

Configurer le VPN site à site Azure vWAN pour sécuriser le pare-feu

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme](#)

[Connectivité vWAN de liaison DIA unique entre Azure et FTD \(équilibrage de charge/redondance Azure\)](#)

[Configurer](#)

[Phase 1 : Configuration du vWAN/concentrateur Azure](#)

[Étape 1: Créer vWAN](#)

[Étape 2: Créer un concentrateur vWAN](#)

[Phase 2 : Configuration du site VPN vWAN Azure](#)

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

[Étape 2: Configurer les paramètres VPN du site vWAN Azure](#)

[Étape 3: Télécharger la configuration du tunnel du site vWAN Azure](#)

[Phase 3 : Configuration FTD](#)

[Étape 1: Analyser la configuration VPN Azure](#)

[Étape 2: Configurer le bouclage](#)

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

[Étape 4: Configurer la connectivité sécurisée vers Azure](#)

[Étape 5: Vérification de la connectivité initiale à Azure](#)

[Étape 6: Configurer le deuxième tunnel vers le point de terminaison Azure Instance1](#)

[Étape 7: Configurer ECMP](#)

[Étape 8: Configuration des routes statiques pour l'instance des adresses IP privées](#)

[Étape 9: Configurer BGP](#)

[Étape 10: Configurer le multichemin BGP](#)

[Vérifier](#)

[Autres considérations](#)

[AS-Path Prepending](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration de la connectivité VPN site à site de Microsoft Azure Virtual WAN (vWAN) à Cisco Secure Firewall.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

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

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

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

Microsoft Azure Virtual WAN (vWAN) combine plusieurs fonctionnalités Azure de mise en réseau, de sécurité et de routage derrière une seule structure de concentrateur. Chaque concentrateur vWAN peut héberger une passerelle VPN site à site gérée par Microsoft et utilisée par les périphériques distants, tels que Secure Firewall, pour accéder à Azure sans avoir à créer et à gérer l'infrastructure de passerelle.

Contrairement à un VPN IPsec classique à deux points de terminaison, la passerelle VPN site à site Azure vWAN se déploie en tant que paire active-active d'instances (Instance0 et Instance1), chacune avec sa propre adresse IP publique et son adresse d'appairage BGP (Border Gateway Protocol). Pour tirer parti des deux instances pour la redondance et le débit supplémentaire, le FTD de branche établit un tunnel de sécurité IP (IPsec) vers chaque instance et utilise le protocole BGP, plutôt que le routage statique seul, pour apprendre et retirer dynamiquement les routes lorsque les instances deviennent disponibles ou indisponibles. Le routage ECMP (Equal-Cost

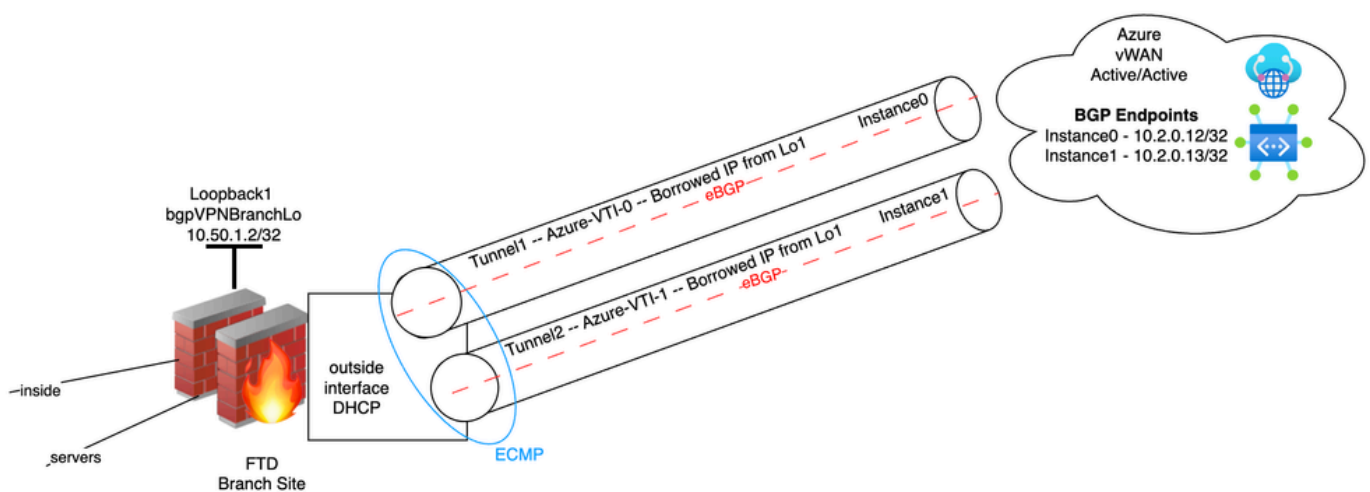
Multi-Path) et le routage multichemin BGP sur le FTD maintiennent alors les deux tunnels actifs en même temps, au lieu de traiter l'un d'entre eux comme une veille passive.

Ce document configure cette conception en trois phases : Les objets Azure vWAN Hub et VPN Site sont d'abord créés, les paramètres de connexion résultants sont téléchargés, puis ces mêmes paramètres sont utilisés pour configurer les interfaces de tunnel virtuel (VTI) correspondantes, les stratégies IKEv2 (Internet Key Exchange Version 2)/IPsec, les routes statiques, ECMP et l'appairage BGP sur le FTD via FMC.

Diagramme

Le schéma illustre la topologie de la configuration décrite dans cet article. La variante d'accès direct à Internet (DIA) source les deux tunnels Azure à partir d'une interface externe sur le FTD.

Connectivité vWAN de liaison DIA unique entre Azure et FTD (équilibre de charge/redondance Azure)



Configurer

Réalisez les trois phases dans l'ordre. Les objets côté Azure créés dans les phases 1 et 2 produisent les adresses IP homologues, les numéros de système autonome BGP et la clé pré-partagée que la phase 3 applique ensuite au FTD.

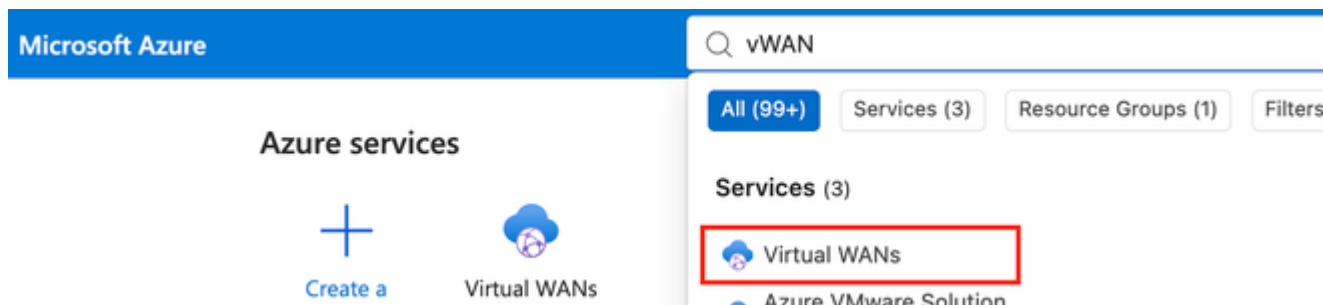
Phase 1 : Configuration du vWAN/concentrateur Azure



Remarque : Les étapes de configuration de ce document sont de haut niveau et fournissent les étapes nécessaires pour connecter le FTD à Azure vWAN. Reportez-vous à la documentation Azure vWAN de Microsoft pour comprendre l'importance des configurations. Voir [Qu'est-ce que le WAN virtuel Azure ?](#) et d'autres documents.

Étape 1: Créer vWAN

a) Recherchez vWAN dans la zone de recherche Azure, cliquez sur Virtual WAN.



b) Cliquez sur + Créer.



c) Entrez un nom pour la nouvelle instance vWAN, cliquez sur Vérifier + créer, puis cliquez sur Créer sur la page Vérifier + Créer de l'assistant.

Create WAN ...

Basics Review + create

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

Project details

Subscription *

Resource group *

[Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >



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

d) Cliquez sur Accéder à la ressource.



VirtualWanDeployment | Overview

Deployment



Delete



Cancel



Redeploy



Download



Refresh

Overview

Inputs

Outputs

Template



Your deployment is complete



Deployment name : VirtualWanDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

Étape 2: Créer un concentrateur vWAN

a) Accédez à Connectivity > Hubs et cliquez sur + New Hub.

CX-vWAN | Hubs

Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub	Hub status	Region
No results		

b) Reportez-vous à la documentation Azure pour obtenir plus d'informations sur la configuration future. Assurez-vous que l'espace d'adressage privé de votre concentrateur alloué ne chevauche aucun de vos espaces d'adressage internes. Configurez le nom, le concentrateur virtuel, la préférence de routage du concentrateur. Cliquez sur Suivant : Site à site >.

Home > CX-vWAN | Hubs

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). [Learn more](#)

Project details

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

Subscription

Resource group

Virtual Hub Details

Region *

Name * ✓

Hub private address space * ⓘ ✓

Virtual hub capacity * ⓘ

Hub routing preference * ⓘ

i Creating a hub with a gateway will take 30 minutes.

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

c) Pour plus d'informations sur les champs présentés, reportez-vous à la documentation du vWAN Hub Microsoft Azure. Sélectionnez Oui pour créer un site à site (passerelle VPN). Le numéro de système autonome BGP (AS) par défaut attribué est 65515, comme attribué par l'IETF (Internet Engineering Task Force) dans la RFC 6996 définissant la réservation AS d'utilisation privée.



