

Configure Secure Access with Secure FTD and ASA for Private Access with NAT

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Configure](#)

[Secure Access and Secure Firewall Threat Defense - Dynamic \(BGP\) route-based VPN with PBR](#)

[FTD Policy Based Routing](#)

[Configure BGP on FTD](#)

[Verify Tunnel Status](#)

[Configure Static Route-based IPsec VPN on Adaptive Security Appliance \(ASA\) with PBR](#)

[VPN Configuration on Secure Access](#)

[VPN Configuration on ASA](#)

[Policy Based Routing](#)

[Verify](#)

Introduction

This document describes how to configure Secure Access Network Tunnel Group with Network Address Translation.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firewall Management Center
- Cisco Secure Firewall Threat Defence
- Cisco Secure Access
- Cisco Adaptive Security Appliance
- Network Address Translation
- Policy Based Routing
- Packet Captures on Firewall

Components Used

The information in this document is based on:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defence 7.10
- Cisco Secure Access
- Cisco Adaptive Security Appliance 9.22
- Cisco Routers

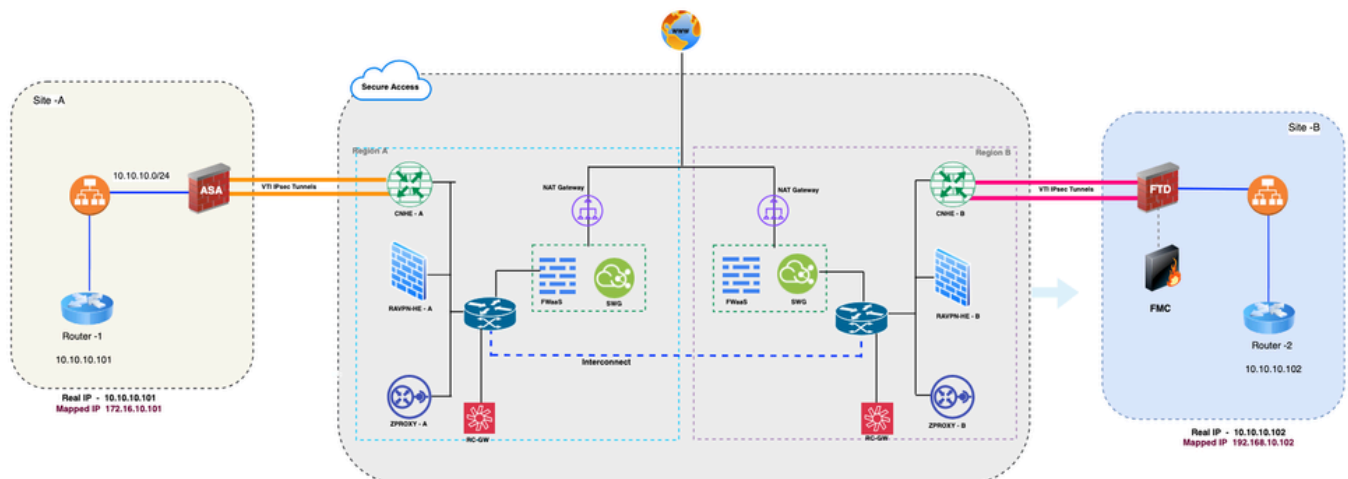
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Secure Access delivers cloud-native Secure Service Edge capabilities including Secure Internet Access (SIA) and Secure Private Access (SPA). For organizations extending private application access to remote users without backhauling all traffic through a datacenter, Secure Access uses IPsec Network Tunnel Groups (NTGs) to create encrypted tunnels between on-premises network devices — such as Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA), — and Cisco Secure Access cloud Points-of-Presence (PoPs).

This document details how to establish a route-based IPsec tunnel using IKEv2 between Cisco FTD, ASA and Cisco Secure Access, enabling Network Address Translation (NAT) on Secure Access and Policy-Based Routing (PBR) on the FTD and ASA to steer only private-access-bound traffic into the tunnel.

