

Azure vWAN Site-to-Site VPN configureren voor een veilige firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Diagram](#)

[Single DIA Link vWAN-connectiviteit tussen Azure en FTD \(Azure Load-Balancing/Redundancy\)](#)

[Configureren](#)

[Fase 1: Azure vWAN/Hub-configuratie](#)

[Stap 1: vWAN maken](#)

[Stap 2: vWAN-hub maken](#)

[Fase 2: Azure vWAN VPN-siteconfiguratie](#)

[Stap 1: Azure vWAN VPN-site maken \(extern FTD-apparaat\)](#)

[Stap 2: Azure vWAN Site VPN-parameters configureren](#)

[Stap 3: Azure vWAN Site Tunnel Configuration downloaden](#)

[Fase 3: FTD-configuratie](#)

[Stap 1: Azure VPN-configuratie analyseren](#)

[Stap 2: Loopback configureren](#)

[Stap 3: Fase 1-/fase 2-beleidsobjecten configureren](#)

[Stap 4: Secure Connectivity configureren naar Azure](#)

[Stap 5: Controleer de eerste connectiviteit met Azure](#)

[Stap 6: Tweede tunnel configureren naar Azure Instance1 Endpoint](#)

[Stap 7: ECMP configureren](#)

[Stap 8: Statische routes configureren naar Instance Private IP's](#)

[Stap 9: BGP configureren](#)

[Stap 10: BGP-multipad configureren](#)

[Verifiëren](#)

[Andere overwegingen](#)

[AS-pad voortekenen](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie van Microsoft Azure Virtual WAN (vWAN) site-to-site VPN-connectiviteit met Cisco Secure Firewall.

Voorwaarden

Vereisten

Cisco adviseert kennis van deze onderwerpen:

- Microsoft Azure Virtual Wide Area Network (vWAN)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure FTD versie 10.0
- Cisco Secure FMC versie 10.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Microsoft Azure Virtual WAN (vWAN) combineert verschillende Azure-netwerk-, beveiligings- en routeringsmogelijkheden achter één Hub-constructie. Elke vWAN-hub kan een door Microsoft beheerde Site-to-Site VPN-gateway hosten die externe apparaten, zoals Secure Firewall, gebruiken om Azure te bereiken zonder dat de gateway-infrastructuur hoeft te worden gebouwd en onderhouden.

In tegenstelling tot een conventioneel IPsec-VPN met twee eindpunten, wordt de Azure vWAN Site-to-Site VPN-gateway geïmplementeerd als een actief-actief paar instanties (Instance0 en Instance1), elk met hun eigen openbare IP-adres en Border Gateway Protocol (BGP) peering-adres. Om te profiteren van beide instanties voor redundantie en extra doorvoer, stelt de FTD-tak één IP-beveiligingstunnel (IPsec) in voor elke instantie en gebruikt BGP, in plaats van alleen statische routing, om routes dynamisch te leren en terug te trekken wanneer instanties beschikbaar of niet beschikbaar worden. Equal-Cost Multi-Path (ECMP) routing en BGP multipath

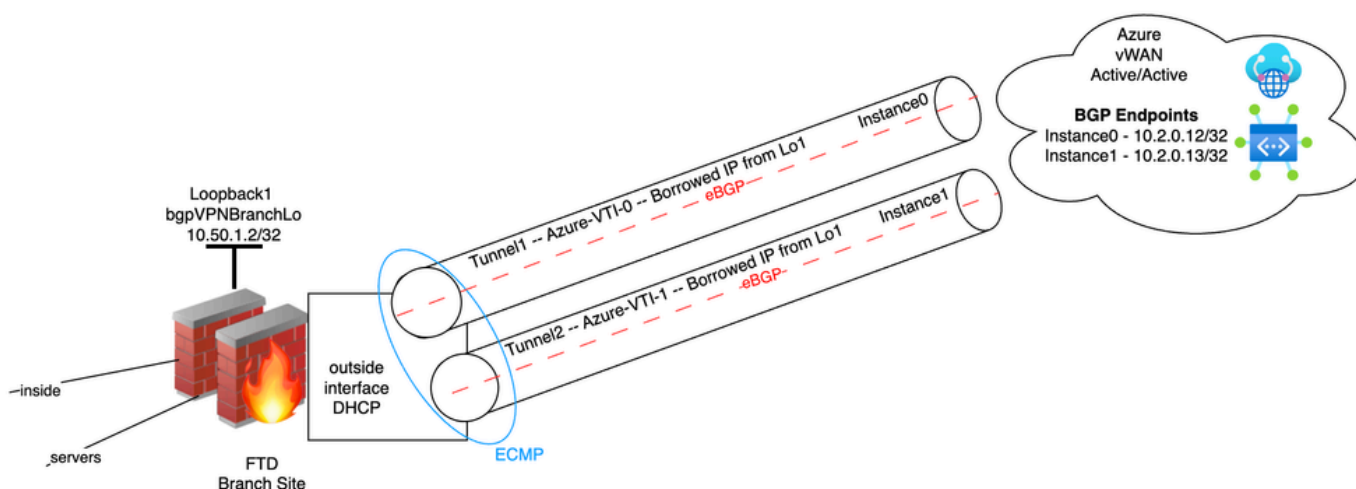
op de FTD houden beide tunnels tegelijkertijd actief, in plaats van er een als passieve standby te behandelen.

Dit document configureert dat ontwerp in drie fasen: de Azure vWAN Hub- en VPN Site-objecten worden eerst gemaakt, de resulterende verbindingsparameters worden gedownload en diezelfde parameters worden vervolgens gebruikt om overeenkomende Virtual Tunnel Interfaces (VTI's), Internet Key Exchange Version 2 (IKEv2) / IPsec-beleid, statische routes, ECMP en BGP peering op de FTD via FMC te configureren.

Diagram

Het diagram toont de topologie van de configuratie die in dit artikel wordt beschreven. De single Direct Internet Access (DIA)-variant haalt beide Azure-tunnels uit één externe interface op de FTD.

Single DIA Link vWAN-connectiviteit tussen Azure en FTD (Azure Load-Balancing/Redundancy)



Configureren

Voltooi de drie fasen op volgorde. De Azure-side-objecten die in fase 1 en fase 2 zijn gemaakt, produceren de peer-IP-adressen, BGP Autonomous System (AS)-nummers en vooraf gedeelde sleutel die fase 3 vervolgens op de FTD van toepassing is.

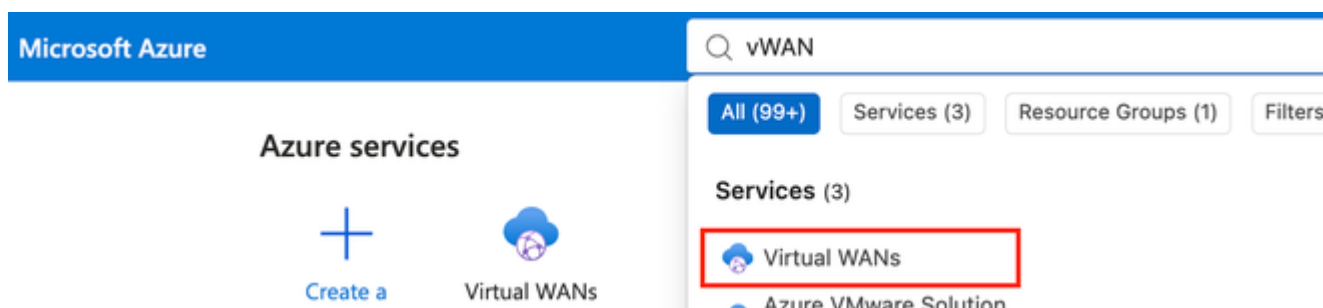
Fase 1: Azure vWAN/Hub-configuratie



Opmerking: de configuratiestappen in dit document zijn van hoog niveau en bieden de nodige stappen om de FTD te verbinden met Azure vWAN. Raadpleeg Azure vWAN-documentatie van Microsoft om de betekenis van de configuraties te begrijpen. Zie [Wat is Azure Virtual WAN?](#) en verdere documentatie.

Stap 1: vWAN maken

a) Zoek naar vWAN in het Azure-zoekvak en klik op Virtuele WAN's.



b) Klik op + Maken.



c) Voer een naam in voor de nieuwe vWAN-instantie, klik op Review + create en klik Create op de Review + Create-pagina in de wizard.

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 >



Opmerking: witruimte die waarden in verschillende velden in de afbeeldingen dekt, is bedoeld voor de publicatie van dit document.

d) Klik op Ga naar resource.



