Configure Secure Access with Secure Firewall Threat Defense for Private Access with Dynamic Routing

Contents

Introduction

This document describes how to configure Secure Access with FTD via IPsec for Secure Private Access with Dynamic Routing.

Prerequisites

Requirements

- Cisco Secure Access knowledge
- Cisco Secure Access dashboard/tenant
- Secure Firewall Threat Defense and Firewall Management Center knowledge
- IPsec knowledge
- Dynamic Routing knowledge

Components Used

- Secure Firewall Running 7.7.10 code
- Cloud-Delivered Firewall Management Center. Configuration also applies for typical virtual FMC
- Cisco Secure Access dashboard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Network tunnels in Secure Access can be used for two primary purposes: Secure Internet Access and Secure Private Access.

For Secure Private Access, organizations can leverage Zero Trust Access (ZTA) and/or VPN as a Service (VPNaaS) to connect users to private resources such as internal applications or data centers. IPsec tunnels play a key role in this architecture by securely encrypting network traffic between users and private resources, ensuring that sensitive data remains protected as it traverses untrusted networks. By integrating IPsec tunnels with ZTA or VPNaaS, organizations can provide seamless and secure access to internal resources while maintaining robust security controls and visibility.

This document describes how to configure Secure Access with Secure Firewall Threat Defense (FTD) via IPsec for Secure Private Access.
Additionally, this guide provides steps for configuring dynamic routing with BGP.

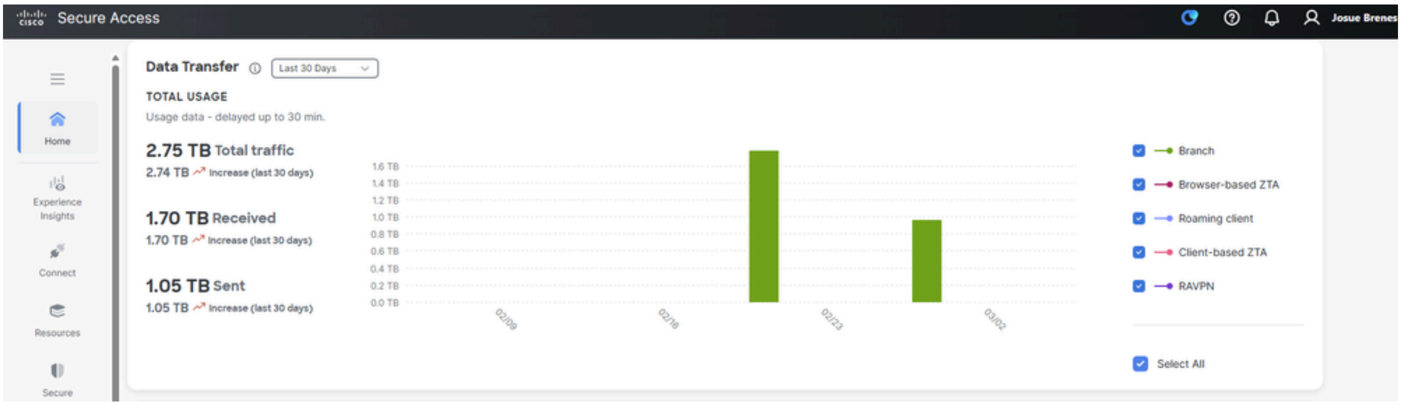
While this document covers the configuration of IPsec tunnels for Secure Private Access, the setup of Zero Trust Access (ZTA) or VPN as a Service (VPNaaS) for accessing private applications is outside the scope of this guide.

Configure

Secure Access Configuration

Network Tunnel Group Configuration

1. Navigate to the admin panel of Secure Access.



Data Transfer

TOTAL USAGE

Usage data - delayed up to 30 min.

2.75 TB Total traffic
2.74 TB Increase (last 30 days)

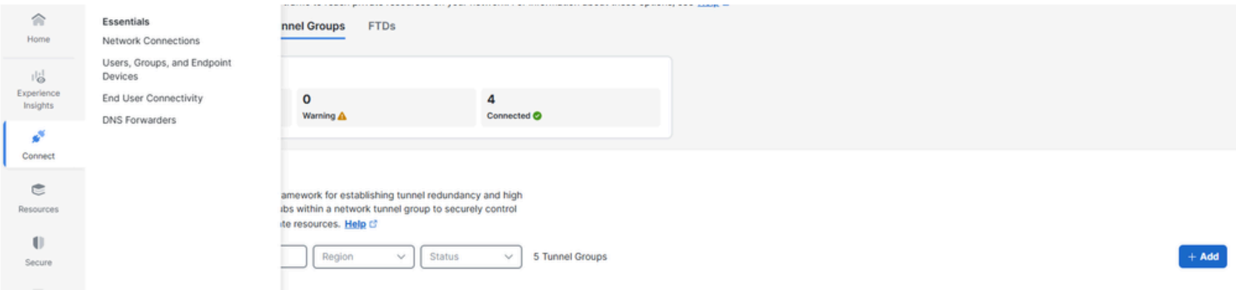
1.70 TB Received
1.70 TB Increase (last 30 days)

1.05 TB Sent
1.05 TB Increase (last 30 days)

CSA Dashboard

2. Add a Network Tunnel Group.

- Click on Connect > Network Connections
  - Under Network Tunnel Groups click on > Add



0 Warning

4 Connected

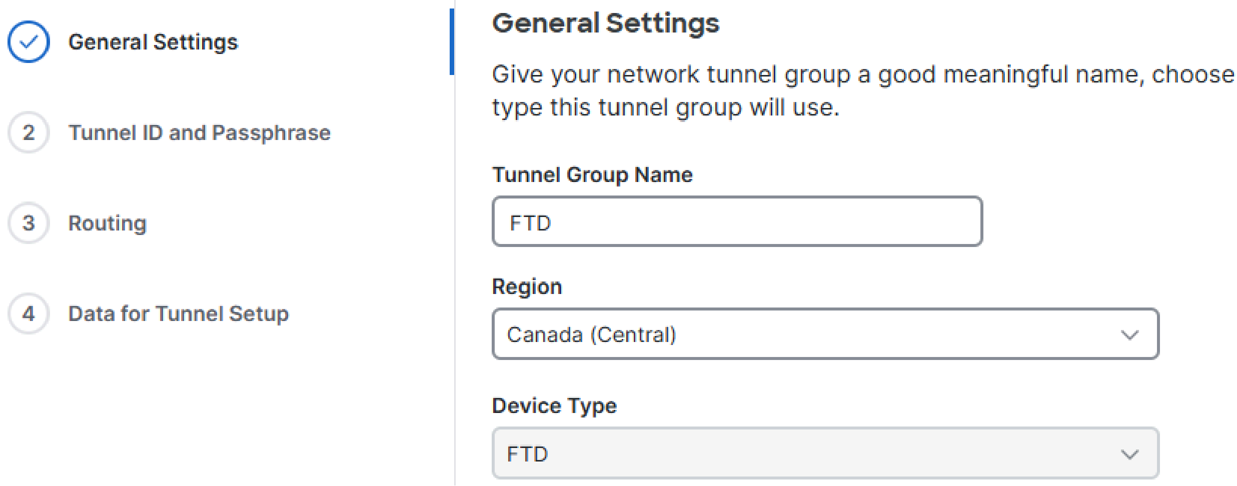
amework for establishing tunnel redundancy and high
ibs within a network tunnel group to securely control
ite resources. Help

5 Tunnel Groups

Check NTG

3. General Settings Configuration.

- Configure the Tunnel Group Name, **Region** and Device Type
  - Click Next



General Settings

Give your network tunnel group a good meaningful name, choose
type this tunnel group will use.

Tunnel Group Name
FTD

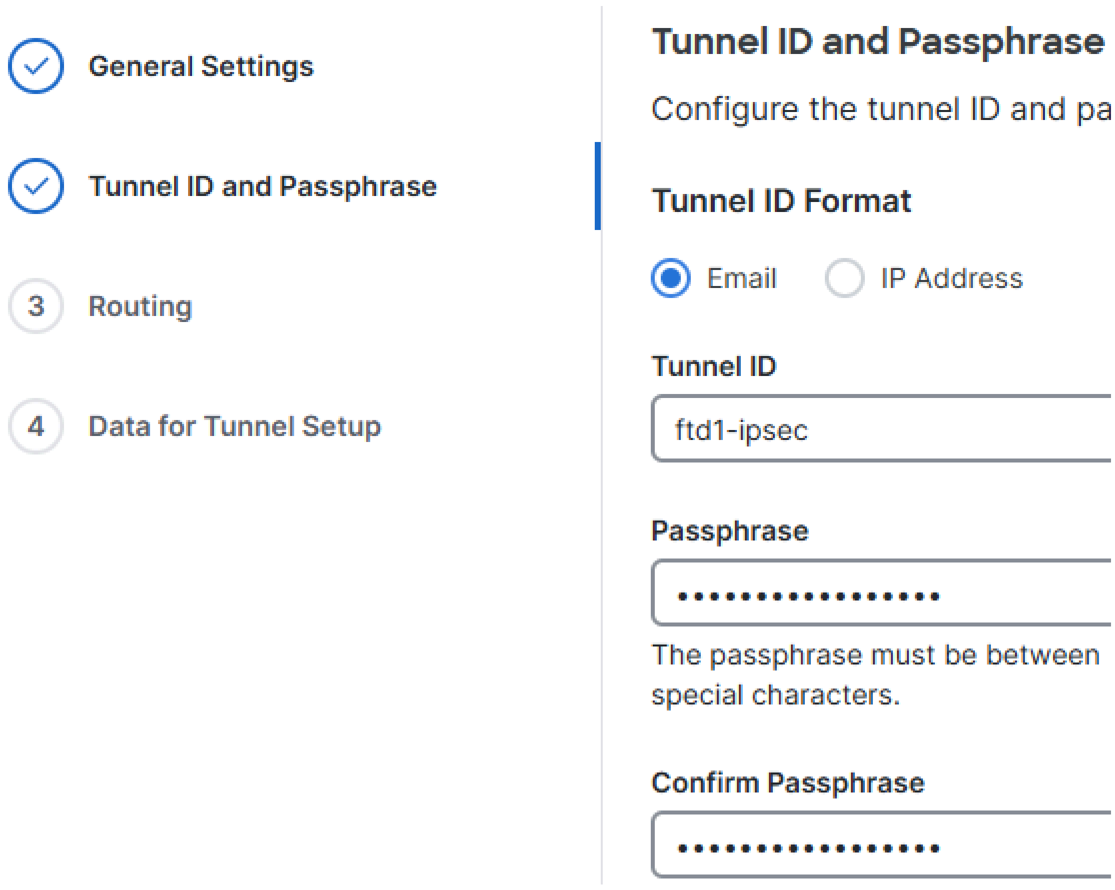
Region
Canada (Central)

Device Type
FTD

General Settings

4. Configure the **Tunnel ID**and Passphrase. This ID is important, as it is required for the FTD configuration

- Click on Next



✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

● Email ○ IP Address

Tunnel ID

ftd1-ipsec

Passphrase

•••••••••••••••••

The passphrase must be between
special characters.

