

セキュアファイアウォールでのAzure Dual ISP vWAN接続の構成

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](#)

[デュアルダイレクトインターネットアクセス\(DIA\)リンク \(Azure + FTDロードバランシング/冗長性 \)](#)

[設定](#)

[フェーズ1: 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 APIPAゲートウェイパラメーターを構成する](#)

[手順3: Azure vWANサイトのVPNパラメーターを構成します](#)

[ステップ4:VPNサイトリンクインスタンスでカスタムBGP APIPAを有効にしてアクティブにする](#)

[ステップ5:VPNサイト設定ファイルのダウンロード](#)

[フェーズ2: Azure vWANへのデュアルISP接続のためのFTDの構成](#)

[ステップ1: ダウンロードしたVPN設定の分析](#)

[ステップ2: リンクBGPアップデートソースループバックインターフェイスの設定](#)

[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](#)

[ステップ4: 仮想トンネルインターフェイス\(VTI\)の設定](#)

[ステップ5:IPsec VPNトポロジのプロビジョニング](#)

[手順6:VPNトポロジを検証する](#)

[ステップ7:ECMPの設定](#)

[ステップ8:BGPの設定](#)

[ステップ9:eBGPマルチパスの設定](#)

[確認/トラブルシューティング](#)

概要

このドキュメントでは、デュアルWANリンクを使用してファイアウォールを保護するようにMicrosoft Azure Virtual WAN(vWAN)サイト間VPN接続を構成する方法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 Virtual WAN (vWAN)
- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)

両方のコンポーネントがAzure環境で最初に構成されていることを確認してください：

- Microsoft Azure vWANインスタンス
- Microsoft Azure vWANハブ

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
- Microsoft Azure vWAN

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

ブランチFTDにインターネットサービスプロバイダー(ISP)向けの外部インターフェイスが2つある場合、それぞれがAzure vWANに冗長的かつアクティブに接続できるため、各ISPリンクが利用されます。Azure vWANでは、サイトリンクごとに2つのIPsecトンネル（1つはAzure Hub Instance0に、1つはInstance1に）が作成されるため、各ISPインターフェイスは2つのトンネルを終端します。この結果、両方のISPリンクにわたって、4つのIPsecトンネルがFTDで終端することになります。

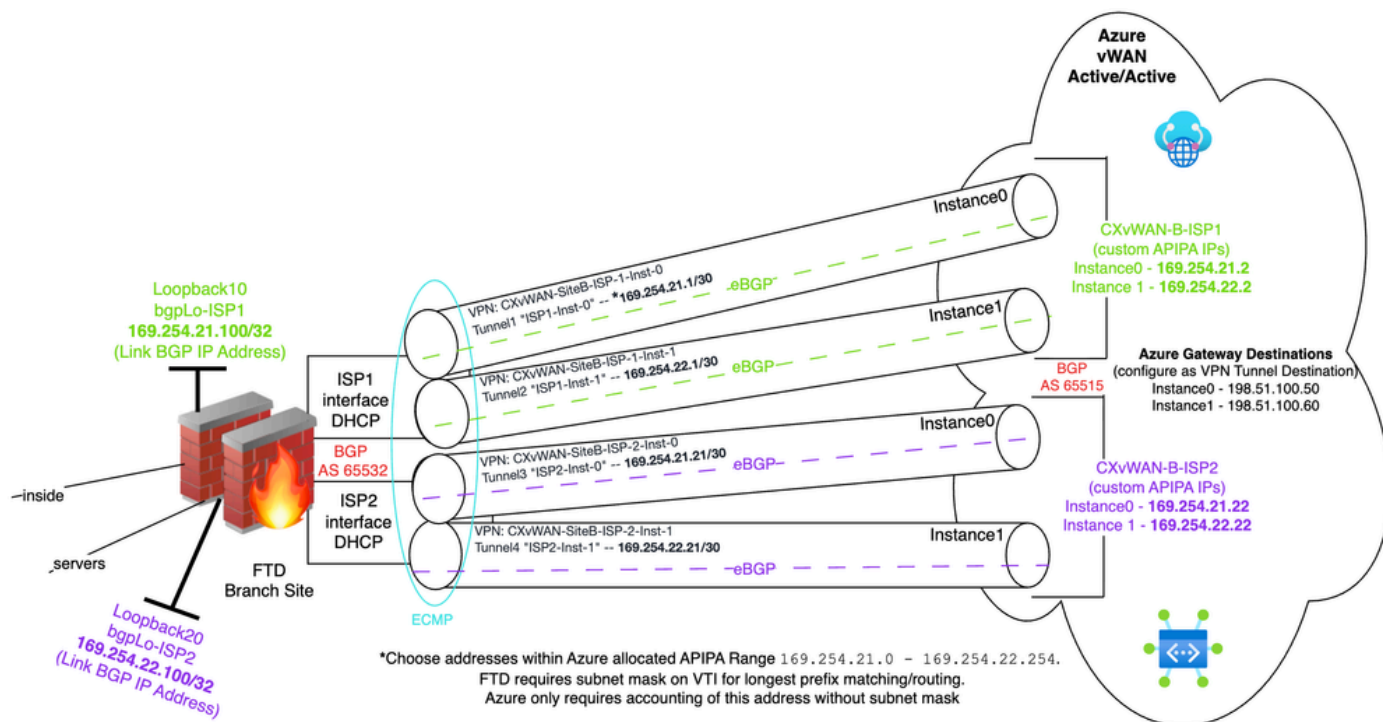
Azureインスタンスは負荷分散と冗長性のためにアクティブ/アクティブモードで動作するため、FTDは4つのIPSecトンネルすべてで等コストマルチパス(ECMP)構成を使用してこれを反映しま

す。カスタムの自動プライベートIPアドレッシング(APIPA)アドレスを使用して、4つのトンネルそれぞれで、個別のプライベート自律システム番号(ASN)を持つ外部ボーダーゲートウェイプロトコル(eBGP)ネイバーシップが確立されます。これにより、BGPマルチパス機能が有効になり、インスタンスの各Azure Hub Site Linkペアに複数の冗長パスが提供されます。



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。デュアルダイレクトインターネットアクセス(DIA)リンクバリエーションは、FTDの2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。

デュアルダイレクトインターネットアクセス(DIA)リンク (Azure + FTDロードバランシング/冗長性)