Remarque : Enregistrez le système autonome BGP pour les étapes de configuration futures sur le FMC.

Create virtual hub ...

Basics Site to site Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

☒ Yes☐ No

Copied

AS Number

65515

Gateway scale units

Routing preference

☒ Microsoft network ☐ Internet

Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

Next : Point to site >

Cliquez sur Vérifier + créer, ou cliquez sur Suivant : Pointez vers site > pour configurer les paramètres facultatifs.

d) Une fois le résumé vérifié, cliquez sur Create (Créer).



Remarque : Comme l'indique Azure, la création du concentrateur prend 30 minutes.

Create virtual hub ...

✓ Validation passed

Basics Site to site Point to site ExpressRoute Tags **Review + create**

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

Basics

Region
Name CX-vWAN-Hub
Hub private address space 10.2.0.0/16
Virtual hub capacity
Hub routing preference

Site to site

Site to site (VPN gateway) Enabled
AS Number 65515
Gateway scale units

Point to site

Point to site (VPN gateway)

ExpressRoute

ExpressRoute gateway

Tags

i Creating a hub with a gateway will take 30 minutes.

Create

Previous

Next

[Download a template for automation](#)

e) Une fois le déploiement terminé, recherchez votre nom de ressource vWAN d'origine. Pour affiner votre recherche, cliquez sur Ressources.

VirtualHubDeployment | Overview ...

Deployment

Search x << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

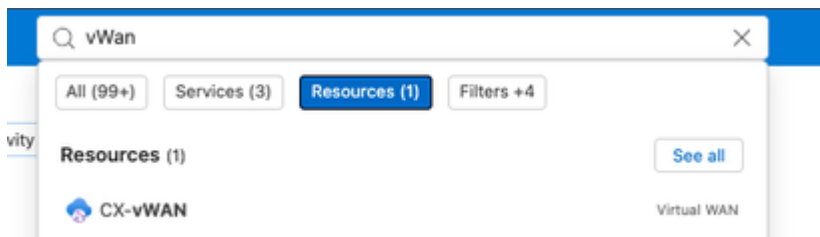
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

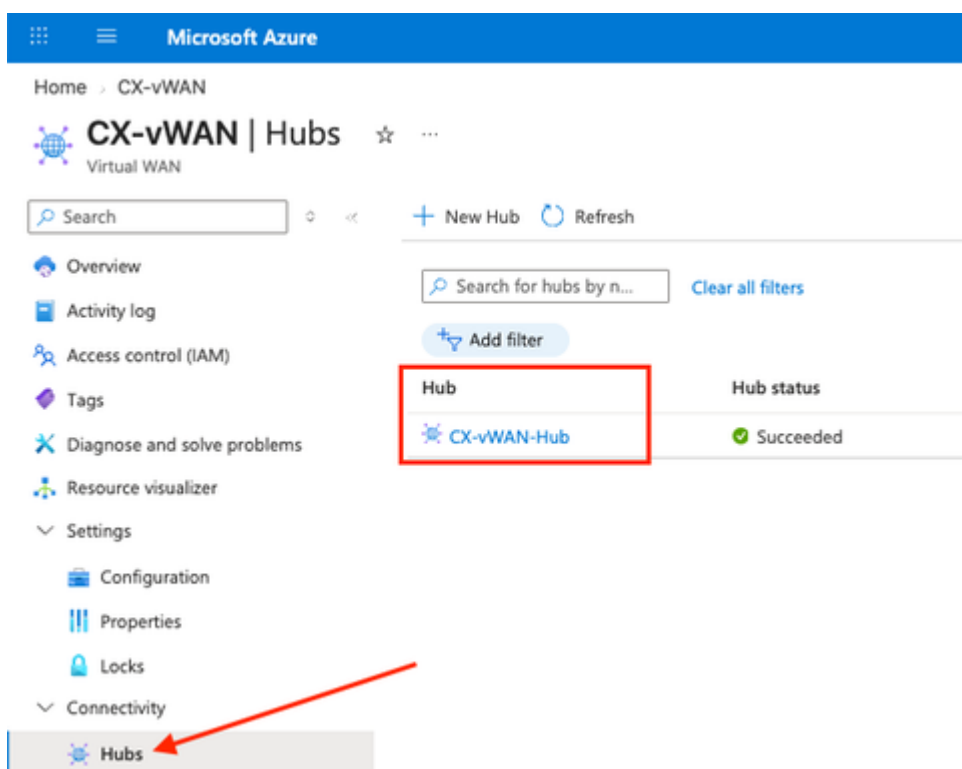
[Go to resource](#)



Phase 2 : Configuration du site VPN vWAN Azure

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

a) Accédez au concentrateur créé via Connectivity > Hubs et cliquez sur le concentrateur créé dans les étapes précédentes.



b) 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		

c) Saisissez 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 *

Device vendor *

Private address space

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

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

Previous

Next : Links >

d) Entrez les informations de liaison requises. Les champs Link BGP Address et Link ASN reflètent l'adresse de destination BGP de couche 3 du tunnel interne et le numéro de système autonome BGP sur le site de filiale avec lequel le voisinage avec Azure 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 précédemment configuré, qu'Azure installe en tant que route /32 à atteindre en tant que voisin BGP. L'adresse IP de liaison/nom de domaine complet est l'adresse IP de destination de couche 3 de l'en-tête externe du trafic allant au site de la succursale nécessaire pour fournir la connectivité IPsec/IKEv2.



Remarque : Si vous utilisez des adresses comprises entre 169.254.21.0 et 169.254.22.255 pour les adresses de tunnel, vérifiez [Comment configurer BGP pour Azure VPN Gateway](#) pour des exigences spécifiques.

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

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

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

Previous

Next : Review + create >

e) Après avoir vérifié que les paramètres sont corrects, 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

Name VPN-Site

Device vendor Cisco

Private address space

Links

Link name	single-dia-link
Link provider name	provider
Link speed	1000
Link IP address / FQDN	
Link ASN	65500
Link BGP address	169.254.10.2

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

Create

Previous

Next

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

Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

Go to resource

Search vWan

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

Resources (1)

See all

CX-vWAN Virtual WAN

Étape 2: Configurer les paramètres VPN du site vWAN Azure

a) Accédez au concentrateur créé via Connectivity > Hubs et cliquez sur le concentrateur créé dans les étapes précédentes.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Configuration
Properties
Locks
Connectivity
Hubs

Search for hubs by n... Clear all filters

+ Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded



b) Accédez de nouveau à Connectivity > VPN (Site to site) et cliquez sur le X pour effacer l'association de concentrateur : Filtrage connecté pour afficher les sites déconnectés.

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview
Connectivity
VPN (Site to site)
ExpressRoute
User VPN (Point to site)
Routing
Security
Third party providers
Monitor

Essentials

Gateway configuration
NAT Rules

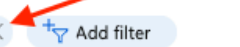
VPN Sites Metrics

Search this page Clear all filters

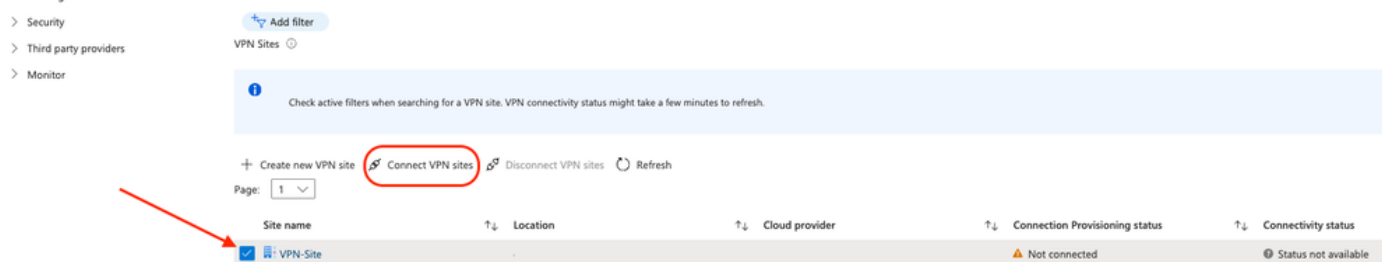
Hub association : **Connected** X + Add filter

VPN Sites ⓘ

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



c) Cochez la case en regard du site VPN précédemment configuré, puis cliquez sur Connect VPN sites, qui devient activé une fois le site sélectionné.



d) Le panneau du tiroir latéral Connecter les sites s'affiche. Saisissez une clé prépartagée (PSK) et configurez les paramètres IKEv2 et IPsec de phase 2 souhaités. Lorsque vous choisissez Custom dans la liste déroulante IPsec, les valeurs sont automatiquement renseignées ; notez ces valeurs, car elles doivent correspondre sur le FTD. Vous devez également choisir si le protocole PFS (Perfect Forward Secrecy) est souhaité. Comme il s'agit d'un tunnel basé sur la route, configurez les paramètres en conséquence. Une fois terminé, cliquez sur Connect pour enregistrer la configuration.



Remarque : Voir [Stratégies IPsec par défaut et personnalisées Azure vWAN](#) pour plus d'informations.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

i When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup24

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

These sites will be connected to the [CX-vWAN-Hub] hub.

Site name



Region



VPN-Site

eastus

Connect

e) Des informations indiquant que la passerelle est en cours de mise à jour s'affichent, ainsi que le temps estimé jusqu'à son achèvement.