Confirm Passphrase

•••••••••••••••••

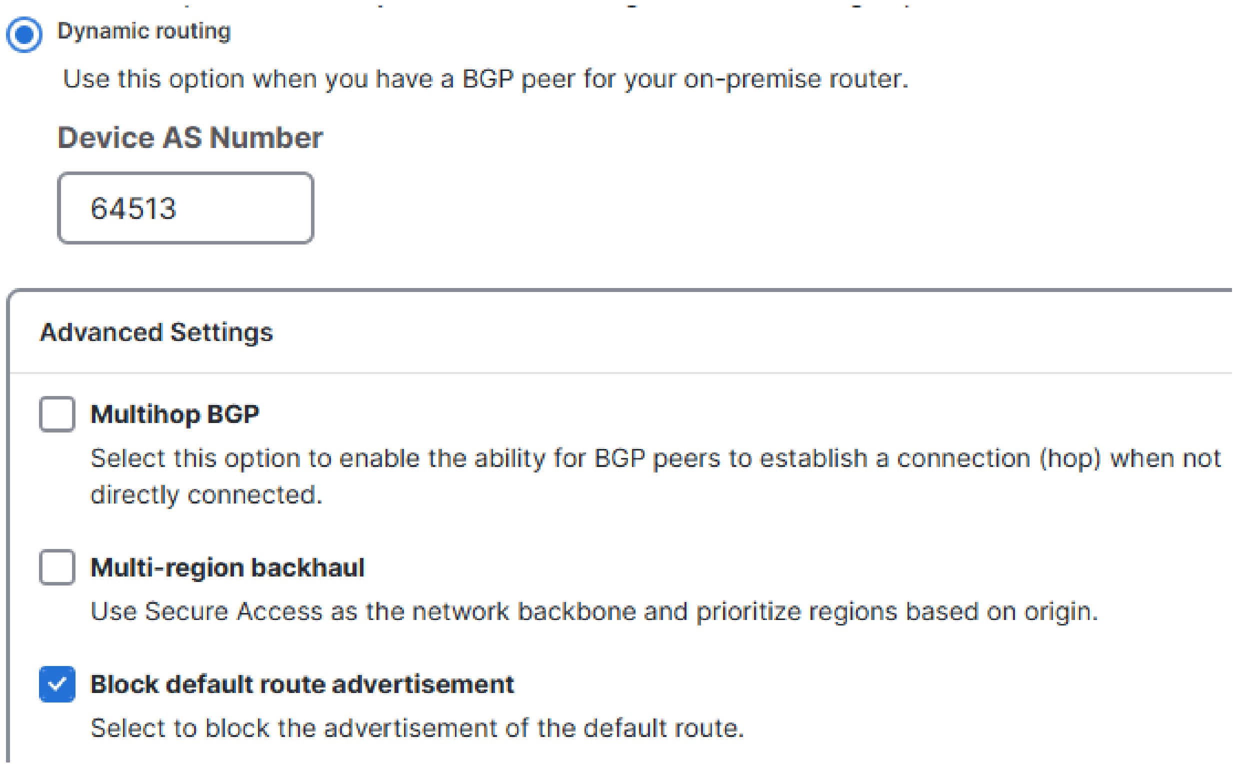
ID and PSK

5. Configure Dynamic Routing.

Secure Access Routing

Dynamic Routing (BGP)

- Specify the BGP Autonomous System (AS) number of the FTD when configuring the BGP peer in Secure Access.
- Click on Routing> Dynamic routing
  - Click on Device AS Number and add the FTDs BGP ASN
  - Check the Block default route advertisementcheck box
  - Click on Save



● Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Device AS Number

64513

Advanced Settings

□ **Multihop BGP**
Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

□ **Multi-region backhaul**
Use Secure Access as the network backbone and prioritize regions based on origin.

☑ **Block default route advertisement**
Select to block the advertisement of the default route.

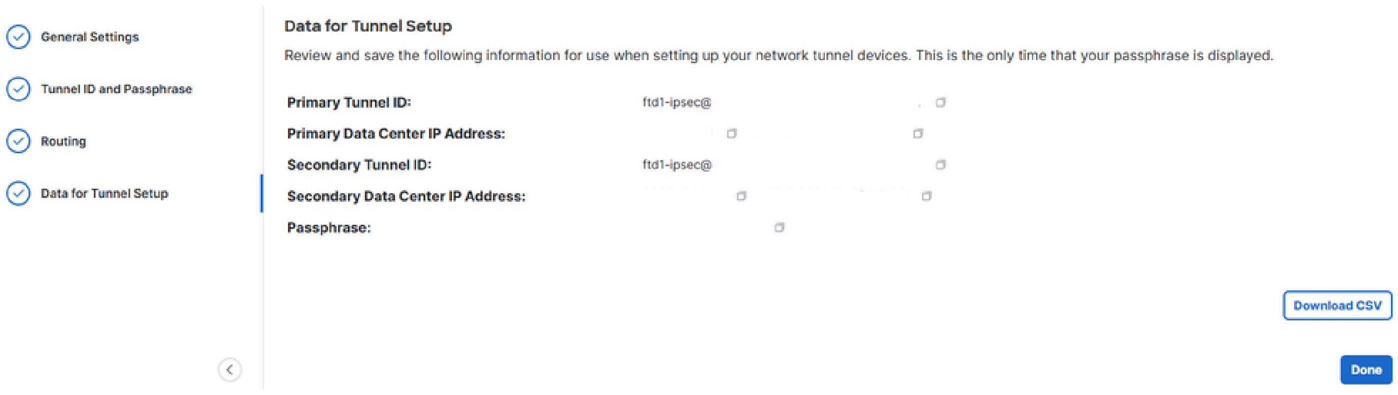
CSA BGP Config

Note: Routes advertised by Secure Access prepend the original AS path to include: 1 for primary tunnels and 2 for secondary tunnels. Multi-Region Backhaul Scenarios are supported. For more information click .

Save Network Tunnel Group Configuration

Download and save the tunnel setup data, as it is needed for the FTD configuration.

- Click on Download CSV
- Click on Done

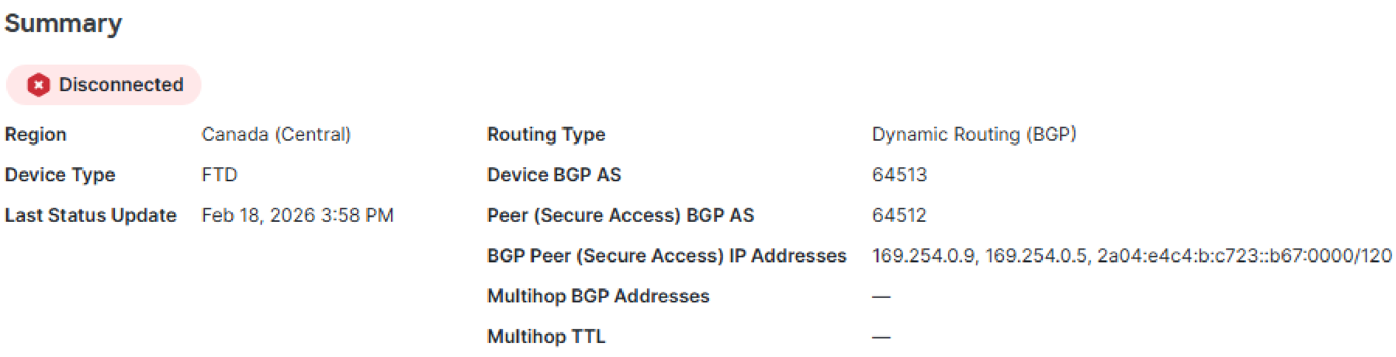


Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	ftd1-ipsec@
Primary Data Center IP Address:	
Secondary Tunnel ID:	ftd1-ipsec@
Secondary Data Center IP Address:	
Passphrase:	

NTG Data



Summary

Disconnected

Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120
		Multihop BGP Addresses	—
		Multihop TTL	—

BGP Settings

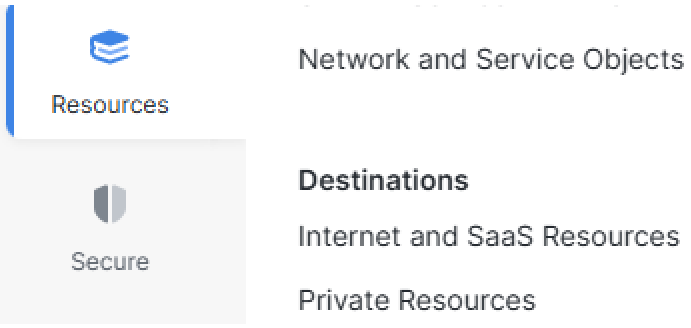
Note: Click on the Network Tunnel Group to view the BGP AS number and BGP peer IP addresses, which are later configured on the FTD side.

Create a Private Resource

Private resources are internal applications, networks, or subnets hosted in your data center or private cloud environment. These resources are not publicly accessible and are protected behind your organization’s infrastructure.

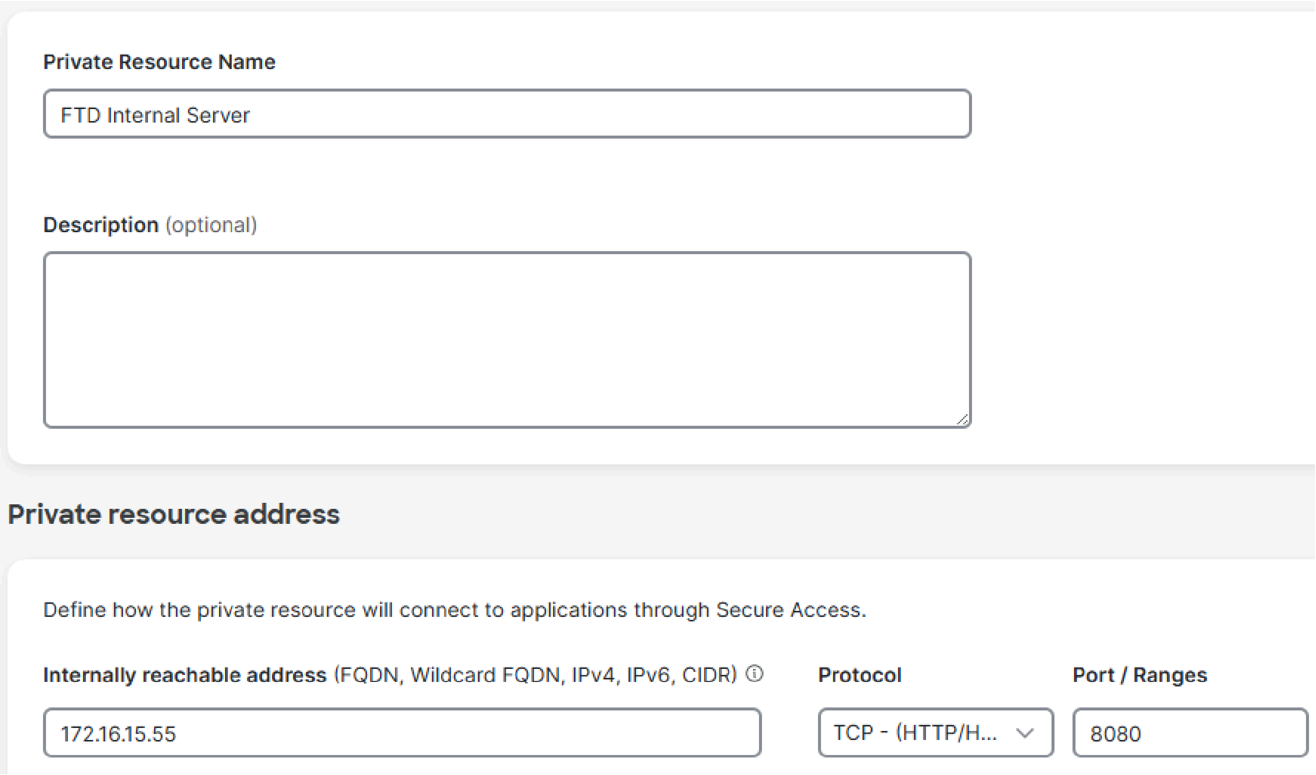
By defining them as Private Resources in Secure Access, you can enable controlled access through solutions like Zero Trust Access (ZTA) or VPN as a Service (VPNaaS). This ensures users can securely connect to internal systems based on identity, device posture, and access policies, without exposing the resources directly to the internet.

Navigate to **Resources** > **Private Resources**> click on Add.



PR

- Specify the **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Specify ports and protocols, and add additional private resources as needed
- Select the desired Connection Method based on your need, example Zero-trust connections and/or VPN Connections, according to your requirements
- Click on Save



Private Resource Name

FTD Internal Server

Description (optional)

Private resource address

Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR): 172.16.15.55

Protocol: TCP - (HTTP/H...

