

Configurazione della connettività vWAN per due ISP di Azure su un firewall protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Diagramma](#)

[Doppi collegamenti DIA \(Direct Internet Access\) \(Azure + bilanciamento del carico FTD/ridondanza\)](#)

[Configurazione](#)

[Fase 1: Configurazione sito VPN vWAN di Azure](#)

[Passaggio 1: Crea sito VPN Azure vWAN \(dispositivo FTD remoto\)](#)

[Passaggio 2: Configura i parametri del gateway APIPA di Azure](#)

[Passaggio 3: Configura parametri della VPN del sito di Azure vWAN](#)

[Passaggio 4: Abilitare e attivare l'API BGP personalizzata sulle istanze del collegamento di sito VPN](#)

[Passaggio 5: Scarica file di configurazione sito VPN](#)

[Fase 2: Configurare FTD per la connettività ISP doppio ad Azure vWAN](#)

[Passaggio 1: Analizza la configurazione VPN scaricata](#)

[Passaggio 2: Configura interfacce di loopback origine aggiornamento BGP collegamento](#)

[Passaggio 3: Configura oggetti criteri Fase 1/Fase 2](#)

[Passaggio 4: Configurazione delle interfacce tunnel virtuali \(VTI\)](#)

[Passaggio 5: Provisioning delle topologie VPN IPsec](#)

[Passaggio 6: Convalida topologie VPN](#)

[Passaggio 7: Configura ECMP](#)

[Passaggio 8: Configurare BGP](#)

[Passaggio 9: Configurazione di eBGP Multipath](#)

[Verifica/Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare la connettività VPN da sito a sito di Microsoft Azure Virtual WAN (vWAN) per proteggere il firewall utilizzando collegamenti WAN doppi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Verificare che entrambi i componenti siano inizialmente configurati nell'ambiente Azure:

- Istanza di Microsoft Azure vWAN
- Hub vWAN di Microsoft Azure

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure FTD versione 10.0
- Cisco Secure FMC versione 10.0
- Microsoft Azure vWAN

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando il FTD della succursale ha due interfacce esterne con interfaccia ISP (Internet Service Provider), ognuna può connettersi in modo ridondante e attivo ad Azure vWAN, in modo che ogni collegamento ISP venga utilizzato. Azure vWAN crea due tunnel IPsec per collegamento di sito, uno per l'istanza dell'hub di Azure0 e uno per l'istanza1, quindi ogni interfaccia ISP termina due tunnel. Su entrambi i collegamenti ISP, il risultato sono quattro tunnel IPsec che terminano sull'FTD.

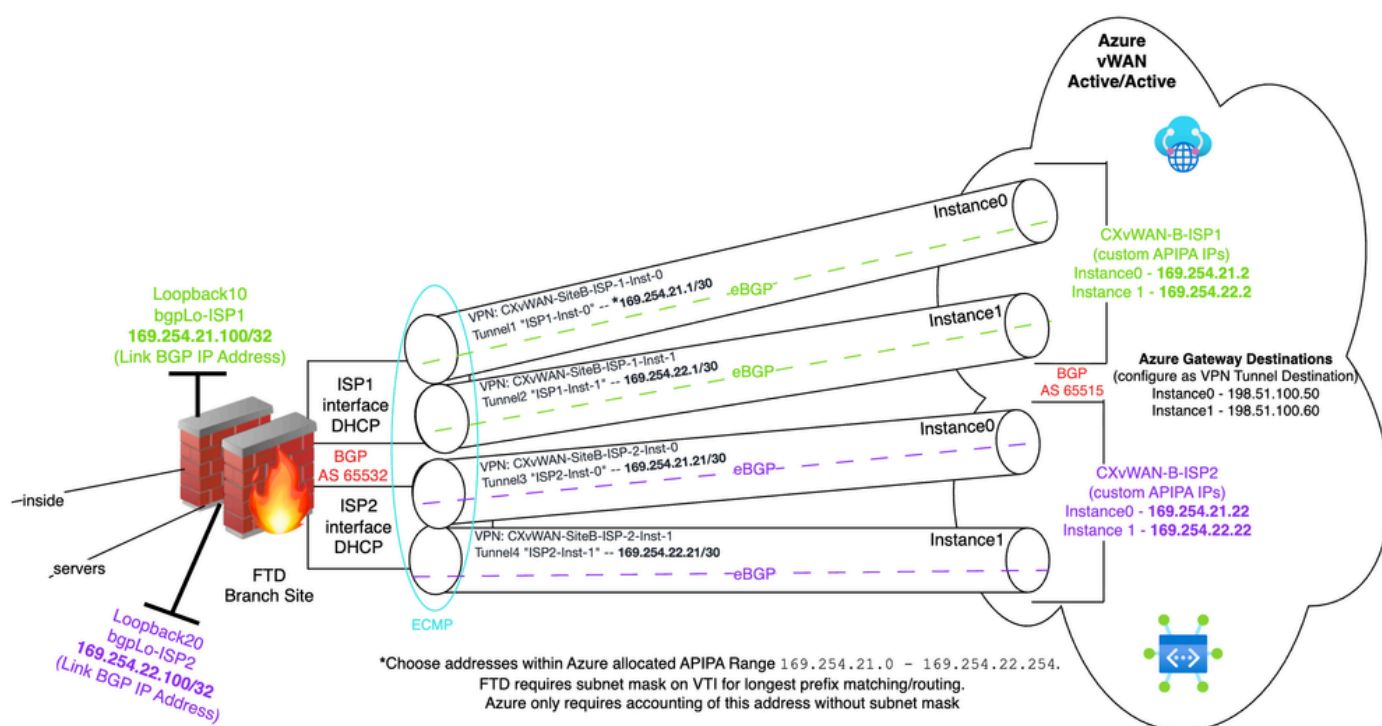
Le istanze di Azure funzionano in modalità attiva/attiva per il bilanciamento del carico e la

ridondanza, quindi l'FTD riflette questa situazione tramite la configurazione ECMP (Equal-Cost Multi-Pathing) in tutti e quattro i tunnel IPsec. Utilizzando indirizzi APIPA (Automatic Private IP Addressing) personalizzati, vengono stabilite relazioni esterne Border Gateway Protocol (eBGP) con numeri di sistema autonomi (ASN) distinti su ciascuno dei quattro tunnel. In questo modo viene abilitata la funzionalità BGP multipath, che fornisce più percorsi ridondanti a ogni coppia di istanze del collegamento al sito hub di Azure.

Diagramma

Il diagramma mostra la topologia della configurazione descritta in questo articolo. La variante di collegamento Dia (Direct Internet Access) doppio ha come origine entrambi i tunnel di Azure da due interfacce esterne sull'FTD.

Doppi collegamenti DIA (Direct Internet Access) (Azure + bilanciamento del carico FTD/ridondanza)



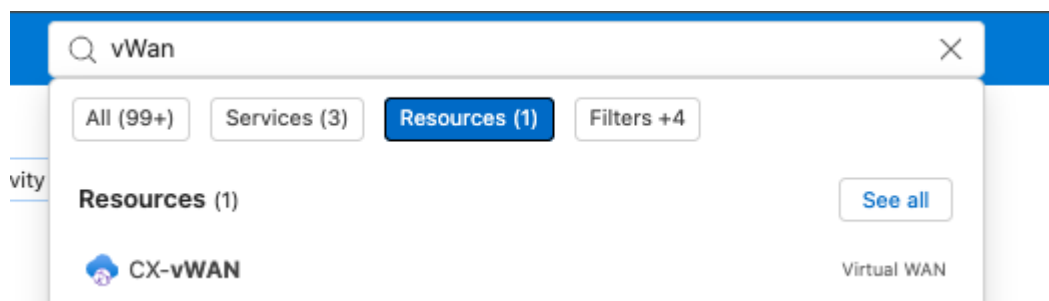
Topologia della connettività Dual Direct Internet Access

