

Azure Dual ISP vWAN-connectiviteit configureren op Secure Firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Diagram](#)

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

[Configureren](#)

[Fase 1: Azure vWAN VPN-siteconfiguratie](#)

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

[Stap 2: Azure APIPA-gatewayparameters configureren](#)

[Stap 3: Azure vWAN Site VPN-parameters configureren](#)

[Stap 4: Aangepaste BGP APIPA inschakelen en activeren op VPN-site linkinstanties](#)

[Stap 5: Het configuratiebestand van de VPN-site downloaden](#)

[Fase 2: FTD configureren voor dubbele ISP-connectiviteit met Azure vWAN](#)

[Stap 1: Analyseer de gedownloade VPN-configuratie](#)

[Stap 2: Link BGP Update Source Loopback-interfaces configureren](#)

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

[Stap 4: Virtuele tunnelinterfaces \(VTI\) configureren](#)

[Stap 5: IPsec VPN-topologieën aanbieden](#)

[Stap 6: Valideren van VPN-topologieën](#)

[Stap 7: ECMP configureren](#)

[Stap 8: BGP configureren](#)

[Stap 9: eBGP-multipad configureren](#)

[Controleren/Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u Microsoft Azure Virtual WAN (vWAN) Site-to-Site VPN-connectiviteit configureert voor Secure Firewall met behulp van dubbele WAN-koppelingen.

Voorwaarden

Vereisten

Cisco adviseert kennis van deze onderwerpen:

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

Zorg ervoor dat deze componenten beide in eerste instantie zijn geconfigureerd in de Azure-omgeving:

- Microsoft Azure vWAN Instance
- Microsoft Azure vWAN Hub

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
- Microsoft Azure vWAN

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

Wanneer de FTD-tak twee interfaces heeft die naar buiten gericht zijn op Internet Service Provider (ISP), kan elk ervan redundant en actief verbinding maken met Azure vWAN, zodat elke ISP-link wordt gebruikt. Azure vWAN maakt twee IPsec-tunnels per sitelink — één naar Azure Hub Instance0 en één naar Instance1 — zodat elke ISP-interface twee tunnels beëindigt. Op beide ISP-koppelingen resulteert dit in vier IPsec-tunnels die eindigen op de FTD.

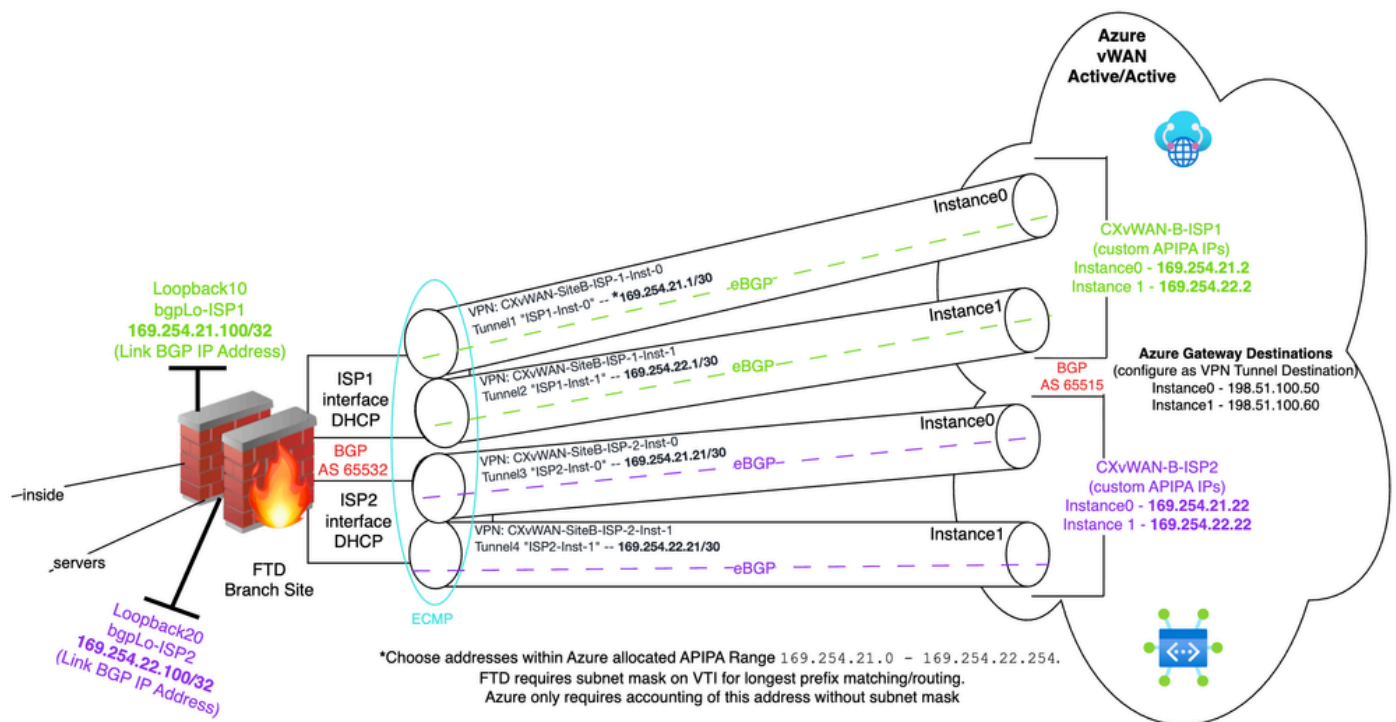
Azure Instances werkt in de actieve/actieve modus voor werklastverdeling en redundantie, dus de FTD weerspiegelt dit door middel van Equal-Cost Multi-Pathing (ECMP)-configuratie in alle vier IPsec-tunnels. Met behulp van aangepaste APIPA-adressen (Automatic Private IP Addressing) worden externe Border Gateway Protocol (eBGP)-buurten met afzonderlijke ASN's (Private Autonomous System Numbers) ingesteld over elk van de vier tunnels. Dit maakt de BGP-

multipadfunctionaliteit mogelijk en biedt meerdere redundante paden naar elk paar exemplaren van Azure Hub Site Link.

Diagram

Het diagram toont de topologie van de configuratie die in dit artikel wordt beschreven. De dual Direct Internet Access (DIA)-linkvariant haalt beide Azure-tunnels uit twee externe interfaces op de FTD.