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

Stap 2: vWAN-hub maken

a) Navigeer naar Connectivity > Hubs en klik op + 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) Raadpleeg Azure-documentatie voor meer context over verdere configuratie. Zorg ervoor dat de toegewezen privé-adresruimte van de hub geen enkele van uw interne adresruimten overlapt. Configureer de naam, de virtuele hub, de voorkeur voor routing van de hub. Klik op Volgende: Site naar 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) Raadpleeg de documentatie van Microsoft Azure vWAN Hub voor informatie over de weergegeven velden. Schakel Ja in om een site naar site (VPN-gateway) te maken. Het standaard toegewezen BGP Autonomous System (AS)-nummer is 65515, zoals toegewezen door de Internet Engineering Task Force (IETF) in Request For Comments (RFC) 6996, waarin Private Use AS Reservation wordt gedefinieerd.



Opmerking: Noteer de BGP AS voor toekomstige configuratiestappen op de 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 >

Klik op Review + create, of klik op Next: Point to site > om optionele instellingen te configureren.

d) Klik op Aanmaken zodra de samenvatting is geverifieerd.



Opmerking: Zoals Azure aangeeft, duurt het maken van de hub 30 minuten.

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) Als de implementatie is voltooid, zoekt u naar uw oorspronkelijke vWAN-bronnaam. Om uw zoekopdracht verder te verfijnen, klikt u op Bronnen.

VirtualHubDeployment | Overview ...

Deployment

Search x << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

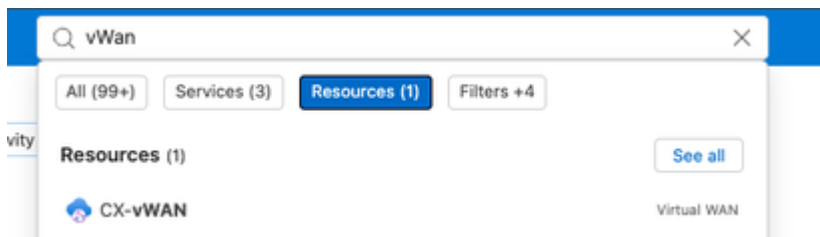
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

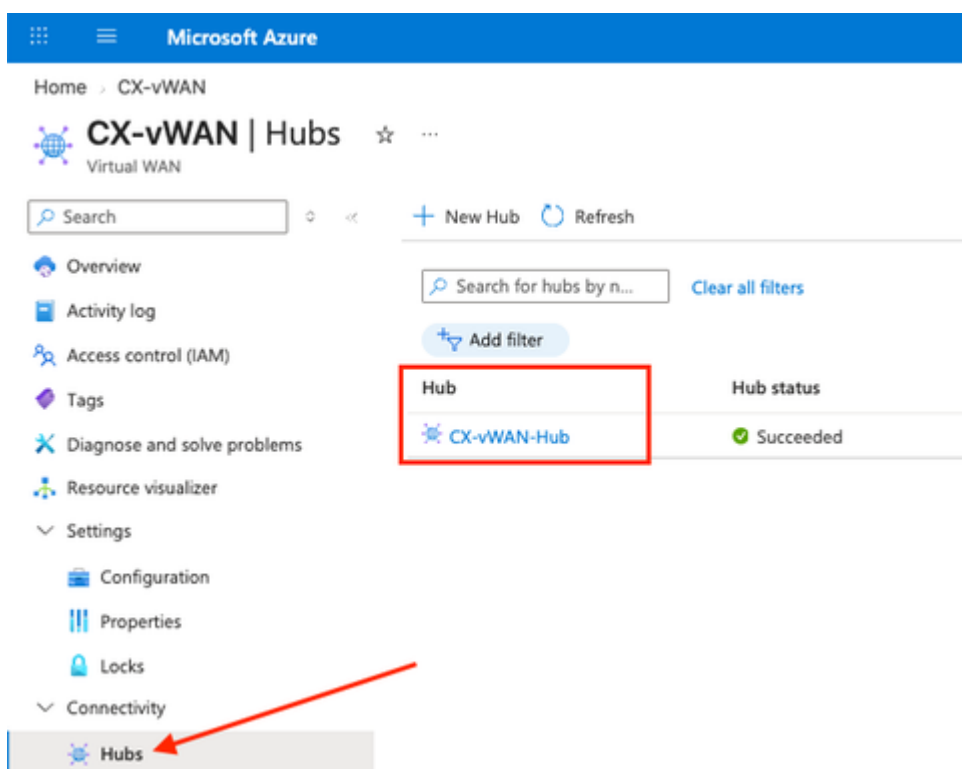
[Go to resource](#)



Fase 2: Azure vWAN VPN-siteconfiguratie

Stap 1: Azure vWAN VPN-site maken (extern FTD-apparaat)

a) Voer de aangemaakte hub in via Connectiviteit > Hubs en klik op de hub die in eerdere stappen is gemaakt.



b) Klik op Connectiviteit > VPN (Site naar site) en klik op + Nieuwe VPN-site maken.

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) Voer de waarden in de vereiste velden in. Als u klaar bent, klikt u op Volgende: Links > om verder te gaan.

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) Voer de vereiste linkgegevens in. Het Link BGP Address en de Link ASN-velden geven het binnentunnel BGP Layer 3-bestemmingsadres en het BGP AS-nummer weer op de filiaalsite waarmee de buurt met Azure wordt gevormd via de site-to-site tunnels. Het Link BGP-adres is een niet-overlappend subnetadres (/32) buiten het eerder geconfigureerde subnet Hub-privéadresruimte, dat Azure installeert als een /32-route om te bereiken als een BGP-buurman. Het Link IP-adres/FQDN is het Layer 3-doeladres van het verkeer naar de filiaalsite dat nodig is om IPsec/IKEv2-connectiviteit te bieden.



Opmerking: als u adressen gebruikt die variëren van 169.254.21.0 tot 169.254.22.255 voor tunneladressen, controleer dan [hoe u BGP voor Azure VPN Gateway configureert](#) voor specifieke vereisten.

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) Nadat u hebt bevestigd dat de instellingen correct zijn, klikt u op Aanmaken.

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) Als de implementatie van de VPN-site is voltooid, gaat u terug naar de vWAN-hubconfiguratie.

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

Stap 2: Azure vWAN Site VPN-parameters configureren

a) Voer de aangemaakte hub in via Connectiviteit > Hubs en klik op de hub die in eerdere stappen is gemaakt.

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) Navigeer nogmaals naar Connectivity > VPN (Site to Site) en klik op de X om de Hub Association: Connected filtering te wissen om niet-verbonden sites te bekijken.

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

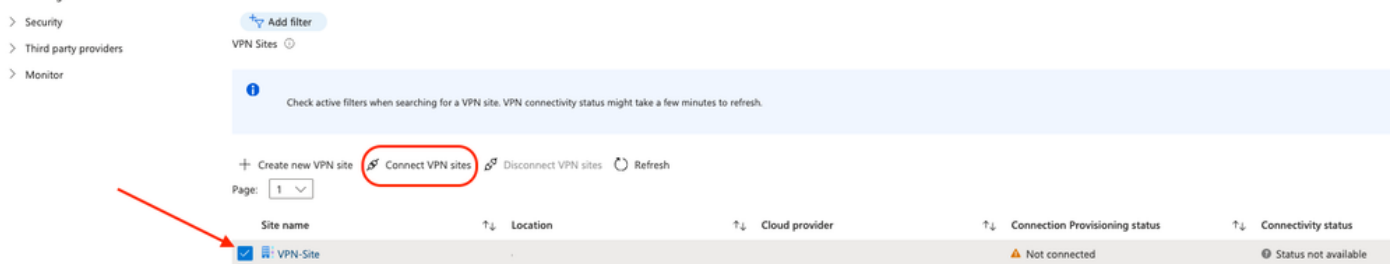
Search this page Clear all filters

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) Schakel het vakje naast de eerder geconfigureerde VPN-site in en klik vervolgens op VPN-sites verbinden, die wordt ingeschakeld nadat de site is geselecteerd.



d) Het zijladepaneel van de Verbindingssites wordt weergegeven. Voer een vooraf gedeelde sleutel (PSK) in en configureer de gewenste fase 1 IKEv2- en fase 2 IPsec-instellingen. Wanneer u Aangepast kiest uit de IPsec vervolgkeuzelijst, worden de waarden automatisch ingevuld. Noteer deze waarden, omdat ze op de FTD moeten overeenkomen. U moet ook kiezen of Perfect Forward Secrecy (PFS) gewenst is. Omdat dit een routegebaseerde tunnel is, configureert u de instellingen dienovereenkomstig. Klik na voltooiing op Verbinden om de configuratie op te slaan.