Configurazione

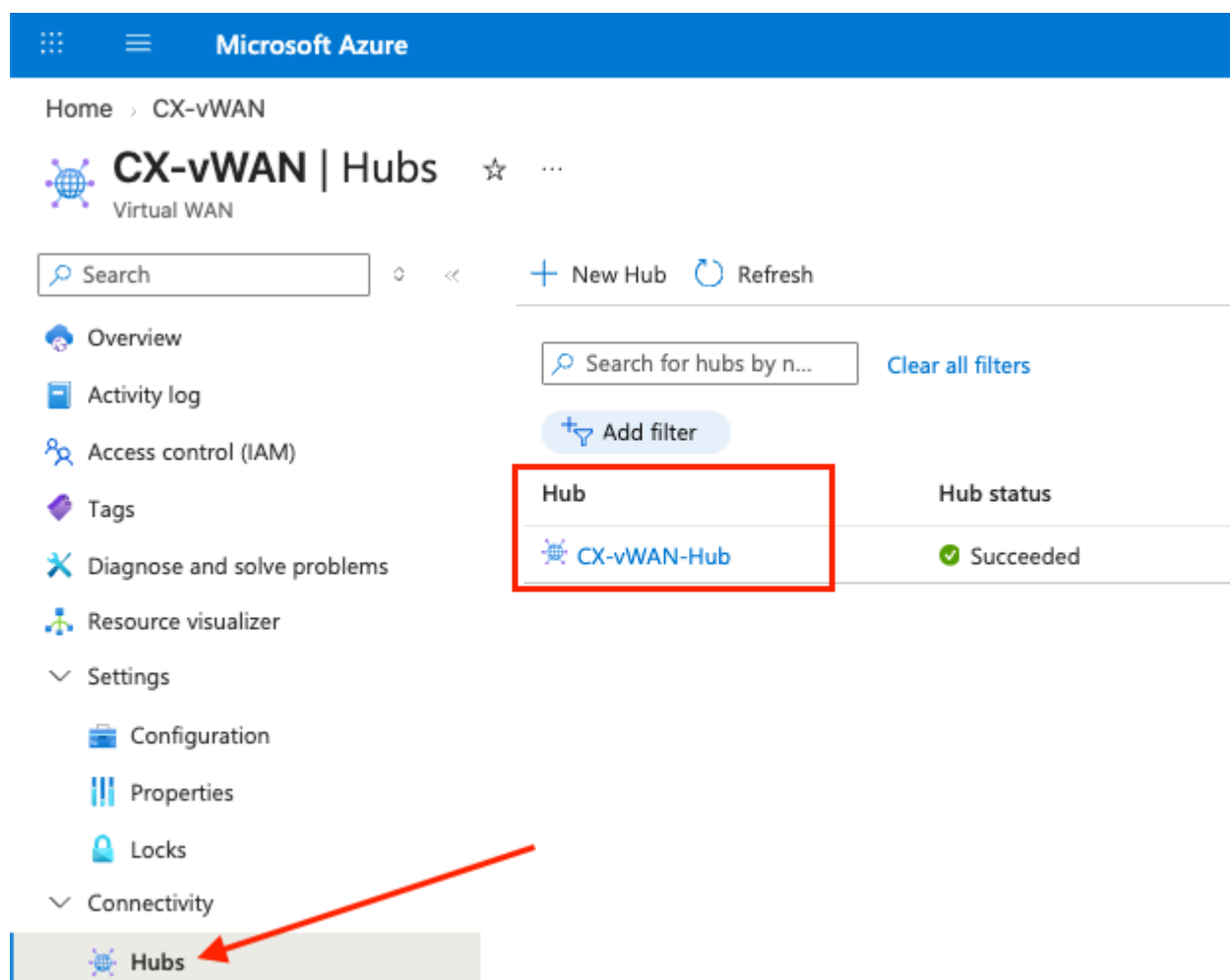
Fase 1: Configurazione sito VPN vWAN di Azure

Passaggio 1: Crea sito VPN Azure vWAN (dispositivo FTD remoto)

1) Cercare vWAN nel campo di ricerca di Azure, fare clic su WAN virtuali per accedere all'hub vWAN di Azure esistente. Passare quindi a Connettività > Hub e fare clic sull'hub vWAN di Azure esistente.



Query di ricerca per WAN virtuale



Seleziona hub WAN virtuale esistente

2) Fare clic su Connettività > VPN (da sito a sito) e fare clic su + Crea nuovo sito VPN

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		

Crea nuovo sito WAN virtuale



Nota: Per la pubblicazione di questo documento è previsto uno spazio vuoto che copre i valori di vari campi delle immagini.

3) Inserire i valori nei campi obbligatori. Al termine, fare clic su Avanti: Collegamenti > per spostarsi in avanti.

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.

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

Previous

Next : Links >

Impostazioni generali configurazione sito VPN

4) Inserire le informazioni sul collegamento richieste. L'indirizzo BGP del collegamento e l'ASN del collegamento sono l'indirizzo di destinazione BGP Layer 3 del tunnel interno e il numero BGP AS sul lato della filiale con cui si forma il vicinato sui tunnel da sito a sito. L'indirizzo BGP del collegamento è un indirizzo subnet non sovrapposto (/32) all'esterno della subnet spazio indirizzi privato dell'hub configurato, che Azure installa come route /32 per raggiungere come router BGP adiacente. Nelle sezioni successive dell'FTD vengono create due interfacce di loopback per rappresentare l'indirizzo BGP del collegamento per ciascun collegamento di sito doppio. L'indirizzo IP del collegamento/nome di dominio completo (FQDN) è l'indirizzo IP di destinazione del layer 3 esterno del traffico diretto al sito della succursale necessario per il provisioning della connettività IP Security (IPsec)/IKEv2 (Internet Key Exchange versione 2). Al termine, procedere al passaggio successivo facendo clic su Avanti: Rivedi + crea >.



Nota: Verificare di aver esaminato la documentazione di Azure specifica se si utilizzano indirizzi compresi tra 169.254.21.0 e 169.254.22.255 per gli indirizzi del tunnel: [Scegliere](#)

[gli indirizzi BGP APIPA.](#)

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 >

Configura parametri collegamento sito

5) Una volta confermate le informazioni come previsto, fare clic su Create (Crea).

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.](#)

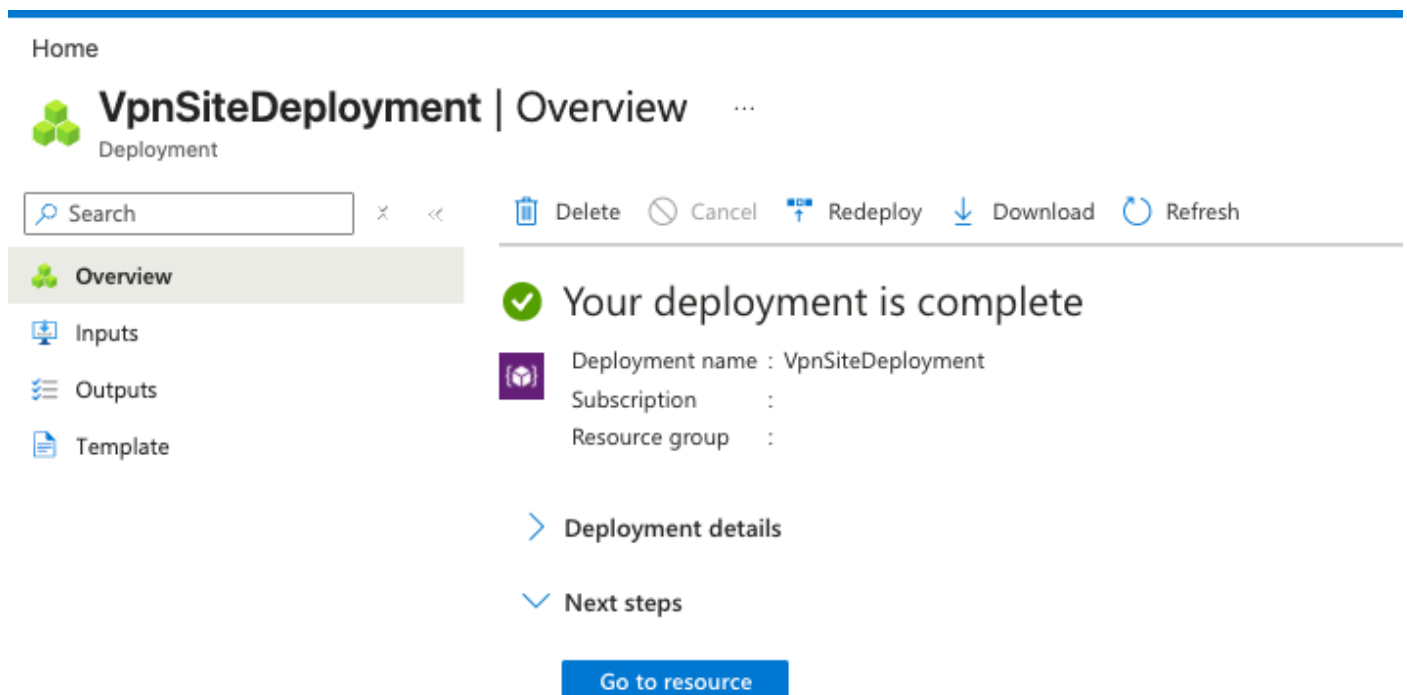
Create

Previous

Next

Verifica e crea un nuovo sito VPN

6) Una volta completata l'installazione del sito VPN, tornare alla configurazione dell'hub vWAN.



Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

✓ Your deployment is complete

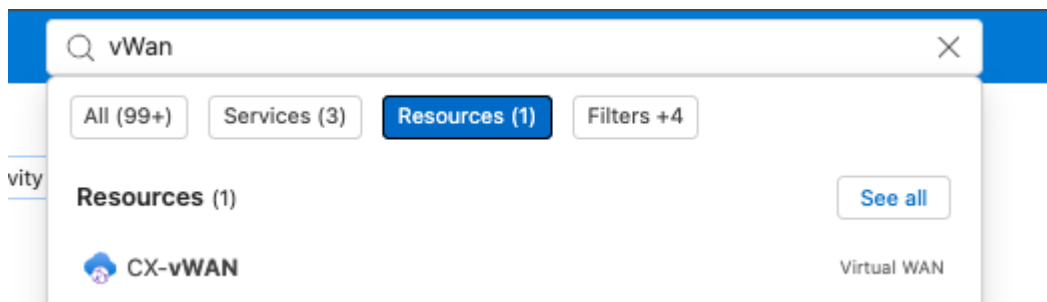
Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

[Go to resource](#)

Stato distribuzione sito WAN virtuale



Search vWan

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

Resources (1) [See all](#)

CX-vWAN Virtual WAN

Query di ricerca per WAN virtuale

Passaggio 2: Configura i parametri del gateway APIPA di Azure

Azure richiede una configurazione aggiuntiva per gli indirizzi APIPA (Automatic Private IP Addressing) nello spazio degli indirizzi IPv4 169.254.0.0/16.

1) Inserire l'hub esistente selezionando Connettività > Hub.

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

Passa a connettività hub WAN virtuale

2) Passare nuovamente a Connettività > VPN (da sito a sito) e fare clic sul collegamento ipertestuale Configurazione gateway.

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 ⓘ

Collegamento ipertestuale configurazione gateway di accesso

3) Viene visualizzato un pannello laterale per modificare il gateway VPN. In VPN Gateway Instance0 e VPN Gateway Instance1, immettere due indirizzi IP BGP personalizzati univoci che fungono da IP adiacenti a ciascuna istanza per i router adiacenti BGP sui tunnel IPsec. Questa operazione è necessaria se si sceglie di utilizzare l'indirizzamento APIPA all'interno di questa topologia. Nel campo Indirizzo peer, immettere l'indirizzo IP del router adiacente BGP da utilizzare per raggiungere le istanze di Azure dall'FTD. Azure non tenta di stabilire il BGP con il FTD se l'indirizzo APIPA è in uso, quindi il FTD tenta di stabilire il router adiacente eBGP su ogni tunnel con Azure.

Il totale risulta da 2 collegamenti x 2 tunnel impliciti; un tunnel verso Instance0 e Instance1 per collegamento ISP; il totale arriva a quattro tunnel IPsec con quartieri BGP tra Azure e le due interfacce ISP FTD.

Questi indirizzi devono essere univoci e, nella dimostrazione, il secondo e l'ultimo indirizzo host nelle subnet /30 assegnate a ciascun tunnel devono essere configurati sull'FTD per l'uso. Una volta configurata, fare clic su Modifica.



Nota: Verificare di aver esaminato la documentazione di Azure specifica se si utilizzano indirizzi compresi tra 169.254.21.0 e 169.254.22.255 per gli indirizzi del tunnel: [Scelta degli indirizzi BGP AP](#)

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

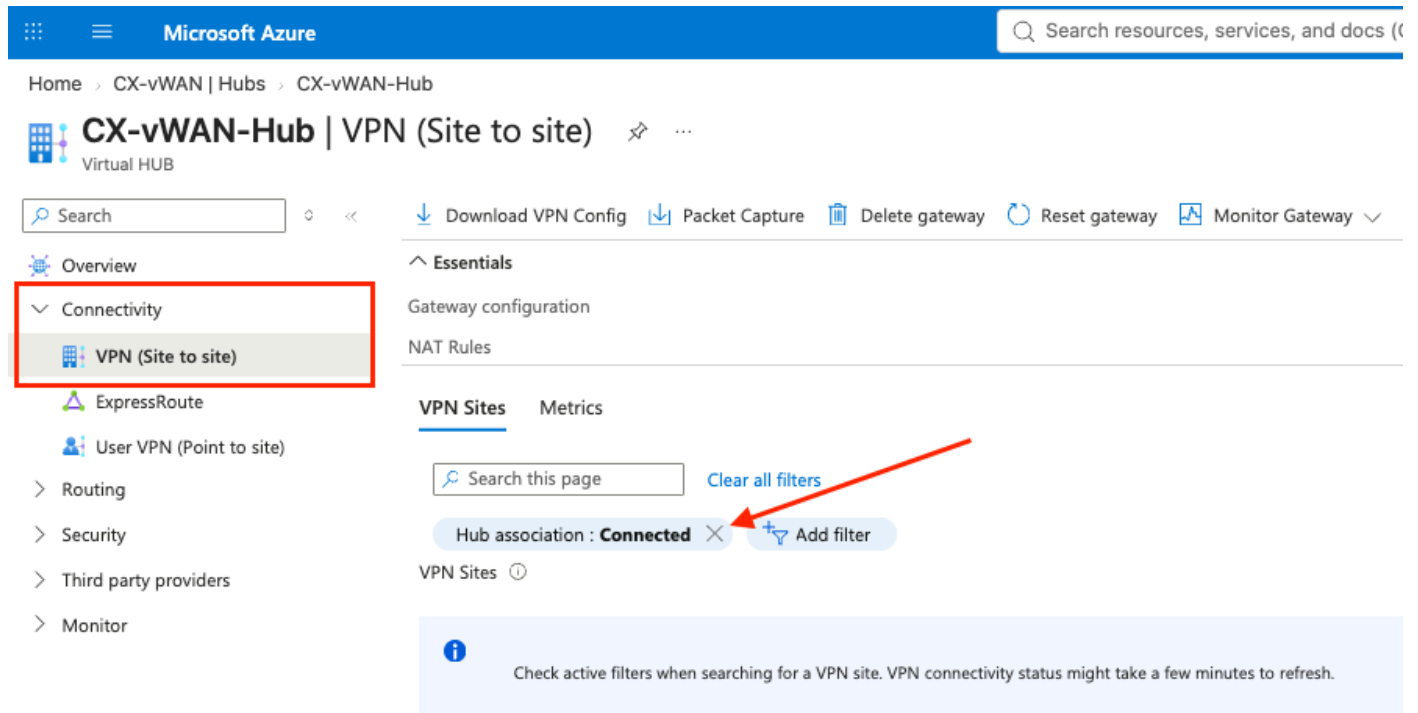
Modifica indirizzi IP BGP personalizzati del gateway VPN



Nota: Come nota di Azure, l'aggiornamento può richiedere fino a 30 minuti o più.

Passaggio 3: Configura parametri della VPN del sito di Azure vWAN

1) Nella pagina Connettività > VPN (da sito a sito) all'interno della configurazione dell'hub vWAN di Azure, fare clic sulla X per cancellare l'associazione dell'hub: Filtro connesso per visualizzare i siti VPN disconnessi.



The screenshot displays the Microsoft Azure portal interface for configuring a vWAN hub. The breadcrumb trail indicates the path: Home > CX-vWAN | Hubs > CX-vWAN-Hub. The main heading is 'CX-vWAN-Hub | VPN (Site to site)'. The left-hand navigation pane shows the 'Connectivity' section expanded, with 'VPN (Site to site)' selected. The right-hand pane shows the 'VPN Sites' tab active. A search bar is present, and a filter 'Hub association : Connected' is applied, with a red arrow pointing to the 'X' icon next to it to indicate removal. A message at the bottom states: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Cancella i filtri di connessione dell'associazione hub

2) Selezionare la casella di controllo accanto al sito VPN di recente provisioning, quindi fare clic su Connetti sito VPN.