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site) ⓘ ...
Virtual HUB

Search



Download VPN Config



Packet Capture



Delete gateway



Reset gateway



Monitor Gateway

Overview

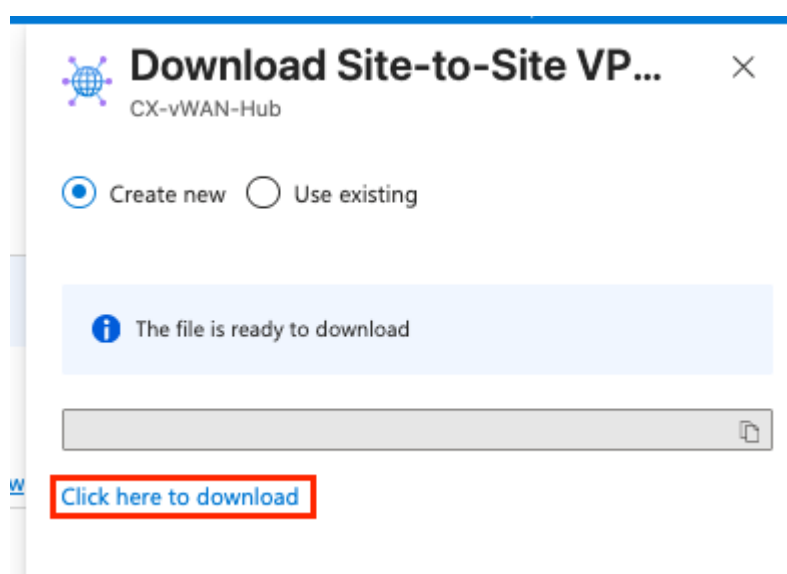
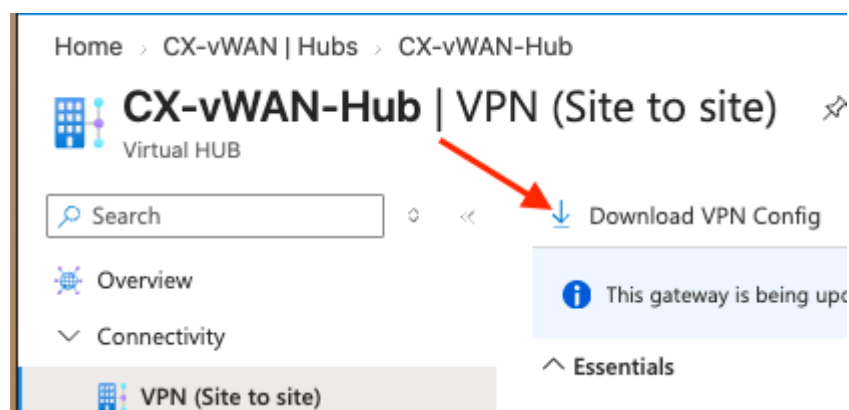
Connectivity



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

Étape 3: Télécharger la configuration du tunnel du site vWAN Azure

a) Pendant la mise à jour de la passerelle, vous pouvez télécharger la configuration VPN.



Une fois le site VPN créé et ses paramètres de connexion (adresses d'homologues, numéros de système autonome BGP et PSK) téléchargés, les mêmes valeurs sont utilisées pour configurer les éléments correspondants sur le FTD dans la phase 3.

Phase 3 : Configuration FTD

Étape 1: Analyser la configuration VPN Azure

a) Ouvrez le fichier de configuration VPN téléchargé à partir d'Azure. Il ressemble à la sortie condensée affichée et fournit des informations utiles :



Remarque : Pour améliorer la mise au point, plusieurs objets non pertinents et paires

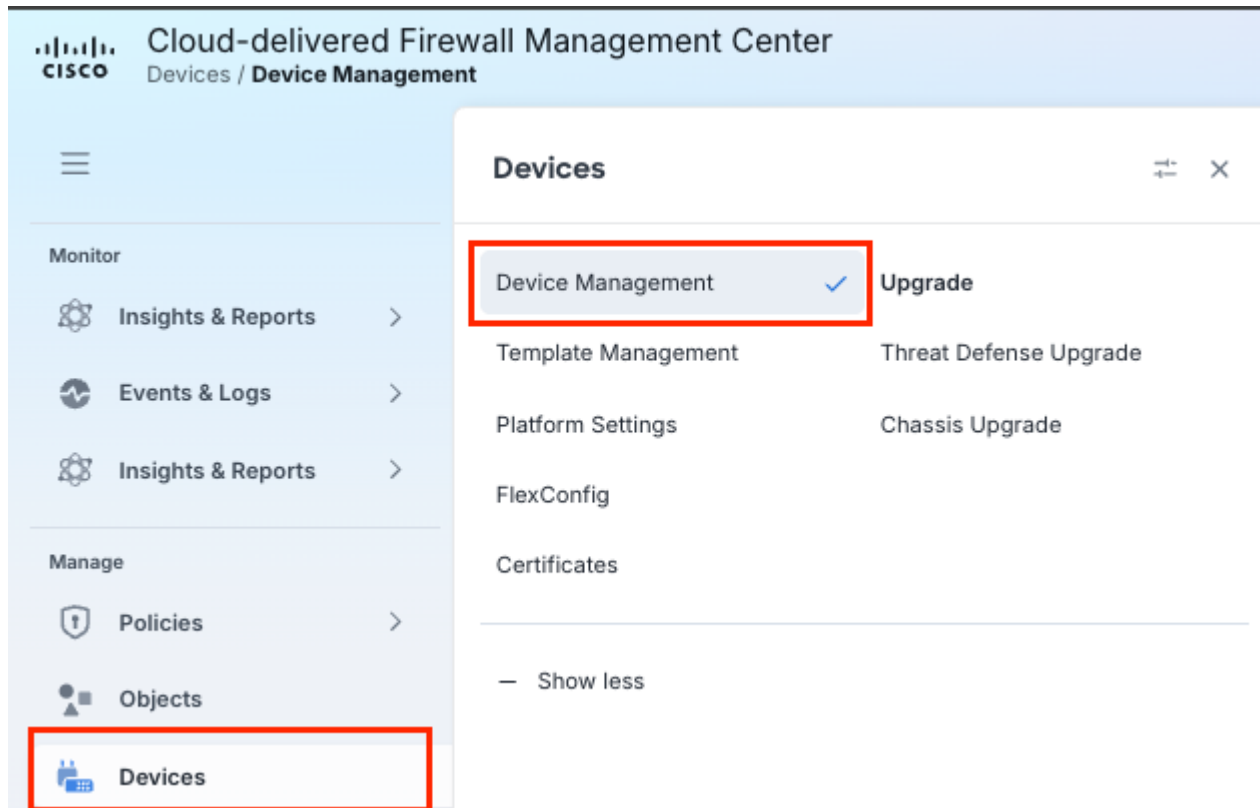
clé/valeur sont élagués pour plus de concision.

```
[
{
  "configurationVersion": {
    "LastUpdateTime": "<Last Update Time>",
    "Version": "<Version UUID>"
  },
  "vpnSiteConfiguration": {
    "Name": "VPN-Site",
    "IPAddress": "<FTD public IP address>",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "Region": "<Azure Region>"
      },
      "gatewayConfiguration": {
        "IpAddresses": {
          "Instance0": "57.x.x.x",
          "Instance1": "52.x.x.x"
        },
        "BgpSetting": {
          "Asn": 65515,
          "BgpPeeringAddresses": {
            "Instance0": "10.2.0.12",
            "Instance1": "10.2.0.13"
          }
        }
      }
    },
    {
      "connectionConfiguration": {
        "IsBgpEnabled": true,
        "PSK": "<IPSec PSK>",
        "IPsecParameters": {
          "IpsecEncryption": "GCMAES256",
          "IpsecIntegrity": "GCMAES256",
          "IkeEncryption": "GCMAES256",
          "IkeIntegrity": "SHA384",
          "PfsGroup": "None",
          "DhGroup": "DHGroup14",
          "SADataSizeInKilobytes": 0,
          "SALifeTimeInSeconds": 27000
        }
      }
    }
  ]
}
]
```

Étape 2: Configurer le bouclage

Chaque VTI configurée ultérieurement a besoin d'une source de tunnel stable, de sorte qu'une interface de bouclage est configurée en premier et partagée entre les deux VTI.

a) Accédez à Périphériques > Gestion des périphériques.

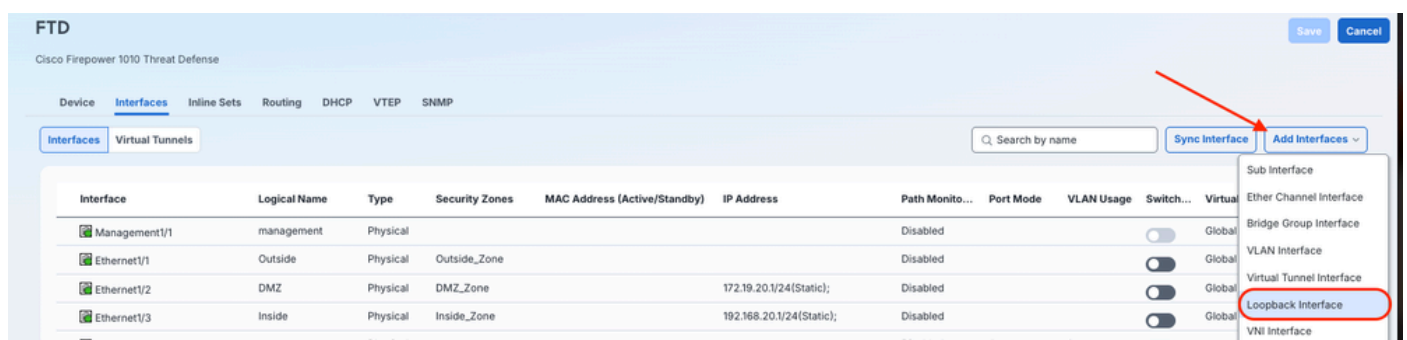


Remarque : Ces travaux pratiques utilisent le centre de gestion des pare-feu (cdFMC) fourni dans le cloud ; toutefois, les étapes restent les mêmes pour le FMC sur site.

b) Sélectionnez le FTD que vous configurez en tant que périphérique VPN de filiale/site.