Port / Ranges: 8080

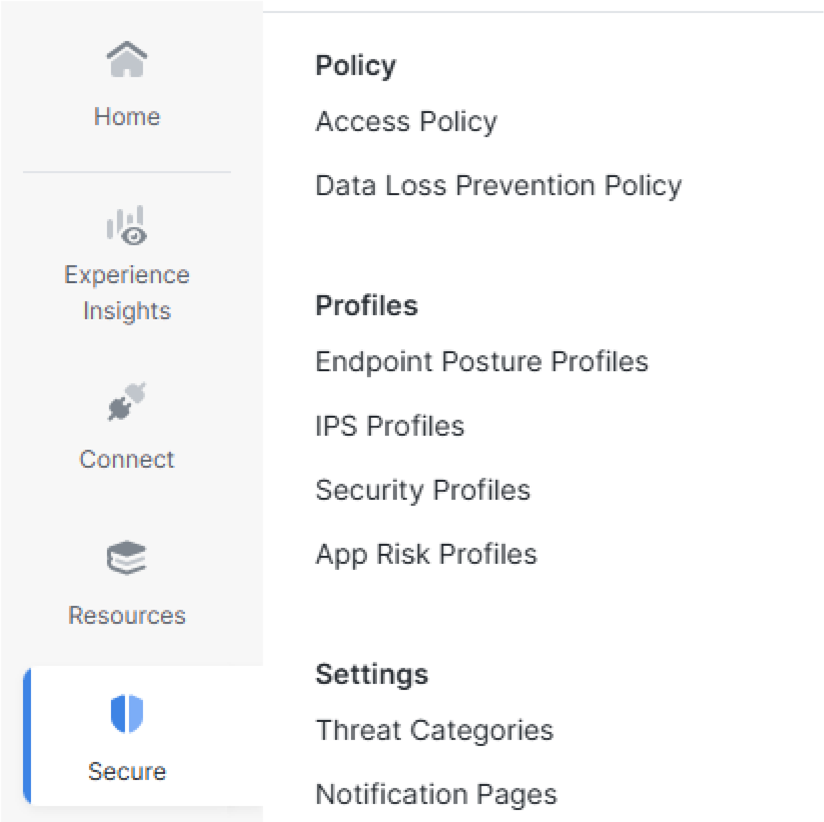
Private Resource

Create an Access Policy Rule

Private access rules define how users can securely connect to internal resources and applications that are not publicly accessible.

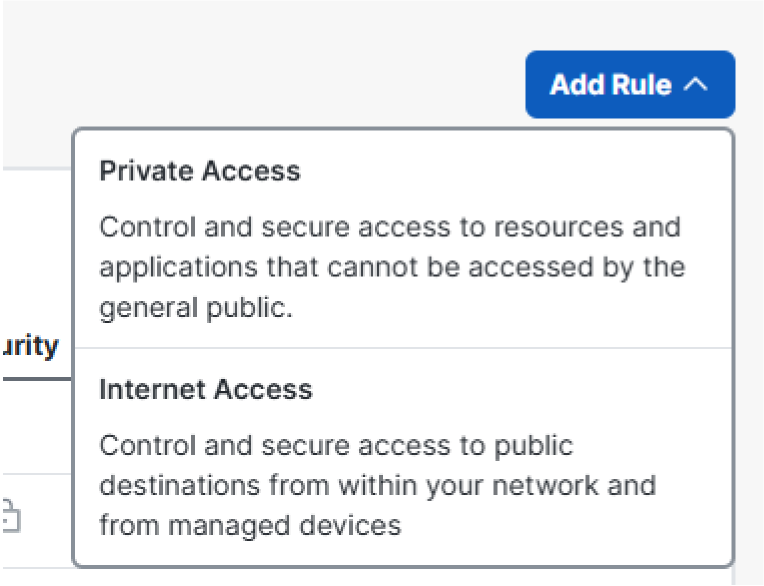
These rules enforce security by controlling who can access specific private resources based on factors such as user identity, group membership, device posture, location, or other policy conditions. This ensures that sensitive internal systems remain protected from general public access while still being securely available to authorized users through ZTA or VPNaaS.

Navigate to Secure>Access Policy



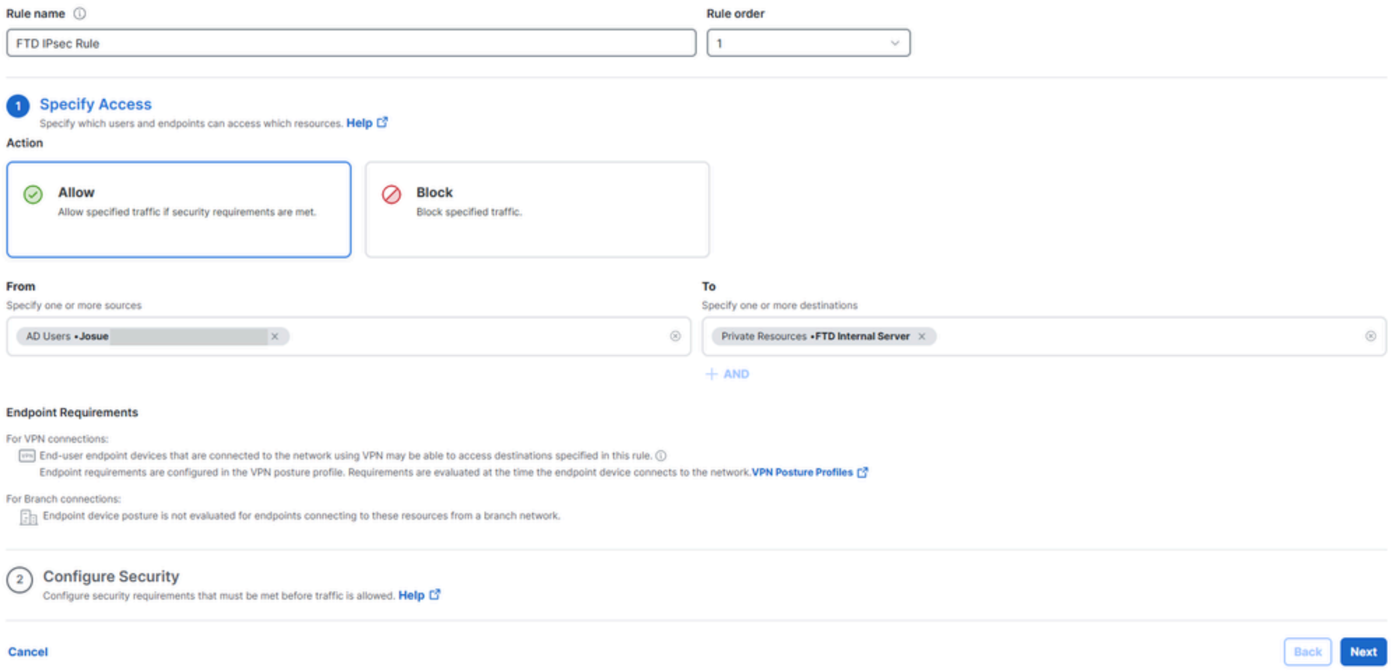
ACP

- Click on Add Rule
  - Click on Private Access


Add Rule
Private Access
Control and secure access to resources and applications that cannot be accessed by the general public.
Internet Access
Control and secure access to public destinations from within your network and from managed devices
ırity

Add ACP

- Click on Rule Name and give it a name
- Click on Action, select Allowto permit this traffic
- Click onFromand specify the users who are grated permission
- Click on Toand specify the access those users have based on this rule
- Click on Next, and then Savein the next page



Rule name ⓘ

FTD IPsec Rule

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. Help

Action

From

Specify one or more sources

AD Users • Josue [redacted]

To

Specify one or more destinations

Private Resources • FTD Internal Server

Endpoint Requirements

For VPN connections:

End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ

Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. VPN Posture Profiles

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security

Configure security requirements that must be met before traffic is allowed. Help

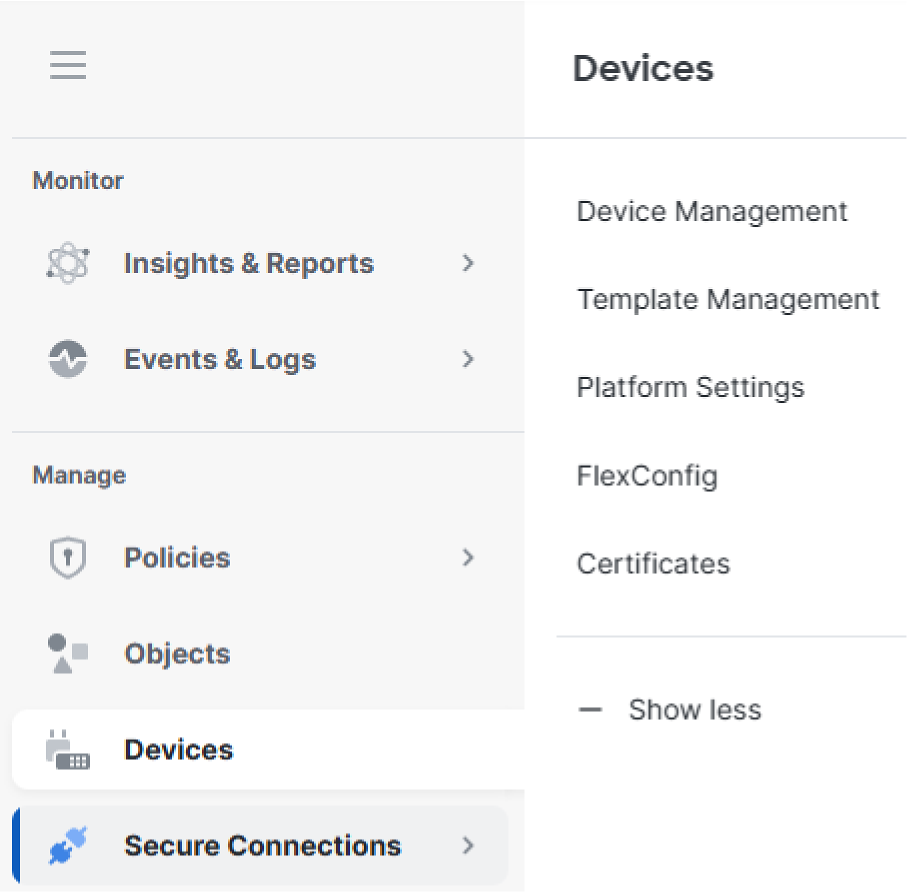
ACP config

Secure Firewall Threat Defense (FTD) Configuration

Virtual Tunnel Interfaces Configuration

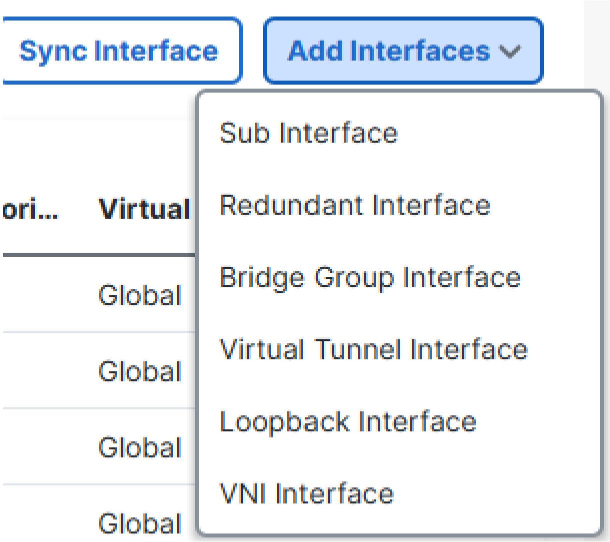
A Virtual Tunnel Interface (VTI) on FTD is a logical Layer 3 interface used to configure route-based IPsec VPN tunnels.

