

Azure vWAN Site-to-Site-VPN für sichere Firewall konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Diagramm](#)

[Eine DIA-Link-vWAN-Verbindung zwischen Azure und FTD \(Azure Load Balancing/Redundanz\)](#)

[Konfigurieren](#)

[Phase 1: Azure vWAN/Hub-Konfiguration](#)

[Schritt 1: vWAN erstellen](#)

[Phase 2: vWAN-Hub erstellen](#)

[Phase 2: Azure vWAN-VPN-Standortkonfiguration](#)

[Schritt 1: Azure vWAN-VPN-Site erstellen \(Remote-FTD-Gerät\)](#)

[Phase 2: Azure vWAN-Site-VPN-Parameter konfigurieren](#)

[Schritt 3: Azure vWAN-Site-Tunnelkonfiguration herunterladen](#)

[Phase 3: FTD-Konfiguration](#)

[Schritt 1: Azure VPN-Konfiguration analysieren](#)

[Phase 2: Loopback konfigurieren](#)

[Schritt 3: Richtlinienobjekte der Phase 1/Phase 2 konfigurieren](#)

[Schritt 4: Sichere Verbindung mit Azure konfigurieren](#)

[Schritt 5: Überprüfen der ersten Verbindung mit Azure](#)

[Schritt 6: Konfigurieren von Second Tunnel zu Azure Instance1-Endpunkt](#)

[Schritt 7: Konfigurieren von ECMP](#)

[Schritt 8: Konfigurieren statischer Routen für private Instanzen von IPs](#)

[Schritt 9: BGP konfigurieren](#)

[Phase 10: Konfigurieren von BGP Multi-Path](#)

[Überprüfung](#)

[Weitere Überlegungen](#)

[AS-Pfad steht vor](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration der standortübergreifenden Microsoft Azure Virtual WAN (vWAN)-VPN-Verbindung mit der Cisco Secure Firewall beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure FTD Version 10.0
- Cisco Secure FMC Version 10.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Microsoft Azure Virtual WAN (vWAN) kombiniert mehrere Azure-Netzwerk-, Sicherheits- und Routing-Funktionen in einem einzigen Hub-Konstrukt. Jeder vWAN-Hub kann ein von Microsoft verwaltetes Site-to-Site-VPN-Gateway hosten, über das Remote-Geräte wie die sichere Firewall auf Azure zugreifen, ohne die Gateway-Infrastruktur erstellen und warten zu müssen.

Im Gegensatz zu einem herkömmlichen IPsec-VPN mit zwei Endpunkten wird das Azure vWAN-Site-to-Site-VPN-Gateway als Aktiv-Aktiv-Paar von Instanzen (Instance0 und Instance1) bereitgestellt, die jeweils eine eigene öffentliche IP-Adresse und eine eigene Border Gateway Protocol (BGP)-Peering-Adresse aufweisen. Um beide Instanzen für Redundanz und zusätzlichen Durchsatz zu nutzen, richtet die FTD der Außenstelle einen IP-Sicherheits- (IPsec)-Tunnel zu jeder Instanz ein und nutzt BGP anstelle von statischem Routing allein, um Routen dynamisch zu erfassen und zu entfernen, wenn Instanzen verfügbar oder nicht verfügbar werden. Beim Equal-

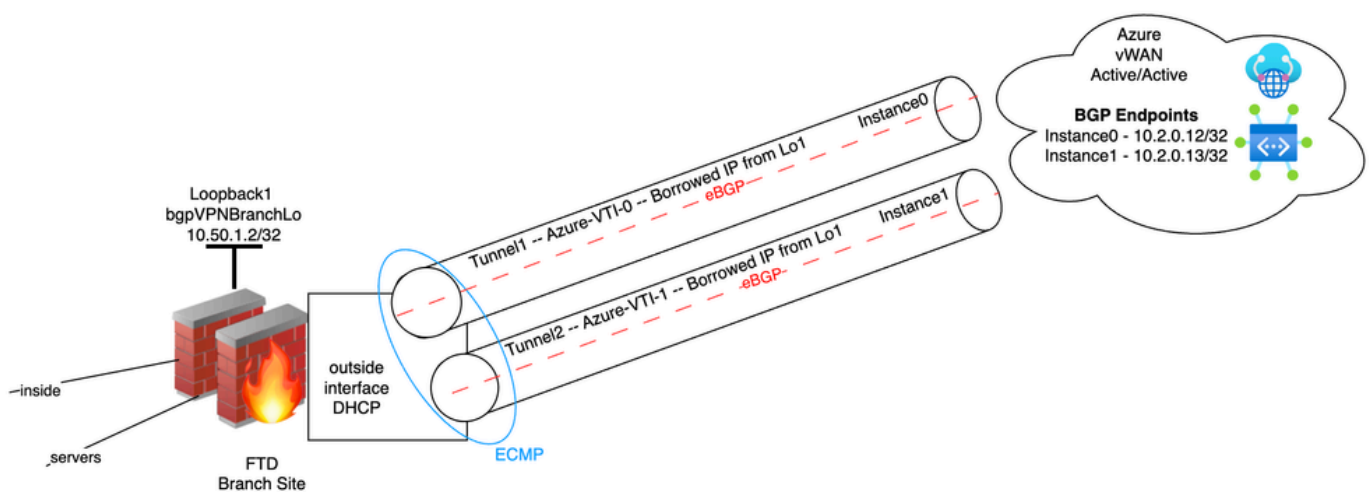
Cost Multi-Path (ECMP)-Routing und BGP Multipath auf dem FTD bleiben dann beide Tunnel gleichzeitig aktiv, anstatt einen als passiven Standby-Tunnel zu behandeln.

In diesem Dokument wird dieses Design in drei Phasen konfiguriert: Die Objekte Azure vWAN Hub und VPN Site werden zuerst erstellt, die resultierenden Verbindungsparameter werden heruntergeladen, und diese Parameter werden dann verwendet, um übereinstimmende Virtual Tunnel Interfaces (VTIs), Internet Key Exchange Version 2 (IKEv2)/IPsec-Richtlinien, statische Routen, ECMP- und BGP-Peering auf dem FTD über FMC zu konfigurieren.

Diagramm

Das Diagramm zeigt die Topologie der in diesem Artikel beschriebenen Konfiguration. Die DIA-Variante (Direct Internet Access) bezieht beide Azure-Tunnel von einer externen Schnittstelle auf dem FTD.

Eine DIA-Link-vWAN-Verbindung zwischen Azure und FTD (Azure Load Balancing/Redundanz)



Konfigurieren

Führen Sie die drei Phasen der Reihe nach aus. Die in Phase 1 und Phase 2 erstellten Azure-seitigen Objekte generieren die Peer-IP-Adressen, BGP Autonomous System (AS)-Nummern und den vorinstallierten Schlüssel, die dann in Phase 3 für die FTD gelten.

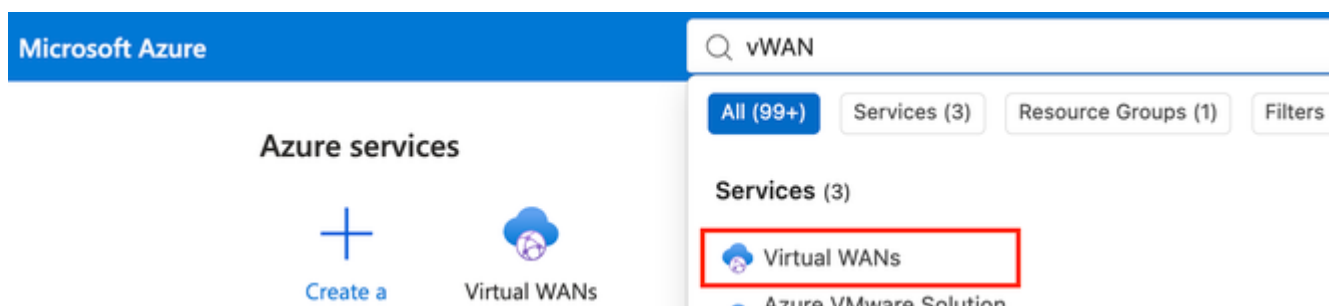
Phase 1: Azure vWAN/Hub-Konfiguration



Anmerkung: Die Konfigurationsschritte in diesem Dokument sind grob aufgebaut und enthalten die erforderlichen Schritte zum Verbinden des FTD mit Azure vWAN. Weitere Informationen zur Bedeutung der Konfigurationen finden Sie in der Azure vWAN-Dokumentation von Microsoft. Siehe [Was ist Azure Virtual WAN?](#) und weitere Dokumentation.

