

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Secure Access Configuration](#)

[Network Tunnel Group Configuration](#)

[Secure Access Routing](#)

[Policy Based Routing](#)

[Save Network Tunnel Group Configuration](#)

[Create a Private Resource](#)

[Create an Access Policy Rule](#)

[Secure Firewall Threat Defense \(FTD\) Configuration](#)

[Virtual Tunnel Interfaces Configuration](#)

[IPsec Tunnel Configuration](#)

[FTD Routing Configuration](#)

[Policy-Based Routing](#)

[Access Policy Configuration](#)

[Verify](#)

[Verify in FTD](#)

[Tunnel Status in FTD](#)

[Verify in Secure Access](#)

[Tunnel Status in Secure Access](#)

[Events in Secure Access](#)

[Related Information](#)

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

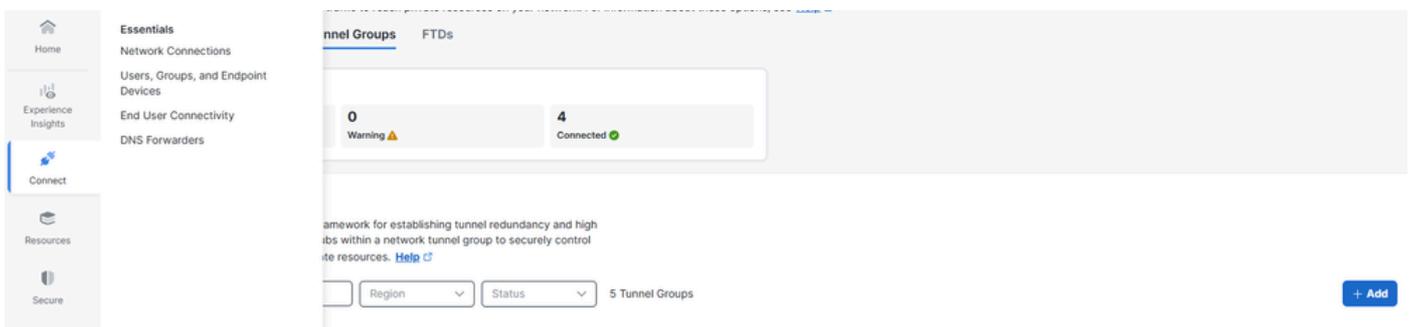
Network Tunnel Group Configuration

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**
- Tunnel ID and Passphrase
- Routing
- Data for Tunnel Setup

General Settings

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

Tunnel Group Name

Region

Device Type

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**

- ✓ 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 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 click Add
 - Click on Save

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

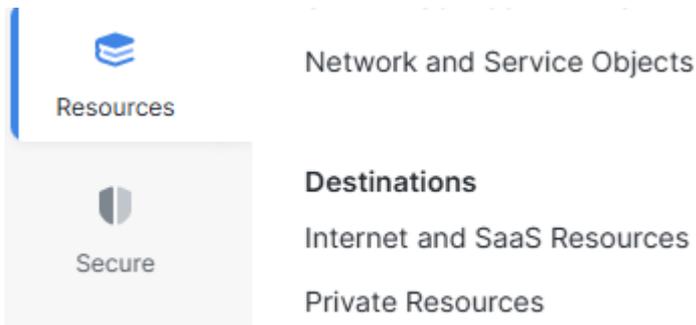
NTG Data

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 Name

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) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H... ▼)	8080

