

Configurare la VPN da sito a sito di Azure vWAN per proteggere il firewall

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Diagramma](#)

[Connettività vWAN con collegamento DIA singolo tra Azure e FTD \(bilanciamento del carico/ridondanza di Azure\)](#)

[Configurazione](#)

[Fase 1: Configurazione di Azure vWAN/Hub](#)

[Passaggio 1: Creazione di vWAN](#)

[Passaggio 2: Crea hub vWAN](#)

[Fase 2: Configurazione sito VPN vWAN di Azure](#)

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

[Passaggio 2: Configura parametri della VPN del sito di Azure vWAN](#)

[Passaggio 3: Scarica configurazione tunnel del sito di Azure vWAN](#)

[Fase 3: Configurazione FTD](#)

[Passaggio 1: Analizza configurazione VPN di Azure](#)

[Passaggio 2: Configura loopback](#)

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

[Passaggio 4: Configura connettività sicura in Azure](#)

[Passaggio 5: Verifica connettività iniziale ad Azure](#)

[Passaggio 6: Configura secondo tunnel all'endpoint Instance1 di Azure](#)

[Passaggio 7: Configura ECMP](#)

[Passaggio 8: Configura route statiche in IP privati dell'istanza](#)

[Passaggio 9: Configurare BGP](#)

[Passaggio 10: Configurazione di BGP Multi-path](#)

[Verifica](#)

[Altre considerazioni](#)

[Previsione AS-Path](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la configurazione della connettività VPN da sito a sito di Microsoft Azure Virtual WAN (vWAN) a Cisco Secure Firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

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

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

Microsoft Azure Virtual WAN (vWAN) combina diverse funzionalità di rete, sicurezza e routing di Azure dietro un singolo costruito Hub. Ogni hub vWAN può ospitare un gateway VPN da sito a sito gestito da Microsoft che i dispositivi remoti, ad esempio Secure Firewall, utilizzano per accedere ad Azure senza dover compilare e gestire l'infrastruttura del gateway.

A differenza di una VPN IPsec a due endpoint convenzionale, il gateway VPN da sito a sito di Azure vWAN viene distribuito come una coppia di istanze attive-attive (Instance0 e Instance1), ognuna con il proprio indirizzo IP pubblico e indirizzo peer BGP (Border Gateway Protocol). Per trarre vantaggio da entrambe le istanze per la ridondanza e il throughput aggiuntivo, la FTD di diramazione stabilisce un tunnel IP Security (IPsec) per ciascuna istanza e utilizza BGP, anziché il solo routing statico, per apprendere e ritirare dinamicamente le route quando le istanze diventano disponibili o non disponibili. Il routing ECMP (Equal-Cost Multi-Path) e il multipath BGP sull'FTD

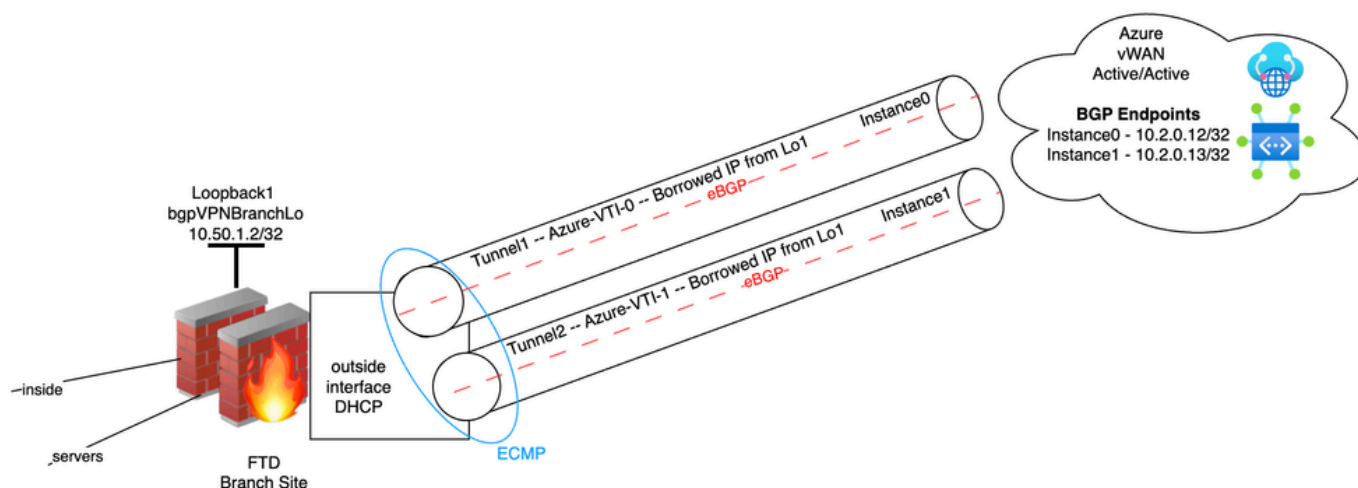
mantengono entrambi i tunnel attivi contemporaneamente, anziché considerarne uno come standby passivo.

Il presente documento configura tale progetto in tre fasi: Gli oggetti Hub vWAN di Azure e Sito VPN vengono creati per primi, i parametri di connessione risultanti vengono scaricati e quindi utilizzati per configurare le VTI (Virtual Tunnel Interfaces), i criteri IKEv2 (Internet Key Exchange versione 2)/IPsec corrispondenti, le route statiche, il protocollo ECMP e il peering BGP su FTD tramite FMC.

Diagramma

Il diagramma mostra la topologia della configurazione descritta in questo articolo. La variante DAS (Direct Internet Access) singola genera entrambi i tunnel di Azure da un'interfaccia esterna sull'FTD.

Connettività vWAN con collegamento DIA singolo tra Azure e FTD (bilanciamento del carico/ridondanza di Azure)



Configurazione

Completate le tre fasi in ordine. Gli oggetti del lato di Azure creati nelle fasi 1 e 2 producono gli indirizzi IP peer, i numeri del sistema autonomo BGP (AS) e la chiave già condivisa che la fase 3 applica all'FTD.

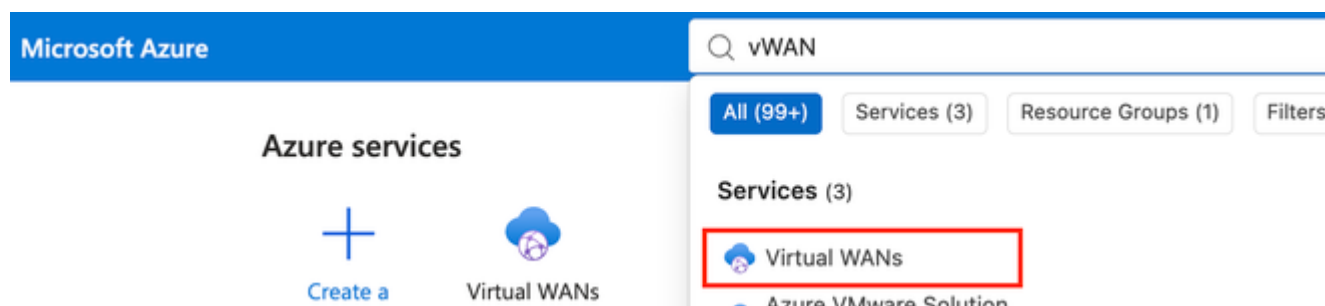
Fase 1: Configurazione di Azure vWAN/Hub



Nota: I passaggi di configurazione in questo documento sono di alto livello e forniscono i passaggi necessari per connettere FTD ad Azure vWAN. Per informazioni sul significato delle configurazioni, consultare la documentazione di Microsoft Azure vWAN. Vedere [Che cos'è Azure Virtual WAN?](#) e ulteriore documentazione.

Passaggio 1: Creazione di vWAN

a) Cercare vWAN nella casella di ricerca di Azure, fare clic su Virtual WAN.



b) Fare clic su + Crea.



c) Immettere un Nome per la nuova istanza vWAN, fare clic su Revisione + Crea, quindi fare clic su Crea nella pagina Revisione + Crea della procedura guidata.

Create WAN ...

Basics Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#) 

Project details

Subscription *

Resource group * [Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >



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

d) Fare clic su Vai alla risorsa.



VirtualWanDeployment | Overview

Deployment



Delete



Cancel



Redeploy



Download



Refresh



Overview



Inputs



Outputs



Template



Your deployment is complete



Deployment name : VirtualWanDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

Passaggio 2: Crea hub vWAN

a) Selezionare Connettività > Hub e fare clic su + Nuovo Hub.



CX-vWAN | Hubs



Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub	Hub status	Region
No results		

b) Per ulteriori informazioni sulla configurazione, consultare la documentazione di Azure. Verificare che lo spazio di indirizzi privato dell'hub allocato non si sovrapponga ad alcuno spazio di indirizzi interno. Configurare Nome, Hub virtuale, Preferenza routing hub. Fare clic su Avanti: Da sito a sito >.

Home > CX-vWAN | Hubs

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpsite). [Learn more](#)

Project details

The hub will be created under the same subscription and resource group as the vWAN. ⓘ

Subscription

Resource group

Virtual Hub Details

Region *

Name * ✓

Hub private address space * ⓘ ✓

Virtual hub capacity * ⓘ

Hub routing preference * ⓘ

Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next: Site to site >](#)

c) Per ulteriori informazioni sui campi presentati, consultare la documentazione dell'hub vWAN di Microsoft Azure. Selezionare Sì per creare un gateway VPN da sito a sito. Il numero BGP Autonomous System (AS) predefinito allocato è 65515, così come allocato da Internet Engineering Task Force (IETF) in Request For Comments (RFC) 6996 che definisce la prenotazione AS per uso privato.



