Configure Secure Access with Secure Firewall Threat Defense for Private Access with Policy Based Routing

Contents

Introduction

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

Prerequisites

Requirements

- Cisco Secure Access knowledge

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

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

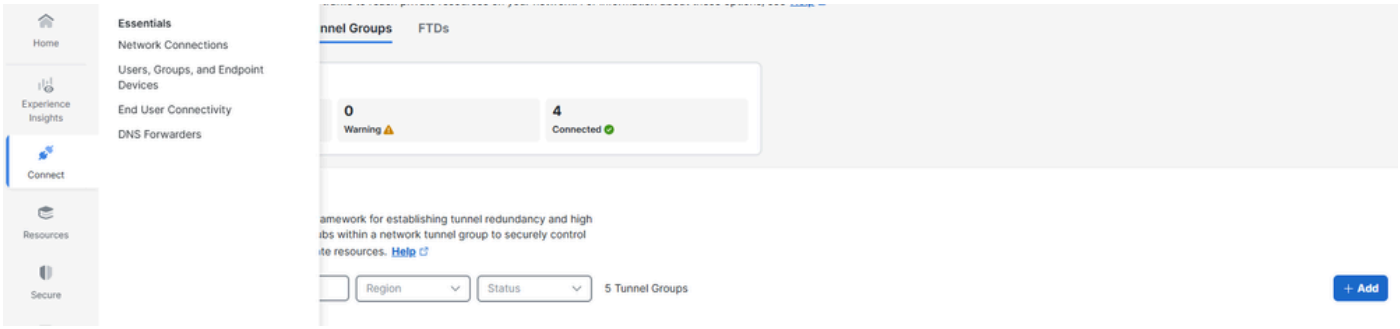
Secure Access Configuration

Network Tunnel Group Configuration

1. Navigate to the admin panel of Secure Access.

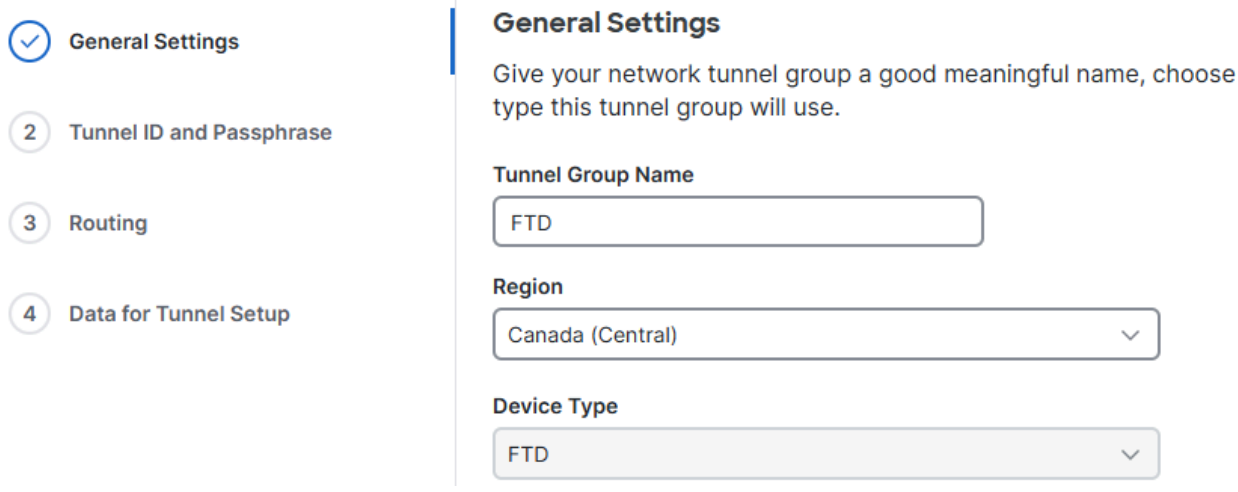
2. Add a Network Tunnel Group.

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



3. General Settings Configuration.

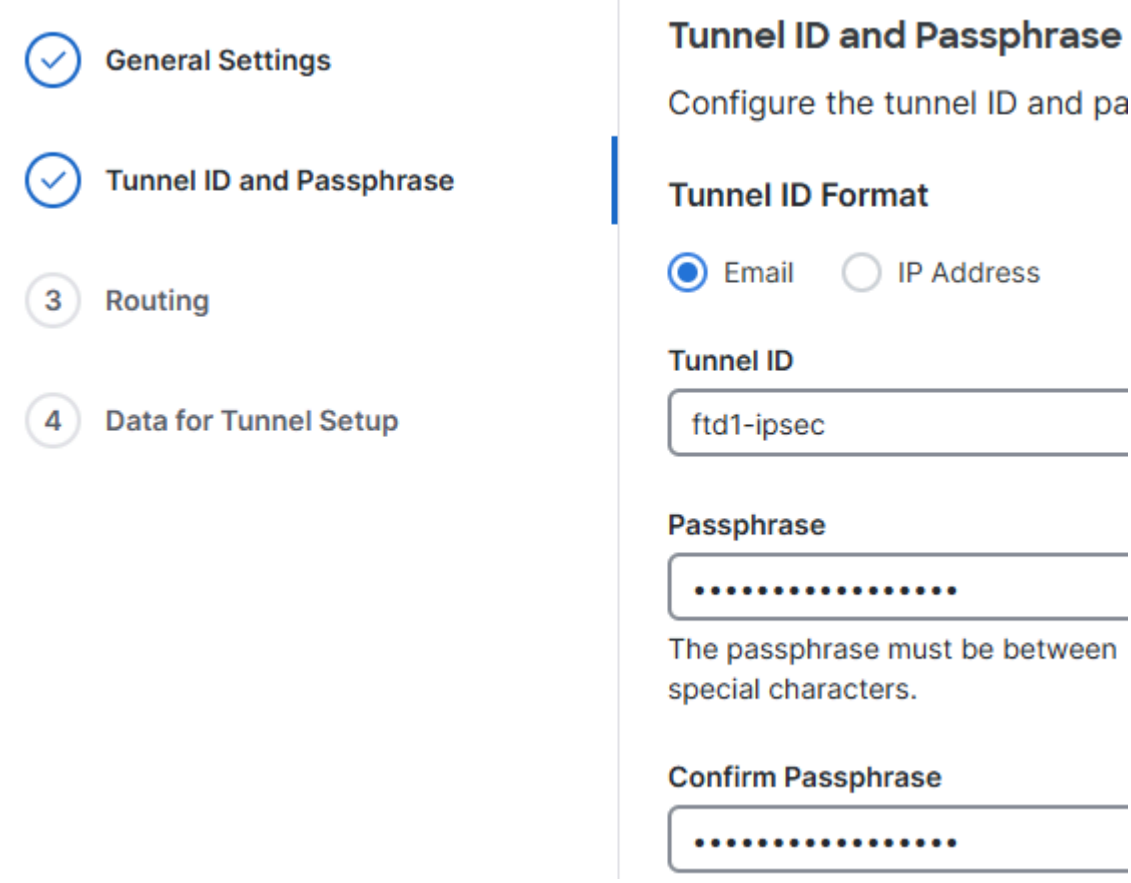
- Configure the Tunnel Group Name, **Region** and Device Type
  - Click Next



General Settings

4. Configure Tunnel ID and Passphrase.

- Configure the **Tunnel ID**and Passphrase. This ID is important, as it is required for the FTD configuration
- Click on Next



ID and PSK

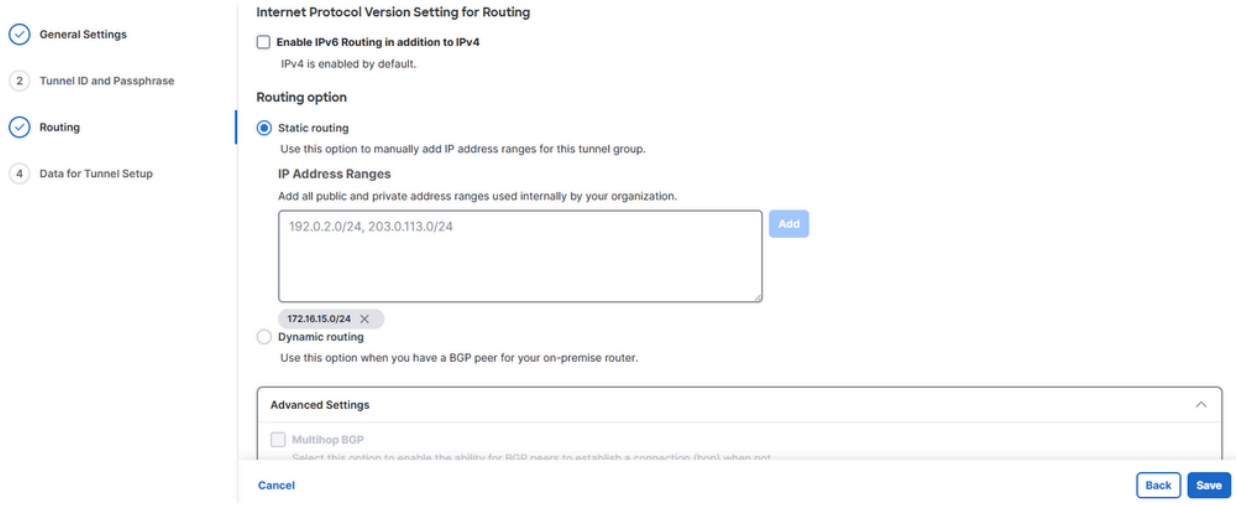
5. Configure Static Routing.

Secure Access Routing

Policy Based Routing

Add the network(s) protected by the FTD that you want remote users to access via ZTA and/or VPNaaS, and click on Save.

