

Azure Dual-ISP-vWAN-Konnektivität in der sicheren Firewall konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Diagramm](#)

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

[Konfigurieren](#)

[Phase 1: Azure vWAN-VPN-Standortkonfiguration](#)

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

[Phase 2: Azure APIPA-Gateway-Parameter konfigurieren](#)

[Schritt 3: Azure vWAN-Site-VPN-Parameter konfigurieren](#)

[Schritt 4: Aktivieren und Aktivieren von benutzerdefiniertem BGP APIPA für VPN-Standortverknüpfungsinstanzen](#)

[Schritt 5: Konfigurationsdatei für den VPN-Standort herunterladen](#)

[Phase 2: FTD für duale ISP-Verbindungen mit Azure vWAN konfigurieren](#)

[Schritt 1: Analysieren der heruntergeladenen VPN-Konfiguration](#)

[Phase 2: Loopback-Schnittstellen für Link-BGP-Update-Quelle konfigurieren](#)

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

[Schritt 4: Virtual Tunnel Interfaces \(VTI\) konfigurieren](#)

[Schritt 5: IPsec-VPN-Topologien bereitstellen](#)

[Schritt 6: Validierung von VPN-Topologien](#)

[Schritt 7: Konfigurieren von ECMP](#)

[Schritt 8: BGP konfigurieren](#)

[Schritt 9: Konfigurieren von eBGP Multipath](#)

[Überprüfung/Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration der standortübergreifenden Microsoft Azure Virtual WAN (vWAN)-VPN-Verbindung zur sicheren Firewall mithilfe von Dual-WAN-Links beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

Stellen Sie sicher, dass beide Komponenten ursprünglich in der Azure-Umgebung konfiguriert wurden:

- Microsoft Azure vWAN-Instanz
- Microsoft Azure vWAN-Hub

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
- Microsoft Azure vWAN

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

Wenn die FTD der Außenstelle über zwei zum Internet Service Provider (ISP) gerichtete externe Schnittstellen verfügt, kann sich jede redundant und aktiv mit Azure vWAN verbinden, sodass jede ISP-Verbindung genutzt wird. Azure vWAN erstellt zwei IPsec-Tunnel pro Standortverbindung - einen zu Azure Hub Instance0 und einen zu Instance1 - sodass jede ISP-Schnittstelle zwei Tunnel terminiert. Auf beiden ISP-Verbindungen werden dadurch vier IPsec-Tunnel auf dem FTD terminiert.

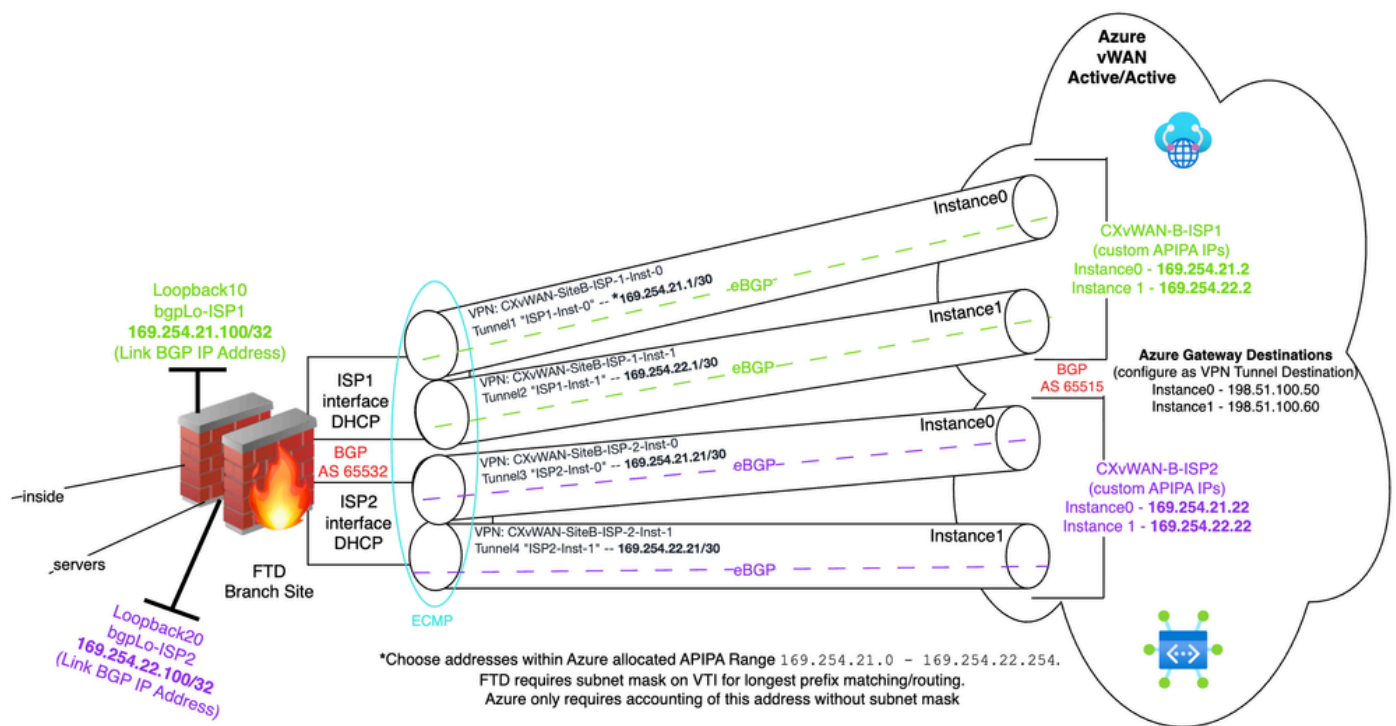
Azure-Instanzen arbeiten für Lastenausgleich und Redundanz im Aktiv/Aktiv-Modus. Daher wird dies im FTD durch die ECMP-Konfiguration (Equal-Cost Multi-Pathing) für alle vier IPsec-Tunnel widergespiegelt. Mithilfe benutzerdefinierter automatischer privater IP-Adressierung (APIPA)

werden externe eBGP-Nachbarschaften (Border Gateway Protocol) mit eindeutigen privaten autonomen Systemnummern (ASNs) über jeden der vier Tunnel eingerichtet. Dadurch wird die BGP-Multipath-Funktion aktiviert, die mehrere redundante Pfade zu jedem Azure Hub-Standortverknüpfungspaar bereitstellt.

Diagramm

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

Dual Direct Internet Access (DIA)-Links (Azure + FTD Load-Balancing/Redundanz)



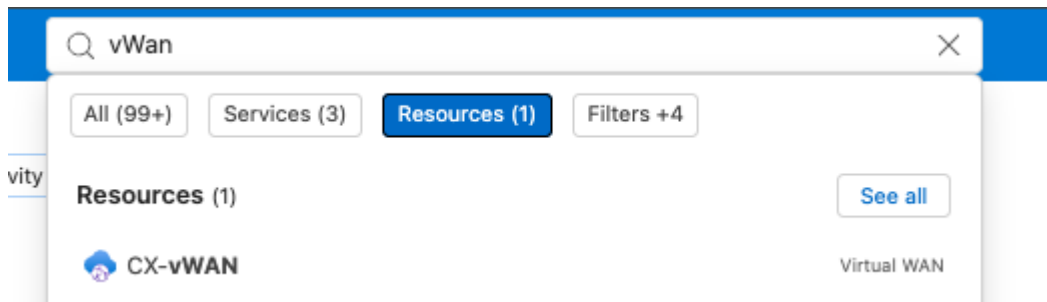
Duale Topologie für direkte Internetverbindungen