Network Diagram

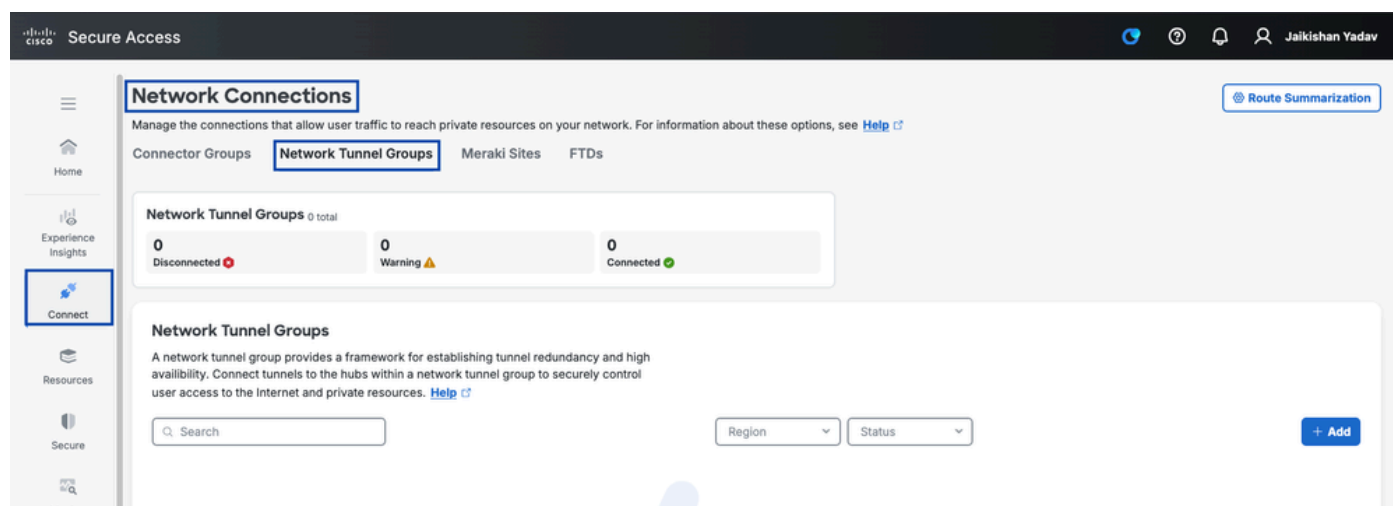


Configure

Secure Access and Secure Firewall Threat Defense - Dynamic (BGP) route-based VPN with PBR

Configure Network Tunnel Group on Secure Access

1. Login to Secure Access dashboard [Secure Access](#)
2. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click on **+Add** to configure the Network Tunnel Group



Secure Access - Network Tunnel Groups

3. Configure Network Tunnel Group - General Settings

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

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Region

Device Type

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

Secure Access - Network Tunnel Groups General Settings

4. Configure **Tunnel ID** and **Passphrase**.

- Configure the Tunnel ID and Passphrase.
- Click on Next

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email
 ☐ IP Address

Tunnel ID

 @<org><hub>.sse.cisco.com

Passphrase

 [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

 [Show](#)

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

Secure Access - Network Tunnel Groups ID and Passphrase

5. Configure **Routing**

- Configure **Device AS Number**

- Click **Save**

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4
 IPv4 is enabled by default.

Routing option

☐ Static routing
 Use this option to manually add IP address ranges for this tunnel group.

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

Device AS Number

65010

Advanced Settings

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

☐ **Override BGP route summarization**
 By default, advertised routes are summarized using the configured summary subnets in the Route Summarization page. Select this option to override route summarization.