1. Navigate to Devices> Device Management.



FTD Devices

- Click on the FTD Device, Interfaces
  - Click on Add Interfaces
  - Click on Virtual Tunnel Interface
  - Create two Virtual Tunnel Interfaces, one for the Primary Secure Access Hub and another one for the Secondary Secure Access Hub

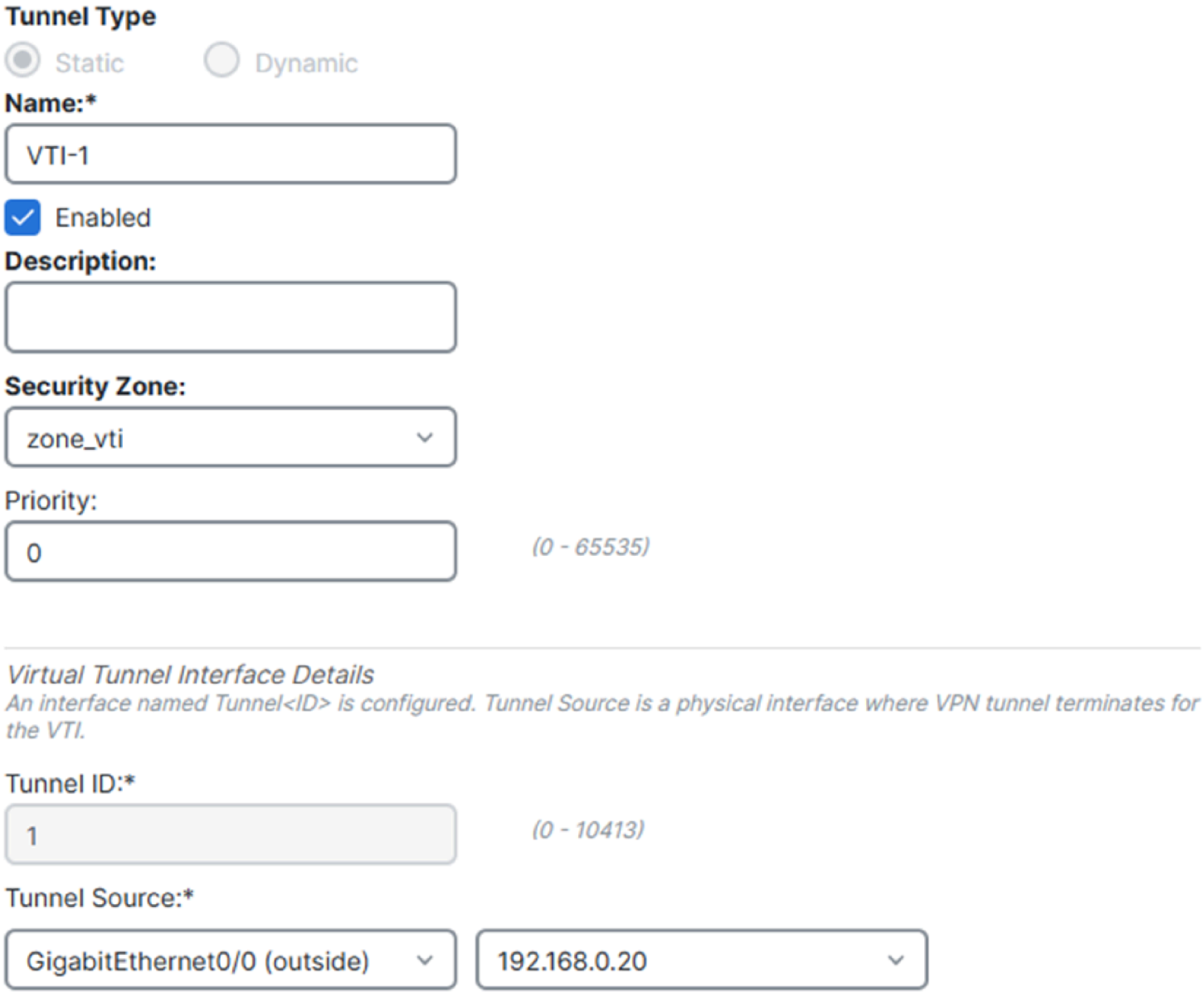


Add VTIs

Virtual Tunnel Interface 1:

- Give it a name, click on Enable
- Select or create a Security Zone
- Click on Tunnel ID and give it a value.
- Click on Tunnel Source and specify the WAN Interface the tunnel is going to be establish from
- Click on IPsec Tunnel Mode, selectIPv4
- Click on IP Address and configure the IP address for the VTI

Click onOK



Tunnel Type

● Static ○ Dynamic

Name:*

VTI-1

☑ Enabled

Description:

Security Zone:

zone_vti

Priority:

0 *(0 - 65535)*

Virtual Tunnel Interface Details

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

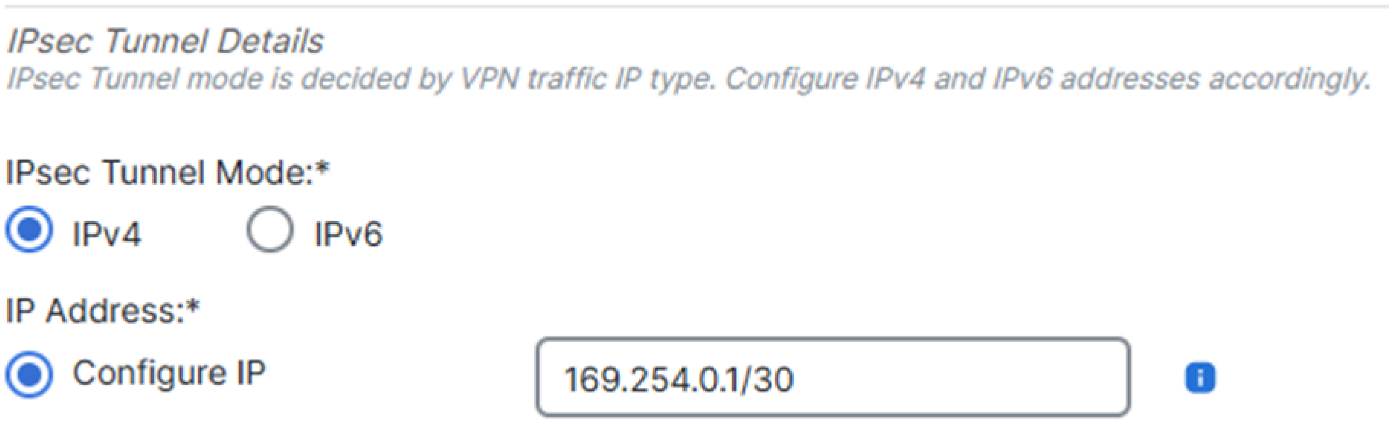
Tunnel ID:*

1 *(0 - 10413)*

Tunnel Source:*

GigabitEthernet0/0 (outside) 192.168.0.20

VTI1.1



IPsec Tunnel Details

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

IPsec Tunnel Mode:*

● IPv4 ○ IPv6

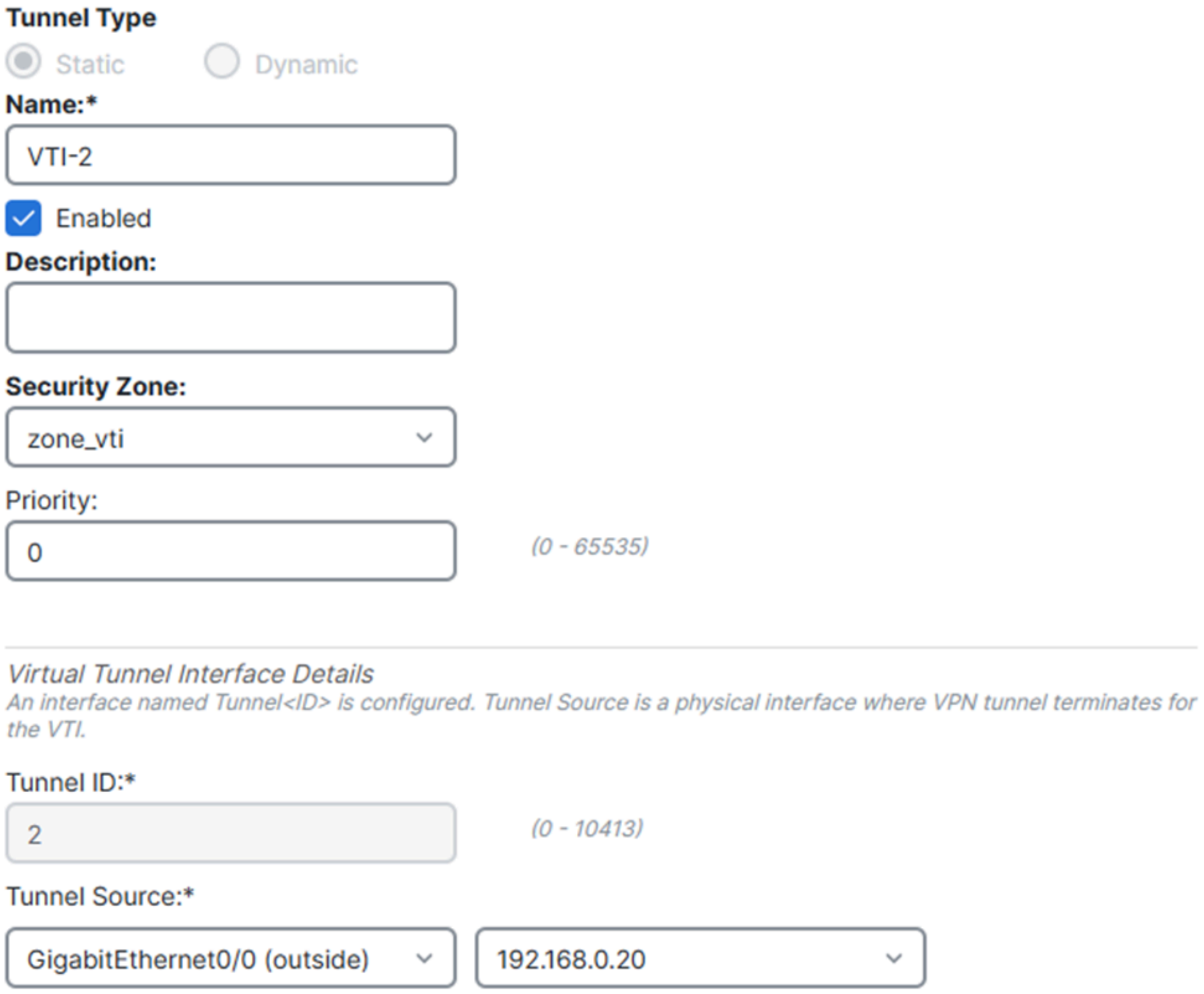
IP Address:*

● Configure IP 169.254.0.1/30

VTI1.2

Virtual Tunnel Interface 2:

- Give it a name, click on Enable
- Select or create a Security Zone
- Click on Tunnel ID and give it a value
- Click on Tunnel Source and specify the WAN Interface the tunnel is going to be establish from
- Click on IPsec Tunnel Mode, selectIPv4
- Click on IP Address and configure the IP address for the VTI
- Click onOK



Tunnel Type

● Static ○ Dynamic

Name:* VTI-2

☑ Enabled

Description:

Security Zone: zone_vti

Priority: 0 *(0 - 65535)*

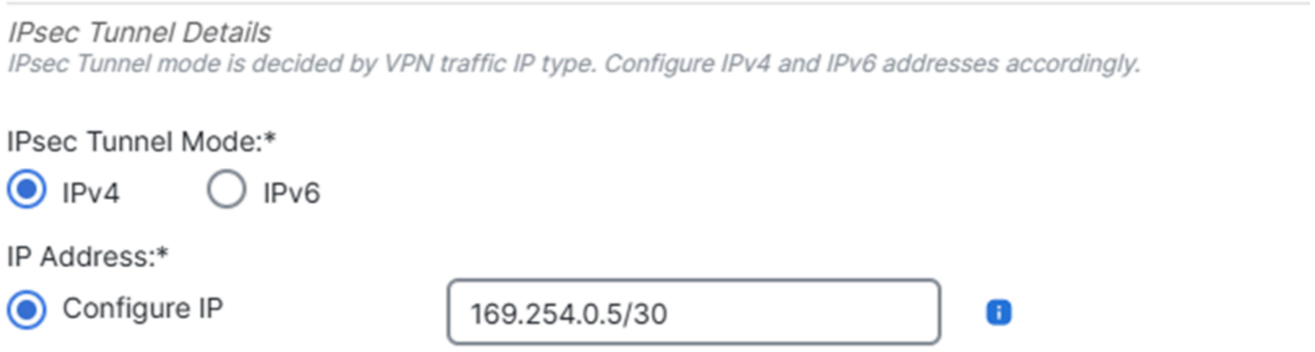
Virtual Tunnel Interface Details

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:* GigabitEthernet0/0 (outside) 192.168.0.20

VTI2.1



IPsec Tunnel Details

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

IPsec Tunnel Mode:*

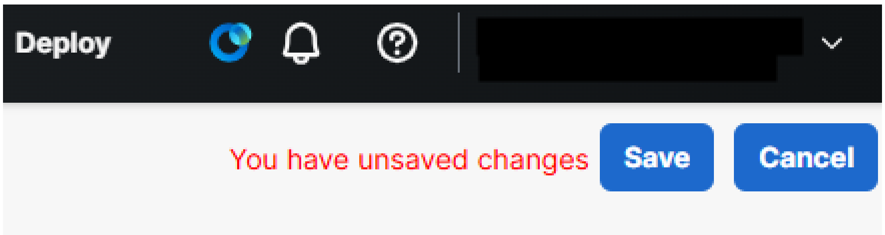
● IPv4 ○ IPv6

IP Address:*

● Configure IP 169.254.0.5/30

VTI2.2

Click on **Save**.



