGP配置。

<#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)确认路由表。

<#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
```

其他注意事项

本文档中的基本配置假设分支机构FTD有一个外部接口和一个ISP。这些考虑因素扩展了设计。

AS路径预置

如果您需要影响Azure或FTD首选哪两个隧道作为主隧道，而不是通过ECMP和BGP多路径等量共享负载，请将本地AS编号提前一次或多次在BGP邻居上作为辅助隧道处理。在标准BGP最佳路径选择过程中，具有更长预置AS路径的邻居将取消优先顺序，而无需从ECMP区域完全删除该邻居。

故障排除

- 第1阶段/第2阶段隧道不出现：确认预共享密钥和IKEv2/IPsec策略参数（加密、完整性、PRF、DH组和生存期）在FMC IKEv2策略/IPsec建议与下载的Azure VPN配置文件中的值之间完全匹配。使用`show crypto isakmp sa`和`show crypto ipsec sa`，如第3阶段第5步所示。
- 隧道已打开，但BGP邻居未形成 `update-source`：验证BGP已设置为环回接口，而不是VTI本身，并且已配置为具有足够高的值，可以到达Azure BGP对等地址，该地址未直接连接到FTD`ebgp-multihop`。
- BGP形成，但只有一个隧道传输流量：确认两个VTI属于同一个ECMP区域，以相同的管理距离安装到两个Azure实例BGP地址的静态路由，并且为两个路径配置BGP多路径，如第3阶段第10步所述。
- 无返回流量，或者到Azure的非对称路由：由于Azure vWAN在两个隧道上通告中心地址空间，请确保在路由配置的其他位置未禁用ECMP，并检查路由映射或可以将流量固定到单一路径的基于策略的路由。
- BGP已启用且路由已安装，但流量似乎被阻止：确保您已使用分配给VTI的安全区域配置了访问控制规则，允许流量进入入口和出口。

相关信息

- [什么是Azure虚拟WAN？](#)
- [如何为Azure VPN网关配置BGP](#)
- [默认与自定义IPsec策略Azure vWAN](#)
- [排除Azure VPN网关的BGP问题](#)
- [关于主用 — 主用模式VPN网关](#)
- [教程：使用Azure虚拟WAN创建站点到站点连接](#)

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）。