Nota: Prendere nota di BGP AS per le future operazioni di configurazione sul FMC.

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

☒ Yes

☐ No

Copied

AS Number

65515

Gateway scale units

Routing preference

☒ Microsoft network ☐ Internet

Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

Next : Point to site >

Fare clic su Rivedi + crea oppure su Avanti: Scegliere sito > per configurare le impostazioni facoltative.

d) Una volta verificato il riepilogo, fare clic su Crea.



Nota: Come per Azure, la creazione dell'hub richiede 30 minuti.

Create virtual hub ...

 Validation passedBasics Site to site Point to site ExpressRoute Tags **Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region
Name CX-vWAN-Hub
Hub private address space 10.2.0.0/16
Virtual hub capacity
Hub routing preference

Site to site

Site to site (VPN gateway) Enabled
AS Number 65515
Gateway scale units

Point to site

Point to site (VPN gateway)

ExpressRoute

ExpressRoute gateway

Time

 Creating a hub with a gateway will take 30 minutes.**Create**

Previous

Next

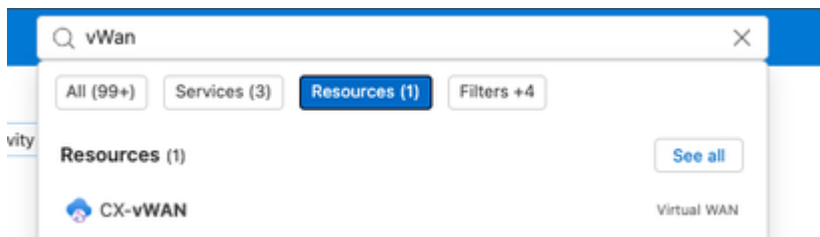
[Download a template for automation](#)

e) Al termine dell'installazione, cercare il nome della risorsa vWAN originale. Per limitare ulteriormente la ricerca, fare clic su Risorse.

 VirtualHubDeployment | Overview ...
Deployment    Delete  Cancel  Redeploy  Download  Refresh Overview Inputs Outputs Template Your deployment is complete

 Deployment name : VirtualHubDeployment
Subscription :
Resource group :

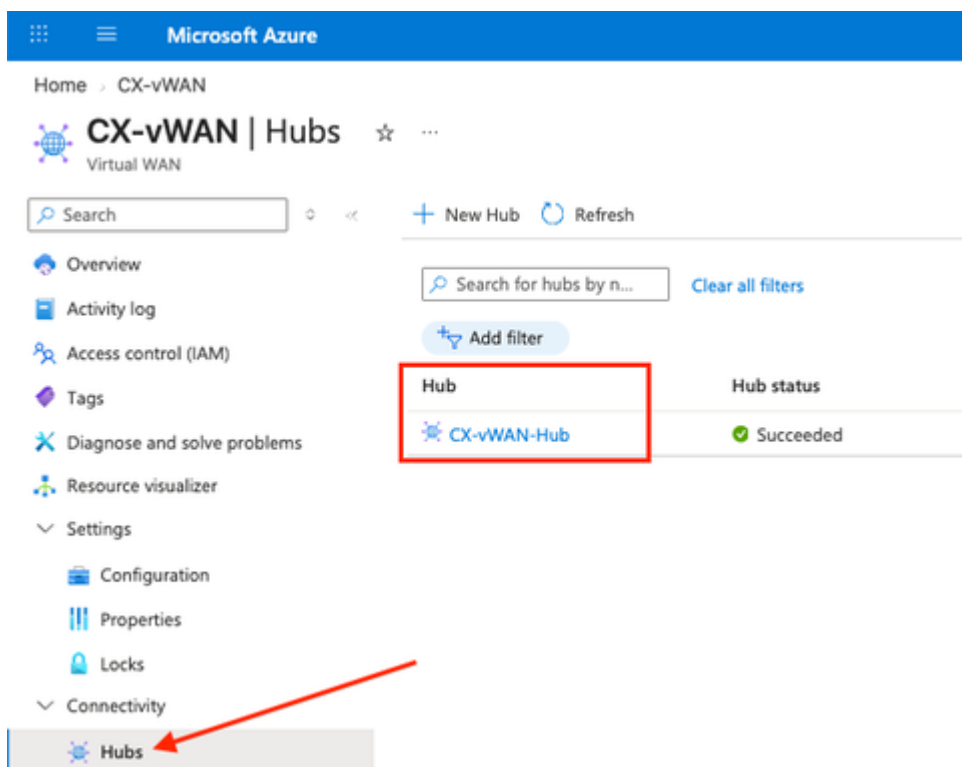
 Deployment details Next steps[Go to resource](#)



Fase 2: Configurazione sito VPN vWAN di Azure

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

a) Accedere al mozzo creato selezionando Connettività > Hub e fare clic sul mozzo creato nei passi precedenti.



b) 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		

c) 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 *

Device vendor *

Private address space

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

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

Previous

Next : Links >

d) Inserire le informazioni richieste sul collegamento. L'indirizzo BGP del collegamento e i campi ASN del collegamento riflettono l'indirizzo di destinazione BGP Layer 3 del tunnel interno e il numero BGP AS sul sito di succursale con cui si è formata la relazione di vicinanza con Azure 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 hub configurata in precedenza, che Azure installa come route /32 per raggiungere come router BGP adiacente. L'indirizzo IP/FQDN del collegamento è l'indirizzo IP di destinazione del layer 3 esterno del traffico diretto al sito della filiale necessario per il provisioning della connettività IPsec/IKEv2.



Nota: Se si utilizzano indirizzi compresi tra 169.254.21.0 e 169.254.22.255 per gli indirizzi del tunnel, verificare [come configurare BGP per Azure VPN Gateway](#) per i requisiti specifici.

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

Link name	Link speed	Link provider name	Link IP address / FQDN	Link BGP address	Link ASN	
single-dia-link ✓	1000 ✓	provider ✓	✓	10.50.1.2 ✓	65500 ✓	...

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

Previous

Next : Review + create >

e) Dopo aver verificato la correttezza delle impostazioni, 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

Name

VPN-Site

Device vendor

Cisco

Private address space

Links

Link name	single-dia-link
Link provider name	provider
Link speed	1000
Link IP address / FQDN	
Link ASN	65500
Link BGP address	169.254.10.2

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

Create

Previous

Next

f) Al termine dell'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](#)

Search vWan

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

Resources (1) [See all](#)

 **CX-vWAN** Virtual WAN

Passaggio 2: Configura parametri della VPN del sito di Azure vWAN

a) Accedere al mozzo creato selezionando Connettività > Hub e fare clic sul mozzo creato nei passi precedenti.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

b) Passare nuovamente a Connettività > VPN (da sito a sito) e fare clic sulla X per cancellare l'Associazione hub: Filtro connesso per visualizzare i siti disconnessi.

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

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

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

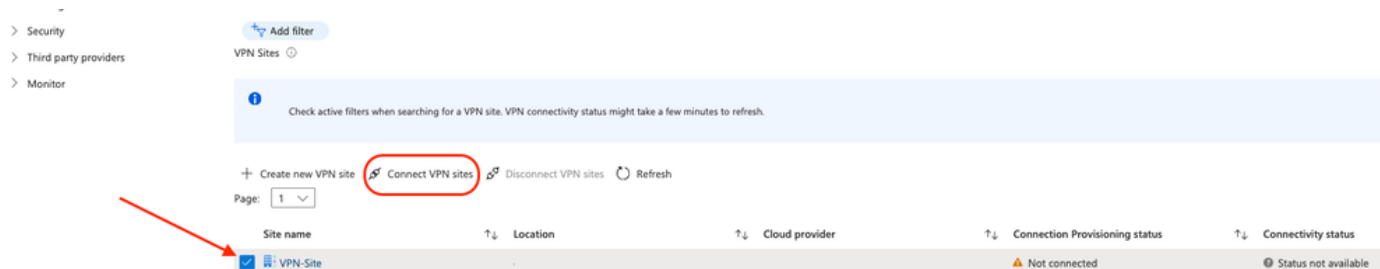
Search this page Clear all filters

Hub association : **Connected** X Add filter

VPN Sites ⓘ

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

c) Selezionare la casella accanto al sito VPN configurato in precedenza, quindi fare clic su Connetti siti VPN, che viene abilitato dopo la selezione del sito.



d) Viene visualizzato il pannello del cassetto laterale Connect sites. Immettere una chiave già condivisa (PSK) e configurare le impostazioni IPsec di fase 1 desiderate per IKEv2 e fase 2. Quando si sceglie Personalizzato dall'elenco a discesa IPsec, i valori vengono popolati automaticamente; annotare questi valori, poiché devono corrispondere sull'FTD. È inoltre necessario scegliere se si desidera utilizzare la funzionalità PFS (Perfect Forward Secrecy). Poiché si tratta di un tunnel basato su routing, configurare le impostazioni di conseguenza. Al termine, fare clic su Connect (Connetti) per salvare la configurazione.