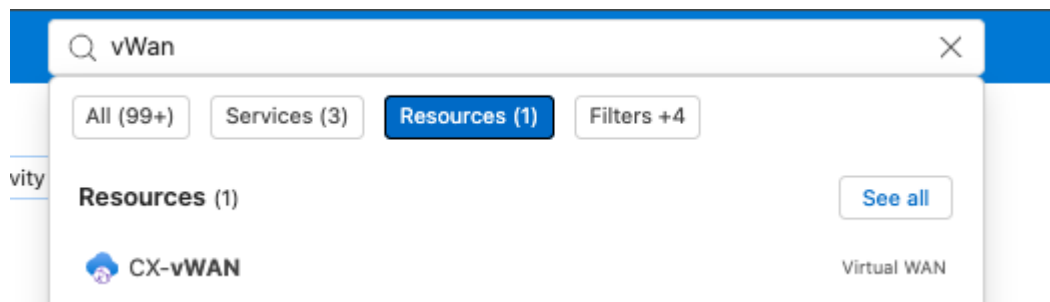
デュアルダイレクトインターネットアクセス接続のトポロジ

設定

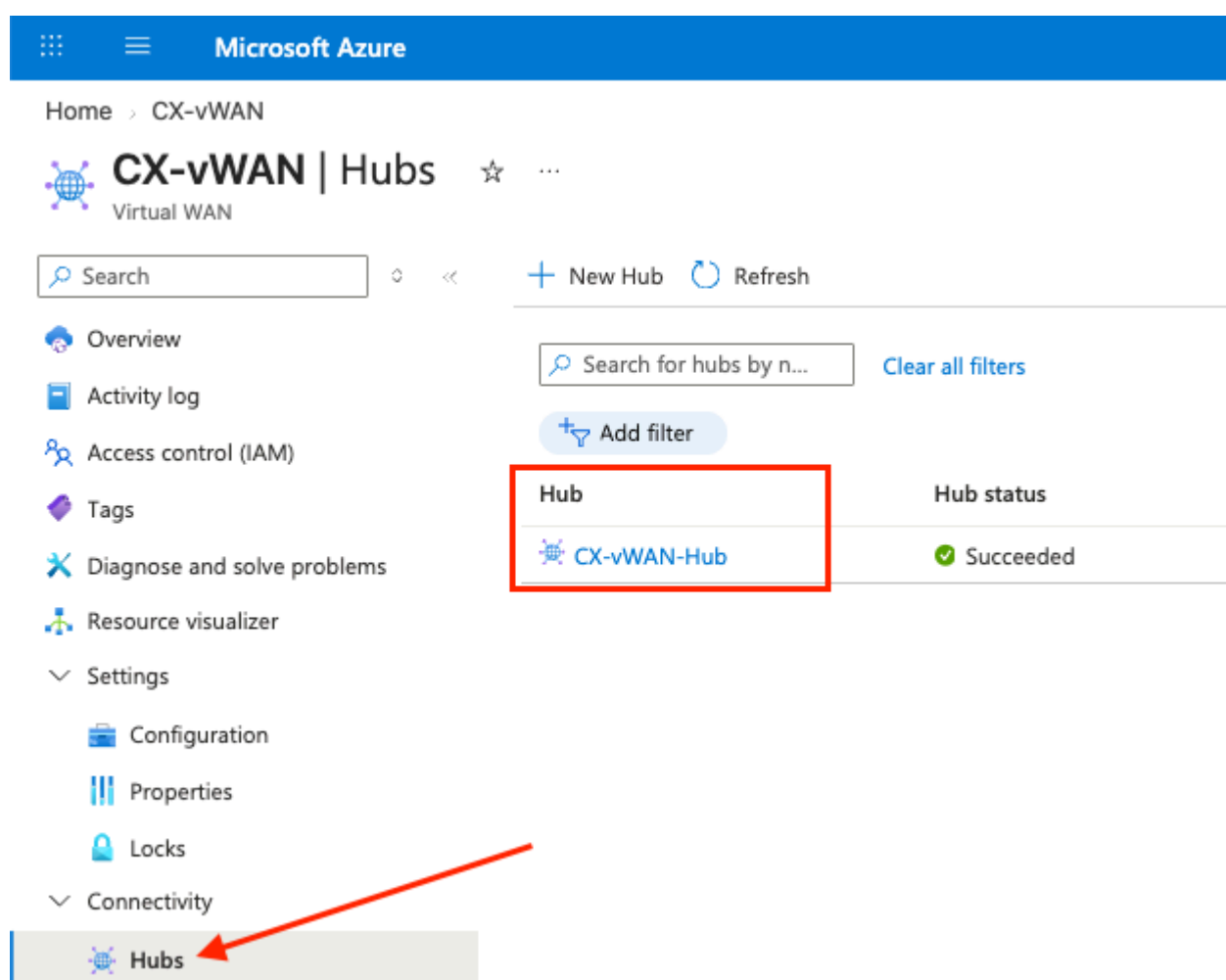
フェーズ1: Azure vWAN VPNサイトの構成

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

1) Azureの検索フィールドでvWANを検索し、Virtual WANsをクリックして既存のAzure vWAN Hubに入力します。次に、Connectivity > Hubsに移動し、既存のAzure vWAN Hubをクリックします。



仮想WANの検索クエリ



既存の仮想WANハブの選択

2) 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		

新しい仮想WANサイトの作成



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。

3) 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 *	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 >

一般的なVPNサイトの構成設定

4)必要なリンク情報を入力します。リンクBGPアドレスとリンクASNは、内部トンネルBGPレイヤ3宛先アドレスと、サイト間トンネルを介してネイバーシップが形成されるブランチ側のBGP AS番号です。リンクBGPアドレスは、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側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。2つのループバックインターフェイスは、各デュアルサイトリンクのリンクBGPアドレスを表すために、FTDの後のセクションで作成されます。リンクIPアドレス/完全修飾ドメイン名(FQDN)は、IPセキュリティ(IPsec)/インターネットキーエクスチェンジバージョン2(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。終了したら、Next : Review + create >をクリックして次のステップに進みます。



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、特定のAzureドキュメントを確認してください：[BGP APIPAアドレスを選択します。](#)

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 >

サイトリンクパラメーターの構成

5)情報が意図したとおりに確認されたら、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	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

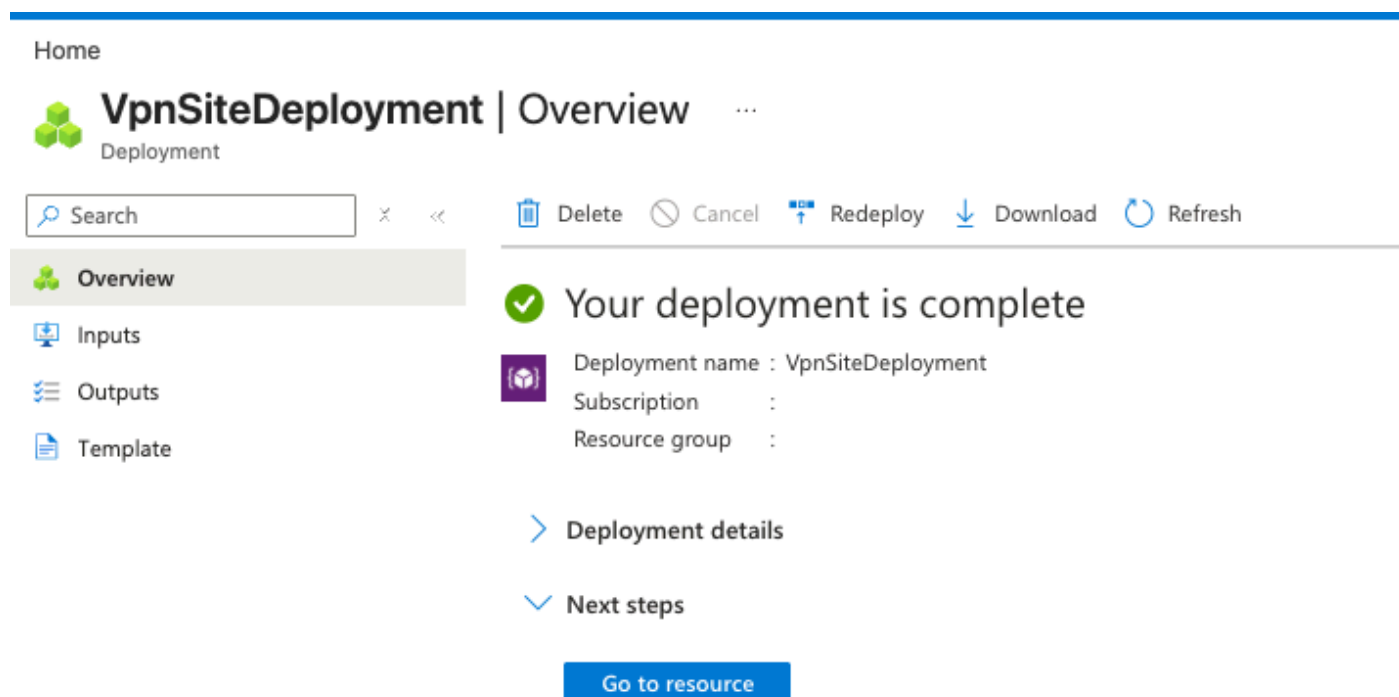
 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Create