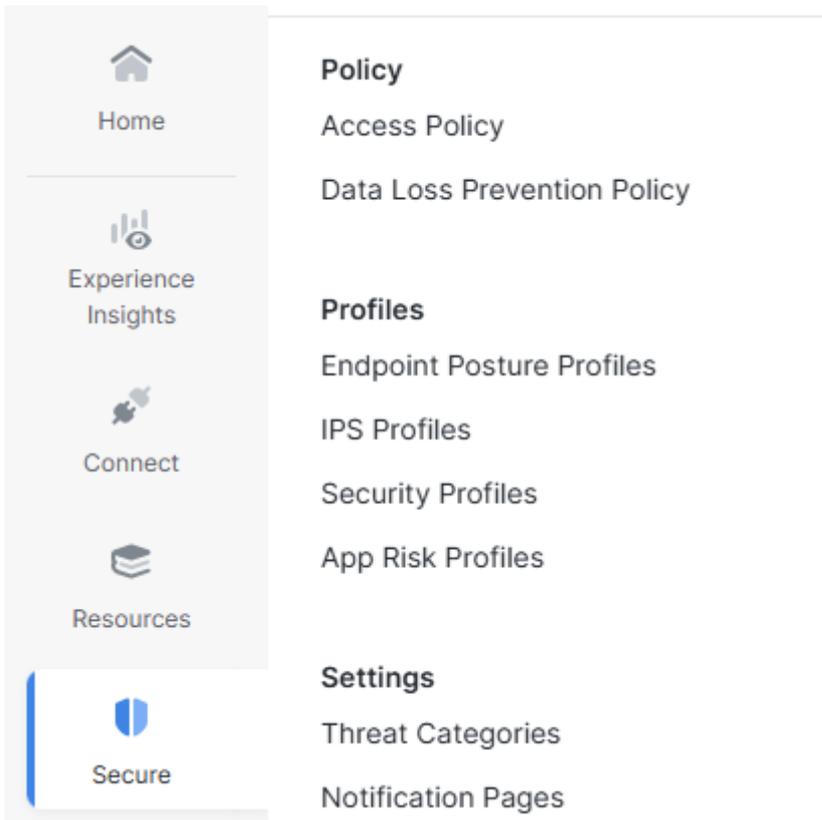
Private Resource

Create an Access Policy Rule

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

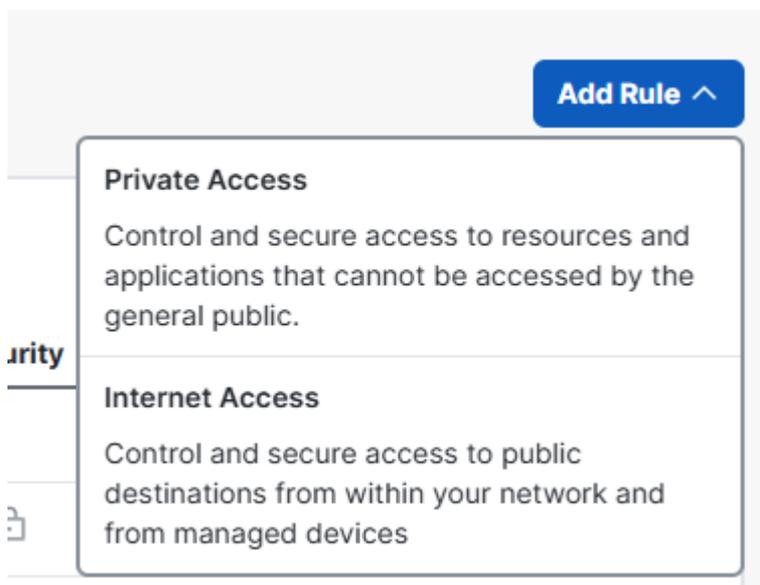
These rules enforce security by controlling who can access specific private resources based on factors such as user identity, group membership, device posture, location, or other policy conditions. This ensures that sensitive internal systems remain protected from general public access while still being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

Navigate to Secure>Access Policy



ACP

- Click on Add Rule
 - Click on Private Access



Add ACP

- Click on Rule Name and give it a name
- Click on Action, select Allow to permit this traffic
- Click on From and specify the users who are granted permission
- Click on To and specify the access those users have based on this rule

- Click on Next, and then Save in the next page

Rule name ⓘ Rule order

1 Specify Access
Specify which users and endpoints can access which resources. [Help](#) 🔗

Action

Allow
Allow specified traffic if security requirements are met.

Block
Block specified traffic.

From
Specify one or more sources

⊗

To
Specify one or more destinations

⊗

[+ AND](#)

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](#) 🔗

[Cancel](#) [Back](#) [Next](#)