Nota: Per ulteriori informazioni, vedere [Azure vWAN con criteri IPsec predefiniti e personalizzati](#).

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

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

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup24

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

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

Site name



Region



VPN-Site

eastus

Connect

e) Vengono visualizzate informazioni indicanti che il gateway è in fase di aggiornamento, insieme al tempo stimato per il completamento.

Home > CX-vWAN | Hubs > CX-vWAN-Hub



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

Virtual HUB

Search



Download VPN Config



Packet Capture



Delete gateway



Reset gateway



Monitor Gateway

Overview

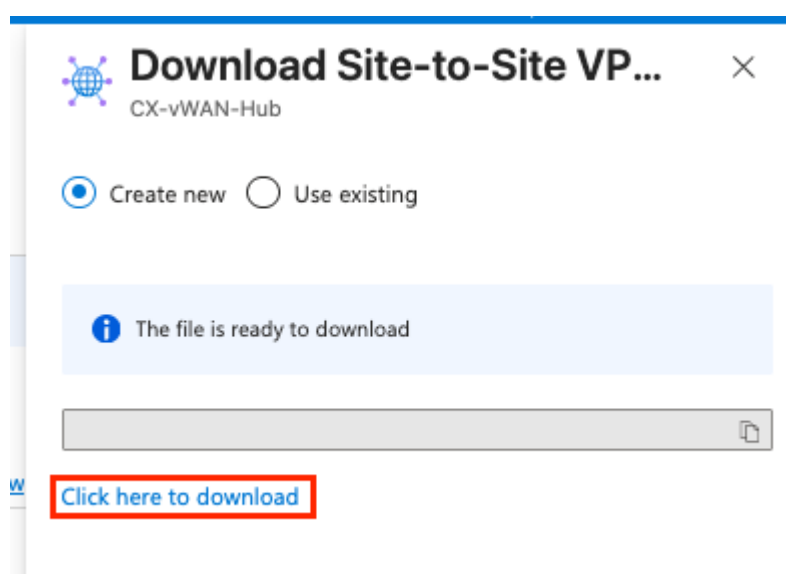
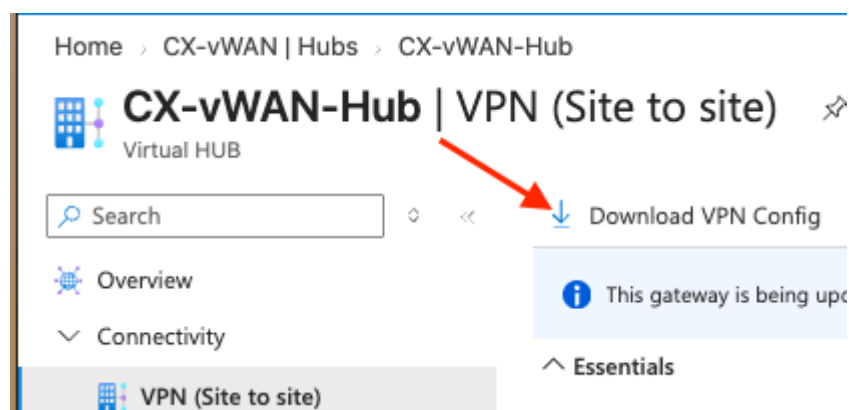
Connectivity



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

Passaggio 3: Scarica configurazione tunnel del sito di Azure vWAN

a) Durante l'aggiornamento del gateway, è possibile scaricare la configurazione VPN.



Con il sito VPN creato e i relativi parametri di connessione (indirizzi peer, numeri BGP AS e PSK) scaricati, gli stessi valori vengono utilizzati per configurare gli elementi corrispondenti sull'FTD nella fase 3.

Fase 3: Configurazione FTD

Passaggio 1: Analizza configurazione VPN di Azure

a) Aprire il file di configurazione VPN scaricato da Azure. Ha un aspetto simile all'output condensato mostrato e fornisce informazioni utili:



Nota: Per una messa a fuoco avanzata, diversi oggetti irrilevanti e coppie chiave/valore

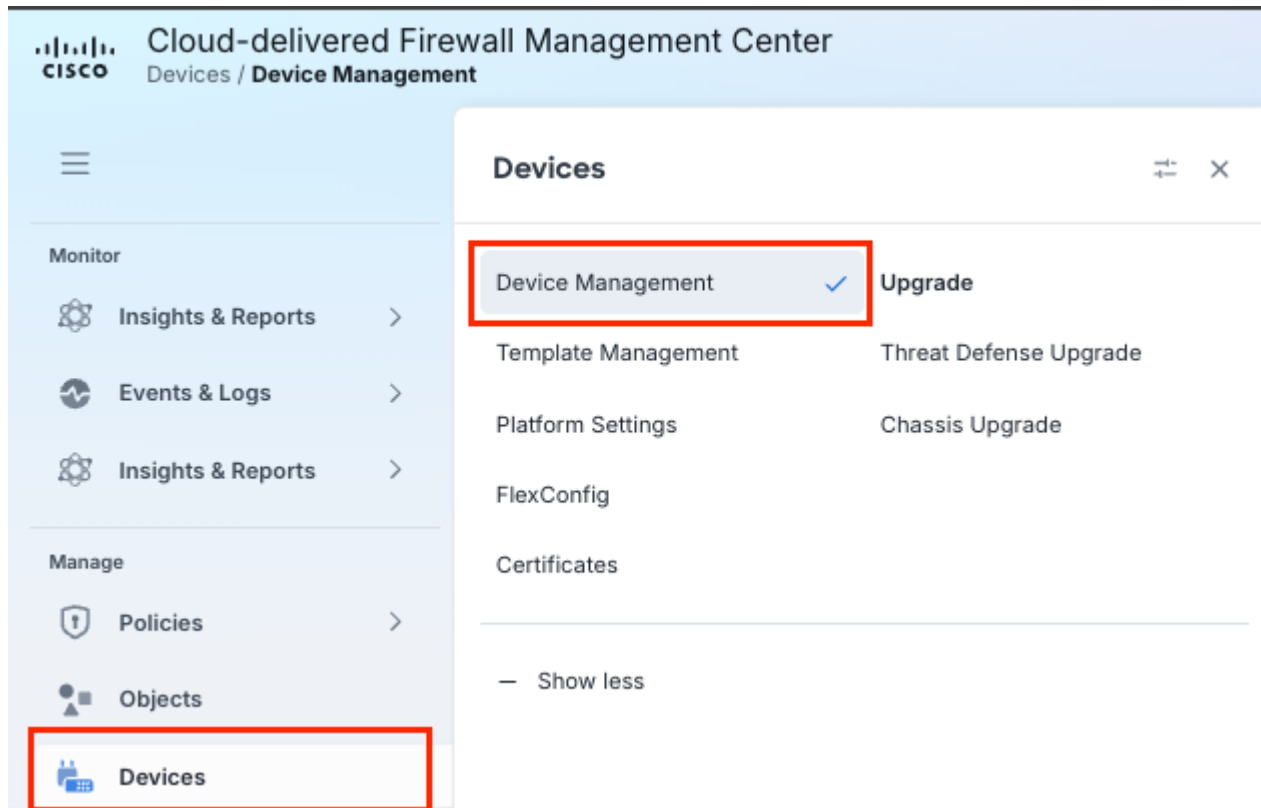
vengono potati per brevità.

```
[
{
  "configurationVersion": {
    "LastUpdatedTime": "<Last Update Time>",
    "Version": "<Version UUID>"
  },
  "vpnSiteConfiguration": {
    "Name": "VPN-Site",
    "IPAddress": "<FTD public IP address>",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "Region": "<Azure Region>"
      },
      "gatewayConfiguration": {
        "IpAddresses": {
          "Instance0": "57.x.x.x",
          "Instance1": "52.x.x.x"
        },
        "BgpSetting": {
          "Asn": 65515,
          "BgpPeeringAddresses": {
            "Instance0": "10.2.0.12",
            "Instance1": "10.2.0.13"
          }
        }
      }
    },
    {
      "connectionConfiguration": {
        "IsBgpEnabled": true,
        "PSK": "<IPSec PSK>",
        "IPsecParameters": {
          "IpssecEncryption": "GCMAES256",
          "IpssecIntegrity": "GCMAES256",
          "IkeEncryption": "GCMAES256",
          "IkeIntegrity": "SHA384",
          "PfsGroup": "None",
          "DhGroup": "DHGroup14",
          "SADataSizeInKilobytes": 0,
          "SALifeTimeInSeconds": 27000
        }
      }
    }
  ]
}
]
```

Passaggio 2: Configura loopback

Ogni VTI configurata successivamente richiede un'origine del tunnel stabile, quindi viene prima configurata un'interfaccia di loopback che viene condivisa tra entrambe le VTI.

a) Selezionare Dispositivi > Gestione dispositivi.