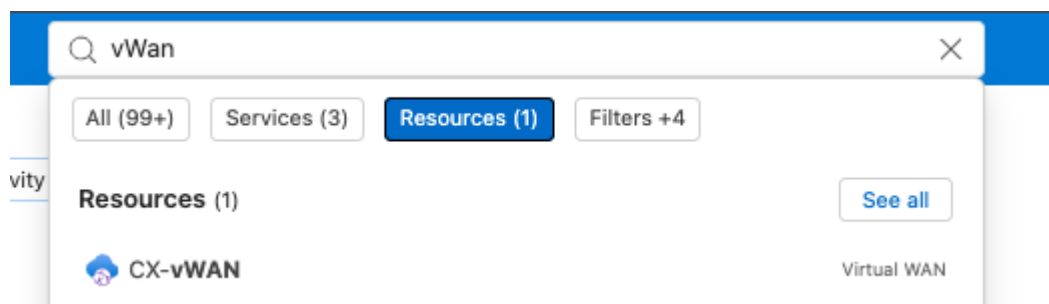
Previous

Next

6) VPNサイトの導入が完了したら、vWANハブ設定に戻ります。



仮想WANサイトの展開の進行状況



仮想WANの検索クエリ

手順2: Azure APIPAゲートウェイパラメーターを構成する

Azureでは、169.254.0.0/16 IPv4アドレス空間内の自動プライベートIPアドレス(APIPA)アドレスの追加構成が必要です。

1) Connectivity > Hubsを使用して、既存のハブを入力します。

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

仮想WAN/ハブ接続に移動します

2)もう一度Connectivity > VPN (Site to site) に移動し、Gateway Configurationハイパーリンクをクリックします。

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/ハイパーリンク

3)側面パネルが表示されますVPNゲートウェイを編集します。VPN Gateway Instance0とVPN Gateway Instance1の下で、IPsecトンネル経由のBGPネイバーシップの各インスタンスに対してネイバーIPとして機能する2つの一意なカスタムBGP IPアドレスを入力します。これは、このトポロジ内でAPIPAアドレスを使用する場合に必要です。Peer Addressとラベル付けされたフィールドに、FTDからAzureインスタンスに到達するために使用するBGPネイバーIPを入力します。APIPAアドレスが使用されている場合、AzureはFTDとのBGP確立を試行しません。そのため、FTDはAzureとの各トンネルでeBGPネイバー確立を試行します。

合計で、2つのリンクx 2つの暗黙のトンネル、Instance0とInstance1へのISPリンクごとに1つのトンネル、Azureと2つのFTD ISPインターフェイス間のBGPネイバーシップを持つ4つのIPsecトンネルが生成されます。

これらのアドレスは一意である必要があります。このデモンストレーションでは、各トンネルに割り当てられた/30サブネットの2番目と最後のホストアドレスをFTDでできるように設定します。設定が完了したら、Editをクリックします。



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、特定のAzureドキュメントを確認してください：[BGP APIPAアドレスの選択](#)

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

VPNゲートウェイのカスタムBGP IPアドレスの編集



注: Azureのメモと同様に、更新に最大30分以上かかる場合があります。

手順3: Azure vWANサイトのVPNパラメーターを構成します

1) Azure vWAN Hub構成のConnectivity > VPN (Site to site)ページで、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VPNサイトを表示します。

ハブ関連付け接続フィルターのクリア

2)最近プロビジョニングしたVPNサイトの横にあるチェックボックスをオンにして、Connect VPN Siteをクリックします。



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

Virtual HUB

[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](#)

VPNサイト接続アクション

3)必要な事前共有キー(PSK)を設定し、カスタム切り替えオプションをクリックして必要なIPsecパラメータを設定します。これらのIPsecパラメータは、後の手順でFMC/FTD設定と一致している必要があります。保存するには、[接続]をクリックします。



注:Diffie-Hellman(DH)グループ24のサポートは、FTD/FMCバージョン6.7で削除されました。

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

事前共有キーとIPSecパラメータの設定

4) VPNサイトのプロビジョニングが正常に完了したことを確認します。

Notifications



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

[Dismiss all](#)



Successfully created VPN connection



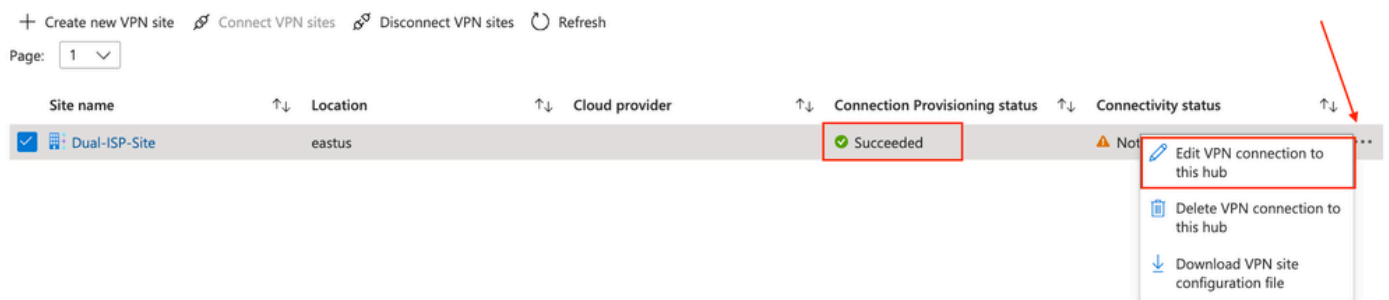
Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

VPNサイトのプロビジョニングステータスの確認

ステップ4:VPNサイトリンクインスタンスでカスタムBGP APIPAを有効にしてアクティブにする

1) VPN (サイト間) ページを更新し、接続プロビジョニングのステータス列に成功と表示されていることを確認します。この列の省略記号をクリックすると、このハブへのVPN接続の編集ドロップダウンメニュー項目をクリックできます。



接続の成功の検証とVPN接続の編集

2) Link Connection 1(ISP1)をクリックして設定し、該当する事前共有キー(PSK)をもう一度入力します。次に、必ずCustom BGP IP Addressの横にあるEnableトグルをクリックして、FTDによって生成されるBGP IPヘッダーの内部トンネル宛先IPアドレスフィールドの値になる/30サブネットの残りのホストアドレスをマップします。

基本的に、ISP1 VTI Tunnel1からAzure Instance0へのアドレス割り当ては169.254.21.1/30であり、FTDで終端する2番目のISP1 VTI Tunnel2にはInstance1に割り当てられたIP 169.254.22.1/30があります。

Next: [Link Connection 2>](#)をクリックして、ISP 2のリンクパラメータに進みます。



注:PSKを再入力し、Azureのドロップダウンメニューで整列されたPFSグループオプションを再クリックする必要がある場合があります。

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)前の手順を繰り返し、リンク接続2 (ISP2リンク) の下で該当するパラメータを適用します。
完了したら、「作成」をクリックします。

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 ⓘ 169.254.21.22 ▾

Instance 1 ⓘ 169.254.22.22 ▾

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 * Integrity/PRF * DH Group *
GCMAES256 ▾ SHA384 ▾ DHGroup14 ▾

IKE Phase 2(ipsec) ⓘ IPsec Encryption * IPsec Integrity * PFS Group *
GCMAES256 ▾ GCMAES256 ▾ NONE ▾