Opmerking: Zie [Standaard vs. Aangepast IPsec-beleid Azure vWAN](#) voor meer informatie.

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) Er wordt informatie weergegeven die aangeeft dat de gateway wordt bijgewerkt, samen met de geschatte tijd tot voltooiing.

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

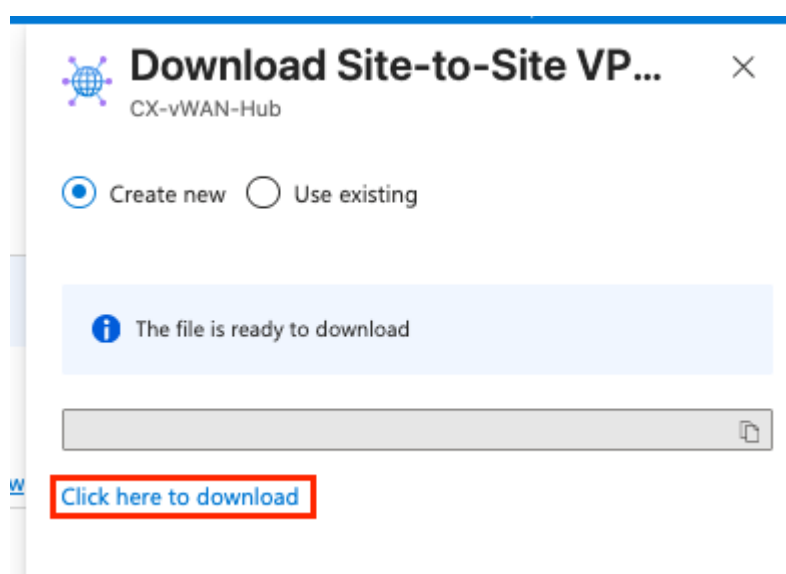
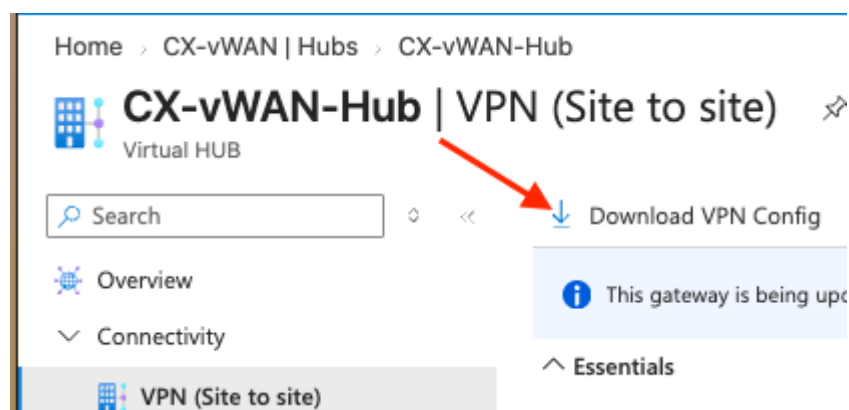
Connectivity



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

Stap 3: Azure vWAN Site Tunnel Configuration downloaden

a) Terwijl de gateway wordt bijgewerkt, kunt u de VPN-configuratie downloaden.



Wanneer de VPN-site is gemaakt en de verbindingsparameters (peer-adressen, BGP AS-nummers en PSK) zijn gedownload, worden dezelfde waarden gebruikt om de overeenkomende elementen op de FTD in fase 3 te configureren.

Fase 3: FTD-configuratie

Stap 1: Azure VPN-configuratie analyseren

a) Open het gedownloade VPN-configuratiebestand van Azure. Het ziet er hetzelfde uit als de getoonde gecondenseerde uitvoer en biedt nuttige informatie:



Opmerking: voor een betere scherpstelling worden verschillende irrelevante objecten en

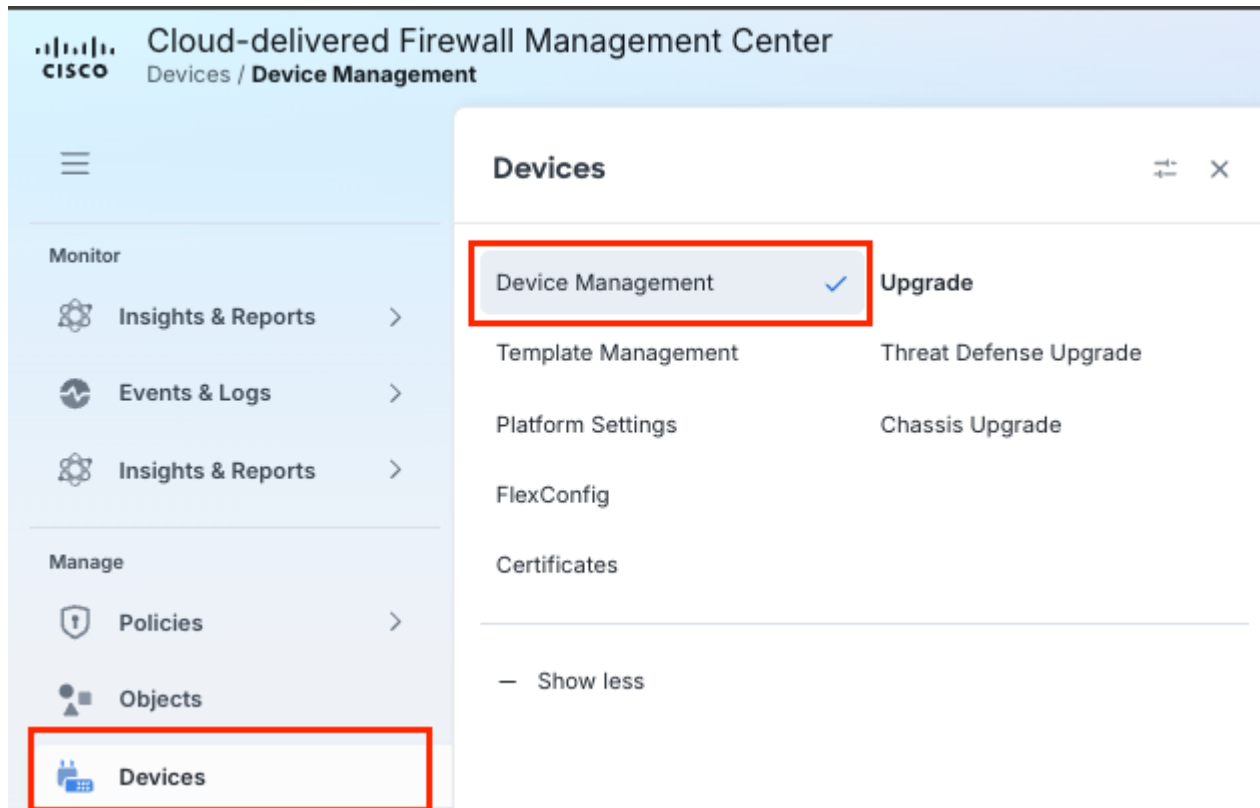
sleutel-/waardeparen gesnoeid voor een kortere duur.

```
[
{
  "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
        }
      }
    }
  ]
}
]
```

Stap 2: Loopback configureren

Elke VTI die later wordt geconfigureerd, heeft een stabiele tunnelbron nodig, dus een loopback-interface wordt eerst geconfigureerd en gedeeld tussen beide VTI's.

a) Navigeer naar Apparaten > Apparaatbeheer.

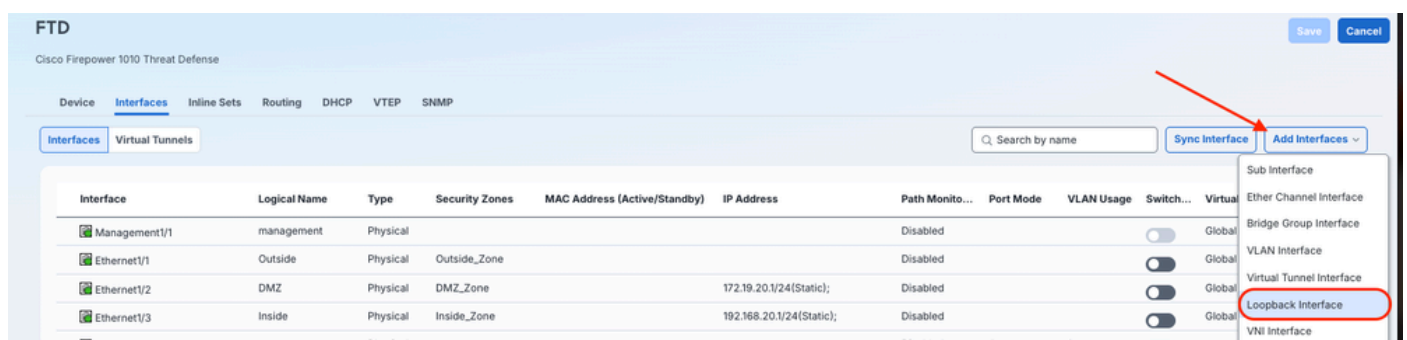


Opmerking: in dit lab wordt gebruikgemaakt van het door de cloud geleverde Firewall Management Center (cdFMC). De stappen blijven echter hetzelfde voor lokale FMC.

b) Selecteer de FTD die u configureert als het filiaal/site VPN-apparaat.



c) Klik op het vervolgkeuzemenu Interfaces toevoegen en klik op Loopback Interface.



d) Geef de Loopback-interface zijn naam, Loopback-ID en beschrijving indien nodig. Klik op IPv4.