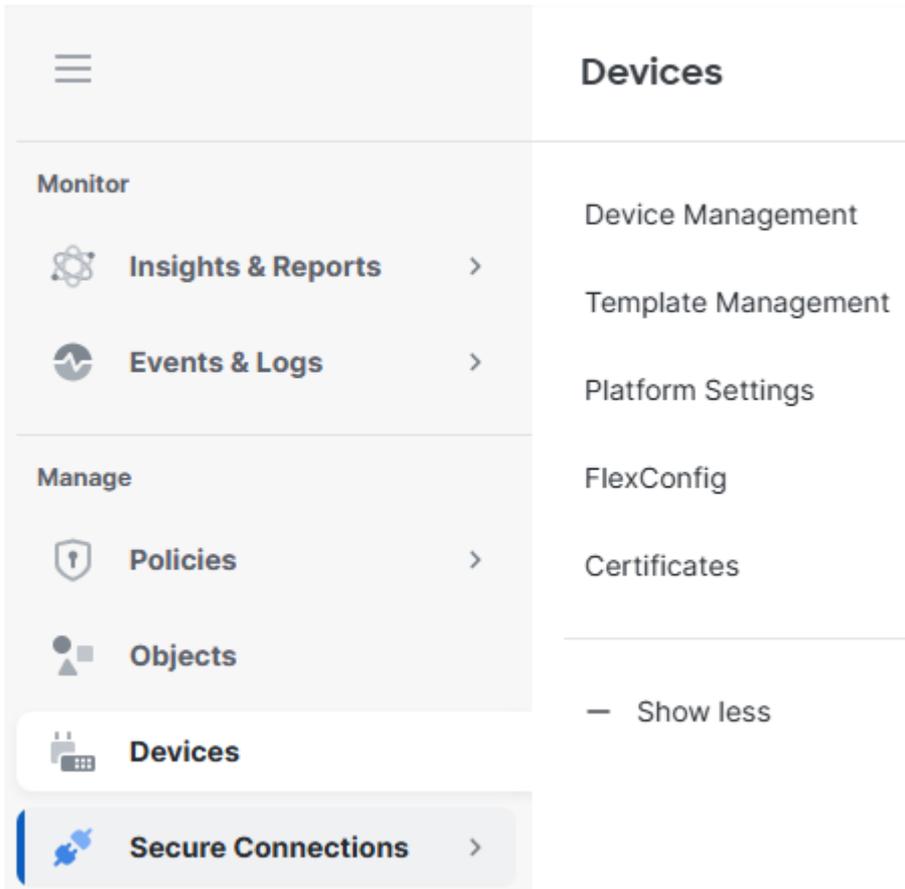
ACP config

Secure Firewall Threat Defense (FTD) Configuration

Virtual Tunnel Interfaces Configuration

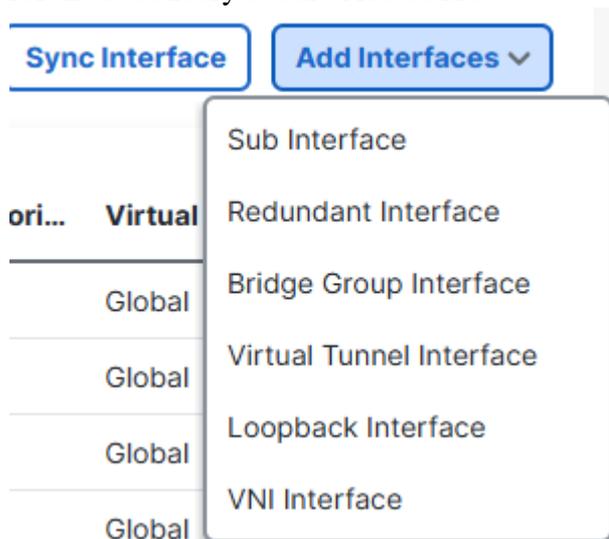
A Virtual Tunnel Interface (VTI) on FTD is a logical Layer 3 interface used to configure route-based IPsec VPN tunnels.

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, select IPv4
- Click on IP Address and configure the IP address for the VTI
- Click on OK

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

VTI.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



VTI.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, select IPv4
- Click on IP Address and configure the IP address for the VTI
- Click on OK

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:*

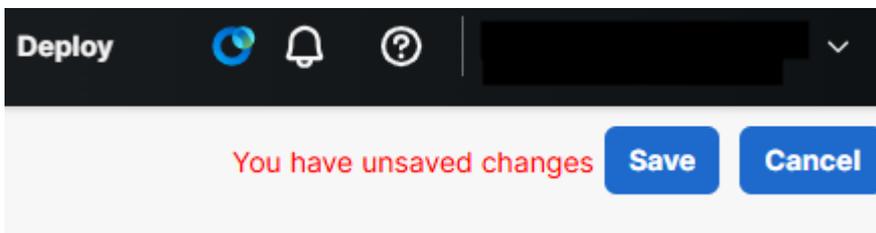
Configure IP

169.254.0.5/30



VTI2.2

- Click on **Save**.