Konfigurieren

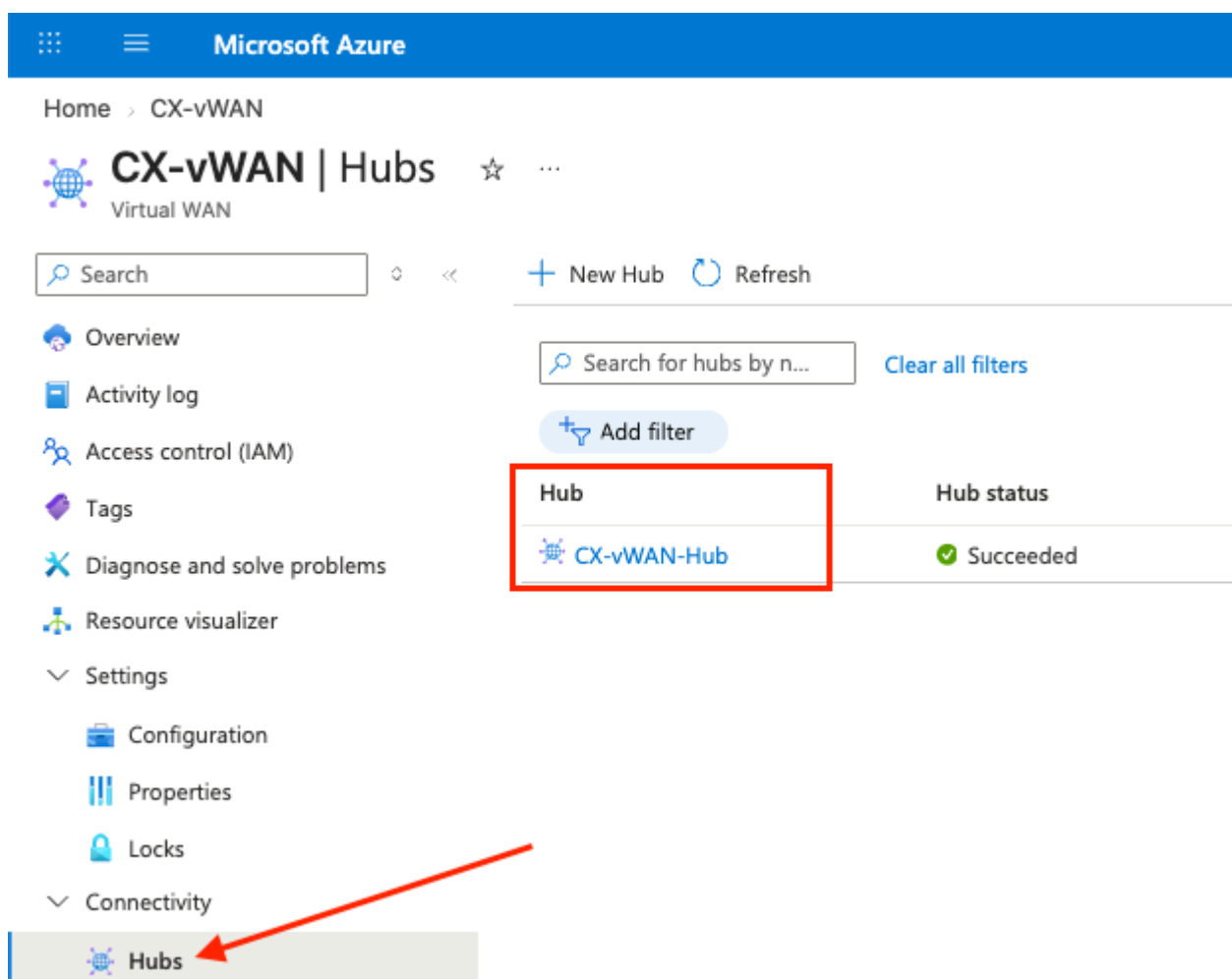
Phase 1: Azure vWAN-VPN-Standortkonfiguration

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

1) Suchen Sie im Azure-Suchfeld nach vWAN, und klicken Sie auf Virtual WANs, um in den vorhandenen Azure vWAN Hub zu wechseln. Navigieren Sie anschließend zu Connectivity > Hubs, und klicken Sie auf den vorhandenen Azure vWAN Hub.



Suchabfrage für virtuelles WAN



Auswählen eines vorhandenen virtuellen WAN-Hubs

2) 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		

Neuen virtuellen WAN-Standort erstellen



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

3) 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 *	Dual-ISP-Site ✓
Device vendor *	Cisco ✓
Private address space	

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

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

[Previous](#)[Next : Links >](#)

Allgemeine Konfigurationseinstellungen für den VPN-Standort

4) Geben Sie die erforderlichen Linkinformationen ein. Die Link-BGP-Adresse und das Link-ASN sind die BGP-Layer-3-Zieladresse im Innentunnel und die BGP-AS-Nummer auf der Zweigstelle, mit der die Nachbarschaft über die Site-to-Site-Tunnel gebildet wird. Die Link-BGP-Adresse ist eine sich nicht überlappende Subnetzadresse (/32) außerhalb des konfigurierten privaten Adressraum-Subnetzes des Hubs, das Azure als /32-Route installiert, um es als BGP-Nachbar zu erreichen. In den nachfolgenden Abschnitten des FTD werden zwei Loopback-Schnittstellen erstellt, die die Link-BGP-Adresse für die einzelnen Links an zwei Standorten darstellen. Die Link-IP-Adresse/der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) ist die Layer-3-Ziel-IP-Adresse des Datenverkehrs, der an die Außenstelle geleitet wird und für die Bereitstellung der IP Security (IPsec)/Internet Key Exchange Version 2 (IKEv2)-Konnektivität erforderlich ist. Fahren Sie mit dem nächsten Schritt fort, indem Sie auf "Weiter" klicken. Überprüfen und erstellen Sie >.



Anmerkung: Überprüfen Sie die Azure-Dokumentation, wenn Sie für Tunneladressen

Adressen zwischen 169.254.21.0 und 169.254.22.255 verwenden: [Auswählen von BGP-APIPA-Adressen](#)

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 >

Standortverknüpfungsparmeter konfigurieren

5) Sobald die Informationen wie vorgesehen bestätigt wurden, 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	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	

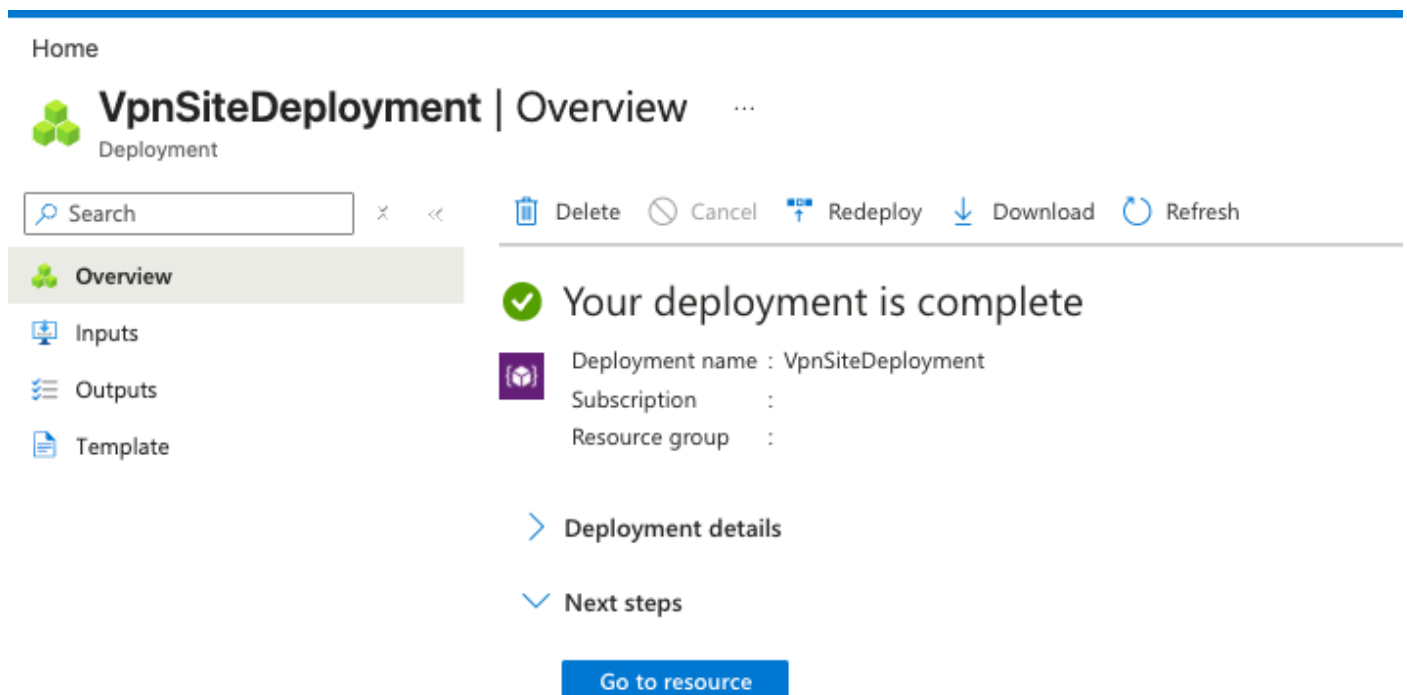
Links

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

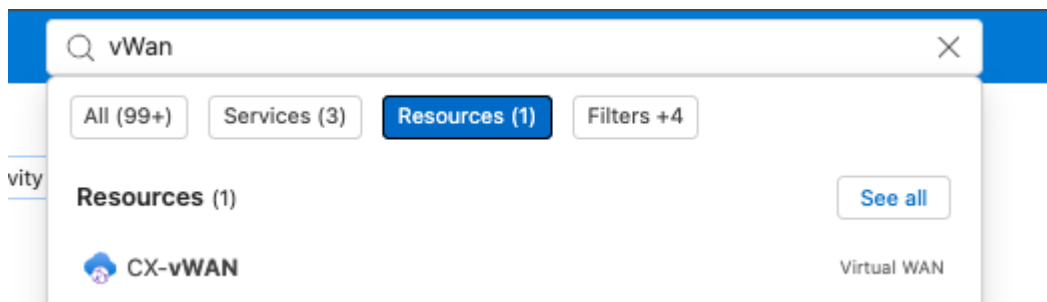
Link name	ISP-2-Link
Link provider name	ISP2
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.22.100

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

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



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 lists 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'.