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



Topologie voor dubbele directe internettoegang

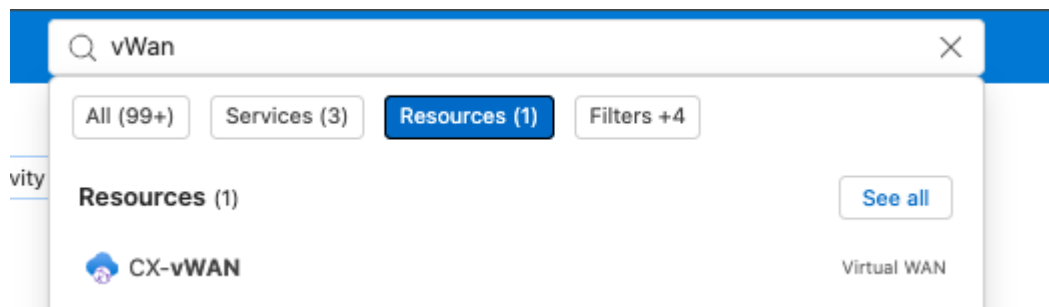
Configureren

Fase 1: Azure vWAN VPN-siteconfiguratie

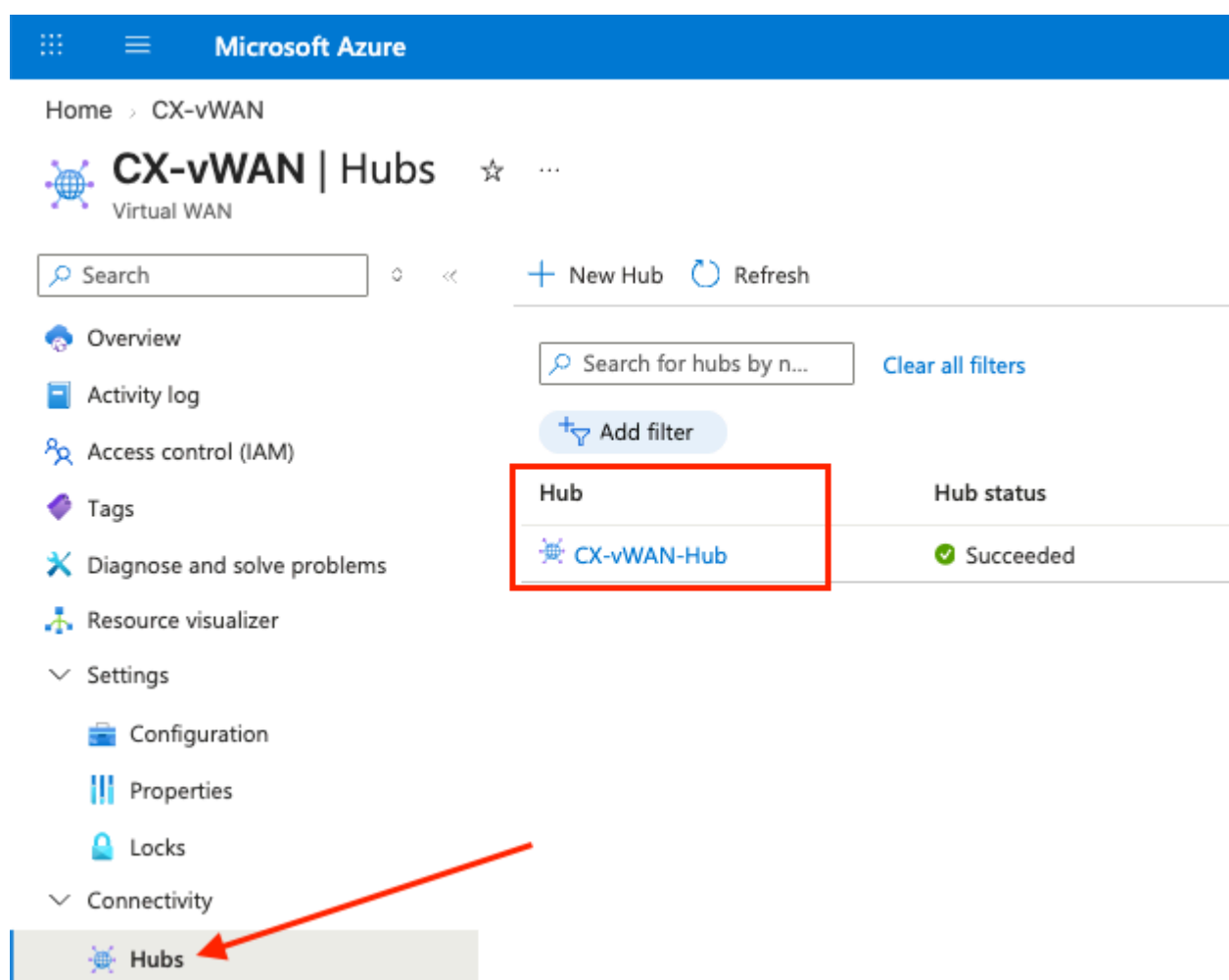
Stap 1: Azure vWAN VPN-site maken (extern FTD-apparaat)

1) Zoek naar vWAN in het Azure-zoekveld en klik op Virtuele WAN's om de bestaande Azure

vWAN-hub te openen. Navigeer vervolgens naar Connectivity > Hubs en klik op de bestaande Azure vWAN Hub.



Zoekopdracht voor virtueel WAN



Bestaande virtuele WAN-hub selecteren

2) Klik op Connectiviteit > VPN (van 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		

Nieuwe virtuele WAN-site maken



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

3) 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 >

Algemene instellingen voor VPN-siteconfiguratie

4) Voer de vereiste linkgegevens in. Het Link BGP-adres en de Link ASN zijn het binnentunnel BGP Layer 3-bestemmingsadres en het BGP AS-nummer aan de aftakkant waarmee de wijk wordt gevormd via de site-to-site tunnels. Het Link BGP-adres is een niet-overlappend subnetadres (/32) buiten het geconfigureerde subnet Hub-privéadresruimte, dat Azure installeert als een /32-route om te bereiken als een BGP-buurman. Twee loopback-interfaces worden in latere secties op de FTD gemaakt om het BGP-adres van de koppeling voor elk van de dubbele sitelinks weer te geven. Het IP-adres van de koppeling/Volledig gekwalificeerde domeinnaam (FQDN) is het IP-adres van de buitenste header Layer 3-bestemming van het verkeer naar de filiaalsite dat nodig is om IP-beveiliging (IPsec)/Internet Key Exchange versie 2 (IKEv2)-connectiviteit te bieden. Ga naar de volgende stap wanneer u klaar bent door op Volgende te klikken: Review + create >.



Opmerking: Controleer of u specifieke Azure-documentatie controleert als u adressen gebruikt die variëren van 169.254.21.0 tot 169.254.22.255 voor tunneladressen: [BGP](#)

[APIPA-adressen kiezen.](#)

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

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

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

Previous

Next : Review + create >

Parameters voor sitekoppelingen configureren

5) Zodra de informatie is bevestigd zoals bedoeld, 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

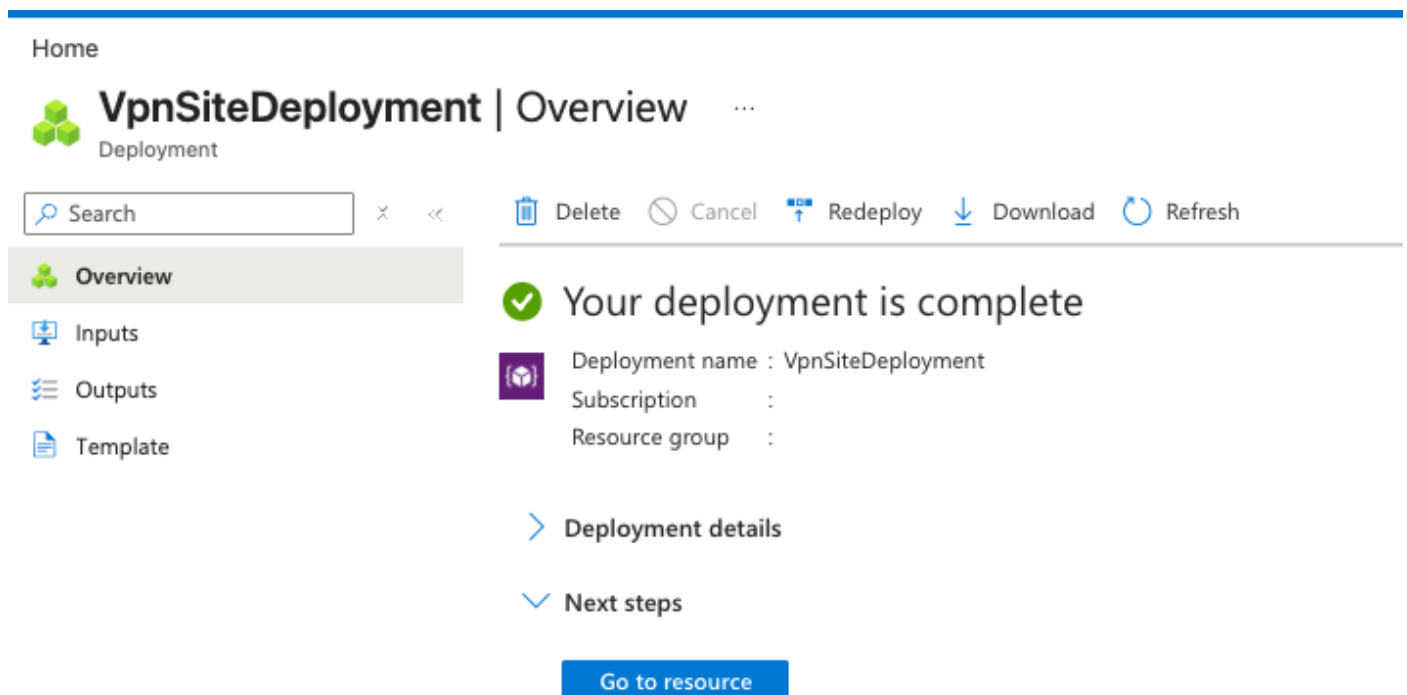
Region	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	
Links	

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

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

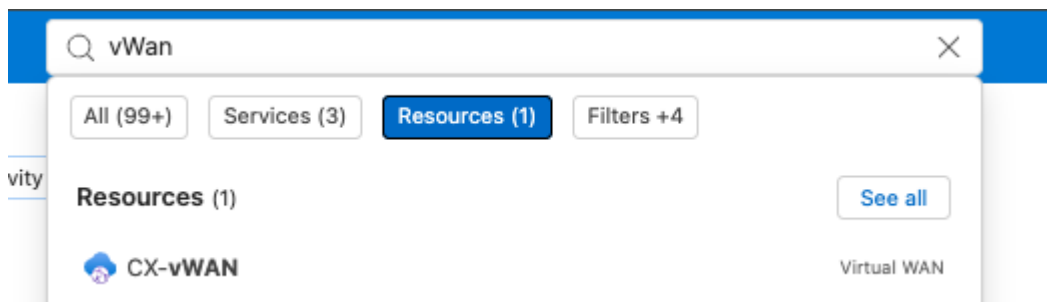
 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

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



The screenshot shows the 'VpnSiteDeployment | Overview' page in the Azure portal. The page has a left-hand navigation pane with links for 'Overview', 'Inputs', 'Outputs', and 'Template'. The main content area displays a green checkmark icon and the text 'Your deployment is complete'. Below this, it shows the deployment details: 'Deployment name : VpnSiteDeployment', 'Subscription :', and 'Resource group :'. There are also links for 'Deployment details' and 'Next steps', and a blue button labeled 'Go to resource'.