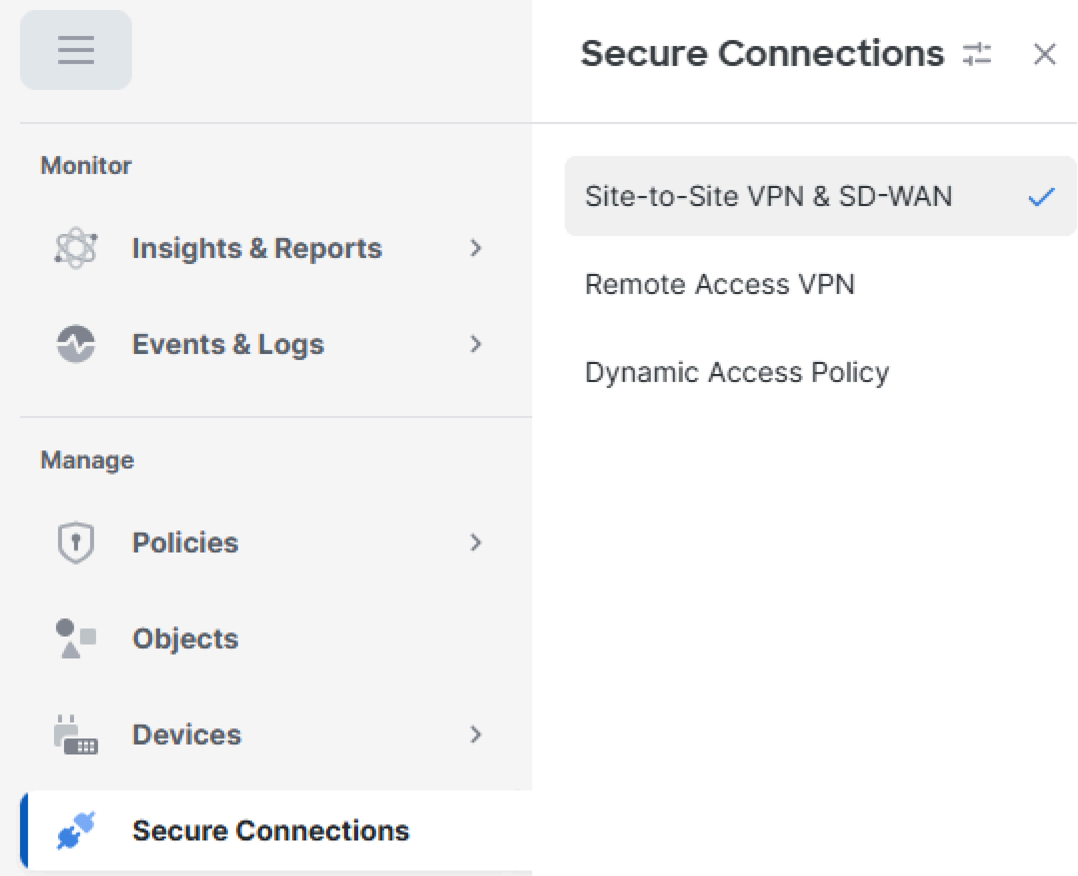
You have unsaved changes

Save VTI Changes

IPsec Tunnel Configuration

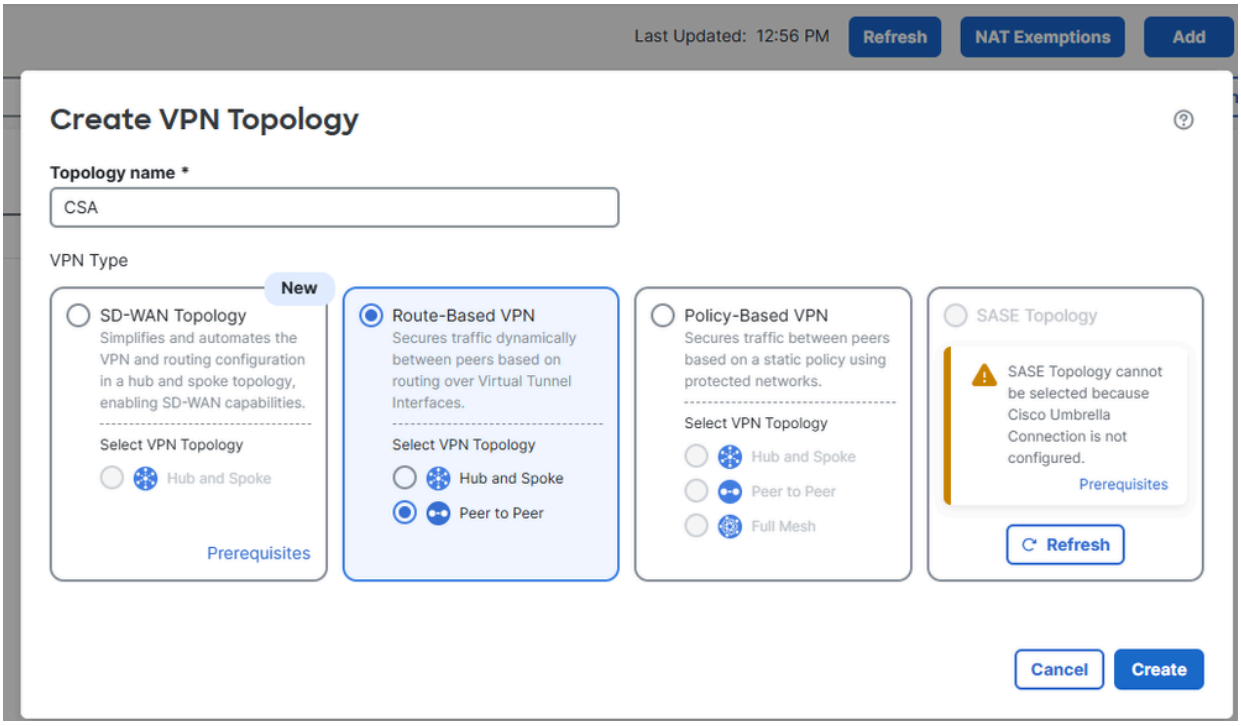
Navigate to your cdFMC dashboard.

- Click on Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Click onAdd
  - Click on Route-Based VPN
  - Click on Peer to Peer



Create VPN Topology

Topology name *

CSA

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

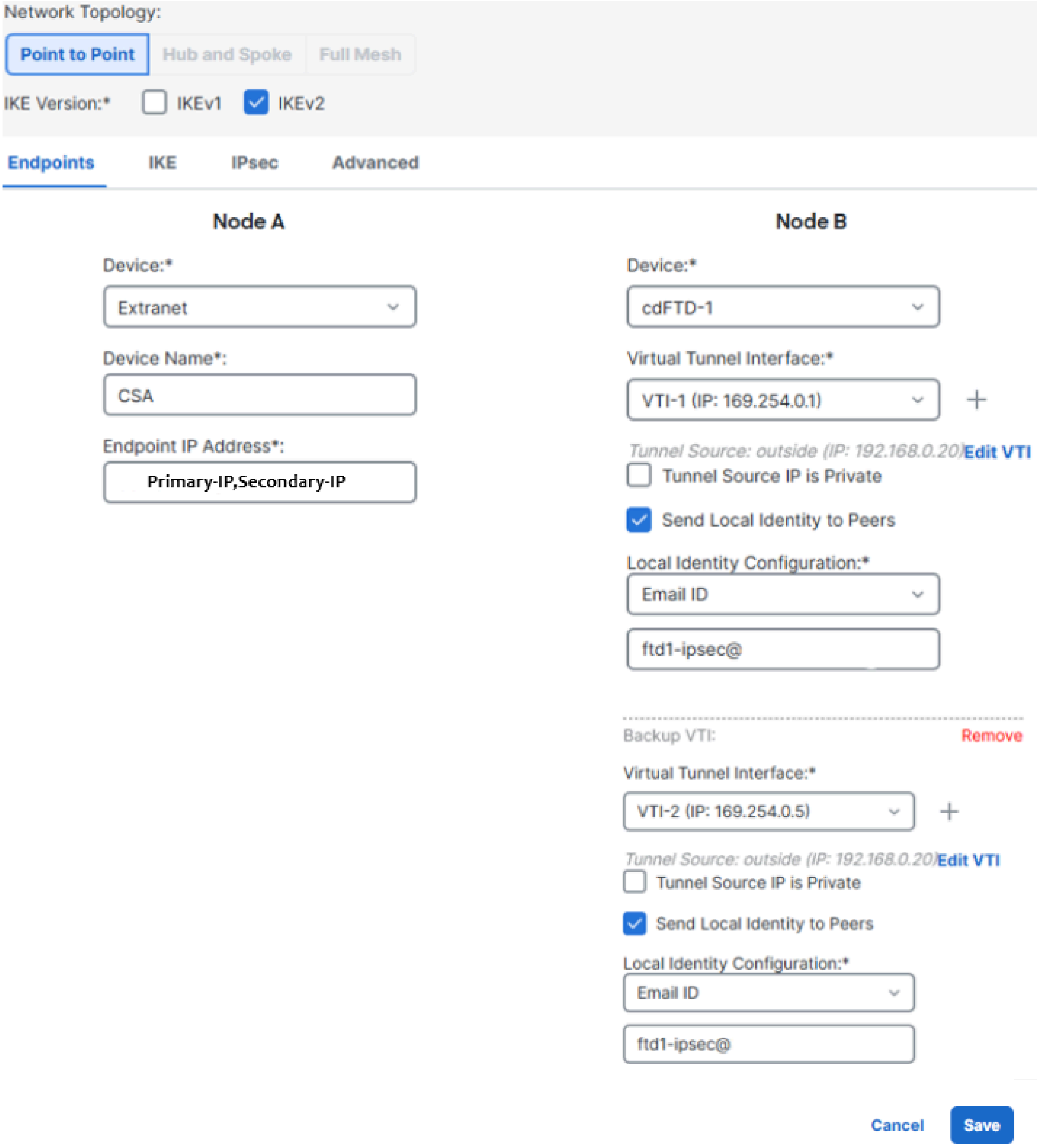
● Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
○ Hub and Spoke
● Peer to Peer

○ 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 Cisco Umbrella Connection is not configured.

Add VPN

- From step 5 of the Secure Access configuration, obtain the tunnel IDs and IP addresses for the primary and secondary data centers
- Click onEndpoints
  - Under Node A, click onDeviceand select Extranet
  - Click on Device Nameand give it a name
  - Click on Enpoint IP Addresses and enter the Secure Access Primary and Secondary IP Addresses separated by a comma (from "Save Network Tunnel Group Configuration" under the Secure Access
    Configuration)
  - Under Node B, click on Device and select your FTD device
  - Click on Virtual Tunnel Interface and select the first VTI interface created in the previous step
  - Click on Send Local Identity to Peers option and select Email ID, enter the primary tunnel ID (from "Save Network Tunnel Group Configuration" under the Secure Access Configuration)
  - Click on Add Backup VTI
  - Click on Virtual Tunnel Interface and select the second VTI interface created in the previous step
  - Click onSend Local Identity to Peersoption and select Email ID, enter the secondary tunnel ID (from "Save Network Tunnel Group Configuration" under the Secure Access Configuration)
  - Click on **Save**



Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:* □ IKEv1 ☑ IKEv2

Endpoints | IKE | IPsec | Advanced

Node A

Device:* Extranet

Device Name*: CSA

Endpoint IP Address*: Primary-IP,Secondary-IP

Node B

Device:* cdFTD-1

Virtual Tunnel Interface:* VTI-1 (IP: 169.254.0.1) +

Tunnel Source: outside (IP: 192.168.0.20) Edit VTI

□ Tunnel Source IP is Private

☑ Send Local Identity to Peers

Local Identity Configuration:* Email ID

ftd1-ipsec@

Backup VTI: Remove

Virtual Tunnel Interface:* VTI-2 (IP: 169.254.0.5) +

Tunnel Source: outside (IP: 192.168.0.20) Edit VTI

□ Tunnel Source IP is Private

☑ Send Local Identity to Peers

Local Identity Configuration:* Email ID

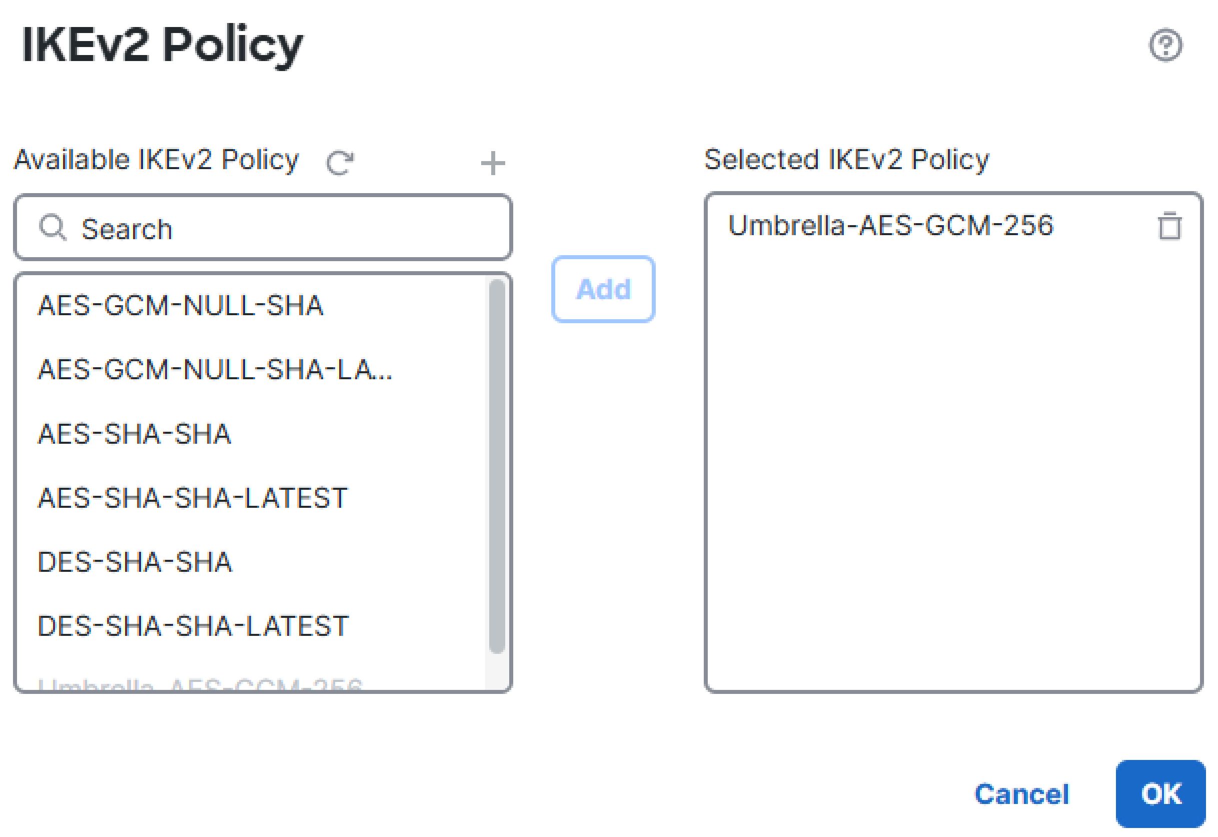
ftd1-ipsec@

Cancel | Save

FTD VTI Configuration

- Click on IKE
  - Click on **IKEv2 Settings** > Policies
  - Select the Umbrella-AES-GCM-256 option

Click on OK



IKEv2 Policy

Available IKEv2 Policy

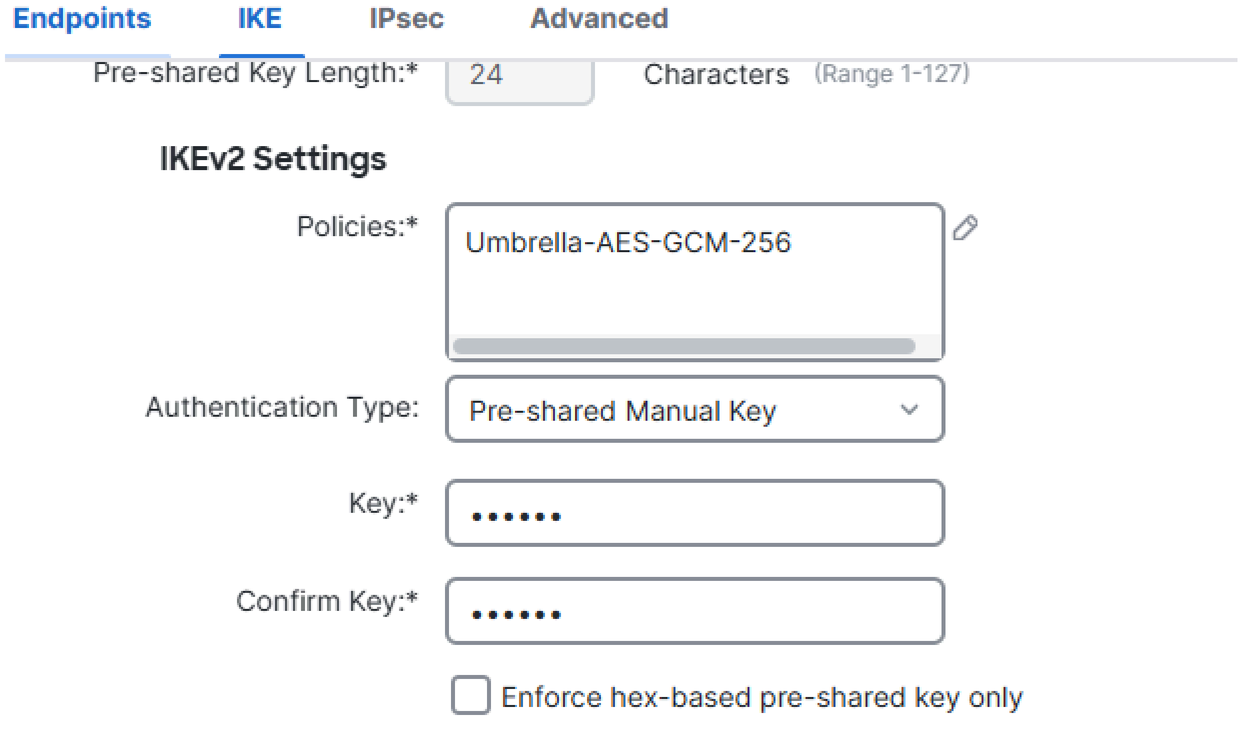
- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LA...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- DES-SHA-SHA
- DES-SHA-SHA-LATEST
- Umbrella-AES-GCM-256

Selected IKEv2 Policy

- Umbrella-AES-GCM-256

IKEv2 Policy

- Click on Authentication Type and selectPre Shared Manual Key, enter the PSK configured in Secure Access (passphrase)



Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policies:* Umbrella-AES-GCM-256

Authentication Type: Pre-shared Manual Key

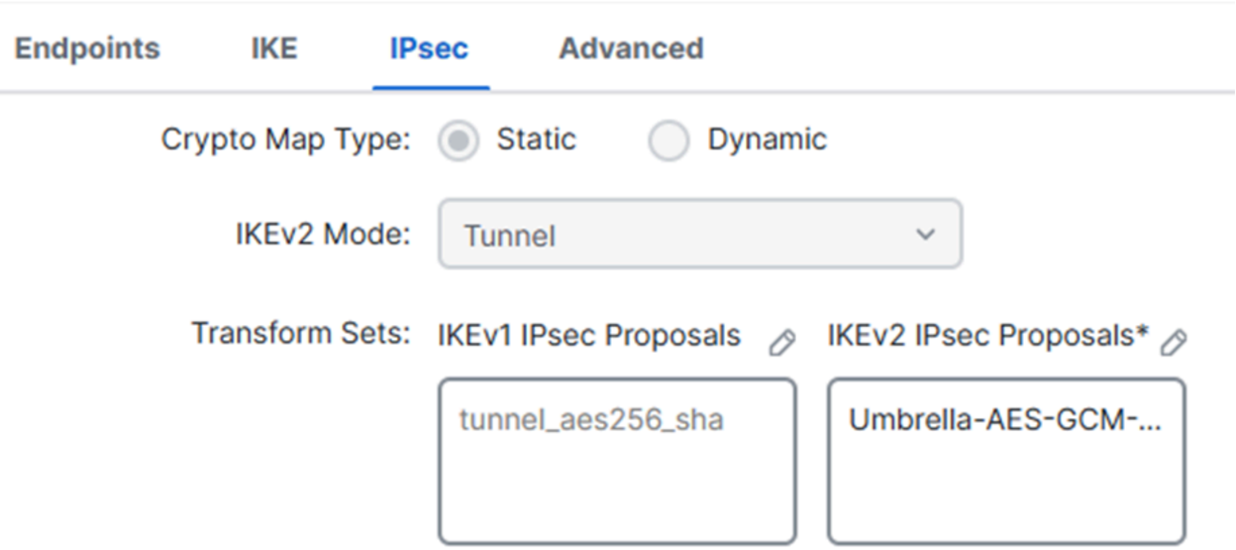
Key:* ••••••

Confirm Key:* ••••••

□ Enforce hex-based pre-shared key only

IKE

- Click on IPSEC
    - Click on IKEv2 Proposals
    - Select Umbrella-AES-GCM-256
    - Click on OK



Crypto Map Type: ● Static ○ Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals: tunnel_aes256_sha

IKEv2 IPsec Proposals*: Umbrella-AES-GCM-...

IPsec

Save IKEv2 Proposals

FTD Routing Configuration

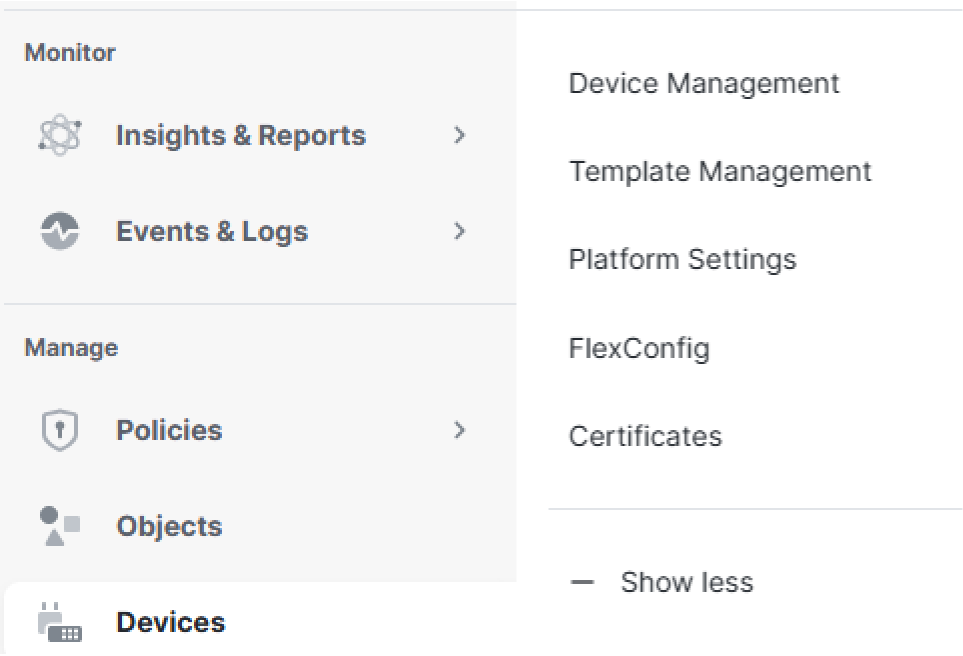
Dynamic Routing (BGP)

Border Gateway Protocol (BGP) is a dynamic routing protocol that automates the exchange of routing information between autonomous systems (AS). It determines the best available path for data traffic based on attributes and policies, rather than relying on static routes.

By dynamically learning and updating routes, BGP improves scalability, optimizes path selection, and provides automatic failover in the event of link or network changes.

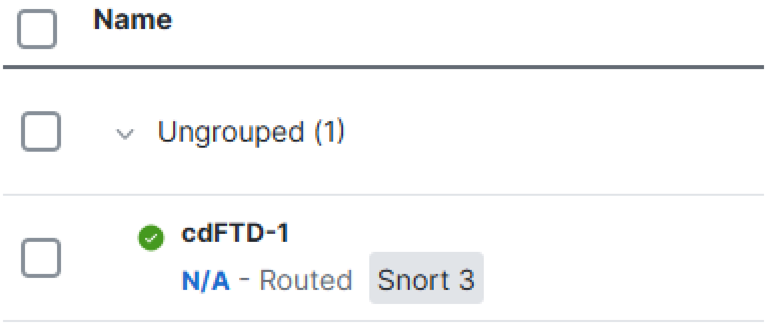
Navigate to your cdFMC dashboard.