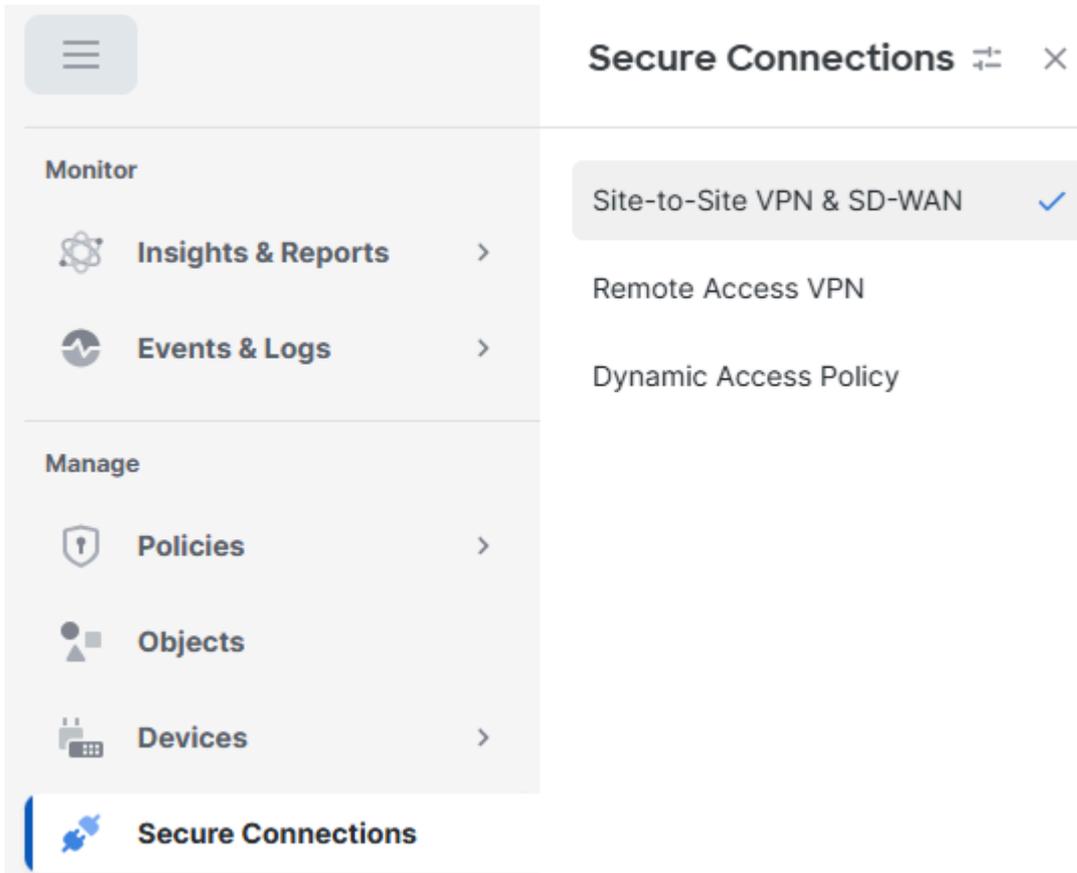


Save VTI Changes

IPsec Tunnel Configuration

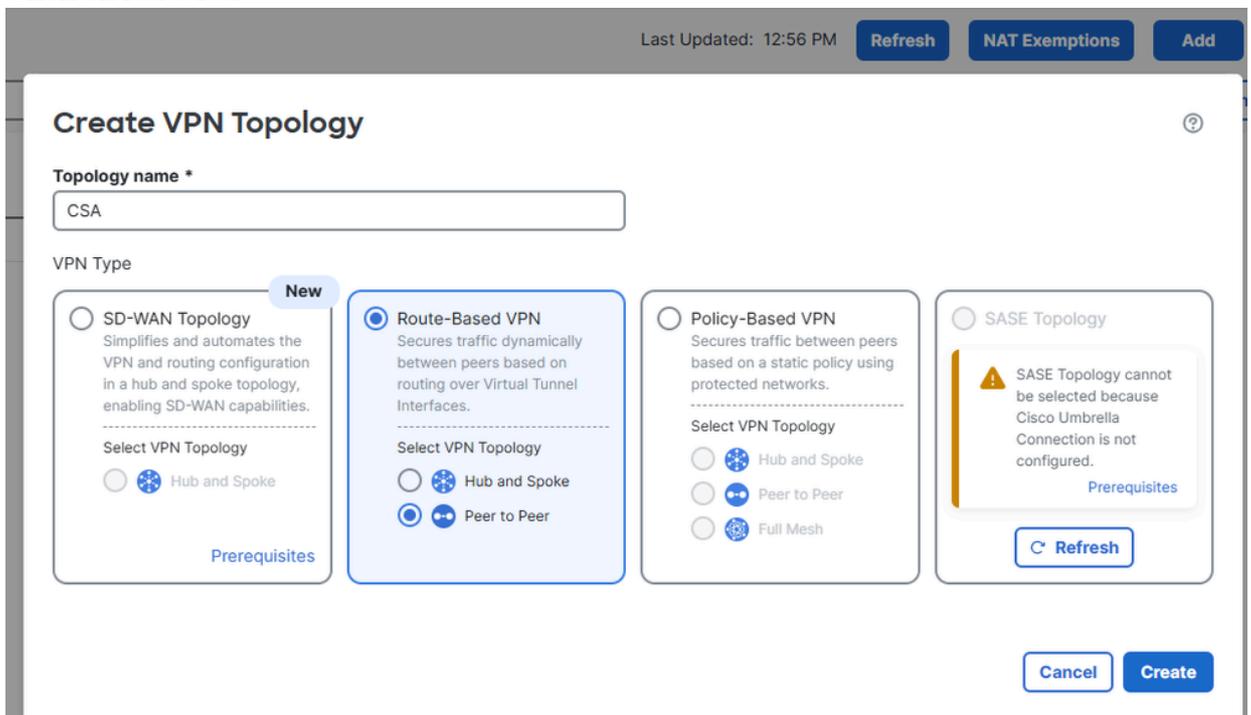
Navigate to your cdFMC dashboard.

- 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 Endpoint 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**

Network Topology:

IKE Version:* IKEv1 IKEv2