- Click on Routing> **Static routing**
  - Add the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access, and clickAdd
  - Click onSave

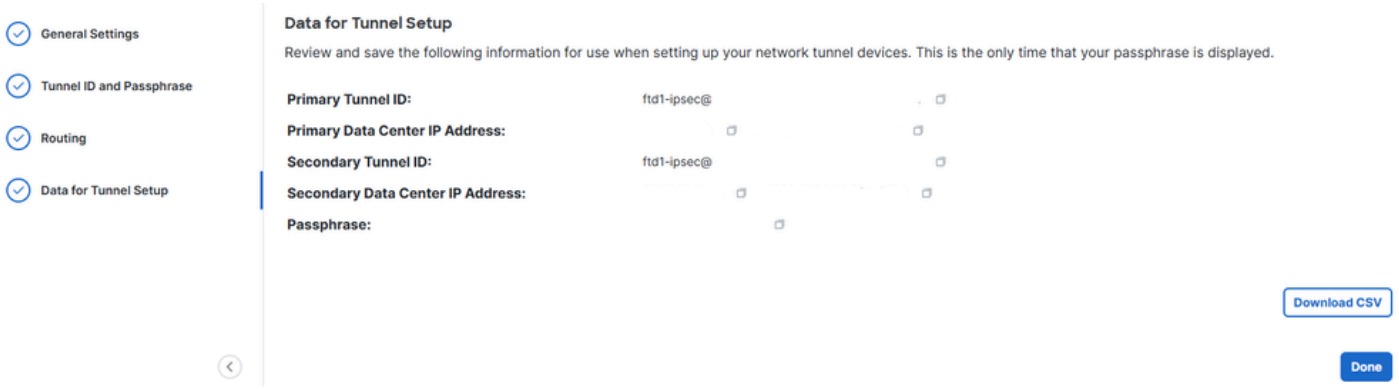


CSA Static Routing

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



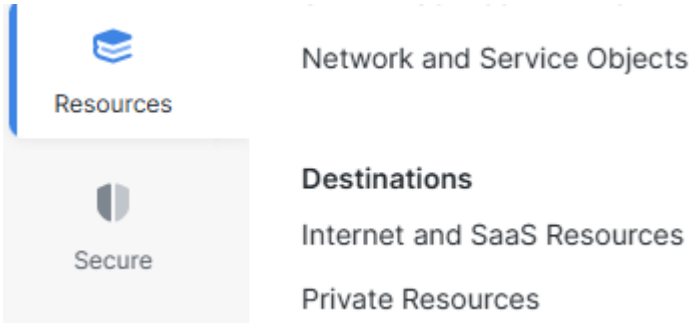
NTG Data

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.

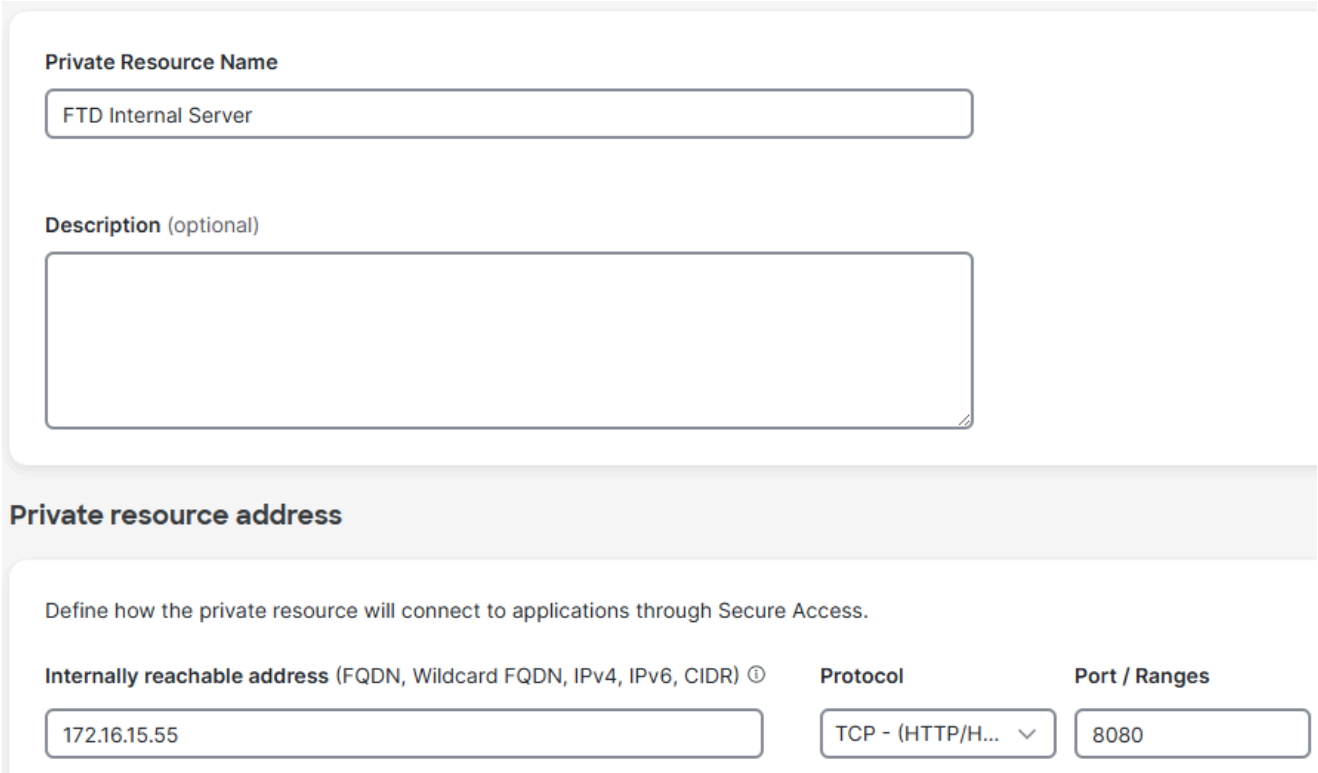
By defining them as Private Resources in Secure Access, you can enable controlled access through solutions like Zero Trust Access (ZTA) or VPN as a Service (VPNaaS). This ensures users can securely connect to internal systems based on identity, device posture, and access policies, without exposing the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



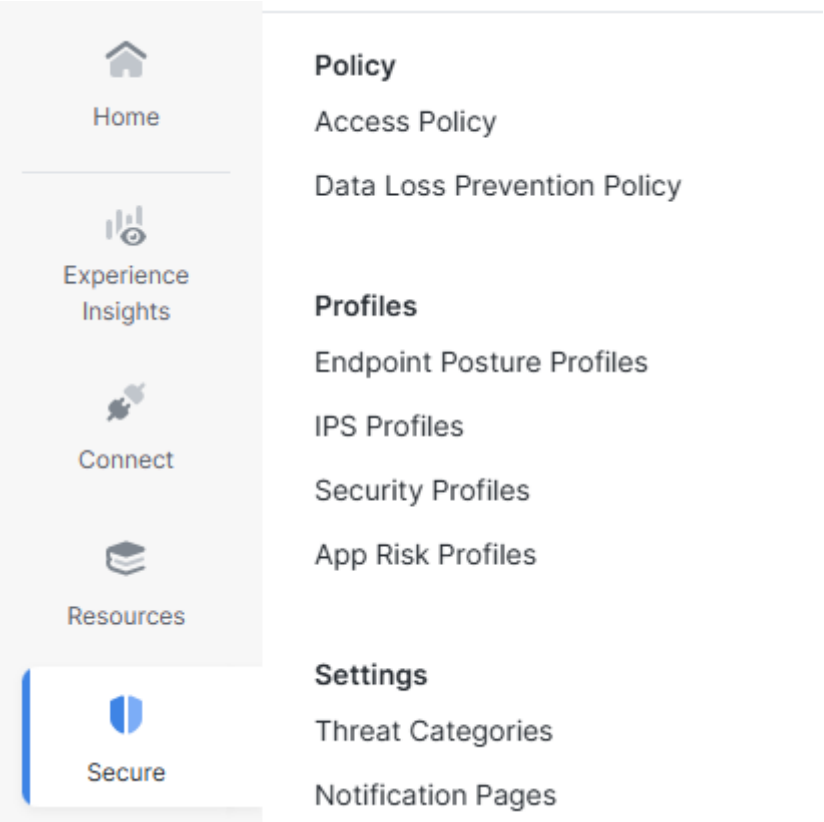
Private Resource

Create an Access Policy Rule

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

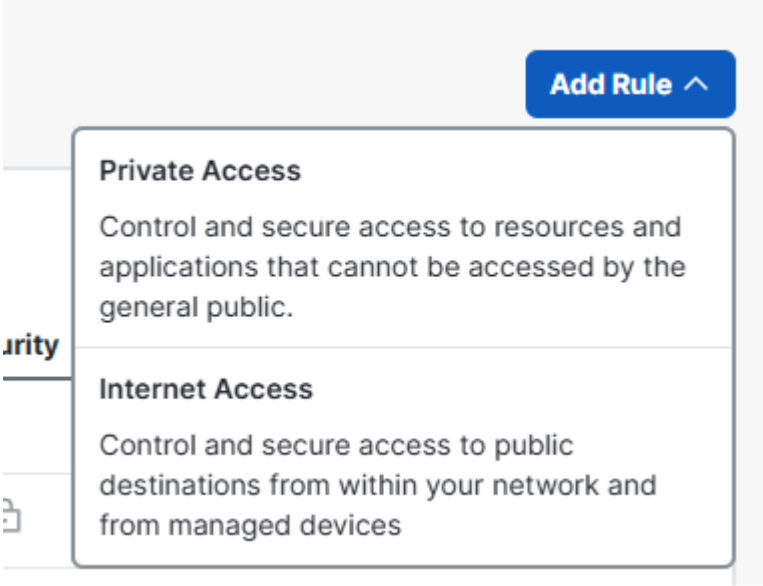
These rules enforce security by controlling who can access specific private resources based on factors such as user identity, group membership, device posture, location, or other policy conditions. This ensures that sensitive internal systems remain protected from general public access while still being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