The screenshot shows the 'Add Loopback Interface' dialog box with the 'IPv4' tab selected. The 'General' tab is also visible. The 'Name' field contains 'bgpVPNBranchLo'. The 'Enabled' checkbox is checked. The 'Loopback ID' field contains '1'. The 'Description' field contains 'Branch Loopback for BGP neighboring and VPN termination from Azure'. Red arrows point to the 'IPv4' tab, the 'Name' field, and the 'Loopback ID' field. The 'Cancel' and 'OK' buttons are at the bottom right.

Add Loopback Interface

General **IPv4** IPv6

Name:
bgpVPNBranchLo

☒ Enabled

Loopback ID: *
1

(1-1024)

Description
Branch Loopback for BGP neighboring and VPN termination from Azure

Cancel OK

e) Zorg ervoor dat het IP-type is gedefinieerd als Statisch IP-adres gebruiken, voer het BGP-adres van de koppeling in zoals geconfigureerd in fase 2, stap 1d. U kunt verwijzen naar de waarde die eerder is gedefinieerd in de gedownloade VPN-configuratie onder JSON `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Opmerking: definieer het adres met een /32-masker en binnen RFC 1918-adresruimte.

The screenshot shows the 'Add Loopback Interface' dialog box with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '10.50.1.2/32'. Red arrows point to the 'Use Static IP' dropdown, the 'IP Address' field, and the 'OK' button. The 'Cancel' and 'OK' buttons are at the bottom right.

Add Loopback Interface

General **IPv4** IPv6

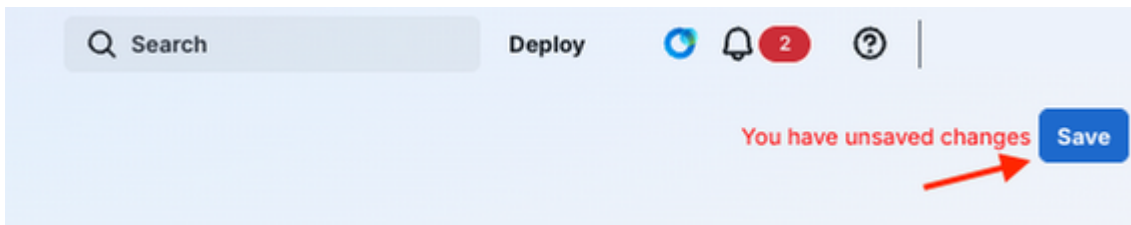
IP Type:
Use Static IP

IP Address:
10.50.1.2/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

f) Klik op Opslaan



Stap 3: Fase 1-/fase 2-beleidsobjecten configureren

a) Om de bijpassende IKEv2/IPsec-configuratie op de FMC te configureren voor toepassing in de FTD VPN-topologieën, bladert u naar Beheer > Objecten, scrolt u omlaag in het linkermenu naar VPN en vouwt u het submenu uit. Configureer het IKEv2 Fase 1-beleid door IKEv2-beleid in het menu te kiezen en op IKEv2-beleid toevoegen te klikken.

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

Name	
AES-GCM-NUL- SHA	Q [icon]
AES-GCM-NUL- SHA-LATEST	Q [icon]
AES-SHA-SHA	Q [icon]
AES-SHA-SHA-LATEST	Q [icon]
DES-SHA-SHA	Q [icon]
DES-SHA-SHA-LATEST	Q [icon]
Umbrella-AES-GCM-256	Q [icon]

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

b) Voer een naam in voor het nieuwe IKEv2-beleid, kies Prioriteit en/of Levensduur. Zorg ervoor dat het beleid aan beide uiteinden van de tunnel overeenkomt met betrekking tot Integriteit, Encryptie, PRF, en Diffie-Hellman (DH) Group. Kies de uitgelijnde algoritme/groep elementen die overeenkomen met de Azure-configuratie en klik op Toevoegen.



Opmerking: u kunt deze exacte waarden in het gedownloade configuratiebestand raadplegen op `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

Selected Algorithms

SHA256 

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

c) Als de configuratie is voltooid, klikt u op Opslaan.

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) Configureer Fase 2/IPsec-parameters in het submenu IKEv2 IPsec Proposal en klik op IKEv2 IPsec Proposal toevoegen.

The screenshot shows the Cisco FMC interface for configuring an IKEv2 IPsec Proposal. On the left, a navigation sidebar lists various configuration objects, with 'IKEv2 IPsec Proposal' selected and highlighted by a red box. The main panel is titled 'IKEv2 IPsec Proposal' and includes a brief description of the proposal's purpose. A red arrow points to a blue button labeled 'Add IKEv2 IPsec Proposal' in the top right corner. Below the description, there is a table with the heading 'Name' that lists four existing proposals: 'AES-GCM', 'AES-SHA', 'DES_SHA-1', and 'Umbrella-AES-GCM-256'.

e) Geef het IKEv2 IPsec-voorstel een naam en zorg ervoor dat dezelfde instellingen op elkaar zijn afgestemd. Als u klaar bent, klikt u op Opslaan.



Opmerking: u kunt deze waarden in uw gedownloade configuratiebestand raadplegen op `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