Voortgang implementatie virtuele WAN-site



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

Zoekopdracht voor virtueel WAN

Stap 2: Azure APIPA-gatewayparameters configureren

Azure vereist extra configuratie voor Automatic Private IP Addressing (APIPA)-adressen binnen de IPv4-adresruimte van 169.254.0.0/16.

1) Voer de bestaande hub in via Connectiviteit > Hubs.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Navigeer naar Virtual WAN Hub Connectivity

2) Navigeer nogmaals naar Connectivity > VPN (Site to Site) en klik op de hyperlink Gateway Configuration.

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

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

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

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites 1

Hyperlink Configuratie toegangspoort

3) Er verschijnt een zijpaneel om VPN Gateway te bewerken. Voer onder VPN Gateway Instance0 en VPN Gateway Instance1 twee unieke aangepaste BGP IP-adressen in die fungeren als naburige IP's voor elke instantie voor BGP-buurten via de IPsec-tunnels. Dit is nodig als u ervoor kiest om APIPA-adressering te gebruiken binnen deze topologie. Voer in het veld met het label Peer Address het IP van de buur van BGP in om de Azure-instanties te bereiken vanuit de FTD. Azure probeert geen BGP-vestiging met de FTD als APIPA-adressering in gebruik is, vandaar dat de FTD probeert eBGP buurvestiging over elke tunnel met Azure.

Het totaal komt uit op 2 links x 2 impliciete tunnels; één tunnel naar Instance0 en Instance1 per ISP-link; het totaal komt uit op vier IPsec-tunnels met BGP-buurten tussen Azure en de twee FTD ISP-interfaces.

Deze adressen moeten uniek zijn en in deze demonstratie moet het tweede en laatste hostadres in de /30-subnetten die aan elke tunnel zijn toegewezen, op de FTD worden geconfigureerd voor gebruik. Klik na configuratie op Bewerken.



Opmerking: controleer of u specifieke Azure-documentatie gebruikt als u adressen gebruikt die variëren van 169.254.21.0 tot 169.254.22.255 voor tunneladressen: [BGP APIPA-adressen kiezen](#)

Edit VPN Gateway



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

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ



Microsoft network



Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



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

Edit

Cancel

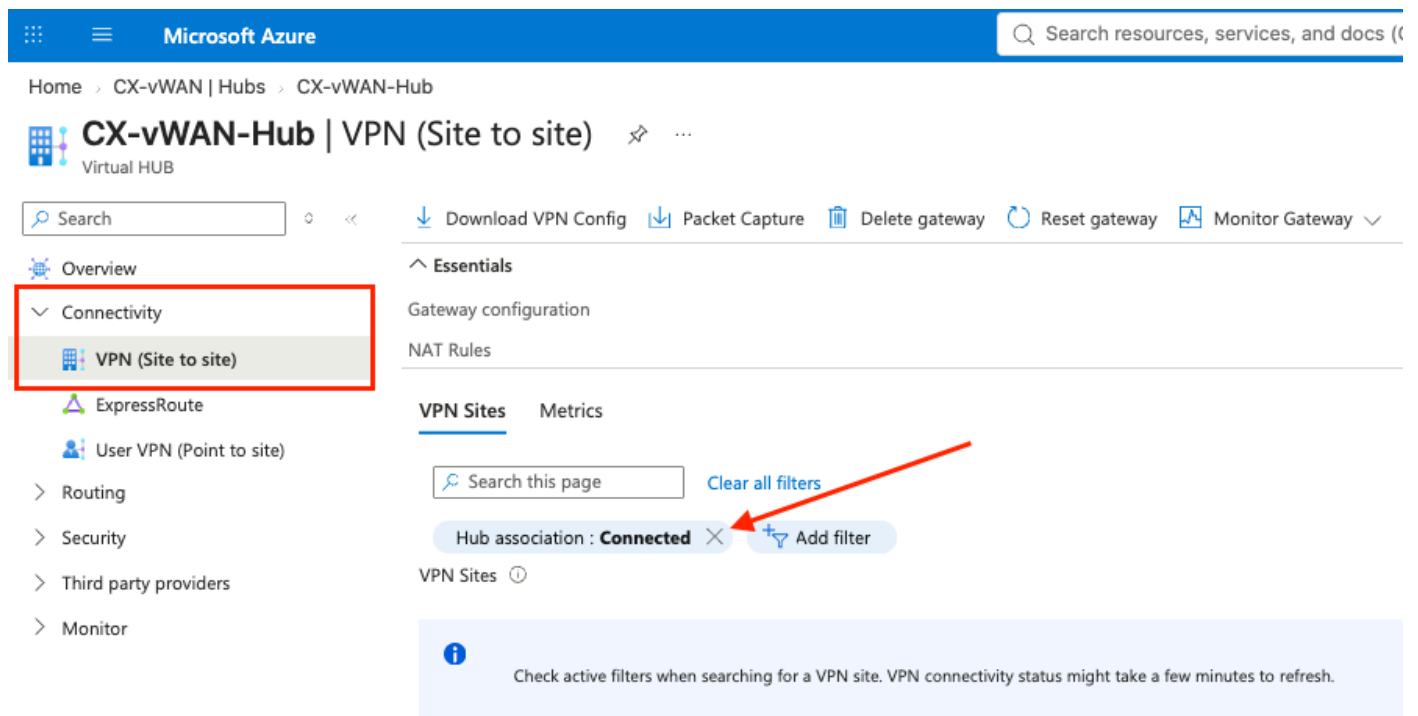
Aangepaste BGP IP-adressen voor VPN Gateway bewerken



Opmerking: Zoals Azure opmerkt, kan dit tot 30 minuten of meer duren om te updaten.

Stap 3: Azure vWAN Site VPN-parameters configureren

1) Klik op de pagina Connectiviteit > VPN (Site naar site) binnen de Azure vWAN Hub-configuratie en klik op de X om de Hub Association: Connected-filtering te wissen om losgekoppelde VPN-sites te bekijken.



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

Verbindingsfilters Hub-koppeling wissen

2) Schakel het selectievakje naast de onlangs geprovisioneerde VPN-site in en klik op VPN-site verbinden.

 Search

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

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

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

VPN Sites Metrics

 Search this page

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



Check active filters when searching for a VPN site. VPN connectivity status might take a few mi

 Create new VPN site  **Connect VPN sites**  Disconnect VPN sites  Refresh

Page: 1 ▼

Site name

↑↓ Location

  **Dual-ISP-Site**

VPN-siteactie verbinden

3) Configureer de gewenste vooraf gedeelde sleutel (PSK) en configureer de gewenste IPsec-parameters door op de optie Aangepaste schakelaar te klikken. Deze IPsec-parameters moeten in latere stappen overeenkomen met de FMC/FTD-configuratie. Klik op Verbinden om op te slaan.



Opmerking: Diffie-Hellman (DH) Group 24 ondersteuning werd verwijderd in FTD/FMC versie 6.7.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

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

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

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

Site name	↑↓	Region	↑↓
 Dual-ISP-Site		eastus	

Connect

Vooraf gedeelde sleutel- en IPsec-parameters configureren

4) Controleer of de VPN-siteprovisioning is voltooid.