The screenshot shows a search results window for 'vWan'. It includes tabs for 'All (99+)', 'Services (3)', 'Resources (1)', and 'Filters +4'. The 'Resources (1)' tab is selected, showing a single resource named 'CX-vWAN' with the type 'Virtual WAN'. A 'See all' button is visible in the top right corner of the results area.

Phase 2: Azure APIPA-Gateway-Parameter konfigurieren

Azure erfordert eine zusätzliche Konfiguration für die automatische private IP-Adressierung (APIPA) im IPv4-Adressbereich 169.254.0.0/16.

1) Geben Sie den vorhandenen Hub über Connectivity > Hubs ein.

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

Navigieren zur Konnektivität des virtuellen WAN-Hubs

2) Navigieren Sie erneut zu Connectivity > VPN (Site-to-Site), und klicken Sie auf den 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 zur Access Gateway-Konfiguration

3) Ein seitlicher Bereich wird angezeigt, um das VPN-Gateway zu bearbeiten. Geben Sie unter "VPN Gateway Instance0" und "VPN Gateway Instance1" zwei eindeutige benutzerdefinierte BGP-IP-Adressen ein, die als Nachbar-IPs für jede Instanz für BGP-Nachbarschaften über die IPsec-Tunnel fungieren. Dies ist erforderlich, wenn Sie die APIPA-Adressierung innerhalb dieser Topologie verwenden möchten. Geben Sie in das Feld Peer Address (Peeradresse) die BGP-Nachbar-IP ein, die verwendet werden soll, um die Azure-Instanzen über die FTD zu erreichen. Azure versucht keine BGP-Einrichtung mit dem FTD, wenn die APIPA-Adressierung verwendet wird. Daher versucht der FTD, über jeden Tunnel mit Azure eine eBGP-Nachbareinrichtung einzurichten.

Die Gesamtzahl ergibt 2 Verbindungen x 2 implizite Tunnel; ein Tunnel zu Instance0 und Instance1 pro ISP-Verbindung; Insgesamt sind vier IPsec-Tunnel mit BGP-Nachbarschaften zwischen Azure und den beiden FTD-ISP-Schnittstellen vorhanden.

Diese Adressen müssen eindeutig sein. In dieser Demonstration müssen die zweite und letzte Host-Adresse in den /30-Subnetzen, die jedem Tunnel zugewiesen sind, auf dem FTD konfiguriert werden. Klicken Sie nach der Konfiguration auf Bearbeiten.



Anmerkung: Überprüfen Sie die Azure-Dokumentation, wenn Sie für Tunneladressen Adressen zwischen 169.254.21.0 und 169.254.22.255 verwenden: [Auswählen von BGP-APIPA-Adressen](#)

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

Benutzerdefinierte BGP-IP-Adressen des VPN-Gateways bearbeiten



Anmerkung: Wie Azure bemerkt, kann die Aktualisierung bis zu 30 Minuten oder länger dauern.

Schritt 3: Azure vWAN-Site-VPN-Parameter konfigurieren

1) Klicken Sie auf der Seite Connectivity > VPN (Site to Site) in der Azure vWAN Hub-Konfiguration auf X, um die Hub-Zuordnung zu löschen: Angeschlossene Filter zum Anzeigen nicht verbundener VPN-Standorte

The screenshot shows the Microsoft Azure portal interface for a vWAN Hub. The left sidebar contains a navigation menu with the following items: Overview, Connectivity (highlighted with a red box), VPN (Site to site) (highlighted with a red box), ExpressRoute, User VPN (Point to site), Routing, Security, Third party providers, and Monitor. The main content area displays the 'VPN Sites' tab. At the top, there are several action buttons: Download VPN Config, Packet Capture, Delete gateway, Reset gateway, and Monitor Gateway. Below these, there are sections for 'Essentials', 'Gateway configuration', and 'NAT Rules'. The 'VPN Sites' section has a search bar and a 'Clear all filters' link. A filter is currently applied: 'Hub association : Connected'. A red arrow points to the 'X' icon next to this filter, indicating it should be removed. Below the filter, there is a button labeled 'Add filter'. At the bottom, there is a message box with an information icon and the text: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Verbindungsfilter für Hub-Zuordnung löschen

2) Aktivieren Sie das Kontrollkästchen neben der kürzlich bereitgestellten VPN-Site, und klicken Sie auf VPN-Site verbinden.



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

Virtual HUB

[Download VPN Config](#)[Packet Capture](#)[Delete gateway](#)[Reset gateway](#)

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Routing Intent and Routing Policies

BGP Peers

Route Tables

Effective Routes

Security

Azure Firewall and Firewall Manager

Third party providers

Essentials

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

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

VPN Sites

Metrics

[Restore previous filters](#)

+ Add filter

VPN Sites ⓘ



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

+ Create new VPN site

Connect VPN sites

Disconnect VPN sites

Refresh

Page:

Site name

↑↓ Location

☒ Dual-ISP-Site

VPN-Standortaktion verbinden

3) Konfigurieren Sie den gewünschten PSK (Pre-Shared Key), und konfigurieren Sie die gewünschten IPsec-Parameter, indem Sie auf die Umschaltoption Benutzerdefiniert klicken. Diese IPsec-Parameter müssen in der FMC/FTD-Konfiguration in späteren Schritten übereinstimmen. Klicken Sie zum Speichern auf Verbinden.



Anmerkung: Die Unterstützung für Diffie-Hellman (DH) Group 24 wurde in FTD/FMC Version 6.7 entfernt.

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

Konfiguration von vorinstallierten Schlüsseln und IPsec-Parametern

4) Bestätigung der erfolgreichen Bereitstellung des VPN-Standorts

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

Bereitstellungsstatus des VPN-Standorts bestätigen

Schritt 4: Aktivieren und Aktivieren von benutzerdefiniertem BGP APIPA für VPN-Standortverknüpfungsinstanzen

1) Aktualisieren Sie die Seite VPN (Site-to-Site) und bestätigen Sie, dass die Spalte Verbindungsbereitstellungsstatus den Erfolg anzeigt. Klicken Sie auf die Auslassungszeichen, und klicken Sie auf den Dropdown-Menüpunkt VPN-Verbindung zu diesem Hub bearbeiten.

The screenshot shows a table of VPN connections. The first row is highlighted and shows a connection named 'Dual-ISP-Site' with location 'eastus' and a 'Succeeded' provisioning status. A dropdown menu is open for this row, showing options: 'Edit VPN connection to this hub', 'Delete VPN connection to this hub', and 'Download VPN site configuration file'. A red arrow points to the dropdown menu.

Site name	Location	Cloud provider	Connection Provisioning status	Connectivity status
Dual-ISP-Site	eastus		Succeeded	Not connected

Überprüfen des Verbindungserfolgs und Bearbeiten der VPN-Verbindung

2) Klicken Sie auf, um Link Connection 1 (ISP1) zu konfigurieren, und geben Sie den entsprechenden Pre-Shared Key (PSK) erneut ein. Stellen Sie sicher, dass Sie neben der benutzerdefinierten BGP-IP-Adresse auf den Umschalter Enable klicken und die verbleibenden Hostadressen der /30-Subnetze zuordnen, die die IP-Zieladressenwerte des generierten BGP-Headers im inneren Tunnel sein werden. durch die FTDs.

Im Wesentlichen hat ISP1 VTI Tunnel1 zu Azure Instance0 die Adressenzuweisung 169.254.21.1/30, und dem zweiten ISP1 VTI Tunnel2, der auf dem FTD endet, wurde die IP 169.254.22.1/30 für Instance1 zugewiesen.

