

Configurer la connectivité vWAN double FAI Azure sur le pare-feu sécurisé

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme](#)

[Liaisons DIA \(Dual Direct Internet Access\) \(Azure + FTD Load-Balancing/Redundancy\)](#)

[Configurer](#)

[Phase 1 : Configuration du site VPN vWAN Azure](#)

[Étape 1: Créer un site VPN vWAN Azure \(périphérique FTD distant\)](#)

[Étape 2: Configurer les paramètres de la passerelle Azure APIPA](#)

[Étape 3: Configurer les paramètres VPN du site vWAN Azure](#)

[Étape 4: Activer et activer l'APIPA BGP personnalisé sur les instances de liaison de site VPN](#)

[Étape 5: Télécharger le fichier de configuration du site VPN](#)

[Phase 2 : Configurer le FTD pour la connectivité double FAI vers le vWAN Azure](#)

[Étape 1: Analyse de la configuration VPN téléchargée](#)

[Étape 2: Configurer les interfaces de bouclage source de mise à jour BGP de liaison](#)

[Étape 3: Configuration des objets de stratégie Phase 1/Phase 2](#)

[Étape 4: Configuration des interfaces de tunnel virtuel \(VTI\)](#)

[Étape 5: Provisionner des topologies VPN IPsec](#)

[Étape 6: Valider les topologies VPN](#)

[Étape 7: Configurer ECMP](#)

[Étape 8: Configurer BGP](#)

[Étape 9: Configurer le multichemin eBGP](#)

[Vérification/dépannage](#)

Introduction

Ce document décrit comment configurer la connectivité VPN site à site de Microsoft Azure Virtual WAN (vWAN) au pare-feu sécurisé à l'aide de liaisons WAN doubles.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

Assurez-vous que ces deux composants ont été configurés initialement dans l'environnement Azure :

- Instance vWAN Microsoft Azure
- Concentrateur vWAN Microsoft Azure

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure FTD version 10.0
- Cisco Secure FMC version 10.0
- Microsoft Azure vWAN

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsque le FTD de la succursale dispose de deux interfaces externes orientées vers le fournisseur d'accès Internet (FAI), chacune peut se connecter de manière redondante et active à Azure vWAN, de sorte que chaque liaison FAI est utilisée. Azure vWAN crée deux tunnels IPsec par liaison de site, un vers Azure Hub Instance0 et un vers Instance1, de sorte que chaque interface ISP termine deux tunnels. Sur les deux liaisons ISP, quatre tunnels IPsec se terminent sur le FTD.

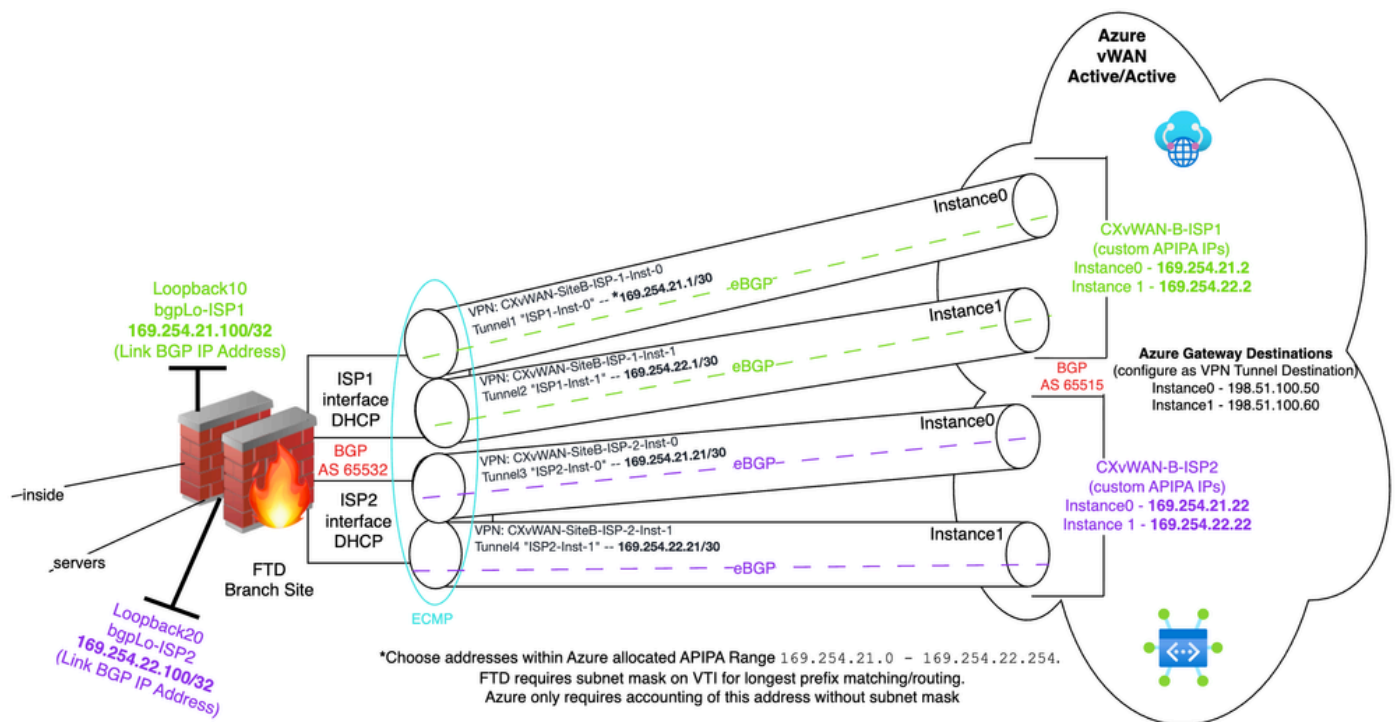
Les instances Azure fonctionnent en mode actif/actif pour l'équilibrage de charge et la redondance, de sorte que le FTD reflète cela via la configuration ECMP (Equal-Cost Multi-Pathing) sur les quatre tunnels IPsec. À l'aide d'adresses APIPA (Automatic Private IP Addressing) personnalisées, des voisins eBGP (Border Gateway Protocol) externes avec des numéros de système autonome privés (ASN) distincts sont établis sur chacun des quatre tunnels.

Cela active la fonctionnalité de chemins d'accès multiples BGP, fournissant plusieurs chemins d'accès redondants à chaque paire d'instances de liaison de site de concentrateur Azure.

Diagramme

Le schéma illustre la topologie de la configuration décrite dans cet article. La variante de liaison DIA (Direct Internet Access) double source les deux tunnels Azure à partir de deux interfaces externes sur le FTD.