Notifications



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

[Dismiss all](#)



Successfully created VPN connection



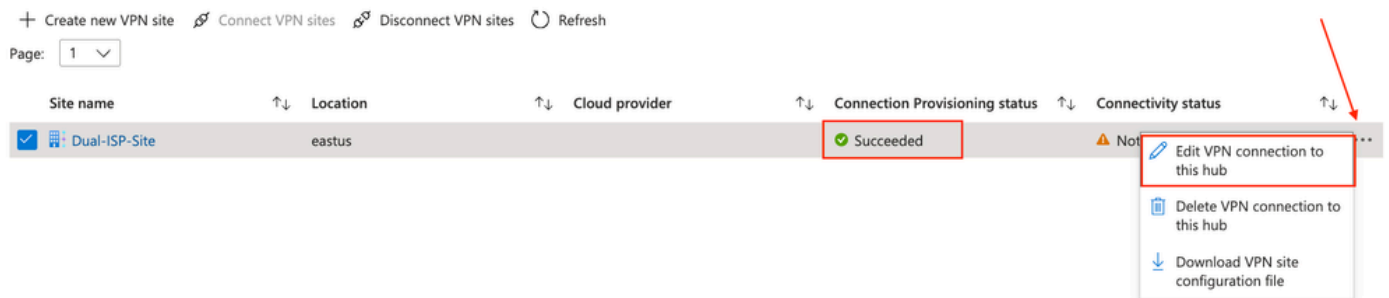
Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

Status VPN-siteprovisioning bevestigen

Stap 4: Aangepaste BGP APIPA inschakelen en activeren op VPN-site linkinstanties

1) Vernieuw de VPN-pagina (Site naar site) en bevestig dat de kolom Verbindingsvoorziening het succes aangeeft, waarmee u op de ellips kunt klikken en kunt klikken op de VPN-verbinding bewerken naar deze hub vervolgkeuzelijst.



Verbindingssucces valideren en VPN-verbinding bewerken

2) Klik om Link Connection 1 (ISP1) te configureren en voer de toepasselijke Pre-Shared Key (PSK) opnieuw in, en zorg ervoor dat u op de Enable toggle naast het Custom BGP IP Address klikt en toewijst wat het resterende hostadres zou zijn van de /30 subnetten die de interne-tunnelbestemming IP-adresveldwaarden zullen zijn van de BGP IP-header die door de FTD's wordt gegenereerd.

In wezen heeft ISP1 VTI Tunnel1 naar Azure Instance0 een adrestoewijzing van 169.254.21.1/30 en de tweede ISP1 VTI Tunnel2 die eindigt op de FTD heeft een IP van 169.254.22.1/30 toegewezen voor Instance1.

Klik op Volgende: Koppelingsverbinding 2> om door te gaan naar ISP 2-koppelingsparameters.



Opmerking: Het is mogelijk dat u uw PSK opnieuw moet invoeren en opnieuw op de optie Uitgelijnde PFS-groep moet klikken in het vervolgkeuzemenu in Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable

Disable

Connection status: NotConnected

Pre-shared key (PSK)

.....

Connection Mode

Default

Initiator Only

Responder Only

Border gateway protocol

Disable

Enable

Custom BGP IP Addresses

Disable

Enable

Custom BGP IP Address

Instance 0

169.254.21.2

Instance 1

169.254.22.2

Use Azure Private IP Address

Yes

No

Protocol

IKEv2

IKEv1

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

Use policy based traffic selector

Enable

Disable

IPsec

Default

Custom

SA Lifetime in seconds

27000

IKE Phase 1

Encryption

GCMAES256

Integrity/PRF

SHA384

DH Group

DHGroup14

IKE Phase 2(ipsec)

IPsec Encryption

GCMAES256

IPsec Integrity

GCMAES256

PFS Group

NONE

DPD timeout in seconds

45

Review + create

Previous

Next : Link connection 2 >

3) Herhaal de voorgaande stappen en pas de toepasselijke parameters toe onder Link Connection 2 (ISP2-link). Klik na voltooiing op Aanmaken.

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection **Enable** Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

Connection Mode ⓘ **Default** Initiator Only Responder Only

Border gateway protocol ⓘ Disable **Enable**

Custom BGP IP Addresses ⓘ Disable **Enable**

Custom BGP IP Address

Instance 0 ⓘ ▼

Instance 1 ⓘ ▼

Use Azure Private IP Address ⓘ Yes **No**

Protocol **IKEv2** IKEv1
To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ Enable **Disable**

IPsec ⓘ Default **Custom**

SA Lifetime in seconds * ⓘ

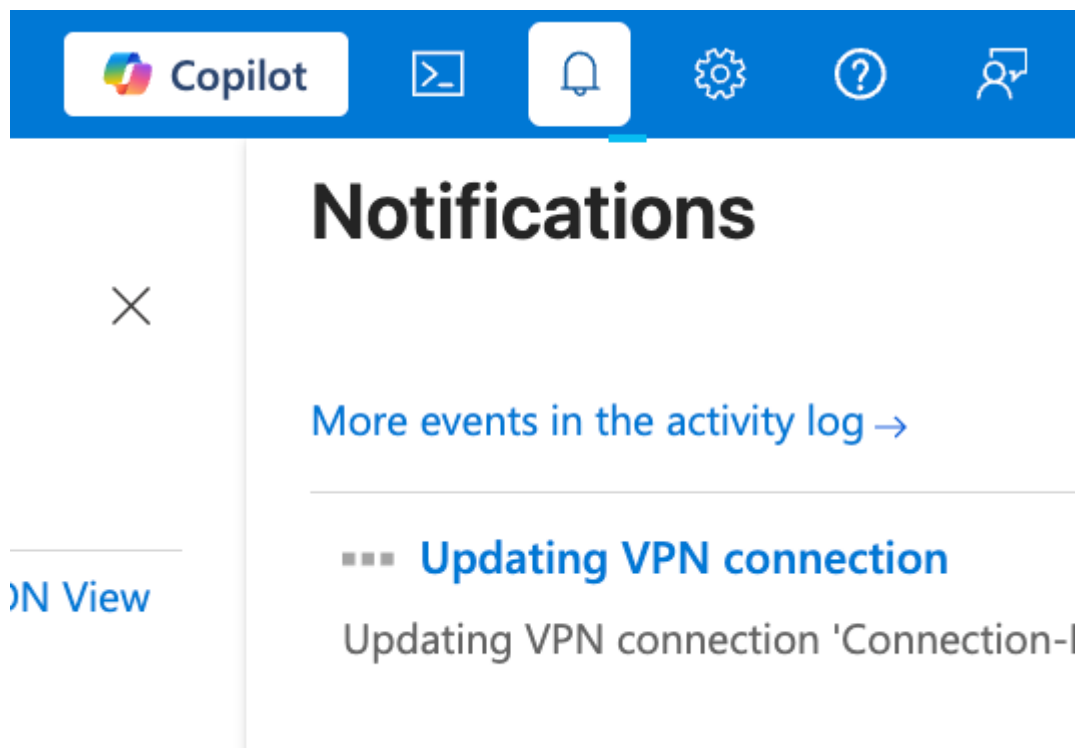
IKE Phase 1 ⓘ Encryption * Integrity/PRF * DH Group *
 ▼ ▼ ▼

IKE Phase 2(ipsec) ⓘ IPsec Encryption * IPsec Integrity * PFS Group *
 ▼ ▼ ▼

DPD timeout in seconds * ⓘ

**Create** Previous Next

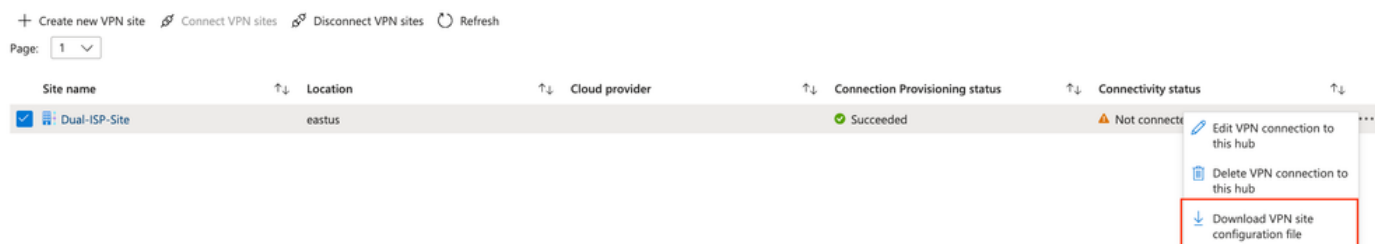
4) Meldingen in Azure UI tonen de updatetaak die begint.



Kennisgeving voor het starten van Azure Update Task

Stap 5: Het configuratiebestand van de VPN-site downloaden

1) Kies in dezelfde VPN-pagina (Site to Site) in Azure het ellipsiepictogram helemaal rechts van de geconfigureerde VPN-site en kies de optie VPN-siteconfiguratiebestand downloaden.



VPN-siteconfiguratiebestands optie downloaden

2) Klik hier om de hyperlink te downloaden.



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



Configuratiebestand VPN-site downloaden

Fase 2: FTD configureren voor dubbele ISP-connectiviteit met Azure vWAN

Stap 1: Analyseer de gedownloade VPN-configuratie

1) Open het gedownloade configuratiebestand en er verschijnt een vergelijkbare JSON-uitvoer (JavaScript Object Notation). De uitvoer toont een van de twee objecten die in het bestand zijn geschreven. Deze informatie biedt een nuttige context voor FTD-configuratie.



