

Azure vWANサイト間VPNをセキュリティで保護されたファイアウォールに構成する

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[図](#)

[AzureとFTD間の単一DIAリンクvWAN接続 \(Azureロードバランシング/冗長性 \)](#)

[設定](#)

[フェーズ1: Azure vWAN/Hub構成](#)

[ステップ1:vWANの作成](#)

[手順2:vWANハブの作成](#)

[フェーズ2: Azure vWAN VPNサイトの構成](#)

[手順1: Azure vWAN VPNサイトの作成 \(リモートFTDデバイス \)](#)

[手順2: Azure vWANサイトのVPNパラメーターを構成します](#)

[手順3: Azure vWANサイトトンネル構成のダウンロード](#)

[フェーズ3:FTDの設定](#)

[手順1: Azure VPN構成の分析](#)

[ステップ2: ループバックの設定](#)

[ステップ3: フェーズ1/フェーズ2ポリシーオブジェクトの設定](#)

[手順4: Azureへのセキュアな接続を構成する](#)

[手順5: Azureへの初期接続を確認します](#)

[手順6: Azure Instance1エンドポイントへの2番目のトンネルを構成します](#)

[ステップ7:ECMPの設定](#)

[ステップ8: プライベートIPをインスタンス化するためのスタティックルートを設定する](#)

[ステップ9:BGPの設定](#)

[ステップ10:BGPマルチパスの設定](#)

[確認](#)

[それ以外に考慮すること](#)

[AS-Pathブリベンド](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Secure FirewallへのMicrosoft Azure Virtual WAN(vWAN)サイト間VPN接続の設定について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Microsoft Azure仮想ワイドエリアネットワーク(vWAN)
- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure FTDバージョン10.0
- Cisco Secure FMCバージョン10.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Microsoft Azure Virtual WAN (vWAN)は、複数のAzureネットワーキング、セキュリティ、ルーティング機能を1つのHub構成にまとめます。各vWANハブは、Microsoftが管理するサイト間VPNゲートウェイをホストできます。このゲートウェイは、ゲートウェイインフラストラクチャを構築および維持することなく、セキュアファイアウォールなどのリモートデバイスがAzureにアクセスするために使用します。

従来の2つのエンドポイントを持つIPsec VPNとは異なり、Azure vWANサイト間VPNゲートウェイは、アクティブ-アクティブインスタンスのペア (Instance0とInstance1) として導入され、それぞれに独自のパブリックIPアドレスとBorder Gateway Protocol (BGP)ピアリングアドレスが割り当てられます。冗長性と追加スループットの両方のインスタンスを利用するために、ブランチFTDは各インスタンスに対して1つのIPセキュリティ(IPsec)トンネルを確立し、スタティックルーティングだけでなくBGPを使用して、インスタンスが使用可能または使用不能になったときに動的にルートを学習して取り消します。FTD上のEqual-Cost Multi-Path(ECMP)ルーティング

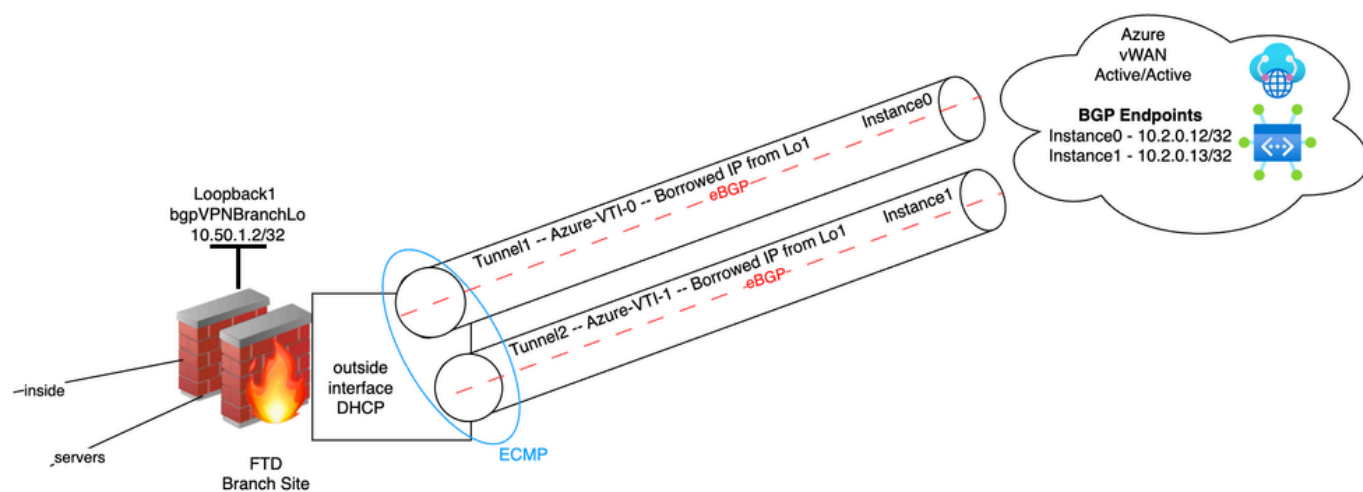
とBGPマルチパスによって、両方のトンネルが同時にアクティブに保たれます。一方をパッシブスタンバイとして扱う必要はありません。

このドキュメントでは、この設計を3つのフェーズで構成します。まず、Azure vWANハブとVPNサイトオブジェクトが作成され、結果として生成される接続パラメータがダウンロードされます。次に、これらの同じパラメータを使用して、一致する仮想トンネルインターフェイス (VTI)、インターネットキーエクスチェンジバージョン2(IKEv2)/IPsecポリシー、スタティックルート、ECMP、およびFMCを介したFTDでのBGPピアリングを設定します。



次の図は、この記事で説明する設定のトポロジを示しています。単一のダイレクトインターネットアクセス(DIA)バリエーションは、FTDの1つの外部インターフェイスから両方のAzureトンネルを取得します。

AzureとFTD間の単一DIAリンクvWAN接続 (Azureロードバランシング/冗長性)



設定

3つのフェーズを順に完了します。フェーズ1とフェーズ2で作成されたAzure側のオブジェクトは、ピアのIPアドレス、BGP自律システム(AS)番号、およびフェーズ3でFTDに適用される事前共有キーを生成します。

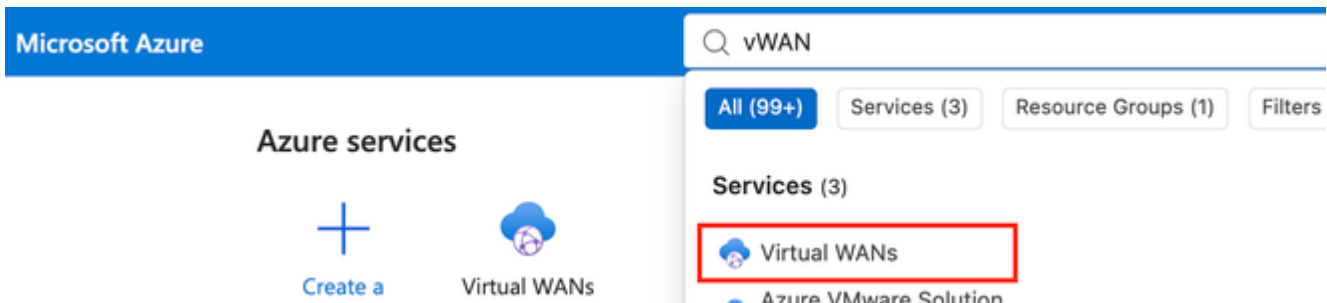
フェーズ1: Azure vWAN/Hub構成



注：このドキュメントの設定手順は概要を説明するもので、FTDをAzure vWANに接続するために必要な手順が記載されています。構成の重要性については、MicrosoftのAzure vWANドキュメントを参照してください。「[Azure Virtual WANとは何ですか](#)」と詳しいドキュメントを参照してください。

ステップ1:vWANの作成

a) Azureの検索ボックスでvWANを検索し、Virtual WANsをクリックします。



b) + Createをクリックします。



c)新しいvWANインスタンスの名前を入力し、Review + createをクリックして、ウィザードのReview + CreateページでCreateをクリックします。

Create WAN ...