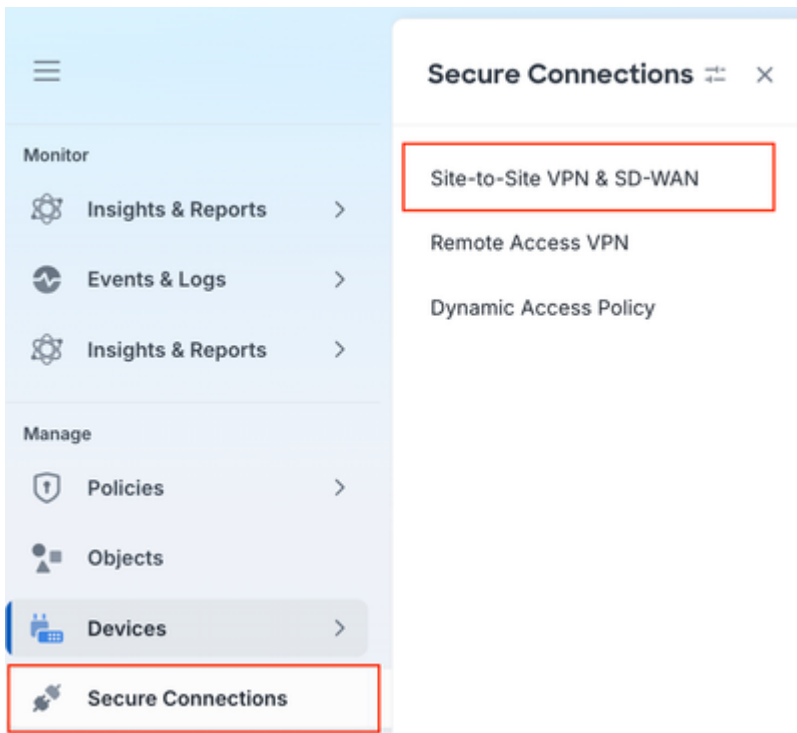


Cancel

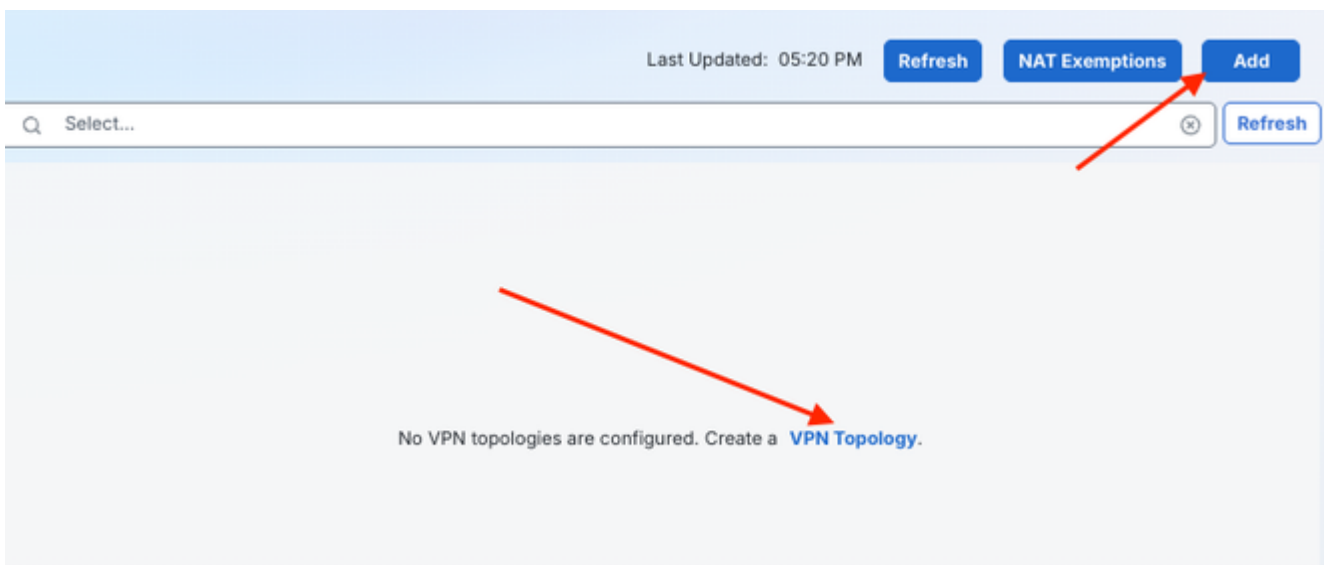
Save

Stap 4: Secure Connectivity configureren naar Azure

a) Navigeer naar Beheer > Beveiligde verbindingen > Site-to-Site VPN & SD-WAN.



b) Klik op de eerste hyperlink voor de VPN-topologieconfiguratie in het midden of klik op Toevoegen.



c) Voer een topologienaam in voor de eerste tunnel naar Azure Instance0, klik op de radioknop Route-Based VPN en klik op het topologietype Peer to Peer VPN. Klik na voltooiing op Aanmaken.

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) Voor knooppunt A klikt u op de vervolgkeuzelijst Apparaat en kiest u de naam van het beheerde FTD/FTD HA-paar waarnaar de configuratie wordt geïmplementeerd. Voor knooppunt B, omdat dit het externe uiteinde van de verbinding is in de topologie die eindigt op Azure vWAN-instanties, kiest u Extranet uit de vervolgkeuzelijst Apparaat. Klik vervolgens voor knooppunt A op het + pictogram naast de Virtual Tunnel Interface (VTI) vervolgkeuzelijst.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

Cancel Save

e) Geef de eerste VTI een naam, en zorg ervoor dat deze is ingeschakeld. Wijs een nieuwe of bestaande beveiligingszone toe aan de VTI, wijs de tunnelbron toe en kies het IP-adres uit de aangrenzende vervolgkeuzelijst.

Add Virtual Tunnel Interface

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Azure-VTI-0

☒ Enabled

Description:

Security Zone:
Azure-Spoke-Zone

Priority:
0 (0 - 65535)

Propagate Security Group Tag: ☒

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

Tunnel ID:*
1 (0 - 10413)

Tunnel Source:*
Ethernet1/1 (Outside) Dynamic

f) Zorg er vervolgens voor dat de keuzerondje IP lenen (IP-nummer) is geselecteerd en kies dezelfde loopback uit de vervolgkeuzelijst rechts. Klik eenmaal voltooid op OK.

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

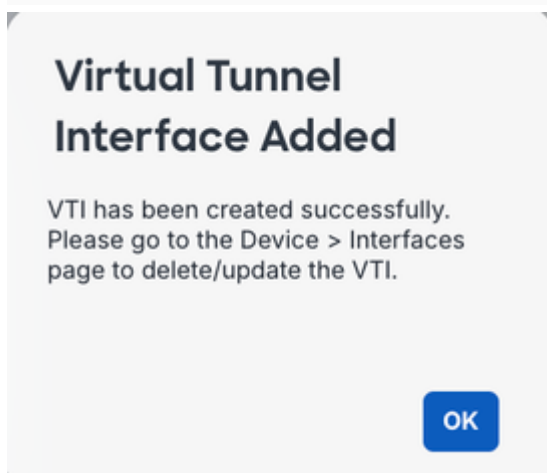
Tunnel ID:*
 (0 - 10413)

Tunnel Source:*

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

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

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



g) Nadat de VTI is geconfigureerd en toegepast, vult u handmatig het Tunnel Source IP-adres in (het vult automatisch in als het bovenliggende interfaceadres is ingevuld vanuit DHCP) en zorgt u ervoor dat de apparaatnaam van Node B is geconfigureerd, evenals het Instance Endpoint IP-adres. Klik na voltooiing op het tabblad IKE.



Opmerking: U kunt naar de waarde van het IP-adres van Instance0 Endpoint verwijzen in het gedownloade configuratiebestand

op `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) Scroll omlaag naar IKEv2-instellingen en zorg ervoor dat het verificatietype is ingesteld op vooraf gedeelde handmatige sleutel, en voer de PSK in Azure in in de vorige stappen in. Configureer het IKEv2 Fase 1-beleid door op het potloodpictogram te klikken om het beschikbare IKEv2-beleid te bewerken.



Opmerking: U kunt de vooraf gedeelde sleutel in het gedownloade configuratiebestand raadplegen op `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

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:* AES-GCM-NUL-**SHA-LATEST** 

Authentication Type: Pre-shared Manual Key 

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) Voeg het IKEv2 Fase 1-beleid toe dat aanvankelijk in stap 3 is geconfigureerd.

IKEv2 Policy



Available IKEv2 Policy  

 Search

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

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

j) Selecteer het tabblad 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) Bewerk het IKEv2 IPsec-voorstel onder Transformatiesets door op het potloodpictogram te klikken.

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) Klik op het pictogram prullenbak om de standaard AES-GCM-transformatieset te verwijderen en voeg de aangepaste Azure_IPsec-transformatieset/IKEv2 IPsec-voorstel toe die in de tweede helft van stap 3 is gemaakt. Klik op OK.

IKEv2 IPsec Proposal



Available Transform Sets +

Q Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec

Cancel

OK

m) Scroll naar beneden en voer 27000 in voor de levensduur van overeenkomende Azure-parameters. Schakel indien van toepassing PFS Group in. Klik op Save (Opslaan).



Opmerking: U kunt de levensduurwaarde in het gedownloadde configuratiebestand raadplegen op `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) Implementeer de wijzigingen.

Search Deploy

Search Device Advanced Deploy **Deploy All**

FTD

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

o) Als de implementatie is voltooid, schakelt u onder Beheren > Beveiligde verbindingen > Site-to-Site VPN & SD-WAN onder Tunnel Status Distribution; succesvolle connectiviteit weerspiegelt Groen (Up).

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	✓	✎ ✕

Bevestig dat de eerste tunnel is geïmplementeerd en bevestig dat deze succesvol is ingesteld op zowel de IKE / IPsec- als BGP-lagen voordat u de tweede tunnel configureert voor redundantie.

Stap 5: Controleer de eerste connectiviteit met Azure

a) SSH in de FTD en voer `system support diagnostic-cli` in, typ `en` en druk op Enter, omdat er geen wachtwoord op de alleen-lezen FTD CLI staat.

```
<#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) Controleer fase 1/fase 2 tunnelstatus.

```
<#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) Captures uitvoeren om te controleren op BGP Transmission Control Protocol (TCP)-pakketten die zijn ontvangen van Azure in de tunnel en Network Address Translation - Traversal (NAT-T) User Datagram Protocol (UDP)-poort 4500/UDP-poort 500-verkeer op de buitenkant vastleggen van het openbare IP-adres van Instance-0 Azure Tunnel.

```
<#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#
```

Als de verbinding met Instance0 is bevestigd, herhaalt u dezelfde VTI- en VPN-topologieconfiguratie voor Instance1, zodat beide Azure-gateway-instanties bereikbaar zijn.

Stap 6: Tweede tunnel configureren naar Azure Instance1 Endpoint

a) Creëer Tweede VTI (Azure-VTI-1) lenen van dezelfde loopback (stap 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) Configureer de VPN-topologie van de tweede instantie (stap 4 g-n).