Klicken Sie auf Weiter: Link Connection 2>, um mit den ISP 2-Verbindungsparametern fortzufahren.



Anmerkung: Möglicherweise müssen Sie Ihr PSK erneut eingeben und im Dropdown-Menü in Azure erneut auf die Option für die ausgerichtete PFS-Gruppe klicken.

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 >

Link-Verbindung konfigurieren und benutzerdefinierte BGP-Einstellungen festlegen

3) Wiederholen Sie die vorherigen Schritte, und wenden Sie die entsprechenden Parameter unter Link Connection 2 (ISP2-Link) an. Klicken Sie abschließend auf Erstellen.

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

Connection Mode ⓘ Default Initiator Only Responder Only

Border gateway protocol ⓘ Disable Enable

Custom BGP IP Addresses ⓘ Disable Enable

Custom BGP IP Address

Instance 0 ⓘ 169.254.21.22 ▼

Instance 1 ⓘ 169.254.22.22 ▼

Use Azure Private IP Address ⓘ Yes No

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

Use policy based traffic selector ⓘ Enable Disable

IPsec ⓘ Default Custom

SA Lifetime in seconds * ⓘ 27000

IKE Phase 1 ⓘ
Encryption * GCM AES256 Integrity/PRF * SHA384 DH Group * DHGroup14

IKE Phase 2(ipsec) ⓘ
IPsec Encryption * GCM AES256 IPsec Integrity * GCM AES256 PFS Group * NONE

DPD timeout in seconds * ⓘ 45

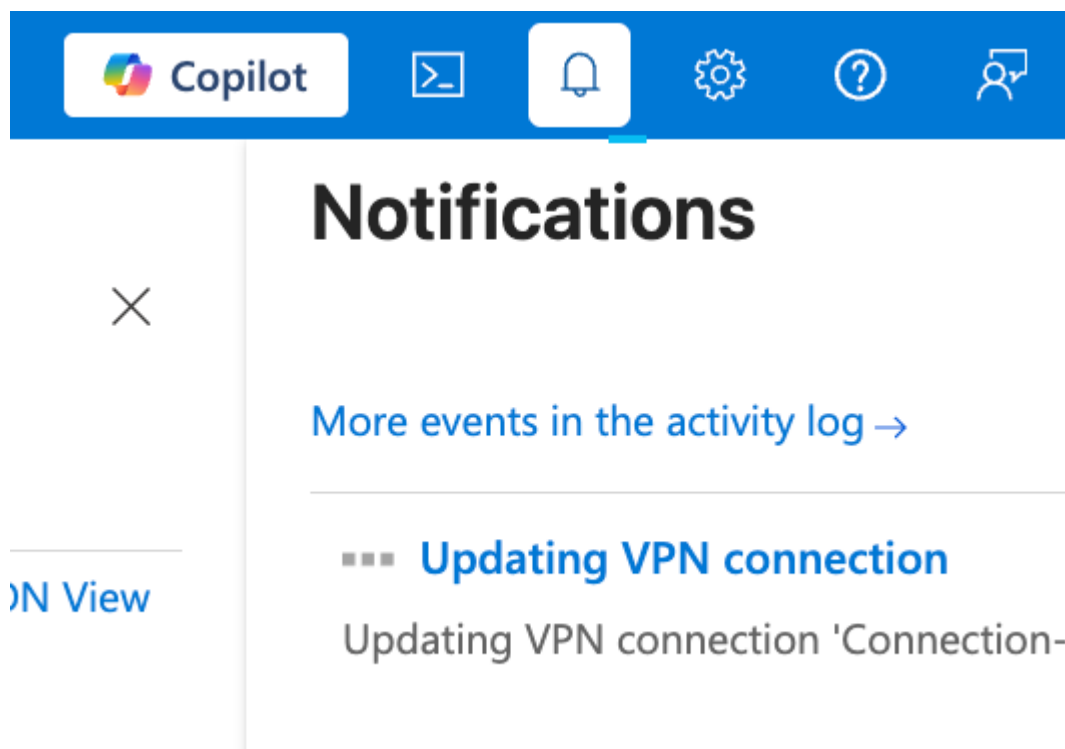
Create

Previous

Next

Konfigurieren der Verbindung Zwei benutzerdefinierte BGP-Einstellungen

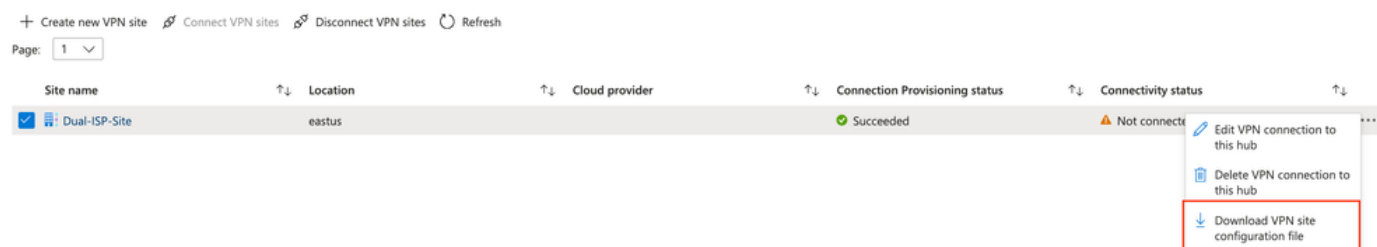
4) Benachrichtigungen in der Azure-Benutzeroberfläche zeigen den Beginn der Aktualisierungsaufgabe an.



Benachrichtigung zum Beginn der Azure-Aktualisierungsaufgabe

Schritt 5: Konfigurationsdatei für den VPN-Standort herunterladen

1) Wählen Sie auf derselben VPN-Seite (Site-to-Site) in Azure das Auslassungszeichen-Symbol ganz rechts neben der konfigurierten VPN-Site aus, und wählen Sie die Option VPN-Standortkonfigurationsdatei herunterladen.



Option "Konfigurationsdatei für VPN-Standort herunterladen"

2) Klicken Sie auf den Hyperlink Klicken Sie hier, um den Download zu starten.



Download Site-to-Site VP...



Dual-ISP-Site



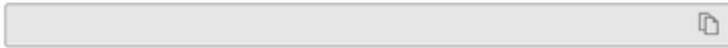
Create new



Use existing



The file is ready to download



[Click here to download](#)



Konfigurationsdatei für den VPN-Standort herunterladen

Phase 2: FTD für duale ISP-Verbindungen mit Azure vWAN konfigurieren

Schritt 1: Analysieren der heruntergeladenen VPN-Konfiguration

1) Öffnen Sie die heruntergeladene Konfigurationsdatei, und eine ähnliche Ausgabe von JavaScript Object Notation (JSON) wird angezeigt. Die Ausgabe zeigt eines der beiden in die Datei geschriebenen Objekte. Diese Informationen stellen hilfreichen Kontext für die FTD-Konfiguration bereit.



Anmerkung: Um den Fokus zu erhöhen, werden mehrere irrelevante Objekte und Schlüssel-Wert-Paare aus Gründen der Kürze abgeschnitten.



Anmerkung: Die Reihenfolge der ISP-Link-1-JSON-Objekte in der heruntergeladenen Datei wird umgekehrt. Die Ellipse in der Codeausgabe stellt das ISP-2-Link-Objekt mit der entsprechenden Konfiguration dar.