Basics Review + create

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

Project details

Subscription *

Resource group *
[Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >



注：イメージのさまざまなフィールドの値をカバーする空白文字は、このドキュメントの発行を意図したものです。

d) Go to resourceをクリックします。



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

手順2:vWANハブの作成

a) Connectivity > Hubsの順に移動し、+ New Hubの順にクリックします。



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) 詳細な構成のコンテキストについては、Azureのドキュメントを参照してください。割り当てられているハブプライベートアドレス空間が、どの内部アドレス空間とも重複していないことを確認してください。名前、仮想ハブ、ハブルーターティング設定を設定します。Next : Site to site > をクリックします。

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

Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next : Site to site >](#)

c) 表示されるフィールドの詳細については、Microsoft Azure vWAN Hubのドキュメントを参照してください。Yesを切り替えて、サイト間 (VPNゲートウェイ) を作成します。割り当てられるデフォルトのBGP自律システム(AS)番号は65515です。これは、Internet Engineering Task Force (IETF ; インターネット技術特別調査委員会) によって、Private Use AS Reservationを定義するRequest For Comments (RFC ; コメント要求) 6996で割り当てられたものです。



注:FMCでの今後の設定手順のために、BGP ASを記録しておきます。

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 >

オプションの設定を行うには、Review + createをクリックするか、Next : Point to site >をクリックします。

d)サマリーを確認したら、Createをクリックします。



注: Azureが言うように、ハブの作成には30分かかります。

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

Time

 Creating a hub with a gateway will take 30 minutes.**Create**

Previous

Next

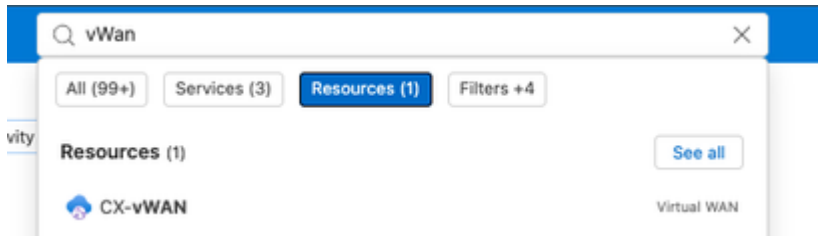
[Download a template for automation](#)

e)導入が完了したら、元のvWANリソース名を検索します。検索をさらに絞り込むには、Resourcesをクリックします。

 VirtualHubDeployment | Overview ...
Deployment Search Delete  Cancel  Redeploy  Download  Refresh Overview Inputs Outputs Template Your deployment is complete

 Deployment name : VirtualHubDeployment
Subscription :
Resource group :

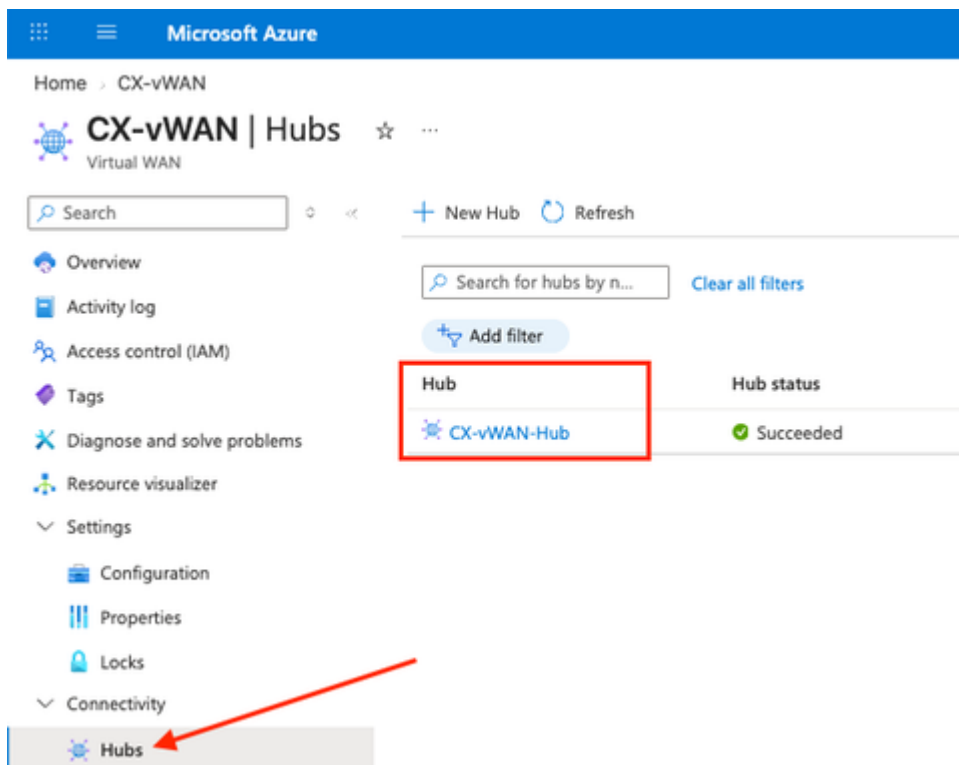
 Deployment details Next steps[Go to resource](#)



フェーズ2: Azure vWAN VPNサイトの構成

手順1: Azure vWAN VPNサイトの作成 (リモートFTDデバイス)

a) Connectivity > Hubsの順に選択し、前のステップで作成したハブをクリックして、作成したハブを入力します。



b) Connectivity > VPN (Site to site)の順にクリックし、+Create new VPN siteをクリックします。

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)必須フィールドに値を入力します。終了したら、Next: Links >をクリックして次に進みます。

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)必要なリンク情報を入力します。Link BGP AddressフィールドとLink ASNフィールドには、Azureとのネイバーシップがサイト間トンネル経由で形成されるブランチサイトの内部トンネルBGPレイヤ3宛先アドレスとBGP AS番号が反映されます。リンクBGPアドレスは、以前に構成されたハブプライベートアドレス空間サブネットの外部にある重複しないサブネットアドレス(/32)です。Azureは、このアドレスをBGPネイバーとして到達する/32ルートとしてインストールします。リンクIPアドレス/FQDNは、IPsec/IKEv2接続をプロビジョニングするために必要な、ブランチサイトに送信されるトラフィックの外部ヘッダーレイヤ3宛先IPアドレスです。



注：トンネルアドレスに169.254.21.0 ~ 169.254.22.255の範囲のアドレスを使用している場合は、「[Azure VPN Gateway用にBGPを構成する方法](#)」を確認して特定の要件を確認してください。

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

Link name	Link speed	Link provider name	Link IP address / FQDN	Link BGP address	Link ASN	
single-dia-link ✓	1000 ✓	provider ✓	✓	10.50.1.2 ✓	65500 ✓	...

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

Previous

Next : Review + create >

e)設定が正しいことを確認したら、Createをクリックします。

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サイトの導入が完了したら、vWANハブの設定に戻ります。

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

手順2: Azure vWANサイトのVPNパラメーターを構成します

a) Connectivity > Hubsの順に選択し、前のステップで作成したハブをクリックして、作成したハブを入力します。

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)再度Connectivity > VPN (Site to site)の順に移動し、XをクリックしてHub Association: Connectedフィルタリングをクリアし、切断されたサイトを表示します。

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

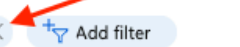
VPN Sites Metrics

Search this page Clear all filters

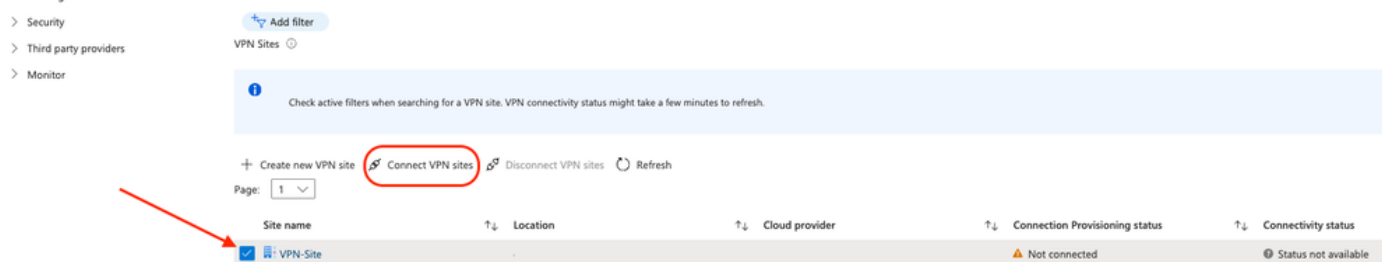
Hub association : **Connected** X Add filter

VPN Sites ⓘ

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



c)以前に設定したVPNサイトの横にあるボックスをオンにし、Connect VPN sitesをクリックします。これは、サイトを選択すると有効になります。



d) [サイトの接続]サイドドロワーパネルが表示されます。事前共有キー(PSK)を入力し、目的のフェーズ1 IKEv2とフェーズ2 IPsec設定を設定します。IPsecドロップダウンリストからCustomを選択すると、値が自動的に入力されます。これらの値はFTDで一致する必要があるため、注意してください。また、Perfect Forward Secrecy (PFS ; 完全転送秘密) が必要かどうかを選択する必要もあります。これはルートベースのトンネルであるため、設定を適宜設定します。完了したら、Connectをクリックして設定を保存します。