DPD timeout in seconds * ⓘ 45

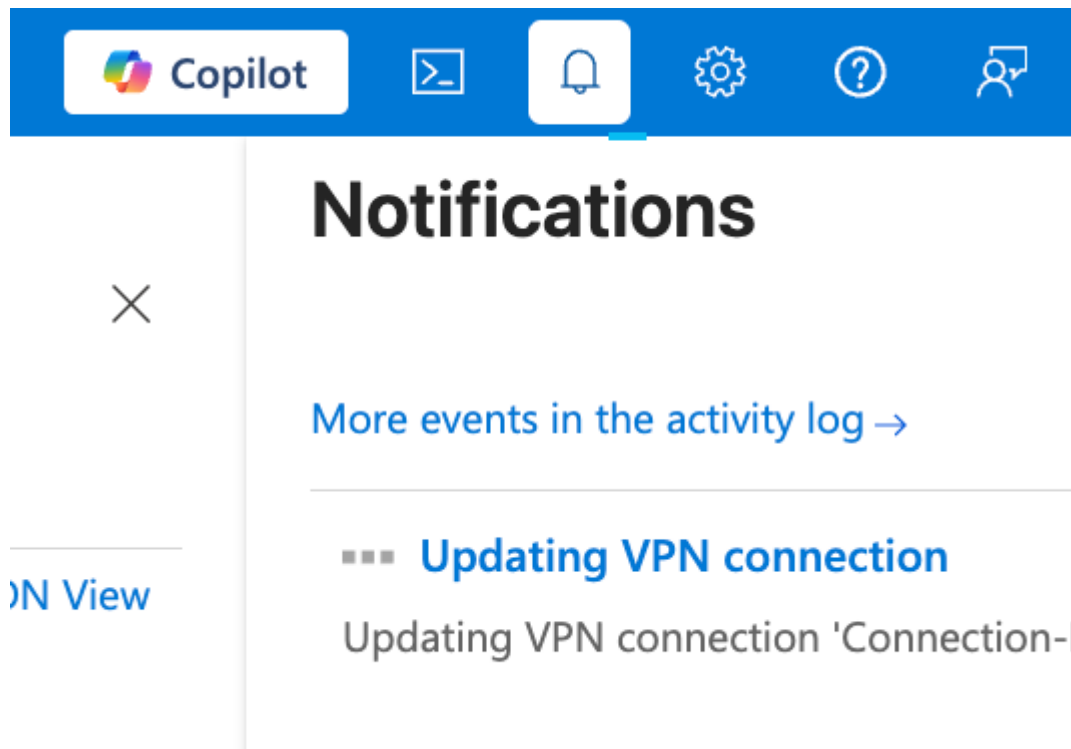
Create

Previous

Next

リンク接続の設定2つのカスタムBGP設定

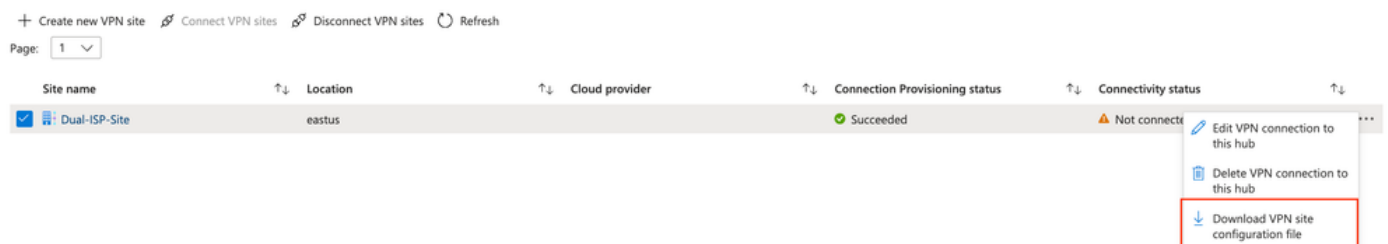
4) Azure UIの通知に、更新タスクの開始が表示されます。



Azure更新タスク開始通知

ステップ5:VPNサイト設定ファイルのダウンロード

1) Azureの同じVPN（サイト間）ページで、設定されたVPNサイトの右端にある省略記号のアイコンを選択し、Download VPN site configuration fileオプションを選択します。



VPNサイト設定ファイルのダウンロードオプション

2) Click here to downloadハイパーリンクをクリックします。



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



VPNサイト設定ファイルのダウンロード

フェーズ2: Azure vWANへのデュアルISP接続のためのFTDの構成

ステップ1: ダウンロードしたVPN設定の分析

1) ダウンロードしたコンフィギュレーションファイルを開くと、同様のJavaScript Object Notation(JSON)出力が表示されます。出力には、ファイルに書き込まれた2つのオブジェクトのいずれかが表示されます。この情報は、FTDの設定に役立つコンテキストを提供します。



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。



注：ダウンロードされたファイルでのISP-Link-1 JSONオブジェクトの順序は逆になっています。コード出力の省略記号(...)は、ISP-2-Linkオブジェクトを適切な設定で表しています。

```
...
{
  "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
        }
      }
    }
  ]
}

```

この出力は、手順を実行する際の参照用として保存してください。

ステップ2：リンクBGPアップデートソースループバックインターフェイスの設定

FTD BGPプロセス下のBGPネイバー構成エントリ（FTDで後の手順で構成）には、対応するリンクBGP IPアドレスを表す安定したソースがAzureサイトリンク構成に必要です。

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

Cloud-delivered Firewall Management Center
Devices / Device Management

Devices

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

— Show less

Monitor

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

Manage

- Policies >
- Objects
- Devices**

Firepower Management CenterのDevice Management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、手順はオンプレミスFMCと同じです。

2)デュアルISP接続を持つブランチ/サイトVPNデバイスとして設定するFTDをクリックします。

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

設定導入用のFTDの選択

3) Add Interfacesドロップダウンメニューをクリックし、Loopback Interfaceをクリックします。

CXvWAN-FTD-2 Save Cancel

Cisco Secure Firewall Threat Defense for AWS

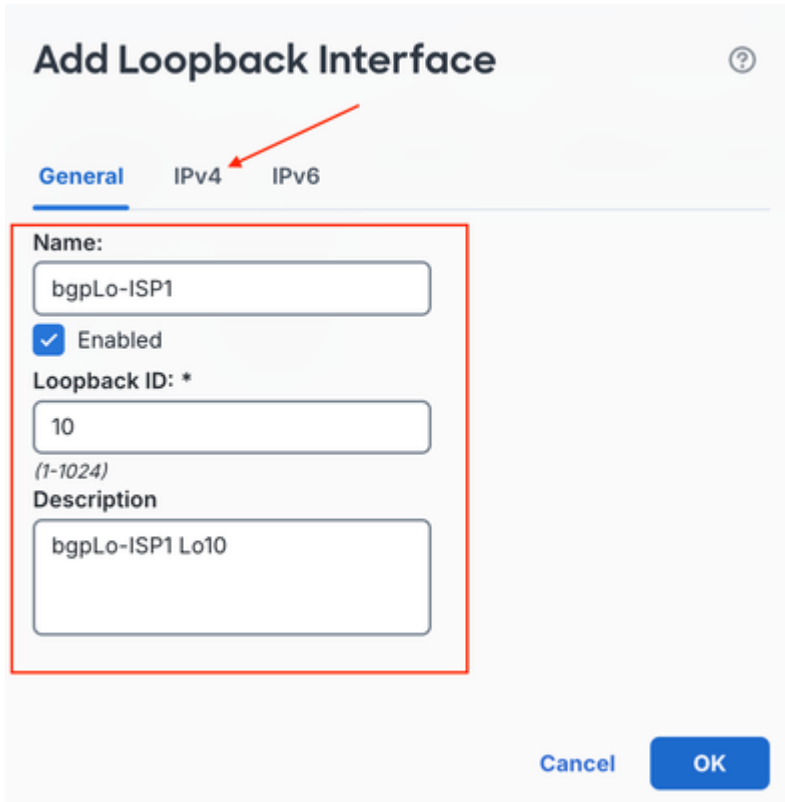
Device **Interfaces** Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels Sync Interface Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/St...	IP Address	Path Mon...	Vir
Management0/0	management	Physical				Disabled	Glc
Ethernet0/0	ISP1	Physical				Disabled	Glc
Ethernet0/1	ISP2	Physical				Disabled	Glc