- Click on Devices> Device Management



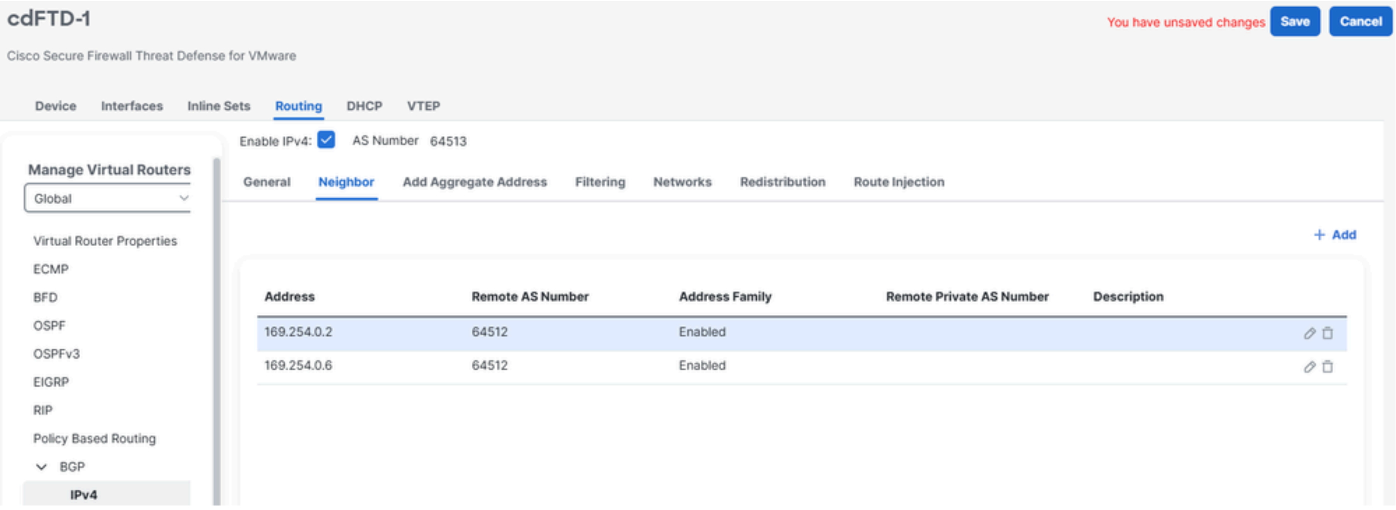
Device

- Click on the FTD



FTD Device

  - Click on Routing > BGP > IPv4 > Enable IPv4
  - Click on Neighbor, and specify the BGP Autonomous System (AS) number for Secure Access, along with the neighbor IP addresses
    Refer to the Note under the Secure Access Configuration, where all relevant configuration details are provided for this process.
  - Click onSave



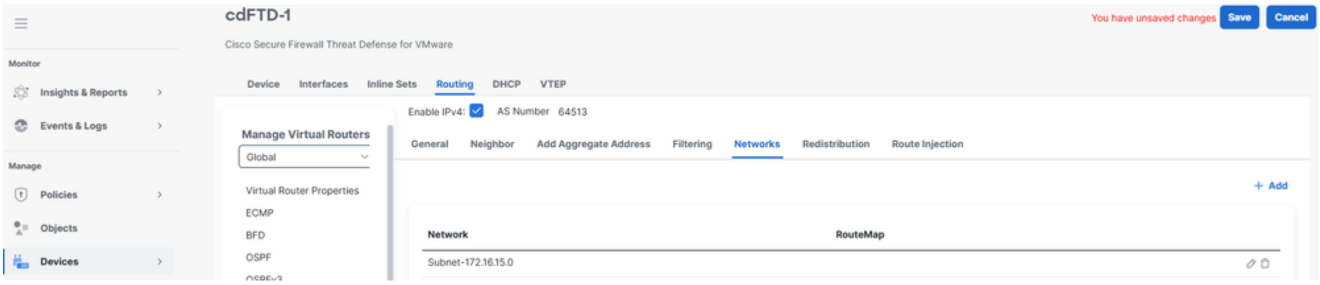
Enable IPv4: ☑ AS Number 64513

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		
169.254.0.6	64512	Enabled		

BGP neighbor

Note: starting November 2025, all newly created Secure Access organizations use the public ASN 32644 by default for BGP peering in network tunnel groups. Existing organizations established prior to November 2025 continue to use the private ASN 64512 that was previously reserved for Secure Access BGP peers.

- Click on Networks, and add the network(s) you want to advertise over to Secure Access
- Click on Save



Enable IPv4: ☑ AS Number 64513

Network	RouteMap
Subnet-172.16.15.0	

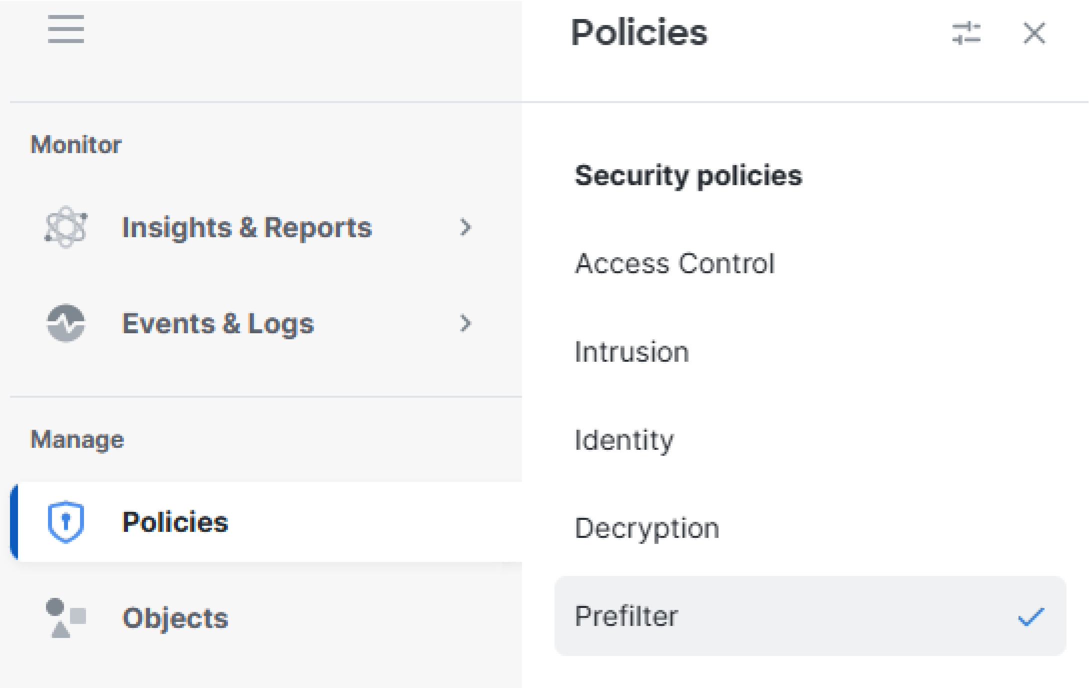
Add Network

Access Policy Configuration

To allow traffic on an Cisco Firepower Threat Defense (FTD) and enable access to private resources, traffic must first pass through the initial stage of access control known as Prefiltering.

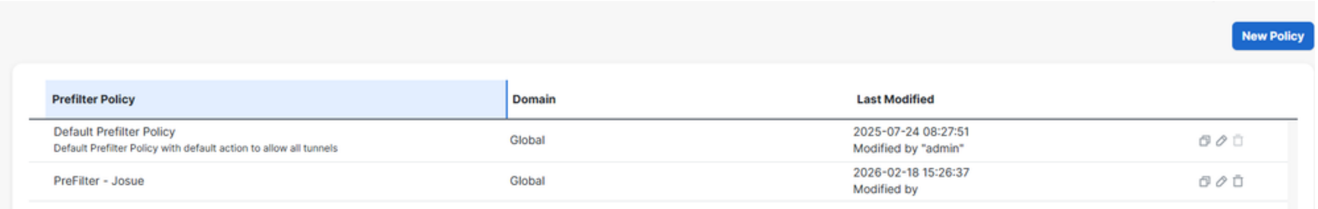
Prefiltering is processed before deeper inspection occurs and is designed to be simple and fast. It evaluates traffic using basic outer-header criteria (such as source and destination IP addresses and ports) to quickly allow, block, or bypass traffic. When traffic is allowed at this stage, it can skip more resource-intensive inspections like deep packet inspection or intrusion policies, improving performance while still maintaining security control.

Navigate to Policies> Prefilter



Prefilter

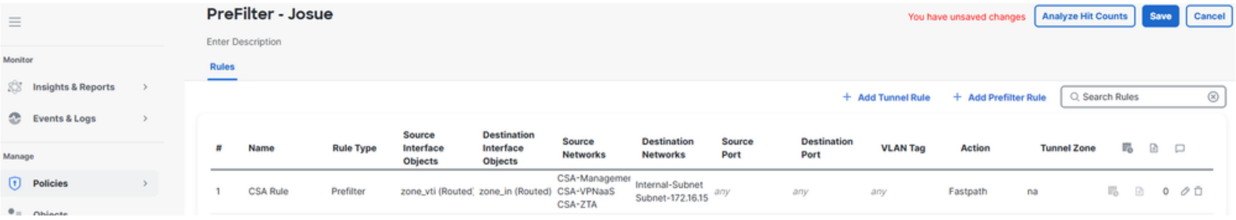
- Click on edit the Prefilter poilcy being used by your Access Policy



Prefilter Policy	Domain	Last Modified
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2025-07-24 08:27:51 Modified by "admin"
PreFilter - Josue	Global	2026-02-18 15:26:37 Modified by

click on prefilter

- Click on Add Tunnel Rule
  - Add and permit the traffic from the VPNaaS network and/or the ZTA Subnet to your Private Resources
  - Click onSave



PreFilter - Josue

Enter Description

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
1	CSA Rule	Prefilter	zone_vti (Routed)	zone_in (Routed)	CSA-Managemer CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na

Save Rule

At this point, once the configuration on the FTD has been completed and verified, you can proceed with the deployment. After deployment, both the IPsec tunnels and BGP neighbor sessions come up successfully, confirming that connectivity and dynamic routing are operating as expected.

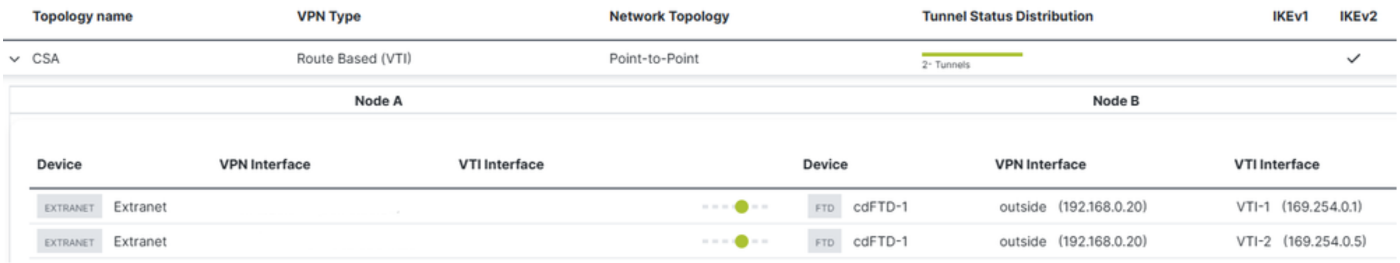
Verify

Verify in FTD

Tunnel Status in FTD

You can view the tunnel’s current status, including whether it is **up** or **down**. This helps verify that the IPsec tunnel is properly established.

- Click on **Secure Connections**
- Click on **Site-to-Site VPN & SD-WAN**
- Click on the **Topology Name**



Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2- Tunnels		✓

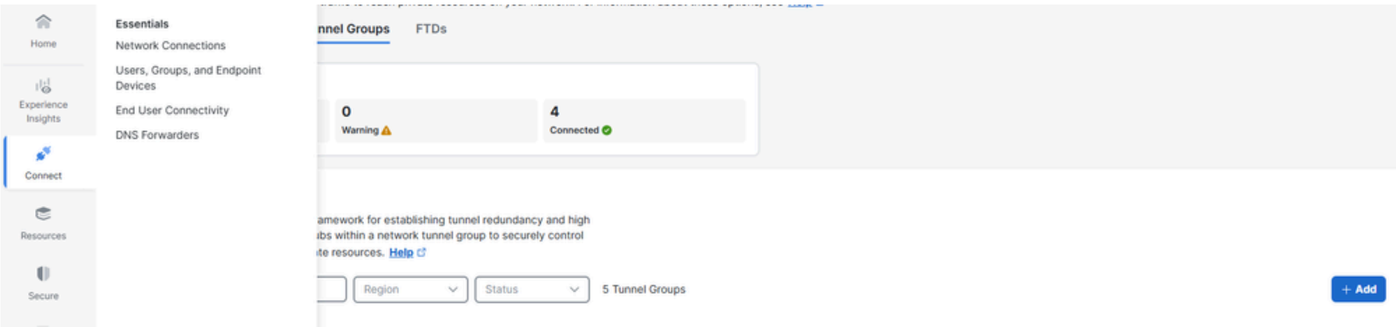
Node A			Node B		
Device	**VPN Interface**	**VTI Interface**	**Device**	**VPN Interface**	**VTI Interface**
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

FTD Tunnel Status

Tunnel Status in Secure Access

You can view the tunnel’s current status, including whether it is Disconnected, Warning or Connected. This helps verify that the IPsec tunnel is properly established.