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

Node A

Device:*

Device Name*:

Endpoint IP Address*:

Node B

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration*:

Backup VTI: [Remove](#)

Virtual Tunnel Interface*
 +

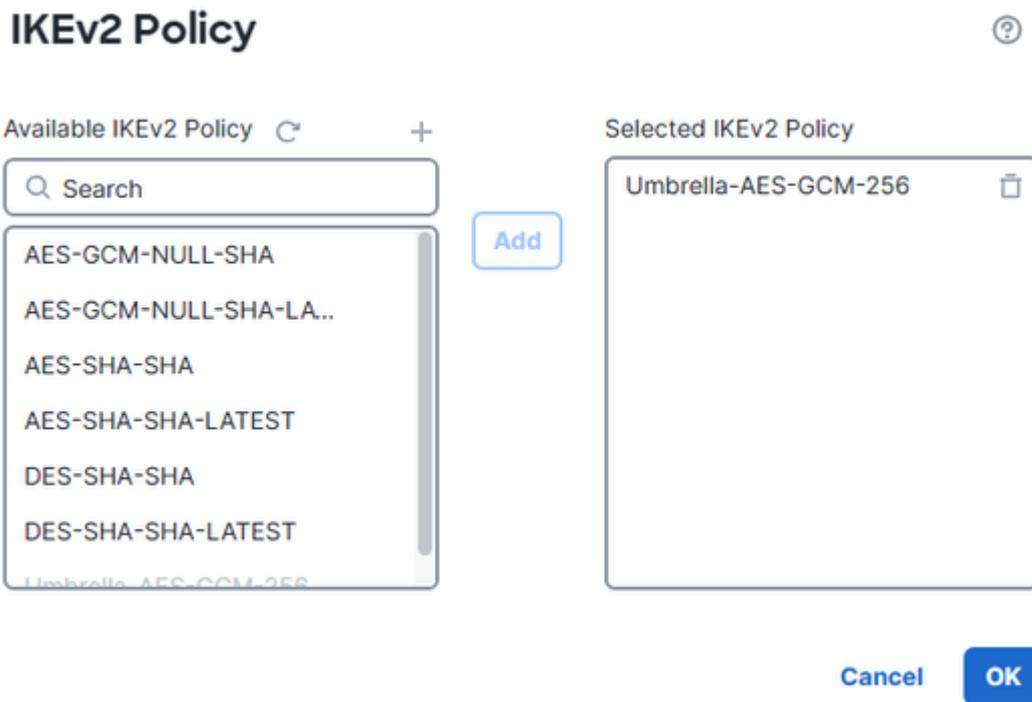
Tunnel Source: outside (IP: 192.168.0.20) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