注：詳細については、「[Default vs. Custom IPsec Policies Azure vWAN](#)」を参照してください。

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)ゲートウェイが更新されていることを示す情報と、完了までの推定時間が表示されます。

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

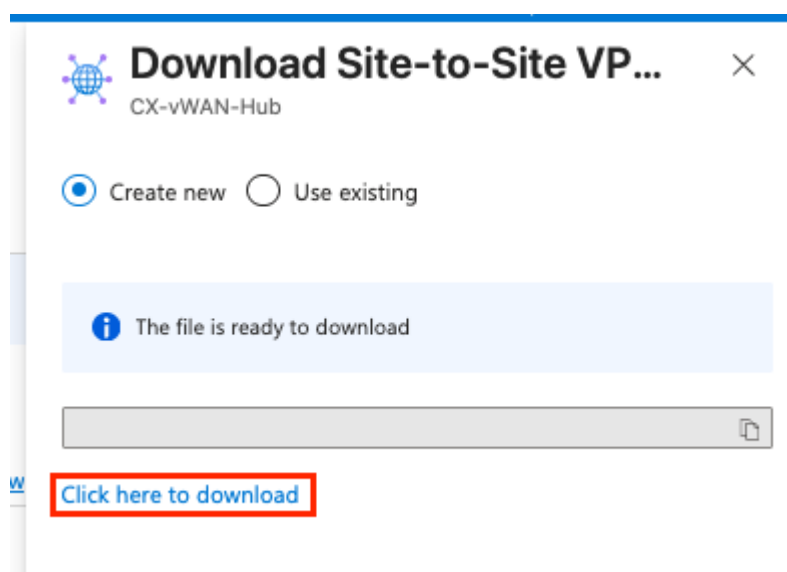
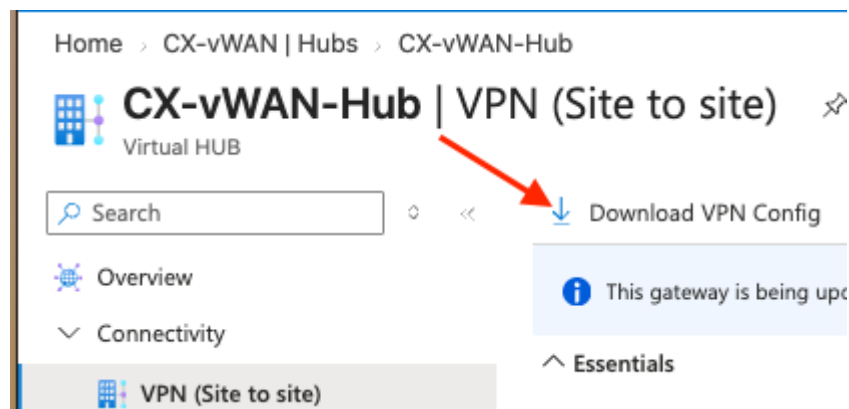
Overview

Connectivity

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

手順3: Azure vWANサイトトンネル構成のダウンロード

a)ゲートウェイの更新中に、VPN設定をダウンロードできます。



VPNサイトが作成され、その接続パラメータ（ピアアドレス、BGP AS番号、およびPSK）がダウンロードされた状態で、フェーズ3のFTDで一致する要素を設定するために同じ値が使用されます。

フェーズ3:FTDの設定

手順1: Azure VPN構成の分析

a)ダウンロードしたVPN設定ファイルをAzureから開きます。この出力は簡潔に示されているものに似ており、役に立つ情報を提供します。



注：焦点を合わせやすくするために、無関係なオブジェクトやキー/値のペアを簡略化す

るためにプルーニングします。

```
[
{
  "configurationVersion": {
    "LastUpdateTime": "

    ",
    "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",
```

```

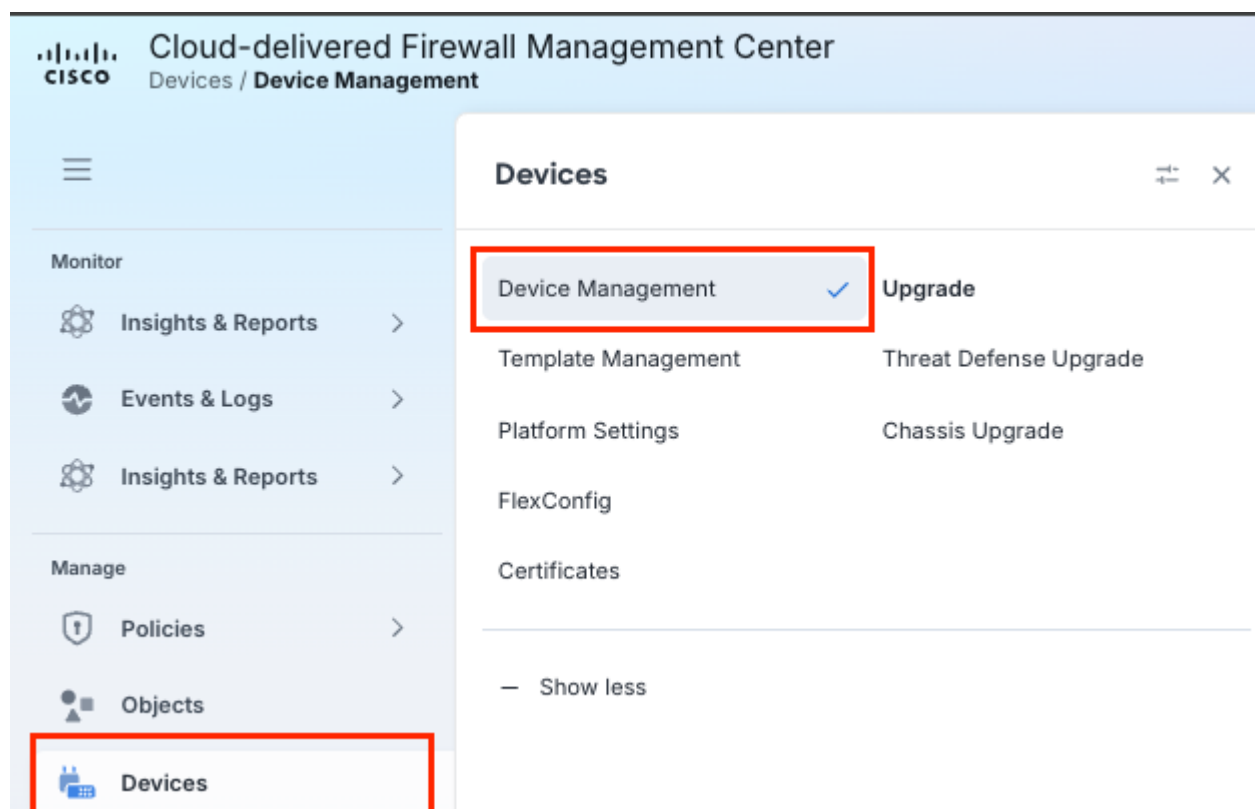
    "SADataSizeInKilobytes": 0,
    "SALifeTimeInSeconds": 27000
  }
}
]
}
]
]

```

ステップ2：ループバックの設定

後で設定する各VTIには安定したトンネルソースが必要であるため、ループバックインターフェイスが最初に設定され、両方のVTI間で共有されます。

a) Devices > Device Managementの順に移動します。

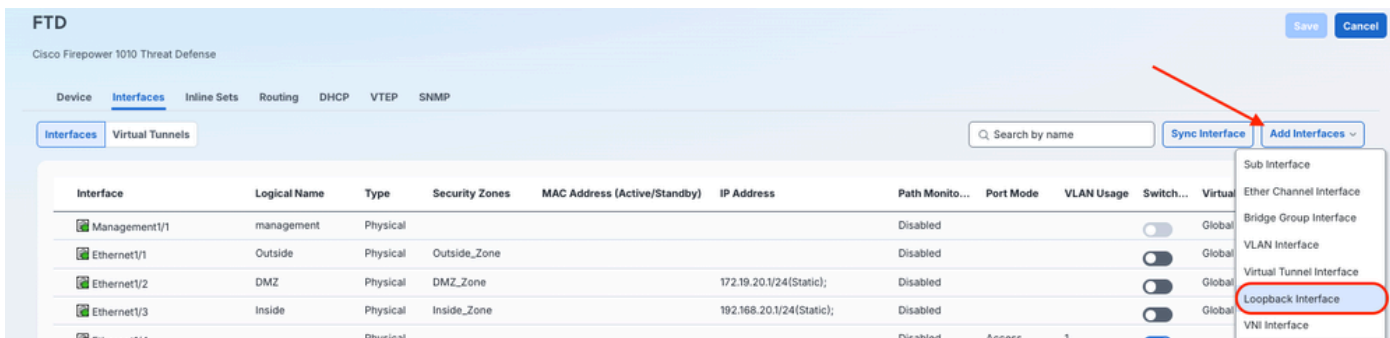


注：この実習では、クラウドで提供されるFirewall Management Center(cdFMC)を使用します。ただし、オンプレミスのFMCでも手順は同じです。

b) ブランチ/サイトのVPNデバイスとして設定するFTDを選択します。



c) Add Interfaces ドロップダウンメニューをクリックして、Loopback Interface をクリックする。



d) 必要に応じて、ループバックインターフェイスに名前、ループバックID、および説明を指定します。IPv4 をクリックします。

A screenshot of the 'Add Loopback Interface' form. The 'General' tab is selected, and the 'IPv4' sub-tab is highlighted with a red circle. The 'Name' field contains 'bgpVPNBranchLo'. The 'Enabled' checkbox is checked. The 'Loopback ID' field contains '1', with a red arrow pointing to it. Below the 'Loopback ID' field, the range '(1-1024)' is indicated. The 'Description' field contains 'Branch Loopback for BGP neighboring and VPN termination from Azure'. At the bottom, there are 'Cancel' and 'OK' buttons.