Liaisons DIA (Dual Direct Internet Access) (Azure + FTD Load-Balancing/Redundancy)



Topologie de connectivité à double accès direct à Internet

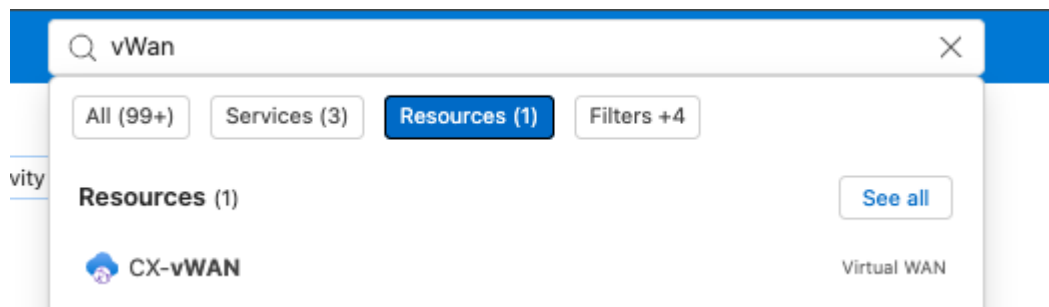
Configurer

Phase 1 : Configuration du site VPN vWAN Azure

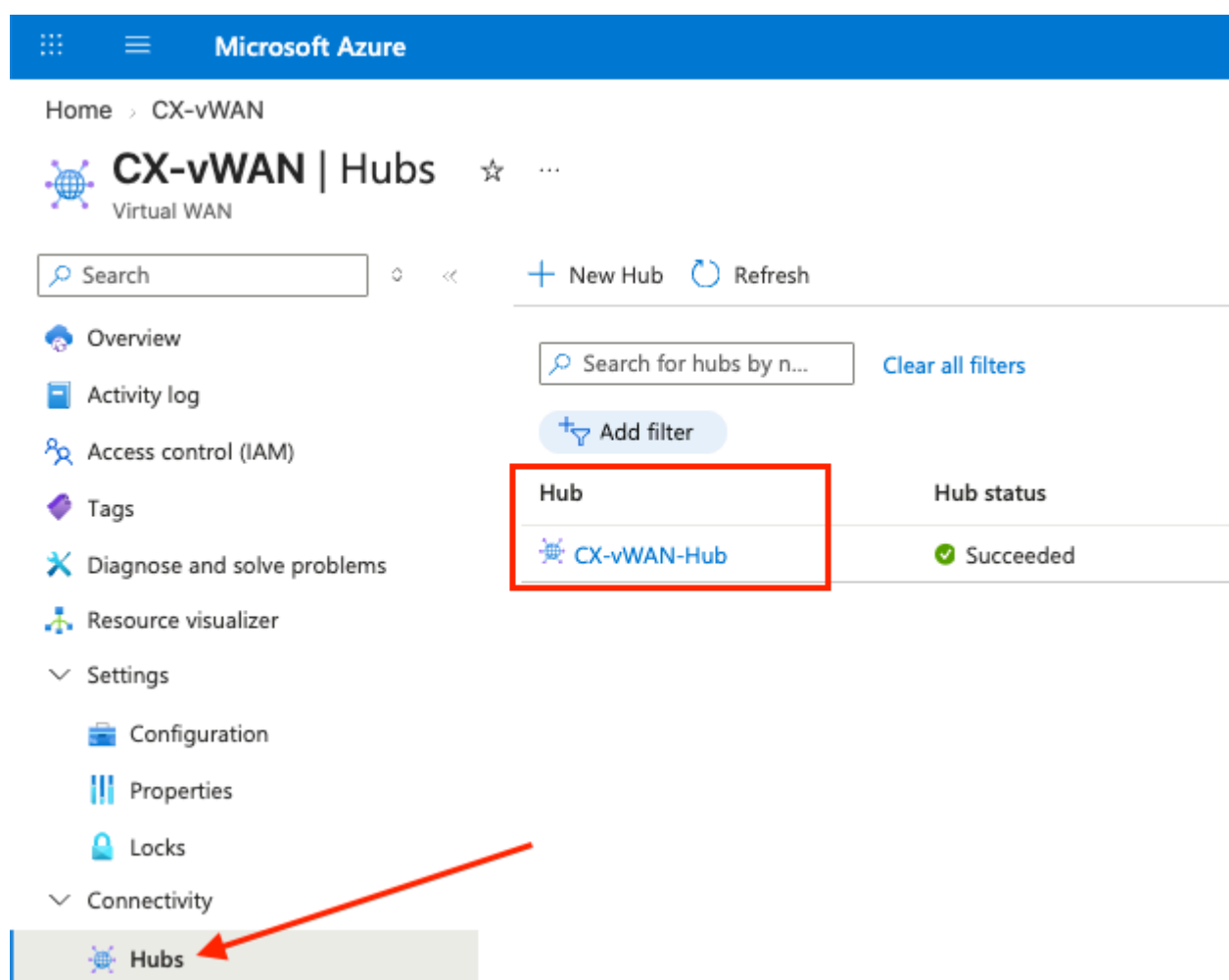
Étape 1: Créer un site VPN vWAN Azure (périphérique FTD distant)

1) Recherchez vWAN dans le champ de recherche Azure, cliquez sur Virtual WAN pour entrer

dans le concentrateur vWAN Azure existant. Accédez ensuite à Connectivity > Hubs et cliquez sur le concentrateur vWAN Azure existant.



Requête de recherche pour le WAN virtuel



Sélectionner un concentrateur WAN virtuel existant

2) Cliquez sur Connectivity > VPN (Site to site) et cliquez sur + 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		

Créer un nouveau site WAN virtuel



Remarque : Les espaces couvrant les valeurs dans divers champs des images sont intentionnels pour la publication de ce document.

3) Entrez les valeurs dans les champs obligatoires. Lorsque vous avez terminé, cliquez sur Next : Liens > pour avancer.

Create VPN site ...

Basics Links Review + create

Project details

Subscription	
Resource group *	

Instance details

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

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

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

Previous

Next : Links >

Paramètres généraux de configuration du site VPN

4) Entrez les informations de liaison requises. L'adresse BGP de liaison et l'ASN de liaison sont l'adresse de destination BGP de couche 3 du tunnel interne et le numéro d'AS BGP du côté de la branche avec laquelle le voisinage est formé sur les tunnels site à site. L'adresse BGP de liaison est une adresse de sous-réseau ne se chevauchant pas (/32) en dehors du sous-réseau d'espace d'adressage privé du concentrateur configuré, qu'Azure installe en tant que route /32 à atteindre en tant que voisin BGP. Deux interfaces de bouclage sont créées dans des sections ultérieures sur le FTD pour représenter l'adresse BGP de liaison pour chacune des liaisons de site doubles. L'adresse IP de liaison/nom de domaine complet (FQDN) est l'adresse IP de destination de couche 3 de l'en-tête externe du trafic destiné au site de la filiale nécessaire pour provisionner la connectivité IP Security (IPsec)/Internet Key Exchange version 2 (IKEv2). Passez à l'étape suivante lorsque vous avez terminé en cliquant sur Next : Vérifier + créer >.



Remarque : Assurez-vous de consulter la documentation Azure spécifique si vous utilisez des adresses comprises entre 169.254.21.0 et 169.254.22.255 pour les adresses de

tunnel : [Choix des adresses APIPA BGP.](#)

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

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

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

Previous

Next : Review + create >

Configurer les paramètres de liaison de site

5) Une fois les informations confirmées comme prévu, cliquez sur Créer.

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

Vérifier et créer un nouveau site VPN

6) Une fois le déploiement du site VPN terminé, revenez à la configuration du concentrateur vWAN.

The screenshot shows the 'VpnSiteDeployment | Overview' page in the Azure portal. The page has a blue header with 'Home' and a search bar. Below the header, there's a sidebar with 'Overview', 'Inputs', 'Outputs', and 'Template'. The main content area shows a green checkmark icon and the text 'Your deployment is complete'. Below this, there's a section for 'Deployment details' with fields for 'Deployment name : VpnSiteDeployment', 'Subscription :', and 'Resource group :'. There are also links for 'Deployment details' and 'Next steps', and a blue button labeled 'Go to resource'.