 Search

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

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

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

VPN Sites Metrics

 Search this page

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



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

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

Page: 1 ▼

Site name

↑↓ Location

  **Dual-ISP-Site**

Azione connessi sito VPN

3) Configurare la chiave precondivisa (PSK) desiderata e configurare i parametri IPSec desiderati facendo clic sull'opzione di attivazione/disattivazione personalizzata. Questi parametri IPSec devono corrispondere nella configurazione FMC/FTD nei passaggi successivi. Per salvare, scegliere Connetti.



Nota: Il supporto per Diffie-Hellman (DH) Group 24 è stato rimosso in FTD/FMC versione 6.7.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

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

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

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

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

Connect

Configura parametri IPsec e chiave già condivisa

4) Conferma del provisioning del sito VPN completata.

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

Conferma stato provisioning sito VPN

Passaggio 4: Abilitare e attivare l'API BGP personalizzata sulle istanze del collegamento di sito VPN

1) Aggiornare la pagina VPN (da sito a sito) e confermare che la colonna Stato del provisioning della connessione indichi la riuscita dell'operazione, che consente di fare clic sui puntini di sospensione e di fare clic sulla voce di menu a discesa Modifica connessione VPN per questo hub.

Table with 5 columns: Site name, Location, Cloud provider, Connection Provisioning status, Connectivity status.

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

Dropdown menu options:

- Edit VPN connection to this hub
- Delete VPN connection to this hub
- Download VPN site configuration file

Convalida connessione riuscita e modifica connessione VPN

2) Fare clic per configurare la connessione di collegamento 1 (ISP1) e immettere nuovamente la chiave precondivisa (PSK) e assicurarsi di fare clic sull'opzione Abilita accanto all'indirizzo IP BGP personalizzato, quindi mappare l'indirizzo host rimanente delle subnet /30 che costituiranno i valori dei campi dell'indirizzo IP di destinazione del tunnel interno dell'installazione IP BGP generata dagli FTD.

In sostanza, ISP1 VTI Tunnel1 per Azure Instance0 ha un'assegnazione di indirizzo di 169.254.21.1/30, e il secondo ISP1 VTI Tunnel2 che termina sull'FTD ha un IP di 169.254.22.1/30

assegnato per Instance1.

Fare clic su Avanti: Link Connection 2> per procedere con i parametri di collegamento dell'ISP 2.



Nota: È possibile che sia necessario immettere nuovamente la chiave primaria e fare nuovamente clic sull'opzione Gruppo PFS allineato nel menu a discesa in Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

.....

Connection Mode ⓘ

Default Initiator Only Responder Only

Border gateway protocol ⓘ

Disable Enable

Custom BGP IP Addresses ⓘ

Disable Enable

Custom BGP IP Address

Instance 0 ⓘ

169.254.21.2

Instance 1 ⓘ

169.254.22.2

Use Azure Private IP Address ⓘ

Yes No

Protocol

IKEv2 IKEv1

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

Use policy based traffic selector ⓘ

Enable Disable

IPsec ⓘ

Default Custom

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

DPD timeout in seconds * ⓘ

45

Review + create

Previous

Next : Link connection 2 >

Configurare la connessione di collegamento con impostazioni BGP personalizzate

3) Ripetere i passaggi precedenti e applicare i parametri applicabili in Connessione link 2 (collegamento ISP2). Al termine, fare clic su Crea.

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

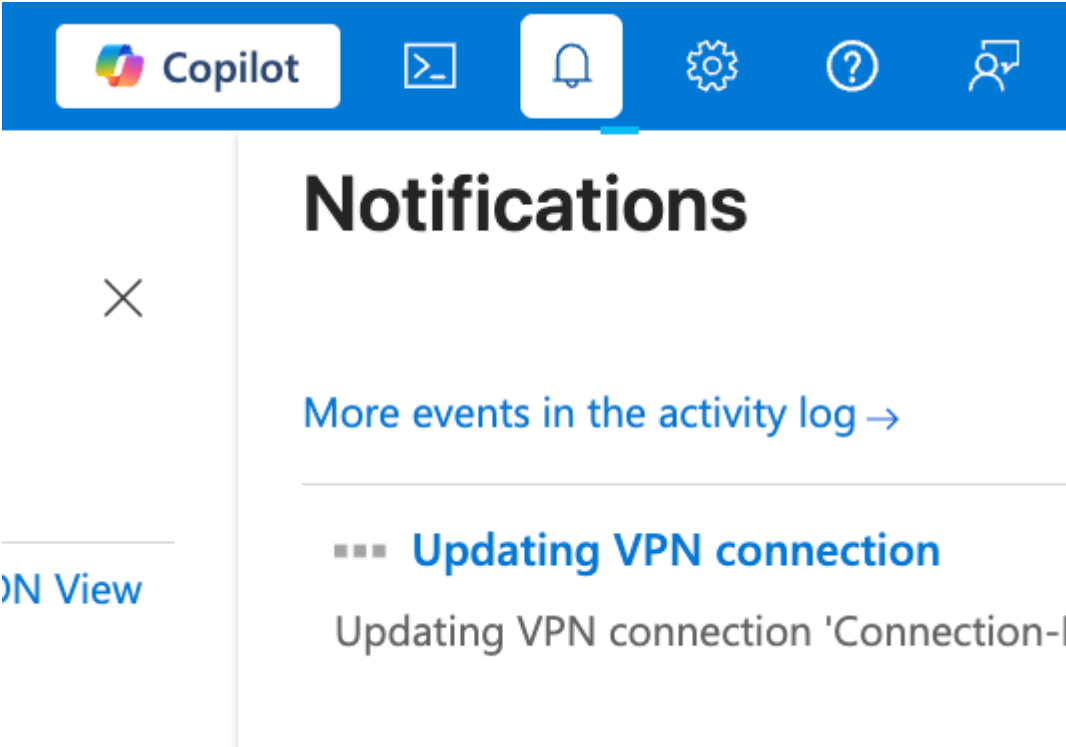
Create

Previous

Next

Configura connessione collegamento due impostazioni BGP personalizzate

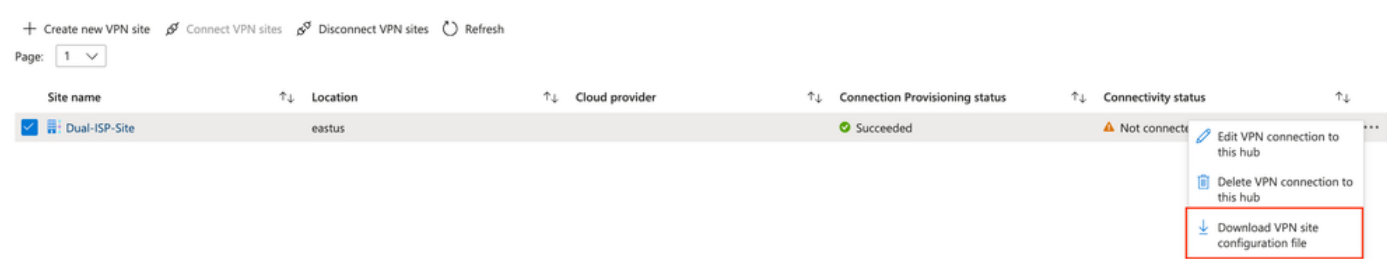
4) Le notifiche nell'interfaccia utente di Azure mostrano l'inizio dell'attività di aggiornamento.



Notifica di inizio attività di aggiornamento di Azure

Passaggio 5: Scarica file di configurazione sito VPN

1) Nella stessa pagina VPN (da sito a sito) in Azure, scegliere l'icona con i puntini di sospensione all'estrema destra del sito VPN configurato e scegliere l'opzione Scarica file di configurazione sito VPN.



Opzione Scarica file di configurazione sito VPN

2) Fare clic su Fare clic qui per scaricare il collegamento ipertestuale.



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



Scarica file di configurazione sito VPN

Fase 2: Configurare FTD per la connettività ISP doppio ad Azure vWAN

Passaggio 1: Analizza la configurazione VPN scaricata

1) Aprire il file di configurazione scaricato e viene visualizzato un output JSON (JavaScript Object Notation) simile. L'output mostra uno dei due oggetti scritti nel file. Queste informazioni forniscono un contesto utile per la configurazione FTD.



Nota: Per una messa a fuoco avanzata, diversi oggetti irrilevanti e coppie chiave/valore vengono potati per brevità.



Nota: L'ordinamento degli oggetti JSON ISP-Link-1 nel file scaricato è invertito. I puntini di sospensione nell'output di codice rappresentano l'oggetto ISP-2-Link con la relativa configurazione applicabile.