e) IP Type が Use Static IP として定義されていることを確認し、フェーズ2手順1dで設定したLink BGP Addressを入力します。vpnSiteConfiguration.BgpSetting.BgpPeeringAddress の下のダウンロードされたVPN設定JSONで事前に定義された値を参照できます。



注:/32マスクを使用して、RFC 1918アドレススペース内でアドレスを定義します。

Add Loopback Interface

General **IPv4** IPv6

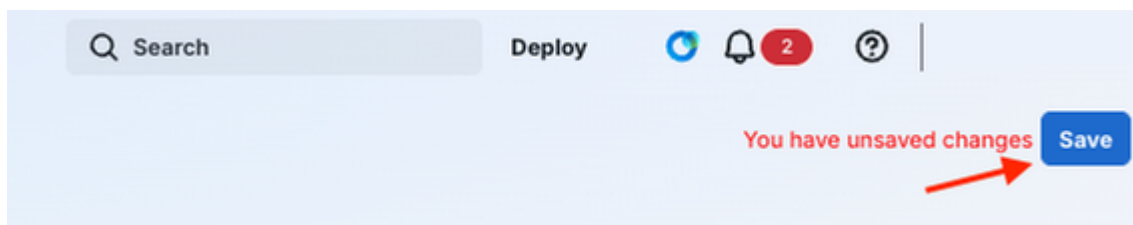
IP Type:
Use Static IP

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) Saveをクリックします。



ステップ3：フェーズ1/フェーズ2ポリシーオブジェクトの設定

a) FTD VPNトポロジに適用する、FMCでの一致するIKEv2/IPsec設定を設定するには、Manage > Objectsの順に移動し、左側のメニューを下にスクロールしてVPNを表示し、サブメニューを展開します。メニューでIKEv2 Policyを選択し、Add IKEv2 Policyをクリックして、IKEv2 Phase 1 Policyを設定します。

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	<input type="edit"/> <input type="delete"/>
AES-GCM-NUL-SHA-LATEST	<input type="edit"/> <input type="delete"/>
AES-SHA-SHA	<input type="edit"/> <input type="delete"/>
AES-SHA-SHA-LATEST	<input type="edit"/> <input type="delete"/>
DES-SHA-SHA	<input type="edit"/> <input type="delete"/>
DES-SHA-SHA-LATEST	<input type="edit"/> <input type="delete"/>
Umbrella-AES-GCM-256	<input type="edit"/> <input type="delete"/>

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

b)新しいIKEv2ポリシーの名前を入力し、PriorityまたはLifetime (あるいはその両方)を選択します。Integrity、Encryption、PRF、およびDiffie-Hellman(DH)グループに関して、トンネルの両端でポリシーが一致していることを確認します。Azureの構成と一致する調整されたアルゴリズム/グループ要素を選択し、追加をクリックします。



注：これらの正確な値は、ダウンロードしたコンフィギュレーションファイル (vpnSiteConnections[0].connectionConfiguration.IPsecParameters)内で参照できます

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

Selected Algorithms

SHA256 

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

c)設定が完了したら、Saveをクリックします。

Edit IKEv2 Policy



Name:*

Azure_IKEv2

Description:

Priority:*

(1-65535)

5

Lifetime:

seconds (120-2147483647)

3600

Available Groups

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

1

2

5

14

15

16

19

20

...

Add

Selected Groups

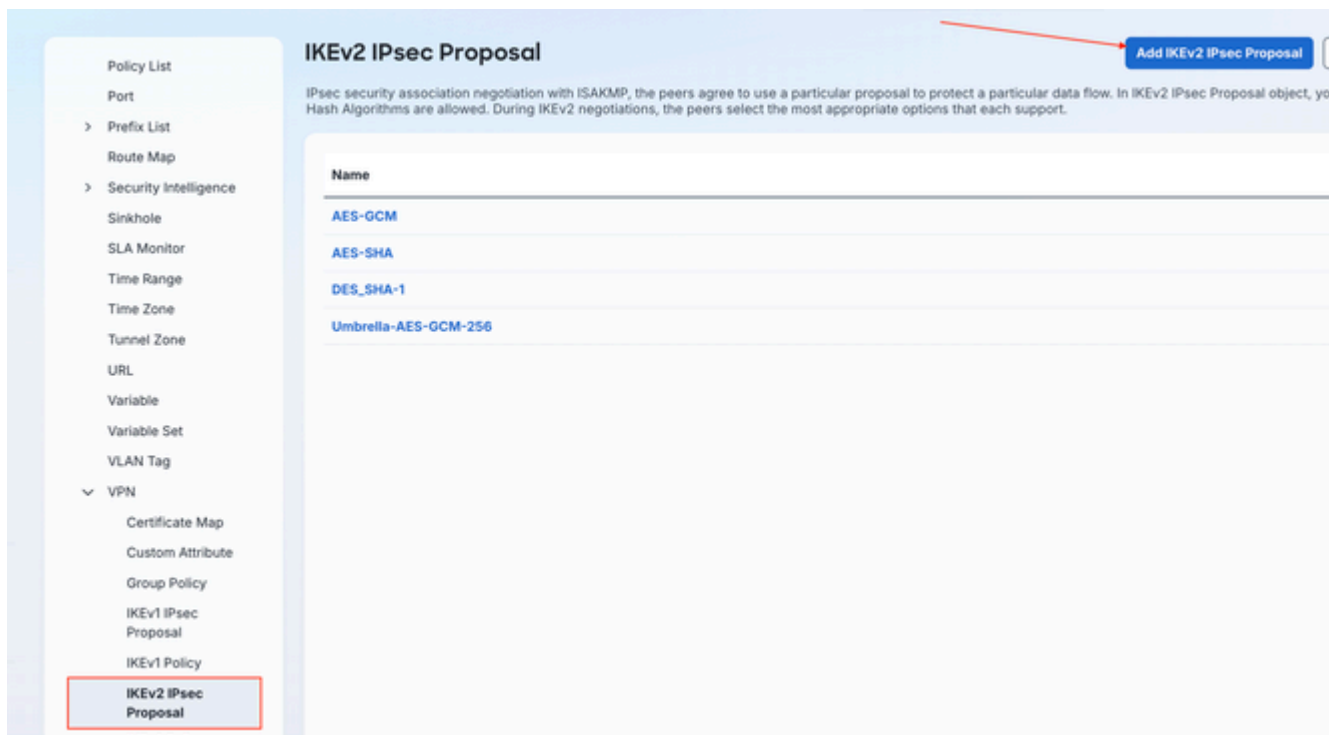
14



Cancel

Save

d) IKEv2 IPsec ProposalサブメニューでPhase 2/IPsecパラメータを設定し、Add IKEv2 IPsec Proposalをクリックします。



e) IKEv2 IPsecプロポーザルに名前を付け、同じ設定が一致していることを確認します。完了したら、Saveをクリックします。



注：これらの値は、ダウンロードしたコンフィギュレーションファイル (vpnSiteConnections[0].connectionConfiguration.IPsecParameters)内で参照できます