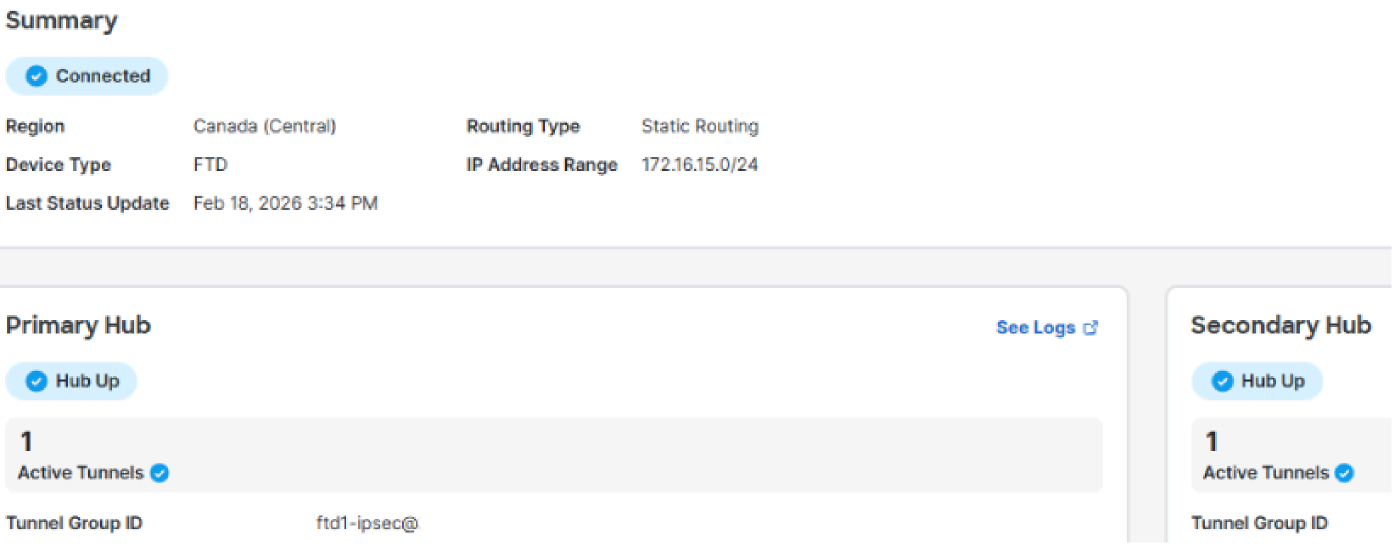
- Click on **Connect** > **Network Connections**
- Click on **Network Tunnel Groups**



amework for establishing tunnel redundancy and high
ıbs within a network tunnel group to securely control
ıte resources. Help

Check NTG

- Click on the **Network Tunnel Group**



Summary

Connected

Region	Canada (Central)	Routing Type	Static Routing
Device Type	FTD	IP Address Range	172.16.15.0/24
Last Status Update	Feb 18, 2026 3:34 PM		

Primary Hub

See Logs

Hub Up

1
Active Tunnels

Tunnel Group ID ftd1-ipsec@

Secondary Hub

Hub Up

1
Active Tunnels

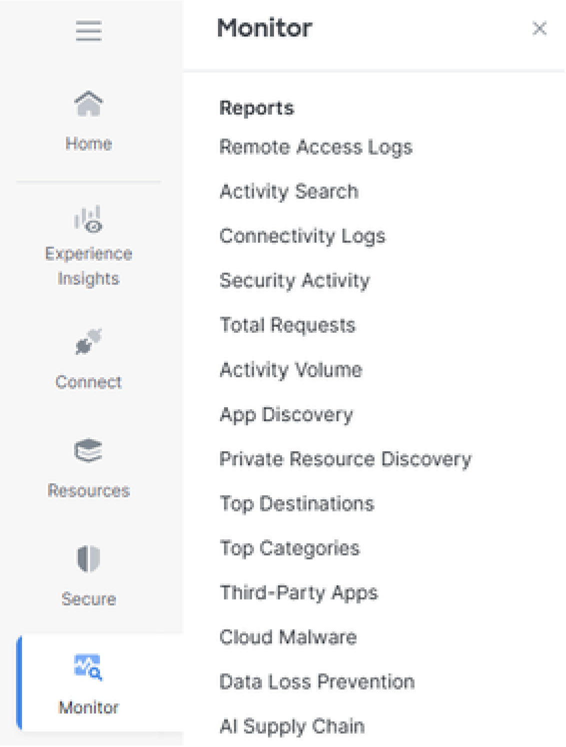
Tunnel Group ID

CSA Tunnel Status

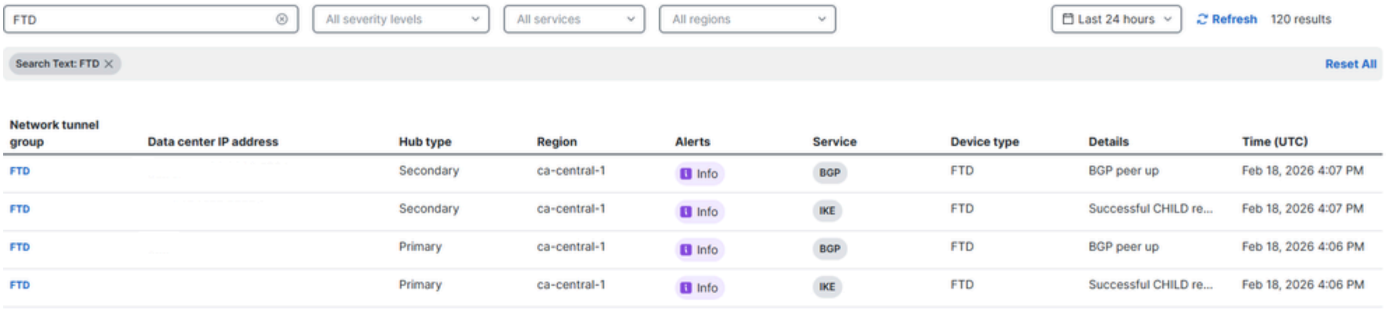
Events in Secure Access

You can view Tunnel and BGP events and confirm if the status of the IPsec tunnels is up and stable, and whether BGP sessions are established.

Click on **Monitor** > **Network Connectivity**.



Monitor Conn Logs



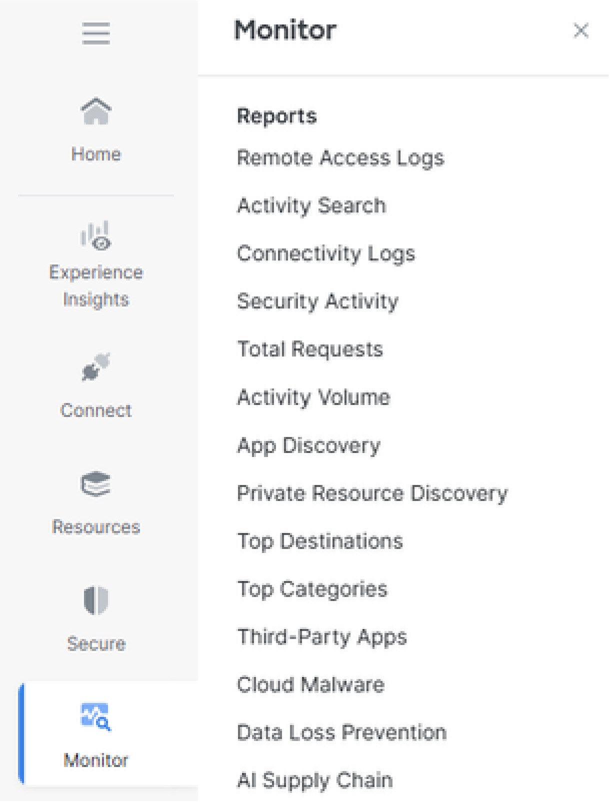
FTD | All severity levels | All services | All regions | Last 24 hours | Refresh | 120 results

Search Text: FTD | Reset All

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

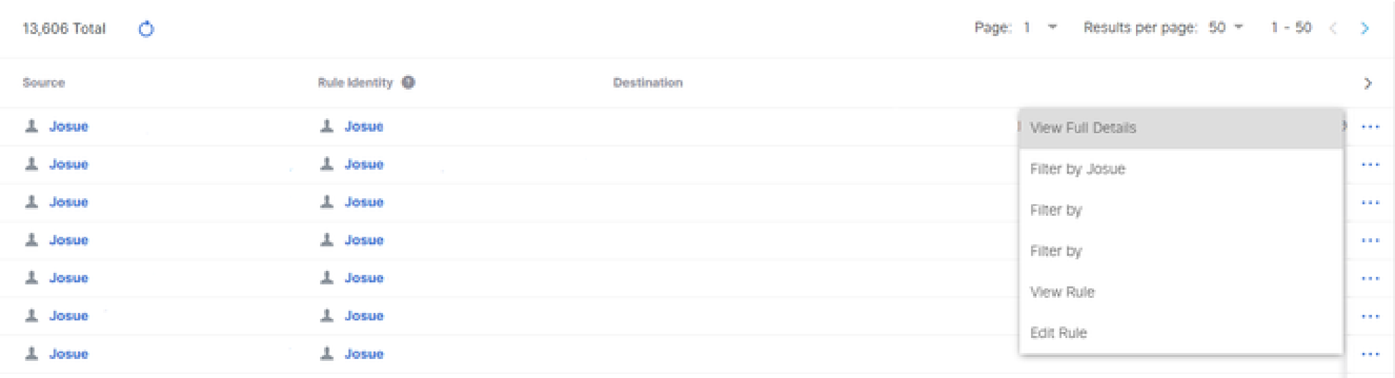
NTG Logs

Navigate to **Monitor** > **Activity Search**.



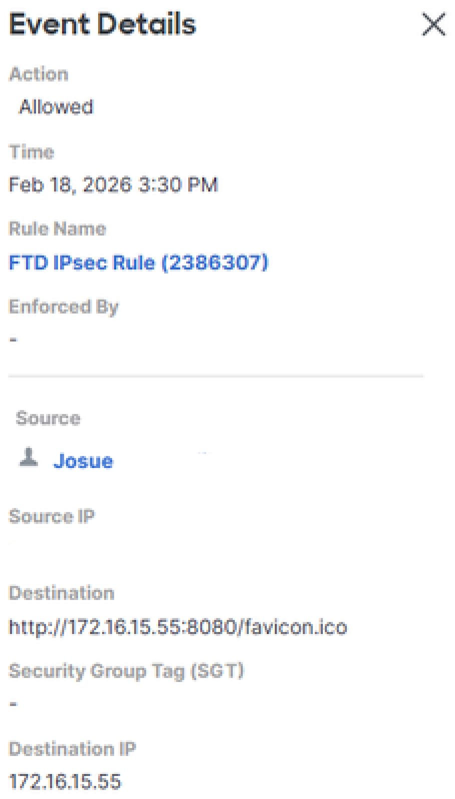
Monitor Conn Logs

On any of the related events, click on View Full Details.


13,606 Total | Page: 1 | Results per page: 50 | 1 - 50

Source	Rule Identity	Destination
Josue	Josue	
Josue	Josue	
Josue	Josue	
Josue	Josue	
Josue	Josue	
Josue	Josue	
Josue	Josue	

Full Details



Event Details

Action
Allowed

Time
Feb 18, 2026 3:30 PM

Rule Name
FTD IPsec Rule (2386307)

Enforced By
-

Source
Josue

Source IP

Destination
http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)
-

Destination IP
172.16.15.55

Activity Search

Related Information

- Cisco Technical Support & Downloads
- Cisco Secure Firewall Management Center Device Configuration Guide, 7.7