Navigate to Secure>Access Policy



ACP

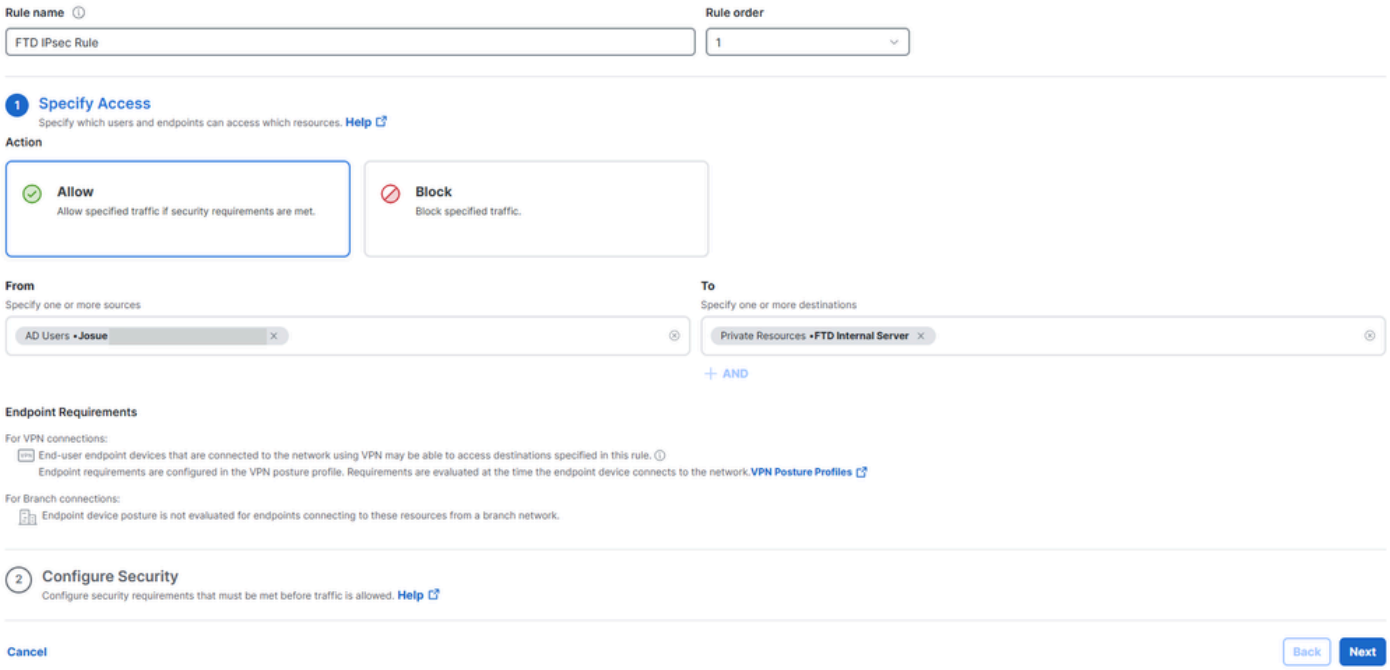
- Click on Add Rule
  - Click on Private Access



Add 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



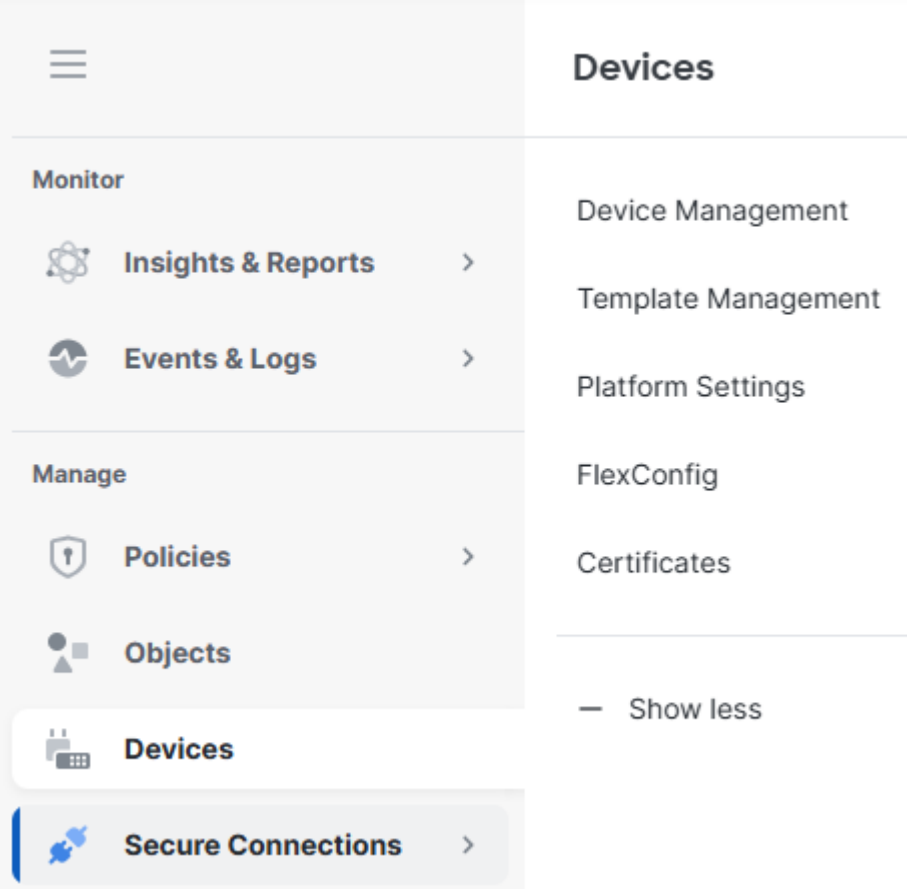
ACP config

Secure Firewall Threat Defense (FTD) Configuration

Virtual Tunnel Interfaces Configuration

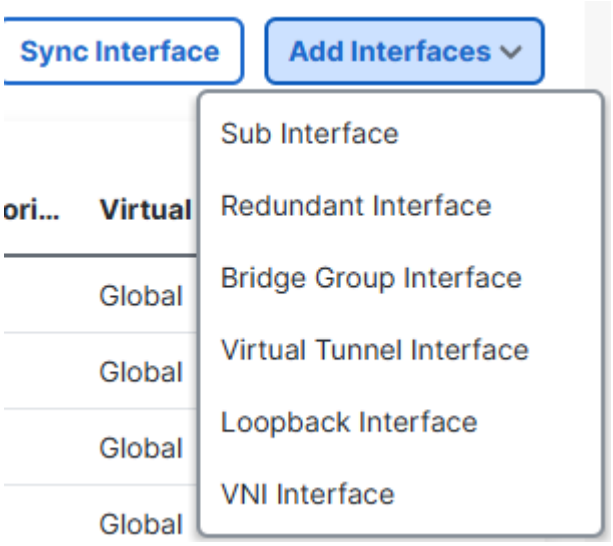
A Virtual Tunnel Interface (VTI) on FTD is a logical Layer 3 interface used to configure route-based IPsec VPN tunnels.