Schritt 1: vWAN erstellen

a) Suchen Sie im Azure-Suchfeld nach vWAN, und klicken Sie auf Virtual WANs.



b) Klicken Sie auf + Erstellen.



c) Geben Sie einen Namen für die neue vWAN-Instanz ein, klicken Sie auf Prüfen + Erstellen, und klicken Sie auf der Seite Prüfen + Erstellen im Assistenten auf Erstellen.

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 >



Anmerkung: Für die Veröffentlichung dieses Dokuments ist Leerraum vorgesehen, der Werte in verschiedenen Feldern in den Bildern abdeckt.

d) Klicken Sie auf Zur Ressource wechseln.



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

Phase 2: vWAN-Hub erstellen

a) Navigieren Sie zu Connectivity > Hubs, und klicken Sie auf + 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) Weitere Informationen zur weiteren Konfiguration finden Sie in der Azure-Dokumentation. Stellen Sie sicher, dass der zugewiesene private Hub-Adressraum keinen der internen Adressräume überschneidet. Konfigurieren des Namens, des virtuellen Hubs, der Hub-Routingeinstellungen. Klicken Sie auf Weiter: Site-to-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

Review + create Previous Next : Site to site >

Creating a hub with a gateway will take 30 minutes.

c) Weitere Informationen zu den vorgestellten Feldern finden Sie in der Dokumentation zu Microsoft Azure vWAN Hub. Schalten Sie auf Ja, um eine Site-to-Site (VPN-Gateway) zu erstellen. Die standardmäßig zugewiesene AS-Nummer (BGP Autonomous System) ist 65515, wie von der Internet Engineering Task Force (IETF) in Request For Comments (RFC) 6996 zur Definition der AS-Reservierung für private Nutzung zugewiesen.



Anmerkung: Notieren Sie sich das BGP AS für zukünftige Konfigurationsschritte auf dem 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 >

Klicken Sie auf Prüfen + Erstellen oder auf Weiter : Zeigen Sie auf Site >, um optionale Einstellungen zu konfigurieren.

d) Klicken Sie nach Überprüfung der Übersicht auf Erstellen.



Anmerkung: Wie Azure angibt, dauert die Erstellung des Hubs 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) Suchen Sie nach Abschluss der Bereitstellung nach dem ursprünglichen vWAN-Ressourcennamen. Um die Suche weiter einzugrenzen, klicken Sie auf Ressourcen.

VirtualHubDeployment | Overview ...

Deployment

Search x << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

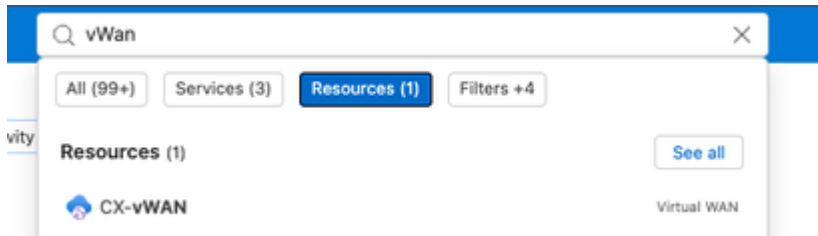
✓ Your deployment is complete

Deployment name : VirtualHubDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

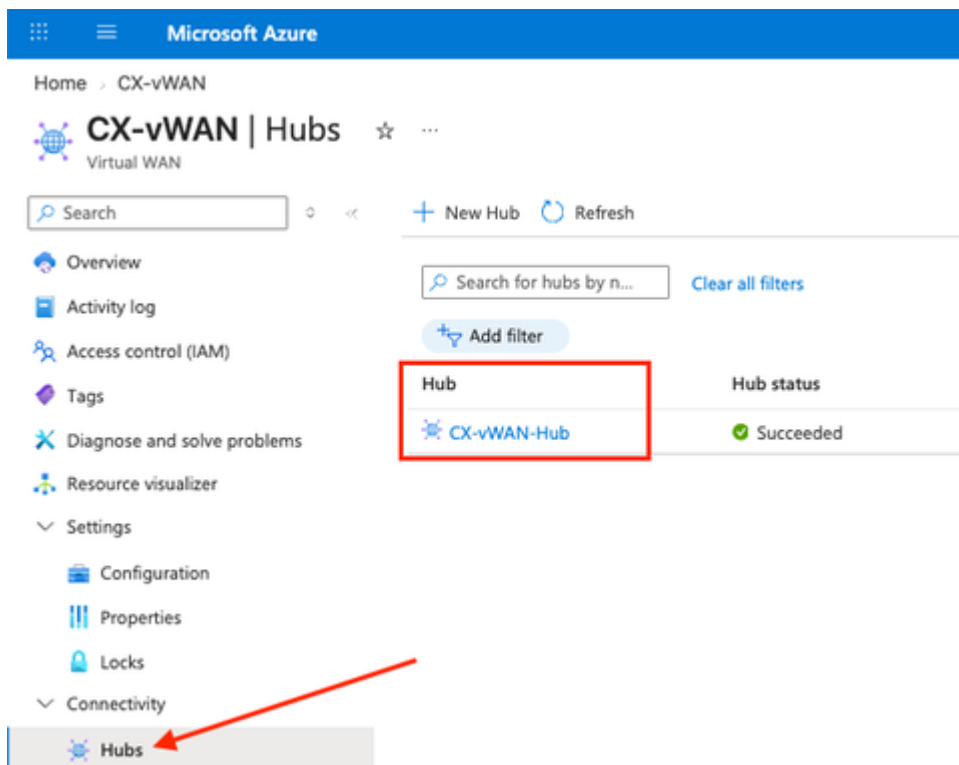
[Go to resource](#)



Phase 2: Azure vWAN-VPN-Standortkonfiguration

Schritt 1: Azure vWAN-VPN-Site erstellen (Remote-FTD-Gerät)

a) Geben Sie über Connectivity > Hubs den erstellten Hub ein, und klicken Sie auf den in den vorherigen Schritten erstellten Hub.



b) Klicken Sie auf Connectivity > VPN (Site to Site), und klicken Sie auf + Create new VPN site (Neue VPN-Site erstellen).

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) Geben Sie die Werte in die erforderlichen Felder ein. Klicken Sie abschließend auf Weiter: Links > um fortzufahren.

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) Geben Sie die erforderlichen Linkinformationen ein. Die Felder Link BGP Address (BGP-Adresse verknüpfen) und Link ASN (ASN verknüpfen) geben die BGP-Layer-3-Zieladresse und die BGP-ASN-Nummer im Innentunnel der Außenstelle wieder, mit der die Nachbarschaft mit Azure über die standortübergreifenden Tunnel gebildet wird. Die Link-BGP-Adresse ist eine sich nicht überlappende Subnetzadresse (/32) außerhalb des zuvor konfigurierten Subnetzes für den privaten Hub-Adressraum, das Azure als /32-Route installiert, um es als BGP-Nachbar zu erreichen. Die Link-IP-Adresse/der FQDN ist die Layer-3-Ziel-IP-Adresse des Datenverkehrs am Außenstellenstandort, der für die Bereitstellung der IPsec-/IKEv2-Verbindung erforderlich ist.



Anmerkung: Wenn Sie für Tunneladressen Adressen zwischen 169.254.21.0 und 169.254.22.255 verwenden, überprüfen Sie, [wie Sie BGP für Azure VPN Gateway](#) für bestimmte Anforderungen [konfigurieren](#).

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) Nachdem Sie die Richtigkeit der Einstellungen bestätigt haben, klicken Sie auf Erstellen.

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) Kehren Sie nach Abschluss der VPN-Bereitstellung zur Konfiguration des vWAN-Hub zurück.

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

Phase 2: Azure vWAN-Site-VPN-Parameter konfigurieren

a) Geben Sie über Connectivity > Hubs den erstellten Hub ein, und klicken Sie auf den in den vorherigen Schritten erstellten Hub.

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) Navigieren Sie erneut zu Connectivity > VPN (Site to Site), und klicken Sie auf das X, um die Hub-Zuordnung zu löschen: Verbundene Filter zum Anzeigen nicht verbundener Standorte.