Opmerking: U kunt de waarde van het Instance1 Endpoint IP-adres in het gedownloade configuratiebestand raadplegen op `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) Implementeer configuratiewijzigingen en controleer de tunnelstatus.

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) Controleren in Azure, zowel Instance0 als Instance1 opbrengst Connected.

Links

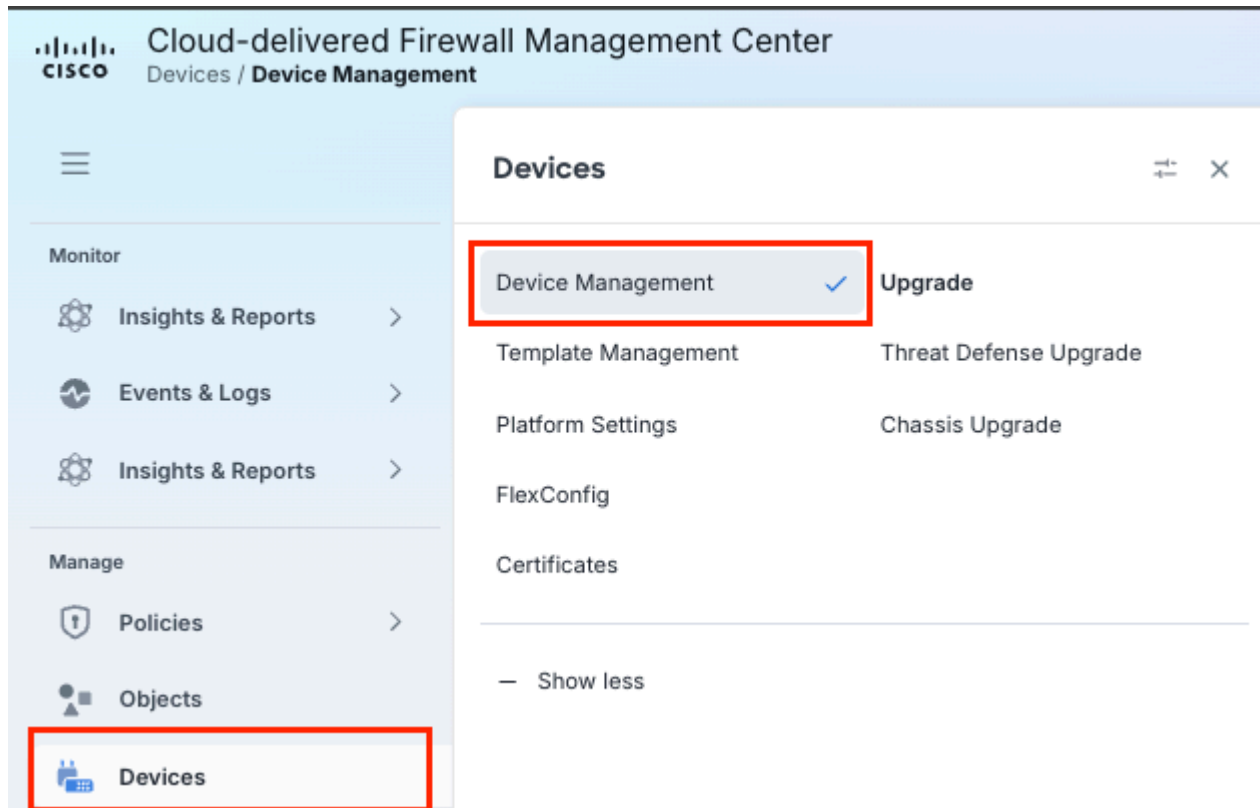
☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Aangezien beide tunnels actief zijn, heeft het FTD ECMP-routing nodig, zodat het verkeer beide paden tegelijkertijd kan gebruiken, in plaats van de tweede tunnel als een passieve stand-by te

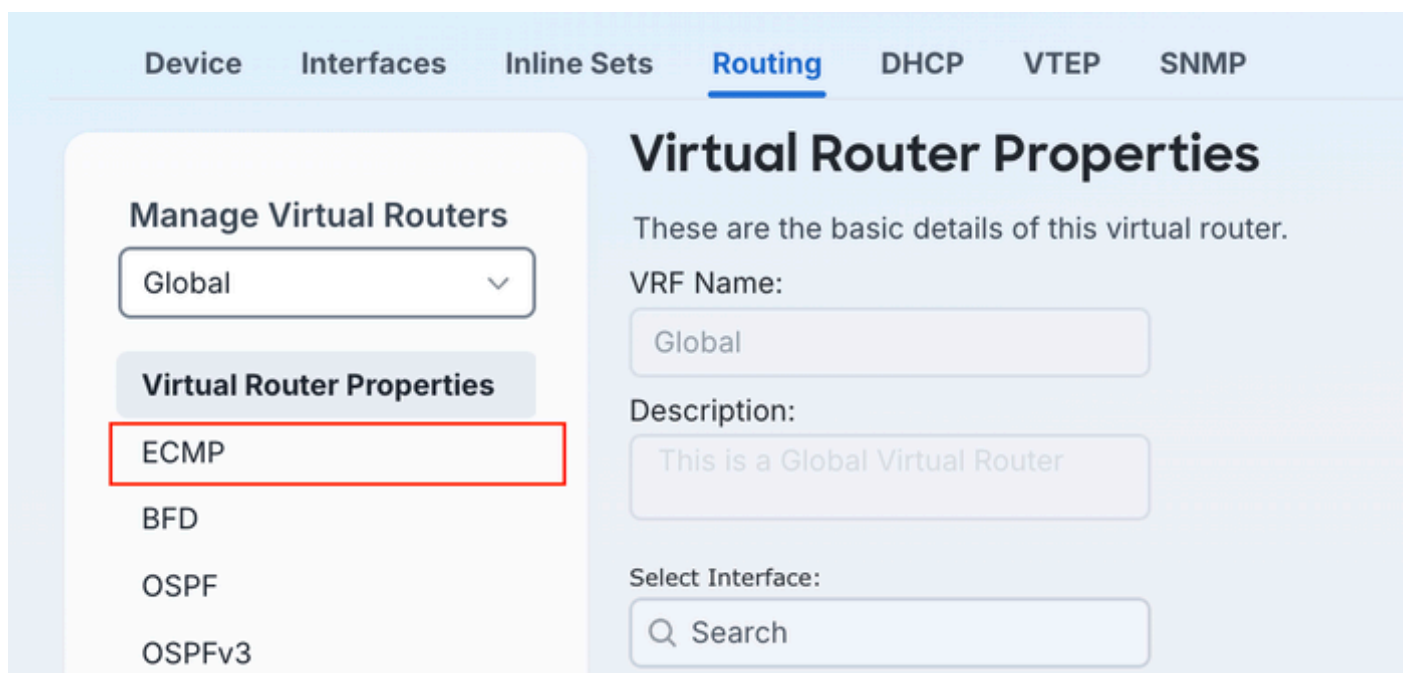
behandelen.

Stap 7: ECMP configureren

a) Navigeer naar Beheer > Apparaten > Apparaatbeheer en selecteer de FTD die is geconfigureerd met VPN's naar Azure.

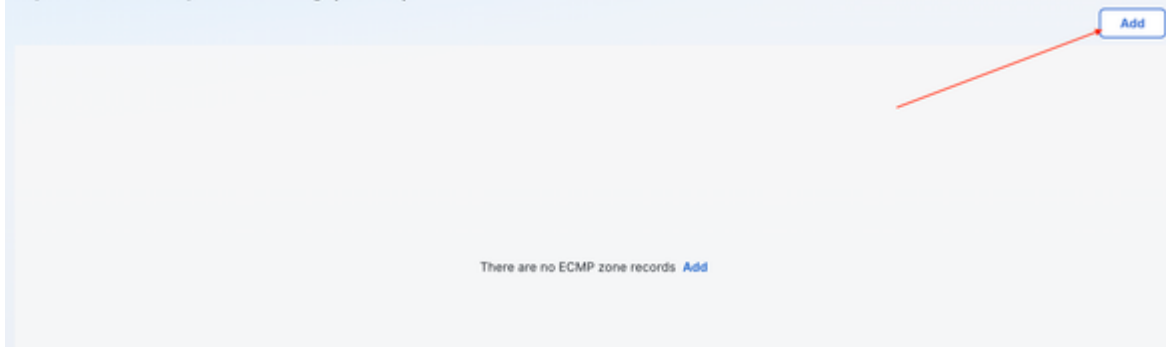


b) Klik op het tabblad Routing en kies ECMP.