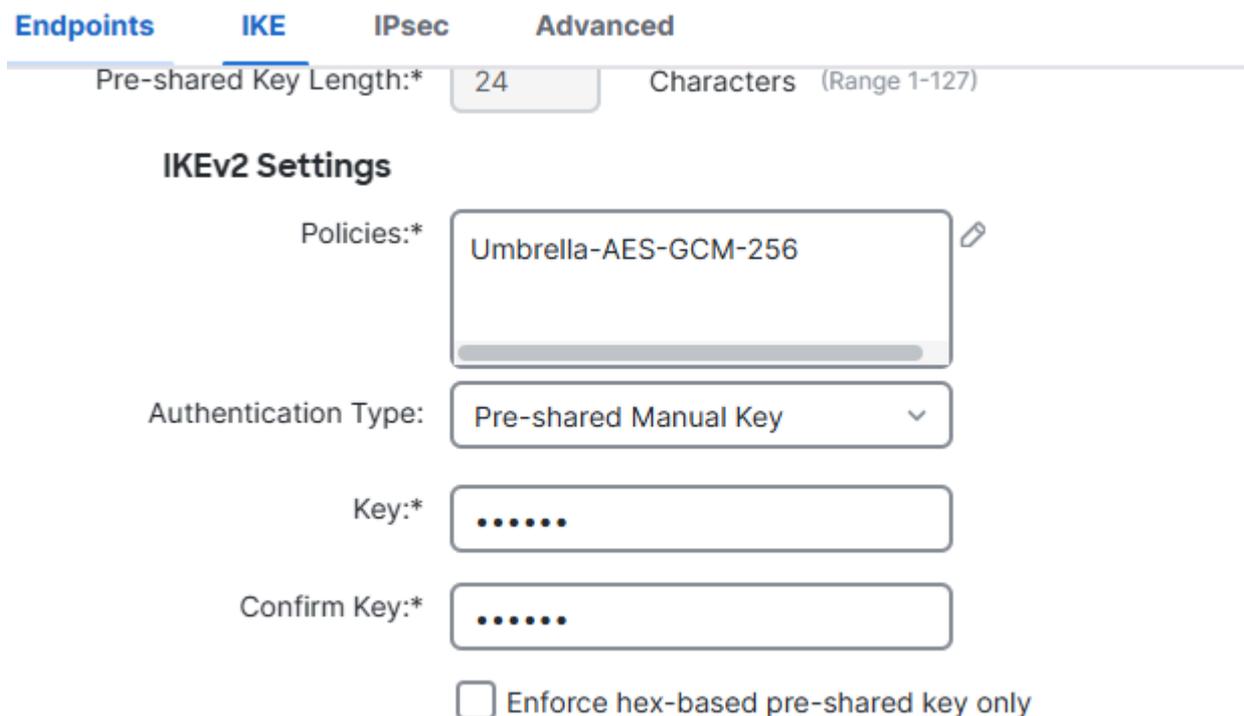
Local Identity Configuration*:

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



IKEv2 Policy

- Click on Authentication Type and select Pre 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

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha Umbrella-AES-GCM-...

Cancel **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 to Objects
 - Click on Access List
 - Click on Extended
 - Click on Add 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).