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



d) Donnez à l'interface de bouclage son nom, son ID de bouclage et sa description si nécessaire. Cliquez sur IPv4.

Add Loopback Interface

General **IPv4** IPv6

Name:

☒ Enabled

Loopback ID: *

(1-1024)

Description

Cancel OK

e) Assurez-vous que le type d'IP est défini comme Use Static IP, entrez l'adresse BGP de liaison telle que configurée à l'étape 1d de la Phase 2. Vous pouvez faire référence à la valeur précédemment définie dans la configuration VPN JSON téléchargée

SOUS `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Remarque : Définissez l'adresse avec un masque /32 et dans l'espace d'adressage RFC 1918.

Add Loopback Interface

General **IPv4** IPv6

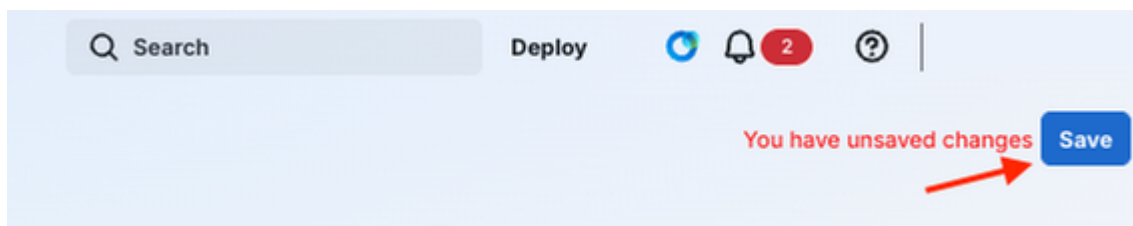
IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

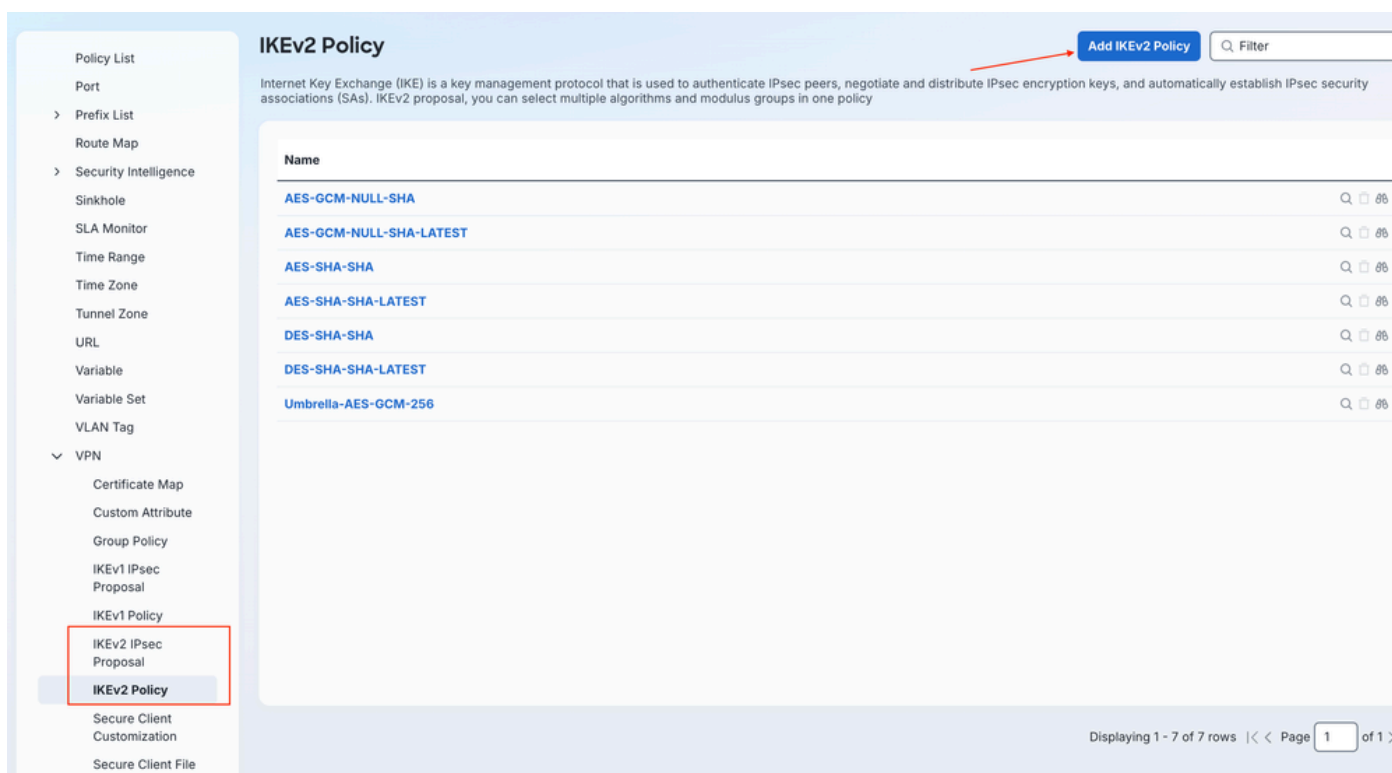
Cancel OK

f) Cliquez sur Enregistrer



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

a) Pour configurer la configuration IKEv2/IPsec correspondante sur le FMC à appliquer dans les topologies VPN FTD, accédez à Manage > Objects, faites défiler le menu de gauche vers 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.



b) 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 le groupe Integrity, Encryption, PRF, et Diffie-Hellman (DH). Choisissez les éléments d'algorithme/groupe alignés à faire correspondre avec la configuration Azure, puis cliquez sur Ajouter.



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

Available Algorithms

MD5

SHA

SHA512

SHA384

NULL

Selected Algorithms

SHA256 

c) Une fois la configuration terminée, cliquez sur Save.

Edit IKEv2 Policy



Name:*

Azure_IKEv2

Description:

Priority:*

(1-65535)

5

Lifetime:

seconds (120-2147483647)

3600

Available Groups

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

1
2
5
14
15
16
19
20
...

Add

Selected Groups

14



Cancel

Save

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

Policy List

Port

> Prefix List

Route Map

> Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

URL

Variable

Variable Set

VLAN Tag

VPN

 Certificate Map

 Custom Attribute

 Group Policy

 IKEv1 IPsec Proposal

 IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 IPsec Proposal

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. 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

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



Remarque : Vous pouvez référencer ces valeurs dans votre fichier de configuration téléchargé à l'adresse `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256