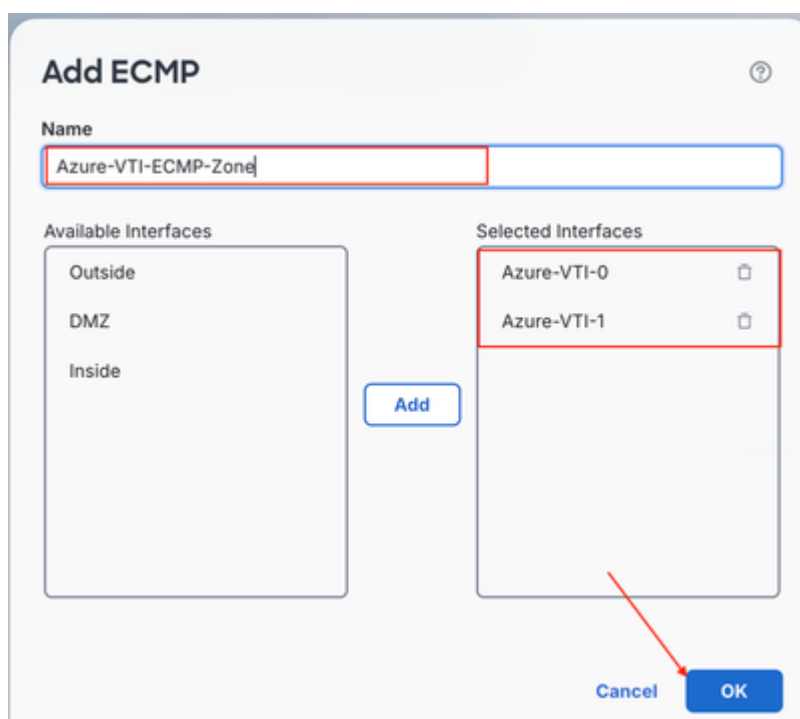


c) Klik op Toevoegen om een nieuwe ECMP-zone te maken.

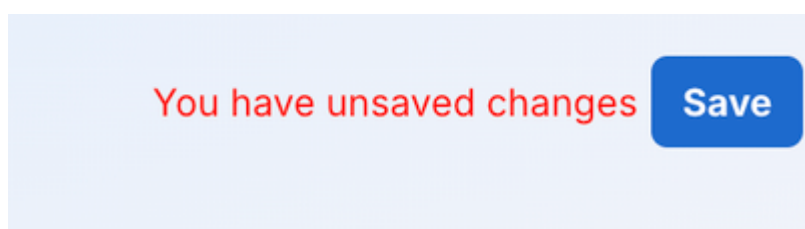
Equal-Cost Multipath Routing (ECMP)



d) Schakelen om de VTI's te markeren door op beide VTI's te klikken in het deelvenster Beschikbare interfaces en op Toevoegen om de VTI's toe te passen op de genoemde ECMP-zone.



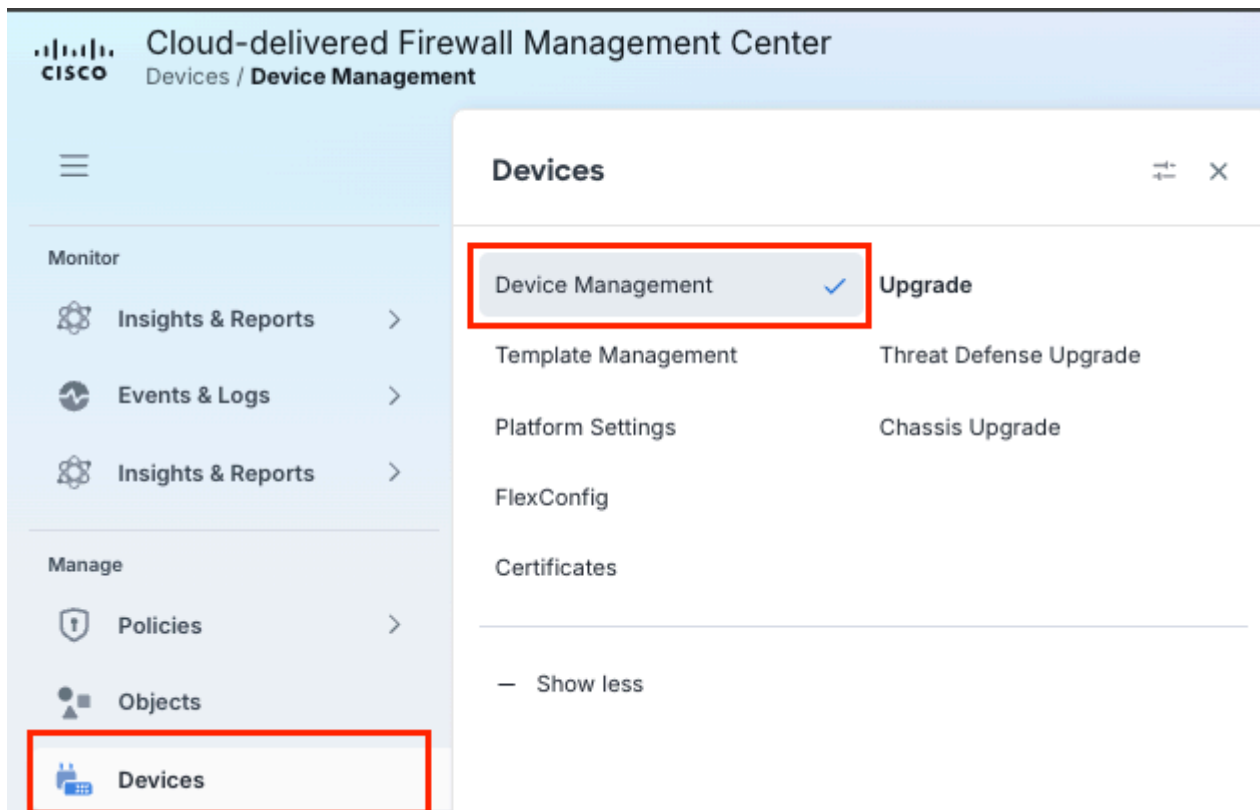
e) Nadat u hebt bevestigd dat de instellingen correct zijn, klikt u op Opslaan.



Stap 8: Statische routes configureren naar Instance Private IP's

BGP vereist routes om succesvol verbinding te maken met burens, en omdat de eindpunten niet direct verbonden zijn, worden er standaard geen routes ingevuld. Met ECMP kunt u statische routes met dezelfde metriek (administratieve afstand) naar dezelfde bestemming configureren, zodat beide routes in de Routing Information Base (RIB) worden geïnstalleerd en tegelijkertijd worden gebruikt.

a) Navigeer naar Beheer > Apparaten > Apparaatbeheer en kies het toepasselijke FTD-apparaat.



b) Navigeer naar Routing > Static Route.

FTD

Cisco Firepower 1010 Threat Defense

Monitor

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

Manage

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

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

Manage Virtual Routers

Global

Virtual Router Properties

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

Network ▲ Inte

IPv4 Routes

IPv6 Routes

c) Klik op + Route toevoegen.

+ Add Route

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

d) Voeg routes voor beide Instance IP-adressen toe door de eerste route naar uw Instance0 VTI te maken en voeg het doelnetworkobject toe door op de + naast Available Network te klikken. Klik vervolgens op het networkobject in de lijst en klik op de knop Toevoegen om het toe te voegen als de bestemming van de statische route. Zorg ervoor dat u de Instance0 IP kiest en deze is ingesteld als de Gateway. Klik na voltooiing op OK.



Opmerking: deze statische routebestemmingsnetwerkwaarden staan onder `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0 en`

`vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` in het gedownloade configuratiebestand.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*:

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

Available Network +

Selected Network

Azure-Instance0-BGP_Peer

Azure-Instance1-BGP_Peer

Ensure that egress virtualrouter has route to that destination

Gateway: +

Metric: (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e) Herhaal stap c-d om de tweede statische route toe te voegen via de Instance1 VTI. Zorg ervoor dat u op Opslaan klikt om uw wijzigingen op te slaan.

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						

Statische routes bereiken alleen de peering adressen van BGP; BGP zelf moet nog steeds worden ingeschakeld en gepeerd, zodat Azure en de FTD-uitwisselingsroutes dynamisch naar / van elkaar grotere netwerken.

Stap 9: BGP configureren

a) Schakel BGP Process 65500 in op FTD onder Routing > General Settings > BGP. Schakel het selectievakje BGP inschakelen in en voer het AS-nummer in dat eerder is geconfigureerd in fase 2, stap 1. Navigeer naast 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) Schakel IPv4 BGP-routing voor proces/AS 65500 in door het aangrenzende selectievakje IPv4 inschakelen in te schakelen en klik op Buurman om BGP-buren te configureren.