Opmerking: voor een betere scherpstelling worden verschillende irrelevante objecten en sleutel-/waardeparen gesnoeid voor een kortere duur.



Opmerking: ISP-Link-1 JSON object bestellen in het gedownloade bestand is omgekeerd. Ellipsis in de code-uitvoer vertegenwoordigt het ISP-2-Link-object met de toepasselijke configuratie.

```
...
{
  "configurationVersion": {
    "LastUpdatedTime": "2026-09-25T20:20:26.7658453Z",
    "Version": "15221e61-4e2c-42f5-b9e4-96d674f5a9a3"
  },
  "vpnSiteConfiguration": {
    "Name": "Dual-ISP-Site",
    "IPAddress": "FTD_ISP1_WAN_IP",
```

```

    "BgpSetting": {
      "Asn": 65532,
      "BgpPeeringAddress": "169.254.21.100",
      "PeerWeight": 32768
    },
    "LinkName": "ISP-1-Link"
  },
  "vpnSiteConnections": [
    {
      "gatewayConfiguration": {
        "IpAddresses": {
          "Instance0": "Inst0IP",
          "Instance1": "Inst1IP"
        },
        "BgpSetting": {
          "Asn": 65515,
          "CustomBgpPeeringAddresses": {
            "Instance0": [
              "169.254.21.22",
              "169.254.21.2"
            ],
            "Instance1": [
              "169.254.22.22",
              "169.254.22.2"
            ]
          }
        }
      },
      "connectionConfiguration": {
        "IsBgpEnabled": true,
        "PSK": "PSK",
        "IPsecParameters": {
          "IpsecEncryption": "GCMAES256",
          "IpsecIntegrity": "GCMAES256",
          "IkeEncryption": "GCMAES256",
          "IkeIntegrity": "SHA384",
          "PfsGroup": "None",
          "DhGroup": "DHGroup14",
          "SALifeTimeInSeconds": 27000
        }
      }
    }
  ]
}

```

Houd deze uitvoer als referentie bij het voltooien van de stappen.

Stap 2: Link BGP Update Source Loopback-interfaces configureren

Voor BGP-configuratievermeldingen in het kader van het FTD BGP-proces (geconfigureerd in latere stappen op de FTD) is een stabiele bron nodig die de corresponderende BGP-IP-adressen van de koppeling in Azure Site Link-configuratie vertegenwoordigt.

1) Ga naar Apparaten > Apparaatbeheer.

Cloud-delivered Firewall Management Center
Devices / Device Management

Monitor

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

Manage

- Policies >
- Objects
- Devices**

Devices

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

— Show less

Navigeer naar Apparaatbeheer in Firepower Management Center



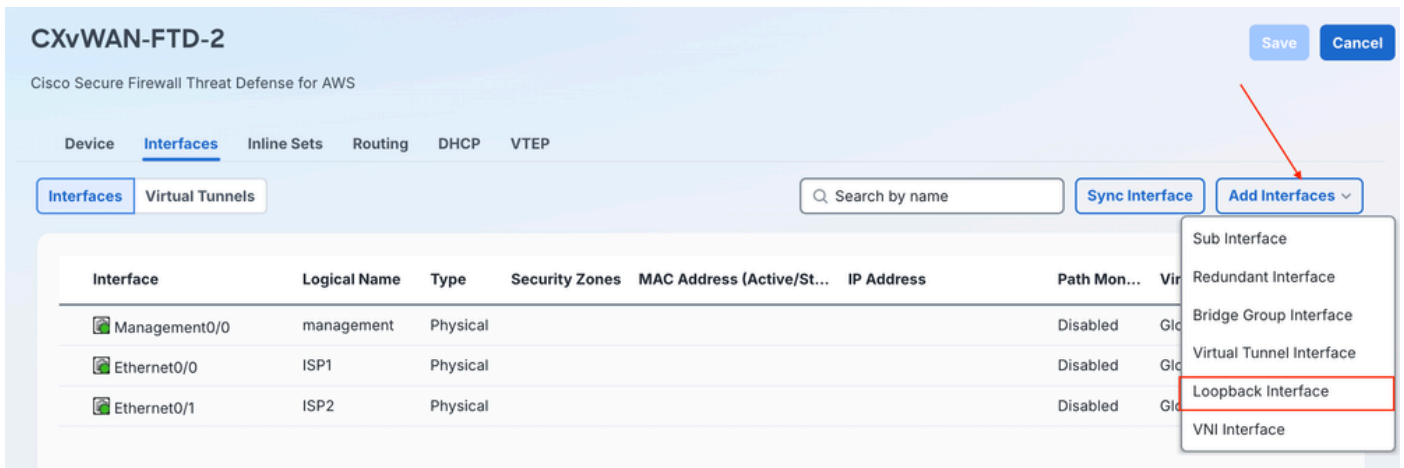
Opmerking: in dit lab wordt gebruikgemaakt van het door de cloud geleverde Firewall Management Center (cdFMC). De stappen blijven echter hetzelfde voor lokale FMC.

2) Klik op de FTD die u configureert als het filiaal / site VPN-apparaat met dubbele ISP-connectiviteit.

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

Selecteer de FTD voor configuratie-implementatie

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



Loopback-interface aan apparaat toevoegen

4) Voer een naam van de loopback-interface in, controleer of het selectievakje Ingeschakeld is ingeschakeld en voer een Loopback-ID in. Voer indien gewenst een beschrijving in. Klik na voltooiing op het tabblad IPv4.

Loopback-interfacegegevens en IPv4-adres configureren

5) Voer het loopback-IP-adres in om het BGP Link-IP-adres te zijn dat in eerdere stappen is geconfigureerd voor de ISP1-sitelink in Azure. Dit IP-adres wordt gebruikt als de BGP-updatebron voor de buurten die zijn geconfigureerd tussen de FTD- en Azure-instanties via ISP1.



Opmerking: U kunt verwijzen naar de waarde die eerder is gedefinieerd in de gedownload VPN-configuratie JSON onder `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress for ISP1`

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](#)

Voer het IPv4-adres in en klik op OK

6) Herhaal substappen c-e in deze reeks voor de ISP2 BGP Loopback-configuratie.

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

Eerste en tweede loopback-interfaces maken

7) Sla uw configuratie op.

You have unsaved changes [Save](#) [Cancel](#)

Wijzigingen opslaan

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

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

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 Policy

Secure Client Customization

Secure Client File

IKEv2 Policy

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

Add IKEv2 Policy

Filter

Name	
AES-GCM-NUL- SHA	Q ☐ ⚙
AES-GCM-NUL- SHA-LATEST	Q ☐ ⚙
AES- SHA - SHA	Q ☐ ⚙
AES- SHA - SHA-LATEST	Q ☐ ⚙
DES- SHA - SHA	Q ☐ ⚙
DES- SHA - SHA-LATEST	Q ☐ ⚙
Umbrella-AES-GCM-256	Q ☐ ⚙

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

Nieuw IKEv2-beleidsobject maken

2) 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, codering, pseudo-willekeurige functie (PRF) en DH Group. Kies welke algoritme/groep-elementen 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

SHA256

Cancel Save

IKEV2-beleid maken

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

Edit IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

1
2
5
14
15
16
19
20

Add

14

Cancel Save

IKEv2-beleid opslaan

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

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

Navigation Menu:

- 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-voorstel maken

5) Noem het IKEv2 IPsec-voorstel en zorg ervoor dat dezelfde instellingen worden uitgelijnd. Als u klaar bent, klikt u op Opslaan.