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

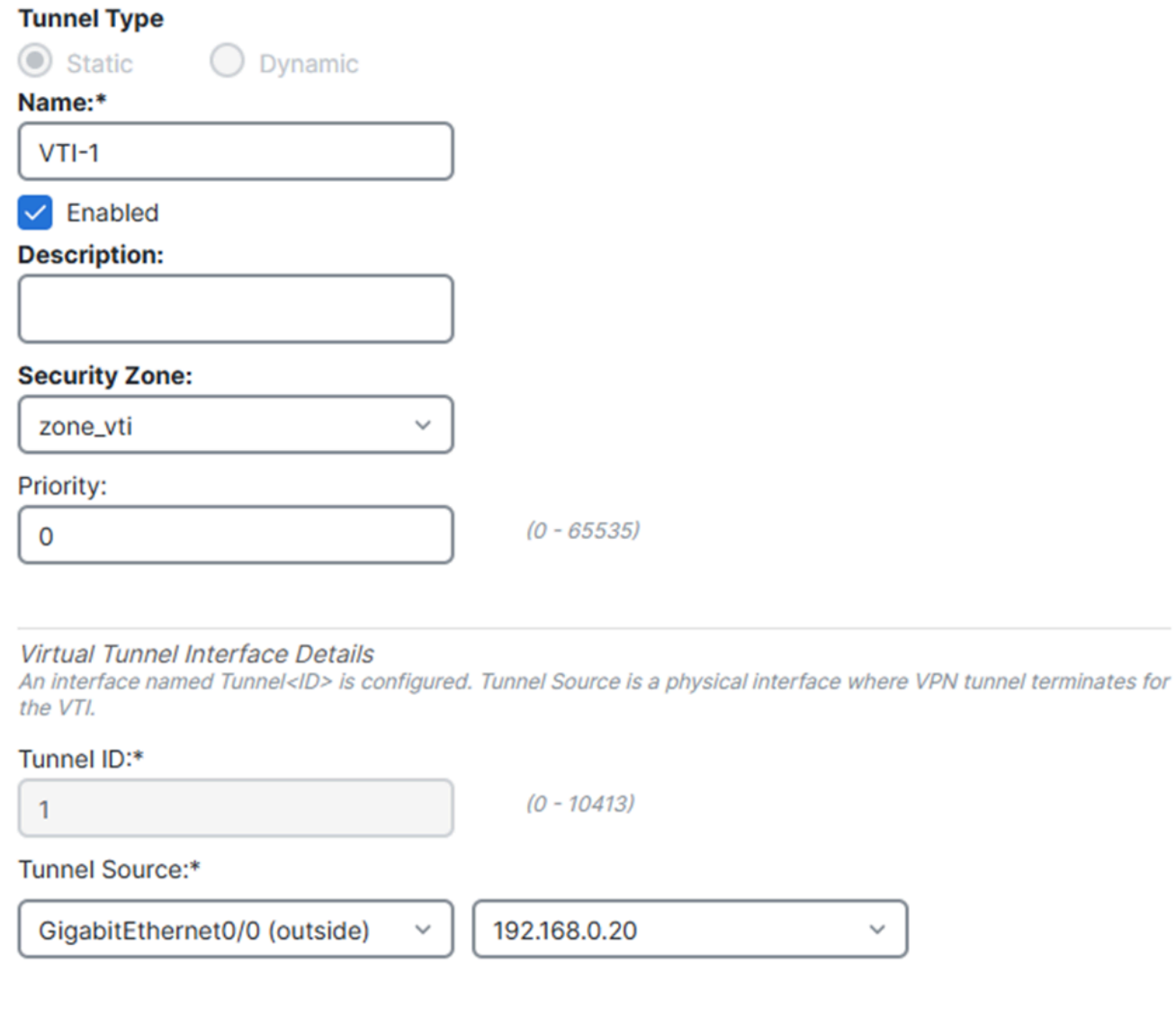


Add VTIs

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

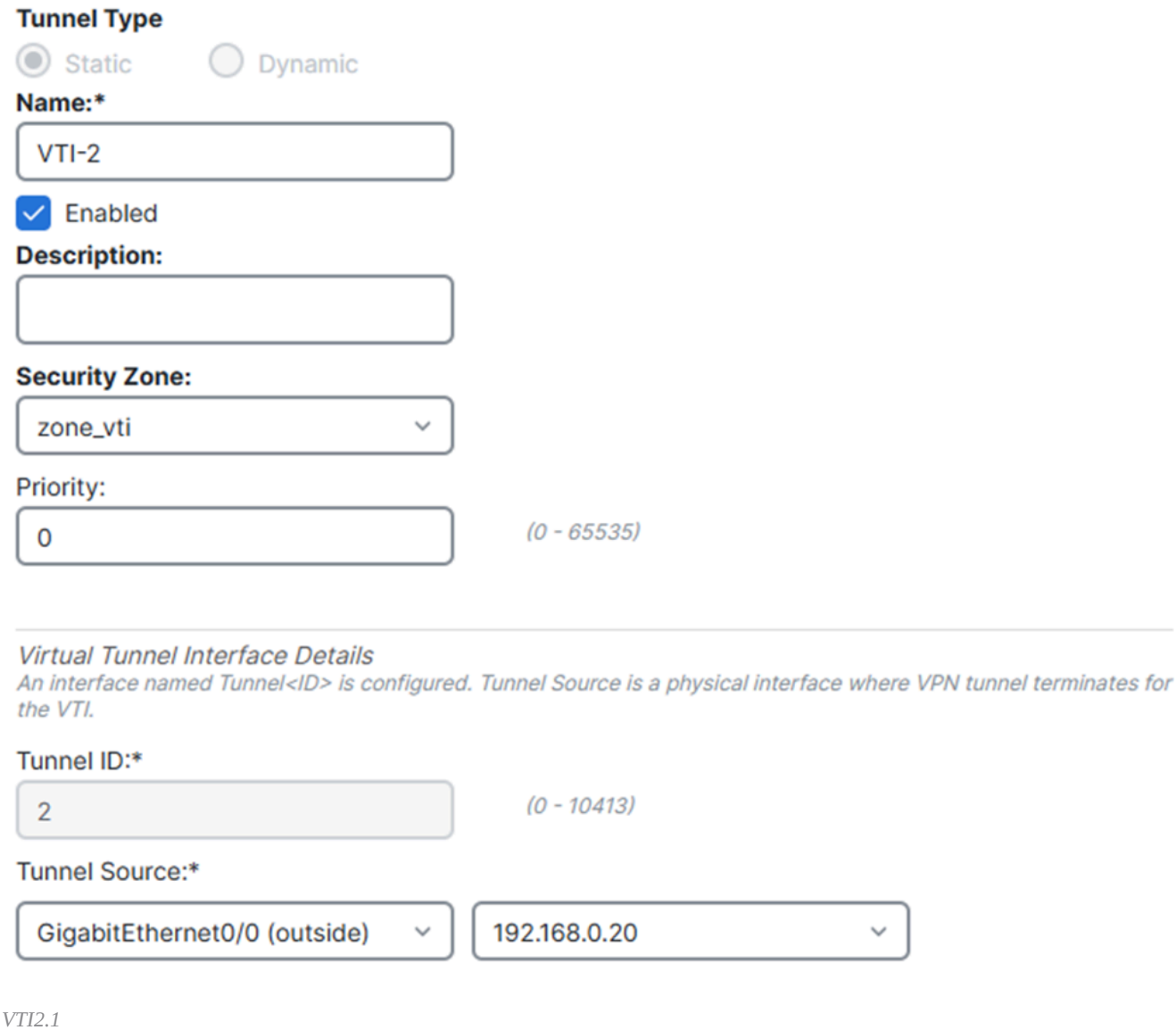


VTI1.1

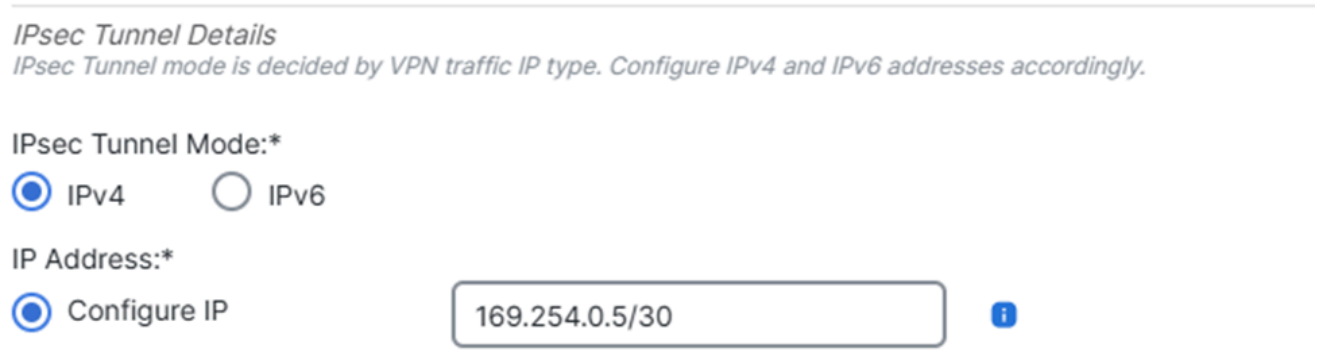
VTI1.2

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

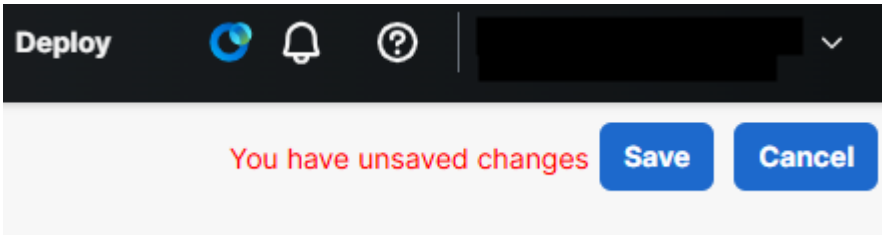


VTI2.1



VTI2.2

- Click on **Save**.

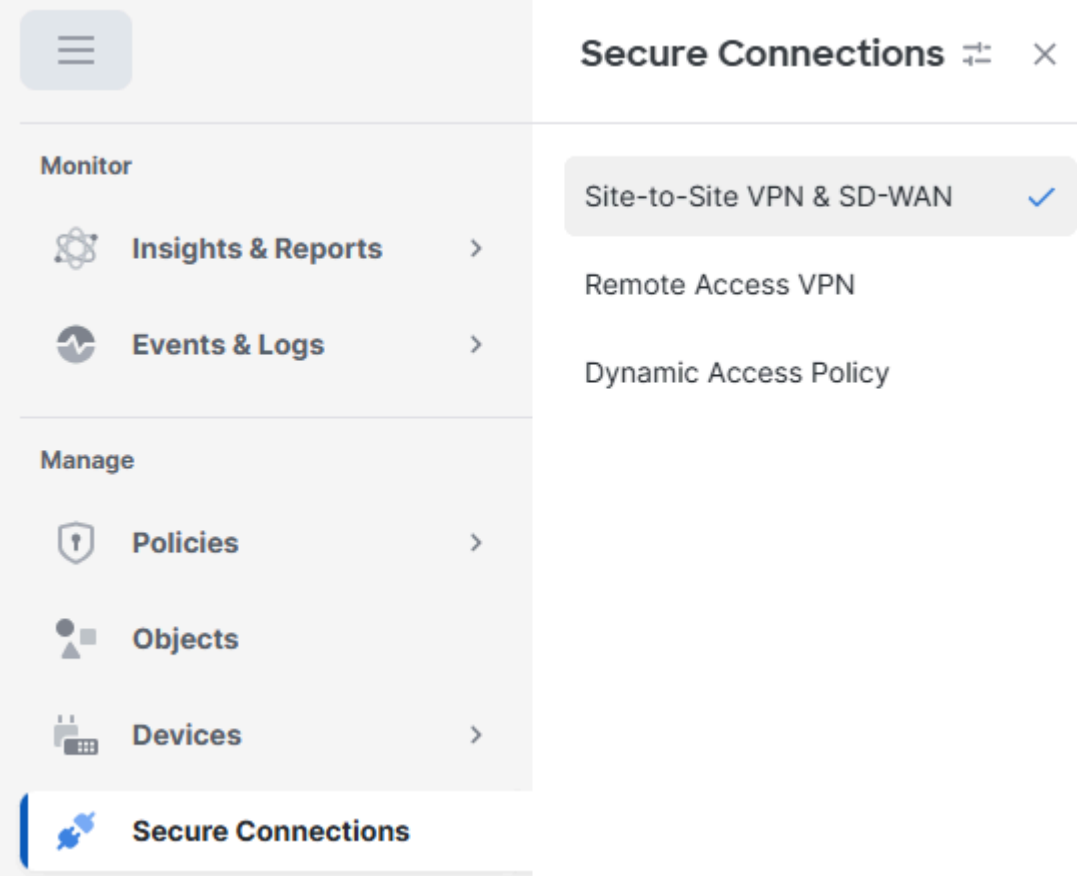


Save VTI Changes

IPsec Tunnel Configuration

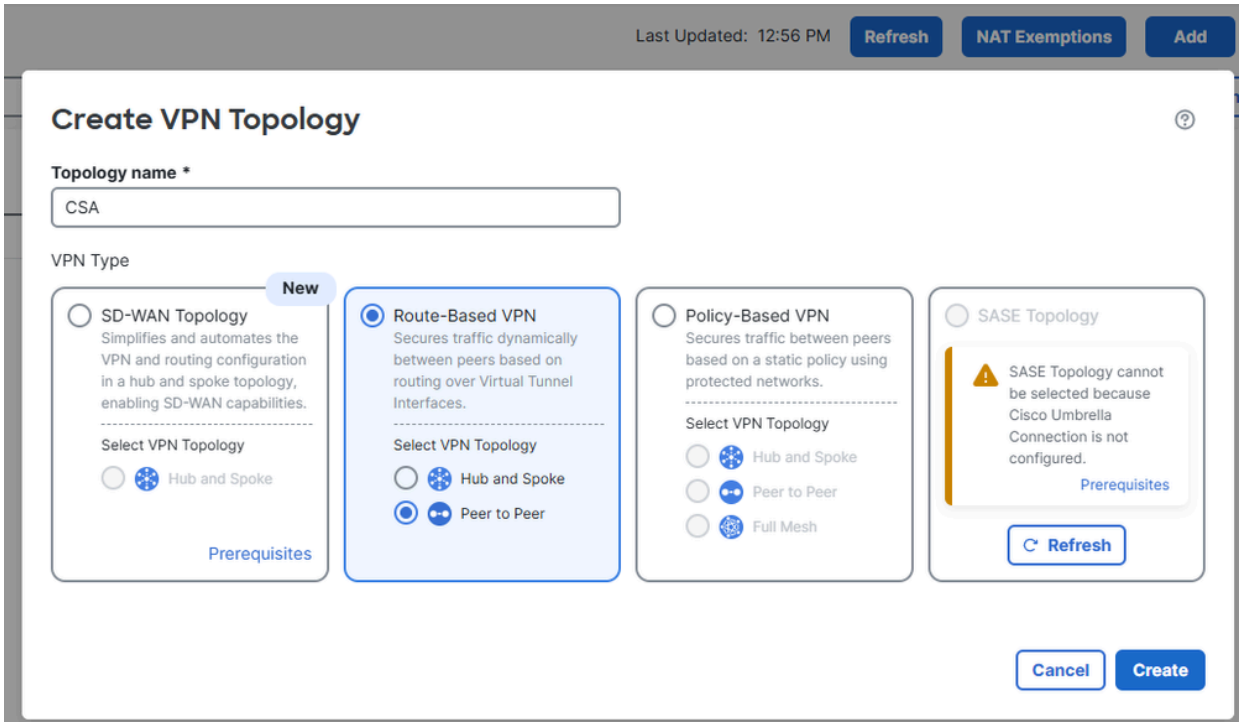
Navigate to your cdFMC dashboard.