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

Cancel

Back Save

Secure Access - Network Tunnel Groups Routing

6. Save Network Tunnel Group Configuration

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

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:

ftdbgpvpn@

Primary Data Center IP Address:

44.228.138.150 2603:5004:13:20e::110:1

Secondary Tunnel ID:

ftdbgpvpn@

Secondary Data Center IP Address:

52.35.201.56 2603:5004:13:20c::110:1

Passphrase:

Download CSV

Done

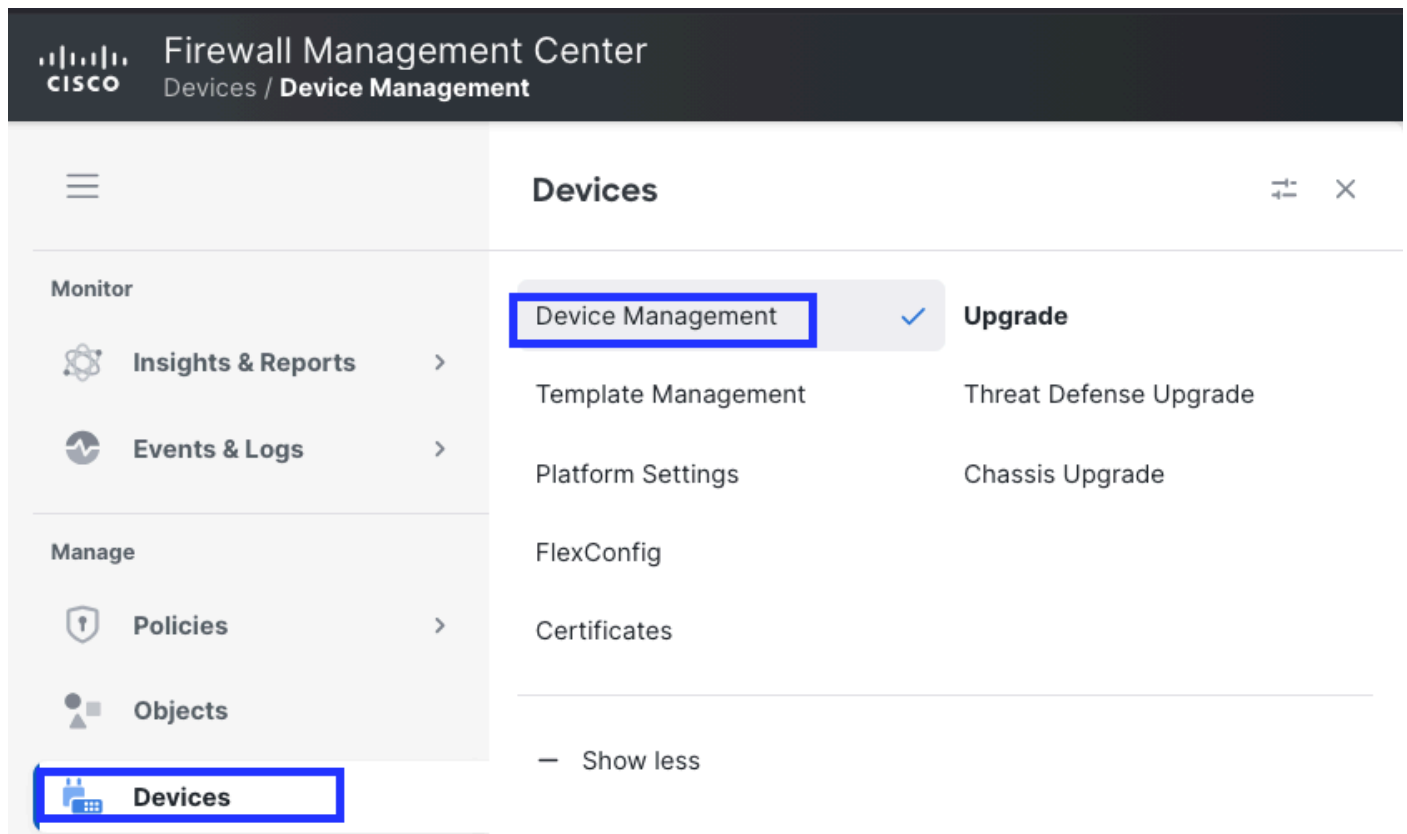
Secure Access - Network Tunnel Groups

Configure Dynamic Route-based IPsec VPN on Secure Firewall Threat Defense (FTD) with PBR