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

```

Mantenere questo output come riferimento mentre si completano i passaggi.

Passaggio 2: Configura interfacce di loopback origine aggiornamento BGP collegamento

Le voci di configurazione dei nodi adiacenti BGP nel processo BGP FTD (configurato nei passaggi successivi dell'FTD) richiedono un'origine stabile che rappresenti l'indirizzo IP BGP del collegamento corrispondente nella configurazione del collegamento al sito di Azure.

1) Selezionare Dispositivi > Gestione dispositivi.

Cloud-delivered Firewall Management Center
Devices / Device Management

Monitor

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

Manage

- Policies >
- Objects
- Devices**

Devices

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

— Show less

Passare A Gestione Periferiche In Firepower Management Center



Nota: Questa esercitazione utilizza un centro di gestione dei firewall (cdFMC) distribuito su cloud; le misure restano tuttavia invariate per i CCP locali.

2) Fare clic sull'FTD che si sta configurando come dispositivo VPN per filiale/sito con connettività ISP doppia.

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

Selezionare l'FTD per la distribuzione della configurazione

3) Fare clic sul menu a discesa Aggiungi interfacce e fare clic su Interfaccia loopback.

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

Aggiungi Interfaccia Di Loopback Al Dispositivo

4) Immettere un Nome dell'interfaccia di loopback, accertarsi di selezionare la casella di controllo Abilitato e immettere un ID di loopback. Se desiderato, immettere una descrizione. Al termine, fare clic sulla scheda IPv4.

Add Loopback Interface

General **IPv4** IPv6

Name:

☒ **Enabled**

Loopback ID: *

(1-1024)

Description

Cancel OK

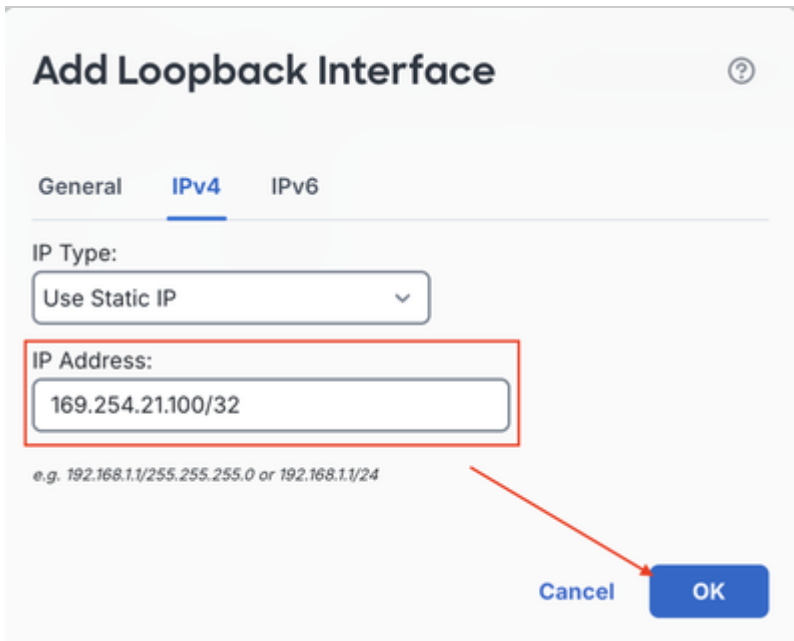
Configurazione Delle Informazioni Dell'interfaccia Di Loopback E Dell'Indirizzo IPv4

5) Immettere l'indirizzo IP di loopback che sarà l'indirizzo IP BGP del collegamento configurato nelle fasi precedenti per il collegamento del sito ISP1 in Azure. Questo IP viene usato come origine di aggiornamento BGP nelle istanze adiacenti configurate tra FTD e Istanze di Azure su ISP1.



Nota: È possibile fare riferimento al valore definito in precedenza nel file JSON di configurazione della VPN scaricato in

vpnSiteConfiguration.BgpSetting.BgpPeeringAddress per ISP1



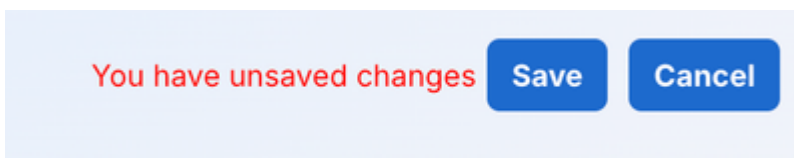
Immettere l'indirizzo IPv4 di loopback e premere OK

6) Ripetere i passaggi secondari c-e in questa sequenza per la configurazione del loopback BGP ISP2.

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

Creazione Della Prima E Della Seconda Interfaccia Di Loopback

7) Salvare la configurazione.



Salva modifiche

Passaggio 3: Configura oggetti criteri Fase 1/Fase 2

1) Per configurare la configurazione IKEv2/IPsec corrispondente sul FMC alle topologie VPN FTD, selezionare Gestisci > Oggetti, scorrere il menu di navigazione fino a VPN ed espandere il sottomenu. Configurare il criterio IKEv2 fase 1 scegliendo Criterio IKEv2 dal menu e facendo clic su Aggiungi criterio IKEv2.

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

Name

AES-GCM-NUL-**SHA**

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

AES-**SHA**-**SHA**

AES-**SHA**-**SHA-LATEST**

DES-**SHA**-**SHA**

DES-**SHA**-**SHA-LATEST**

Umbrella-AES-GCM-256

Q

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

Crea nuovo oggetto criterio IKEv2

2) Inserire un nome per il nuovo criterio IKEv2, scegliere Priorità e/o Durata. Verificare che i criteri corrispondano su entrambe le estremità del tunnel per quanto riguarda integrità, crittografia, funzione pseudo-casuale (PRF) e gruppo DH. Scegliere gli elementi dell' algoritmo/gruppo da associare alla configurazione di Azure e fare clic su Aggiungi.



Nota: È possibile fare riferimento a questi valori esatti nel file di configurazione scaricato in `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

New IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

SHA256

Cancel Save

Crea criterio IKEv2

3) Al termine della configurazione, fare clic su Save (Salva).

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

Salva criterio IKEv2

4) Configurare i parametri per la fase 2/IPSec nel sottomenu Proposta IPsec IKEv2 e fare clic su Aggiungi proposta IPsec IKEv2.

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 algorithms that are supported by both peers 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

Crea proposta IPsec IKEv2

5) Assegnare un nome alla proposta IPsec IKEv2 e verificare che le stesse impostazioni siano allineate. Al termine, fare clic su Salva.

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



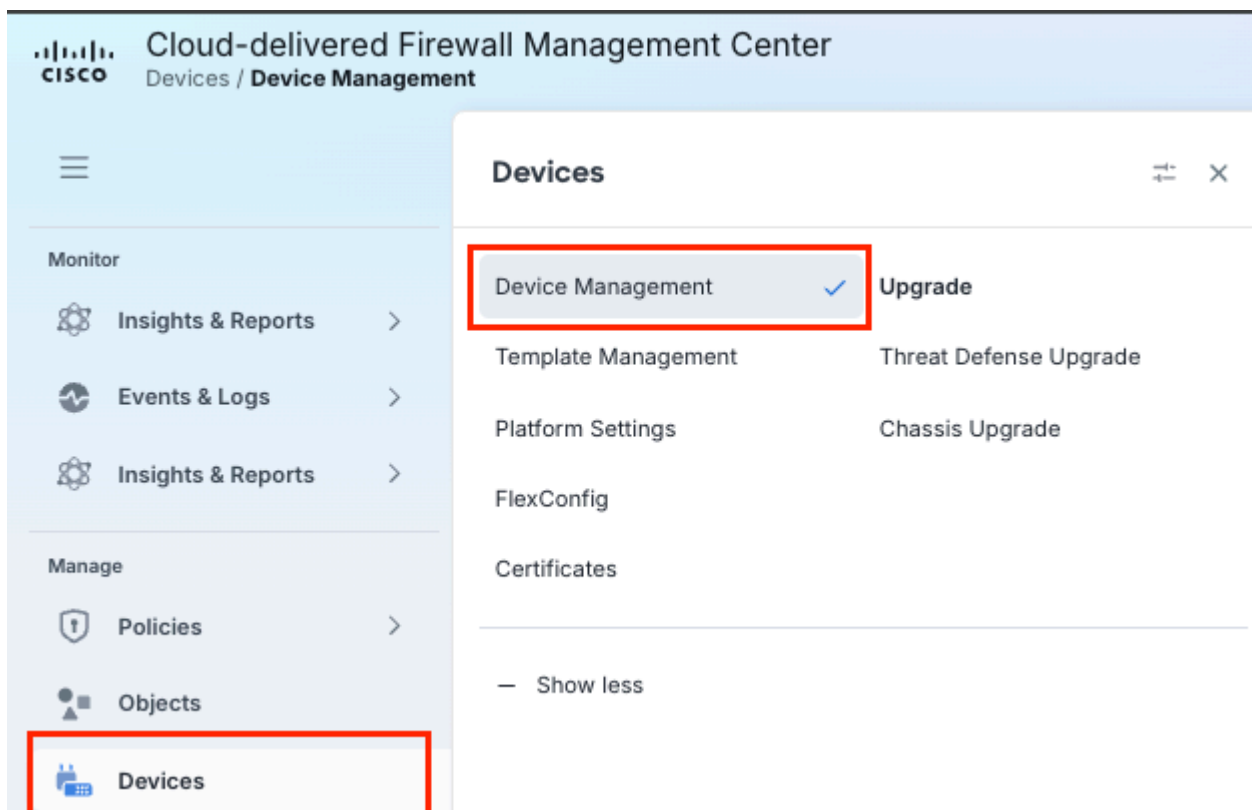
Cancel

Save

Denominare la proposta IPSec IKEv2 e fare clic su Salva

Passaggio 4: Configurazione delle interfacce tunnel virtuali (VTI)

1) Selezionare Dispositivi > Gestione dispositivi.



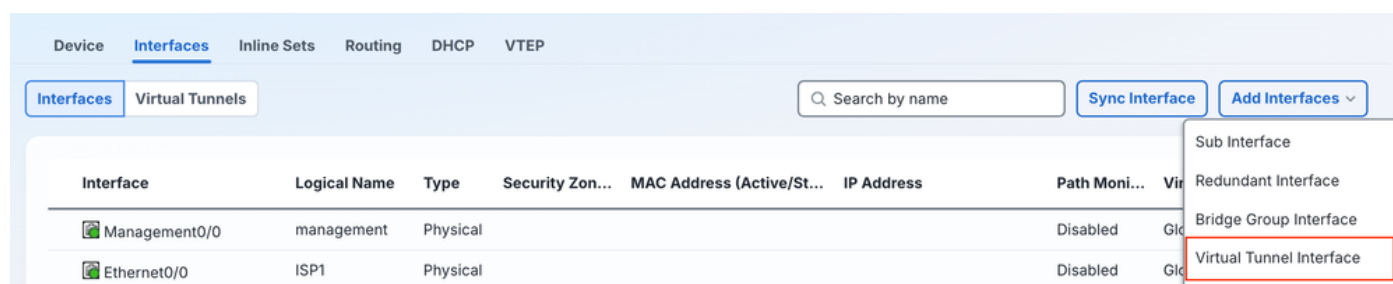
Passare A Gestione Periferiche In Firepower Management Center

2) Fare clic sull'FTD che si sta configurando come dispositivo VPN per filiale/sito con connettività ISP doppia.

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

Selezionare l'FTD per la distribuzione della configurazione

3) Fare clic sul menu a discesa Add Interfaces (Aggiungi interfacce) e selezionare Virtual Tunnel Interface (VTI).



Crea interfaccia tunnel virtuale

4) Inserire le informazioni sul tunnel. Verificare che la casella di controllo Abilitato sia selezionata, che Nome sia stato immesso (anche Descrizione, se desiderato) e che Area di protezione facoltativa sia stata scelta. Allineare l'interfaccia padre corretta con connessione ISP per configurare la VTI in e configurare l'indirizzo IP appropriato per la connettività IPsec del tunnel