- Sub Interface
- Redundant Interface
- Bridge Group Interface
- Virtual Tunnel Interface
- Loopback Interface**
- VNI Interface

4)ループバックインターフェイスの名前を入力し、Enabled チェックボックスにチェックマークが付いていることを確認してから、Loopback IDを入力します。必要な場合は、[Description] に説明を入力します。完了したら、IPv4タブをクリックします。



Add Loopback Interface ⓘ

General IPv4 IPv6

Name:
bgpLo-ISP1

☒ Enabled

Loopback ID: *
10
(1-1024)

Description
bgpLo-ISP1 Lo10

Cancel OK

5)ループバックIPアドレスを入力して、AzureのISP1サイトリンクに対して、前の手順で構成したリンクBGP IPアドレスにします。このIPは、ISP1経由でFTDとAzureインスタンス間に設定されたネイバーシップのBGPアップデートソースとして使用されます。



注:ISP1のvpnSiteConfiguration.BgpSetting.BgpPeeringAddressの下のダウンロードされたVPNコンフィギュレーションJSONで以前に定義された値を参照できます

Add Loopback Interface ?

General **IPv4** IPv6

IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

ループバックIPv4アドレスを入力し、OKをクリックします

6) ISP2 BGPループバック設定に対して、サブステップc ~ eをこの順序で繰り返します。

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

第1および第2のループバックインターフェイスの作成

7)設定を保存します。

You have unsaved changes Save Cancel

変更の保存

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

1) FMCとFTD VPNのトポロジで一致するIKEv2/IPsec設定を設定するには、Manage > Objectsの順に選択し、ナビゲーションメニューをVPNにスクロールして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ポリシーを設定します。

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-STA	☐ ☐
AES-GCM-NUL-STA-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

新しいIKEv2ポリシーオブジェクトの作成

2)新しいIKEv2ポリシーの名前を入力し、PriorityとLifetimeの両方（またはいずれか）を選択します。Integrity, Encryption, Pseudo Random Function(PRF)、および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の構成と一致させるアルゴリズム/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