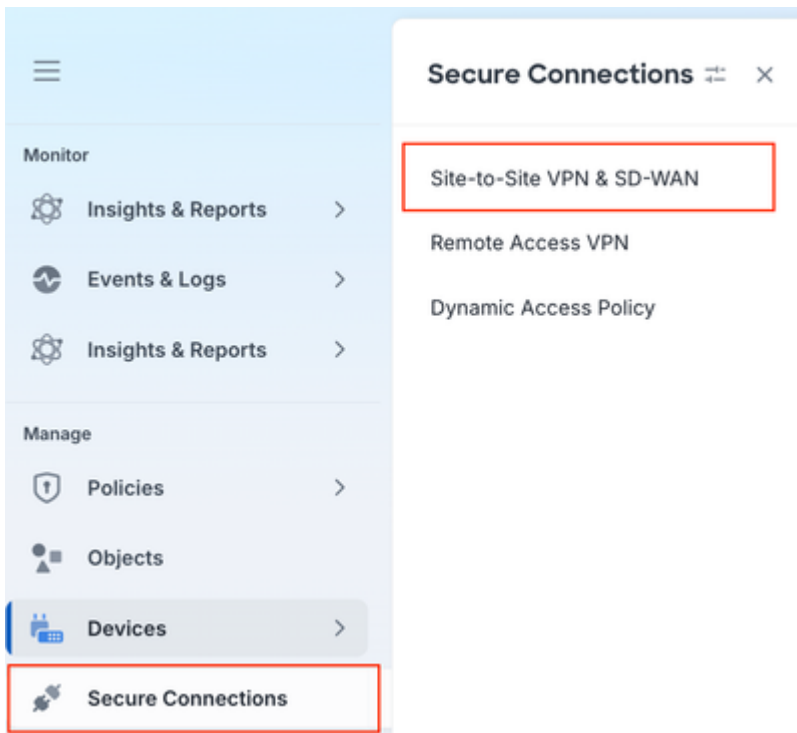


Cancel

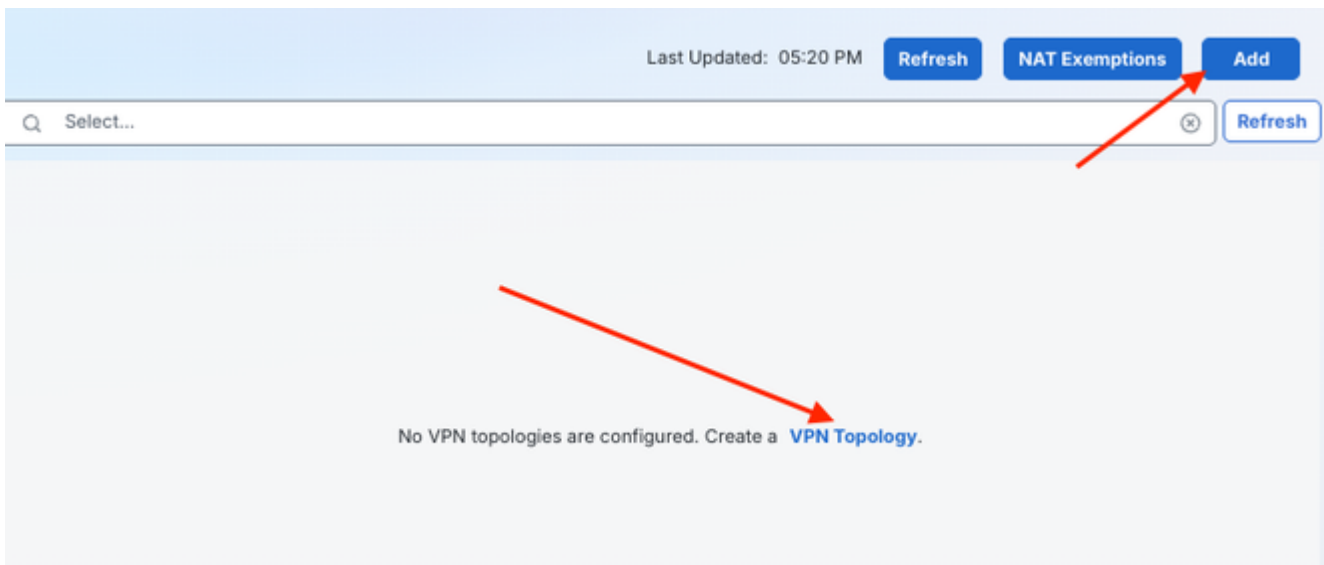
Save

Étape 4: Configurer la connectivité sécurisée vers Azure

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



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



c) Entrez un nom de topologie pour le premier tunnel vers 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 *

Azure-VTI-Instance0

VPN Type

☐ SD-WAN Topology

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

Select VPN Topology

☐ Hub and Spoke

Prerequisites

☒ **Route-Based VPN**

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

Select VPN Topology

☐ Hub and Spoke

☒ **Peer to Peer**

☐ Policy-Based VPN

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

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

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

[Prerequisites](#)

[Refresh](#)

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

d) Pour le noeud A, cliquez sur la liste déroulante Device et choisissez le nom de la paire HA FTD/FTD gérée vers laquelle la configuration est déployée. Pour le noeud B, car il s'agit de l'extrémité distante de la connexion dans la topologie se terminant sur des instances vWAN Azure, choisissez Extranet dans la liste déroulante Device. Ensuite, pour le noeud A, cliquez sur l'icône + en regard de la liste déroulante Virtual Tunnel Interface (VTI).

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

[Point to Point](#) [Hub and Spoke](#) [Full Mesh](#)

IKE Version:*

☐ IKEv1 ☒ **IKEv2**

[Endpoints](#) [IKE](#) [IPsec](#) [Advanced](#)

Node A

Device:*

FTD

Virtual Tunnel Interface:*

[+](#)

☐ Tunnel Source IP is Private [Edit VTI](#)

☐ Send Local Identity to Peers

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

[> Advanced Settings](#)

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

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

e) Attribuez un nom à la première interface VTI et assurez-vous qu'elle est activée. Attribuez une zone de sécurité nouvelle ou existante au VTI, attribuez la source de tunnel, et choisissez l'adresse IP dans la liste déroulante adjacente.

Add Virtual Tunnel Interface ?

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Azure-VTI-0

☒ Enabled

Description:

Security Zone:
Azure-Spoke-Zone

Priority:
0 (0 - 65535)

Propagate Security Group Tag: ☒

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

Tunnel ID:*
1 (0 - 10413)

Tunnel Source:*
Ethernet1/1 (Outside) Dynamic

The screenshot shows the 'Add Virtual Tunnel Interface' configuration page. Red arrows point to the following fields: 'Name' (set to 'Azure-VTI-0'), 'Security Zone' (set to 'Azure-Spoke-Zone'), 'Tunnel ID' (set to '1'), 'Tunnel Source' (set to 'Ethernet1/1 (Outside)'), and the 'Dynamic' option in the 'Tunnel Source' dropdown.

f) Vérifiez ensuite que la case d'option Borrow IP (IP unnumbered) est sélectionnée, puis choisissez le même bouclage dans la liste déroulante de droite. Cliquez sur OK une fois terminé.

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

Tunnel ID:*
 (0 - 10413)

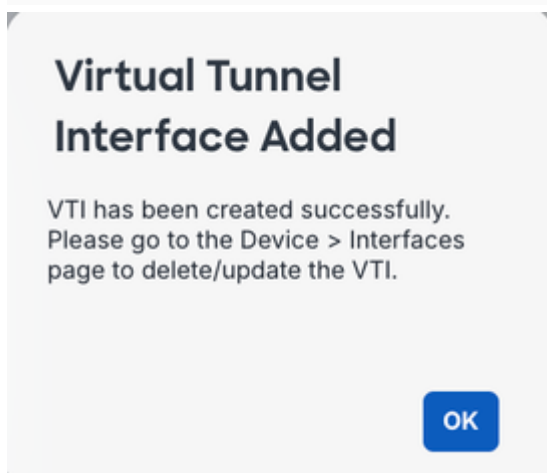
Tunnel Source:*

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

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

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

Cancel OK



g) Une fois la VTI configurée et appliquée, renseignez manuellement l'adresse IP source du tunnel (elle est automatiquement renseignée si l'adresse de l'interface parente est renseignée à partir de DHCP), et assurez-vous que le nom du périphérique Node B est configuré, ainsi que l'adresse IP du point de terminaison de l'instance. Une fois terminé, cliquez sur l'onglet IKE.



Remarque : Vous pouvez référencer la valeur d'adresse IP du point d'extrémité Instance0 dans le fichier de configuration téléchargé à l'adresse `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:* ?

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

h) Faites défiler jusqu'à IKEv2 Settings et vérifiez que le type d'authentification est défini sur Pre-shared Manual Key, et entrez le PSK configuré dans Azure dans les étapes précédentes. Configurez les stratégies IKEv2 Phase 1 en cliquant sur l'icône représentant un crayon pour modifier les stratégies IKEv2 disponibles.



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

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

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

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

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

i) Ajoutez la stratégie IKEv2 Phase 1 configurée initialement à l'étape 3.

IKEv2 Policy



Available IKEv2 Policy  

 Search

AES-GCM-NUL-
AES-GCM-NUL-SHA-LAT...
AES-SHA-SHA
AES-SHA-SHA-LATEST
Azure_IKEv2
DES-SHA-SHA
DES-SHA-SHA-LATEST

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

j) Sélectionnez l'onglet IPsec.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐

IKEv1

☒

IKEv2

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Azure_IKEv2



Authentication Type:

Pre-shared Manual Key



Key:*

.....

Confirm Key:*

.....

☐

Enforce hex-based pre-shared key only

k) Modifiez la proposition IKEv2 IPsec sous Transform Sets en cliquant sur l'icône du crayon.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

l) Cliquez sur l'icône de la corbeille pour supprimer l'ensemble de transformation AES-GCM par défaut et ajouter l'ensemble de transformation Azure_IPsec personnalisé/IKEv2 IPsec Proposal créé dans la seconde moitié de l'étape 3. Cliquez sur OK.

IKEv2 IPsec Proposal



Available Transform Sets  +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec 

Cancel

OK

m) Faites défiler vers le bas et entrez 27 000 pour la durée de vie correspondant aux paramètres Azure. Activez le groupe PFS si applicable. Cliquez sur Save.



Remarque : Vous pouvez référencer la valeur de durée de vie dans le fichier de configuration téléchargé à

l'adresse `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

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

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

> ESPv3 Settings

Cancel Save

n) Déployez les modifications.

Search Deploy

Search Device Advanced Deploy Deploy All

☐ FTD

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

o) Une fois le déploiement terminé, cochez la case Manage > Secure Connections > Site-to-Site VPN & SD-WAN sous Tunnel Status Distribution ; une connectivité réussie reflète l'état Vert (haut).

Last Updated: 11:11 PM Refresh NAT Exemptions Add					
Q Select... Refresh					
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✎ ✕

Une fois le premier tunnel déployé, vérifiez qu'il s'établit correctement au niveau des couches IKE/IPsec et BGP avant de configurer le second tunnel pour la redondance.

Étape 5: Vérification de la connectivité initiale à Azure

a) Connectez SSH au FTD et saisissez `system support diagnostic-cli`, tapez `en`, puis appuyez sur Entrée, car l'interface de ligne de commande du FTD en lecture seule ne contient pas de mot de passe.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftd>
```

```
en
```

```
Password:
```

```
ftd#
```

b) Vérifiez l'état du tunnel de la phase 1/phase 2.

```
<#root>
```

```
ftd#
```

```
show crypto isakmp sa | i Status:
```

```
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show crypto ipsec sa | i State|spi
```

```
current outbound spi: 5E83023A
```

```
current inbound spi : 62BC7C9E
```

```
spi: 0x62BC7C9E (0x00010B45)
```

```
SA State: active
```

```
spi: 0x5E83023A (0x0002029B)
```

```
SA State: active
```

```
ftd#
```

c) Effectuez des captures pour vérifier les paquets TCP (Transmission Control Protocol) BGP reçus d'Azure dans le tunnel et le trafic NAT-T (Network Address Translation - Traversal) User Datagram Protocol (UDP) port 4500/UDP port 500 sur la capture externe à partir de l'IP publique du tunnel Azure Instance-0.