interno per la VTI. Al termine, premere OK.



Suggerimento: Il diagramma di riferimento mostra un ulteriore contesto sulla potenziale configurazione VPN per la connettività Azure dual-WAN con 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) Configurare 3 VTI aggiuntive sulle interfacce ISP1 e ISP2 padre.

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

Configurazione di interfacce tunnel virtuali aggiuntive

f) Assicurarsi di fare clic su Salva per salvare le modifiche.

You have unsaved changes

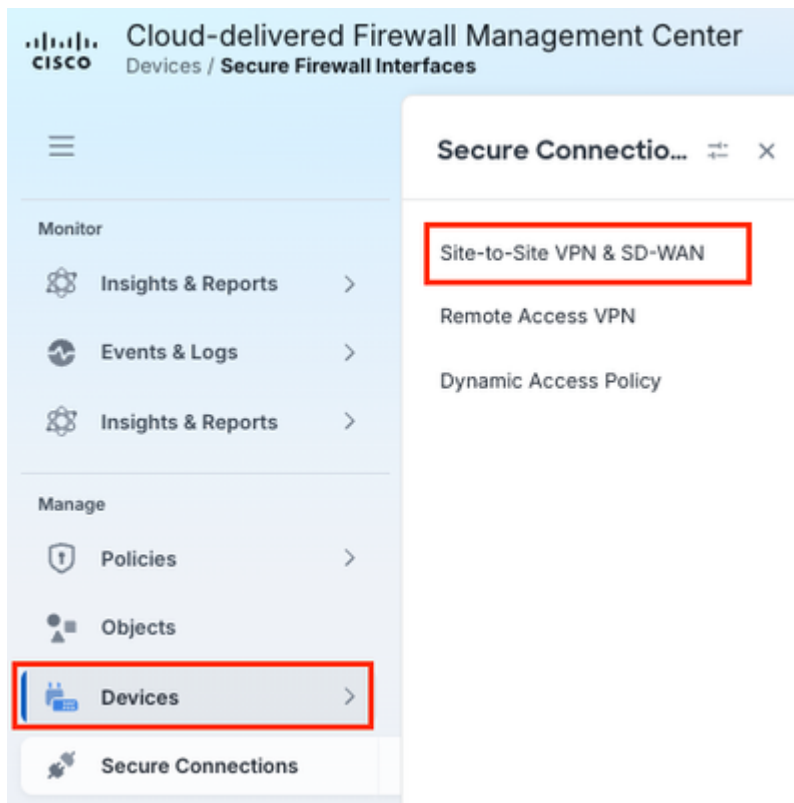
Save

Cancel

Salva modifiche

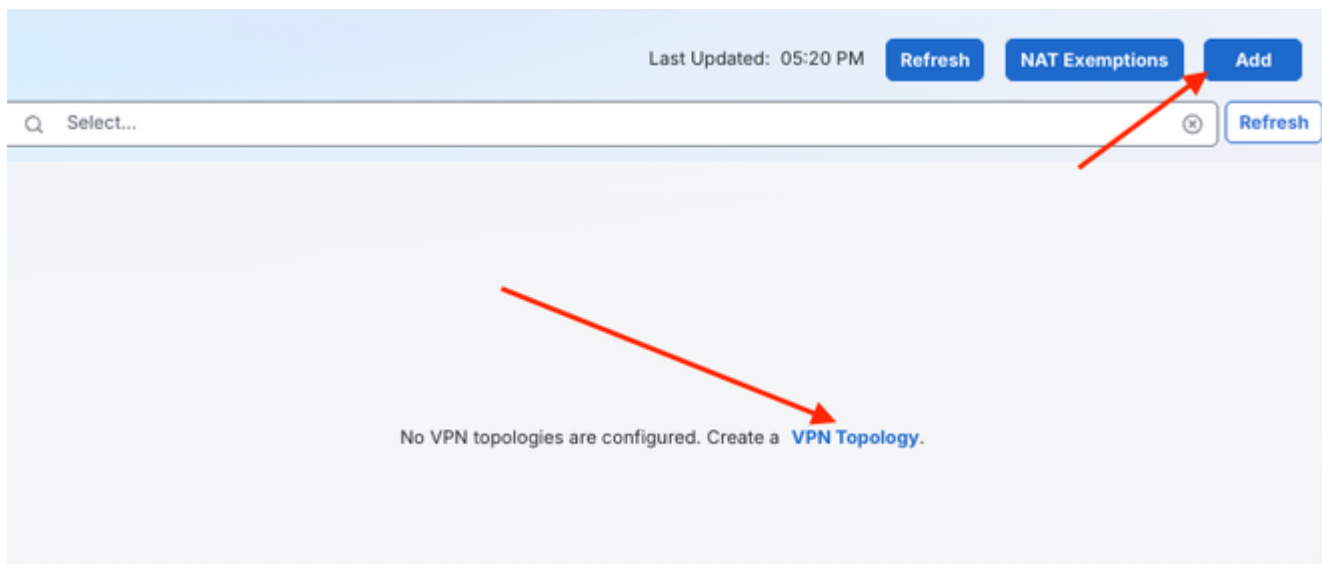
Passaggio 5: Provisioning delle topologie VPN IPsec

1) Selezionare Manage > Secure Connections > Site-to-Site VPN & SD-WAN (Gestione > Connessioni sicure > VPN da sito a sito e SD-WAN).



Gestire connessioni VPN e SD-WAN da sito a sito

2) Fare clic sul collegamento ipertestuale iniziale della configurazione della topologia VPN al centro dell'output iniziale oppure fare clic sul pulsante Add (Aggiungi).



Aggiungi nuova configurazione topologia VPN

3) Immettere un nome di topologia per il primo tunnel su ISP1 collegato all'istanza di Azure0. Fare clic sul pulsante di opzione VPN basata su route, quindi fare clic sul tipo di topologia VPN peer-to-peer. Al termine, fare clic su Crea.

Create VPN Topology

Topology name *

CXvWAN-SiteB-ISP-1-Inst-0

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

Configura tipo di topologia VPN basata su route

4) Innanzitutto, scegliere il dispositivo Nodo A e nell'elenco a discesa Dispositivo indicare che l'FTD sta terminando i tunnel VPN da Azure. Dopo che la procedura guidata ha recuperato le VTI disponibili dal dispositivo, selezionare la VTI appropriata per l'interfaccia padre e l'istanza che si sta configurando dal menu a discesa. Dal menu Dispositivo del nodo B, scegliere il lato Azure come nodo Extranet nella configurazione della topologia VPN. Verificare di aver configurato un nome descrittivo per il nodo B e di aver immesso l'indirizzo IP dell'endpoint appropriato. Al termine, fare clic sulla scheda IKE per implementare la configurazione del tunnel per la fase 1.



Nota: È possibile fare riferimento ai valori degli indirizzi IP degli endpoint dell'istanza nel file di configurazione scaricato in
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` e
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*
CXvWAN-SiteB-ISP-1-Inst-0

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*
CXvWAN-FTD-2

Virtual Tunnel Interface:*
ISP1-Inst-0 (IP: 169.254.21.1) +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*
Extranet

Device Name*:
Azure-ISP1-Link-Inst0

Endpoint IP Address*:

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

Definizione Degli Endpoint Della Topologia Del Nodo A E Del Nodo B

5) Scorrere il menu di navigazione fino a Impostazioni IKEv2 e fare clic sull'icona a forma di matita per modificare i criteri in base ai criteri IKEv2 configurati di recente. Scegliere quindi l'opzione Chiave manuale già condivisa dal menu a discesa Tipo di autenticazione e immettere la chiave già configurata in Azure. Al termine, fare clic sulla scheda IPsec per configurare i parametri del tunnel IPsec fase 2.



Nota: È possibile fare riferimento alla chiave già condivisa nel file di configurazione scaricato in `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology

Topology Name:*
CXvWAN-SiteB-ISP-1-Inst-0

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Azure_IKEv2 

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

Modifica impostazioni IKEv2 e chiave di autenticazione

6) Fare clic sull'icona a forma di matita accanto al set di trasformazioni proposte IPsec IKEv2, quindi selezionare i parametri dei criteri IPsec configurati in precedenza. Assicurarsi di modificare il valore Durata affinché corrisponda alle impostazioni VPN di Azure vWAN. Una volta confermate le informazioni sulla configurazione, fare clic su Salva.



Nota: È possibile fare riferimento al valore Lifetime nel file di configurazione scaricato in `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

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

Configura durata proposta IPsec

7) Ripetere i passaggi secondari precedenti nel Passaggio 5 per creare gli altri tunnel di Azure nell'istanza 1 dell'ISP1, nell'istanza 0 dell'ISP2 e nell'istanza 1 dell'ISP2.

> 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	✓		

Crea topologie VPN aggiuntive da sito a sito

Passaggio 6: Convalida topologie VPN

Immettere in system support diagnostic-cli, digitare en e premere Invio (CLI di sola lettura).

1) Controllare la connettività del tunnel IKE fase 1.

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

2) Controllare la connettività IPsec fase 2.

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



Nota: Quando si visualizzano l'output delle associazioni di sicurezza (SA) IPsec e i decriptati e i contatori di decrittografia PKTS sono in aumento, mentre gli incapsulamenti PKTS e i PKTScriptati non lo sono. Questa situazione è prevista in questo scenario. Azure sta tentando di formare relazioni di vicinato BGP tramite gli indirizzi dello spazio IP privato dell'hub e Azure non avvia la negoziazione se l'estremità adiacente utilizza indirizzi BGP APIPA. È responsabilità del dispositivo che si connette ad Azure avviare la negoziazione BGP quando viene utilizzata l'API personalizzata.

3) Controllare La Connettività Di Layer 2.