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

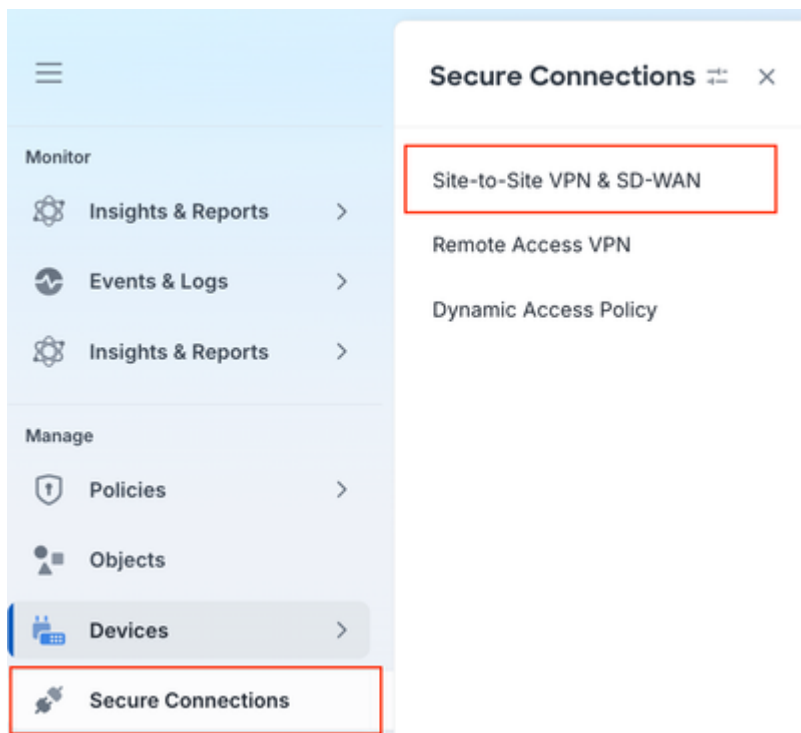


Cancel

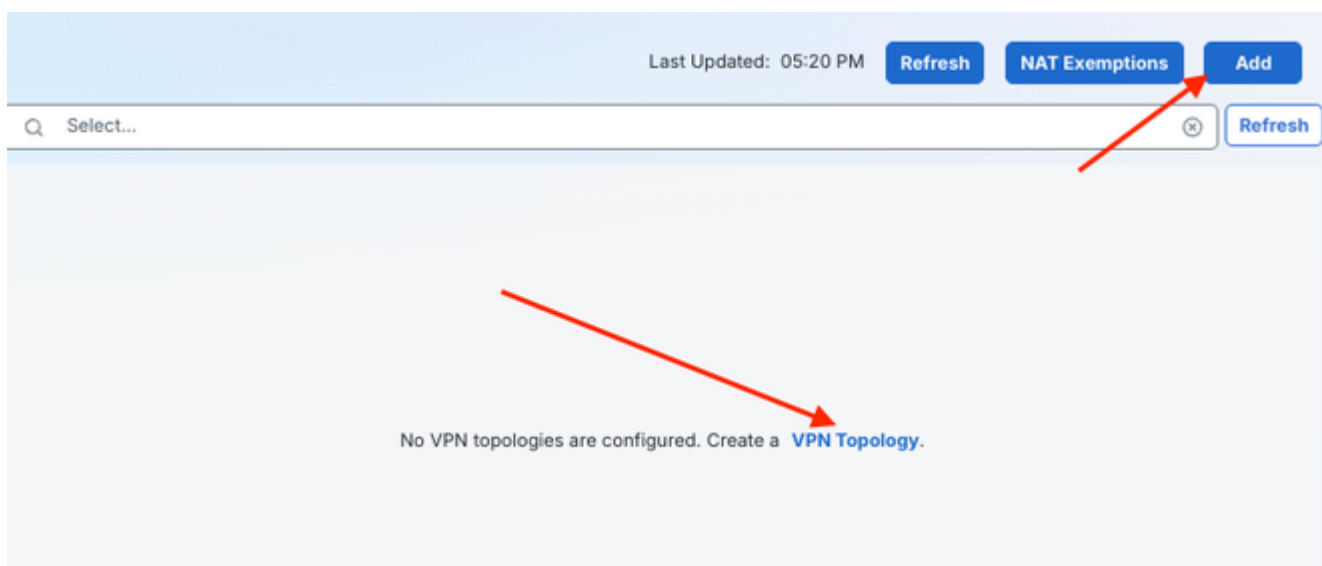
Save

手順4: Azureへのセキュアな接続を構成する

a) Manage > Secure Connections > Site-to-Site VPN & SD-WANの順に移動します。



b)最初のVPN Topology設定ハイパーリンクを中央でクリックするか、Addをクリックします。



c) Azure Instance0への最初のトンネルのトポロジ名を入力し、Route-Based VPNオプションボタンをクリックし、Peer to Peer VPNトポロジタイプをクリックします。完了したら、Createをクリックします。

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) ノードAで、Deviceドロップダウンリストをクリックし、設定が導入される管理対象FTD/FTD HAペアの名前を選択します。ノードBは、Azure vWANインスタンスを終端とするトポロジ内の接続のリモートエンドであるため、デバイスドロップダウンリストからエクストラネットを選択します。次に、ノードAで、仮想トンネルインターフェイス(VTI)ドロップダウンリストの横にある+アイコンをクリックします。

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)最初のVTIにNameを指定し、Enabledであることを確認します。新規または既存のセキュリティゾーンをVTIに割り当て、トンネル送信元を割り当て、隣接するドロップダウンリストからIPアドレスを選択します。

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)次に、Borrow IP (IP unnumbered)オプションボタンが選択されていることを確認し、右側のドロップダウンリストから同じループバックを選択します。完了したら、OKをクリックします。

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

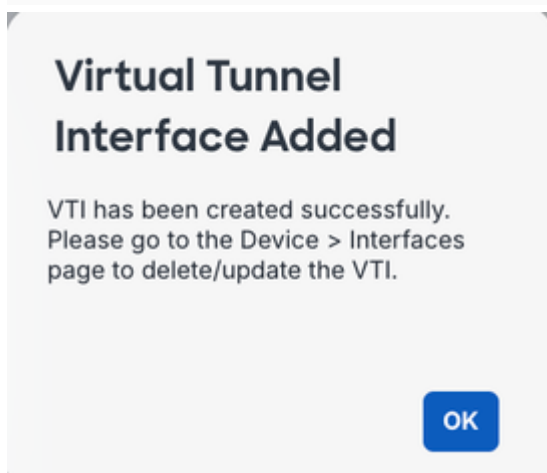
Tunnel ID:*
 (0 - 10413)

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)VTIを設定して適用したら、トンネル送信元IPアドレス（親インターフェイスアドレスがDHCPから設定される場合は自動的に入力されます）を手動で入力し、ノードBのデバイス名、およびインスタンスエンドポイントIPアドレスが設定されていることを確認します。完了したら、IKEタブをクリックします。



注:vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0からダウンロードしたコンフィギュレーションファイルのInstance0エンドポイントのIPアドレスの値を参照できます

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:* ⓘ

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

h) IKEv2 Settingsまでスクロールダウンして、Authentication TypeがPre-shared Manual Keyに設定されていることを確認し、前の手順でAzureに設定したPSKを入力します。鉛筆アイコンをクリックして、使用可能なIKEv2ポリシーを編集し、IKEv2フェーズ1 ポリシーを設定します。



注：事前共有キーは、ダウンロードしたコンフィギュレーションファイル (vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK)で参照できます。

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

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

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) ステップ3で最初に設定したIKEv2フェーズ1ポリシーを追加します。

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) IPsecタブを選択します。

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) トランスフォームセットの下のIKEv2 IPsecプロポーザルを、鉛筆アイコンをクリックして編集します。

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

1)ごみ箱のアイコンをクリックしてデフォルトのAES-GCMトランスフォームセットを削除し、手順3の後半で作成したカスタムAzure_IPsecトランスフォームセット/IKEv2 IPsecプロポーザルを追加します。[OK] をクリックします。

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)スクロールダウンして、Azureパラメータに一致するライフタイム期間に27000と入力します。必要に応じて、PFSグループを有効にします。[Save] をクリックします。



注：ダウンロードされたコンフィギュレーションファイルのlifetime値は、`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`で参照できます。

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)変更を展開します。

Search Deploy

Search Device Advanced Deploy **Deploy All**

☐ FTD

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

o)導入が終了したら、Tunnel Status Distributionの下Manage > Secure Connections > Site-to-Site VPN & SD-WANの順にチェックします。接続が成功すると、Green (Up)と表示されます。

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

最初に導入したトンネルで、IKE/IPsecとBGPの両方のレイヤでトンネルが正常に確立されたことを確認してから、2番目のトンネルに冗長性を設定します。

手順5: Azureへの初期接続を確認します

a) FTDにSSHで接続し、`system support diagnostic-cli`と入力します。次に、`en`と入力し、Enterキーを押します。これは、読み取り専用のFTD CLIにパスワードがないためです。

```
<#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) フェーズ1/フェーズ2のトンネルステータスをチェックします。