1. Login to Firewall Management Center (FMC)

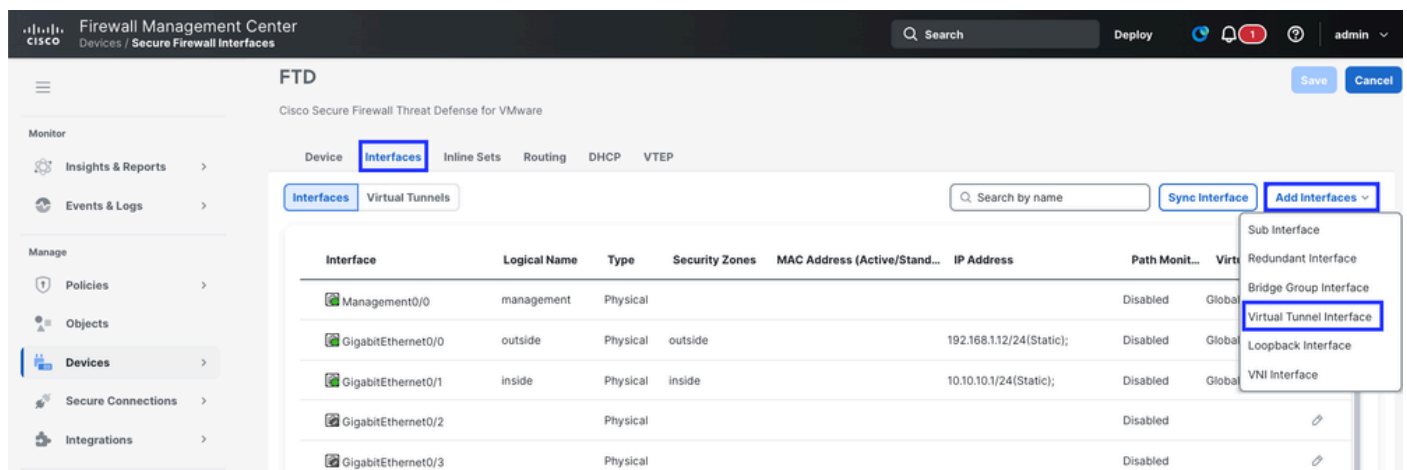
2. Configure Virtual Tunnel Interface [VTI](#)

- Navigate to Devices > Device Management



Secure Firewall Management - Dashboard

- Click on Pencil icon next to device and navigate to Interface section
- Click on **Add interfaces** and select **Virtual Tunnel Interface**



- Configure VTI

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type



Static



Dynamic

Name:*

VTI-1



Enabled

Description:

Virtual Tunnel interface for
Primary VTI VPN

Security Zone:

vti

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

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) 192.168.1.12

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 169.254.2.1/30

☐ Borrow IP (IP unnumbered) Select Interface +

Cancel

OK

Secure Firewall Management - FTD VTI Configuration

- Configure VTI-2 as well for secondary IPsec VPN with Secure Access

FTD

Cisco Secure Firewall Threat Defense for VMware

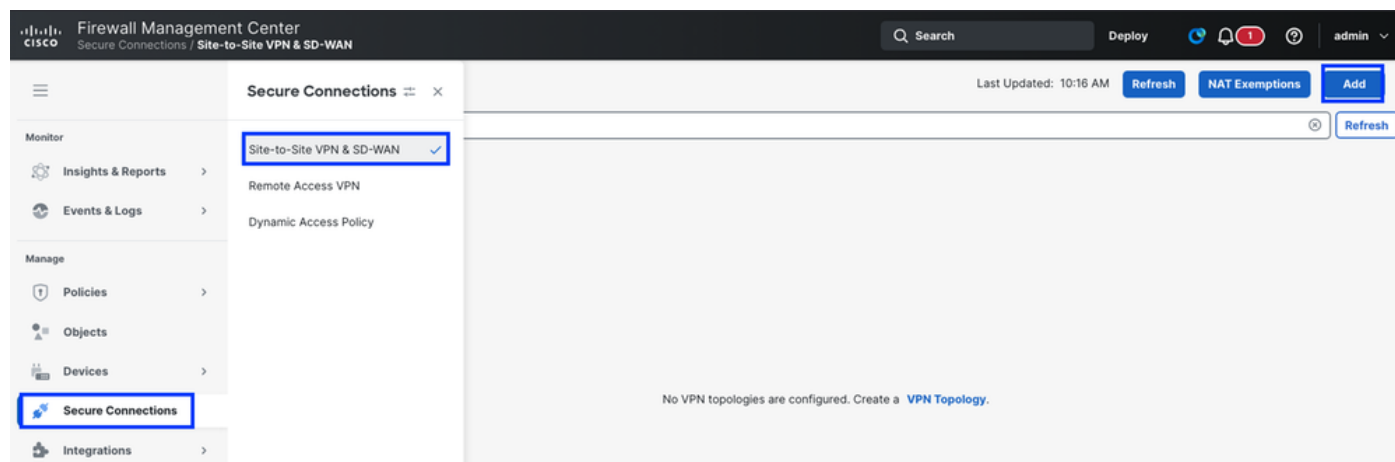
Device Interfaces Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels

Search by name Sync Interface Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...	IP Address	Path Monit...	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outside		192.168.1.12/24(Static);	Disabled	Global
Tunnel1	VTI-1	VTI	vti		169.254.2.1/30(Static);	Disabled	Global
Tunnel2	VTI-2	VTI	vti		169.254.2.5/30(Static);	Disabled	Global
GigabitEthernet0/1	inside	Physical	inside		10.10.10.1/24(Static);	Disabled	Global

3. Navigate to Secure **Connections** > **Site-to-Site VPN & SD-WAN** and click on **Add** to configure the VPN



- Create VPN topology

Create VPN Topology ?

Topology Name *

SecureAccess-VPN-Primary

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

New

☒ **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 Cisco Umbrella Connection is not configured.

Prerequisites

Refresh

Cancel

Create

- From step 6 of the **Configure Network Tunnel Group on Secure Access** , 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 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 Configure Network Tunnel Group on Secure Access)
- Under Node B, 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 Configure Network Tunnel Group on Secure Access)
- 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 Configure Network Tunnel Group on Secure Access)
- Click on Save

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ 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:*

VTI-1 (IP: 169.254.2.1)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:*

Email ID

ftdbgpvpn(

Node B

Device:*

Extranet

Device Name:*

Secure Access

Endpoint IP Address:*

44.228.138.150,52.35.201.56

Cancel

Save

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ 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

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.2.5)



Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)



Tunnel Source IP is Private



Send Local Identity to Peers

Local Identity Configuration:*

Email ID

tdbgpvpn@

22-

Additional
Configuration



Route traffic to the VTI

: [Routing Policy](#)

Permit VPN traffic

: [AC Policy](#)

Cancel

Save

Secure FTD - VPN Endpoint Configuration

- Configure **IKEv2 Settings** as per [Supported IPsec Parameters](#)
 - Select Policies as **Umbrella-AES-GCM-256**
 - Select Authentication Type as **Pre-Shared Manual Key**

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

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

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*



IKEv1



IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

Secure FTD - VPN IKE Settings

- Configure IPsec settings
 - Select **IKEv2 IPsec Proposals** as Umbrella-AES-GCM-256
 - Enable **PFS** as select **Modulus Group** as 20

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ 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

Umbrella-AES-GCM-...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group:

20

Cancel

Save

Secure FTD - VPN IPsec Settings

- Advanced Settings
- Click **Save**

Edit VPN Topology



Topology Name:*

SecureAccess-VPN-Primary

☐ 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

IPsec

Tunnel

IKE Keepalive:

Enable

Threshold:

10

Seconds

(Range 10 - 3600)

Retry Interval:

2

Seconds

(Range 2 - 10)

Identity Sent to Peers:

autoOrDN

Peer Identity Validation:

Do not check

Cancel

Save

Secure FTD - VPN Advanced Settings

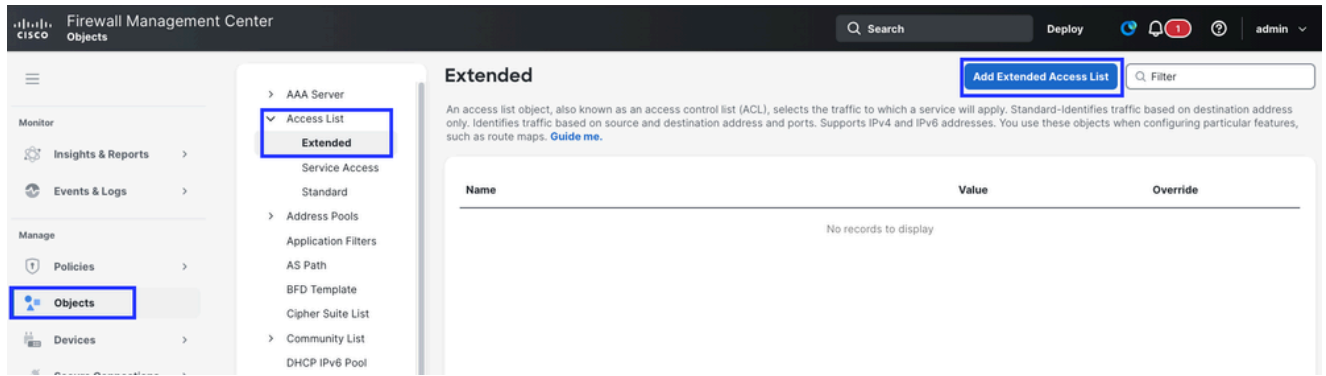
FTD Policy Based Routing

In traditional routing, packets are routed based on the destination IP address. Changing the routing of specific traffic in a destination-based routing system is difficult. Policy Based Routing (PBR) extends and complements the mechanisms provided by routing protocols, giving you more control over routing.

PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link. With PBR, you can define routing that is based on criteria other than destination network such as source port, destination address, destination port, protocol, applications, or a combination of these objects. For more information, refer [Policy Based Routing](#)

1. Configure Access List

- Navigate to **Objects > Access List > Extended**
- Click on **Add Extended Access List**



Secure FTD - Extended Access List

- Give the Access List Name
- Define the Action
 - Allow. - Traffic defined will be sent to IPsec tunnel
 - Block - Traffic will be bypassed from IPsec Tunnel
 - Rule will be matched based on Sequence Number (Lower to higher)
 - Click on **Add**
 - Click **Save**

Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks +

10.10.10.0

obj_10.10.10.0

Add to Source

Add to Destination

Source Networks (1)

obj_10.10.10.0

Destination Networks (0)

any

Cancel Add

Secure FTD - Extended Access List

New Extended Access List Object



Name
PBR

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	obj_10.10.10.0	Any	Any	Any	Any	Any	