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

```

Behalten Sie diese Ausgabe als Referenz bei, während Sie die Schritte durchführen.

Phase 2: Loopback-Schnittstellen für Link-BGP-Update-Quelle konfigurieren

BGP-Nachbarkonfigurationseinträge im FTD-BGP-Prozess (die in späteren Schritten auf dem FTD konfiguriert werden) benötigen eine stabile Quelle, die die entsprechenden Link-BGP-IP-Adressen in der Azure Site Link-Konfiguration repräsentiert.

1) Navigieren Sie zu Geräte > Geräteverwaltung.

Cloud-delivered Firewall Management Center

Devices / Device Management

☰

Monitor

Insights & Reports

>

Events & Logs

>

Insights & Reports

>

Manage

Policies

>

Objects

Devices

Devices

Device Management

Template Management

Platform Settings

FlexConfig

Certificates

Upgrade

Threat Defense Upgrade

Chassis Upgrade

— Show less

Navigieren Sie zum Gerätemanagement im FirePOWER Management Center

Anmerkung: Bei dieser Übung wird ein über die Cloud bereitgestelltes Firewall Management Center (cdFMC) verwendet. Bei standortbasiertem FÜZ bleiben die Schritte jedoch unverändert.

2) Klicken Sie auf das FTD, das Sie als VPN-Gerät der Außenstelle/des Standorts mit dualer ISP-Verbindung konfigurieren.

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

FTD für Konfigurationsbereitstellung auswählen

3) Klicken Sie auf das Dropdown-Menü Add Interfaces (Schnittstellen hinzufügen) und dann auf Loopback Interface (Loopback-Schnittstelle).

CXvWAN-FTD-2 Save Cancel

Cisco Secure Firewall Threat Defense for AWS

Device **Interfaces** Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels Sync Interface Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/St...	IP Address	Path Mon...	Vir
Management0/0	management	Physical				Disabled	Glo
Ethernet0/0	ISP1	Physical				Disabled	Glo
Ethernet0/1	ISP2	Physical				Disabled	Glo

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

Hinzufügen einer Loopback-Schnittstelle zum Gerät

4) Geben Sie einen Namen für die Loopback-Schnittstelle ein, aktivieren Sie das Kontrollkästchen Aktiviert, und geben Sie eine Loopback-ID ein. Geben Sie bei Bedarf eine Beschreibung ein. Klicken Sie abschließend auf die Registerkarte IPv4.

Add Loopback Interface

General **IPv4** IPv6

Name:

☒ Enabled

Loopback ID: *

(1-1024)

Description

Cancel OK

Konfigurieren der Loopback-Schnittstelleninformationen und der IPv4-Adresse

5) Geben Sie die Loopback-IP-Adresse ein, die als Link-BGP-IP-Adresse in früheren Schritten für die ISP1-Standortverbindung in Azure konfiguriert wurde. Diese IP wird als BGP-Update-Adresse in den Nachbarschaften verwendet, die zwischen den FTD- und Azure-Instanzen über ISP1 konfiguriert wurden.



Anmerkung: Sie können auf den zuvor in der heruntergeladenen VPN-Konfiguration JSON definierten Wert unter `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress` für ISP1

verweisen.

Add Loopback Interface

General **IPv4** IPv6

IP Type:
Use Static IP

IP Address:
169.254.21.100/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

Geben Sie die Loopback-IPv4-Adresse ein, und klicken Sie auf OK.

6) Wiederholen Sie die Unterschritte c-e in dieser Sequenz für die ISP2-BGP-Loopback-Konfiguration.

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

Erstellen der ersten und zweiten Loopback-Schnittstellen

7) Speichern Sie Ihre Konfiguration.

You have unsaved changes

Save Cancel

Änderungen speichern

Schritt 3: Richtlinienobjekte der Phase 1/Phase 2 konfigurieren

1) Um die IKEv2/IPsec-Konfiguration für die FMC- zu FTD-VPN-Topologien zu konfigurieren, navigieren Sie zu Manage > Objects, scrollen Sie im Navigationsmenü 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.

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 >

Neues IKEv2-Richtlinienobjekt erstellen

2) Geben Sie einen Namen für die neue IKEv2-Richtlinie ein, und wählen Sie Priority (Priorität) und/oder Lifetime (Lebensdauer). Stellen Sie sicher, dass die Richtlinien bezüglich Integrität, Verschlüsselung, Pseudo Random Function (PRF) und DH Group an beiden Enden des Tunnels übereinstimmen. Wählen Sie die Algorithm-/Group-Elemente 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

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

SHA256

Cancel Save

IKEv2-Richtlinie erstellen

3) Klicken Sie nach Abschluss der Konfiguration auf Speichern.

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-Richtlinie speichern

4) 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. Only the Hash Algorithms are allowed. During IKEv2 negotiations, the peers select the most appropriate options that each support.

[Add IKEv2 IPsec Proposal](#)

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

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**

Angebot für IKEv2 IPsec erstellen

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

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



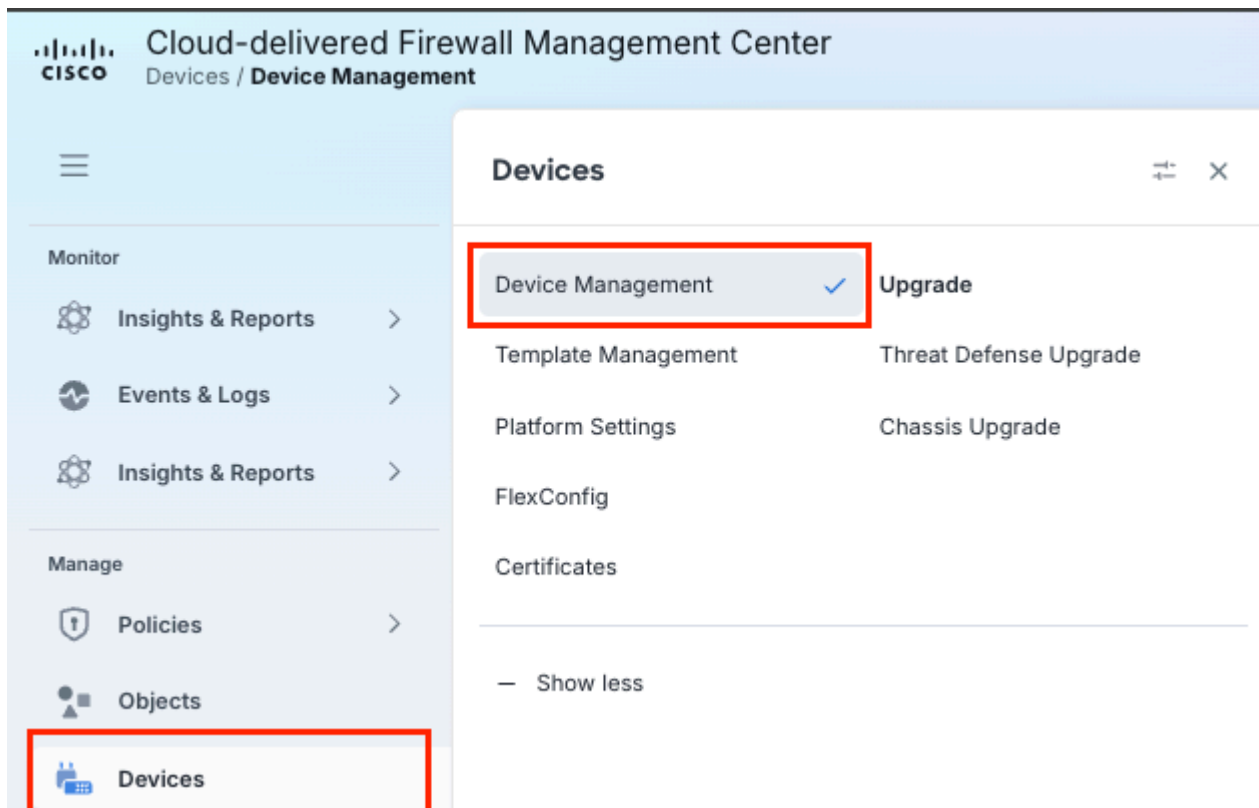
Cancel

Save

Geben Sie dem Angebot IKEv2 IPsec einen Namen, und klicken Sie auf Speichern.

Schritt 4: Virtual Tunnel Interfaces (VTI) konfigurieren

1) Navigieren Sie zu Geräte > Geräteverwaltung.



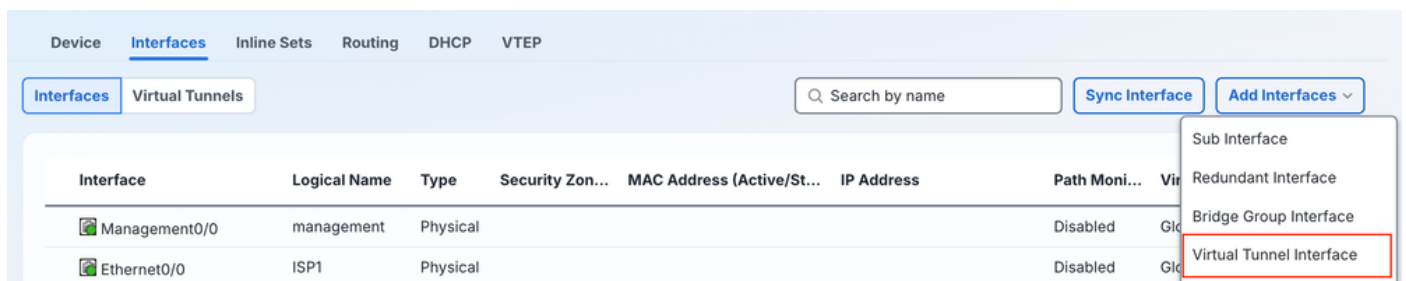
Navigieren Sie zum Gerätemanagement im FirePOWER Management Center

2) Klicken Sie auf das von Ihnen konfigurierte FTD als VPN-Gerät der Außenstelle/des Standorts mit dualer ISP-Verbindung.

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

FTD für Konfigurationsbereitstellung auswählen

3) Klicken Sie auf das Dropdown-Menü Add Interfaces (Schnittstellen hinzufügen), und wählen Sie Virtual Tunnel Interface (VTI) aus.