Progression du déploiement du site WAN virtuel

The screenshot shows a search results window for 'vWan'. The search bar at the top contains 'vWan'. Below the search bar, there are tabs for 'All (99+)', 'Services (3)', 'Resources (1)', and 'Filters +4'. The 'Resources (1)' tab is selected. Below the tabs, there's a section titled 'Resources (1)' with a 'See all' button. The resource listed is 'CX-vWAN' with a 'Virtual WAN' label.

Requête de recherche pour le WAN virtuel

Étape 2: Configurer les paramètres de la passerelle Azure APIPA

Azure nécessite une configuration supplémentaire pour les adresses APIPA (Automatic Private IP Addressing) dans l'espace d'adressage IPv4 169.254.0.0/16.

1) Accédez au concentrateur existant via Connectivity > Hubs.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Accéder à la connectivité du concentrateur WAN virtuel

2) Accédez de nouveau à Connectivity > VPN (Site to site) et cliquez sur le lien hypertexte Gateway Configuration.

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

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

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

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ⓘ

Accéder au lien hypertexte de configuration de passerelle

3) Un panneau latéral apparaît pour Modifier la passerelle VPN. Sous VPN Gateway Instance0 et VPN Gateway Instance1, entrez deux adresses IP BGP personnalisées uniques qui agissent comme des adresses IP de voisinage pour chaque instance pour les voisins BGP sur les tunnels IPsec. Cela est nécessaire si vous choisissez d'utiliser l'adressage APIPA dans cette topologie. Dans le champ intitulé Peer Address, entrez l'adresse IP voisine BGP à utiliser pour atteindre les instances Azure à partir du FTD. Azure ne tente pas l'établissement BGP avec le FTD si l'adressage APIPA est utilisé, par conséquent le FTD tente l'établissement de voisin eBGP sur chaque tunnel avec Azure.

Le total se compose de 2 liaisons x 2 tunnels implicites ; un tunnel vers Instance0 et Instance1 par liaison ISP ; le total s'élève à quatre tunnels IPsec avec des voisins BGP entre Azure et les deux interfaces FTD ISP.

Ces adresses doivent être uniques et, dans cette démonstration, la deuxième et dernière adresse d'hôte des sous-réseaux /30 affectés à chaque tunnel doit être configurée sur le FTD pour être utilisée. Une fois configuré, cliquez sur Edit.



Remarque : Assurez-vous de consulter la documentation Azure spécifique si vous utilisez des adresses comprises entre 169.254.21.0 et 169.254.22.255 pour les adresses de tunnel : [Choix des adresses BGP APIPA](#)

Edit VPN Gateway



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

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ

☒ Microsoft network ☐ Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



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

Edit

Cancel

Modifier les adresses IP BGP personnalisées de la passerelle VPN



Remarque : Comme le remarque Azure, la mise à jour peut prendre jusqu'à 30 minutes ou plus.

Étape 3: Configurer les paramètres VPN du site vWAN Azure

1) Sur la page Connectivity > VPN (Site to site) dans la configuration du concentrateur vWAN Azure, et cliquez sur le X pour effacer l'association de concentrateur : Filtrage connecté pour afficher les sites VPN déconnectés.

The screenshot shows the Microsoft Azure portal interface for a CX-vWAN-Hub. The left sidebar contains a navigation menu with 'Connectivity' expanded and 'VPN (Site to site)' selected. The main content area shows the 'VPN Sites' tab with a search bar and a filter bar. The filter bar displays 'Hub association : Connected' with a red 'X' icon next to it, and a red arrow points to this icon. Below the filter bar, there is a message: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Effacer les filtres de connexion d'association de concentrateur

2) Cochez la case en regard du site VPN récemment configuré, puis cliquez sur Connect VPN Site.



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

Action Connecter le site VPN

3) Configurez la clé prépartagée (PSK) souhaitée, puis configurez les paramètres IPsec souhaités en cliquant sur l'option de basculement Personnalisé. Ces paramètres IPSec doivent correspondre à la configuration FMC/FTD dans les étapes ultérieures. Pour enregistrer, cliquez sur Connect.



Remarque : La prise en charge du groupe 24 Diffie-Hellman (DH) a été supprimée dans FTD/FMC version 6.7.

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

Configuration de la clé pré-partagée et des paramètres IPsec

4) Confirmez que la mise en service du site VPN a réussi.

Notifications



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

[Dismiss all](#)



Successfully created VPN connection



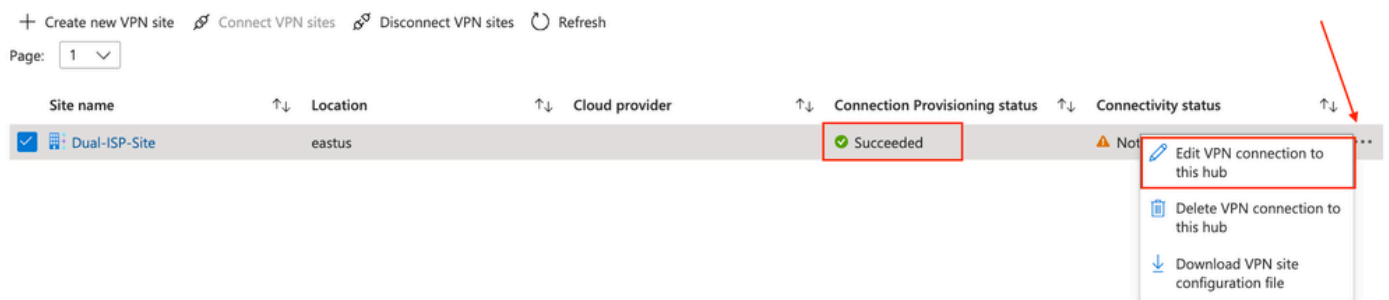
Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

Confirmer l'état de provisionnement du site VPN

Étape 4: Activer et activer l'APIPA BGP personnalisé sur les instances de liaison de site VPN

1) Actualisez la page VPN (site à site) et confirmez que la colonne Connection Provision status indique son succès, ce qui vous permet de cliquer sur les points de suspension et vous permet de cliquer sur l'élément de menu déroulant Edit VPN connection to this hub.



Valider la connexion et modifier la connexion VPN

2) Cliquez pour configurer Link Connection 1 (ISP1) et entrez de nouveau la clé prépartagée (PSK) applicable, et assurez-vous que vous cliquez sur le bouton Enable en regard de l'adresse IP BGP personnalisée, et mappez ce qui serait l'adresse d'hôte restante des sous-réseaux /30 qui vont être les valeurs du champ d'adresse IP de destination du tunnel interne de l'en-tête IP BGP généré par les FTD.

Essentiellement, le tunnel VTI1 du FAI1 vers l'instance0 d'Azure a une affectation d'adresse de 169.254.21.1/30, et le deuxième tunnel VTI2 du FAI1 se terminant sur le FTD a une adresse IP de 169.254.22.1/30 affectée à l'instance1.

Cliquez sur Suivant : Link Connection 2> pour passer aux paramètres de liaison du FAI 2.