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



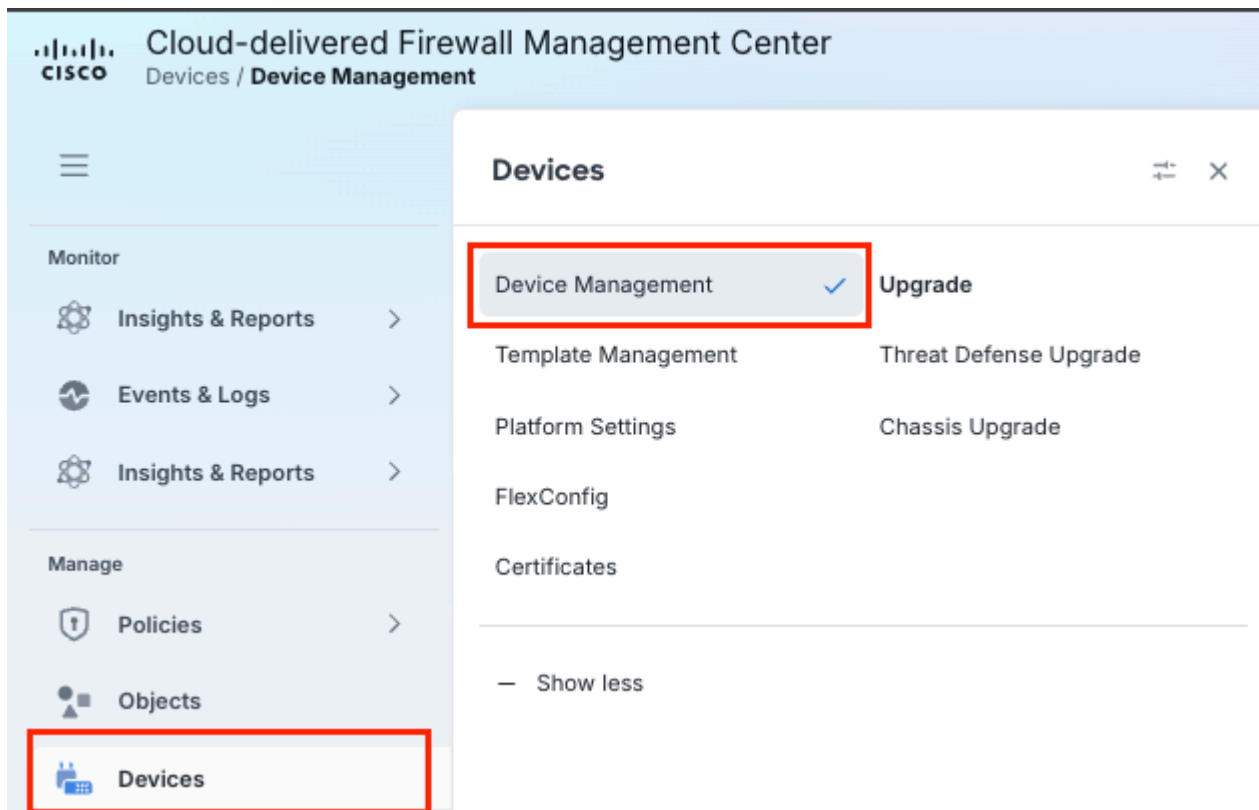
Cancel

Save

Geef het IKEv2 IPsec-voorstel een naam en klik op Opslaan

Stap 4: Virtuele tunnelinterfaces (VTI) configureren

1) Navigeer naar Apparaten > Apparaatbeheer.



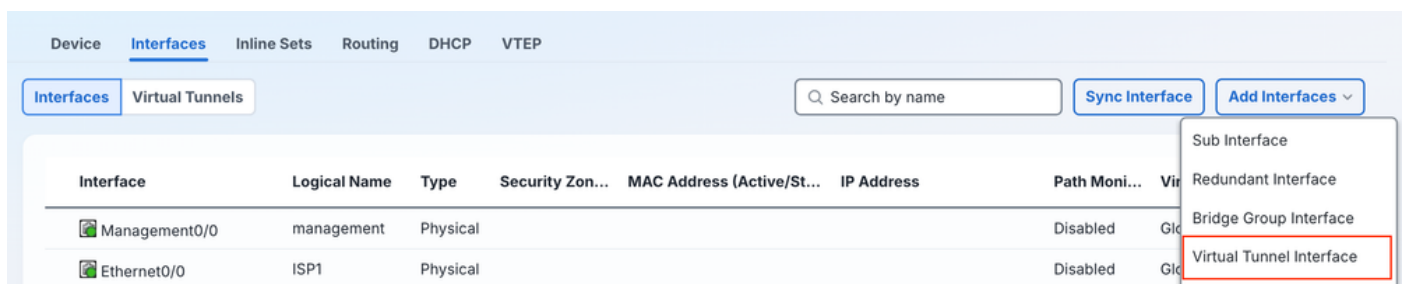
Navigeer naar Apparaatbeheer in Firepower Management Center

2) Klik op de FTD die u configureert als het filiaal / site VPN-apparaat met dubbele ISP-connectiviteit.

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

Selecteer de FTD voor configuratie-implementatie

3) Klik op het vervolgkeuzemenu Interfaces toevoegen en kies Virtual Tunnel Interface (VTI).



Virtuele tunnelinterface maken

4) Voer de tunnelinformatie in. Zorg ervoor dat het selectievakje Ingeschakeld is ingeschakeld, dat de naam is ingevoerd (desgewenst ook de beschrijving) en dat de optionele beveiligingszone is gekozen. Lijn de juiste ISP-interface van de bovenliggende interface uit om de VTI onder te configureren en configureer het juiste IP-adres voor de IPsec-connectiviteit in de binnentunnel voor de VTI. Druk op OK als u klaar bent.



Tip: Referentiediagram toont verdere context over mogelijke VPN-configuratie voor Azure dual-WAN-connectiviteit met FTD.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

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

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



Cancel

OK

5) Configureer 3 extra VTI's voor ISP1- en ISP2-interfaces van moedermaatschappijen.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
Ethernet0/0	ISP1	Physical				Disabled	Global
Tunnel1	ISP1-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.1/30(Static);	Disabled	Global
Tunnel2	ISP1-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.1/30(Static);	Disabled	Global
Ethernet0/1	ISP2	Physical				Disabled	Global
Tunnel3	ISP2-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.21/30(Static);	Disabled	Global
Tunnel4	ISP2-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.21/30(Static);	Disabled	Global
Loopback10	bgpLo-ISP1	Loopback			169.254.21.100/32(Static);	Disabled	Global
Loopback20	bgpLo-ISP2	Loopback			169.254.22.100/32(Static);	Disabled	Global

Extra virtuele tunnelinterfaces configureren

f) Zorg ervoor dat u op Opslaan klikt om uw wijzigingen op te slaan.