Virtuelle Tunnelschnittstelle erstellen

4) Geben Sie die Tunnelinformationen ein. Stellen Sie sicher, dass das Kontrollkästchen Aktiviert aktiviert ist, Name eingegeben wird (ggf. auch Beschreibung) und optionale Sicherheitszone ausgewählt wird. Richten Sie die richtige zum ISP gerichtete übergeordnete Schnittstelle aus, um den VTI unter zu konfigurieren, und konfigurieren Sie die entsprechende IP-Adresse für die IPsec-

Verbindung für den Innentunnel für den VTI. Klicken Sie abschließend auf OK.



Tipp: Das Referenzdiagramm zeigt einen weiteren Kontext zur potenziellen VPN-Konfiguration für Azure Dual-WAN-Verbindungen mit 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) Konfigurieren Sie drei zusätzliche VTIs über übergeordnete ISP1- und ISP2-Schnittstellen.

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

Zusätzliche virtuelle Tunnelschnittstellen konfigurieren

f) Klicken Sie auf "Speichern", um die Änderungen zu speichern.

You have unsaved changes

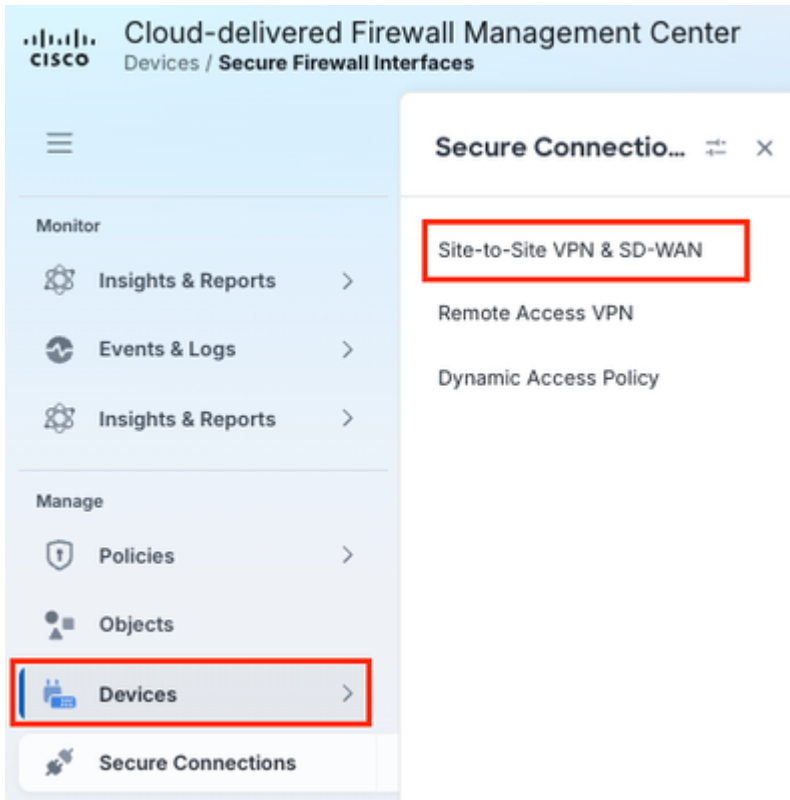
Save

Cancel

Änderungen speichern

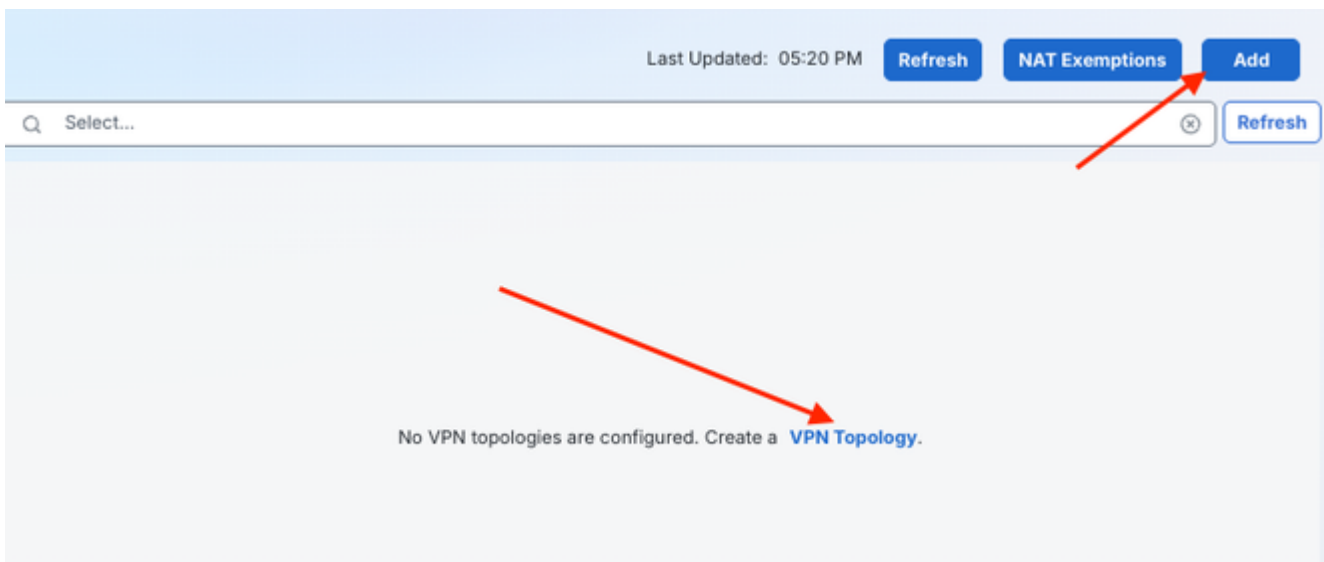
Schritt 5: IPsec-VPN-Topologien bereitstellen

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



Verwalten von Site-to-Site-VPN- und SD-WAN-Verbindungen

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



Neue VPN-Topologiekonfiguration hinzufügen

3) Geben Sie einen Topologienamen für die erste Tunnel-over-ISP1-Verbindung 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 *

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](#)

Konfigurieren des routenbasierten VPN-Topologietyps

4) Wählen Sie zunächst das Node A-Gerät und anschließend in der Dropdown-Liste Device (Gerät) die FTD aus, die die VPN-Tunnel von Azure terminiert. Nachdem der Assistent die verfügbaren VTIs vom Gerät abgerufen hat, wählen Sie im Dropdown-Menü die VTI aus, die für die übergeordnete Schnittstelle und Instanz, die Sie konfigurieren, geeignet ist. Wählen Sie aus dem Menü "Node B Device" (Knoten B) die Azure-Seite als Extranet-Knoten in der VPN-Topologiekonfiguration aus. Stellen Sie sicher, dass Sie einen benutzerfreundlichen Namen für Knoten B konfigurieren und die entsprechende Endpunkt-IP-Adresse eingeben. Klicken Sie abschließend auf die Registerkarte IKE, um die Tunnelkonfiguration für Phase 1 zu implementieren.



Anmerkung: Sie können in der heruntergeladenen Konfigurationsdatei unter `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` und `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1` auf Werte der Instanz-Endpunkt-IP-Adresse verweisen.

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

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

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

Endgeräte für Knoten A- und Knoten B-Topologie definieren

5) Navigieren Sie im Navigationsmenü zu IKEv2-Einstellungen, und klicken Sie auf das Bleistiftsymbol, um die Richtlinien in der kürzlich konfigurierten IKEv2-Richtlinie zu bearbeiten. Wählen Sie anschließend die Option Pre-shared Manual Key (Vorinstallierter manueller Schlüssel) aus dem Dropdown-Menü Authentication Type (Authentifizierungstyp), und geben Sie den zuvor in Azure konfigurierten PSK ein. Klicken Sie abschließend auf die Registerkarte IPsec, um IPsec-Tunnelparameter für Phase 2 zu konfigurieren.



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

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-Einstellungen und Authentifizierungsschlüssel bearbeiten

6) Klicken Sie auf das Bleistiftsymbol neben dem IKEv2 IPsec Proposal Transform Set, und wählen Sie die zuvor konfigurierten IPsec-Richtlinienparameter aus. Ändern Sie den Wert für die Lebenszeitdauer so, dass er mit den Azure vWAN VPN-Einstellungen übereinstimmt. Nachdem die konfigurierten Informationen bestätigt wurden, klicken Sie auf Speichern.



Anmerkung: Sie können in der heruntergeladenen Konfigurationsdatei unter `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds` auf den Lebenszeitwert verweisen.

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Azure_IPsec

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:



Lifetime Duration*:

27000

Seconds (Range 120-2147483647)

Lifetime Size:

Unlimited

Kbytes (Range 10-2147483647)

Cancel

Save

Lebensdauer des IPsec-Angebots konfigurieren

7) Wiederholen Sie die vorherigen Unterschritte in Schritt 5, um die anderen Azure-Tunnel für ISP1 Instance1, ISP2 Instance0 und ISP2 Instance1 zu erstellen.

> 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	✓		

Erstellung zusätzlicher Site-to-Site-VPN-Topologien

Schritt 6: Validierung von VPN-Topologien

Geben Sie in system support diagnostic-cli ein, geben Sie en ein, und drücken Sie die Eingabetaste (schreibgeschützte CLI).

1) Überprüfen Sie die IKE Phase 1-Tunnelverbindung.

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

2) Überprüfen Sie die IPsec Phase 2-Verbindung.

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



Anmerkung: Beim Anzeigen der Ausgabe von IPsec Security Associations (SA) und der Pkts-Decaps und Pkts-Entschlüsselungszähler werden inkrementiert, Pkts-Encaps und Pkts-Encrypt jedoch nicht. Dies wird in diesem Szenario erwartet. Azure versucht, BGP-Nachbarschaften über die privaten Hub-IP-Space-Adressen zu bilden, und Azure initiiert keine Aushandlung, wenn das benachbarte Ende die APIPA-BGP-Adressierung verwendet. Es ist Aufgabe des Geräts, das eine Verbindung mit Azure herstellt, die BGP-Aushandlung zu initiieren, wenn ein benutzerdefiniertes APIPA verwendet wird.

3) Überprüfen der Layer-2-Anbindung