```
<#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) トンネル内のAzureから受信したBGP Transmission Control Protocol(TCP)パケットと、Instance-0 AzureトンネルのパブリックIPから外部キャプチャした、ネットワークアドレス変換 – トラバーサル(NAT-T)ユーザデータグラムプロトコル(UDP)ポート4500/UDPポート500トラフィックを確認するためにキャプチャを実行します。

<#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#

Instance0への接続が確認されたら、Instance1に対して同じVTIおよびVPNトポロジ構成を繰り返し、両方のAzureゲートウェイインスタンスに到達できるようにします。

手順6: Azure Instance1エンドポイントへの2番目のトンネルを構成します

a)同じループバックから2番目のVTI(Azure-VTI-1)を作成します (ステップ3 b-f)。

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

Tunnel ID:*
2 (0 - 10413)

Tunnel Source:*
Ethernet1/1 (Outside) Dynamic

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

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☐ Configure IP
☒ Borrow IP (IP unnumbered) Loopback1 (bgpVPNBranchLo) +

VPN Topology Usage
Azure-VTI-Instance1 (Tunnel Destination IP -

b)第2インスタンスのVPNトポロジを設定する (ステップ4g-n)。



注:vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1にダウンロードしたコンフィギュレーションファイルのInstance1エンドポイントのIPアドレス値を参照できます。

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

Node B

Device:*

Device Name*:

Endpoint IP Address*:

+ Add Backup VTI (optional)

Additional

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

c) 設定変更を導入し、トンネルステータスを確認します。

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) Azureをチェックインすると、Instance0とInstance1の両方がConnectedになります。

Links

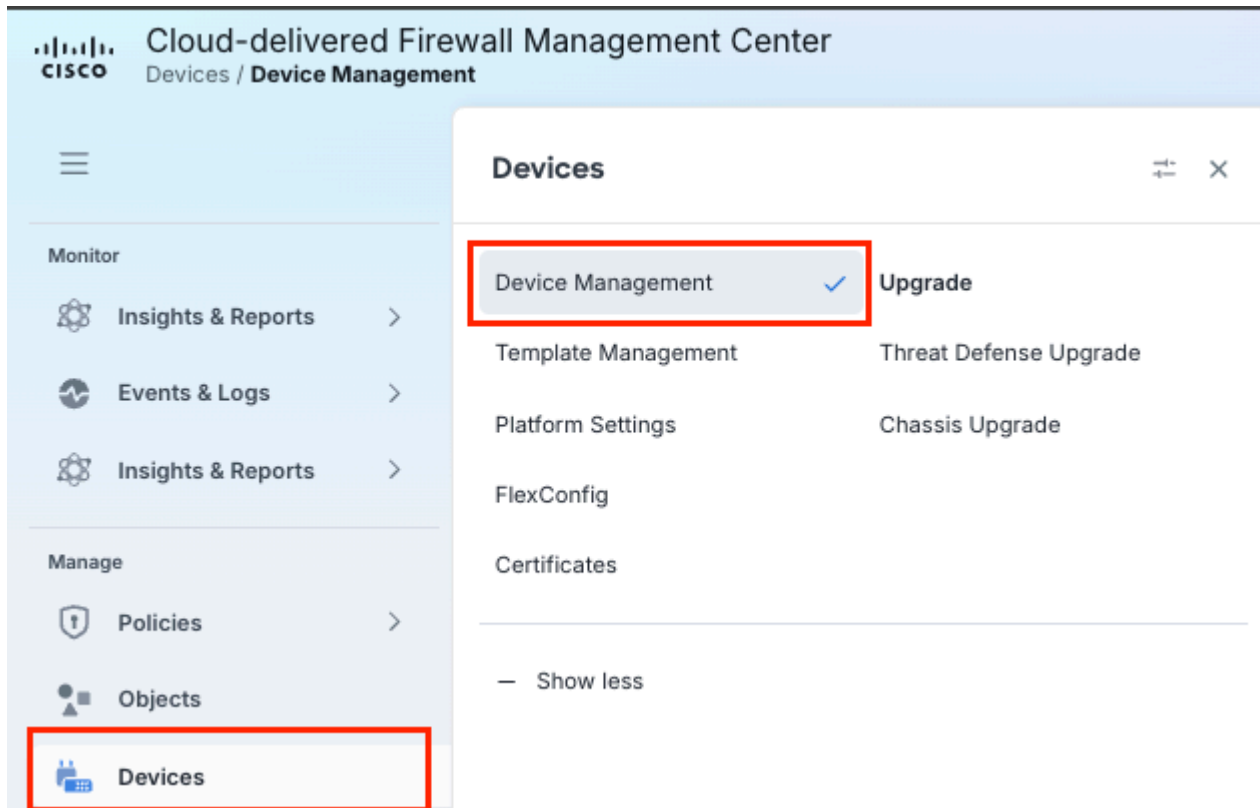
☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

両方のトンネルがアクティブな状態で、トラフィックが両方のパスを同時に使用できるように、FTDは2番目のトンネルをパッシブスタンバイとして扱うのではなく、ECMPルーティングを必要

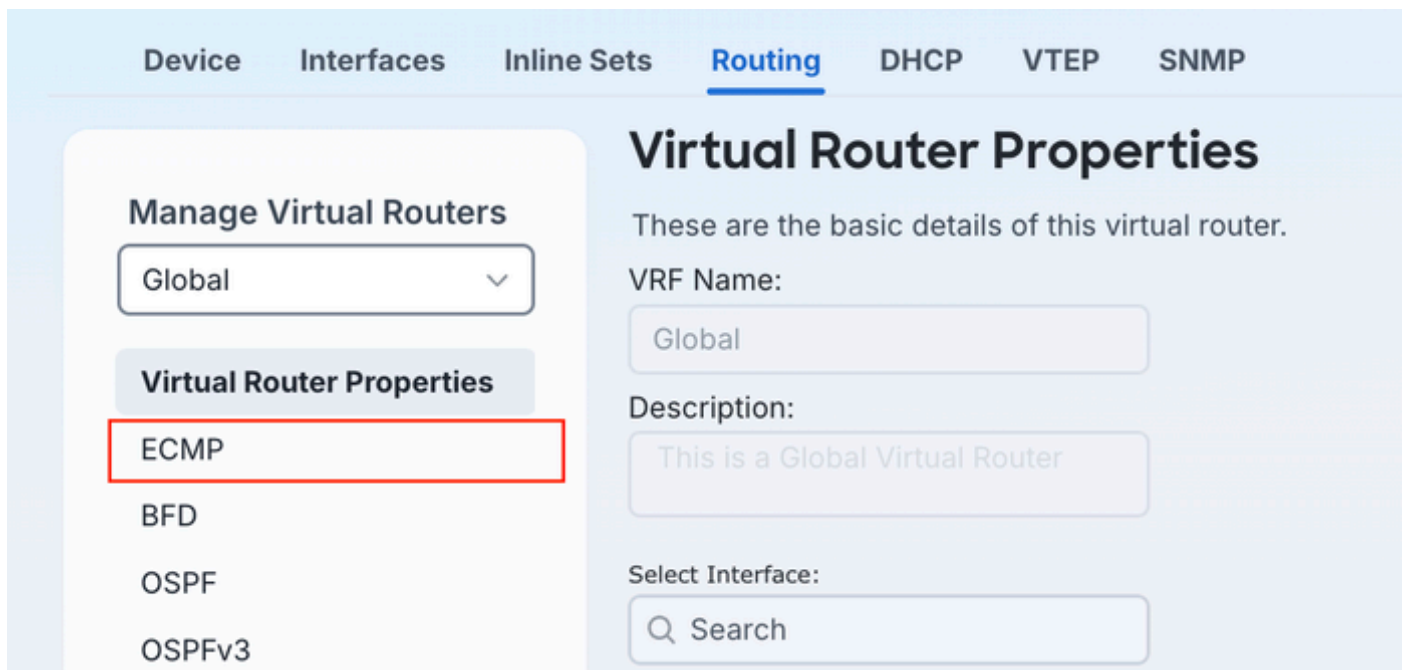
とします。

ステップ7:ECMPの設定

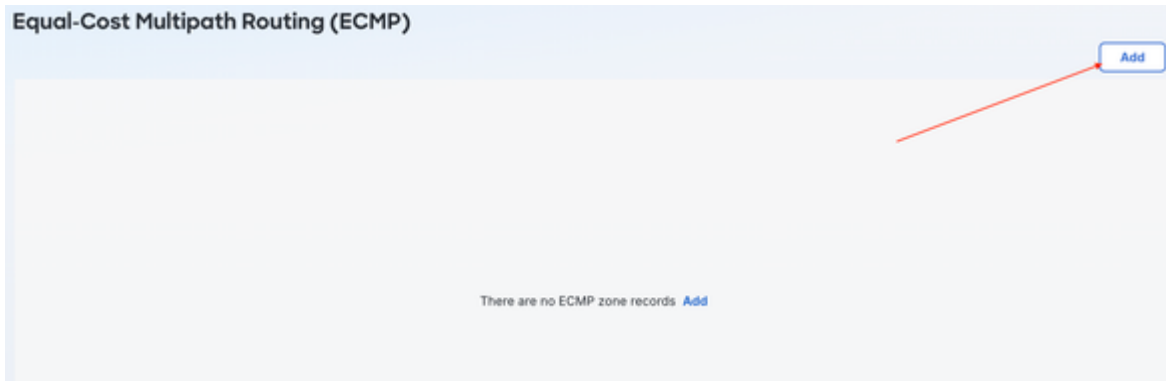
a) Manage > Devices > Device Managementの順に移動し、AzureへのVPNが設定されているFTDを選択します。