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

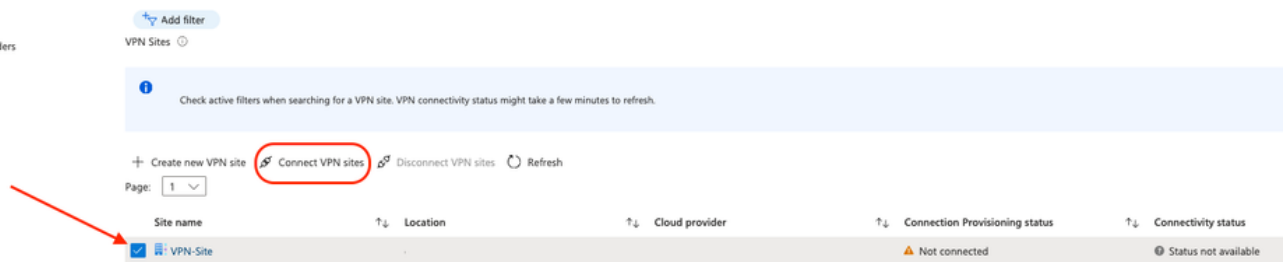
Search this page Clear all filters

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) Aktivieren Sie das Kontrollkästchen neben dem zuvor konfigurierten VPN-Standort, und klicken Sie dann auf VPN-Standorte verbinden, das aktiviert wird, nachdem der Standort ausgewählt wurde.



d) Die Seitenleiste "Standorte verbinden" wird angezeigt. Geben Sie einen Pre-Shared Key (PSK) ein, und konfigurieren Sie die gewünschten IPsec-Einstellungen für Phase 1 IKEv2 und Phase 2. Wenn Sie Benutzerdefiniert aus der IPsec-Dropdown-Liste auswählen, werden die Werte automatisch eingetragen. Beachten Sie diese Werte, da sie auf dem FTD übereinstimmen müssen. Sie müssen außerdem auswählen, ob Perfect Forward Secrecy (PFS) gewünscht wird. Da es sich um einen routenbasierten Tunnel handelt, konfigurieren Sie die Einstellungen entsprechend. Klicken Sie abschließend auf Verbinden, um die Konfiguration zu speichern.



Anmerkung: Weitere Informationen finden Sie unter [Standard- und benutzerdefinierte IPsec-Richtlinien Azure vWAN](#).

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) Es werden Informationen zur Aktualisierung des Kabelmodems sowie zur voraussichtlichen Fertigstellungszeit angezeigt.

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

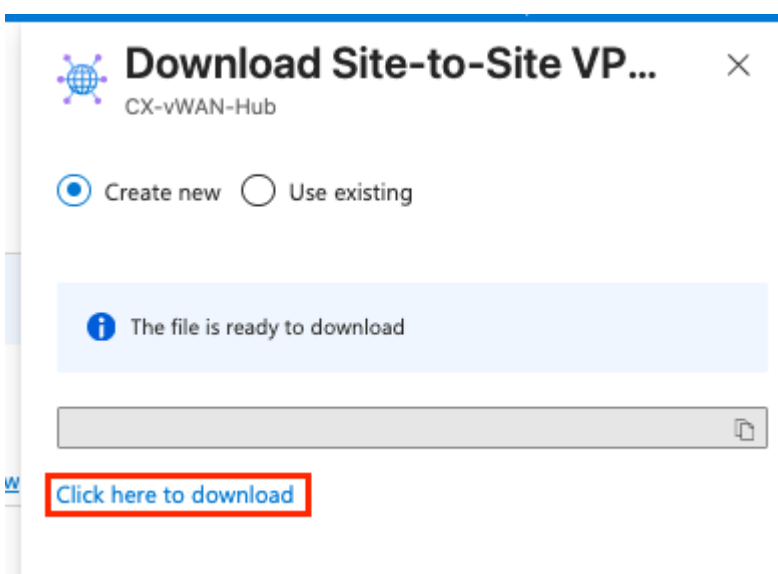
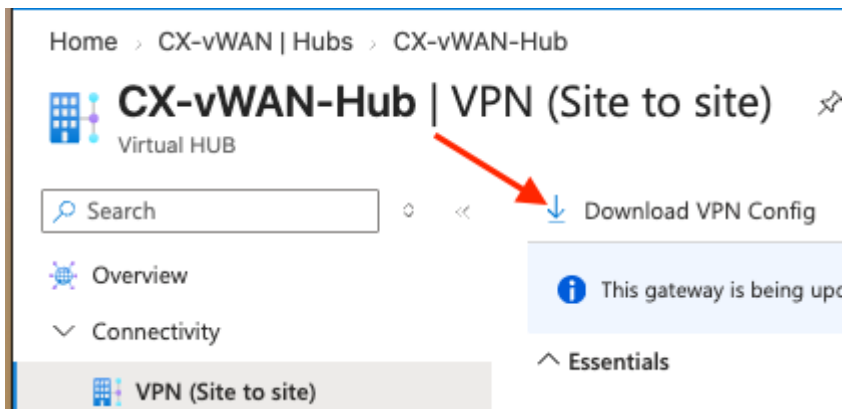
Connectivity



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

Schritt 3: Azure vWAN-Site-Tunnelkonfiguration herunterladen

a) Sie können die VPN-Konfiguration herunterladen, während das Gateway aktualisiert wird.



Nachdem der VPN-Standort erstellt und die entsprechenden Verbindungsparameter (Peer-Adressen, BGP-AS-Nummern und PSK) heruntergeladen wurden, werden in Phase 3 dieselben Werte für die Konfiguration der übereinstimmenden Elemente auf dem FTD verwendet.

Phase 3: FTD-Konfiguration

Schritt 1: Azure VPN-Konfiguration analysieren

a) Öffnen Sie die heruntergeladene VPN-Konfigurationsdatei von Azure. Es ähnelt der gezeigten zusammengefassten Leistung und bietet hilfreiche Informationen:



Anmerkung: Um den Fokus zu erhöhen, werden mehrere irrelevante Objekte und

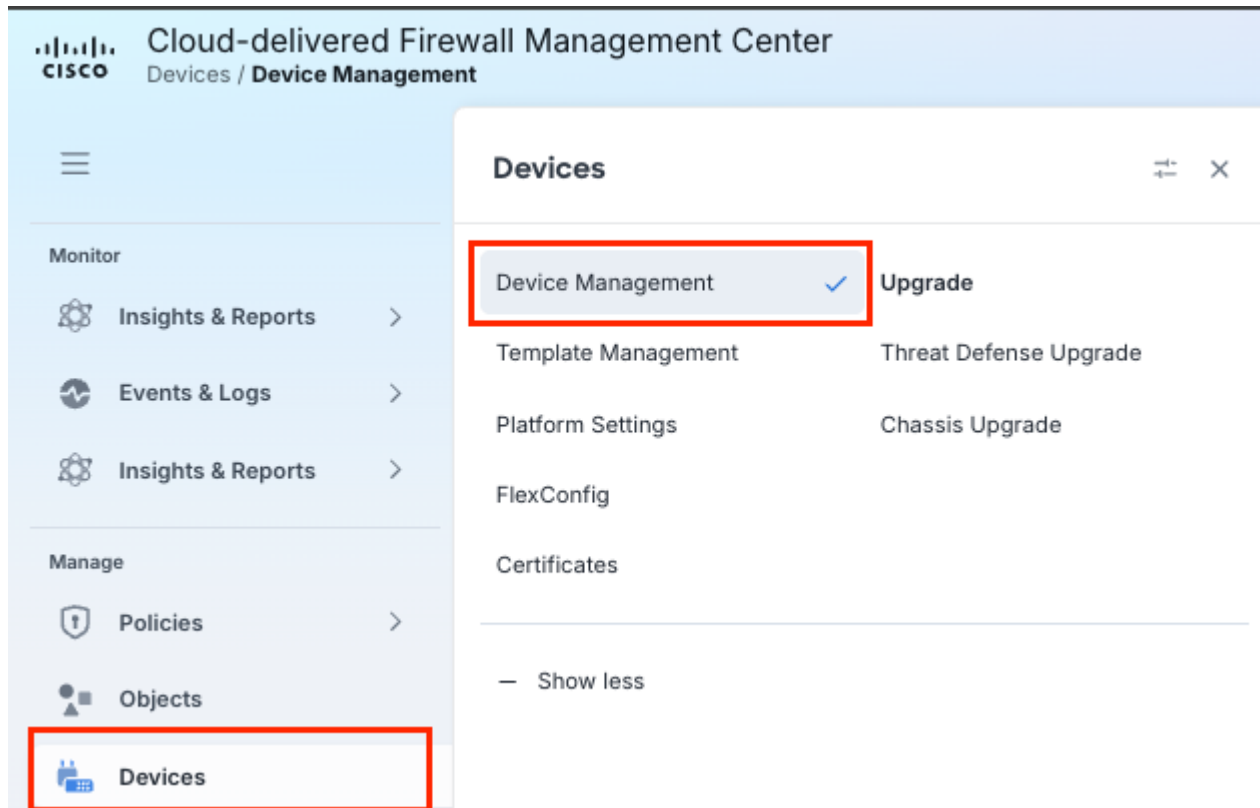
Schlüssel-Wert-Paare aus Gründen der Kürze abgeschnitten.