```
show arp
```

4) Aktivieren Sie IP-Routing.

```
show route
```

5) Führen Sie die Erfassung an den ISP1- und ISP2-Schnittstellen durch.

```
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-Überprüfung - Navigieren Sie zu vWAN Hub > Connectivity.> VPN Sites > Choose the site configured (Konfigurierten Standort auswählen).

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

Azure Link-Verbindungsüberprüfung

Schritt 7: Konfigurieren von ECMP

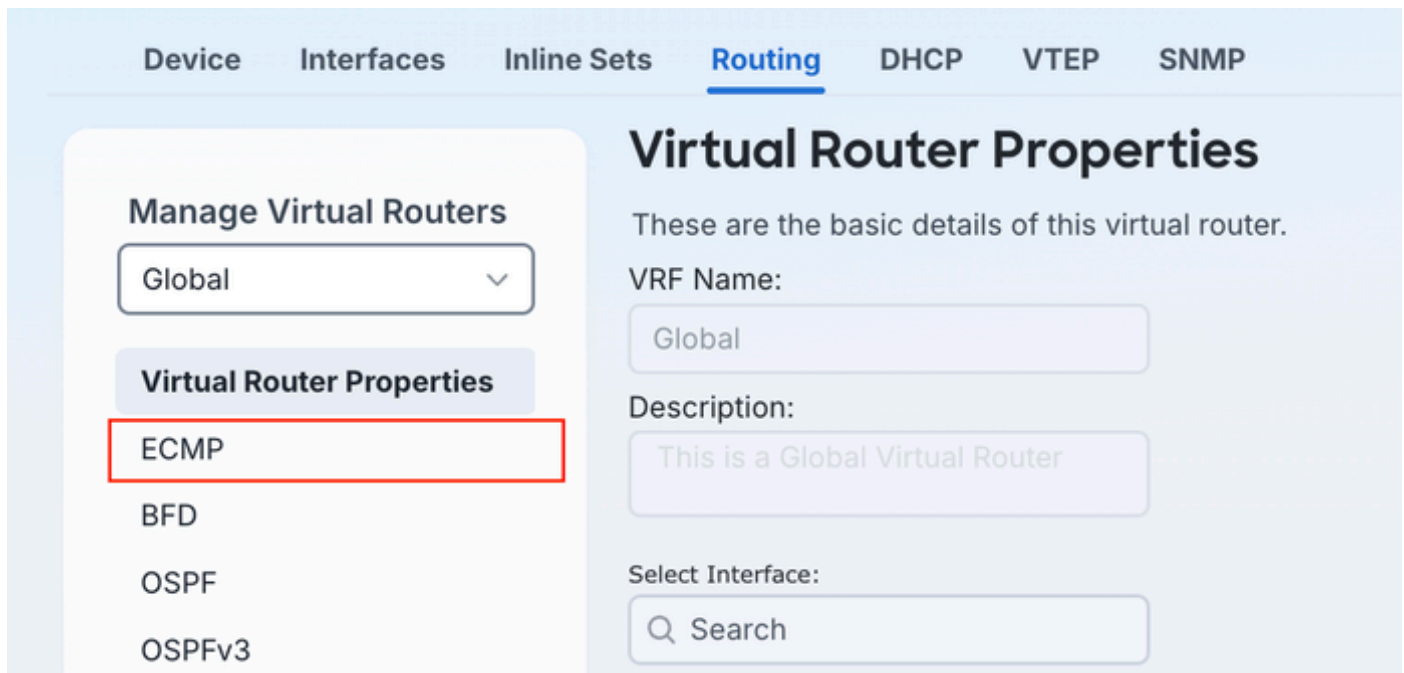
1) Navigieren Sie zu Verwalten > Geräte > Gerätemanagement, und klicken Sie auf die FTD.

Navigieren Sie zum Gerätemanagement im FirePOWER Management Center

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

FTD für Konfigurationsbereitstellung auswählen

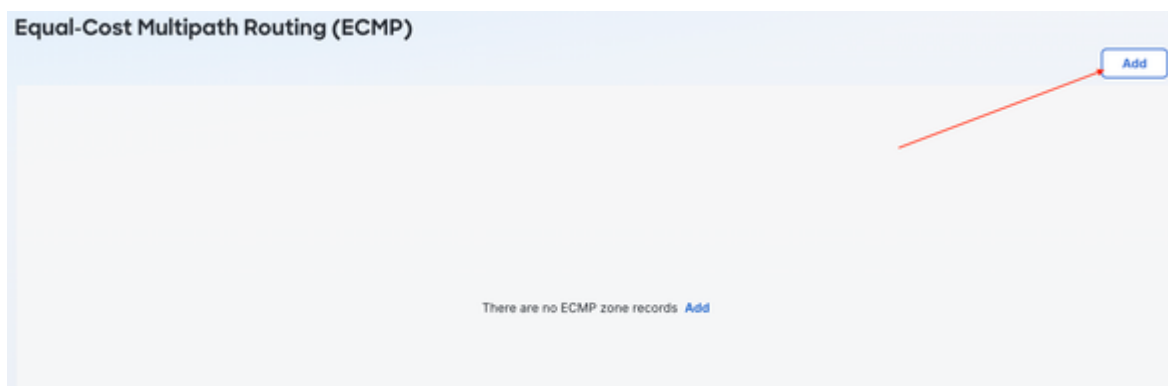
2) Klicken Sie auf die Registerkarte Routing, und wählen Sie ECMP aus.



The screenshot shows the 'Virtual Router Properties' configuration page. The 'Routing' tab is active. On the left, under 'Manage Virtual Routers', the 'Global' VRF is selected. Below this, under 'Virtual Router Properties', the 'ECMP' option is highlighted with a red box. The main configuration area on the right includes a 'VRF Name' field with 'Global' entered, a 'Description' field with 'This is a Global Virtual Router' entered, and a 'Select Interface' field with a search icon and the text 'Search'.

Equal Cost Multi Path-Konfigurationseinstellungen

3) Klicken Sie auf Hinzufügen.



The screenshot shows the 'Equal-Cost Multipath Routing (ECMP)' configuration page. In the top right corner, there is a blue 'Add' button, which is pointed to by a red arrow. Below the button, the text 'There are no ECMP zone records' is displayed, followed by a blue 'Add' link.