```
show arp
```

4) Controllare il routing IP.

```
show route
```

5) Eseguire l'acquisizione sulle interfacce ISP1 e ISP2.

```
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) Verifica di Azure - Passare a Hub vWAN > Connettività.> Siti VPN > Scegliere il sito configurato.

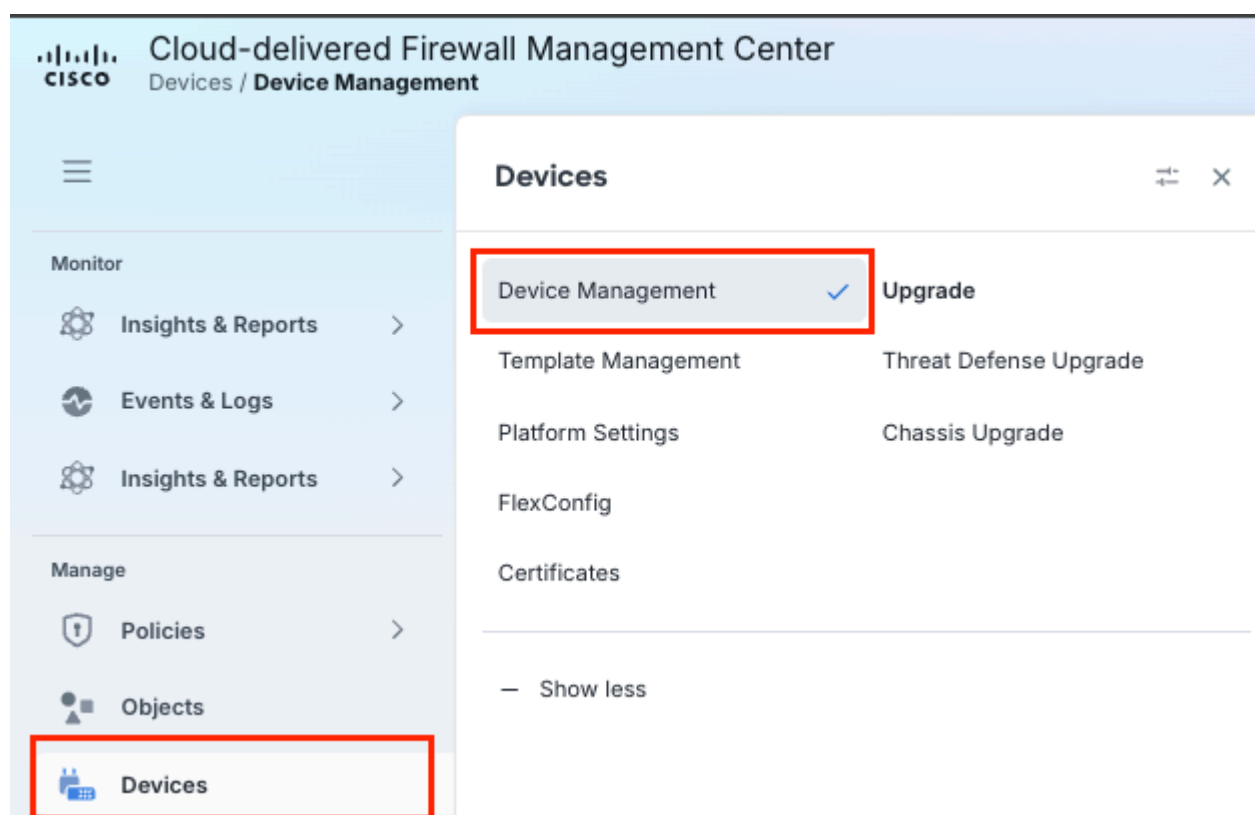
Links

☐ 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

Verifica della connettività di Azure Link

Passaggio 7: Configura ECMP

1) Selezionare Gestisci > Dispositivi > Gestione dispositivi e fare clic su FTD.