You have unsaved changes

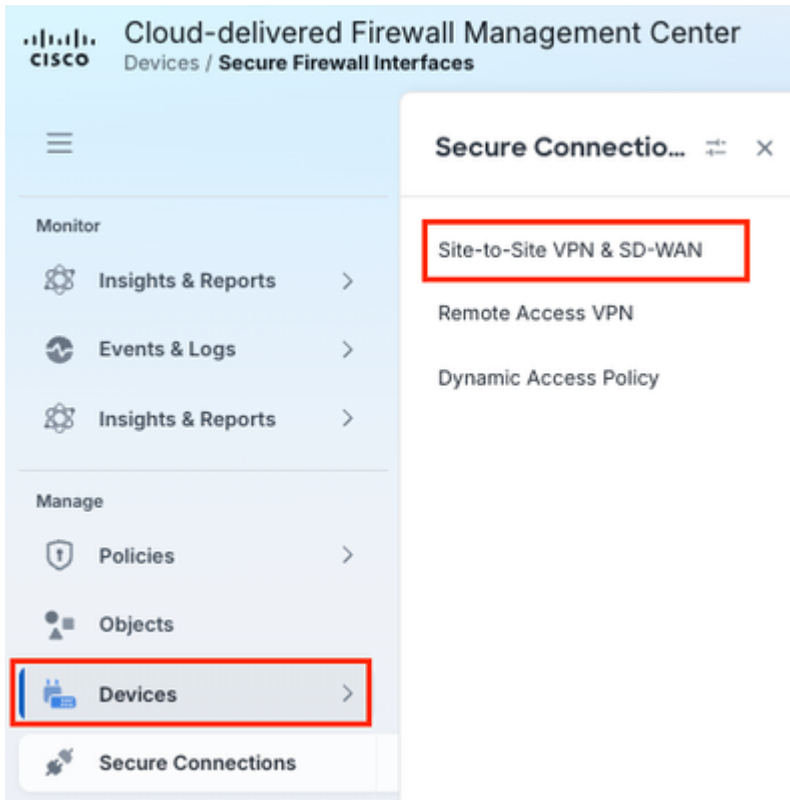
Save

Cancel

Wijzigingen opslaan

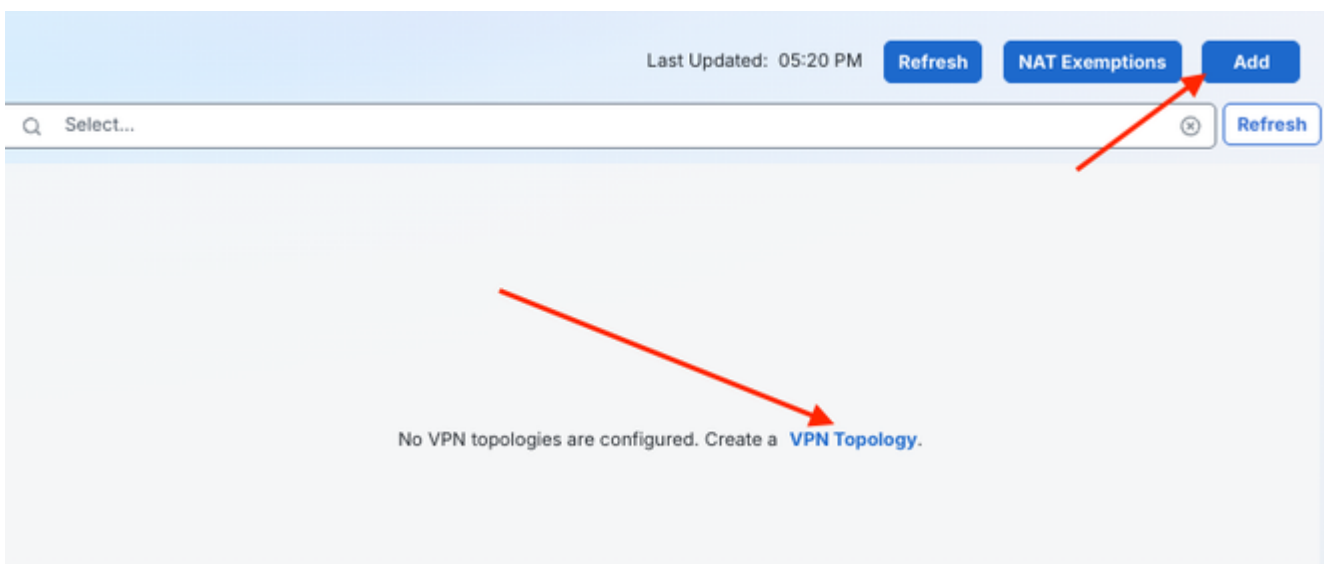
Stap 5: IPsec VPN-topologieën aanbieden

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



Site-naar-site VPN- en SD-WAN-verbindingen beheren

2) Klik op de eerste hyperlink voor de VPN-topologieconfiguratie in het midden van de eerste uitvoer of klik op de knop Toevoegen.



Nieuwe VPN-topologieconfiguratie toevoegen

3) Voer een topologienaam in voor de eerste tunnel via ISP1-koppeling naar Azure Instance0. Klik op de keuzerondje Route-Based VPN en klik op het topologietype Peer to Peer VPN. Klik na voltooiing op Aanmaken.

Create VPN Topology ?

Topology name *
 CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

☐ SD-WAN Topology New

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](#)

Type routegebaseerde VPN-topologie configureren

4) Kies eerst het Node A-apparaat en onder de vervolgkeuzelijst Apparaat die de FTD aangeeft die de VPN-tunnels van Azure beëindigt. Nadat de wizard de beschikbare VTI's van het apparaat heeft opgehaald, selecteert u de VTI die geschikt is voor de bovenliggende interface en instantie die u configureert in het vervolgkeuzemenu. In het menu Node B Device kiest u de Azure-zijde als Extranet-knooppunt in de VPN-topologieconfiguratie. Zorg ervoor dat u een vriendelijke naam configureert voor knooppunt B en zorg ervoor dat u het juiste IP-adres voor eindpunt invoert. Klik na voltooiing op het tabblad IKE om de fase 1-tunnelconfiguratie te implementeren.



Opmerking: U kunt de waarden voor het IP-adres van de instantie in het gedownloadede configuratiebestand raadplegen op
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` en
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Node A

Node B

Device:*

CXvWAN-FTD-2

Virtual Tunnel Interface:*

ISP1-Inst-0 (IP: 169.254.21.1)



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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

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

Additional



Device:*

Extranet

Device Name:*

Azure-ISP1-Link-Inst0

Endpoint IP Address:*

Cancel

Save

Knooppunt A- en knooppunt B-topologieeindpunten definiëren

5) Blader in het navigatiemenu naar IKEv2-instellingen en klik op het potloodpictogram om het beleid te bewerken naar het onlangs geconfigureerde IKEv2-beleid. Kies vervolgens de optie Handmatige sleutel vooraf in het vervolgkeuzemenu Verificatietype en voer de PSK in die eerder in Azure is geconfigureerd. Klik na voltooiing op het tabblad IPsec om de IPsec-tunnelparameters van fase 2 te configureren.



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

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Azure_IKEv2

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

IKEv2-instellingen en verificatiesleutel bewerken

6) Klik op het potloodpictogram naast de IKEv2 IPsec Proposal Transform Set en kies de eerder geconfigureerde IPsec-beleidsparameters. Zorg ervoor dat u de waarde Levensduur wijzigt om deze aan te passen aan de Azure vWAN VPN-instellingen. Zodra de geconfigureerde gegevens zijn bevestigd, klikt u op Opslaan.



Opmerking: U kunt de levensduurwaarde in het gedownloade configuratiebestand raadplegen op `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

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

Levensduur IPsec-voorstel configureren

7) Herhaal de vorige substappen binnen stap 5 om de andere Azure Tunnels te maken in ISP1 Instance1, ISP2 Instance0 en ISP2 Instance1.

> CXvWAN-SiteB-ISP-1-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-1-Inst-1	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-2-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-2-Inst-1	Route Based (VTI)	Point-to-Point	0- Tunnels	✓		

Aanvullende site naar site VPN-topologieën maken

Stap 6: Valideren van VPN-topologieën

Voer diagnostische cli voor systeemondersteuning in, typ en druk op enter (alleen-lezen CLI).

1) Controleer de connectiviteit van de IKE-tunnel in fase 1.

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

2) Controleer de IPsec fase 2-connectiviteit.

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



Opmerking: bij het bekijken van IPsec Security Associations (SA) -uitvoer en pkts nemen decaps en pkts decrypt-tellers toe, maar pkts encaps en pkts encrypt zijn dat niet, dit wordt in dit scenario verwacht. Azure probeert BGP-buurten te vormen via de Hub Private IP Space-adressen en Azure start geen onderhandelingen als het naburige einde APIPA BGP-adressen gebruikt. Het is de verantwoordelijkheid van het apparaat dat verbinding maakt met Azure om BGP-onderhandelingen te starten wanneer aangepaste APIPA wordt gebruikt.

3) Controleer de Layer 2-connectiviteit.

```
show arp
```

4) Controleer IP-routing.

```
show route
```

5) Capture uitvoeren op ISP1 en ISP2 interfaces.

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

6) Azure-verificatie - Navigeer naar vWAN Hub > Connectiviteit.> VPN-sites > Kies de geconfigureerde site.

Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ ISP-1-Link	ISP1	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub
☐ ISP-2-Link	ISP2	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Verificatie van Azure Link Connectivity

Stap 7: ECMP configureren

1) Navigeer naar Beheer > Apparaten > Apparaatbeheer en klik op de FTD.

The screenshot shows the Cisco Cloud-delivered Firewall Management Center interface. The left sidebar contains a navigation menu with sections 'Monitor' and 'Manage'. Under 'Monitor', there are three 'Insights & Reports' items. Under 'Manage', there are 'Policies' and 'Objects'. The 'Devices' item at the bottom of the 'Manage' section is highlighted with a red box. The main panel is titled 'Devices' and contains a list of management options: 'Device Management' (which is selected with a blue checkmark and highlighted with a red box), 'Template Management', 'Platform Settings', 'FlexConfig', and 'Certificates'. To the right of these options are buttons for 'Upgrade', 'Threat Defense Upgrade', and 'Chassis Upgrade'. At the bottom of the main panel, there is a 'Show less' link.

Navigeer naar Apparaatbeheer in Firepower Management Center

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

Selecteer de FTD voor configuratie-implementatie

2) Klik op het tabblad Routing en kies ECMP.

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

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

Configuratie-instellingen voor meerdere paden voor gelijke kosten

3) Klik op Toevoegen.

Equal-Cost Multipath Routing (ECMP)

Add

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

Configuratie-instellingen voor meerdere paden voor gelijke kosten toevoegen

4) Geef de ECMP-zone een naam en klik op de beschikbare VTI-interfaces, klik vervolgens op de knop Toevoegen om deze toe te passen op de kolom Geselecteerde interfaces en klik op OK.

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

Selecteer interfaces voor de Equal Cost Multi Path Zone

5) Zorg ervoor dat u uw wijzigingen opslaat.

You have unsaved changes

Save

Cancel

Wijzigingen opslaan

Stap 8: BGP configureren

1) Schakel het BGP-proces in op de FTD onder Routing > Algemene instellingen > BGP. Schakel het selectievakje BGP inschakelen in en voer het AS-nummer in dat eerder is geconfigureerd in fase 1, stap 1d. Navigeer naast Routing > BGP > IPv4.