Remarque : Il est possible que vous deviez saisir à nouveau votre clé PSK et cliquer à nouveau sur l'option Groupe PFS alignée dans le menu déroulant dans Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK)

.....

Connection Mode

Default Initiator Only Responder Only

Border gateway protocol

Disable Enable

Custom BGP IP Addresses

Disable Enable

Custom BGP IP Address

Instance 0

169.254.21.2

Instance 1

169.254.22.2

Use Azure Private IP Address

Yes No

Protocol

IKEv2 IKEv1

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

Use policy based traffic selector

Enable Disable

IPsec

Default Custom

SA Lifetime in seconds

27000

IKE Phase 1

Encryption

GCMAES256

Integrity/PRF

SHA384

DH Group

DHGroup14

IKE Phase 2(ipsec)

IPsec Encryption

GCMAES256

IPsec Integrity

GCMAES256

PFS Group

NONE

DPD timeout in seconds

45

Review + create

Previous

Next : Link connection 2 >

3) Répétez les étapes précédentes et appliquez les paramètres applicables sous Connexion de liaison 2 (liaison ISP2). Une fois terminé, cliquez sur Créer.

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 * 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

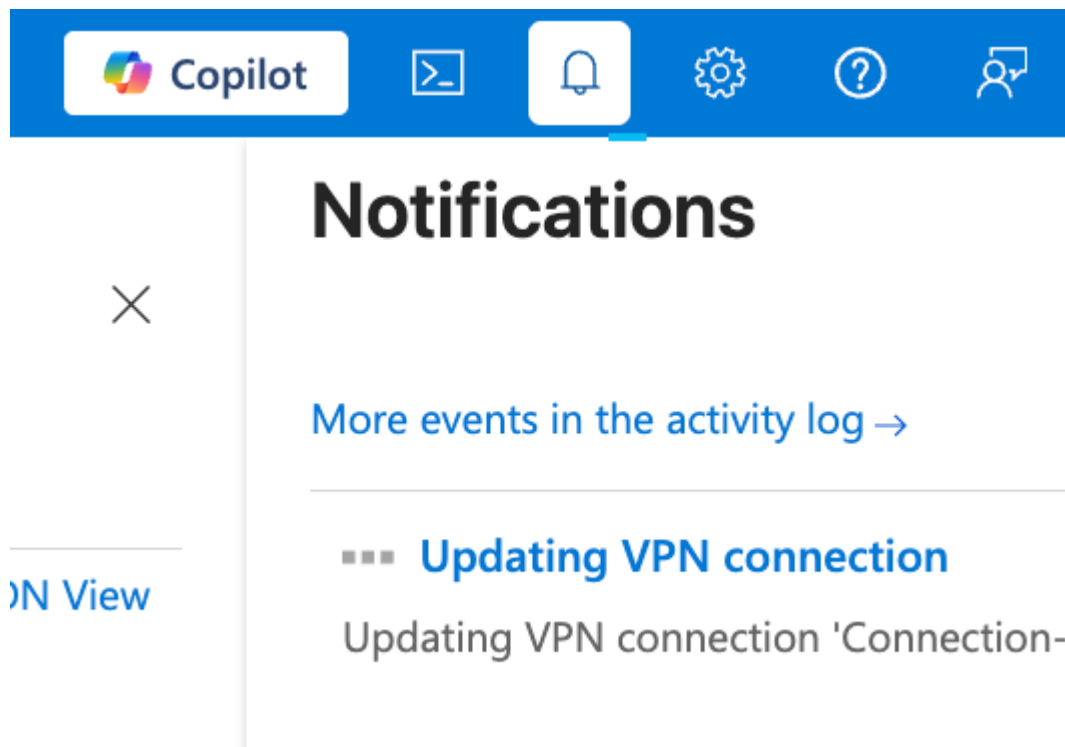
Create

Previous

Next

Configuration de la connexion de liaison avec deux paramètres BGP personnalisés

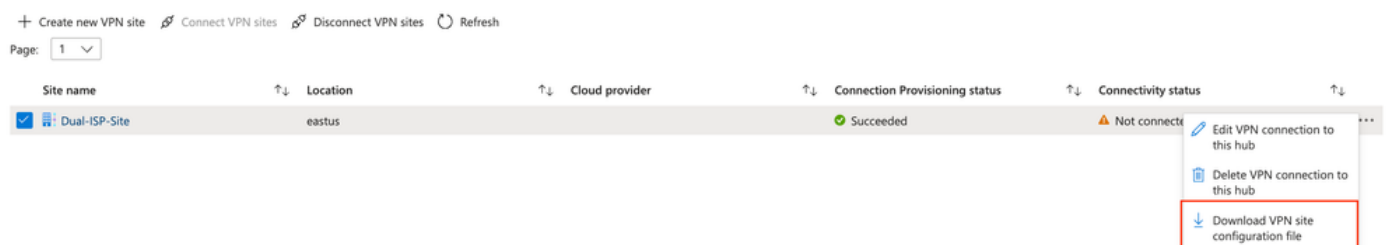
4) Les notifications de l'interface utilisateur Azure indiquent que la tâche de mise à jour commence.



Notification de début de tâche Azure Update

Étape 5: Télécharger le fichier de configuration du site VPN

1) Dans la même page VPN (site à site) dans Azure, choisissez l'icône en forme de point de suspension à l'extrême droite du site VPN configuré et choisissez l'option Télécharger le fichier de configuration du site VPN.



Option de téléchargement du fichier de configuration du site VPN

2) Cliquez sur le lien hypertexte Cliquez ici pour télécharger.



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



Télécharger le fichier de configuration du site VPN

Phase 2 : Configurer le FTD pour la connectivité double FAI vers le vWAN Azure

Étape 1: Analyse de la configuration VPN téléchargée

1) Ouvrez le fichier de configuration téléchargé et une sortie JavaScript Object Notation (JSON) similaire s'affiche. Le résultat montre l'un des deux objets écrits dans le fichier. Ces informations fournissent un contexte utile pour la configuration de FTD.



Remarque : Pour améliorer la mise au point, plusieurs objets non pertinents et paires clé/valeur sont élagués pour plus de concision.



Remarque : L'ordre des objets JSON ISP-Link-1 dans le fichier téléchargé est inversé. Les points de suspension dans le code représentent l'objet ISP-2-Link avec sa configuration applicable.