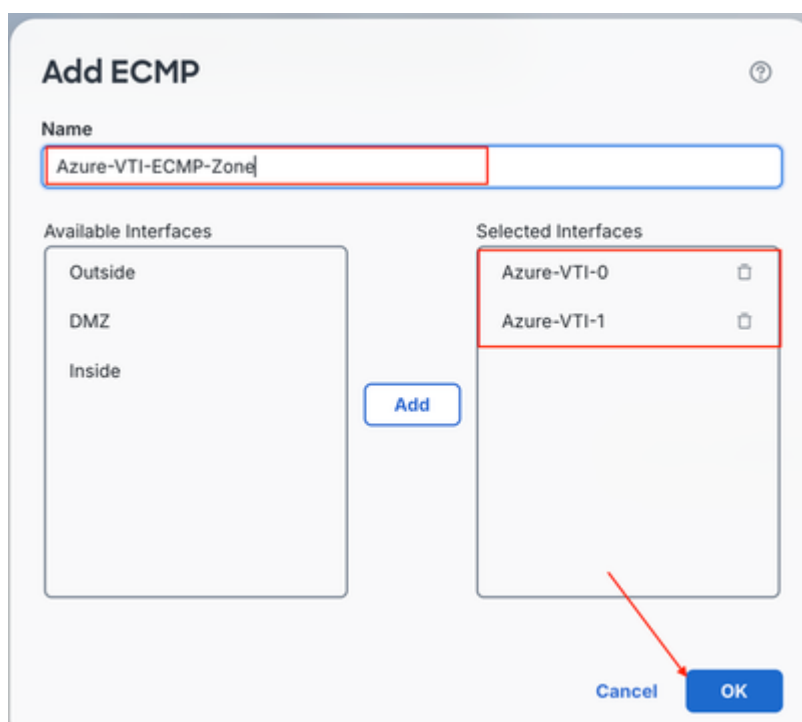
b) Routingタブをクリックして、ECMPを選択します。



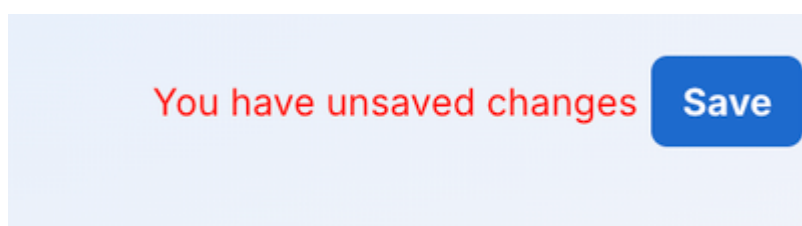
c) Addをクリックして、新しいECMPゾーンを作成します。



d) Available Interfacesパネルで両方のVTIをクリックしてVTIを強調表示に切り替え、Addをクリックして、名前付きECMPゾーンにVTIを適用します。



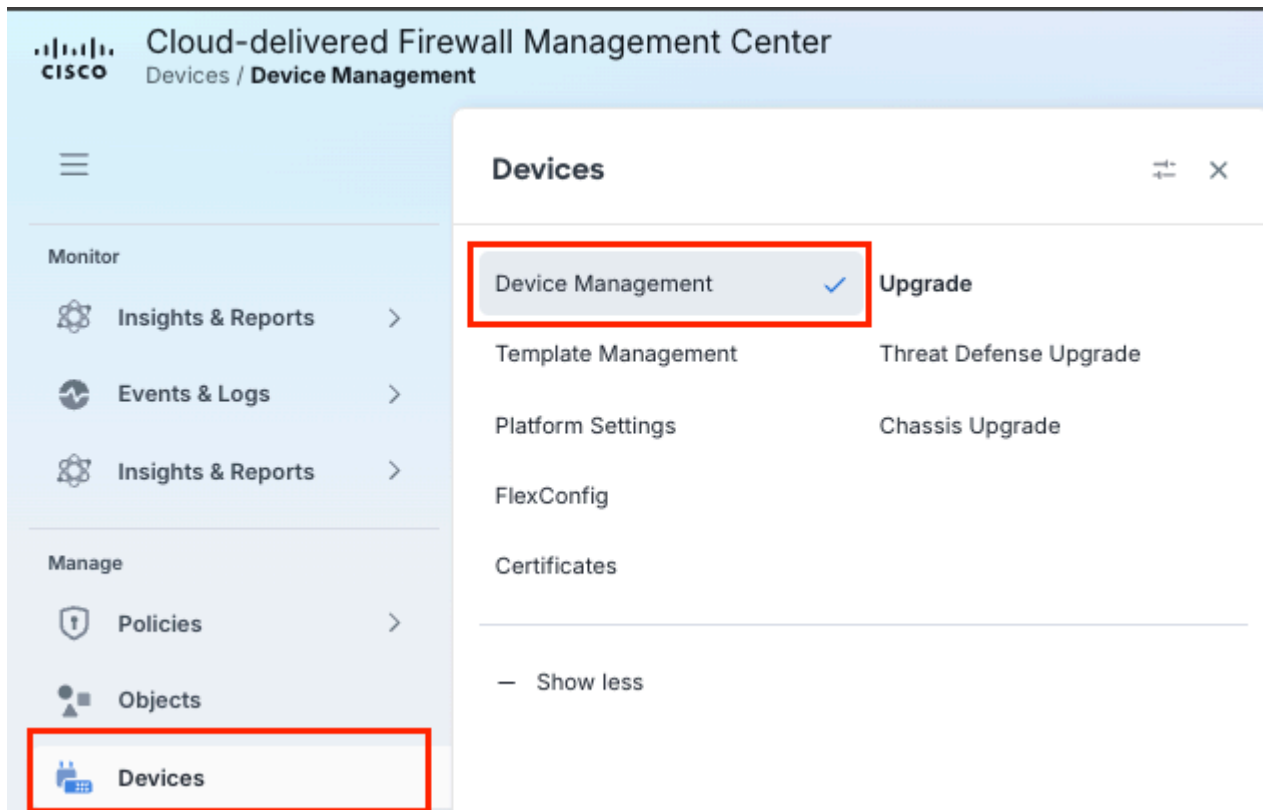
e)設定が正しいことを確認したら、Saveをクリックします。



ステップ8：プライベートIPをインスタンス化するためのスタティックルートを設定する

BGPでは、ネイバーに正常に接続するためにルートが必要です。エンドポイントは直接接続されていないため、デフォルトではルートは設定されません。ECMPでは、同じ宛先に対して同じメトリック（アドミニストレーティブディスタンス）のスタティックルートを設定できるため、両方のルートがルーティング情報ベース(RIB)にインストールされて同時に使用されます。

a) Manage > Devices > Device Managementの順に移動し、該当するFTDデバイスを選択します。



b) Routing > Static Routeの順に選択します。

FTD

Cisco Firepower 1010 Threat Defense

Monitor

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

Manage

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

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

Manage Virtual Routers

Global

Virtual Router Properties

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

Network ▲ Inte

IPv4 Routes

IPv6 Routes

c) + Add Routeをクリックします。

+ Add Route

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

d) Instance0 VTIへの最初のルートを作成して両方のインスタンスIPアドレスのルートを追加し、Available Networkの横の+をクリックして、それに対する宛先ネットワークオブジェクトを追加します。次に、リストからネットワークオブジェクトをクリックし、Addボタンをクリックしてスタティックルートの宛先として追加します。Instance0 IPを選択し、それがゲートウェイとして設定されていることを確認します。完了したら、OKをクリックします。



注：これらのスタティックルートの宛先ネットワーク値は、ダウンロードした設定ファイルの `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` および

vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1にあります。

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*: Azure-VTI-0

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

Available Network: Azure-Instance0-BGP_Peer, Azure-Instance1-BGP_Peer

Selected Network: Azure-Instance0-BGP_Peer

Gateway: Azure-Instance0-BGP_Peer

Metric: 1

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e)手順c ~ dを繰り返して、Instance1 VTI経由の2番目のスタティックルートを追加します。Saveをクリックして変更を保存したことを確認します。