Konfigurationseinstellungen für mehrere Pfade zu Equal Cost hinzufügen

4) Nennen Sie die ECMP-Zone, und klicken Sie auf die verfügbaren VTI-Schnittstellen. Klicken Sie dann auf die Schaltfläche Hinzufügen, um sie auf die Spalte Ausgewählte Schnittstellen anzuwenden, und klicken Sie auf 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

Schnittstellen für Equal Cost Multi Path Zone auswählen

5) Stellen Sie sicher, dass Ihre Änderungen gespeichert werden.

You have unsaved changes

Save

Cancel

Änderungen speichern

Schritt 8: BGP konfigurieren

1) Aktivieren Sie den BGP-Prozess auf dem FTD unter Routing > General Settings > BGP. Aktivieren Sie das Kontrollkästchen Enable BGP, und geben Sie die zuvor in Phase 1, Schritt 1d konfigurierte AS-Nummer ein. Navigieren Sie neben 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

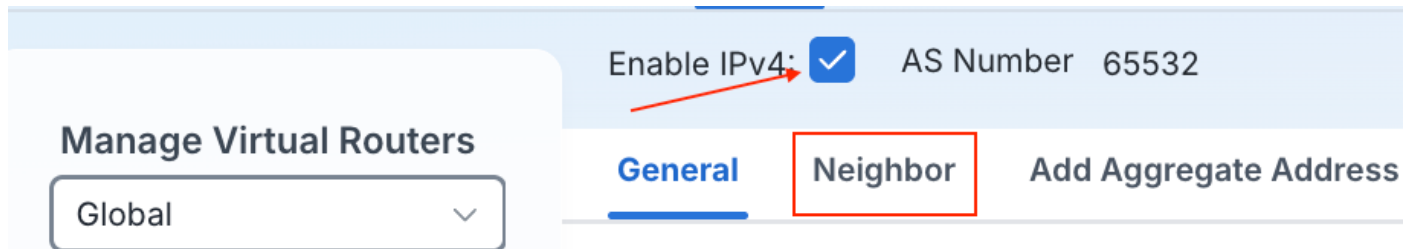
Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

Border Gateway Protocol-Prozess unter "Allgemeine Einstellungen" aktivieren

2) Aktivieren Sie das Kontrollkästchen IPv4 aktivieren für den BGP-Prozess, und klicken Sie auf Neighbor, um BGP-Nachbarn in Azure zu konfigurieren.



Manage Virtual Routers

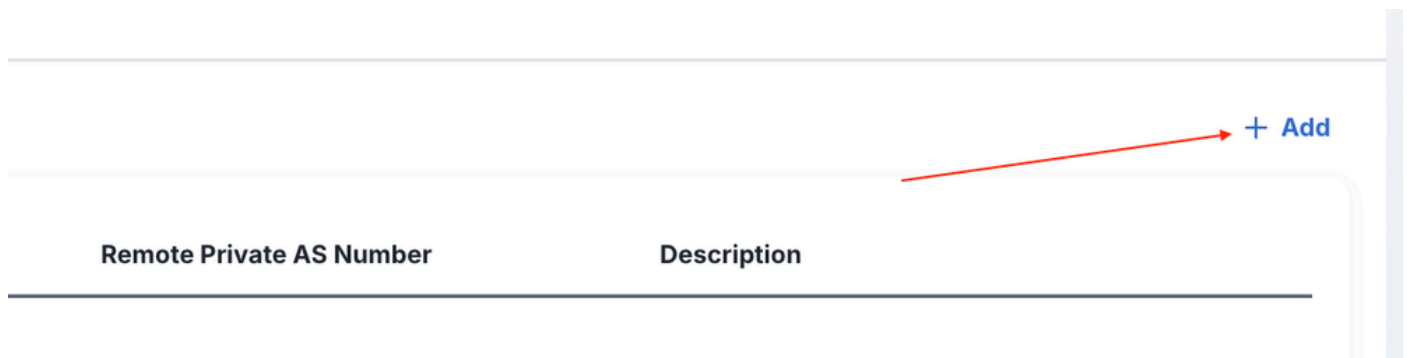
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

IPv4 Border Gateway Protocol-Prozess aktivieren

3) Klicken Sie auf + Hinzufügen.



Remote Private AS Number	Description
+ Add	

Neuen Border Gateway Protocol Neighbor hinzufügen

4) Geben Sie die BGP-Peering-Informationen von ISP1 Instance0 ein, verweisen Sie auf die vermerkten BGP-AS aus dem vWAN-Hub, geben Sie sie als Neighbor Remote AS ein, und fügen Sie bei Bedarf eine Beschreibung hinzu. Klicken Sie auf Erweitert.



Anmerkung: Stellen Sie sicher, dass Sie die BGP-Update-Quelle auswählen, um auf das Loopback für VTI-Schnittstellen auf dem FTD zu verweisen, das dem in Azure konfigurierten ISP1-Link zugeordnet ist.

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

Peering-Informationen für das Border Gateway Protocol konfigurieren

5) Im Menü Advanced (Erweitert) der BGP Neighbor-Konfiguration auf FTD können Sie die Anzahl der TTL-Hops (Time To Live) von der eBGP-StandardEinstellung von 1 Hop auf eine variable Zahl 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. Klicken Sie auf OK.

☐ Enable Authentication

Enable Encryption

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

 (1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Weight

 (0-65535)

BGP Version

Cancel

OK

Erweiterte Border Gateway Protocol-Nachbareinstellungen

6) Wiederholen Sie die Unterschritte 3-5, um Tunnel2 für ISP1 Instance1 zu konfigurieren.

7) Wiederholen Sie die Unterschritte 3-5 zweimal, um die BGP-Peering-Informationen für ISP2 Instance0/Instance1 zu konfigurieren.



Anmerkung: Stellen Sie sicher, dass Sie die zugeordnete BGP-Update-Quelle auswählen, die auf das Loopback für VTI-Schnittstellen auf dem FTD verweist, das dem in Azure konfigurierten ISP2-Link zugeordnet ist.

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

Konfiguration des BGP-Nachbarn von ISP2-Instanz 1

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

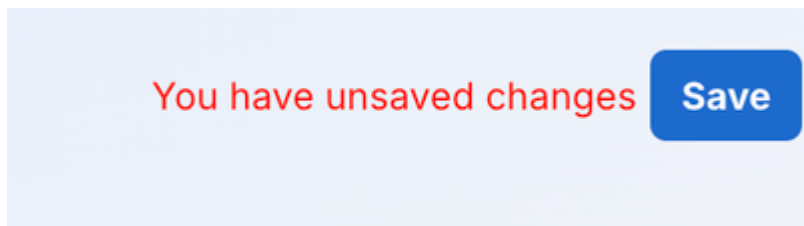
Cancel

OK

Konfiguration des BGP-Nachbarn von ISP 2 Instanz 2

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		

Klicken Sie abschließend auf Speichern.



Änderungen speichern

Standardmäßig installiert das BGP nur einen optimalen Pfad in der Routing-Tabelle, obwohl ECMP für alle VTIs zu Azure konfiguriert ist. BGP Multipath muss separat aktiviert werden, damit beide erlernten Pfade gleichzeitig installiert und verwendet werden können.

Schritt 9: Konfigurieren von eBGP Multipath

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

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global 

Virtual Router Properties

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

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting 

Learned Route Map

Administrative Route Distances 

External	20
Internal	200
Local	200

Routes and Synchronization 

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

Forward Packets Over Multiple Paths 

Number of Paths	1
IBGP number of paths	1

Einstellung "Pakete über mehrere Pfade weiterleiten"

2) Ändern Sie den Standardwert des Felds Number of Paths von 1 auf 4. Klicken Sie auf OK.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Ändern von Weiterleitungspaketen über mehrere Pfade Einstellung

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

Überprüfung/Fehlerbehebung

Nachdem die Bereitstellung abgeschlossen ist, stellen Sie sicher, dass der FTD-BGP-Prozess Nachbarumgebungen mit beiden Azure-Instanzen in den jeweiligen Tunneln herstellt und dass Routen abgerufen, Schnittstellen aktiviert und Protokollverbindungen in der Verbindungstabelle zurückgegeben werden.

Navigieren Sie wie in Phase 2, Schritt 7 beschrieben zur `system support diagnostic-cli` FTD-CLI.

1) Nach der Bereitstellung werden BGP-Nachbarn erwartet, die Präfixe empfangen.

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

```
<#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) Überprüfen Sie die Auffüllung der 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 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) Überprüfung der Verbindungstabelle für BGP-Sitzungen

<#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
```

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.