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



S2S

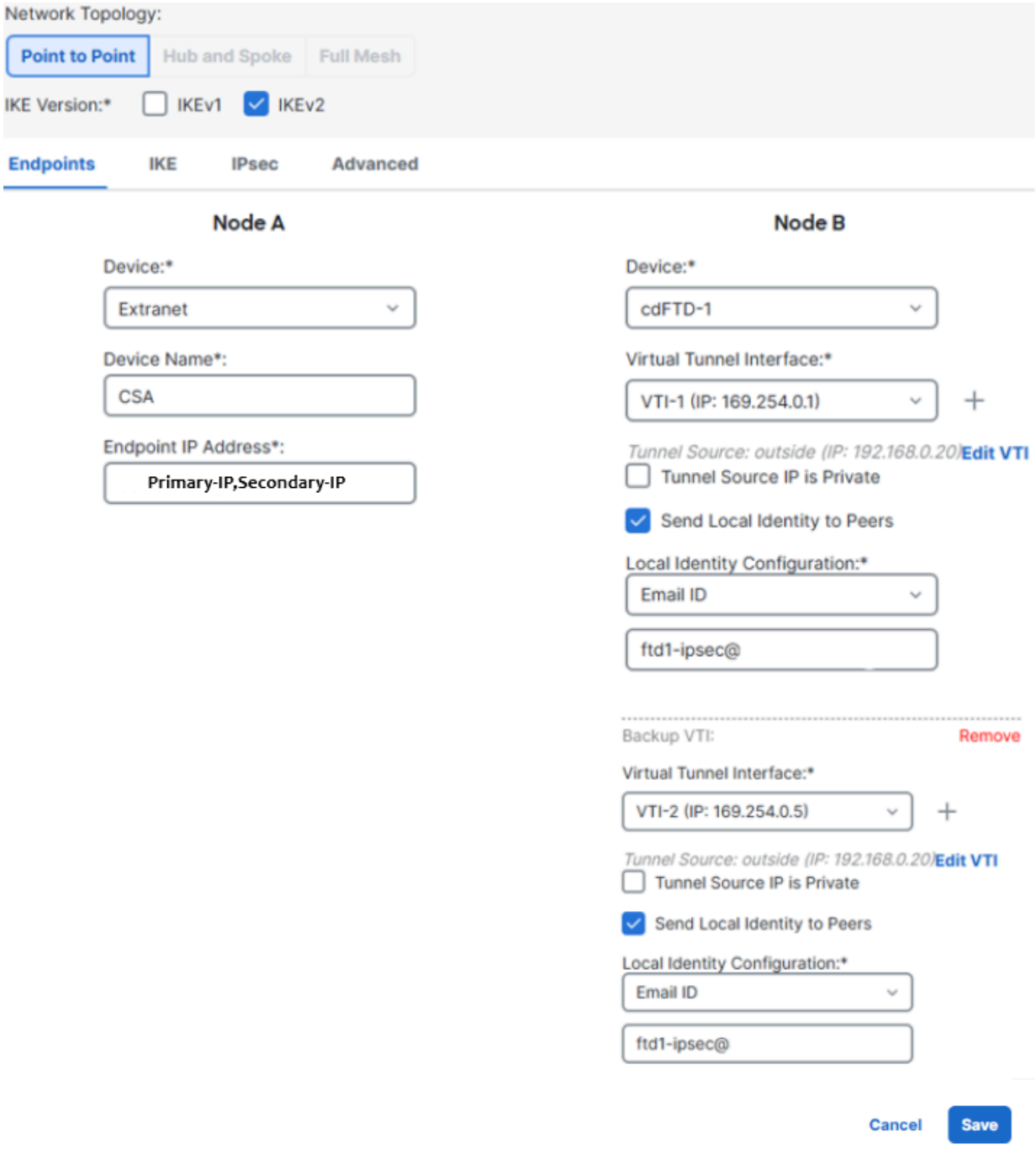
- Click on Add
  - Click on Route-Based VPN
  - Click on Peer to Peer



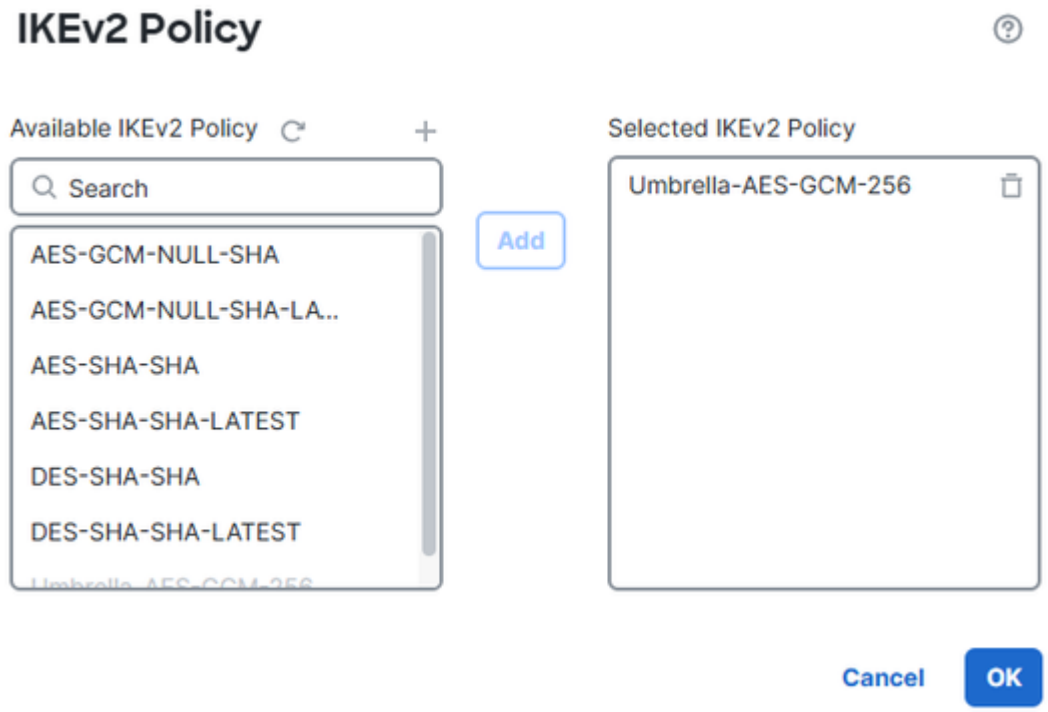
Add VPN

- From step 5 of the Secure Access configuration, obtain the tunnel IDs and IP addresses for the primary and secondary data centers

- Click on Endpoints
  - Under Node A, click on Device and select Extranet
  - Click on Device Name and 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 on Send Local Identity to Peers option and select Email ID, enter the secondary tunnel ID (from "Save Network Tunnel Group Configuration" under the Secure Access Configuration)
  - Click on **Save**

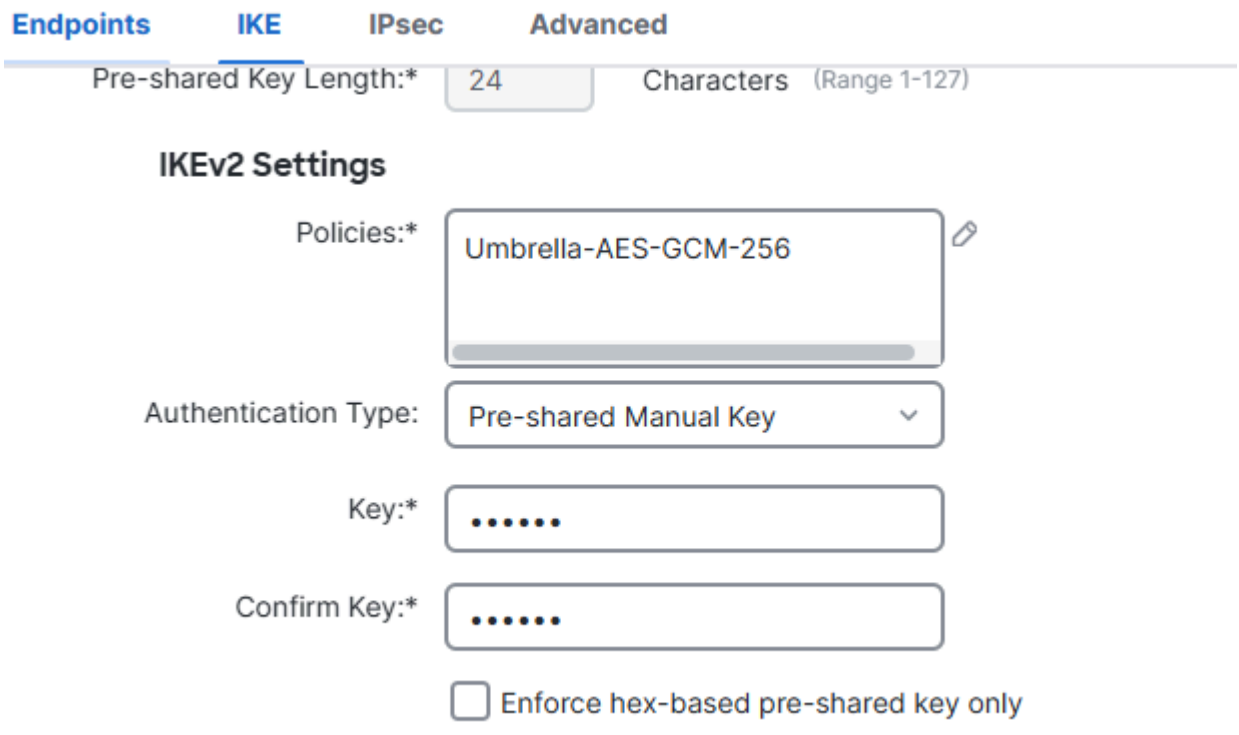


- Click onIKE
  - Click on **IKEv2 Settings** > Policies
  - Select the Umbrella-AES-GCM-256 option
  - Click on OK