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

Phase 2: Loopback konfigurieren

Für jede später konfigurierte VTI ist eine stabile Tunnelquelle erforderlich, sodass zunächst eine Loopback-Schnittstelle konfiguriert wird, die von beiden VTIs gemeinsam genutzt wird.

a) Navigieren Sie zu Geräte > Geräteverwaltung.

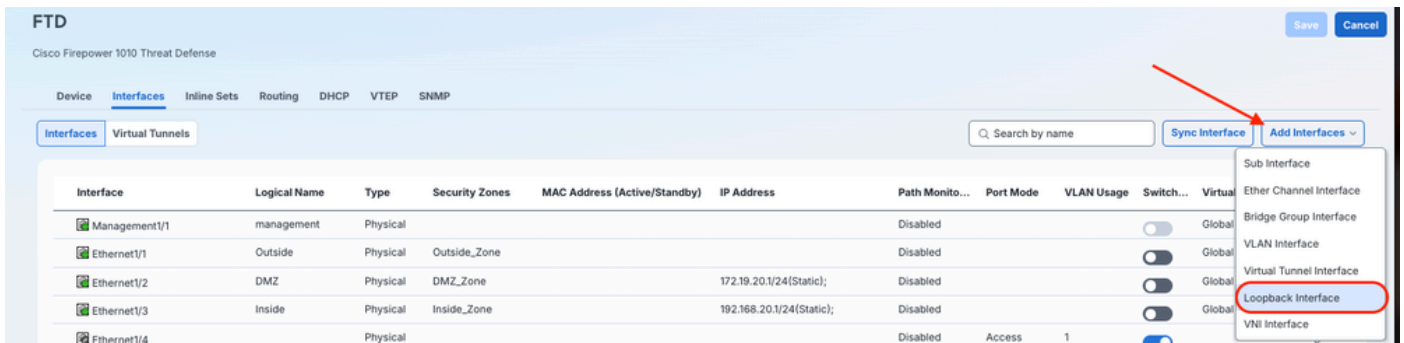


Anmerkung: Bei dieser Übung wird ein über die Cloud bereitgestelltes Firewall Management Center (cdFMC) verwendet. Die Schritte bleiben für standortbasiertes FMC jedoch unverändert.

b) Wählen Sie den von Ihnen konfigurierten FTD als VPN-Gerät für die Außenstelle/den Standort aus.



c) Klicken Sie auf das Dropdown-Menü Add Interfaces (Schnittstellen hinzufügen), und klicken Sie auf Loopback Interface (Loopback-Schnittstelle).



d) Geben Sie der Loopback-Schnittstelle ggf. ihren Namen, ihre Loopback-ID und ihre Beschreibung. Klicken Sie auf IPv4.

e) Stellen Sie sicher, dass der IP-Typ als Statische IP verwenden definiert ist, und geben Sie die Link-BGP-Adresse wie in Phase 2, Schritt 1d konfiguriert ein. Sie können den zuvor in der heruntergeladenen VPN-Konfiguration JSON definierten Wert unter `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Anmerkung: Definieren Sie die Adresse mit einer /32-Maske und innerhalb des RFC 1918-Adressbereichs.

Add Loopback Interface ⓘ

General **IPv4** IPv6

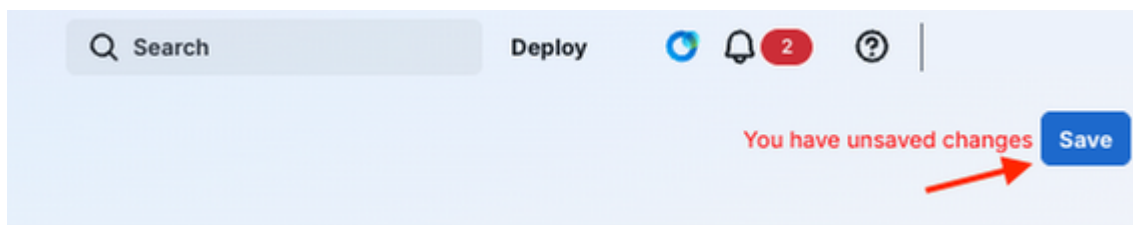
IP Type:
Use Static IP ▼

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) Klicken Sie auf Speichern



Schritt 3: Richtlinienobjekte der Phase 1/Phase 2 konfigurieren

a) Um die IKEv2/IPsec-Konfiguration auf dem FMC so zu konfigurieren, dass sie in den FTD VPN-Topologien angewendet wird, navigieren Sie zu Manage > Objects, scrollen Sie im linken Menü nach unten zu VPN, und erweitern Sie das Untermenü. Konfigurieren Sie die IKEv2 Phase 1-Richtlinie, indem Sie im Menü IKEv2 Policy (IKEv2-Richtlinie) auswählen und auf Add IKEv2 Policy (IKEv2-Richtlinie hinzufügen) klicken.

IKEv2 Policy

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

[Add IKEv2 Policy](#)

Name	
AES-GCM-NUL-SSH	<input type="search"/> <input type="refresh"/> <input type="delete"/>
AES-GCM-NUL-SSH-LATEST	<input type="search"/> <input type="refresh"/> <input type="delete"/>
AES-SHA-SHA	<input type="search"/> <input type="refresh"/> <input type="delete"/>
AES-SHA-SHA-LATEST	<input type="search"/> <input type="refresh"/> <input type="delete"/>
DES-SHA-SHA	<input type="search"/> <input type="refresh"/> <input type="delete"/>
DES-SHA-SHA-LATEST	<input type="search"/> <input type="refresh"/> <input type="delete"/>
Umbrella-AES-GCM-256	<input type="search"/> <input type="refresh"/> <input type="delete"/>

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

b) Geben Sie einen Namen für die neue IKEv2-Richtlinie ein, und wählen Sie Priority (Priorität) und/oder Lifetime (Lebensdauer). Stellen Sie sicher, dass die Richtlinie an beiden Tunnelenden in Bezug auf Integrität, Verschlüsselung, PRF und Diffie-Hellman (DH)-Gruppe übereinstimmt. Wählen Sie die ausgerichteten Algorithmus-/Gruppenelemente aus, die mit der Azure-Konfiguration übereinstimmen sollen, und klicken Sie auf Hinzufügen.



Anmerkung: Auf diese genauen Werte können Sie in der heruntergeladenen Konfigurationsdatei unter `vpnSiteConnections[0].connectionConfiguration.IPsecParameters` verweisen.

New IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
-
- SHA384
- NULL

Selected Algorithms

- SHA256

c) Klicken Sie nach Abschluss der Konfiguration auf Speichern.

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) Konfigurieren Sie die Parameter für Phase 2/IPsec im Untermenü "IKEv2 IPsec-Angebot", und klicken Sie auf IKEv2 IPsec-Angebot hinzufügen.

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**

e) Nennen Sie den IKEv2-IPsec-Vorschlag, und stellen Sie sicher, dass die gleichen Einstellungen übereinstimmen. Klicken Sie abschließend auf Speichern.