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

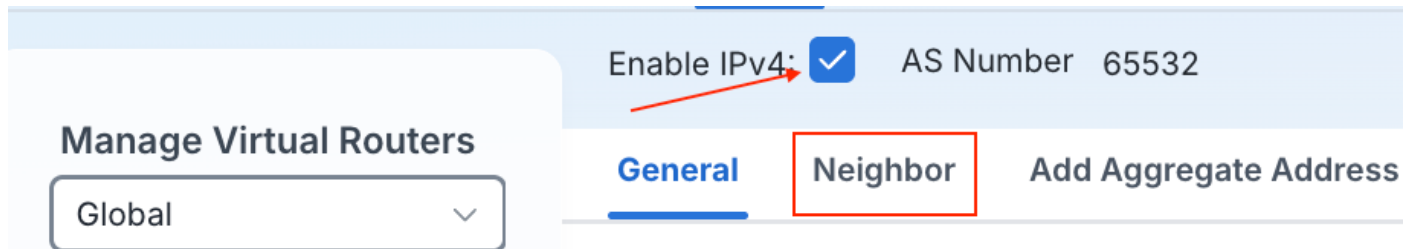
Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

Het Border Gateway Protocol-proces inschakelen onder Algemene instellingen

2) Zorg ervoor dat u het selectievakje IPv4 inschakelen voor het BGP-proces aanvinkt en klik op **Buurman** om BGP-buren in Azure te configureren.



Manage Virtual Routers

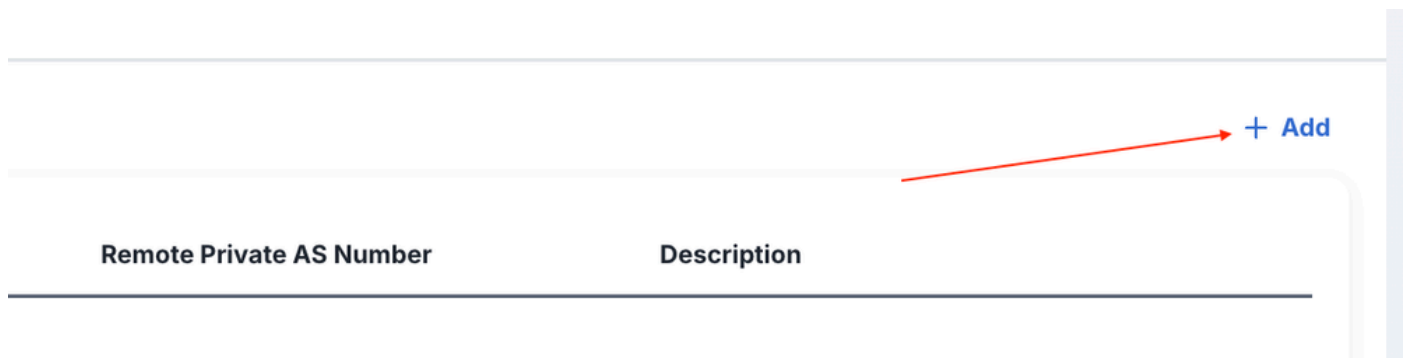
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

IPv4 Border Gateway-protocolproces inschakelen

3) Klik op + Toevoegen.



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

+ Add

Nieuw Border Gateway-protocol toevoegen

4) Voer de ISP1 Instance0 BGP peering-informatie in, verwijst naar de genoteerde BGP AS van de vWAN Hub en voer deze in als de Neighbor Remote AS, en voeg desgewenst een Beschrijving toe. Klik op **Advanced** (Geavanceerd).



Opmerking: Zorg ervoor dat u de BGP-updatebron kiest om te verwijzen naar de Loopback voor VTI-interfaces op de FTD die is toegewezen aan de ISP1-koppeling die is geconfigureerd in Azure.

Add Neighbor ?

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Peeringgegevens van randgateway-protocol configureren

5) In het Geavanceerde menu van de BGP Neighbor configuratie op FTD, kunt u het aantal Time To Live (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. Klik op OK.

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Geavanceerde instellingen voor het Border Gateway Protocol Neighbor

6) Herhaal substappen 3-5 om Tunnel2 voor ISP1 Instance1 te configureren.

7) Herhaal substappen 3-5 tweemaal om de ISP2 Instance0/Instance1 BGP peering informatie te configureren.



Opmerking: Zorg ervoor dat u de uitgelijnde BGP-updatebron kiest die verwijst naar de Loopback voor VTI-interfaces op de FTD die is toegewezen aan de ISP2 Link die is geconfigureerd in Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

Configuratie ISP2-instantie 1 BGP-buurman

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

- ☒ Enabled address
- ☐ AS Override
- ☐ Shutdown administratively
- ☐ Configure graceful restart (failover/spanned mode)
- ☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes Routes Timers **Advanced** Migration

- ☐ Enable Authentication
- Enable Encryption
- 0
- Password
-
- Confirm Password
-
- ☐ Send Community attribute to this neighbor
- ☐ Use itself as next hop for this neighbor
- ☐ Disable Connection Verification
- ☒ Allow connections with neighbor that is not directly connected
- ☐ Limited number of TTL hops to neighbor
- TTL Hops
- 10
- (1-255)
- ☐ Use TCP path MTU discovery
- TCP Transport Mode
-

Cancel

OK

Configuratie ISP 2-instantie 2 BGP-buurman

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.21.2	65515	Enabled		
169.254.22.2	65515	Enabled		
169.254.21.22	65515	Enabled		
169.254.22.22	65515	Enabled		

Klik na voltooiing op Opslaan.

You have unsaved changes

Save

Wijzigingen opslaan

Standaard installeert BGP slechts één beste pad in de routingstabel, hoewel ECMP is geconfigureerd voor alle VTI's naar Azure. BGP-multipad moet afzonderlijk worden ingeschakeld, zodat beide aangeleerde paden tegelijkertijd worden geïnstalleerd en gebruikt.

Stap 9: eBGP-multipad configureren

1) Navigeer naar Routing > BGP > IPv4, klik op het tabblad General en klik op het potloodpictogram naast Forward Packets Over Multiple Paths.

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

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

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Routes

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	No
(Use filtering to limit the number of prefixes that are redistributed)	

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

Pakketten doorsturen via meerdere paden instellen

2) Wijzig de standaardwaarde van het veld Aantal paden van 1 naar 4. Klik op OK.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Vooruitpakketten wijzigen via meerdere paden instellen

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

Controleren/Problemen oplossen

Nadat de implementatie is voltooid, moet u bevestigen dat het FTD BGP-proces aangrenzende verbindingen met beide Azure-instanties op de respectieve tunnels tot stand brengt en dat routes worden geleerd, interfaces worden geopend en protocolverbindingen worden geretourneerd in de verbindingstabel.

Navigeer naar `system support diagnostic-cli` op FTD CLI zoals gedaan in fase 2, stap 7.

1) Eenmaal geïmplementeerd, worden BGP-buren verwacht te komen en prefixes 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#
```

```
ftd#
```

```
show bgp summary
```

```

BGP router identifier 169.254.22.100, local AS number 65532
BGP table version is 29, main routing table version 29
2 network entries using 400 bytes of memory
8 path entries using 640 bytes of memory
2 multipath network entries and 8 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1272 total bytes of memory
BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

```

```

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.21.2 4 65515 20 17 29 0 0 00:13:14 2
169.254.22.2 4 65515 20 20 29 0 0 00:13:22 2
169.254.21.22 4 65515 19 21 29 0 0 00:13:19 2
169.254.22.22 4 65515 20 19 29 0 0 00:13:17 2
ftd#

```

2) Controleer of de routes die van Azure zijn ontvangen, worden weergegeven als multipath-routes.

```
<#root>
```

```
ftd#
```

```
show bgp
```

```

BGP table version is 29, local router ID is 169.254.22.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i
*m 172.27.0.0	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i

3) Controleer de populatie van 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 172.31.3.33 to network 0.0.0.0

```

B          10.2.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
          [20/0] via 169.254.22.2, 00:20:53
          [20/0] via 169.254.21.22, 00:20:53
          [20/0] via 169.254.21.2, 00:20:53
B          172.27.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
          [20/0] via 169.254.22.2, 00:20:53
          [20/0] via 169.254.21.22, 00:20:53
          [20/0] via 169.254.21.2, 00:20:53
  
```

4) Controleer de verbindingstabel voor BGP-sessies.

<#root>

ftd#

show conn all | include TCP|179

```

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

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.