Passare A Gestione Periferiche In Firepower Management Center

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

Selezionare l'FTD per la distribuzione della configurazione

2) Fare clic sulla scheda Instradamento e scegliere ECMP.

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

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

Impostazioni di configurazione a percorsi multipli Equal Cost

3) Fare clic su Add.

Equal-Cost Multipath Routing (ECMP)

Add

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

Aggiunta di impostazioni di configurazione a percorsi multipli pari costo

4) Assegnare un nome alla zona ECMP, fare clic sulle interfacce VTI disponibili, quindi sul pulsante Aggiungi per applicarle alla colonna Interfacce selezionate e fare clic su 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

Selezione delle interfacce per una zona a percorsi multipli pari costo

5) Assicurarsi di salvare le modifiche.

You have unsaved changes

Save

Cancel

Salva modifiche

Passaggio 8: Configurare BGP

1) Abilitare il processo BGP sull'FTD in Routing > General Settings > BGP. Selezionare la casella di controllo Enable BGP e immettere il numero AS configurato in precedenza in Fase 1, Fase 1d. Fare clic su accanto a 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)

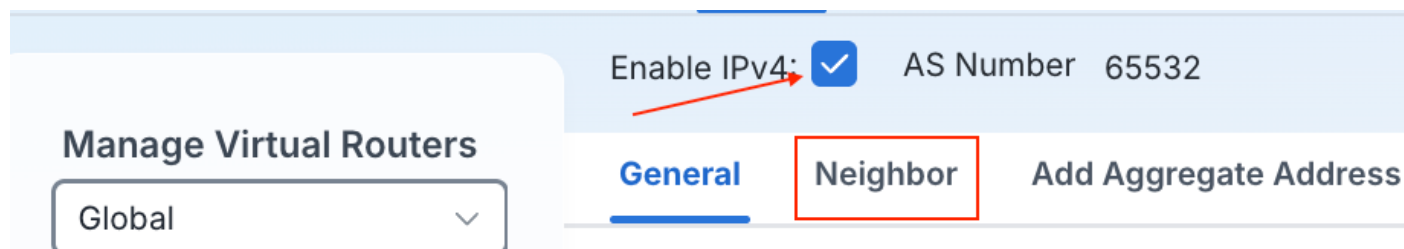
Best Path Selection

Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

2) Verificare di aver selezionato la casella di controllo Abilita IPv4 per il processo BGP, quindi fare clic su Router adiacente per configurare i router adiacenti BGP in Azure.



Manage Virtual Routers

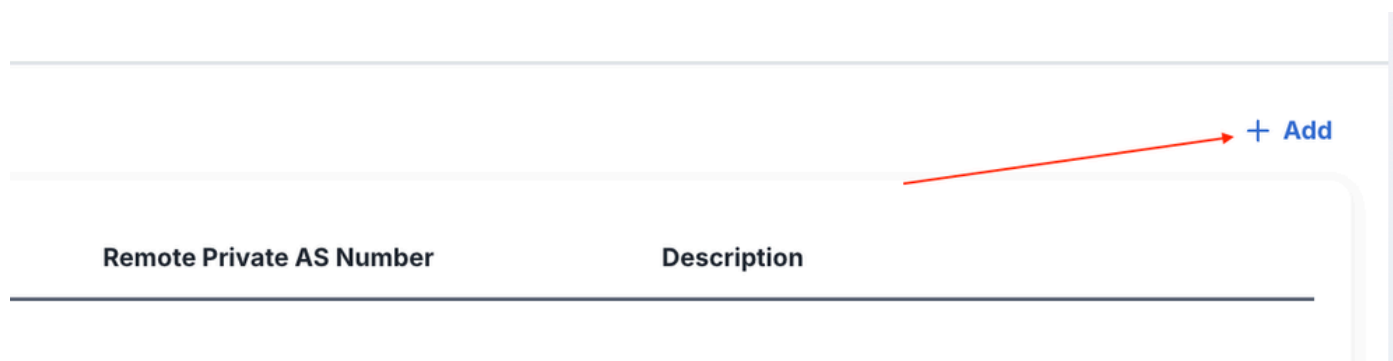
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

Abilita processo IPv4 Border Gateway Protocol

3) Fare clic su + Aggiungi.



+ Add

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

Aggiungi nuovo router adiacente Border Gateway Protocol

4) Immettere le informazioni sul peering BGP Instance0 dell'ISP1, fare riferimento all'ASA BGP annotata dall'hub vWAN e immetterla come AS remoto adiacente, quindi aggiungere una descrizione se desiderato. Fare clic su Avanzate.



Nota: Scegliere l'origine aggiornamento BGP per fare riferimento al loopback per le interfacce VTI nell'FTD mappato al collegamento ISP1 configurato in Azure.

Add Neighbor ?

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Update Source:

bgpLo-ISP1

Description

Filtering Routes

Routes

Timers

Advanced

Migration

Configurazione delle informazioni di peering del protocollo Border Gateway

5) Nel menu Advanced (Avanzate) della configurazione BGP Neighbor su FTD, è possibile modificare il numero di hop TTL (Time To Live) dall'impostazione predefinita eBGP di 1 hop a un numero variabile. Gli endpoint BGP di Azure non sono connessi direttamente all'infrastruttura di Azure tramite il tunnel e nell'endpoint tendono a essere presenti più hop rispetto al valore TTL eBGP predefinito di 1 permesso. Fare clic su OK.

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

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Impostazioni avanzate router adiacente Border Gateway Protocol

6) Ripetere i passaggi secondari 3-5 per configurare Tunnel2 per l'istanza 1 del provider di servizi Internet1.

7) Ripetere i passaggi secondari da 3 a 5 due volte per configurare le informazioni sul peering BGP Instance0/Instance1 dell'ISP2.



Nota: Assicurarsi di scegliere l'origine aggiornamento BGP allineata che fa riferimento al loopback per le interfacce VTI nell'FTD mappato al collegamento ISP2 configurato in Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

Configurazione router adiacente BGP istanza 1 ISP2

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
-

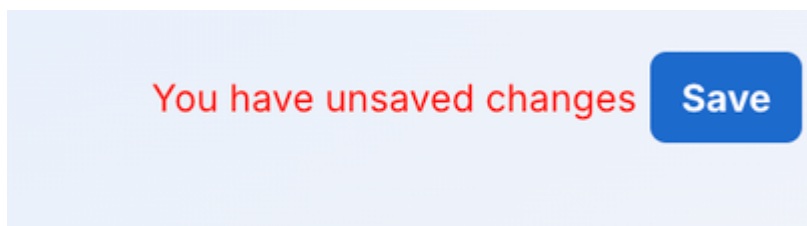
Cancel

OK

Configurazione router adiacente BGP istanza 2 ISP 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		

Al termine, fare clic su Salva.



Salva modifiche

Per impostazione predefinita, BGP installa un solo percorso ottimale nella tabella di routing, anche se ECMP è configurato in tutte le VTI di Azure. È necessario abilitare BGP multipath separatamente in modo che entrambi i percorsi appresi vengano installati e utilizzati contemporaneamente.

Passaggio 9: Configurazione di eBGP Multipath

1) Selezionare Routing > BGP > IPv4, fare clic sulla scheda General (Generale), quindi sull'icona della matita accanto a Forward Packets Over Multiple Paths (Inoltra pacchetti su più percorsi).

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

Impostazione Inoltra pacchetti su più percorsi

2) Modificare il valore predefinito del campo Numero di percorsi da 1 a 4. Fare clic su OK.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Impostazione Cambia Pacchetti Di Inoltro Su Più Percorsi

3) Assicurarsi di salvare e distribuire le modifiche.

Verifica/Risoluzione dei problemi

Al termine della distribuzione, verificare che il processo BGP FTD stabilisca le adiacenze di router adiacenti con entrambe le istanze di Azure nei rispettivi tunnel, che le route vengano apprese, che le interfacce siano attive e che le connessioni di protocollo vengano restituite nella tabella delle connessioni.

Passare alla `system support diagnostic-cli` CLI FTD come fatto nella Fase 2, Fase 7.

1) Una volta implementati, i vicini BGP dovrebbero comparire e ricevere i prefissi.

```
<#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) Verificare che le route ricevute da Azure vengano visualizzate come route a percorsi multipli.

```
<#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) Controllare la popolazione della tabella di routing.

```
<#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) Controllare la tabella di connessione per le sessioni BGP.

<#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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).