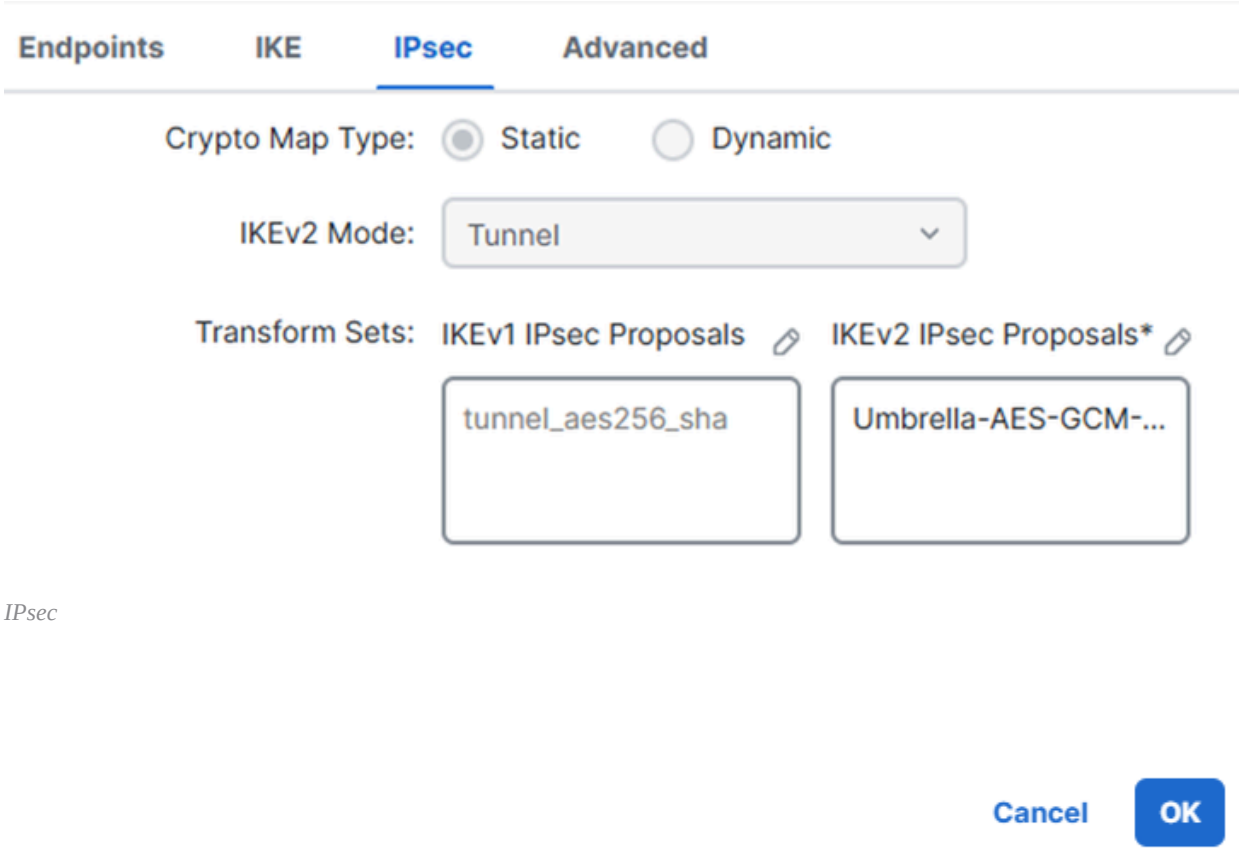
IKEv2 Policy

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



IKE

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



IPsec

Save IKEv2 Proposals

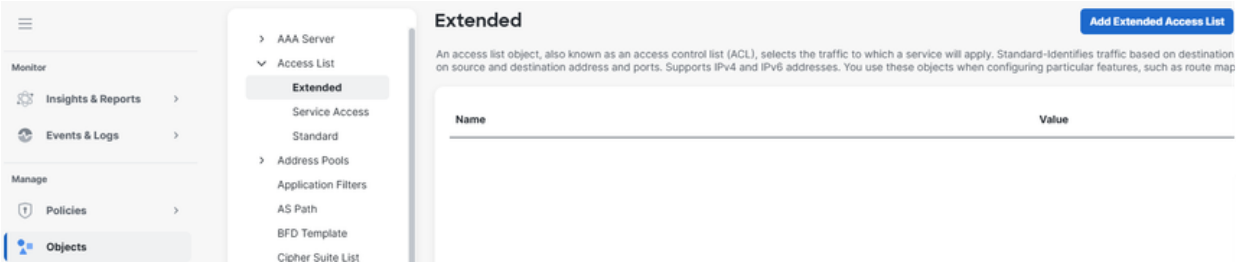
FTD Routing Configuration

Policy-Based Routing (PBR) allows you to control traffic forwarding based on criteria beyond just the destination IP address. Instead of relying solely on the routing table, PBR can route traffic based on source, application, protocol, ports, or other defined policies.

This enables organizations to steer specific or high-priority traffic over preferred links (such as a high-bandwidth or direct internet link), optimize performance, and securely break out selected applications without sending all traffic through a VPN tunnel.

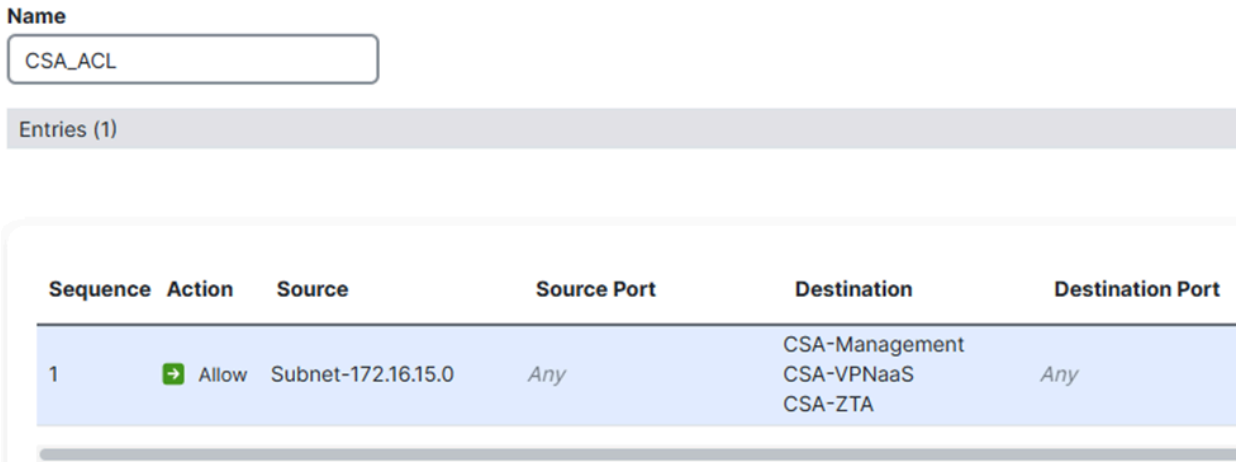
Policy-Based Routing

- Navigate toObjects
  - Click on Access List
  - Click on Extended
  - Click onAdd Extended Access List



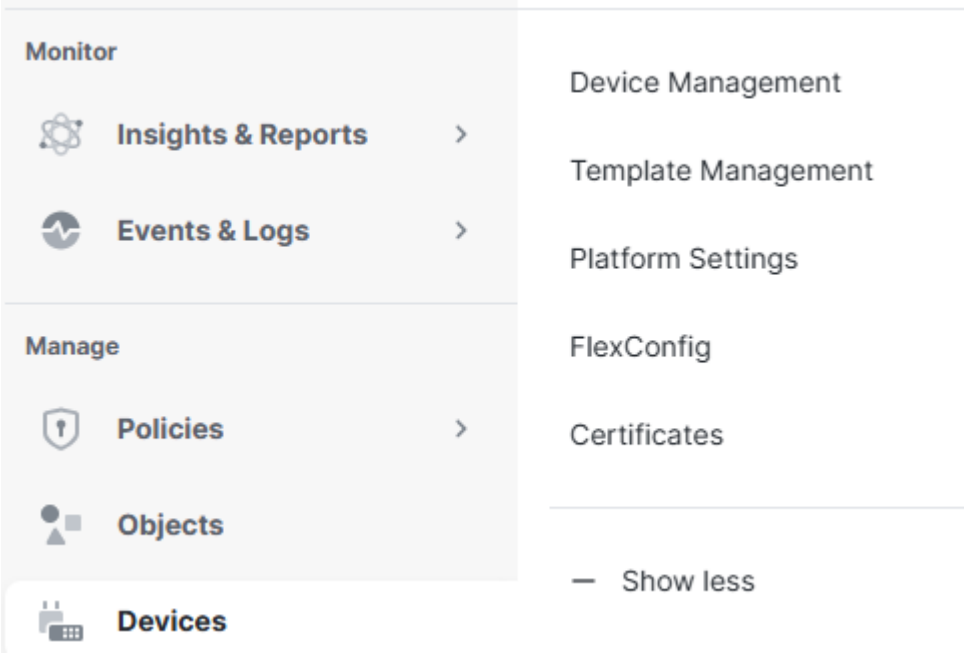
Add ACL

Create an extended access control list (ACL) that matches your source network protected by the FTD (for example, 172.16.15.0/24) to be sent through the tunnel. For the destination, add the networks used by ZTA (CGNAT range) and the network used by your VPNaaS (check Virtual Private Network IP Pool).