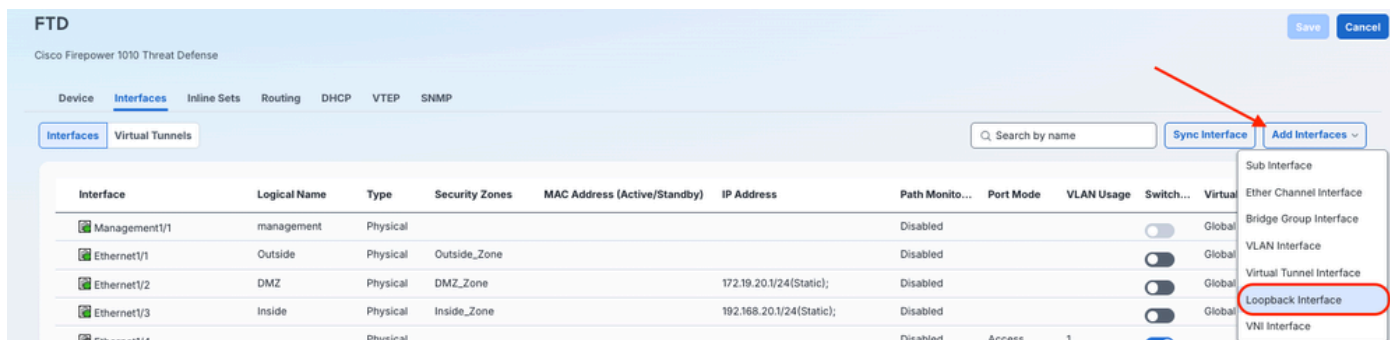


Nota: Questa esercitazione utilizza un centro di gestione dei firewall (cdFMC) distribuito su cloud; tuttavia, i passaggi restano gli stessi per i CCP locali.

b) Selezionare l'FTD che si sta configurando come dispositivo VPN per filiale/sito.

☐	 FTD N/A - ROUTED	10.0.0	Firepower 1010 Threat Defense
--------------------------	--	--------	-------------------------------

c) Fare clic sul menu a discesa Add Interfaces, quindi fare clic su Loopback Interface (Interfaccia loopback).



d) Fornire all'interfaccia di loopback il nome, l'ID e la descrizione, se necessario. Fare clic su IPv4.

e) Verificare che il tipo di IP sia definito come Use Static IP, immettere il collegamento BGP Address in base alla configurazione della fase 2, fase 1d. È possibile fare riferimento al valore definito in precedenza nel file JSON di configurazione della VPN scaricato

in `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress`



Nota: Definire l'indirizzo con una maschera /32 e all'interno dello spazio degli indirizzi RFC 1918.

Add Loopback Interface

General **IPv4** IPv6

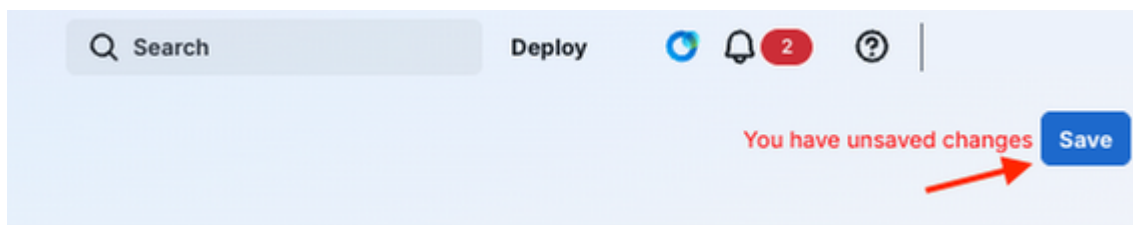
IP Type:
Use Static IP

IP Address:
10.50.1.2/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel OK

f) Fare clic su Salva



Passaggio 3: Configura oggetti criteri Fase 1/Fase 2

a) Per configurare la configurazione IKEv2/IPsec corrispondente sul FMC da applicare alle topologie VPN FTD, selezionare Gestisci > Oggetti, scorrere verso il basso il menu a sinistra per VPN, quindi espandere il sottomenu. Configurare il criterio IKEv2 fase 1 scegliendo Criterio IKEv2 dal menu e facendo clic su Aggiungi criterio IKEv2.

IKEv2 Policy

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

[Add IKEv2 Policy](#)

Name	
AES-GCM-NUL-SSH	☐ ☐
AES-GCM-NUL-SSH-LATEST	☐ ☐
AES-SSH-SSH	☐ ☐
AES-SSH-SSH-LATEST	☐ ☐
DES-SSH-SSH	☐ ☐
DES-SSH-SSH-LATEST	☐ ☐
Umbrella-AES-GCM-256	☐ ☐

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

b) Inserire un nome per il nuovo criterio IKEv2, scegliere Priorità e/o Durata. Verificare che il criterio corrisponda su entrambe le estremità del tunnel per quanto riguarda Integrità, Crittografia, PRF, e Gruppo Diffie-Hellman (DH). Scegliere gli elementi dell'algoritmo/gruppo allineati che devono corrispondere alla configurazione di Azure, quindi 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

Available Algorithms

- MD5
- SHA
- SHA512
-
- SHA384
- NULL

Selected Algorithms

- SHA256

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

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

Edit IKEv2 Policy



Name:*

Azure_IKEv2

Description:

Priority:*

(1-65535)

5

Lifetime:

seconds (120-2147483647)

3600

Available Groups

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

1

2

5

14

15

16

19

20

...

Add

Selected Groups

14



Cancel

Save

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

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

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



Nota: È possibile fare riferimento a questi valori all'interno del file di configurazione scaricato in `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256

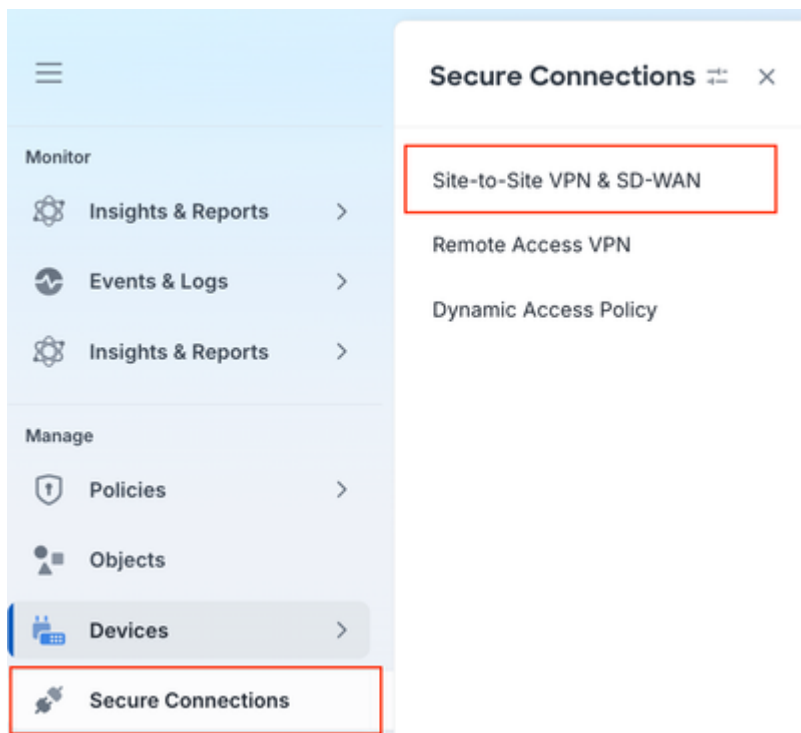


Cancel

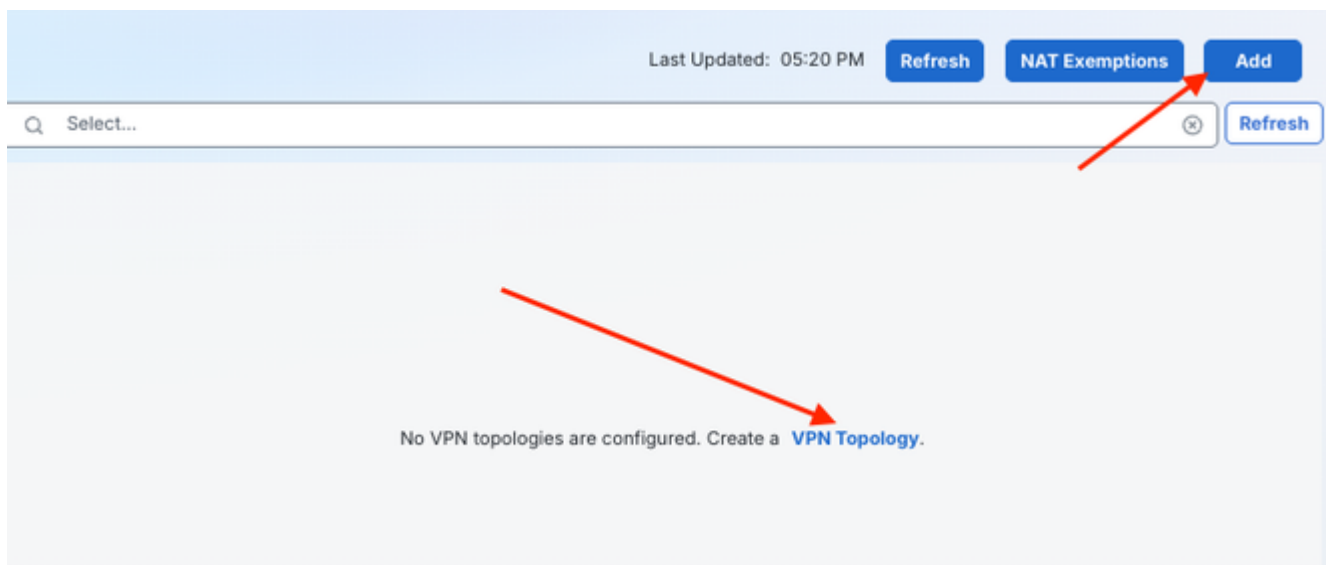
Save

Passaggio 4: Configura connettività sicura in Azure

a) Selezionare Gestisci > Connessioni sicure > VPN da sito a sito e SD-WAN.



b) Fare clic sul collegamento ipertestuale iniziale VPN Topology configuration al centro o fare clic su Add.