SHA256

Cancel Save

IKEv2ポリシーの作成

3)設定が完了したら、Saveをクリックします。

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

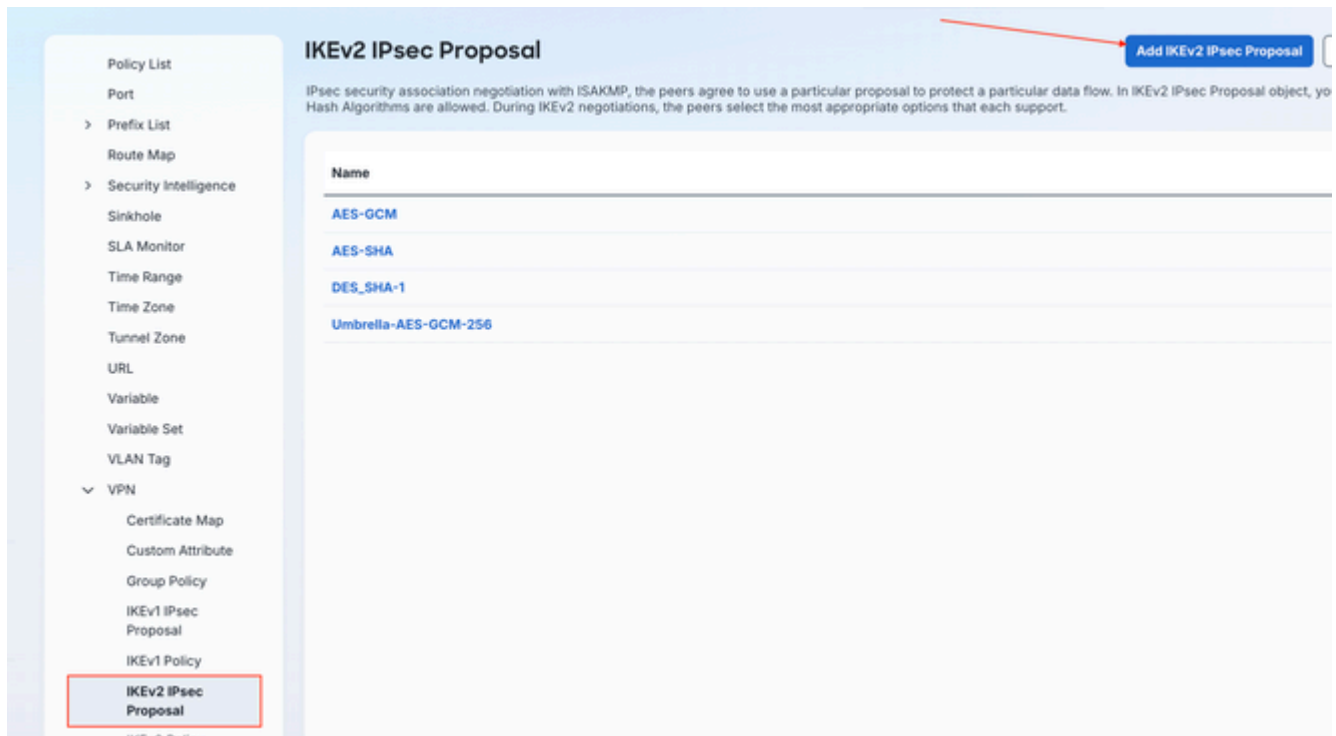
Add

14

Cancel Save

IKEv2ポリシーの保存

4) 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。



IKEv2 IPsecプロポーザルの作成

5) 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。

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



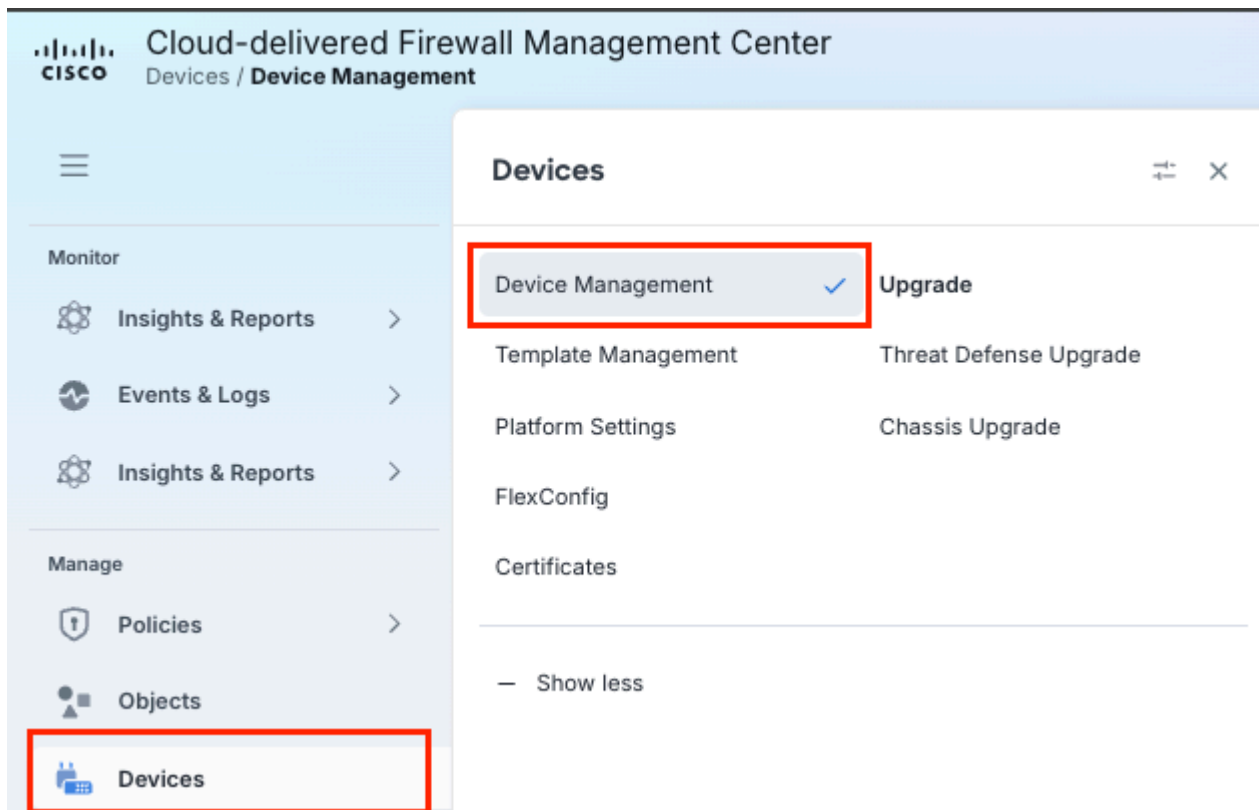
Cancel

Save

IKEv2 IPsec Proposalという名前を付けてSaveをクリックする

ステップ4：仮想トンネルインターフェイス(VTI)の設定

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



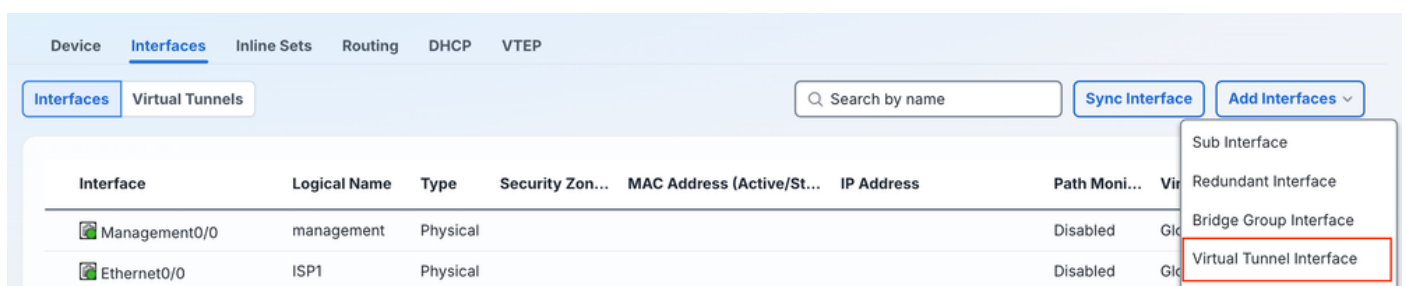
Firepower Management CenterのDevice Managementに移動します。

2)デュアルISP接続のブランチ/サイトVPNデバイスとして設定しているFTDをクリックします。

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

設定導入用のFTDの選択

3) Add Interfaces ドロップダウンメニューをクリックして、Virtual Tunnel Interface (VTI)を選択します。



仮想トンネルインターフェイスの作成

4)トンネル情報を入力します。Enabledチェックボックスにチェックマークが付いていて、Name (名前) が入力されていて (必要に応じてDescription も入力)、オプションでSecurity Zoneが選択されていることを確認します。正しい親ISP側インターフェイスを配置してVTIを設定し、VTIの内部トンネルIPSec接続に適切なIPアドレスを設定します。完了したらOKを押します。

。



ヒント：参照図は、FTDを使用したAzureデュアルWAN接続の潜在的なVPN設定の詳細なコンテキストを示しています。

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)親ISP1およびISP2インターフェイスに3つの追加VTIを設定します。