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

```

Conservez ce résultat comme référence au fur et à mesure que vous effectuez les étapes.

Étape 2: Configurer les interfaces de bouclage source de mise à jour BGP de liaison

Les entrées de configuration de voisin BGP sous le processus BGP FTD (configuré dans les étapes ultérieures sur le FTD) ont besoin d'une source stable représentant l'adresse IP BGP de liaison correspondante dans la configuration de liaison de site Azure.

1) Accédez à Périphériques > Gestion des périphériques.

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

Accédez À Device Management Sur Firepower Management Center



Remarque : Ces travaux pratiques utilisent le centre de gestion des pare-feu (cdFMC) fourni dans le cloud ; toutefois, les étapes restent les mêmes pour le FMC sur site.

2) Cliquez sur le FTD que vous configurez en tant que périphérique VPN de filiale/site avec une connectivité double FAI.

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

Sélectionnez Le FTD Pour Le Déploiement De La Configuration

3) Cliquez sur le menu déroulant Add Interfaces, puis sur Loopback Interface.

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	Glo
Ethernet0/0	ISP1	Physical				Disabled	Glo
Ethernet0/1	ISP2	Physical				Disabled	Glo

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

Ajouter Une Interface De Bouclage Au Périphérique

4) Entrez le nom de l'interface de bouclage, assurez-vous de cocher la case Enabled et entrez un ID de bouclage. Entrez une description si vous le souhaitez. Une fois terminé, cliquez sur l'onglet IPv4.

Add Loopback Interface

General **IPv4** IPv6

Name:

☒ Enabled

Loopback ID: *

(1-1024)

Description

Cancel OK

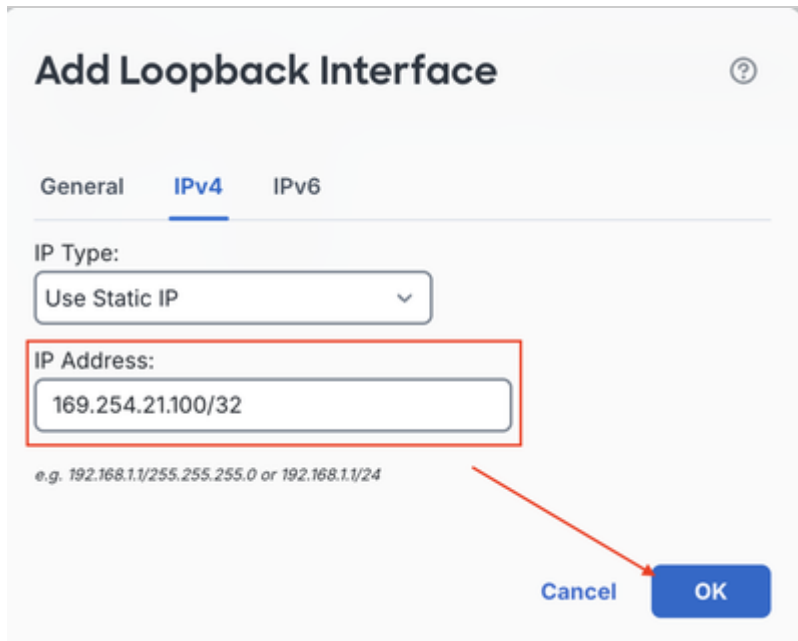
Configuration Des Informations D'Interface De Bouclage Et De L'Adresse IPv4

5) Entrez l'adresse IP de bouclage à utiliser comme adresse IP BGP de liaison configurée dans les étapes précédentes pour la liaison de site ISP1 dans Azure. Cette adresse IP est utilisée comme source de mise à jour BGP sur les voisins configurés entre le FTD et les instances Azure sur ISP1.



Remarque : Vous pouvez référencer la valeur précédemment définie dans la configuration VPN JSON téléchargée sous `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress` pour

ISP1



Add Loopback Interface

General **IPv4** IPv6

IP Type:
Use Static IP

IP Address:
169.254.21.100/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

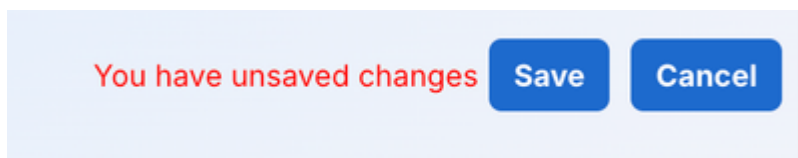
Entrez L'Adresse IPv4 De Bouclage Et Cliquez Sur OK

6) Répétez les sous-étapes c à e de cette séquence pour la configuration de bouclage BGP du routeur ISP2.

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

Créer une première et une deuxième interface de bouclage

7) Enregistrez votre configuration.



You have unsaved changes Save Cancel

Enregistrer les modifications

Étape 3: Configuration des objets de stratégie Phase 1/Phase 2

1) Pour configurer la configuration IKEv2/IPsec correspondante sur les topologies FMC à FTD VPN, accédez à Manage > Objects, faites défiler le menu de navigation jusqu'à VPN, et développez le sous-menu. Configurez la stratégie IKEv2 Phase 1 en choisissant IKEv2 Policy dans le menu et en cliquant sur Add IKEv2 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](#)

Name		
AES-GCM-NUL-SSH		
AES-GCM-NUL-SSH-LATEST		
AES-SSH-SSH		
AES-SSH-SSH-LATEST		
DES-SSH-SSH		
DES-SSH-SSH-LATEST		
Umbrella-AES-GCM-256		

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

Créer un nouvel objet de stratégie IKEv2

2) Entrez un nom pour la nouvelle stratégie IKEv2, choisissez Priority (Priorité) et/ou Lifetime (Durée de vie). Assurez-vous que la stratégie correspond aux deux extrémités du tunnel en ce qui concerne l'intégrité, le chiffrement, la fonction pseudo-aléatoire (PRF) et le groupe DH. Choisissez les éléments Algorithm/Group à faire correspondre avec la configuration Azure, puis cliquez sur Add.



Remarque : Vous pouvez référencer ces valeurs exactes dans le fichier de configuration téléchargé sur `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

New IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

SHA256

Cancel Save

Créer une stratégie IKEv2

3) Une fois la configuration terminée, cliquez sur 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

Enregistrer la stratégie IKEv2

4) Configurez les paramètres Phase 2/IPsec dans le sous-menu IKEv2 IPsec Proposal et cliquez sur Add IKEv2 IPsec Proposal.

IKEv2 IPsec Proposal

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can specify the encryption and authentication algorithms. Only the algorithms that are supported by the peers are allowed. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Add IKEv2 IPsec Proposal

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

VPN

- Certificate Map
- Custom Attribute
- Group Policy
- IKEv1 IPsec Proposal
- IKEv1 Policy
- IKEv2 IPsec Proposal**

Créer une proposition IKEv2 IPsec

5) Nommez la proposition IKEv2 IPsec et assurez-vous que les mêmes paramètres sont alignés. Une fois terminé, cliquez sur Enregistrer.

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



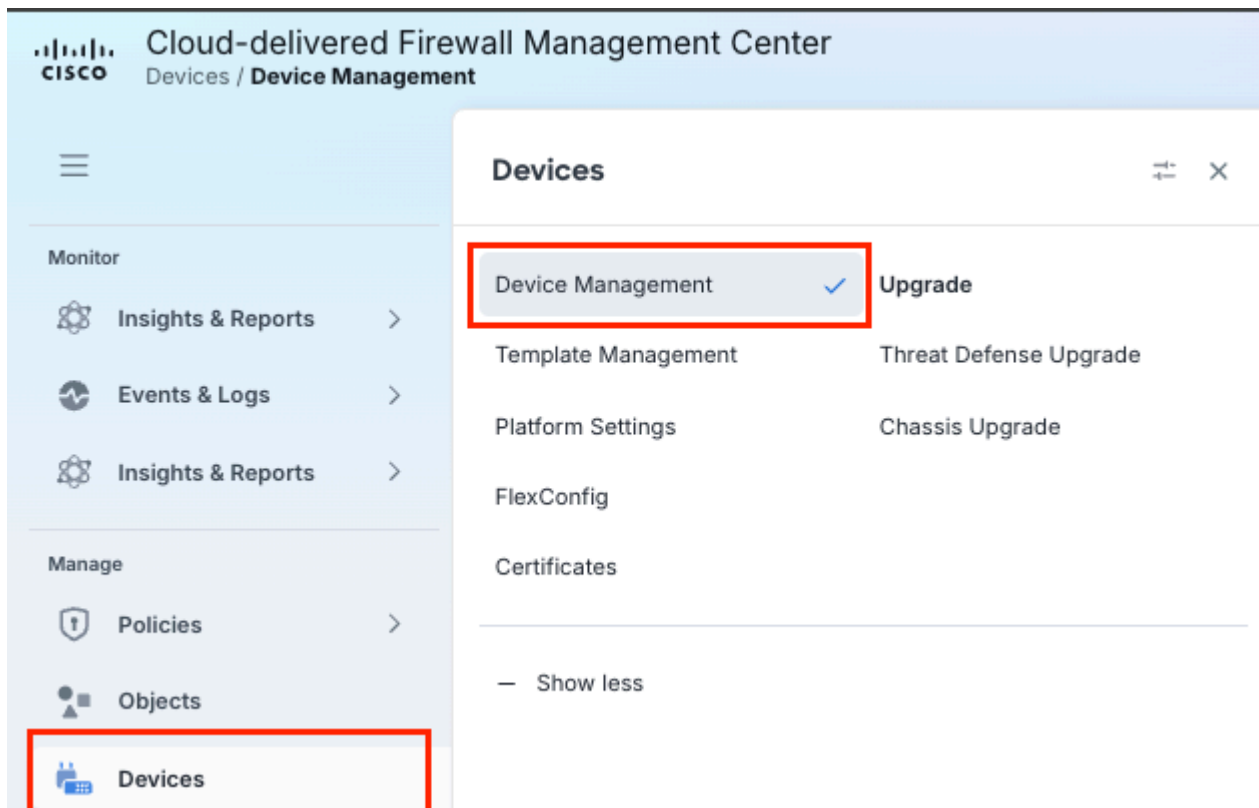
Cancel

Save

Nommez IKEv2 IPsec Proposal, puis cliquez sur Save

Étape 4: Configuration des interfaces de tunnel virtuel (VTI)

1) Accédez à Périphériques > Gestion des périphériques.



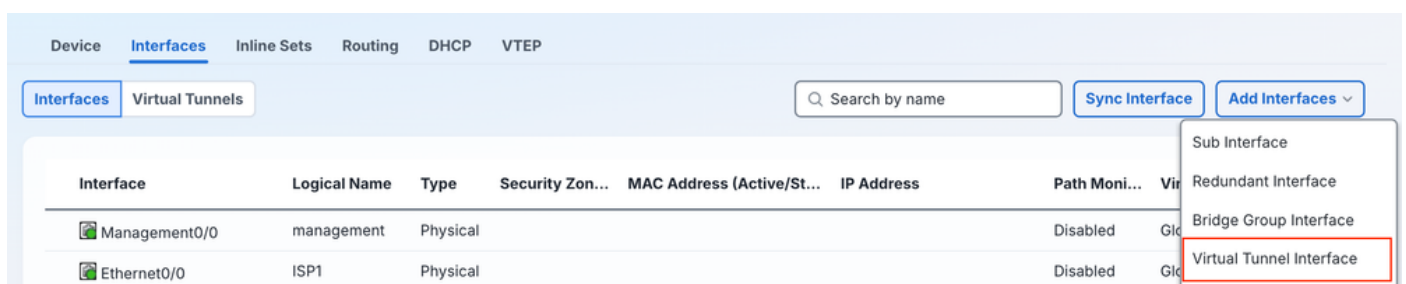
Accédez À Device Management Sur Firepower Management Center

2) Cliquez sur le FTD que vous configurez en tant que périphérique VPN de filiale/site avec une connectivité double FAI.

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

Sélectionnez Le FTD Pour Le Déploiement De La Configuration

3) Cliquez sur le menu déroulant Add Interfaces et choisissez Virtual Tunnel Interface (VTI).



Créer une interface de tunnel virtuel

4) Entrez les informations du tunnel. Assurez-vous que la case Enabled est cochée, que le nom est entré (Description également, si vous le souhaitez) et que la zone de sécurité facultative est sélectionnée. Alignez l'interface parente appropriée orientée ISP pour configurer le VTI sous, et configurez l'adresse IP appropriée pour la connectivité IPsec du tunnel interne pour le VTI. Cliquez sur OK lorsque vous avez terminé.



Conseil : Le schéma de référence présente un contexte supplémentaire sur la configuration VPN potentielle pour la connectivité double WAN Azure avec FTD.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

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

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



Cancel

OK

5) Configurez 3 interfaces VTI supplémentaires sur les interfaces parent ISP1 et ISP2.

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

Configuration d'interfaces de tunnel virtuel supplémentaires

f) Assurez-vous de cliquer sur Save pour enregistrer vos modifications.

You have unsaved changes

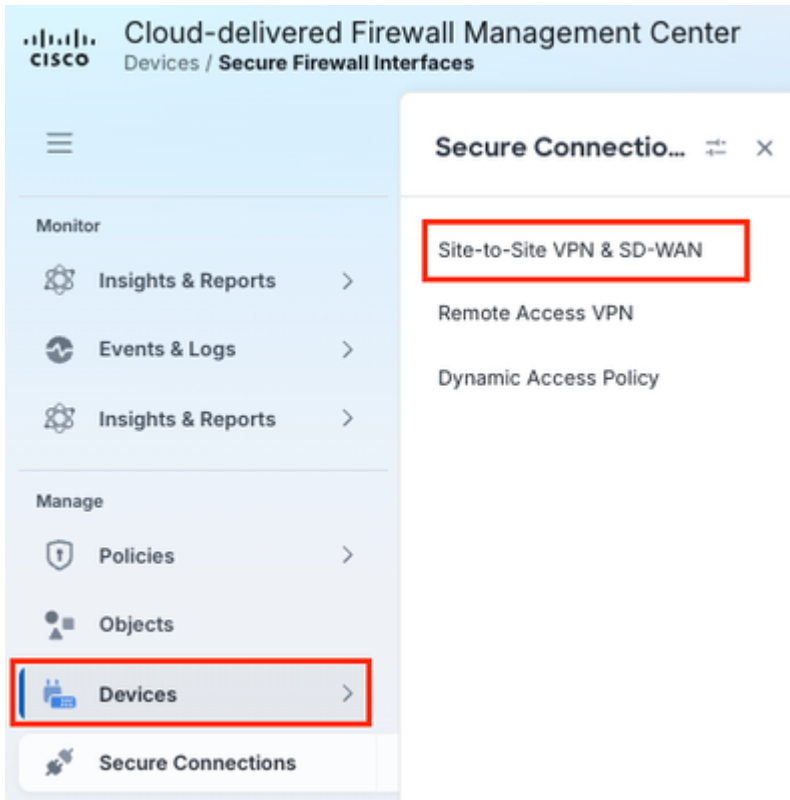
Save

Cancel

Enregistrer les modifications

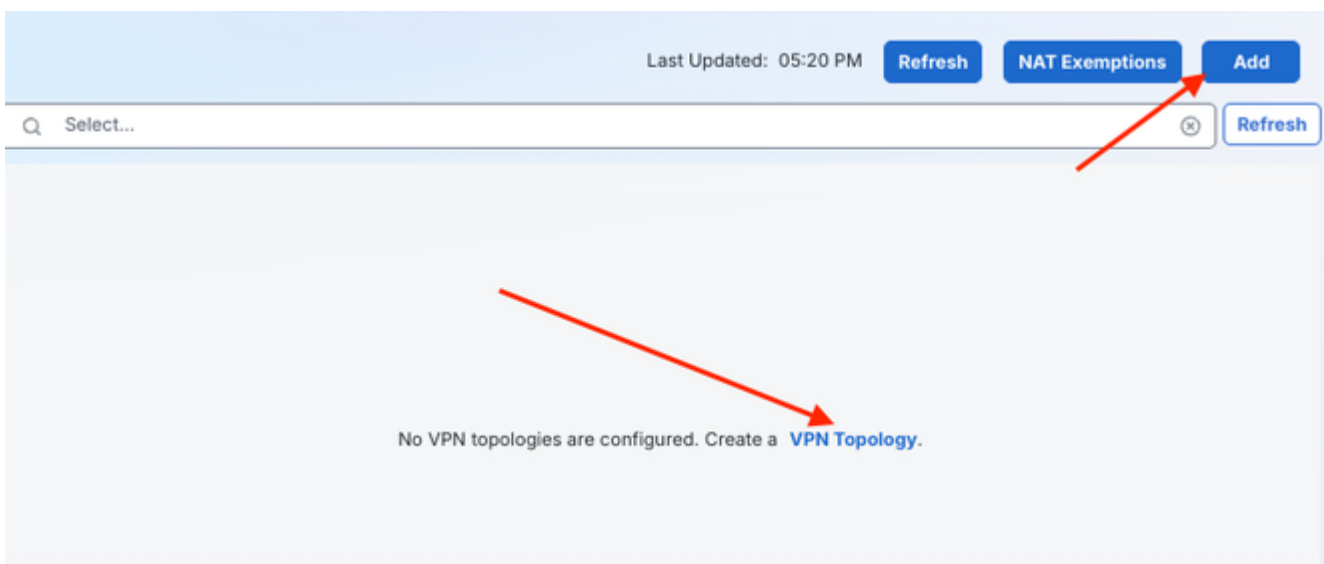
Étape 5: Provisionner des topologies VPN IPsec

1) Accédez à Manage > Secure Connections > Site-to-Site VPN & SD-WAN.



Gérer les connexions VPN site à site et SD-WAN

2) Cliquez sur le lien hypertexte de configuration initiale de la topologie VPN au milieu de la sortie initiale, ou cliquez sur le bouton Add.



Ajouter une nouvelle configuration de topologie VPN

3) Entrez un nom de topologie pour le premier tunnel sur la liaison ISP1 à Azure Instance0. Cliquez sur la case d'option VPN basé sur la route, puis cliquez sur le type de topologie VPN Peer to Peer. Une fois terminé, cliquez sur Créer.

Create VPN Topology

Topology name *

CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

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

Select VPN Topology

☐ Hub and Spoke

[Prerequisites](#)

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

Select VPN Topology

☒ Hub and Spoke

☒ Peer to Peer

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

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

SASE Topology

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