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

Create VPN Topology

Topology name *

Azure-VTI-Instance0

VPN Type

☐ SD-WAN Topology

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

Select VPN Topology

☐ Hub and Spoke

Prerequisites

☒ **Route-Based VPN**

Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ **Peer to Peer**

☐ Policy-Based VPN

Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

☐ SASE Topology

Warning: SASE topology cannot be selected because Secure Access and Umbrella are not configured.

[Prerequisites](#)

[Refresh](#)

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

d) Per il nodo A, fare clic sull'elenco a discesa Device (Dispositivo) e scegliere il nome della coppia HA FTD/FTD gestita su cui distribuire la configurazione. Per il nodo B, poiché si tratta dell'estremità remota della connessione nella topologia che termina sulle istanze di Azure vWAN, scegliere Extranet dall'elenco a discesa Device. Quindi, per il nodo A, fare clic sull'icona + accanto all'elenco a discesa VTI (Virtual Tunnel Interface).

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

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

IKE Version:*

☐ IKEv1 ☒ **IKEv2**

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

Node A

Device:*

FTD

Virtual Tunnel Interface:*

+

☐ Tunnel Source IP is Private [Edit VTI](#)

☐ Send Local Identity to Peers

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

[> Advanced Settings](#)

Node B

Device:*

Extranet

Device Name*:

Endpoint IP Address*:

Primary IP*, [Backup Peer IPs]

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

e) Assegnare un nome alla prima VTI e verificare che sia attivata. Assegnare un'area di sicurezza nuova o esistente alla VTI, assegnare l'origine del tunnel e scegliere l'indirizzo IP dall'elenco a discesa adiacente.

Add Virtual Tunnel Interface ?

Tunnel Type
☒ Static ☐ Dynamic

Name:*

☒ Enabled

Description:

Security Zone:

Priority:
 (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:*
 (0 - 10413)

Tunnel Source:*

f) Quindi, accertarsi che il pulsante di opzione Borrow IP (IP senza numero) sia selezionato, quindi scegliere lo stesso loopback dall'elenco a discesa a destra. Fare clic su OK una volta completato.

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

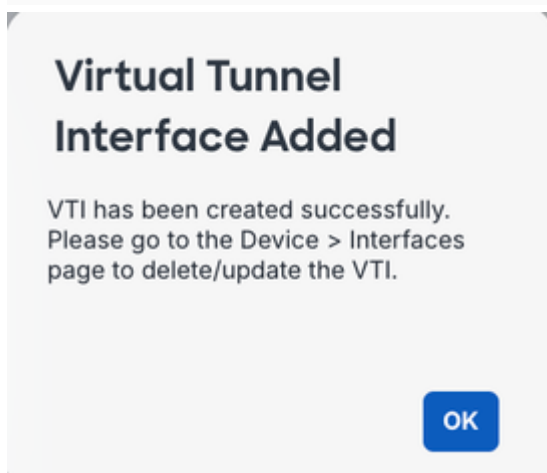
Tunnel ID:*
 (0 - 10413)

Tunnel Source:*

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

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

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



g) Dopo aver configurato e applicato la VTI, popolare manualmente l'indirizzo IP di origine del tunnel (che viene popolato automaticamente se l'indirizzo dell'interfaccia padre viene popolato da DHCP) e verificare che il nome del dispositivo Nodo B sia configurato, nonché l'indirizzo IP dell'endpoint dell'istanza. Al termine, fare clic sulla scheda IKE.



Nota: È possibile fare riferimento al valore Instance0 Endpoint IP Address nel file di configurazione scaricato in `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0`

Edit VPN Topology ?

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:* ?

☐ Send Local Identity to Peers

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

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

h) Scorrere verso il basso fino a Impostazioni IKEv2 e verificare che Tipo di autenticazione sia impostato su Chiave manuale precondivisa, quindi immettere la chiave PSK configurata in Azure nei passaggi precedenti. Configurare i criteri IKEv2 fase 1 facendo clic sull'icona a forma di matita per modificare i criteri IKEv2 disponibili.



Nota: 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:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

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

IKEv2 Settings

Policies:* 

Authentication Type:

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

i) Aggiungere il criterio IKEv2 fase 1 configurato inizialmente nel passaggio 3.

IKEv2 Policy



Available IKEv2 Policy



Search

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

Add

Selected IKEv2 Policy

Azure_IKEv2

Cancel

OK

j) Selezionare la scheda IPsec.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐

IKEv1

☒

IKEv2

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Azure_IKEv2

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐

Enforce hex-based pre-shared key only

k) Modificare la proposta IPsec IKEv2 in Insiemi di trasformazioni facendo clic sull'icona della matita.

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

l) Fare clic sull'icona Cestino per rimuovere il set di trasformazioni AES-GCM predefinito e aggiungere la proposta IPsec Azure_IPsec personalizzata creata nella seconda metà del passaggio 3. Fare clic su OK.

IKEv2 IPsec Proposal



Available Transform Sets  +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec 

Cancel

OK

m) Scorrere verso il basso e immettere 27000 per la durata corrispondente ai parametri di Azure. Abilitare Gruppo PFS, se applicabile. Fare clic su Save (Salva).



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

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

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

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Lifetime Duration*: 27000 Seconds (Range 120-2147483647)

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

> ESPv3 Settings

Cancel Save

n) Distribuire le modifiche.

Search Deploy

Search Device Advanced Deploy Deploy All

FTD

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

o) Al termine dell'installazione, selezionare Gestione > Connessioni sicure > VPN da sito a sito e SD-WAN in Distribuzione dello stato del tunnel; il successo della connettività si traduce in una riduzione dei costi (verso l'alto).

Last Updated: 11:11 PM Refresh NAT Exemptions Add					
Q Select... Refresh					
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✎ ✕

Con il primo tunnel implementato, verificare che venga stabilito correttamente sui livelli IKE/IPsec e BGP prima di configurare il secondo tunnel per la ridondanza.

Passaggio 5: Verifica connettività iniziale ad Azure

a) SSH nell'FTD e immettere `system support diagnostic-cli`, digitare `en` e premere Invio, in quanto non è presente alcuna password nella CLI FTD di sola lettura.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftd>
```

```
en
```

```
Password:
```

```
ftd#
```

b) Controllare lo stato del tunnel per la fase 1/fase 2.

```
<#root>
```

```
ftd#
```

```
show crypto isakmp sa | i Status:
```

```
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show crypto ipsec sa | i State|spi
```

```
current outbound spi: 5E83023A
```

```
current inbound spi : 62BC7C9E
```

```
spi: 0x62BC7C9E (0x00010B45)
```

```
SA State: active
```

```
spi: 0x5E83023A (0x0002029B)
```

```
SA State: active
```

```
ftd#
```

c) Eseguire le acquisizioni per controllare i pacchetti TCP (Transmission Control Protocol) BGP ricevuti da Azure nel tunnel e il traffico della porta NAT-T (Network Address Translation - Traversal) UDP (User Datagram Protocol) 4500/UDP 500 sull'acquisizione esterna dall'IP pubblico del tunnel di Azure Instance-0.

```
<#root>
```

```
ftd#
```

```
capture out-instance-0 trace interface Outside match ip host <Azure-instance0-IP> any
```

```
ftd#
```

```
capture tun-vti-0 interface Azure-VTI-0 trace match ip host <Link BGP IP> any
```