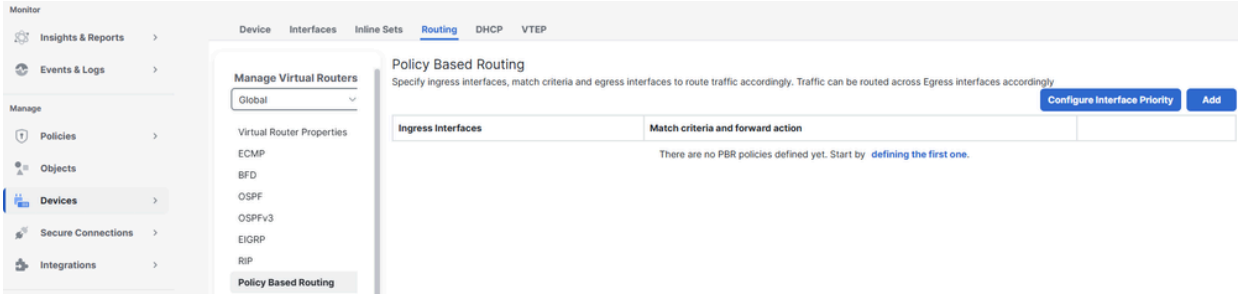
ACL

- Click on Devices> Device Management



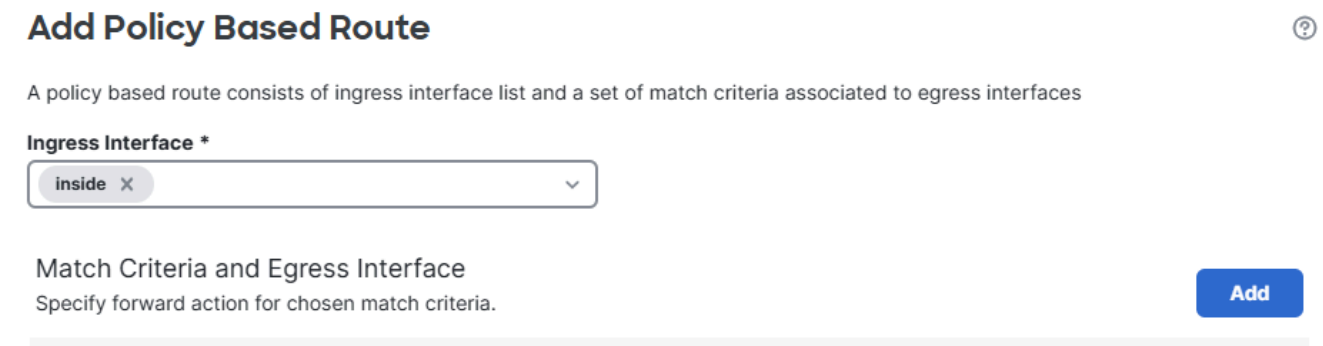
Device

- Click on the FTD
  - Click onRouting
  - Click on Policy Based Routing
  - Click on Add



Add PBR

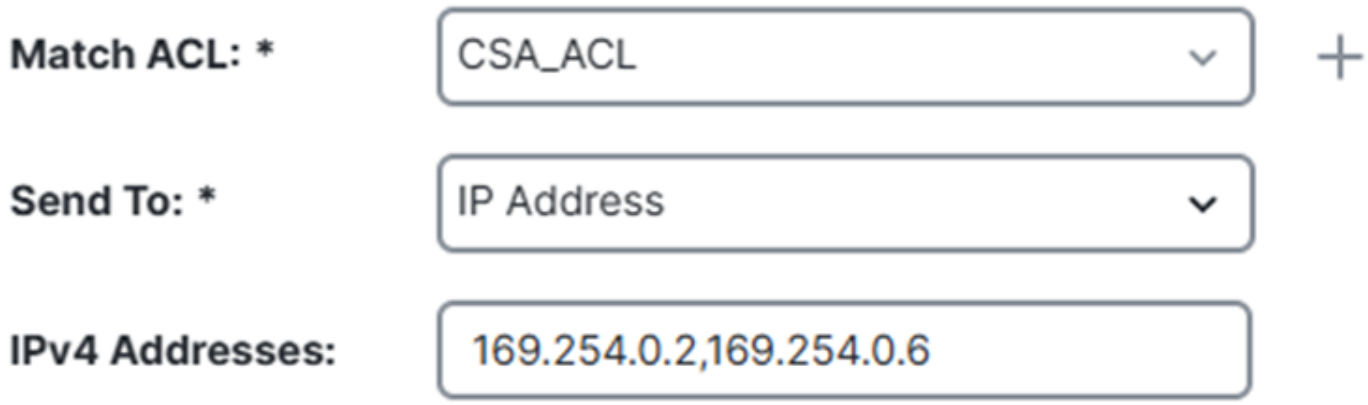
- Click on Ingress Interface and select the ingress interface where traffic from internal networks enters
- Under Match Criteria and Egress Interface click on Add



Ingress Interface

- Click on Match ACL and select the the extended ACL created earlier

- Click on Send To and select IP Address
- Click on IPv4 Addresses and set as next hops the IP addresses within the VTI interface subnets configured earlier in the FTD (169.254.0.2 and 169.254.0.6)
- Click on Save



Policy Based Config

Save PBR

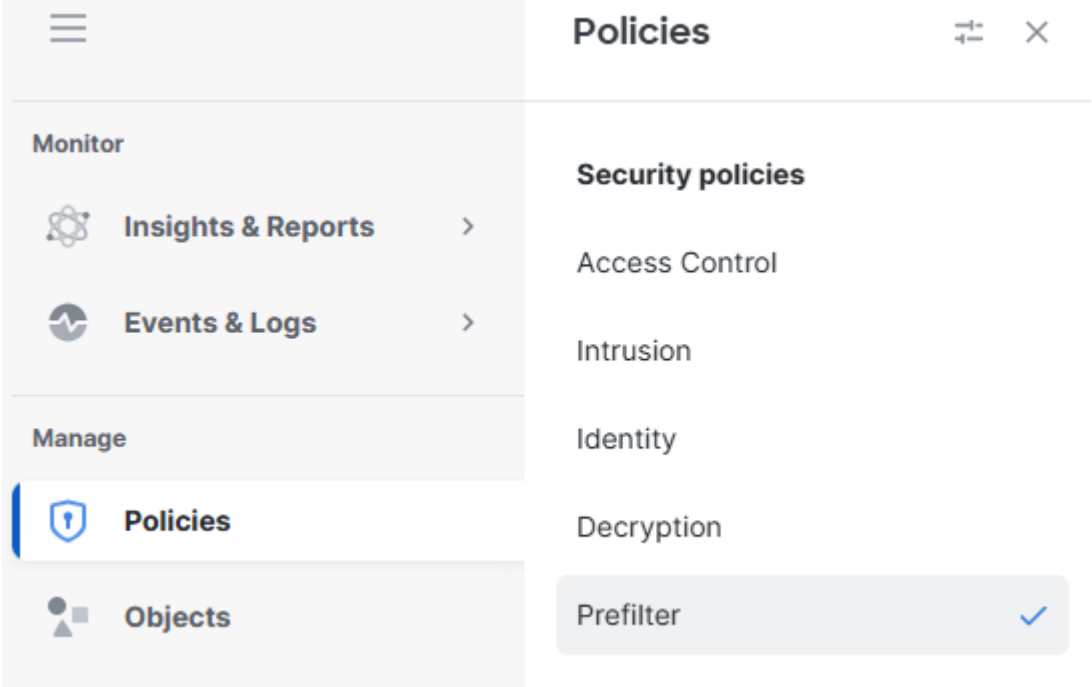
Make sure you select the Send To > IP Address option, and not the Egress Interface option.

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

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

Save Rule

At this point, once the configuration on the FTD has been completed and verified, you can proceed with the deployment. After deployment, the IPsec tunnels come up successfully, confirming that secure connectivity to the private resources is established.

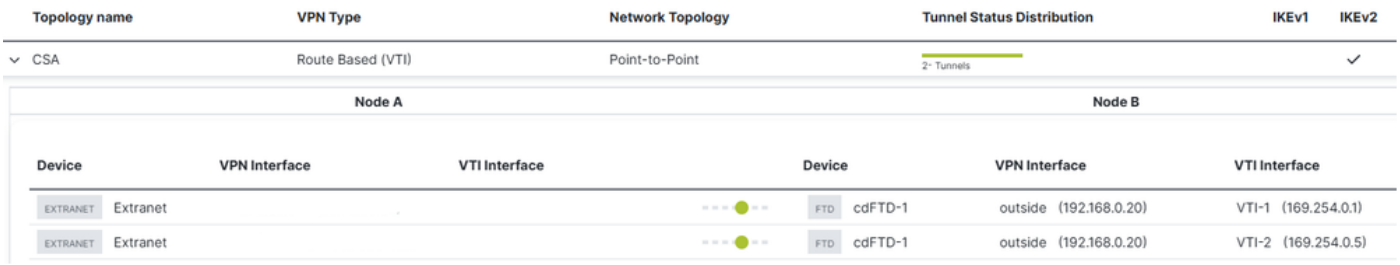
Verify

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**.



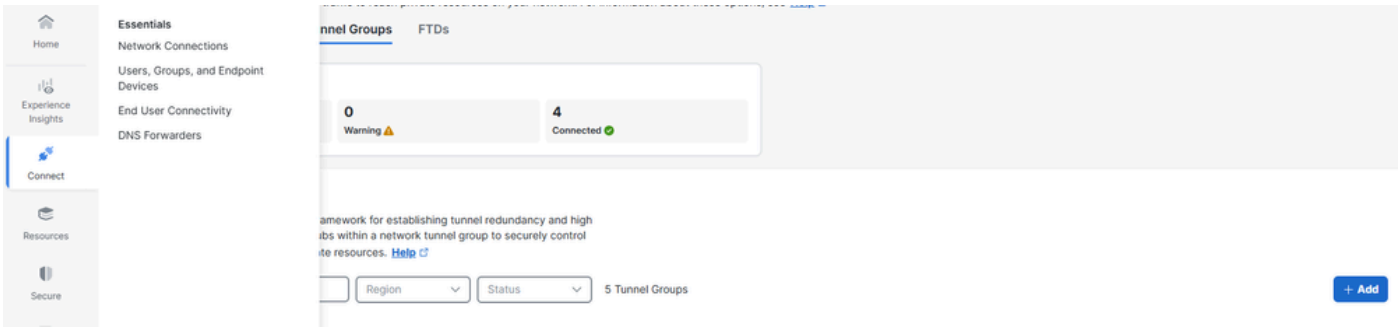
FTD Tunnel Status

Verify in Secure Access

Tunnel Status in Secure Access

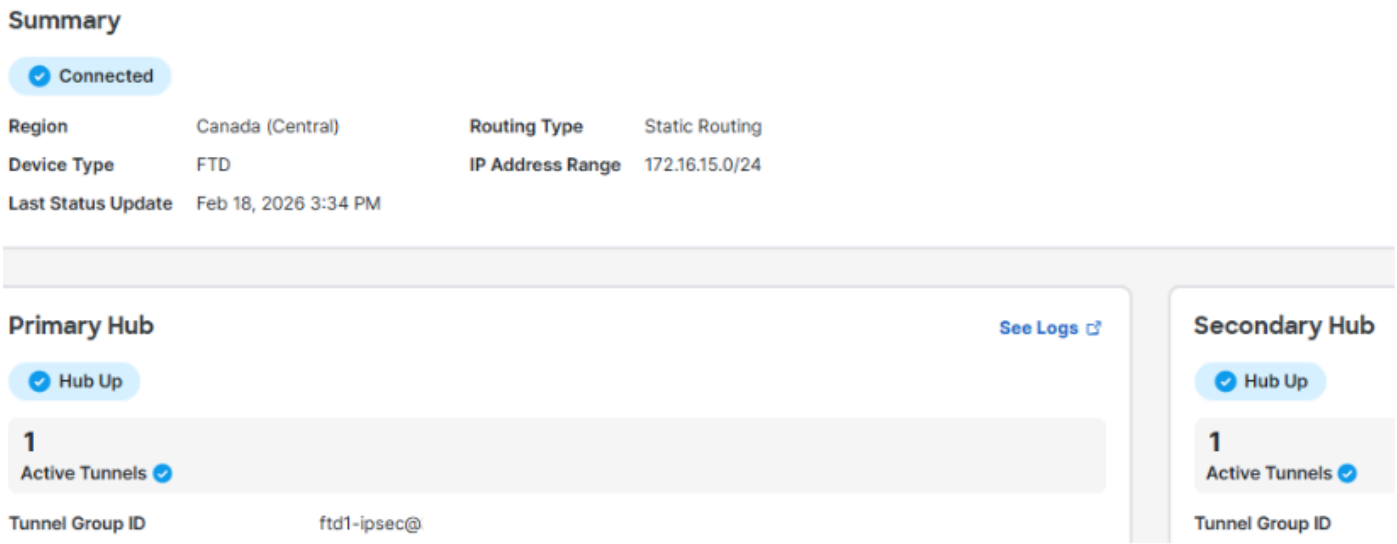
You can view the tunnel's current status, including whether it is Disconnected, Warnning or Connected. This helps verify that the IPsec tunnel is properly established.