Anmerkung: Sie können diese Werte in der heruntergeladenen Konfigurationsdatei unter `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

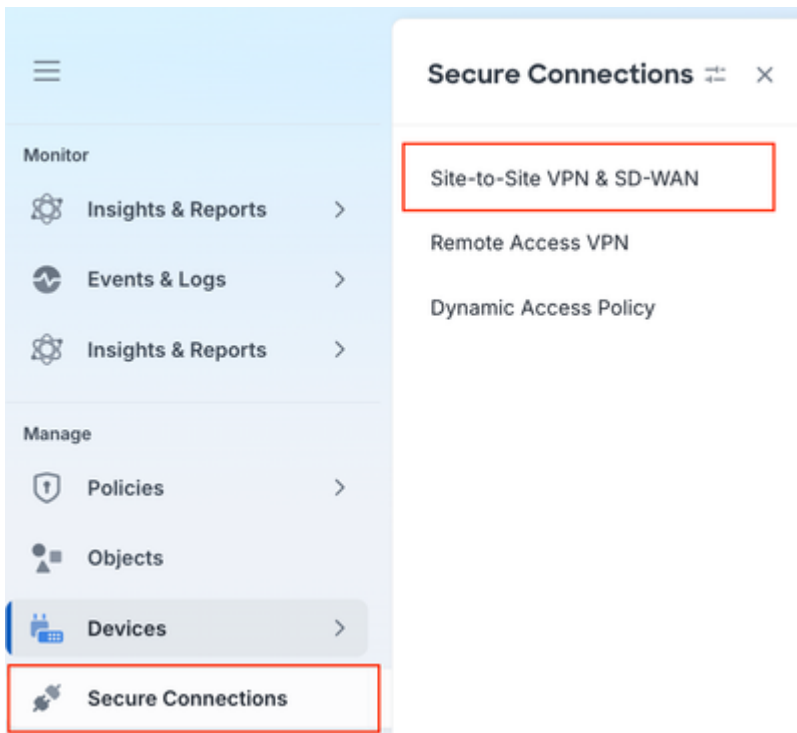


Cancel

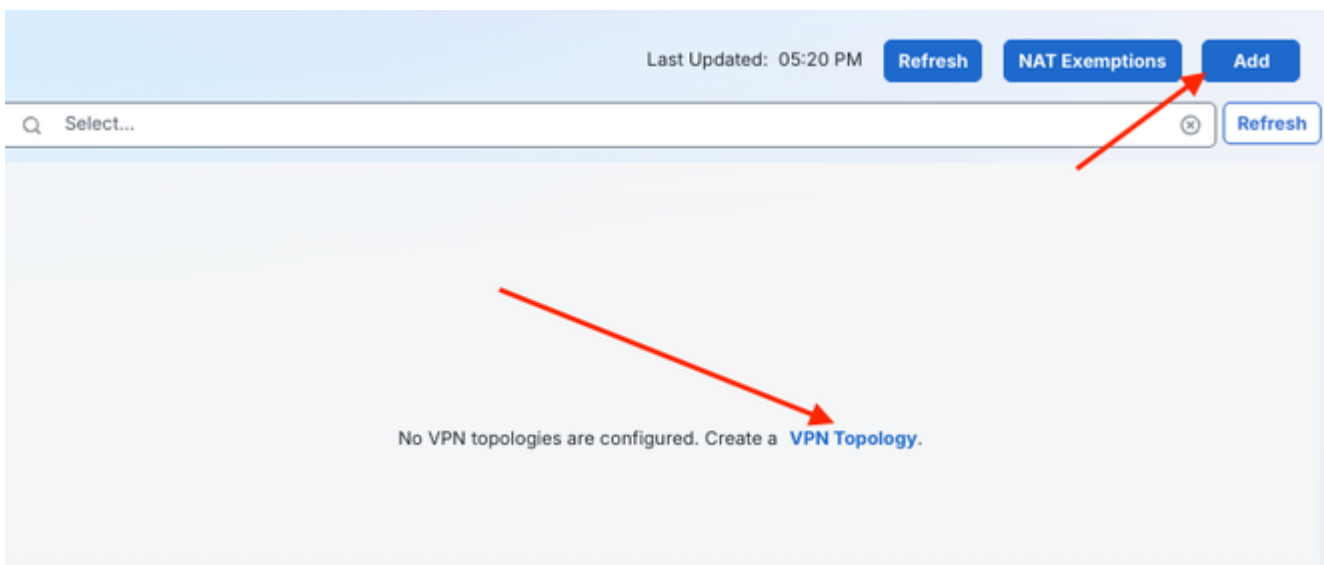
Save

Schritt 4: Sichere Verbindung mit Azure konfigurieren

a) Navigieren Sie zu Verwalten > Sichere Verbindungen > Site-to-Site-VPN und SD-WAN.



b) Klicken Sie entweder auf den Hyperlink für die anfängliche VPN-Topologiekonfiguration in der Mitte, oder klicken Sie auf Hinzufügen.



c) Geben Sie einen Topologienamen für den ersten Tunnel zu Azure Instance0 ein, klicken Sie auf das Optionsfeld Routenbasiertes VPN, und klicken Sie auf den Topologietyp Peer-to-Peer VPN. Klicken Sie abschließend auf Erstellen.

Create VPN Topology

Topology name *

Azure-VTI-Instance0

VPN Type

New

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

Select VPN Topology
☐ Hub and Spoke

Prerequisites

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

Select VPN Topology
☐ Hub and Spoke
☒ **Peer to Peer**

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

Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh

☐ SASE Topology

⚠ SASE topology cannot be selected because Secure Access and Umbrella are not configured.
[Prerequisites](#)

[Refresh](#)

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

d) Klicken Sie für Knoten A auf die Dropdown-Liste Device (Gerät) und wählen Sie den Namen des verwalteten FTD/FTD HA-Paars aus, auf dem die Konfiguration bereitgestellt wird. Wählen Sie für Knoten B, da er das Remote-Ende der Verbindung in der Topologie ist, die auf Azure vWAN-Instanzen terminiert, Extranet aus der Geräte-Dropdown-Liste aus. Klicken Sie anschließend für Knoten A auf das +-Symbol neben der Dropdown-Liste Virtual Tunnel Interface (VTI).

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

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

IKE Version:*

☐ IKEv1 ☒ IKEv2

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

Node A

Device:*

FTD

Virtual Tunnel Interface:*

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name:*

Endpoint IP Address:*

Primary IP*, [Backup Peer IPs]

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

e) Geben Sie dem ersten VTI einen Namen, und stellen Sie sicher, dass dieser aktiviert ist. Weisen Sie dem VTI eine neue oder vorhandene Sicherheitszone zu, weisen Sie die Tunnelquelle zu, und wählen Sie die IP-Adresse aus der angrenzenden Dropdown-Liste aus.

The screenshot shows the 'Add Virtual Tunnel Interface' configuration page. It includes a header with the title and a help icon. The main configuration area has the following fields and settings:

- Tunnel Type:** Radio buttons for 'Static' (selected) and 'Dynamic'.
- Name:*** Text input field containing 'Azure-VTI-0'.
- Enabled:** Checkmark icon.
- Description:** Empty text input field.
- Security Zone:** Dropdown menu showing 'Azure-Spoke-Zone'.
- Priority:** Text input field containing '0', with a range '(0 - 65535)' indicated to the right.
- Propagate Security Group Tag:** Checkmark icon.

Below the main configuration area is a section titled 'Virtual Tunnel Interface Details' with a descriptive paragraph: 'An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.'

The 'Tunnel ID:*' field contains '1', with a range '(0 - 10413)' indicated to the right. The 'Tunnel Source:*' section contains two dropdown menus: the first shows 'Ethernet1/1 (Outside)' and the second shows 'Dynamic'. Red arrows point to the 'Name', 'Security Zone', 'Tunnel ID', and the first dropdown of the 'Tunnel Source' section.

f) Stellen Sie anschließend sicher, dass das Optionsfeld Borrow IP (IP ohne Nummer) aktiviert ist, und wählen Sie dann dieselbe Loopback-Adresse aus der rechten Dropdown-Liste aus. Klicken Sie abschließend auf 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) ▾ +

Cancel OK



g) Nachdem der VTI konfiguriert und angewendet wurde, füllen Sie die Tunnel-Quell-IP-Adresse manuell aus (sie wird automatisch ausgefüllt, wenn die Adresse der übergeordneten Schnittstelle von DHCP übernommen wird), und stellen Sie sicher, dass der Node B-Gerätenamen sowie die Instanz-Endpunkt-IP-Adresse konfiguriert sind. Klicken Sie abschließend auf die Registerkarte IKE.