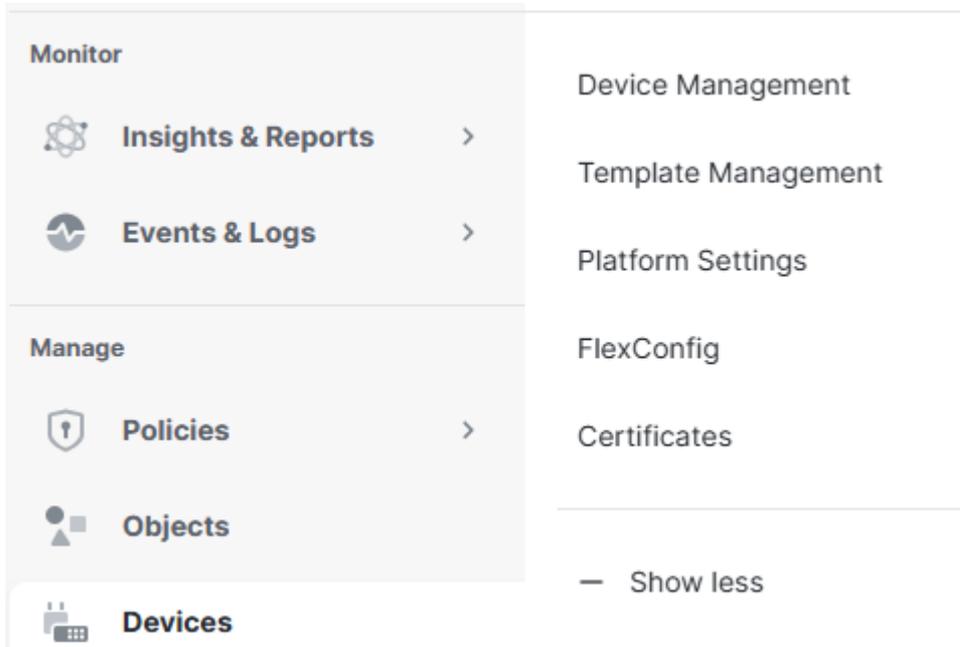
Name

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Allow	Subnet-172.16.15.0	Any	CSA-Management CSA-VPNaaS CSA-ZTA	Any

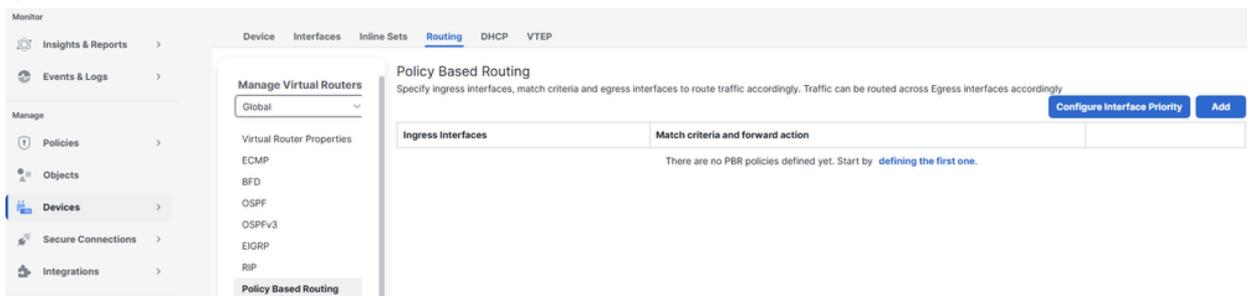
ACL

- Click on Devices> Device Management



Device

- Click on the FTD
 - Click on Routing
 - 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

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

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**

Match ACL: * +

Send To: *

IPv4 Addresses:

Policy Based Config

Save PBR

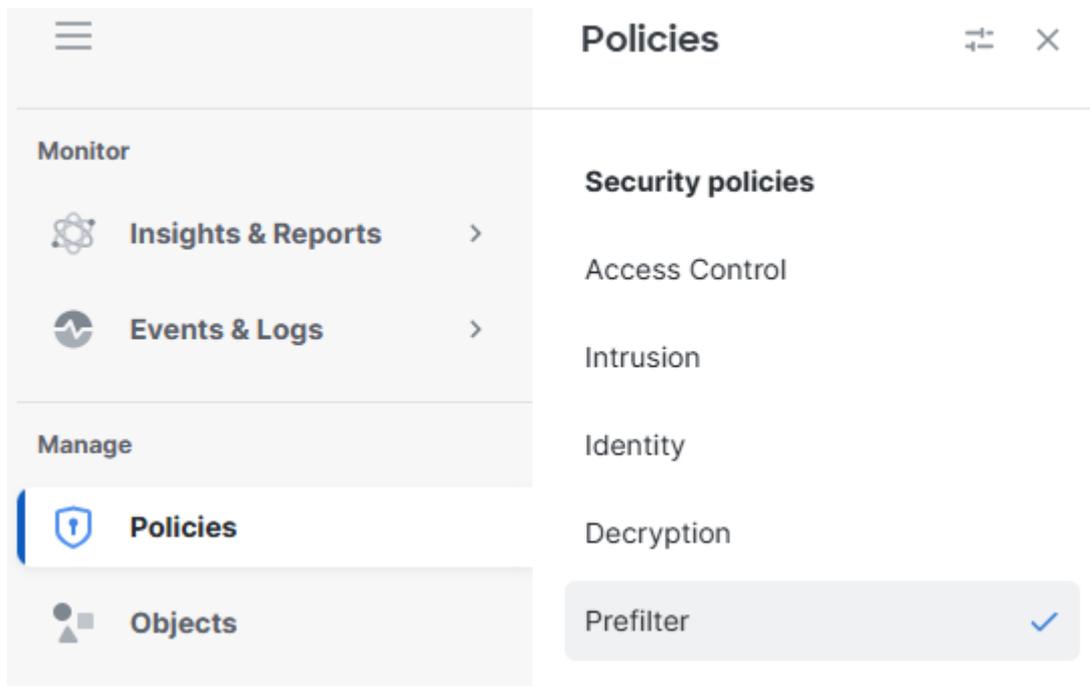
Make sure you select the **Send To > IP Address** option, and not the **Egress Interface** option.