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) Klik op + Toevoegen.

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) Voer de peering-informatie van Instance0 BGP in, verwijst naar de vermelde BGP AS van de vWAN-hub en voer deze in als de Neighbor Remote AS, en voeg desgewenst een description toe. Klik op Advanced (Geavanceerd).



Belangrijk: zorg ervoor dat u de BGP-updatebron wijzigt om te verwijzen naar de bovenliggende Loopback van beide VTI-interfaces op de 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

Update Source:
bgpVPNBranchLo

Description
Instance0 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

e) In het Geavanceerde menu van de BGP Neighbor configuratie op FTD, kunt u het aantal TTL hop van eBGP standaard van 1 hop naar een variabel nummer wijzigen. Azure BGP-eindpunten zijn niet rechtstreeks via de tunnel verbonden met Azure-infrastructuur en er zijn meestal meer sprongen naar het eindpunt dan de standaard eBGP TTL van 1-vergunningen.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Herhaal dezelfde stappen voor Azure Instance1 BGP Peer.

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

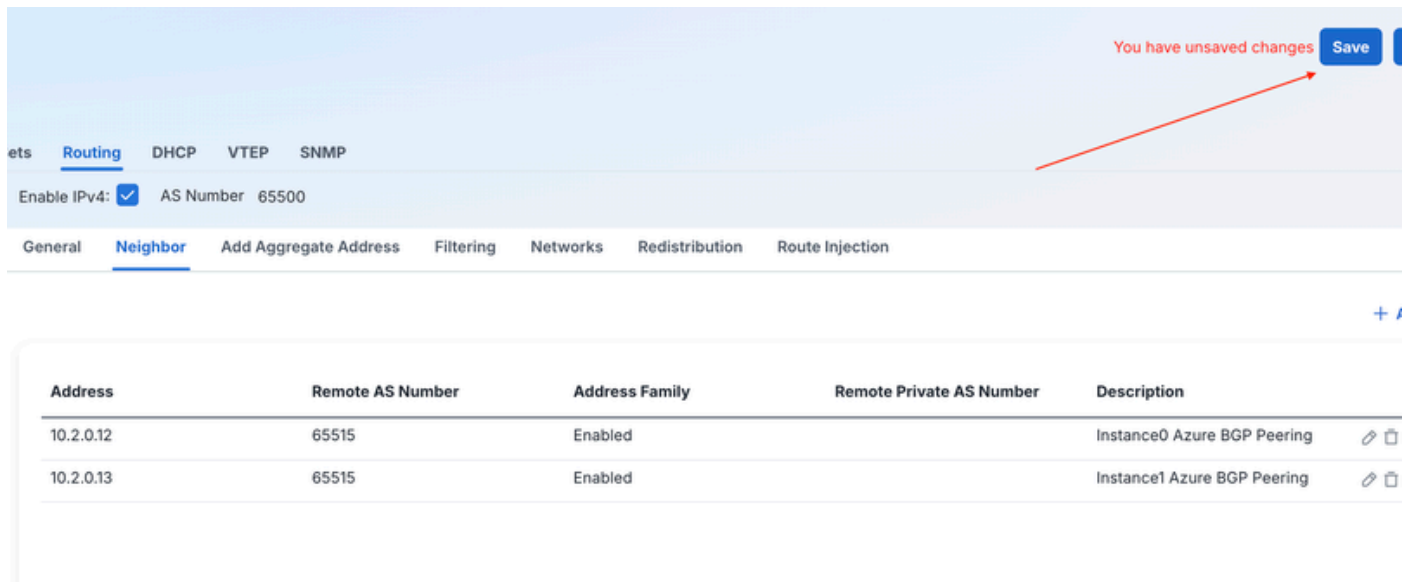
☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

g) Zorg ervoor dat u wijzigingen opslaat zodra deze zijn voltooid.



Standaard installeert BGP slechts één beste pad in de routingstabel, hoewel ECMP beide statische routes beschikbaar stelt. BGP-multipad moet afzonderlijk worden ingeschakeld, zodat beide aangeleerde paden tegelijkertijd worden geïnstalleerd en gebruikt.

Stap 10: BGP-multipad configureren

a) Navigeer naar Routing > BGP > IPv4, klik op het tabblad General en klik op het potloodpictogram naast 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) Wijzig de standaardwaarde van het veld Aantal paden van 1 naar 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Zorg ervoor dat u de wijzigingen opslaat en implementeert.

Verifiëren

Nadat de implementatie is voltooid, bevestigt u dat BGP aangrenzende verbindingen vormt met beide Azure-instanties. Bevestig vervolgens dat routes via beide tunnels worden geleerd en dat verkeer beide VTI's gebruikt, met behulp van dezelfde diagnostische CLI-toegang als vastgesteld in fase 3, stap 5.

Navigeer naar `system support diagnostic-cli` op FTD CLI.

a) Zodra de BGP-buren zijn geïmplementeerd, wordt verwacht dat ze naar voren komen en voorvoegsels worden ontvangen.

<#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) Controleer of de routes die van Azure zijn ontvangen, worden weergegeven als routes met meerdere paden.

<#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) Controleer het aantal VTI-pakketten.

```
<#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) Statische routes voor BGP-buurten bevestigen.

```
<#root>
```

```
ftd#
```

```
show running-config route
```

```

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

```

e) ECMP-zones bevestigen.

```
<#root>
```

```
ftd#
```

```
show zone
```

```

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

```

```
ftd#
```

f) BGP-configuratie bevestigen.

<#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) Bevestig de routingstabel.

<#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
```

Andere overwegingen

De basisconfiguratie in dit document gaat uit van één externe interface en één ISP bij de FTD-vestiging. Deze overwegingen breiden dat ontwerp uit.

AS-pad voortekenen

Als u wilt beïnvloeden welke van de twee tunnels Azure of de FTD de voorkeur geeft als primaire, in plaats van de belasting gelijk te delen via ECMP en BGP multipath, stel dan de lokale AS nummer een of meer extra keren op de BGP buurman te worden behandeld als secundaire. De buurman met het langere, vooraf ingestelde AS-pad krijgt geen prioriteit tijdens de standaardselectie van het beste pad voor BGP, zonder dat die buurman volledig uit de ECMP-zone hoeft te worden verwijderd.

Problemen oplossen

- Fase 1/fase 2-tunnel komt niet naar voren: Bevestig dat de vooraf gedeelde sleutel en de beleidsparameters IKEv2/IPsec (codering, integriteit, PRF, DH-groep en levensduur) exact overeenkomen tussen het FMC IKEv2-beleid/IPsec-voorstel en de waarden in het gedownload Azure VPN-configuratiebestand. Gebruik `show crypto isakmp sa` en `show crypto ipsec sa`, zoals weergegeven in fase 3, stap 5.
- Tunnel is up, maar BGP-buren vormen `update-source` zich niet: Controleer of de BGP is ingesteld op de loopback-interface, niet de VTI zelf, en dat `ebgp-multihop` is geconfigureerd met een waarde die hoog genoeg is om het Azure BGP-peering-adres te bereiken, dat niet rechtstreeks is verbonden met de FTD.
- BGP-formulieren, maar slechts één tunnel vervoert verkeer: Bevestig dat beide VTI's lid zijn van dezelfde ECMP-zone, dat statische routes naar beide BGP-adressen van Azure-instanties met dezelfde administratieve afstand zijn geïnstalleerd en dat BGP multipath is geconfigureerd voor twee paden, zoals beschreven in fase 3, stap 10.
- Geen retourverkeer of asymmetrische routing naar Azure: omdat Azure vWAN de adresruimte van de hub via beide tunnels adverteert, moet u ervoor zorgen dat ECMP niet elders in de routeringsconfiguratie is uitgeschakeld en moet u controleren op routekaarten of beleidsgebaseerde routing die het verkeer op één pad kan vastpinnen.
- BGP is up en routes zijn geïnstalleerd, maar het verkeer lijkt te zijn geblokkeerd: Zorg ervoor dat u toegangscontroleregels hebt geconfigureerd met de beveiligingszone die is toegewezen aan de VTI's, zodat het verkeer kan binnendringen en uitstappen.

Gerelateerde informatie

- [Wat is een Azure Virtual WAN?](#)
- [BGP configureren voor Azure VPN Gateway](#)
- [Standaard vs. Aangepast IPsec-beleid Azure vWAN](#)

- [Problemen met BGP oplossen voor Azure VPN Gateway](#)
- [Informatie over VPN-gateways in de actieve modus](#)
- [Zelfstudie: maak een site-to-site verbinding met Azure Virtual WAN](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.