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

追加の仮想トンネルインターフェイスの設定

f) Saveをクリックして、変更を保存します。

You have unsaved changes

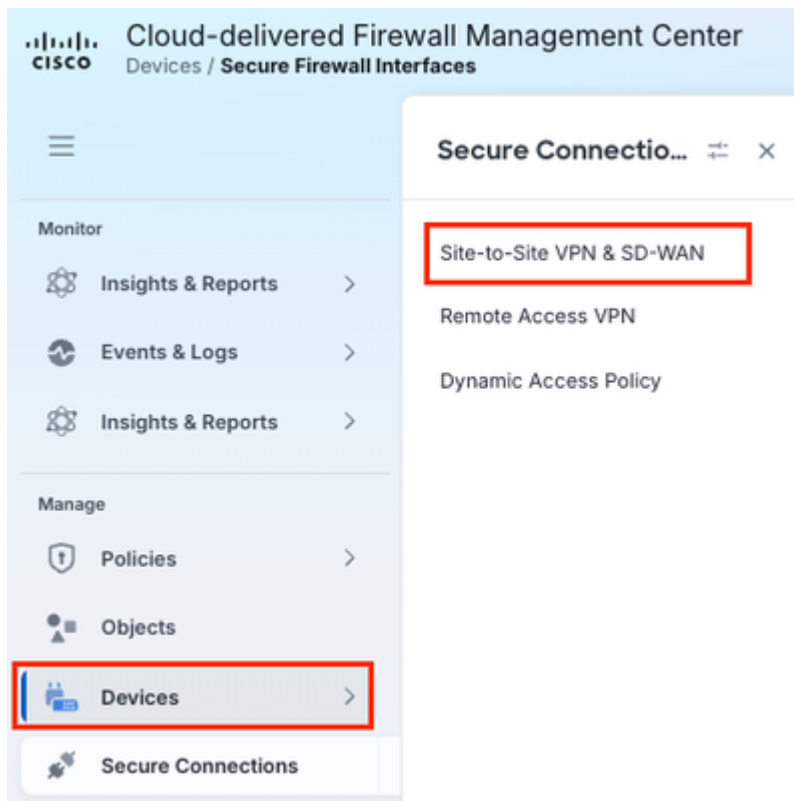
Save

Cancel

変更の保存

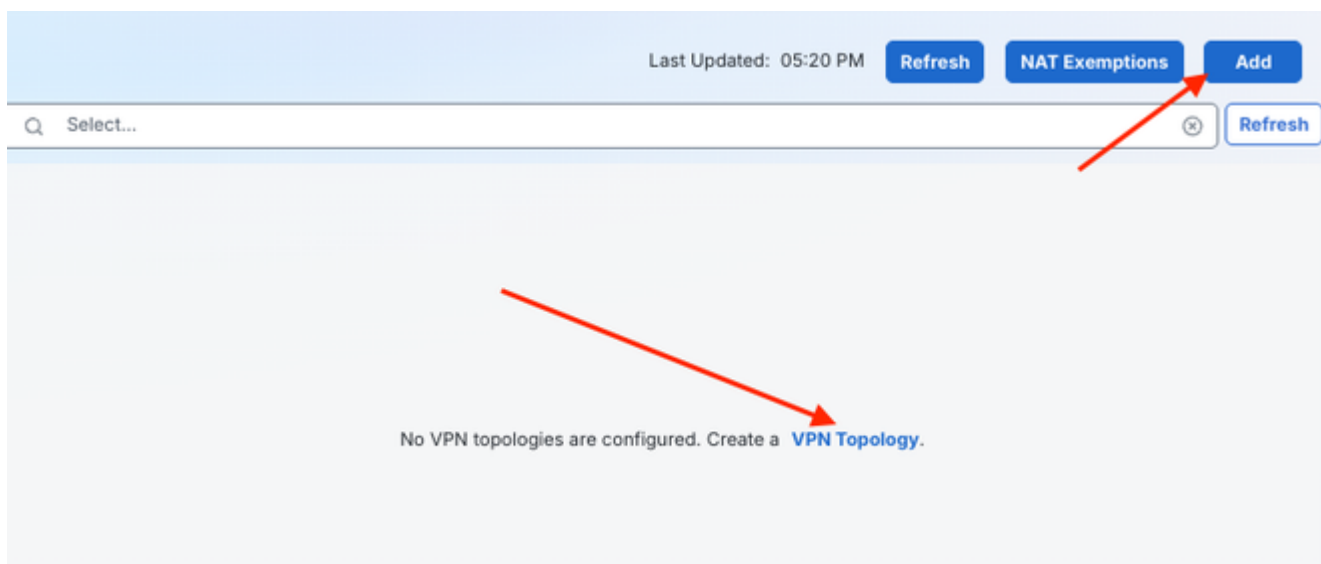
ステップ5:IPsec VPNトポロジのプロビジョニング

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



サイト間VPNおよびSD-WAN接続の管理

2)初期出力の中央にある初期VPN Topology設定ハイパーリンクをクリックするか、Addボタンをクリックします。



新しいVPNトポロジ設定の追加

3) ISP1リンク経由でAzure Instance0への最初のトンネルのトポロジ名を入力します。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 *
CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

New

☐ SD-WAN Topology

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

Select VPN Topology

☐ ☒ Hub and Spoke

Prerequisites

☒ **Route-Based VPN**

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

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Policy-Based VPN

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

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ Full Mesh

☐ SASE Topology

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

Prerequisites

Refresh

Cancel Create

ルートベースのVPNトポロジタイプの設定

4)最初に、ノードAデバイスを選択し、Deviceドロップダウンリストで、AzureからのVPNトンネルを終端するFTDを示します。ウィザードがデバイスから使用可能なVTIを取得したら、ドロップダウンメニューから、設定している親インターフェイスとインスタンスに適したVTIを選択します。Node B Deviceメニューから、VPNトポロジ構成でExtranetノードになるAzure側を選択します。ノードBのフレンドリ名を設定し、適切なエンドポイントIPアドレスを入力していることを確認します。完了したら、IKEタブをクリックして、フェーズ1トンネル設定を実装します。



注：インスタンスのエンドポイントIPアドレスの値は、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].gatewayConfiguration.IpAddresses.Instance0および
vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1) で参照できます

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](#)

ノードAとノードBのトポロジエンドポイントを定義する

5)ナビゲーションメニューをIKEv2 Settingsまでスクロールし、鉛筆アイコンをクリックして、最近設定したIKEv2ポリシーのポリシーを編集します。次に、Authentication TypeドロップダウンメニューからPre-shared Manual Keyオプションを選択し、Azureで以前に設定したPSKを入力します。完了したら、IPsecタブをクリックして、フェーズ2 IPsecトンネルパラメータを設定します。



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:*
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

IKEv2設定と認証キーの編集

6) IKEv2 IPsec Proposal Transform Setの横にある鉛筆アイコンをクリックし、以前設定したIPsecポリシーパラメータを選択します。Lifetime Durationの値は、必ずAzure vWAN VPNの設定に合わせて変更してください。設定情報を確認したら、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:*

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

IPSecプロポーザルの有効期間の構成

7)手順5の前のサブステップを繰り返して、ISP1 Instance1、ISP2 Instance0、およびISP2 Instance1間に他のAzureトンネルを作成します。

> 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	✓		

追加のサイト間VPNトポロジの作成

手順6:VPNトポロジを検証する

system support diagnostic-cliに入り、enと入力してEnterキーを押します (読み取り専用CLI)。

1) IKE Phase 1 Tunnel connectivityをチェックします。

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

2) IPSecフェーズ2接続を確認します。

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



注:IPSecセキュリティアソシエーション(SA)の出力を表示すると、pkts decapsおよびpkts decryptカウンタが増加しますが、pkts encapsおよびpkts encryptは増加しません。このシナリオでは、このような増加が予想されます。Azureは、ハブプライベートIP空間アドレスを使用してBGPネイバーシップを形成しようとしていますが、ネイバーエンドがAPIPA BGPアドレスを使用している場合は、ネゴシエーションを開始しません。カスタムAPIPAが使用される場合、Azureに接続するデバイスがBGPネゴシエーションを開始する責任があります。