```
ftd#
```

```
show cap tun-vti-0
```

```
3 packets captured
```

```
1: 03:23:43.510074      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240 <ms
2: 03:23:44.511204      10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240 <ms
3: 03:23:46.512211      10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240 <mss
ftd#
```

Con la connettività a Instance0 confermata, ripetere la stessa configurazione della topologia VTI e VPN per Instance1 in modo che entrambe le istanze del gateway di Azure siano raggiungibili.

Passaggio 6: Configura secondo tunnel all'endpoint Instance1 di Azure

a) Creare un secondo VTI (Azure-VTI-1) che prende in prestito dallo stesso loopback (Fase 3 b-f).

Virtual Tunnel Interface Details

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

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

Ethernet1/1 (Outside)

Dynamic

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

☒ IPv4

☐ IPv6

IP Address:*

☐ Configure IP

☒ Borrow IP (IP unnumbered)

Loopback1 (bgpVPNBranchLo)



VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

b) Configurare la topologia VPN della seconda istanza (passo 4 g-n).



Nota: È possibile fare riferimento al valore dell'indirizzo IP dell'endpoint Instance1 nel file di configurazione scaricato in `vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*

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

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

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

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

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

c) Implementare le modifiche alla configurazione e controllare lo stato del tunnel.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	
> Azure-VTI-Instance1	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	

d) Il controllo in Azure comporta la cessione di Instance0 e Instance1 Connected.

Links

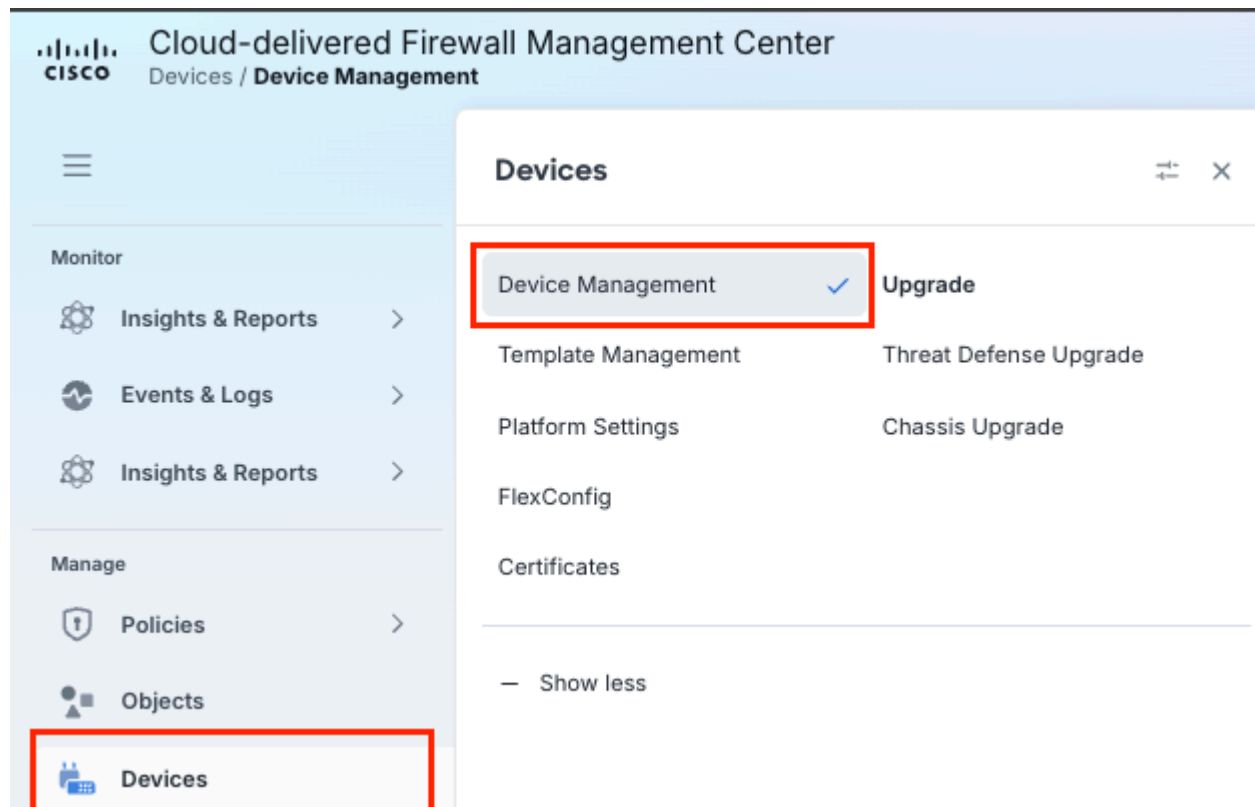
☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Con entrambi i tunnel attivi, l'FTD richiede il routing ECMP in modo che il traffico possa usare entrambi i percorsi contemporaneamente, anziché trattare il secondo tunnel come standby

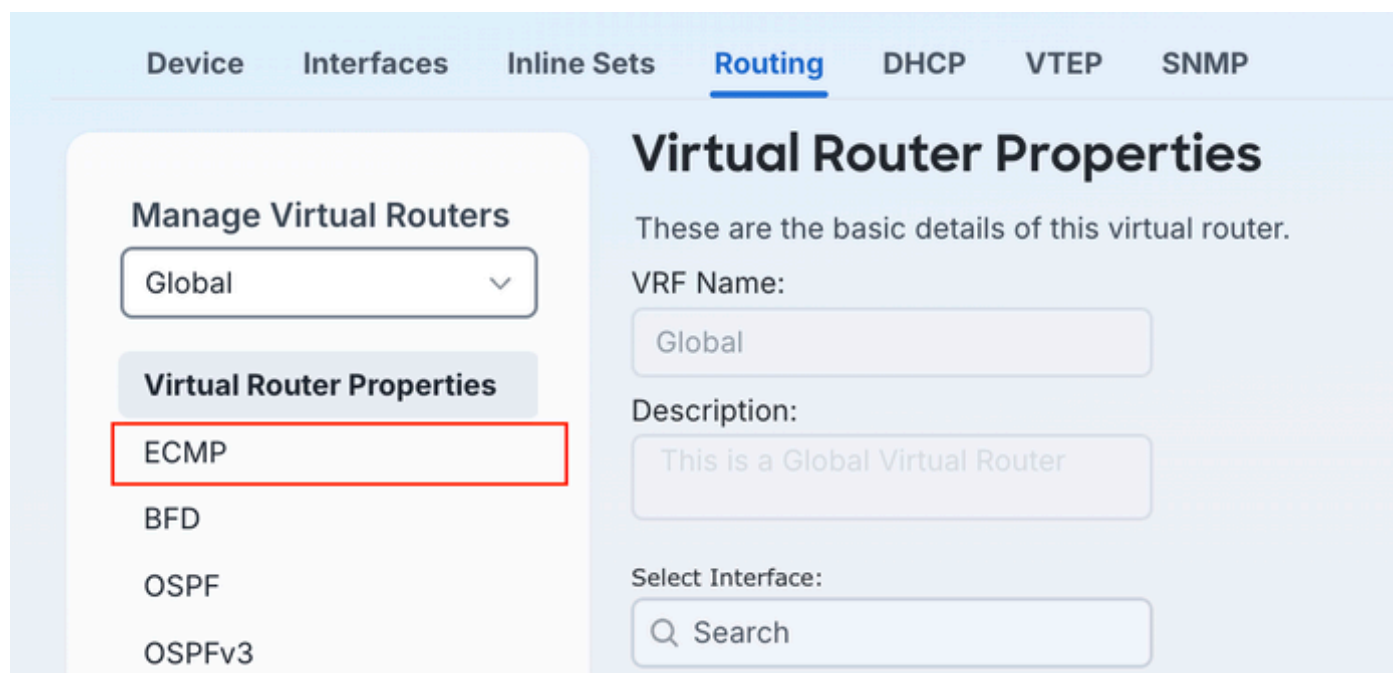
passivo.

Passaggio 7: Configura ECMP

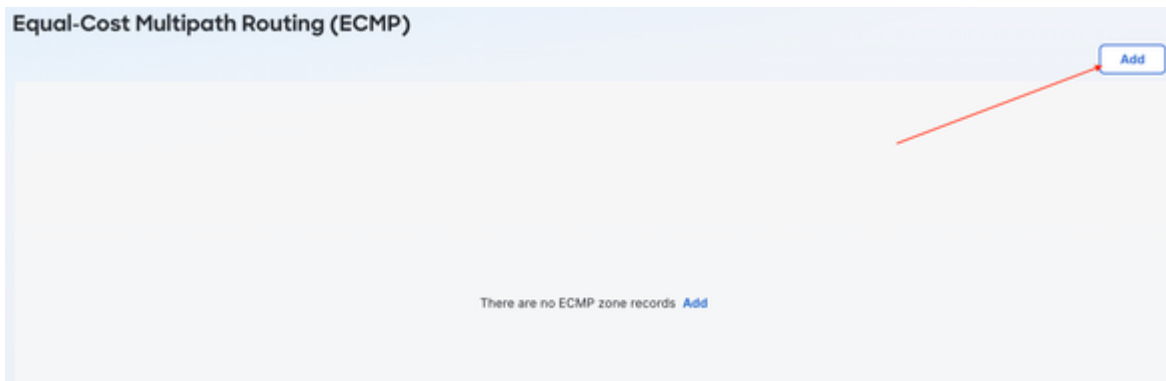
a) Passare a Gestisci > Dispositivi > Gestione dispositivi e selezionare l'FTD configurato con le VPN per Azure.



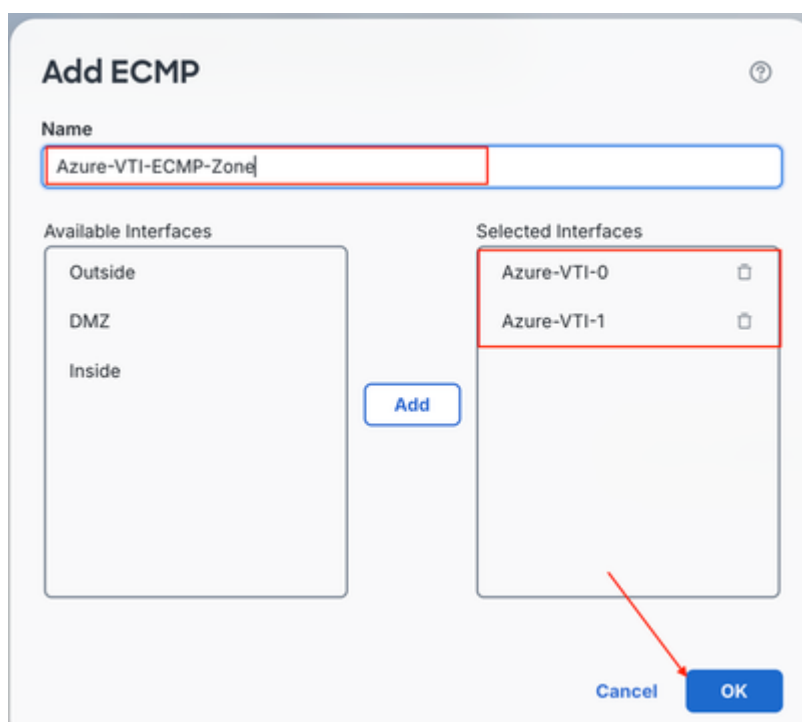
b) Fare clic sulla scheda Instradamento e scegliere ECMP.



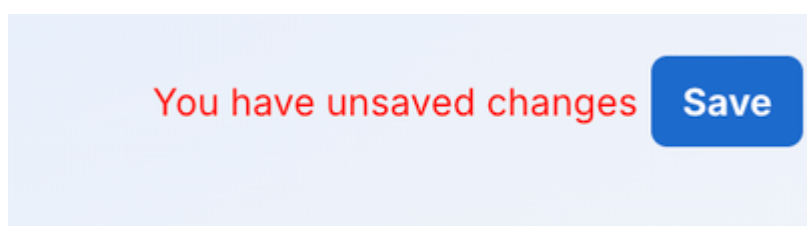
c) Fare clic su Add per creare una nuova zona ECMP.



d) Attivare o disattivare l'evidenziazione delle VTI facendo clic su entrambe le VTI nel pannello Interfacce disponibili e fare clic su Aggiungi per applicare le VTI alla zona ECMP indicata.



e) Dopo aver verificato la correttezza delle impostazioni, fare clic su Save (Salva).

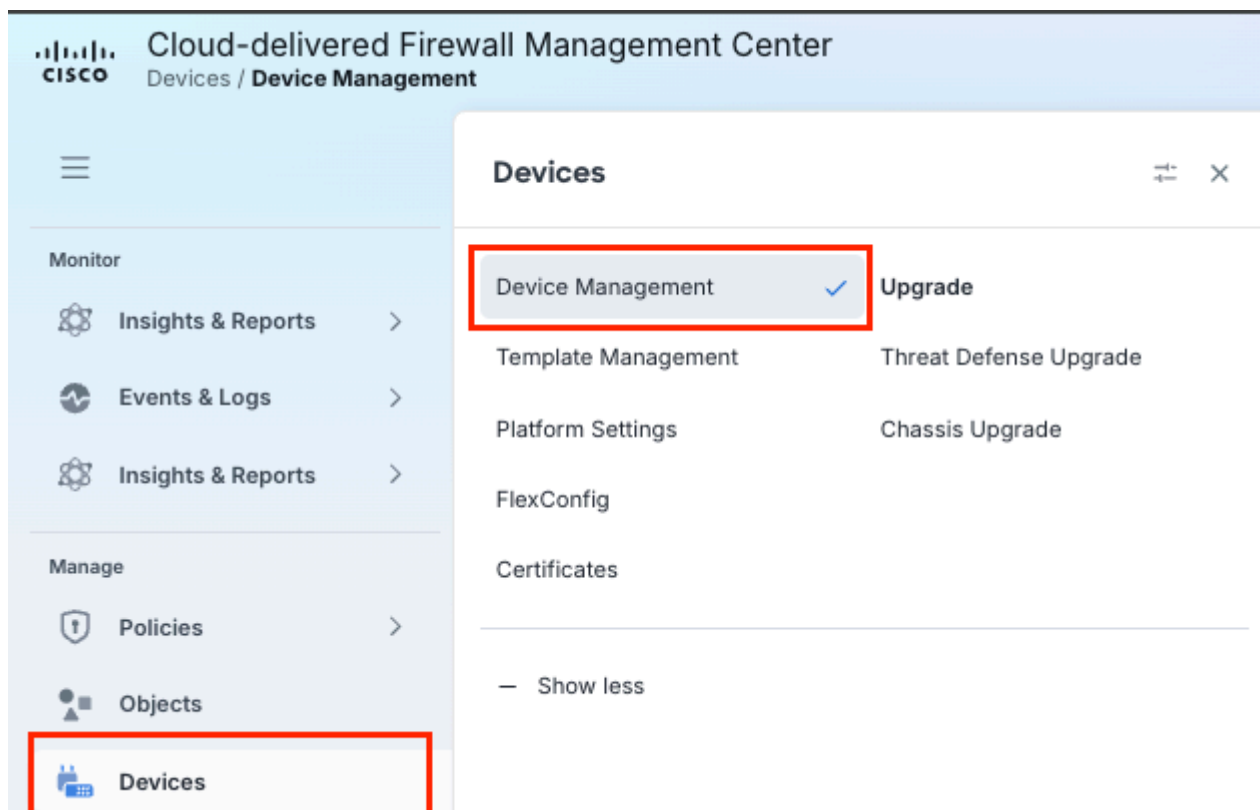


Passaggio 8: Configura route statiche in IP privati dell'istanza

BGP richiede route per la connessione ai router adiacenti e, poiché gli endpoint non sono connessi direttamente, per impostazione predefinita non vengono popolate route. ECMP consente di configurare route statiche con la stessa metrica (Distanza amministrativa) per la stessa destinazione, in modo che entrambe le route vengano installate nella base RIB (Routing Information Base) e utilizzate contemporaneamente.

a) Selezionare Gestisci > Dispositivi > Gestione dispositivi e scegliere il dispositivo FTD

applicabile.



b) Selezionare Ciclo > Ciclo statico.

c) Fare clic su + Aggiungi instradamento.

d) Aggiungere le route per entrambi gli indirizzi IP dell'istanza creando la prima route alla VT Instance0 e aggiungere l'oggetto di rete di destinazione per esso facendo clic sul segno + accanto a Rete disponibile. Quindi, fare clic sull'oggetto di rete dalla lista e fare clic sul pulsante Aggiungi per aggiungerlo come destinazione della route statica. Assicurarsi di scegliere l'IP Instance0 e che sia impostato come Gateway. Al termine, fare clic su OK.



Nota: I valori statici della rete di destinazione della route si trovano sotto `vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance0` e

vpnSiteConnections[0].BgpSetting.BgpPeeringAddresses.Instance1 nel file di configurazione scaricato.

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*:

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

Available Network +

Selected Network

Azure-Instance0-BGP_Peer

Azure-Instance1-BGP_Peer

Ensure that egress virtualrouter has route to that destination

Gateway: +

Metric: (1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

Cancel OK

e) Ripetere le fasi c-d per aggiungere la seconda route statica tramite la VTI di Instance1. Accertarsi di fare clic su Salva per salvare le modifiche.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