```
<#root>
```

```
ftd#
```

```
capture out-instance-0 trace interface Outside match ip host <Azure-instance0-IP> any
```

```
ftd#
```

```
capture tun-vti-0 interface Azure-VTI-0 trace match ip host <Link BGP IP> any
```

```
ftd#
```

```
show cap tun-vti-0
```

```
3 packets captured
```

```
1: 03:23:43.510074      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240 <ms
2: 03:23:44.511204      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240 <ms
3: 03:23:46.512211      10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240 <mss
ftd#
```

Une fois la connectivité à Instance0 confirmée, répétez la même configuration de topologie VTI et VPN pour Instance1 afin que les deux instances de la passerelle Azure soient accessibles.

Étape 6: Configurer le deuxième tunnel vers le point de terminaison Azure Instance1

a) Créez une deuxième interface VTI (Azure-VTI-1) empruntant à la même boucle (étape 3 b-f).

Virtual Tunnel Interface Details

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

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

Ethernet1/1 (Outside)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4

☐ IPv6

IP Address:*

☐ Configure IP

☒ Borrow IP (IP unnumbered)

Loopback1 (bgpVPNBranchLo)



VPN Topology
Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b) Configurez la topologie VPN de deuxième instance (étape 4 g-n).



Remarque : Vous pouvez référencer la valeur de l'adresse IP du point de terminaison Instance1 dans le fichier de configuration téléchargé à l'adresse `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

c) Déployez les modifications de configuration et vérifiez l'état du tunnel.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	
> Azure-VTI-Instance1	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	

d) Lors de l'archivage dans Azure, Instance0 et Instance1 sont toutes deux connectées.

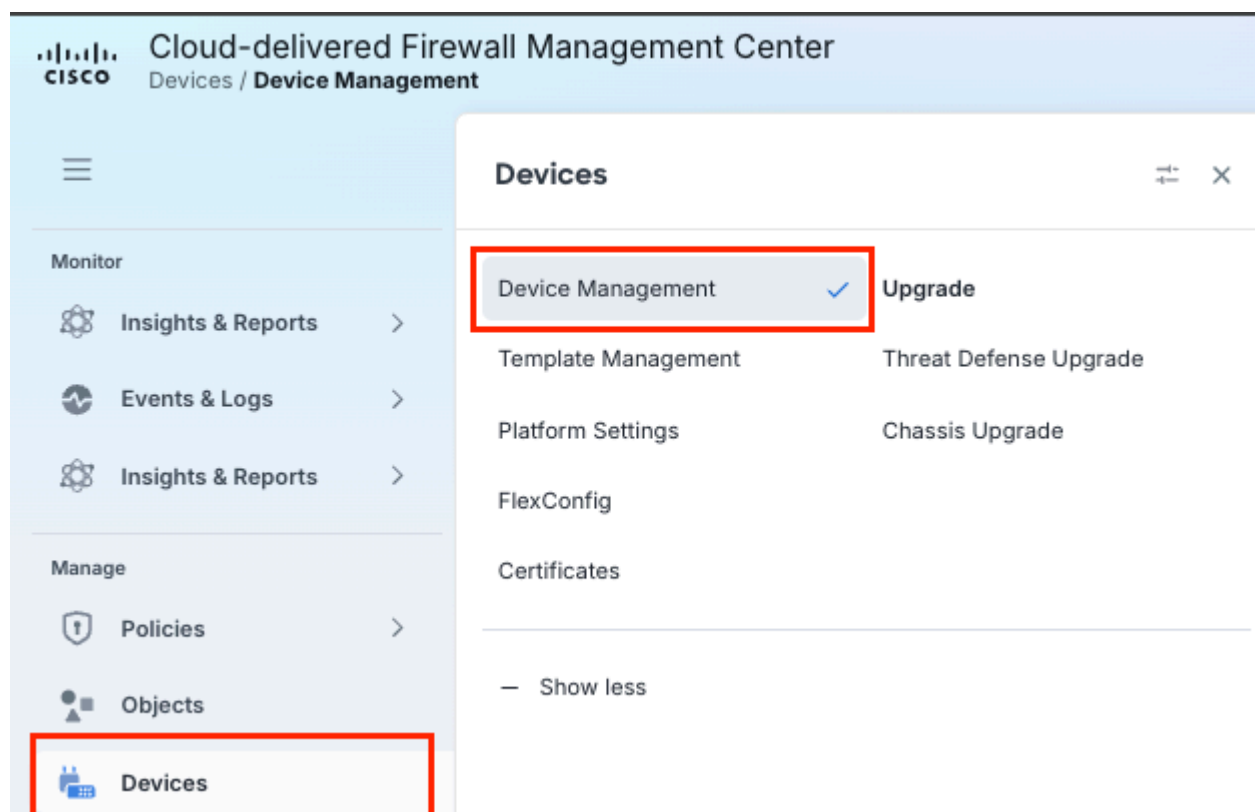
Links

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

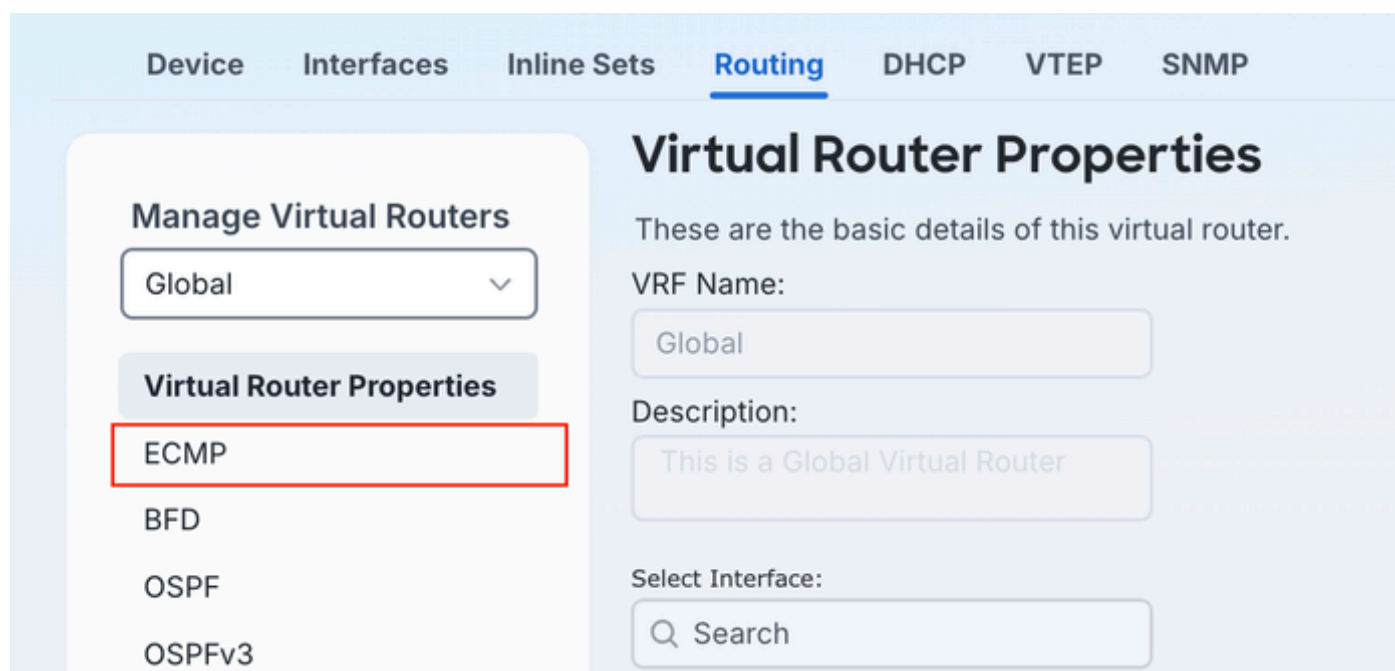
Avec les deux tunnels actifs, le FTD a besoin du routage ECMP pour que le trafic puisse utiliser les deux chemins en même temps, au lieu de traiter le second tunnel comme un standby passif.

Étape 7: Configurer ECMP

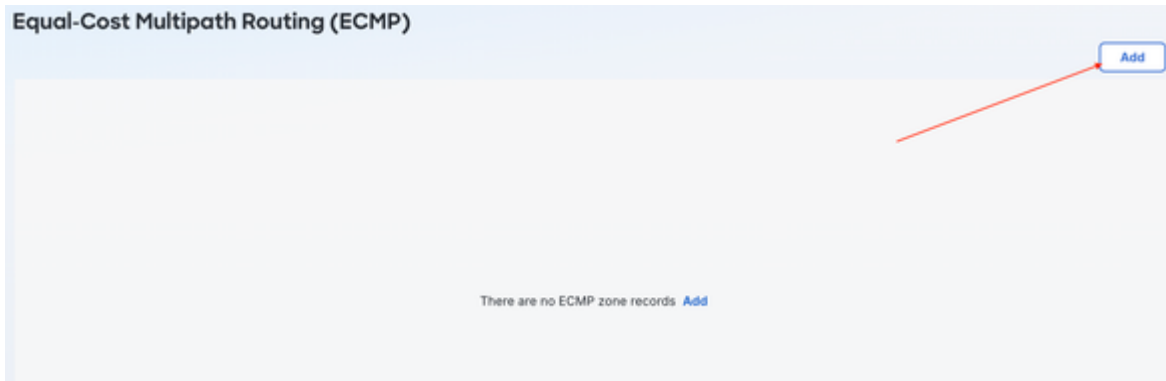
a) Accédez à Manage > Devices > Device Management et sélectionnez le FTD configuré avec les VPN vers Azure.



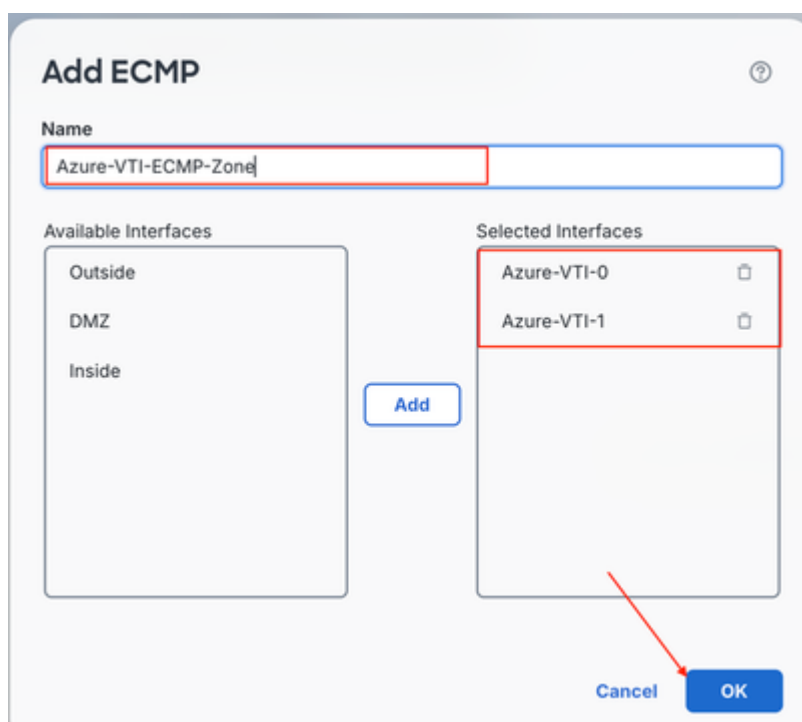
b) Cliquez sur l'onglet Routing et choisissez ECMP.



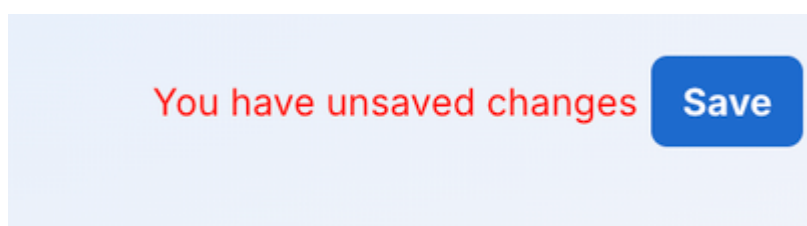
c) Cliquez sur Add pour créer une nouvelle zone ECMP.



d) Activez la mise en surbrillance des VTI en cliquant sur les deux VTI dans le panneau Interfaces disponibles et cliquez sur Ajouter pour appliquer les VTI à la zone ECMP nommée.



e) Après avoir vérifié que les paramètres sont corrects, cliquez sur Enregistrer.

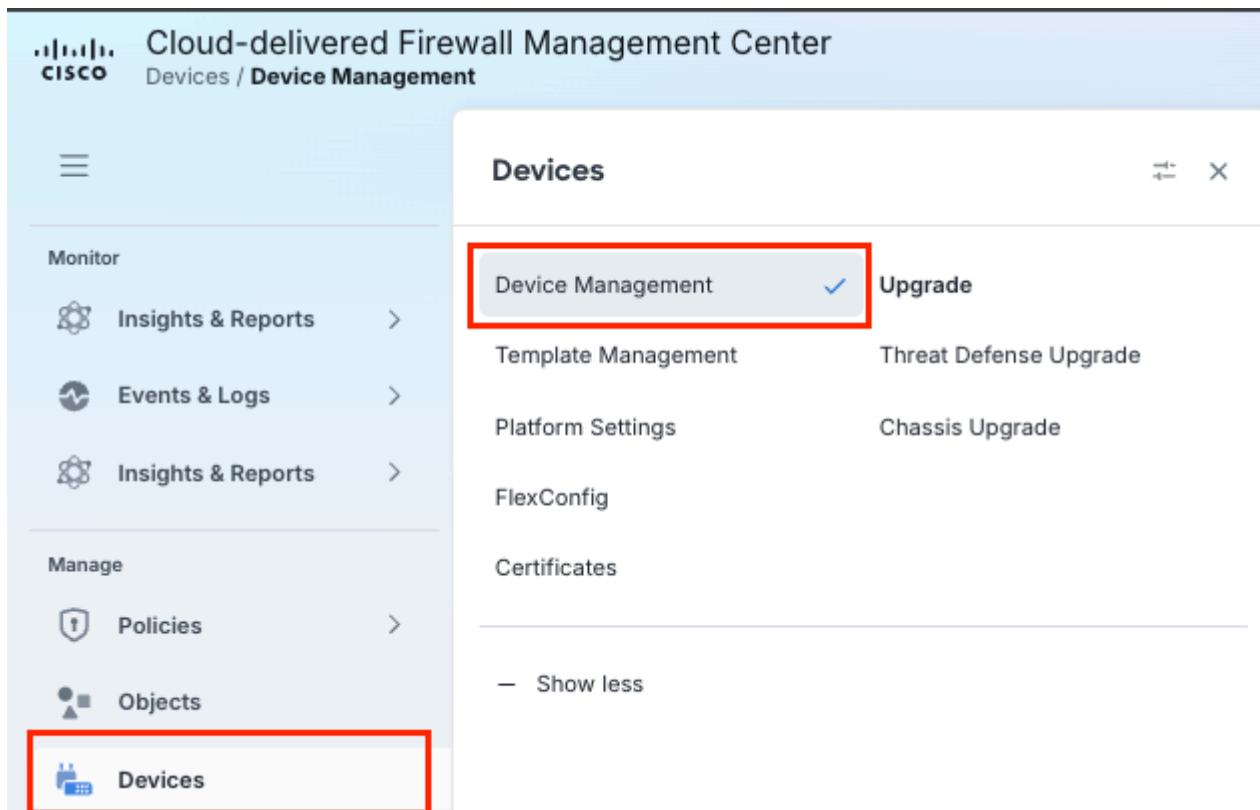


Étape 8: Configuration des routes statiques pour l'instance des adresses IP privées

Le protocole BGP nécessite des routes pour se connecter correctement aux voisins, et comme les points d'extrémité ne sont pas connectés directement, aucune route n'est remplie par défaut. ECMP vous permet de configurer des routes statiques avec la même métrique (distance administrative) vers la même destination, de sorte que les deux routes soient installées dans la base d'informations de routage (RIB) et utilisées simultanément.

a) Accédez à Manage > Devices > Device Management et sélectionnez le périphérique FTD

applicable.



b) Accédez à Routing > Static Route.

c) Cliquez sur + Ajouter une route.

d) Ajoutez des routes pour les deux adresses IP d'instance en créant la première route vers votre VTI Instance0, et ajoutez l'objet réseau de destination pour celui-ci en cliquant sur le signe + en regard de Réseau disponible. Cliquez ensuite sur l'objet réseau dans la liste et cliquez sur le bouton Ajouter pour l'ajouter en tant que destination de la route statique. Assurez-vous que vous choisissiez l'adresse IP d'instance0 et qu'elle est définie en tant que passerelle. Une fois terminé, cliquez sur OK.



Remarque : Ces valeurs de réseau de destination de route statique se trouvent

SOUS `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` et `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` dans le fichier de configuration téléchargé.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*: Azure-VTI-0

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

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

Selected Network: Azure-Instance0-BGP_Peer

Ensure that egress virtualrouter has route to that destination

Gateway: Azure-Instance0-BGP_Peer