[Prerequisites](#)

[Refresh](#)

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

Configuration du type de topologie VPN basée sur la route

4) Tout d'abord, choisissez le Node A device et sous la liste déroulante Device signifiant le FTD terminant les tunnels VPN à partir d'Azure. Une fois que l'assistant a récupéré les VTI disponibles sur le périphérique, sélectionnez le VTI approprié à l'interface et à l'instance parente que vous configurez dans le menu déroulant. Dans le menu Périphérique du noeud B, choisissez le côté Azure comme noeud Extranet dans la configuration de la topologie VPN. Assurez-vous que vous configurez un nom convivial pour le noeud B, ainsi que de vous assurer d'entrer l'adresse IP du point de terminaison appropriée. Une fois terminé, cliquez sur l'onglet IKE pour implémenter la configuration du tunnel de la Phase 1.



Remarque : Vous pouvez référencer les valeurs d'adresse IP de point de terminaison d'instance dans le fichier de configuration téléchargé à l'adresse `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` et `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](#)

Définition Des Termiaux De Topologie Noeud A Et Noeud B

5) Faites défiler le menu de navigation jusqu'à IKEv2 Settings et cliquez sur l'icône représentant un crayon pour modifier les stratégies de la stratégie IKEv2 récemment configurée. Ensuite, choisissez l'option Pre-shared Manual Key dans le menu déroulant Authentication Type, et entrez le PSK précédemment configuré dans Azure. Une fois terminé, cliquez sur l'onglet IPsec pour configurer les paramètres du tunnel IPsec de phase 2.



Remarque : Vous pouvez référencer la clé pré-partagée dans le fichier de configuration téléchargé sur `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology

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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Azure_IKEv2

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

Modifier les paramètres IKEv2 et la clé d'authentification

6) Cliquez sur l'icône représentant un crayon à côté de l'ensemble de transformation de proposition IPsec IKEv2, et choisissez les paramètres de stratégie IPsec précédemment configurés. Assurez-vous de modifier la valeur Lifetime Duration pour correspondre aux paramètres VPN vWAN Azure. Une fois les informations configurées confirmées, cliquez sur Save.



Remarque : Vous pouvez référencer la valeur Lifetime dans le fichier de configuration téléchargé sur
`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

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

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha Azure_IPsec

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: 27000 Seconds (Range 120-2147483647)

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

Cancel Save

Configuration de la durée de vie de proposition IPsec

7) Répétez les sous-étapes précédentes de l'étape 5 pour créer les autres tunnels Azure sur ISP1 Instance1, ISP2 Instance0 et ISP2 Instance1.

> 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	✓		

Créer des topologies VPN site à site supplémentaires

Étape 6: Valider les topologies VPN

Entrez dans system support diagnostic-cli, tapez en et appuyez sur Entrée (CLI en lecture seule).

1) Vérifiez la connectivité du tunnel IKE Phase 1.

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

2) Vérifiez la connectivité IPsec Phase 2.

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



Remarque : Lors de l'affichage de la sortie des associations de sécurité IPsec et des compteurs de décodage et de décodage des paquets s'incrémentent, mais pas les compteurs de décodage et de chiffrement des paquets, ce qui est attendu dans ce scénario. Azure tente de former des voisins BGP sur les adresses de l'espace IP privé du concentrateur, et Azure n'initie pas de négociation si l'extrémité voisine utilise l'adressage BGP APIPA. Il est de la responsabilité de l'appareil se connectant à Azure d'initier la négociation BGP lorsque l'APIPA personnalisé est utilisé.

3) Vérifiez la connectivité de couche 2.