Anmerkung: Sie können in der heruntergeladenen Konfigurationsdatei unter auf den IP-Adresswert von Instance0 Endpoint verweisen. `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:* i

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

h) Blättern Sie nach unten zu IKEv2-Einstellungen, und stellen Sie sicher, dass der Authentifizierungstyp auf Pre-shared Manual Key festgelegt ist, und geben Sie den in Azure konfigurierten PSK ein. Konfigurieren Sie die IKEv2 Phase 1-Richtlinien, indem Sie auf das Bleistiftsymbol klicken, um verfügbare IKEv2-Richtlinien zu bearbeiten.



Anmerkung: Anmerkung: Sie können auf den vorinstallierten Schlüssel in der heruntergeladenen Konfigurationsdatei zugreifen unter `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

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

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

i) Fügen Sie die anfänglich in Schritt 3 konfigurierte IKEv2 Phase 1-Richtlinie hinzu.

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) Wählen Sie die Registerkarte IPsec aus.

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) Bearbeiten Sie den IKEv2 IPsec-Vorschlag unter Transformationssätze, indem Sie auf das Bleistiftsymbol klicken.

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) Klicken Sie auf das Papierkorb-Symbol, um den standardmäßigen AES-GCM-Transformationssatz zu entfernen, und fügen Sie den benutzerdefinierten Azure_IPsec-Transformationssatz/IKEv2-IPsec-Vorschlag hinzu, der in der zweiten Hälfte von Schritt 3 erstellt wurde. Klicken Sie auf OK.

IKEv2 IPsec Proposal



Available Transform Sets  

 Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec

Cancel

OK

m) Blättern Sie nach unten, und geben Sie 2700 für die Lebensdauer ein, die mit den Azure-Parametern übereinstimmt. Aktivieren Sie ggf. die PFS-Gruppe. Klicken Sie auf Speichern.



Anmerkung: Sie können den Lebensdauerwert in der heruntergeladenen Konfigurationsdatei

unter `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

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

> ESPv3 Settings

n) Bereitstellen der Änderungen

Search **Deploy** 2

 Advanced Deploy

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

o) Aktivieren Sie nach Abschluss der Bereitstellung unter Manage > Secure Connections > Site-to-Site VPN & SD-WAN unter Tunnel Status Distribution (Tunnelstatus-Verteilung). Die erfolgreiche Konnektivität spiegelt Grün (Oben) wider.

Last Updated: 11:11 PM

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

Nachdem der erste Tunnel bereitgestellt wurde, stellen Sie sicher, dass die Einrichtung sowohl auf der IKE/IPsec- als auch auf der BGP-Ebene erfolgreich war, bevor Sie den zweiten Tunnel aus Redundanzgründen konfigurieren.

Schritt 5: Überprüfen der ersten Verbindung mit Azure

a) Geben Sie SSH in das FTD ein, geben Sie `system support diagnostic-cli` ein, geben Sie ein, `en` und drücken Sie die Eingabetaste, da auf der schreibgeschützten FTD-CLI kein Kennwort vorhanden ist.

```
<#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) Tunnelstatus Phase 1/Phase 2 prüfen.

```
<#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) Durchführung von Erfassungen zur Überprüfung auf BGP Transmission Control Protocol (TCP)-Pakete, die von Azure im Tunnel empfangen werden, und entweder Network Address Translation - Traversal (NAT-T) User Datagram Protocol (UDP)-Port 4500/UDP-Port 500-Datenverkehr auf der externen Erfassung von der öffentlichen IP des Instance-0 Azure-Tunnels.

```
<#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#
```

Wenn die Verbindung mit Instance0 bestätigt wurde, wiederholen Sie die gleiche VTI- und VPN-Topologiekonfiguration für Instance1, sodass beide Azure-Gateway-Instanzen erreichbar sind.

Schritt 6: Konfigurieren von Second Tunnel zu Azure Instance1-Endpunkt

a) Erstellen Sie einen zweiten VTI (Azure-VTI-1), der aus demselben Loopback ausgeliehen wird (Schritt 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:*

 (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) Konfigurieren der VPN-Topologie der zweiten Instanz (Schritt 4 g-n)



Anmerkung: Sie können in der heruntergeladenen Konfigurationsdatei unter auf den Wert der IP-Adresse von Instance1 Endpoint
verweisen. `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

Node B

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

Device:*

Device Name*:

Endpoint IP Address*:

Cancel

Save

c) Stellen Sie Konfigurationsänderungen bereit, und überprüfen Sie den 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) Azure wird überprüft, und sowohl Instanz0 als auch Instanz1 ergeben Verbunden.

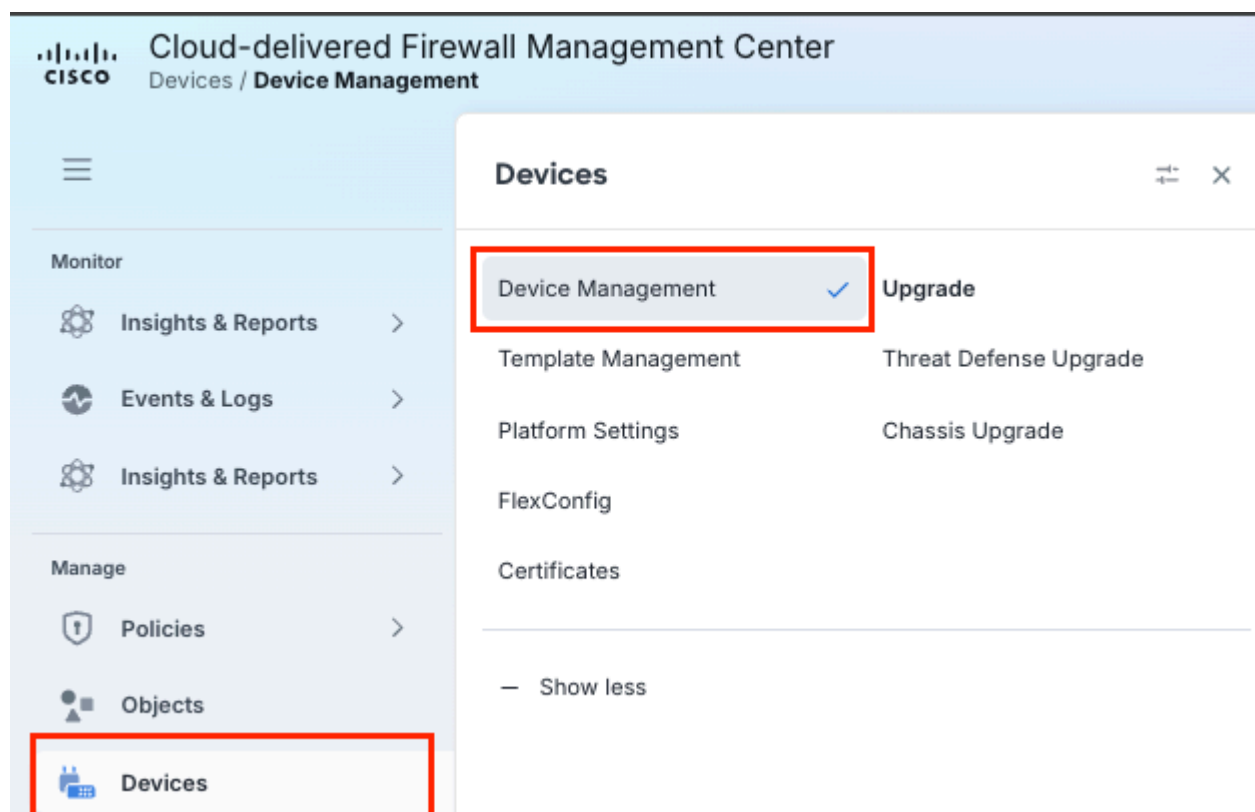
Links

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

Wenn beide Tunnel aktiv sind, benötigt die FTD ECMP-Routing, damit der Datenverkehr beide Pfade gleichzeitig nutzen kann, anstatt den zweiten Tunnel als passiven Standby-Tunnel zu behandeln.

Schritt 7: Konfigurieren von ECMP

a) Navigieren Sie zu Verwalten > Geräte > Geräteverwaltung, und wählen Sie die FTD aus, die mit VPNs zu Azure konfiguriert wurde.



b) Klicken Sie auf die Registerkarte Routing, und wählen Sie ECMP aus.

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

c) Klicken Sie auf Hinzufügen, um eine neue ECMP-Zone zu erstellen.