Metric: 1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e) Répétez les étapes c à d pour ajouter la deuxième route statique via le VTI Instance1. Assurez-vous que vous cliquez sur Save pour enregistrer vos modifications.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Azure-Instance1-BGP_Peer	Azure-VTI-1	Global	Azure-Instance1-BGP_Peer (10.2.0.13)	false	1	
Azure-Instance0-BGP_Peer	Azure-VTI-0	Global	Azure-Instance0-BGP_Peer (10.2.0.12)	false	1	
IPv6 Routes						

Les routes statiques atteignent uniquement les adresses d'appairage BGP ; Le protocole BGP lui-même doit toujours être activé et appairé de sorte qu'Azure et le FTD échangent des routes de manière dynamique vers/depuis des réseaux plus étendus.

Étape 9: Configurer BGP

a) Activez le processus BGP 65500 sur FTD sous Routing > General Settings > BGP. Cochez la case Enable BGP, et entrez le numéro AS configuré précédemment dans Phase 2, Étape 1. Naviguez à côté de Routing > BGP > IPv4.

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

b) Activez le routage BGP IPv4 pour le processus/AS 65500 en cochant la case à cocher Enable IPv4 adjacente, puis cliquez sur Neighbor pour configurer les voisins BGP.

FTD
Cisco Firepower 1010 Threat Defense

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

Enable IPv4: ☒ AS Number 65500

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3

General **Neighbor** Add Aggregate Address Filtering Networks Redis

Setting
Learned Route Map

c) Cliquez sur + Ajouter.

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

+ Add

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
No records to display				

d) Entrez les informations d'appairage BGP Instance0, référez le BGP AS noté du concentrateur vWAN et entrez-le en tant que voisin distant AS, et ajoutez une description si vous le souhaitez. Cliquez sur Avancé.



Important : Assurez-vous de modifier la source de mise à jour BGP pour référencer le parent de bouclage des deux interfaces VTI sur le FTD.

Add Neighbor

IP Address*
10.2.0.12

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

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover
none

Description
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e) Dans le menu Advanced de la configuration de voisin BGP sur FTD, vous pouvez changer le nombre de sauts 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.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Répétez les mêmes étapes pour l'homologue BGP Azure Instance1.

Add Neighbor ?

IP Address*
10.2.0.13

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

BFD Fallover
none

Update Source:
bgpVPNBranchLo

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description
Instance1 Azure BGP Peering

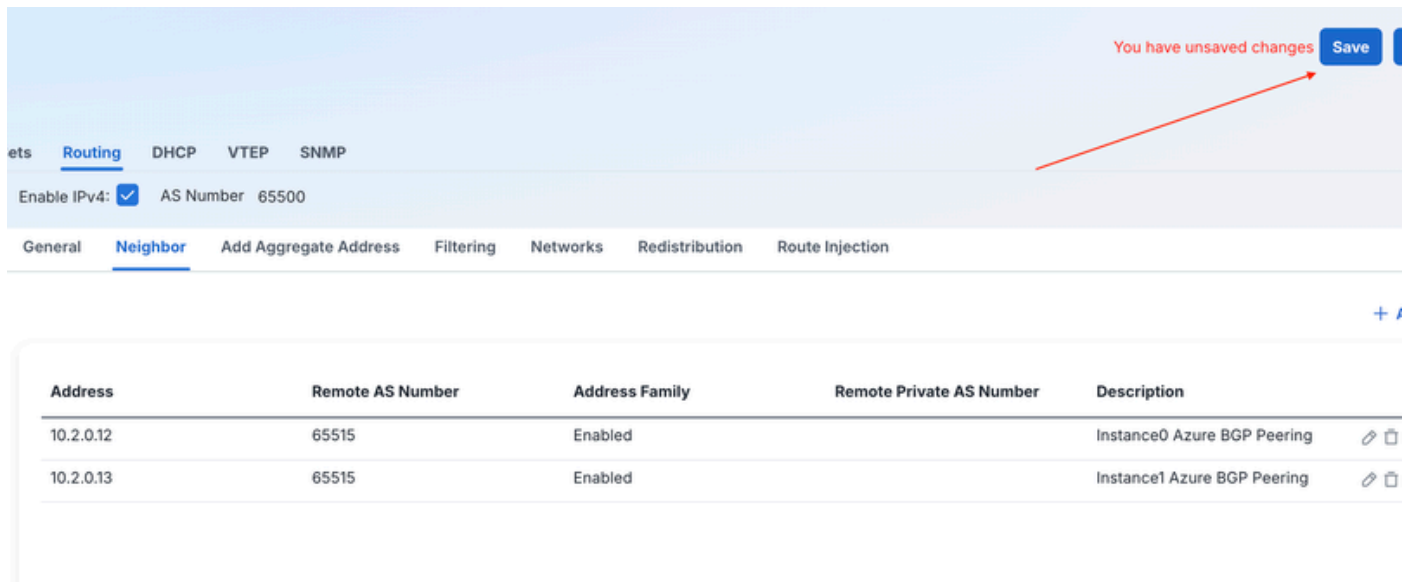
Filtering Routes Routes Timers **Advanced** Migration

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops
50
(1-255)

g) Assurez-vous d'enregistrer les modifications une fois terminé.



Par défaut, BGP installe seulement un meilleur chemin unique dans la table de routage, même si ECMP rend les deux routes statiques disponibles. Le multichemin BGP doit être activé séparément afin que les deux chemins appris soient installés et utilisés en même temps.

Étape 10: Configurer le multichemin BGP

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

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

Enable IPv4: ☒ AS Number 65500

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP (Use filtering to limit the number of prefixes that are redistributed)	No

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

b) Modifiez la valeur par défaut du champ Nombre de chemins de 1 à 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

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

Vérifier

Une fois le déploiement terminé, vérifiez que BGP forme des contiguïtés avec les deux instances Azure. Confirmez ensuite que les routes sont apprises sur les deux tunnels et que le trafic utilise les deux VTI, en utilisant le même accès CLI de diagnostic établi à l'étape 5 de la Phase 3.

Accédez à `sur system support diagnostic-cli` l'interface de ligne de commande FTD.

a) 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#

`show bgp summary`

BGP router identifier 10.50.1.2, local AS number 65500
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
2 multipath network entries and 4 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 952 total bytes of memory
BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.2.0.12	4	65515	5	3	5	0	0	00:01:02	2
10.2.0.13	4	65515	3	4	5	0	0	00:00:55	2

ftd#

b) Vérifiez que les routes reçues d'Azure s'affichent en tant que routes multichemins.

<#root>

ftd#

`show bgp`

BGP table version is 7, local router ID is 10.50.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i
*m 172.27.0.0	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i

ftd#

c) Vérifiez le nombre de paquets VTI.

<#root>

ftd#

show interface Tunnel1 | i packets