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						

スタティックルートはBGPピアリングアドレスにのみ到達します。AzureとFTDが相互により大きなネットワークとの間でルートを動的に交換できるように、BGP自体を引き続き有効にしてピア接続する必要があります。

ステップ9:BGPの設定

a) FTDでRouting > General Settings > BGPの順に選択し、BGP Process 65500を有効にします。Enable BGPチェックボックスをオンにして、フェーズ2手順1で設定したAS番号を入力します。Routing > BGP > IPv4の順に選択します。

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)隣接するEnable IPv4チェックボックスをオンにしてプロセス/AS 65500のIPv4 BGPルーティングを有効にし、NeighborをクリックしてBGPネイバーを設定します。

FTD

Cisco Firepower 1010 Threat Defense

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

Enable IPv4: ☒ AS Number 65500

General

Neighbor

Add Aggregate Address

Filtering

Networks

Redis

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

Setting

Learned Route Map

c) + Addをクリックします。

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) Instance0 BGPピアリング情報を入力し、表示されたvWANハブからのBGP ASを参照し、それをネイバーリモートASとして入力し、必要に応じて説明を追加します。[Advanced] をクリックします。



重要:FTDの両方のVTIインターフェイスのループバックペアレントを参照するように、BGP Update Sourceを必ず変更してください。

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) FTDのBGP Neighbor設定にあるAdvancedメニューで、TTLホップの数をeBGPデフォルトの1ホップから可変数に変更できます。Azure BGPエンドポイントは、トンネル経由でAzureインフラストラクチャに直接接続されておらず、エンドポイントへのホップ数はデフォルトのeBGP TTLの1許可を超える傾向があります。

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Azure Instance1 BGPピアに対して同じ手順を繰り返します。

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

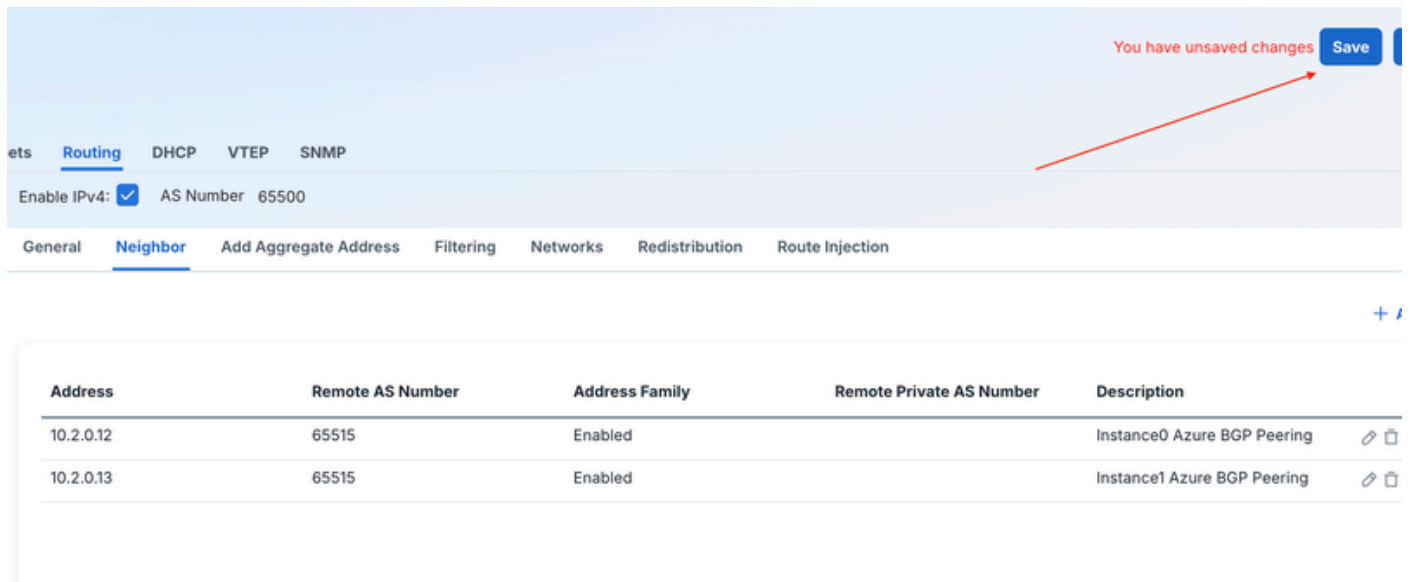
☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

g)完了したら、必ず変更を保存してください。



デフォルトでは、ECMPによって両方のスタティックルートが使用可能になっていても、BGPはルーティングテーブルにベストパスを1つだけインストールします。両方の学習パスがインストールされ、同時に使用されるように、BGPマルチパスは個別に有効にする必要があります。

ステップ10:BGPマルチパスの設定

a) Routing > BGP > IPv4の順に移動し、Generalタブをクリックして、Forward Packets Over Multiple Pathsの横にある鉛筆アイコンをクリックします。

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) Number of Pathsフィールドのデフォルト値を1から2に変更します。

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c)変更を保存して展開したことを確認します。

確認

デプロイが完了したら、BGPが両方のAzureインスタンスとアジャセンシー関係を形成することを確認します。その後、ルートが両方のトンネルを介して学習され、トラフィックがフェーズ3の手順5で確立された同じ診断CLIアクセスを使用して両方のVTIを使用することを確認します。

ftd CLIで、system support diagnostic-cliに移動します。

a)展開すると、BGPネイバーが起動し、プレフィックスが受信されることが想定されます。

<#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) Azureから受信したルートがマルチパスルートとして表示されることを確認します。

<#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) VTIパケットカウントをチェックします。

<#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) BGPネイバーシップのスタティックルートを確認します。

<#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) ECMPゾーンを確認します。

<#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) BGPの設定を確認します。

<#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)ルーティングテーブルを確認します。

<#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
```

それ以外に考慮すること

このドキュメントの基本設定では、ブランチFTDで単一の外部インターフェイスと単一のISPが想定されています。これらの考慮事項により、その設計が拡張されます。

AS-Pathプリペンド

ECMPおよびBGPマルチパスによって負荷を均等に共有するのではなく、2つのトンネルのどちらがAzureまたはFTDでプライマリとして優先されるかを変更する必要がある場合は、セカンダリとして扱われるBGPネイバーでローカルAS番号を1回以上プリペンドします。先頭に付加された長いASパスを持つネイバーは、標準BGPベストパス選択中に優先が付けられ、そのネイバーをECMPゾーンから完全に削除する必要はありません。

トラブルシューティング

- フェーズ1/フェーズ2トンネルが起動しない：事前共有キーとIKEv2/IPsecポリシーパラメーター（暗号化、整合性、PRF、DHグループ、およびライフタイム）が、FMC IKEv2ポリシー/IPsecプロポーザルとダウンロードされたAzure VPN構成ファイルの値の間で正確に一致していることを確認します。フェーズ3のステップ5に示されているように、`show crypto isakmp sa`および`show crypto ipsec sa`を使用します。
- トンネルはアップ状態ですが、BGPネイバーは`update-source`を形成しません。BGPがVTI自体ではなくループバックインターフェイスに設定されていること、および`ebgp-multihop`がFTDに直接接続されていないAzure BGPピアリングアドレスに到達するのに十分な高さの値で設定されていることを確認します。
- BGPが形成されるが、トラフィックを伝送するのは1つのトンネルのみ：両方のVTIが同じECMPゾーンのメンバーであること、両方のAzureインスタンスのBGPアドレスへのステイックルルートが同じアドミニストレーティブディスタンスでインストールされていること、およびBGPマルチパスが2つのパスに対して設定されていることを確認します（フェーズ3の手順10を参照）。
- リターントラフィックなし、またはAzureへの非対称ルーティング：Azure vWANが両方のトンネルでハブアドレス空間をアドバタイズするため、ルーティング構成の他の部分でECMPが無効になっていないことを確認し、単一のパスにトラフィックを固定する可能性があるルートマップまたはポリシーベースルーティングを確認してください。
- BGPはアップ状態で、ルートはインストールされていますが、トラフィックはブロックされているようです。トラフィックの入出力を許可するセキュリティゾーンがVTIに割り当てられたアクセスコントロールルールを設定していることを確認してください。

関連情報

- [Azure Virtual WANとは](#)
- [Azure VPN GatewayのBGPの設定方法](#)
- [既定のIPsecポリシーとカスタムのIPsecポリシーの比較Azure vWAN](#)

- [Azure VPN GatewayのBGP問題のトラブルシューティング](#)
- [アクティブ – アクティブモードのVPNゲートウェイについて](#)
- [チュートリアル： Azure Virtual WANを使用してサイト間接続を作成する](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせ、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。