Equal-Cost Multipath Routing (ECMP)

Add

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

d) Markieren Sie die VTIs, indem Sie im Bereich "Verfügbare Schnittstellen" auf beide VTIs klicken, und klicken Sie auf Hinzufügen, um die VTIs auf die genannte ECMP-Zone anzuwenden.

Add ECMP

Name

Azure-VTI-ECMP-Zone

Available Interfaces

Outside

DMZ

Inside

Add

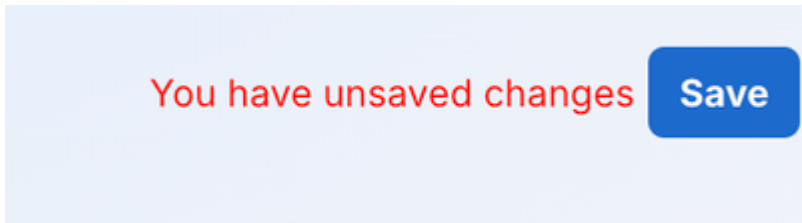
Selected Interfaces

Azure-VTI-0

Azure-VTI-1

Cancel OK

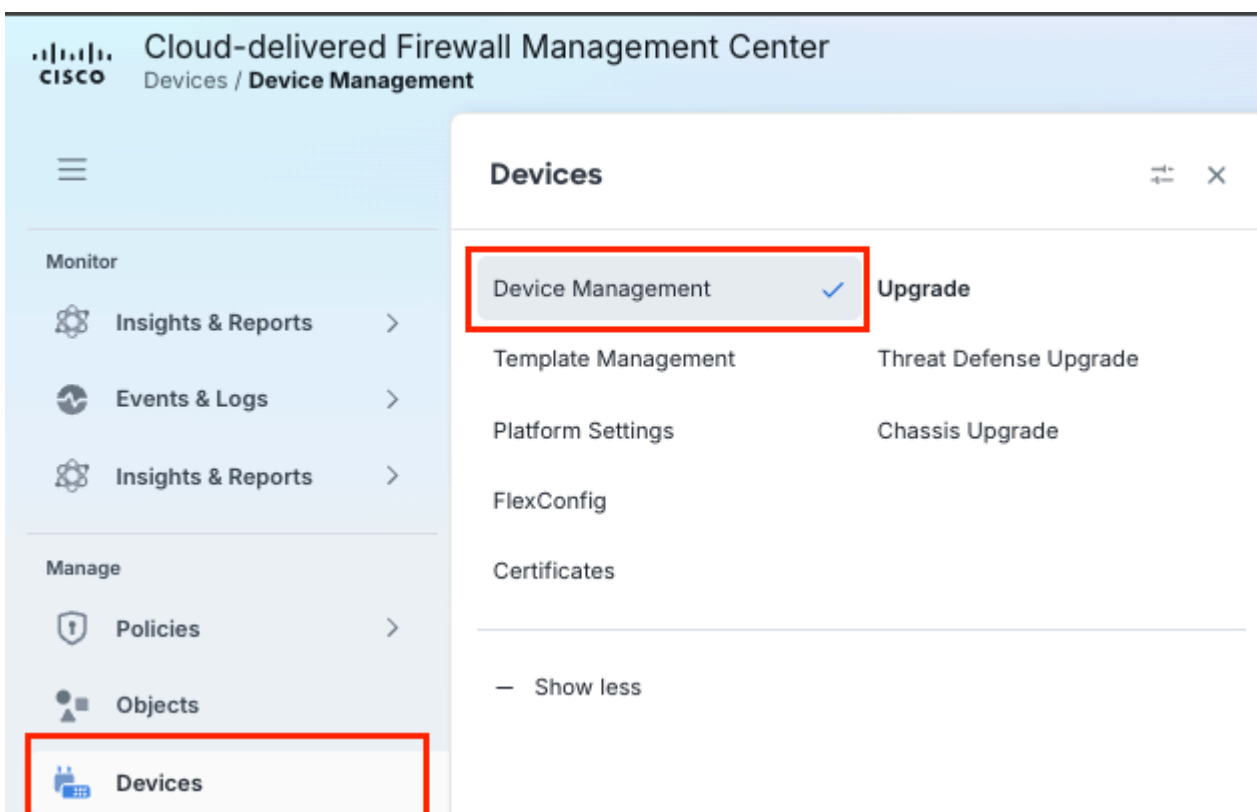
e) Nachdem Sie die Richtigkeit der Einstellungen bestätigt haben, klicken Sie auf Speichern.



Schritt 8: Konfigurieren statischer Routen für private Instanzen von IPs

Für das BGP sind Routen für die erfolgreiche Verbindung mit Nachbarn erforderlich. Da die Endpunkte nicht direkt verbunden sind, werden standardmäßig keine Routen aufgefüllt. Mit ECMP können Sie statische Routen mit derselben Metrik (Administrative Distance) für dasselbe Ziel konfigurieren, sodass beide Routen in der Routing Information Base (RIB) installiert und gleichzeitig verwendet werden.

a) Navigieren Sie zu Verwalten > Geräte > Gerätemanagement, und wählen Sie das entsprechende FTD-Gerät aus.



b) Navigieren Sie zu 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) Klicken Sie auf + Route hinzufügen.

+ Add Route

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

d) Fügen Sie Routen für beide Instanz-IP-Adressen hinzu, indem Sie die erste Route zu Ihrer Instanz0-VTI erstellen, und fügen Sie das Zielnetzwerkobjekt hinzu, indem Sie auf das + neben "Verfügbares Netzwerk" klicken. Klicken Sie dann auf das Netzwerkobjekt aus der Liste, und klicken Sie auf die Schaltfläche Hinzufügen, um es als Ziel der statischen Route hinzuzufügen. Stellen Sie sicher, dass Sie die Instanz0- IP und als Gateway festlegen. Klicken Sie abschließend auf OK.



Anmerkung: Diese Netzwerkwerte für statische Routenziele befinden sich

unter `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` und `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1` in der heruntergeladenen Konfigurationsdatei.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*: Azure-VTI-0

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

Available Network +

Azure-Instance0-BGP_Peer
Azure-Instance1-BGP_Peer

Add

Selected Network

Azure-Instance0-BGP_Peer
10.2.0.12

Ensure that egress virtualrouter has route to that destination

Gateway: Azure-Instance0-BGP_Peer +

Metric: 1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking: +

Cancel OK

e) Wiederholen Sie die Schritte c-d, um die zweite statische Route über Instance1 VTI hinzuzufügen. Stellen Sie sicher, dass Sie auf Speichern klicken, um die Änderungen zu speichern.

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 Routen erreichen nur die BGP-Peering-Adressen; Das BGP selbst muss jedoch weiterhin aktiviert und Peering ausgeführt werden, damit Azure und der FTD-Austausch dynamisch größere Netzwerke untereinander bzw. voneinander routen können.

Schritt 9: BGP konfigurieren

a) Aktivieren Sie den BGP-Prozess 65500 auf FTD unter Routing > General Settings > BGP. Aktivieren Sie das Kontrollkästchen Enable BGP, und geben Sie die zuvor konfigurierte AS-Nummer in Phase 2, Schritt 1, ein. Navigieren Sie neben 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) Aktivieren Sie IPv4-BGP-Routing für Prozess/AS 65500, indem Sie das benachbarte Kontrollkästchen IPv4 aktivieren aktivieren, und klicken Sie auf Neighbor, um BGP-Nachbarn zu konfigurieren.

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) Klicken Sie auf + Hinzufügen.

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) Geben Sie die Instance0 BGP-Peering-Informationen ein, referenzieren Sie das angegebene BGP-AS vom vWAN-Hub, und geben Sie es als Neighbor Remote AS ein, und fügen Sie bei Bedarf eine Beschreibung hinzu. Klicken Sie auf Erweitert.



Wichtig: Stellen Sie sicher, dass Sie die BGP-Update-Quelle ändern und auf das Loopback verweisen, das von beiden VTI-Schnittstellen auf dem FTD übergeordnet ist.