Azure-Instance1-BGP_Peer	Azure-VTI-1	Global	Azure-Instance1-BGP_Peer (10.2.0.13)	false	1	
Azure-Instance0-BGP_Peer	Azure-VTI-0	Global	Azure-Instance0-BGP_Peer (10.2.0.12)	false	1	
IPv6 Routes						

Le route statiche raggiungono solo gli indirizzi di peering BGP; Lo stesso BGP deve essere ancora abilitato e sottoposto a peer in modo che Azure e l'FTD si instradino dinamicamente l'uno verso l'altro o da reti più grandi.

Passaggio 9: Configurare BGP

a) Abilitare il processo BGP 65500 su FTD in Routing > General Settings > BGP. Selezionare la casella di controllo Abilita BGP e immettere il numero AS configurato in precedenza in Fase 2, Fase 1. Passare a Routing > BGP > IPv4.

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id
Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

b) Abilitare il routing BGP IPv4 per il processo/AS 65500 selezionando la casella di controllo Enable IPv4 adiacente e fare clic su Adiacente per configurare i router adiacenti BGP.

FTD
Cisco Firepower 1010 Threat Defense

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

Enable IPv4: ☒ AS Number 65500

Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3

General **Neighbor** Add Aggregate Address Filtering Networks Redis

Setting
Learned Route Map

c) Fare clic su + Aggiungi.

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

+ Add

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
No records to display				

d) Immettere le informazioni sul peering Instance0 BGP, fare riferimento al BGP AS annotato dall'hub vWAN e immetterlo come Neighbor Remote AS, quindi aggiungere una descrizione se desiderato. Fare clic su Avanzate.



Importante: Accertarsi di modificare l'origine aggiornamento BGP in modo che faccia riferimento all'elemento padre di loopback di entrambe le interfacce VTI sull'FTD.

Add Neighbor

IP Address*
10.2.0.12

Remote AS*
65515
(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover
none

Description
Instance0 Azure BGP Peering

Update Source:
bgpVPNBranchLo

Filtering Routes Routes Timers **Advanced** Migration

e) Nel menu Advanced (Avanzate) della configurazione BGP Neighbor su FTD, è possibile modificare il numero di hop TTL 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.

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Ripetere gli stessi passaggi per Azure Instance1 BGP Peer.

Add Neighbor ?

IP Address*
10.2.0.13

Remote AS*
65515
(1-4294967295 or 1.0-65535.65535)

BFD Fallover
none

Update Source:
bgpVPNBranchLo

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description
Instance1 Azure BGP Peering

Filtering Routes Routes Timers **Advanced** Migration

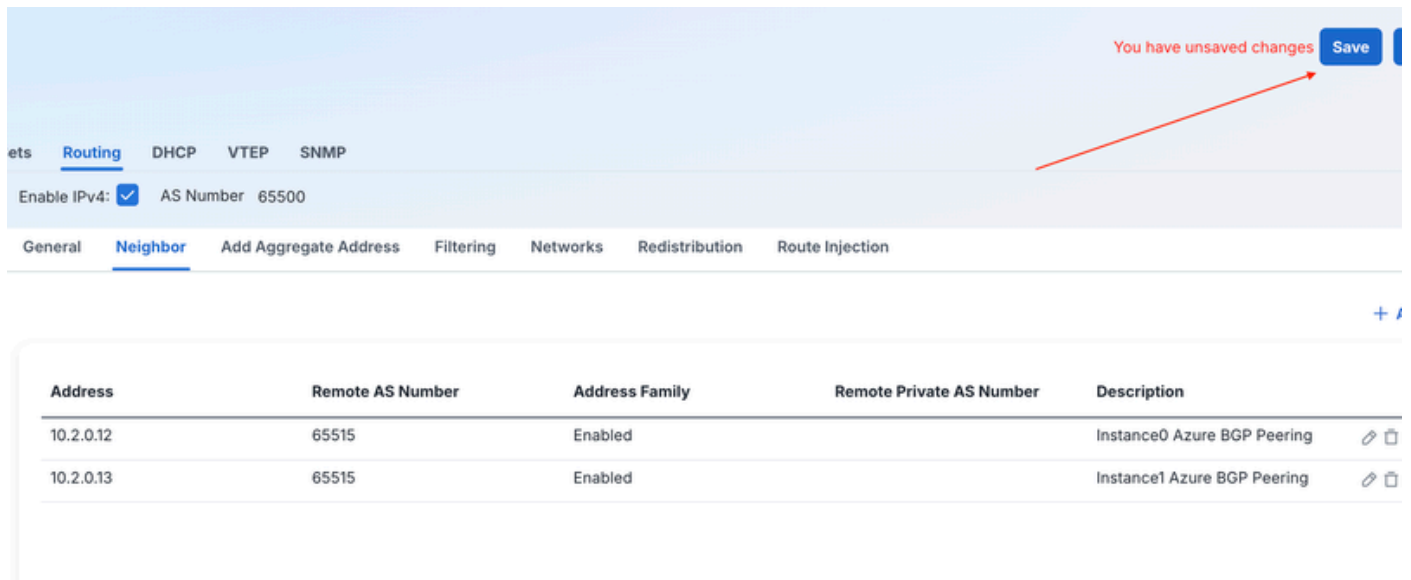
☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50
(1-255)

g) Salvare le modifiche una volta completate.



Per impostazione predefinita, BGP installa solo un singolo percorso ottimale nella tabella di routing, anche se in ECMP sono disponibili entrambe le route statiche. È necessario abilitare BGP multipath separatamente in modo che entrambi i percorsi appresi vengano installati e utilizzati contemporaneamente.

Passaggio 10: Configurazione di BGP Multi-path

a) Selezionare Routing > BGP > IPv4, fare clic sulla scheda General (Generale), quindi fare clic sull'icona a forma di matita accanto a Forward Packets Over Multiple Paths (Pacchetti inoltrati su percorsi multipli).

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

Enable IPv4: ☒ AS Number 65500

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

IPv6

Static Route

▼ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

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

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

b) Modificare il valore predefinito del campo Numero di percorsi da 1 a 2.

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

c) Assicurarsi di salvare e distribuire le modifiche.

Verifica

Al termine della distribuzione, verificare che il modulo BGP formi adiacenze con entrambe le istanze di Azure. Successivamente confermare che le route vengono apprese su entrambi i tunnel e che il traffico utilizza entrambe le VTI, utilizzando lo stesso accesso CLI diagnostico stabilito nella fase 3, fase 5.

Passare alla `system support diagnostic-cli` CLI FTD.

a) Una volta installati, 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#
```

```
show bgp summary
```

```
BGP router identifier 10.50.1.2, local AS number 65500
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
2 multipath network entries and 4 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 952 total bytes of memory
BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.2.0.12	4	65515	5	3	5	0	0	00:01:02	2
10.2.0.13	4	65515	3	4	5	0	0	00:00:55	2