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



Check NTG

- Click on the **Network Tunnel Group**

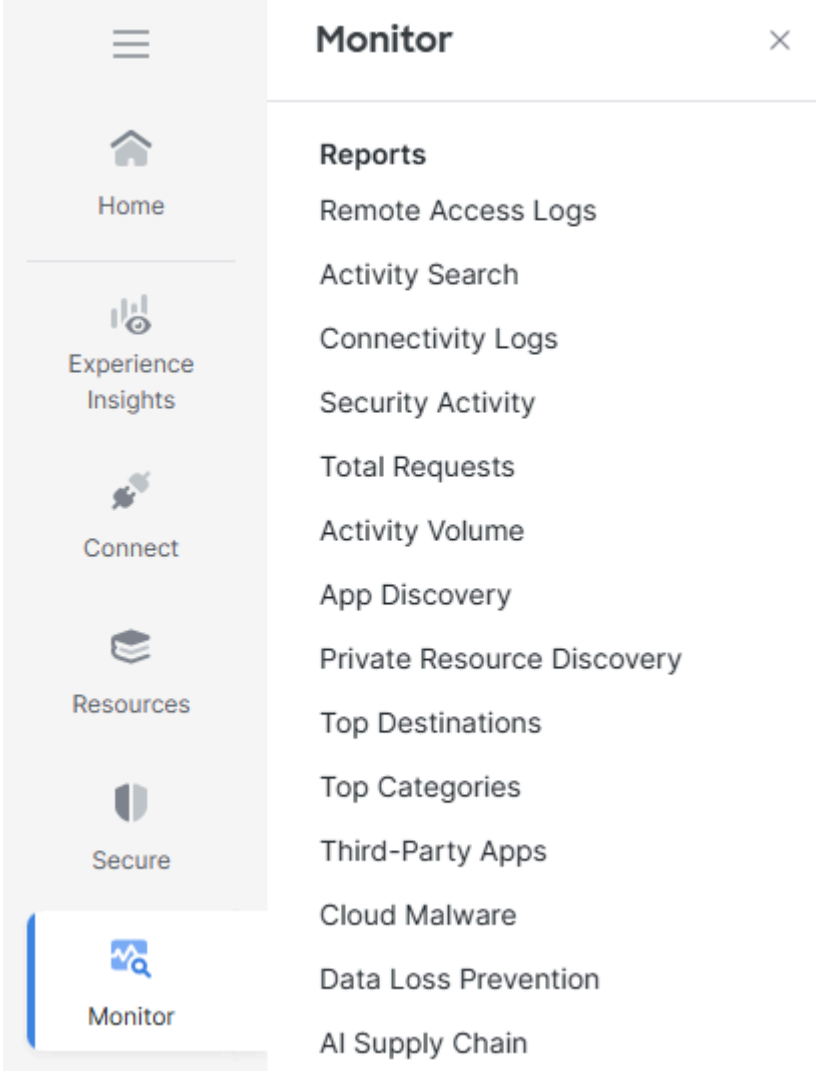


CSA Tunnel Status

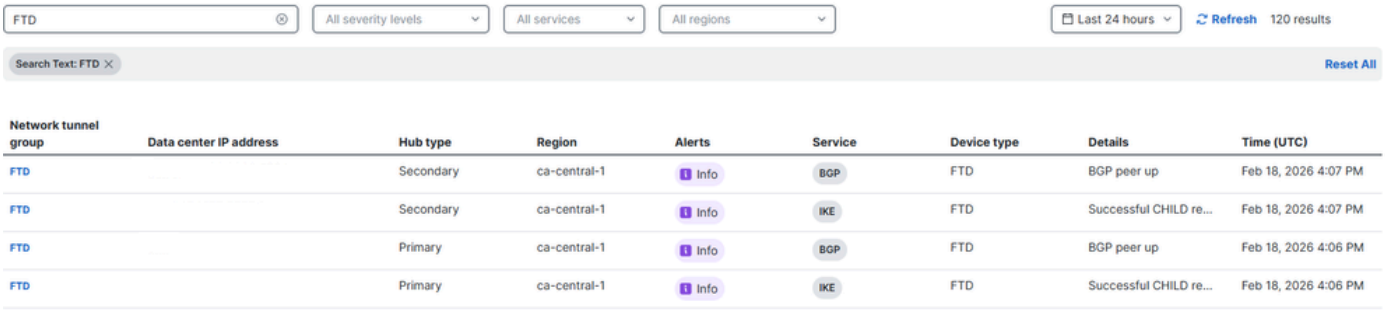
Events in Secure Access

You can view Tunnel events and confirm if the status of the IPsec tunnels is up and stable**.**

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

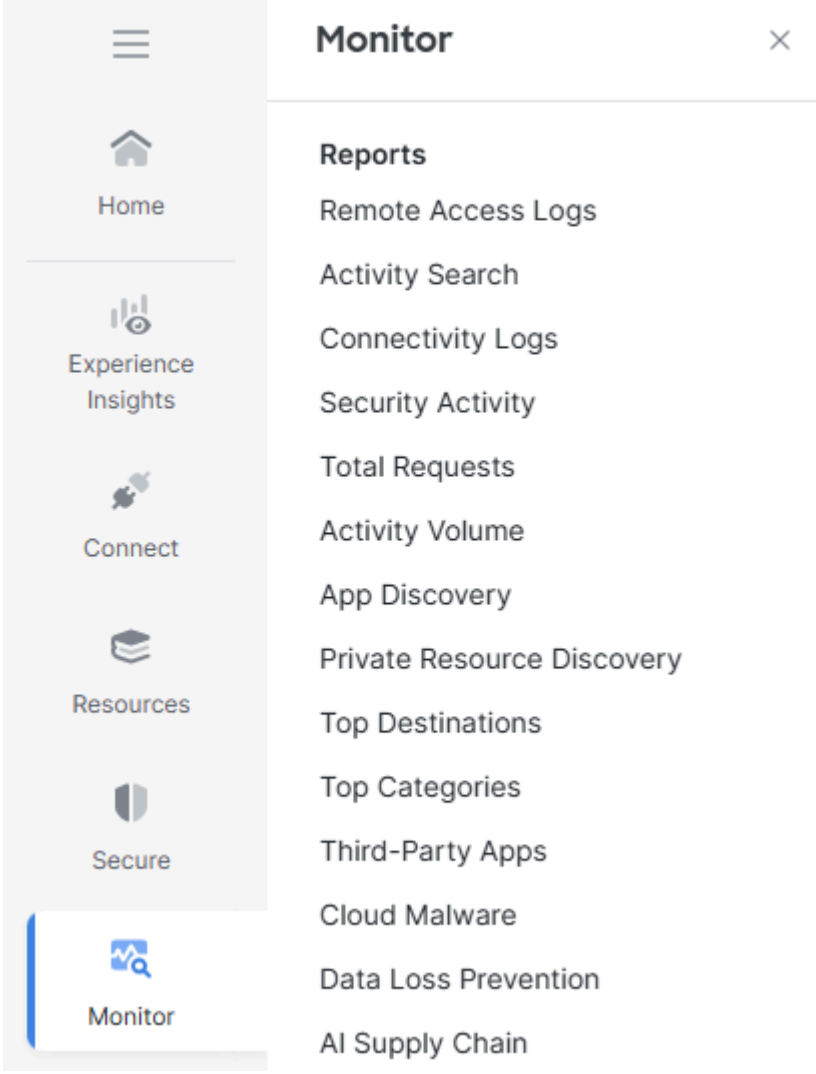


Monitor Conn Logs



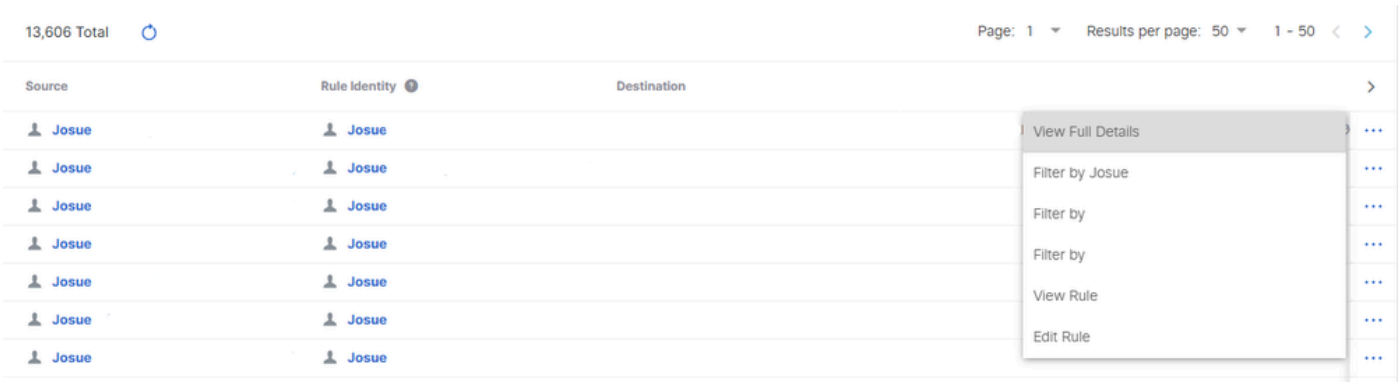
Conn Logs

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



Monitor Conn Logs

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



Full Details

Activity Search

Related Information

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