```
118 packets input, 31385 bytes
134 packets output, 8780 bytes
0 packets dropped
```

ftd#

show interface Tunnel2 | i packets

```
127 packets input, 33629 bytes
230 packets output, 15119 bytes
0 packets dropped
```

ftd#

d) Confirmez les routes statiques pour les voisins BGP.

<#root>

ftd#

show running-config route

```
route Azure-VTI-0 10.2.0.12 255.255.255.255 10.2.0.12 1
route Azure-VTI-1 10.2.0.13 255.255.255.255 10.2.0.13 1
ftd#
```

e) Confirmez les zones ECMP.

<#root>

ftd#

show zone

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

ftd#

f) Confirmez la configuration BGP.

<#root>

ftd#

show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.2.0.12 remote-as 65515
    neighbor 10.2.0.12 description Instance0 Azure BGP Peering
    neighbor 10.2.0.12 ebgp-multihop 50
    neighbor 10.2.0.12 transport path-mtu-discovery disable
    neighbor 10.2.0.12 update-source bgpVPNBranchLo
    neighbor 10.2.0.12 activate
    neighbor 10.2.0.13 remote-as 65515
    neighbor 10.2.0.13 description Instance1 Azure BGP Peering
    neighbor 10.2.0.13 ebgp-multihop 50
    neighbor 10.2.0.13 transport path-mtu-discovery disable
    neighbor 10.2.0.13 update-source bgpVPNBranchLo
    neighbor 10.2.0.13 activate
  no auto-summary
  no synchronization
  exit-address-family
ftd#
```

g) Confirmez 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 10.0.0.1 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
B      172.27.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
```

Autres considérations

La configuration de base de ce document suppose une interface externe unique et un FAI unique au niveau du FTD de la filiale. Ces considérations étendent cette conception.

AS-Path Prepending

Si vous devez influencer lequel des deux tunnels Azure ou le FTD préfère comme principal, plutôt que de partager la charge de manière égale via le multichemin ECMP et BGP, faites précéder le numéro de système autonome local d'une ou plusieurs fois sur le voisin BGP à traiter comme secondaire. Le voisin avec le chemin AS plus long et pré-ajouté est déclassé lors de la sélection du meilleur chemin BGP standard, sans avoir besoin de supprimer complètement ce voisin de la zone ECMP.

Dépannage

- Le tunnel de phase 1/phase 2 n'apparaît pas : Vérifiez que la clé pré-partagée et les paramètres de stratégie IKEv2/IPsec (chiffrement, intégrité, PRF, groupe DH et durée de vie) correspondent exactement entre la stratégie IKEv2 FMC/proposition IPsec et les valeurs du fichier de configuration VPN Azure téléchargé. Utilisez `show crypto isakmp sa` et `show crypto ipsec sa` comme indiqué à l'étape 5 de la Phase 3.
- Le tunnel est actif, mais les voisins BGP ne forment pas : Vérifiez que le BGP est défini sur l'interface de bouclage, pas sur le VTI lui-même, et qu'il est configuré avec une valeur suffisamment élevée pour atteindre l'adresse d'appairage Azure BGP, qui n'est pas directement connectée au FTD.
- BGP se forme, mais un seul tunnel transporte le trafic : Vérifiez que les deux VTI sont membres de la même zone ECMP, que les routes statiques vers les deux adresses BGP d'instance Azure sont installées avec la même distance administrative et que le multichemin BGP est configuré pour deux chemins, comme décrit dans la Phase 3, Étape 10.
- Aucun trafic de retour ou routage asymétrique vers Azure : Étant donné qu'Azure vWAN annonce l'espace d'adressage du concentrateur sur les deux tunnels, assurez-vous que le protocole ECMP n'est pas désactivé ailleurs dans la configuration de routage et recherchez des mappages de route ou un routage basé sur des stratégies qui pourraient épingler le trafic à un chemin unique.
- Le protocole BGP est activé et les routes sont installées, mais le trafic semble être bloqué : Assurez-vous que les règles de contrôle d'accès sont configurées avec la zone de sécurité affectée aux interfaces virtuelles permettant au trafic d'entrer et de sortir.

Informations connexes

- [Qu'est-ce que le WAN virtuel Azure ?](#)
- [Comment configurer BGP pour Azure VPN Gateway](#)

- [Stratégies IPsec par défaut et personnalisées Azure vWAN](#)
- [Dépanner les problèmes BGP pour Azure VPN Gateway](#)
- [À propos des passerelles VPN en mode actif-actif](#)
- [Didacticiel : Créer une connexion de site à site à l'aide d'Azure Virtual WAN](#)

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.