```
ftd#
```

b) Verificare che le route ricevute da Azure siano visualizzate come route a percorsi multipli.

```
<#root>
```

```
ftd#
```

```
show bgp
```

```
BGP table version is 7, local router ID is 10.50.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	10.2.0.12			0	65515 i
*>	10.2.0.13			0	65515 i

```
*m 172.27.0.0      10.2.0.12      0 65515 i
*>                10.2.0.13      0 65515 i
ftd#
```

c) Controllare il numero di pacchetti VTI.

```
<#root>
```

```
ftd#
```

```
show interface Tunnel1 | i packets
```

```
118 packets input, 31385 bytes
134 packets output, 8780 bytes
0 packets dropped
```

```
ftd#
```

```
show interface Tunnel2 | i packets
```

```
127 packets input, 33629 bytes
230 packets output, 15119 bytes
0 packets dropped
```

```
ftd#
```

d) Confermare le route statiche per i quartieri BGP.

```
<#root>
```

```
ftd#
```

```
show running-config route
```

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

e) Confermare le zone ECMP.

```
<#root>
```

```
ftd#
```

```
show zone
```

```
Zone: Azure-VTI-ECMP-Zone ecmp
  Security-level: 0
  Zone member(s): 2
    Azure-VTI-1      Tunne12
    Azure-VTI-0      Tunne11
```

```
ftd#
```

f) Confermare la configurazione BGP.

<#root>

ftd#

show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.2.0.12 remote-as 65515
    neighbor 10.2.0.12 description Instance0 Azure BGP Peering
    neighbor 10.2.0.12 ebgp-multihop 50
    neighbor 10.2.0.12 transport path-mtu-discovery disable
    neighbor 10.2.0.12 update-source bgpVPNBranchLo
    neighbor 10.2.0.12 activate
    neighbor 10.2.0.13 remote-as 65515
    neighbor 10.2.0.13 description Instance1 Azure BGP Peering
    neighbor 10.2.0.13 ebgp-multihop 50
    neighbor 10.2.0.13 transport path-mtu-discovery disable
    neighbor 10.2.0.13 update-source bgpVPNBranchLo
    neighbor 10.2.0.13 activate
  no auto-summary
  no synchronization
  exit-address-family
ftd#
```

g) Confermare la 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 10.0.0.1 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
B      172.27.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
      [20/0] via 10.2.0.12, 15:50:50
```

Altre considerazioni

La configurazione di base descritta in questo documento presuppone una singola interfaccia esterna e un singolo ISP presso la filiale FTD. Queste considerazioni estendono il progetto.

Previsione AS-Path

Se è necessario influenzare quale dei due tunnel Azure o FTD preferisce come tunnel primario, anziché condividere il carico in modo uguale tramite ECMP e BGP multipath, anteporre al numero AS locale una o più volte aggiuntive sul router BGP adiacente per considerarlo secondario. Al router adiacente con il percorso AS più lungo e anteposto viene assegnata la priorità durante la selezione del miglior percorso BGP standard, senza che sia necessario rimuoverlo completamente dalla zona ECMP.

Risoluzione dei problemi

- Il tunnel per la fase 1/fase 2 non viene visualizzato: Confermare che la chiave precondivisa e i parametri dei criteri IKEv2/IPsec (crittografia, integrità, PRF, gruppo DH e durata) corrispondano esattamente tra la proposta di criteri/IPSec IKEv2 FMC e i valori nel file di configurazione VPN di Azure scaricato. Utilizzare `show crypto isakmp sa` e `show crypto ipsec sa`, come mostrato nella Fase 3, Fase 5.
- Il tunnel è attivo, ma i router BGP adiacenti non si formano `update-source`: Verificare che il BGP sia impostato sull'interfaccia di loopback, non sulla VTI stessa, e che `ebgp-multihop` sia configurato con un valore sufficientemente alto da raggiungere l'indirizzo peer BGP di Azure, che non è connesso direttamente al FTD.
- Il BGP si forma, ma un solo tunnel trasporta il traffico: Confermare che entrambe le VTI siano membri della stessa zona ECMP, che le route statiche per entrambi gli indirizzi BGP dell'istanza di Azure siano installate con la stessa distanza amministrativa e che il multipath BGP sia configurato per due percorsi, come descritto nella fase 3, passaggio 10.
- Nessun traffico di ritorno o routing asimmetrico ad Azure: Poiché Azure vWAN annuncia lo spazio degli indirizzi dell'hub su entrambi i tunnel, verificare che ECMP non sia disabilitato in altre posizioni della configurazione di routing e verificare la presenza di route map o routing basato su criteri che possano bloccare il traffico su un singolo percorso.
- BGP è attivo e le route sono installate, ma il traffico sembra essere bloccato: Verificare di disporre di regole di controllo di accesso configurate con l'area di sicurezza assegnata alle VTI che consentono il traffico in entrata e in uscita.

Informazioni correlate

- [Che cos'è la rete WAN virtuale di Azure?](#)
- [Come configurare BGP per il gateway VPN di Azure](#)
- [Criteri IPsec predefiniti e personalizzati Azure vWAN](#)

- [Risoluzione dei problemi BGP per il gateway VPN di Azure](#)
- [Informazioni sui gateway VPN in modalità attiva-attiva](#)
- [Esercitazione: Creare una connessione da sito a sito utilizzando Azure Virtual WAN](#)

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).