3)レイヤ2接続をチェックします。

```
show arp
```

4) IP Routingにチェックマークを付けます。

```
show route
```

5) ISP1およびISP2のインターフェイスでキャプチャを実行します。

```
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 Verification - vWAN Hub > Connectivity.> VPN Sites > Choose the site configuredに移動します。

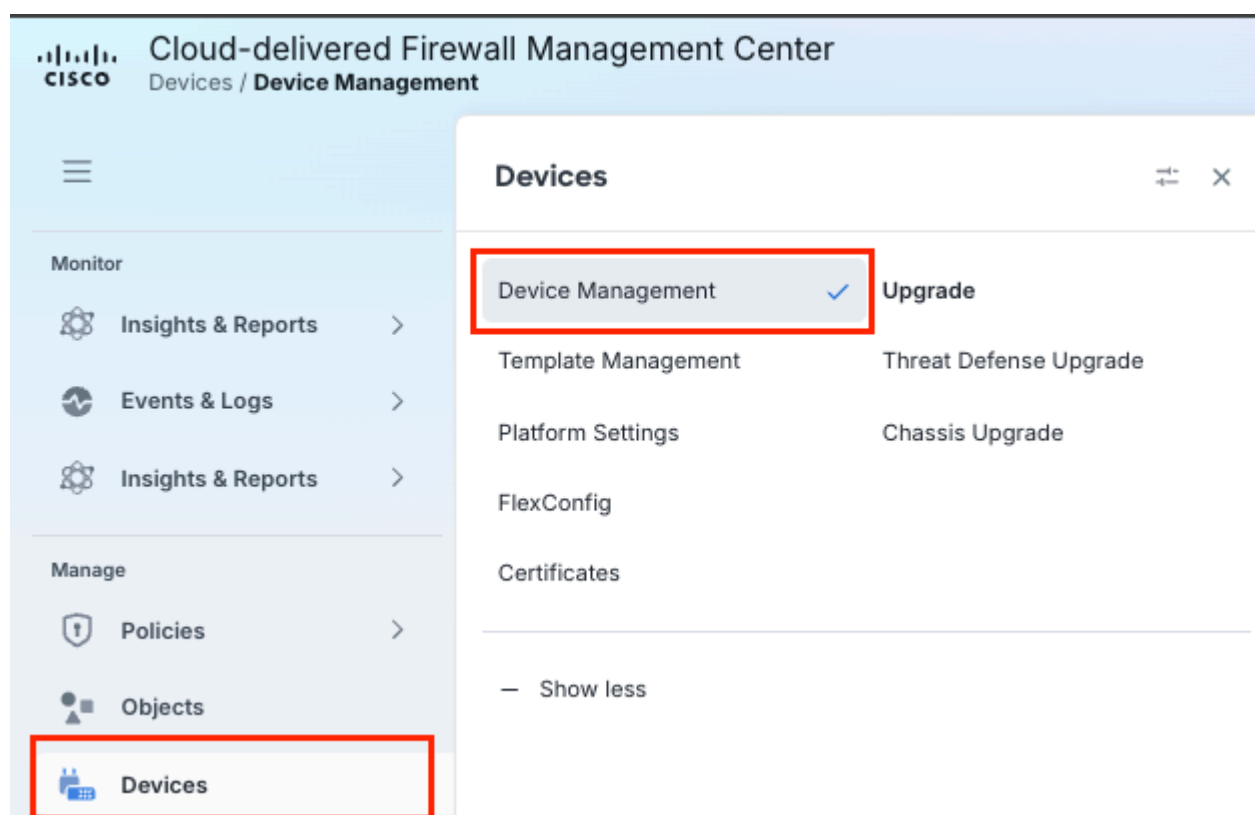
Links

☐ 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リンク接続の検証

ステップ7:ECMPの設定

1) Manage > Devices > Device Managementの順に移動し、FTDをクリックします。



The screenshot shows the Cisco Cloud-delivered Firewall Management Center interface. The left sidebar contains a navigation menu with sections 'Monitor' and 'Manage'. Under 'Manage', the 'Devices' option is highlighted with a red box. The main content area displays the 'Devices' page, where 'Device Management' is selected and highlighted with a red box. Other options visible include 'Template Management', 'Platform Settings', 'FlexConfig', 'Certificates', 'Upgrade', 'Threat Defense Upgrade', and 'Chassis Upgrade'.

Firepower Management CenterのDevice Managementに移動します。

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

設定導入用のFTDの選択

2) Routingタブをクリックして、ECMPを選択します。

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

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

等コストマルチパスの設定値

3) Addをクリックします。

Equal-Cost Multipath Routing (ECMP)

Add

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

等コストマルチパス設定の追加

4) ECMPゾーンに名前を付け、使用可能なVTI Interfacesをクリックしてから、AddボタンをクリックしてそれらをSelected Interfaces列に適用し、OKをクリックします。

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

等コストマルチパスゾーンのインターフェイスの選択

5)変更を保存したことを確認します。

You have unsaved changes

Save

Cancel

変更の保存

ステップ8:BGPの設定

1) FTDでRouting > General Settings > BGPの順に選択し、BGPプロセスを有効にします。
Enable BGPチェックボックスをオンにして、フェーズ1の手順1d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

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

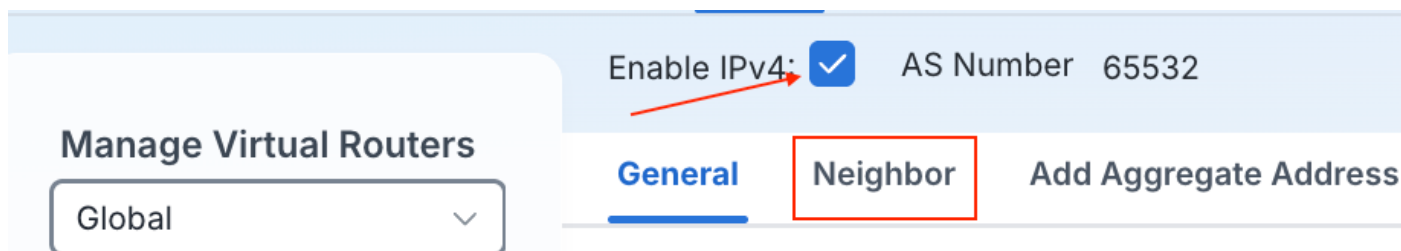
Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

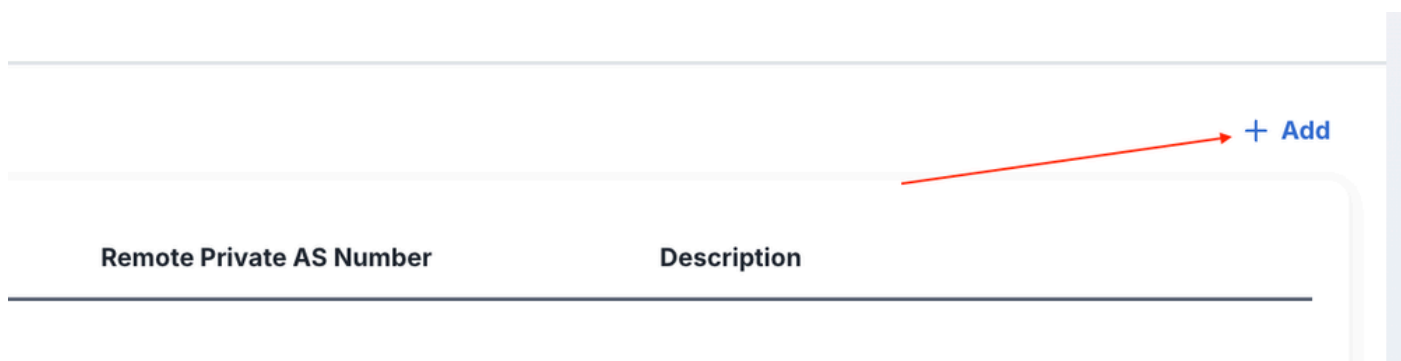
General SettingsでBorder Gateway Protocol(BGP)プロセスを有効にする

2) BGPプロセスのEnable IPv4チェックボックスにチェックマークが入っていることを確認し、NeighborをクリックしてAzureでBGPネイバーを設定します。



IPv4 Border Gateway Protocol(BGP)プロセスの有効化

3) + Addをクリックします。



新しいBorder Gateway Protocol(BGP)ネイバーの追加

4)ISP1 Instance0 BGPピアリング情報を入力し、表示されたBGP ASをvWANハブから参照し、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。



注: Azureで構成されているISP1リンクにマッピングされているFTD上のVTIインターフェイスのループバックを参照するには、BGP Update Sourceを選択していることを確認してください。

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

Border Gateway Protocol(BGP)ピアリング情報の設定

5) FTDのBGP Neighbor設定にあるAdvancedメニューで、eBGPのデフォルトの1ホップからの存続可能時間(TTL)ホップの数を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。[OK] をクリックします。

☐ 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

Border Gateway Protocol(BGP)ネイバーの詳細設定

6)サブステップ3 ~ 5を繰り返して、ISP1のInstance1に対してTunnel2を設定します。

7)サブステップ3 ~ 5を2回繰り返して、ISP2 Instance0/Instance1 BGPピアリング情報を設定します。



注：Azureで構成されたISP2リンクにマッピングされたFTD上のVTIインターフェイスのループバックを参照する、アライメントされたBGP Update Sourceを選択していることを確認してください。

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インスタンス1 BGPネイバーの設定

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インスタンス2 BGPネイバーの設定

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		

BGPネイバー結果の設定の終了

完了したら、Saveをクリックします。

You have unsaved changes

Save

変更の保存

デフォルトでは、ECMPがAzureへのすべてのVTIで設定されていても、BGPはルーティングテーブルに1つのベストパスのみを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9:eBGPマルチパスの設定

1) Routing > BGP > IPv4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。

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

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

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP (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

Forward Packets Over Multiple Paths設定

2) Number of Pathsフィールドのデフォルト値を1から4に変更します。[OK] をクリックします。

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Forward Packets Over Multiple Pathsの設定の変更

3)変更を保存して展開したことを確認します。

確認/トラブルシューティング

導入が完了したら、FTD BGPプロセスがそれぞれのトンネルの両方のAzureインスタンスとネイバー隣接関係を確立し、ルートが学習され、インターフェイスが起動し、プロトコル接続が接続テーブルに返されることを確認します。

フェーズ2のステップ7で実行したように、FTD CLIで `system support diagnostic-cli` に移動します。

1)展開されると、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#
```

```
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) 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 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)ルーティングテーブルの作成を確認します。

```
<#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 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) BGPセッションの接続テーブルを確認します。

<#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
TCP bgpLo-ISP2 169.254.22.22:179 NP Identity Ifc 169.254.22.100:41883, idle 0:00:01, bytes 751, flags
TCP bgpLo-ISP1 169.254.21.2:179 NP Identity Ifc 169.254.21.100:61287, idle 0:00:04, bytes 639, flags
```

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て、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。