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) Im Menü "Advanced" der BGP Neighbor-Konfiguration auf FTD können Sie die Anzahl der TTL-Hops von der eBGP-StandardEinstellung von 1 Hop in eine variable Anzahl ändern. Azure-BGP-Endpunkte sind nicht direkt über den Tunnel mit der Azure-Infrastruktur verbunden, und es gibt tendenziell mehr Hops zum Endpunkt, als der eBGP-TTL-Standardwert von 1 zulässt.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Wiederholen Sie die gleichen Schritte für 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

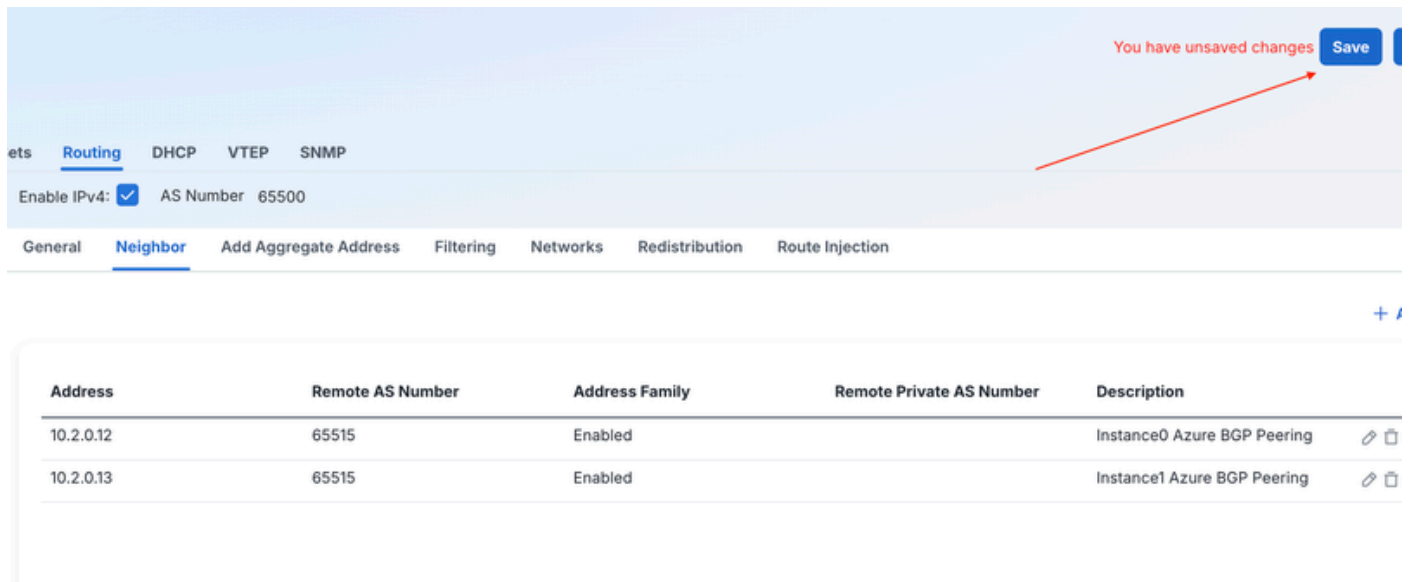
☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50
(1-255)

g) Stellen Sie sicher, dass Sie die Änderungen speichern, sobald Sie fertig sind.



Standardmäßig installiert das BGP nur einen besten Pfad in der Routing-Tabelle, obwohl ECMP beide statischen Routen verfügbar macht. BGP Multipath muss separat aktiviert werden, damit beide erlernten Pfade gleichzeitig installiert und verwendet werden können.

Phase 10: Konfigurieren von BGP Multi-Path

a) Navigieren Sie zu Routing > BGP > IPv4, klicken Sie auf die Registerkarte General (Allgemein), und klicken Sie auf das Bleistiftsymbol neben Forward Packets Over Multiple Paths (Pakete über mehrere Pfade weiterleiten).

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) Ändern Sie den Standardwert des Felds Number of Paths von 1 auf 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Stellen Sie sicher, dass Sie die Änderungen speichern und bereitstellen.

Überprüfung

Bestätigen Sie nach Abschluss der Bereitstellung, dass das BGP Adjacencies mit beiden Azure-Instanzen bildet. Stellen Sie anschließend sicher, dass die Routen über beide Tunnel abgerufen werden und dass der Datenverkehr beide VTIs verwendet. Verwenden Sie dazu den gleichen diagnostischen CLI-Zugriff, der in Phase 3, Schritt 5, eingerichtet wurde.

Navigieren Sie zu `system support diagnostic-cli` auf FTD CLI.

a) Nach der Bereitstellung wird erwartet, dass BGP-Nachbarn aktiviert werden und Präfixe empfangen werden.

<#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) Überprüfen Sie, ob die von Azure empfangenen Routen als Multipath-Routen angezeigt werden.

<#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) Überprüfen Sie die VTI-Paketanzahl.

```
<#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) Bestätigen Sie statische Routen für BGP-Nachbarschaften.

```
<#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) Bestätigen Sie die ECMP-Zonen.

```
<#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) Bestätigung der BGP-Konfiguration

<#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) Bestätigen Sie die Routing-Tabelle.

<#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
```

Weitere Überlegungen

Bei der Basiskonfiguration in diesem Dokument wird von einer einzigen externen Schnittstelle und einem einzigen ISP in der FTD der Außenstelle ausgegangen. Diese Überlegungen erweitern das Design.

AS-Pfad steht vor

Wenn Sie beeinflussen müssen, welcher der beiden Tunnel Azure oder FTD als primär bevorzugt, anstatt die Last gleichmäßig über ECMP und BGP Multipath zu teilen, stellen Sie der lokalen AS-Nummer eine oder mehrere zusätzliche Male auf dem BGP-Nachbarn voran, um als sekundär behandelt zu werden. Der Nachbar mit dem längeren vorgeschalteten AS-Pfad wird bei der standardmäßigen BGP-Auswahl des besten Pfads nicht priorisiert, ohne dass dieser Nachbar vollständig aus der ECMP-Zone entfernt werden muss.

Fehlerbehebung

- Phase-1-/Phase-2-Tunnel wird nicht genutzt: Bestätigen Sie, dass der vorinstallierte Schlüssel und die IKEv2/IPsec-Richtlinienparameter (Verschlüsselung, Integrität, PRF, DH-Gruppe und Lebensdauer) genau zwischen dem IKEv2-FMC-Richtlinienvorschlag/IPsec und den Werten in der heruntergeladenen Azure VPN-Konfigurationsdatei übereinstimmen. Verwenden Sie `show crypto isakmp sa` und `show crypto ipsec sa`, wie in Phase 3, Schritt 5 gezeigt.
- Der Tunnel ist aktiv, aber BGP-Nachbarn bilden `update-sources` sich nicht: Stellen Sie sicher, dass das BGP auf die Loopback-Schnittstelle eingestellt ist und nicht auf den VTI selbst, und dass `ebgp-multihop` ein Wert konfiguriert ist, der hoch genug ist, um die Azure BGP-Peering-Adresse zu erreichen, die nicht direkt mit dem FTD verbunden ist.
- BGP-Formulare, aber nur ein Tunnel überträgt den Datenverkehr: Vergewissern Sie sich, dass beide VTIs Mitglieder derselben ECMP-Zone sind, dass statische Routen zu beiden Azure-Instanz-BGP-Adressen mit derselben administrativen Distanz installiert sind und dass BGP Multipath für zwei Pfade konfiguriert ist, wie in Phase 3, Schritt 10 beschrieben.
- Kein Rückverkehr oder asymmetrisches Routing zu Azure: Da Azure vWAN den Hub-Adressraum über beide Tunnel ankündigt, stellen Sie sicher, dass ECMP an keiner anderen Stelle in der Routing-Konfiguration deaktiviert ist, und prüfen Sie, ob Routenzuordnungen oder richtlinienbasiertes Routing den Datenverkehr an einen einzigen Pfad anheften können.
- BGP ist aktiv und Routen sind installiert, aber der Datenverkehr scheint blockiert zu sein: Stellen Sie sicher, dass Sie Zugriffskontrollregeln konfiguriert haben, die den VTIs die zugewiesene Sicherheitszone vorsehen, sodass ein- und ausgehender Datenverkehr möglich ist.

Zugehörige Informationen

- [Was ist Azure Virtual WAN?](#)

- [Konfigurieren von BGP für Azure VPN Gateway](#)
- [Standard- und benutzerdefinierte IPsec-Richtlinien Azure vWAN](#)
- [Fehlerbehebung bei BGP-Problemen für Azure VPN Gateway](#)
- [Informationen zu VPN-Gateways im aktiven Modus](#)
- [Tutorial: Erstellen einer Site-to-Site-Verbindung mit Azure Virtual WAN](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.