```
show arp
```

4) Vérifiez le routage IP.

```
show route
```

5) Effectuez la capture sur les interfaces ISP1 et ISP2.

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

6) Vérification Azure - Accédez à vWAN Hub > Connectivity.> VPN Sites > Choisissez le site configuré.

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

Vérification de la connectivité Azure Link

Étape 7: Configurer ECMP

1) Accédez à Manage > Devices > Device Management et cliquez sur le FTD.

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

Accédez À Device Management Sur Firepower Management Center

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

Sélectionnez Le FTD Pour Le Déploiement De La Configuration

2) Cliquez sur l'onglet Routing et choisissez ECMP.

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

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

Paramètres de configuration multi-chemin à coût égal

3) Cliquez sur Add.

Equal-Cost Multipath Routing (ECMP)

Add

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

Ajouter des paramètres de configuration multichemin à coût égal

4) Nommez la zone ECMP, puis cliquez sur les interfaces VTI disponibles, puis cliquez sur le bouton Add pour les appliquer à la colonne Selected Interfaces et cliquez sur OK.

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

Sélectionner Des Interfaces Pour La Zone À Chemins Multiples À Coût Égal

5) Assurez-vous d'enregistrer vos modifications.

You have unsaved changes

Save

Cancel

Enregistrer les modifications

Étape 8: Configurer BGP

1) Activez le processus BGP sur le FTD sous Routing > General Settings > BGP. Cochez la case Enable BGP, et entrez le numéro AS configuré précédemment dans Phase 1, Étape 1d. Naviguez à côté de Routing > BGP > IPv4.

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

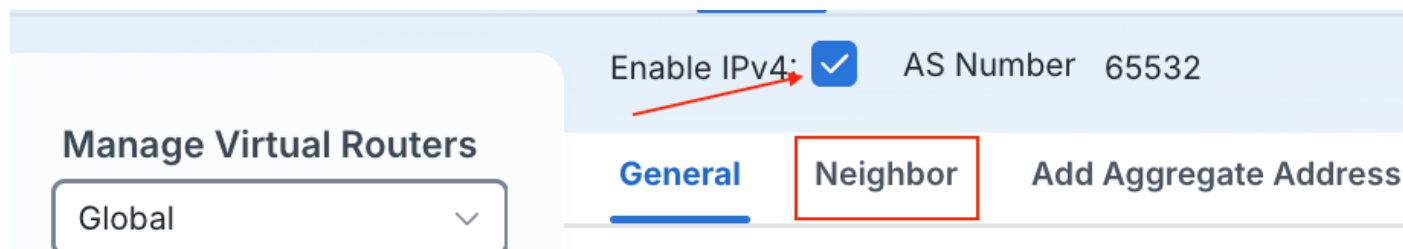
Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

2) Assurez-vous de cocher la case Enable IPv4 pour le processus BGP, et cliquez sur Neighbor pour configurer les voisins BGP dans Azure.



Manage Virtual Routers

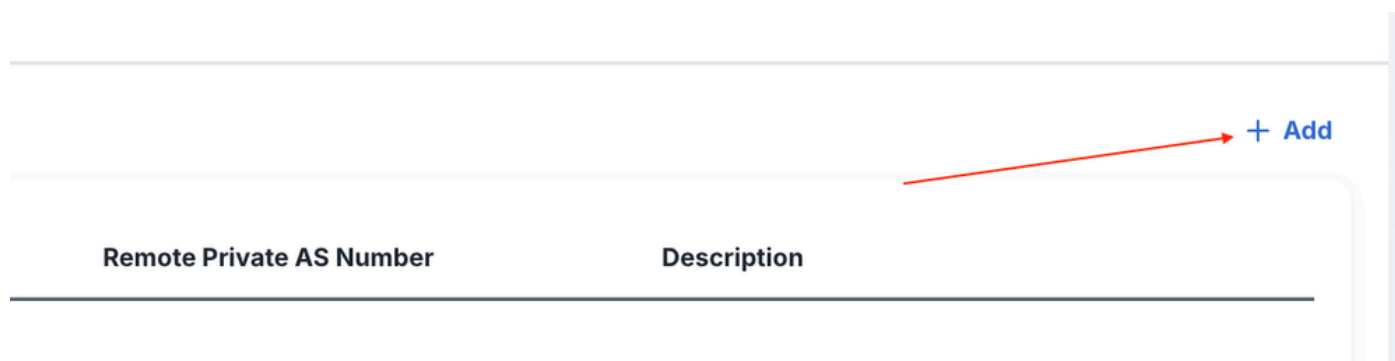
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

Activer le processus de protocole de passerelle de périphérie IPv4

3) Cliquez sur + Ajouter.



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

+ Add

Ajouter un nouveau voisin de protocole Border Gateway

4) Entrez les informations d'appairage BGP de l'instance 0 du routeur ISP1, référez le système autonome BGP noté à partir du concentrateur vWAN et entrez-le comme système autonome distant voisin, et ajoutez une description si vous le souhaitez. Cliquez sur Avancé.



Remarque : Assurez-vous que vous choisissiez la source de mise à jour BGP pour référencer le bouclage pour les interfaces VTI sur le FTD mappé à la liaison ISP1 configurée dans Azure.

Add Neighbor ?

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Configurer les informations d'appairage du protocole BGP

5) Dans le menu Advanced de la configuration de voisin BGP sur FTD, vous pouvez changer le nombre de sauts de durée de vie (TTL) de la valeur par défaut d'eBGP de 1 saut à un nombre variable. Les points de terminaison Azure BGP ne sont pas directement connectés via le tunnel à l'infrastructure Azure, et il y a généralement plus de sauts vers le point de terminaison que le TTL eBGP par défaut de 1 ne l'autorise. Click OK.

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Paramètres avancés du voisin Border Gateway Protocol

6) Répétez les sous-étapes 3 à 5 pour configurer Tunnel2 pour ISP1 Instance1.

7) Répétez les sous-étapes 3 à 5 deux fois pour configurer les informations d'appairage BGP Instance0/Instance1 d'ISP2.



Remarque : Assurez-vous que vous choisissez la source de mise à jour BGP alignée faisant référence au bouclage pour les interfaces VTI sur le FTD mappé à la liaison ISP2 configurée dans Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

Configuration du voisin BGP de l'instance 1 du FAI2

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

Configuration du voisin BGP de l'instance 2 du FAI

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		

Fin de la configuration des résultats du voisin BGP

Une fois terminé, cliquez sur Save.

You have unsaved changes

Save

Enregistrer les modifications

Par défaut, BGP installe seulement un meilleur chemin unique dans la table de routage, même si ECMP est configuré sur tous les VTI vers Azure. Le multichemin BGP doit être activé séparément afin que les deux chemins appris soient installés et utilisés en même temps.

Étape 9: Configurer le multichemin eBGP

1) Accédez à Routing > BGP > IPv4, cliquez sur l'onglet General , et cliquez sur l'icône de crayon adjacente à Forward Packets Over Multiple Paths.

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

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

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

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

Paramètre de transfert de paquets sur plusieurs chemins

2) Modifiez la valeur par défaut du champ Nombre de chemins de 1 à 4. Cliquez sur OK.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Modification du paramètre Transférer les paquets sur plusieurs chemins

3) Assurez-vous d'enregistrer et de déployer les modifications.

Vérification/dépannage

Une fois le déploiement terminé, vérifiez que le processus BGP FTD établit des contiguïtés de voisinage avec les deux instances Azure sur les tunnels respectifs, et que les routes sont apprises, que les interfaces sont actives et que les connexions de protocole sont renvoyées dans la table de connexion.

Accédez à l' `system support diagnostic-cli` interface de ligne de commande FTD comme indiqué à l'étape 7 de la Phase 2.

1) Une fois déployés, les voisins BGP sont supposés apparaître et des préfixes sont reçus.

```
<#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) Vérifiez que les routes reçues d'Azure s'affichent en tant que routes multichemins.

```
<#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) Vérifiez le remplissage de la table de routage.

```
<#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) Vérifiez la table de connexion pour les sessions BGP.

<#root>

ftd#

show conn all | include TCP|179

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.