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 policy 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 on Save



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**.

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)

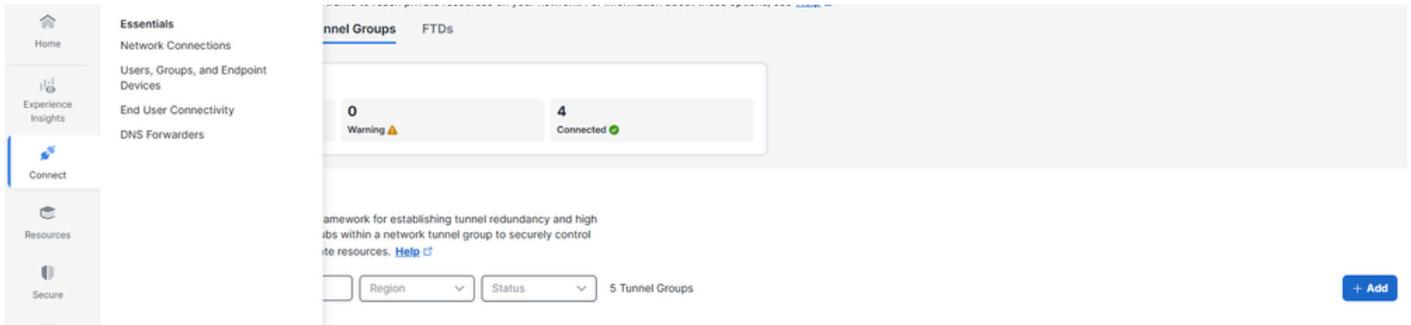
FTD Tunnel Status

Verify in Secure Access

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**



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		

<h4>Primary Hub</h4> <p>Hub Up</p> <p>1 Active Tunnels</p> <p>Tunnel Group ID: ftd1-ipsec@</p>	<p>See Logs</p>	<h4>Secondary Hub</h4> <p>Hub Up</p> <p>1 Active Tunnels</p> <p>Tunnel Group ID</p>
--	---------------------------------	---

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**.


 Home


 Experience Insights


 Connect


 Resources


 Secure


Monitor

Monitor ×

Reports

- Remote Access Logs
- Activity Search
- Connectivity Logs
- Security Activity
- Total Requests
- Activity Volume
- App Discovery
- Private Resource Discovery
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- AI Supply Chain

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	i Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	i Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	i Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	i Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

Conn Logs

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

☰


 Home


 Experience Insights


 Connect


 Resources


 Secure


Monitor

Monitor ×

Reports

- Remote Access Logs
- Activity Search
- Connectivity Logs
- Security Activity
- Total Requests
- Activity Volume
- App Discovery
- Private Resource Discovery
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- AI Supply Chain

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		View Full Details > ⋮
👤 Josue	👤 Josue		⋮
👤 Josue	👤 Josue		⋮
👤 Josue	👤 Josue		⋮
👤 Josue	👤 Josue		⋮
👤 Josue	👤 Josue		⋮
👤 Josue	👤 Josue		⋮

- View Full Details >
- Filter by Josue ⋮
- Filter by ⋮
- Filter by ⋮
- View Rule ⋮
- Edit Rule ⋮

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](#)