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

☐ Allow Overrides

Cancel Save

Secure FTD - Extended Access List

2. Configure Policy Based Routing

- Navigate to **Devices > Device Management > FTD > Routing**

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, 'Firewall Management Center', 'Devices / Secure Firewall Routing', a search bar, a 'Deploy' button, and user information 'admin'. The left sidebar contains a menu with 'Monitor', 'Manage', and 'Administration' sections. Under 'Manage', 'Devices' is highlighted. The main content area is titled 'FTD' and 'Cisco Secure Firewall Threat Defense for VMware'. It has tabs for 'Device', 'Interfaces', 'Inline Sets', 'Routing' (which is selected), 'DHCP', and 'VTEP'. In the 'Routing' tab, 'Manage Virtual Routers' is set to 'Global'. Under 'Virtual Router Properties', 'Policy Based Routing' is selected. The 'Virtual Router Properties' section shows fields for 'VRF Name' (Global), 'Description' (This is a Global Virtual Router), and 'Select Interface'. Below these are two lists: 'Available Interfaces' (outside, inside, management, VTI-1, VTI-2) and 'Selected Interfaces' (outside, VTI-1, inside, management, VTI-2). An 'Add' button is located between the two lists.

Secure FTD - Policy Based Routing

- Click on Add
- Select Ingress Interface - Ingress interface for the subnet we defined in the Access List

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.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

Secure FTD - Policy Based Routing

- Define Match Criteria and Egress Interface
 - Click on **Add**
 - Select the **Match ACL**
 - Select **Send to** as IP address
 - Add Next hop IP address. - VTIs interface IP addresses are. 169.254.2.130 and. 169.254.2.5/30. So, the next hop IP addresses for VTI -1 and VTI-2 would be 169.254.2.2 and. 169.254.2.6 respectively
 - Click on **Save**

Add Forwarding Actions

Match ACL: * +

Send To: *

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

IPv4 settings **IPv6 settings**

Recursive:

Default:

☐ Peer Address

Cancel

Save

Secure FTD - Policy Based Routing

FTD

You have unsaved changes Save Cancel

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Ingress Interfaces

inside

Match criteria and forward action

If traffic matches the Access List

PBR

Send through

169.254.2.2

169.254.2.6

Configure Interface Priority

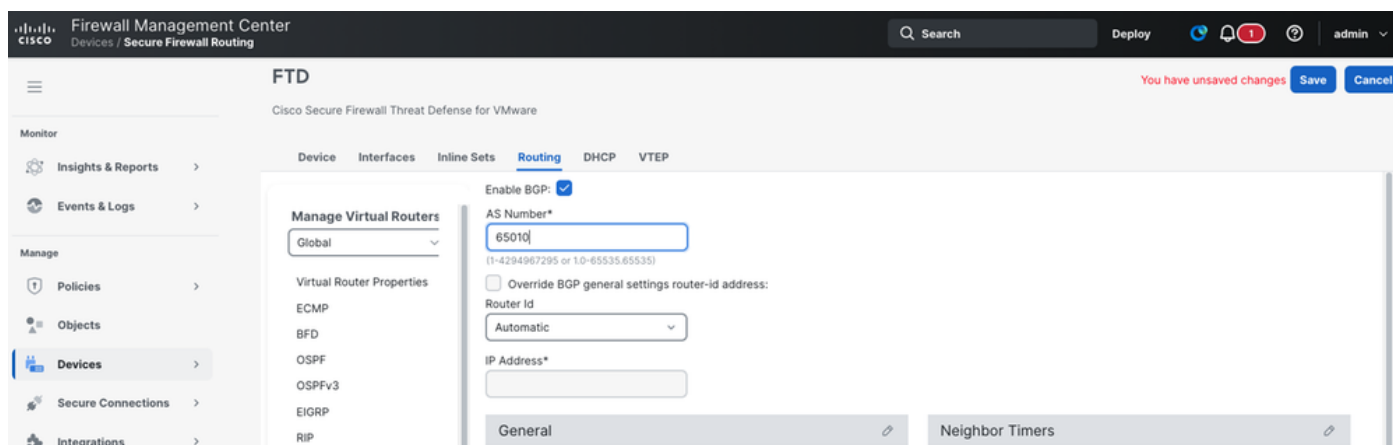
Add

Secure FTD - Policy Based Routing

Configure BGP on FTD

1. Enable BGP

- Navigate to **Devices > Device Management > FTD > Routing > General Settings > BGP**
- Enable BGP and add the AS number (FTD local AS number)
- Click **Save**



Secure FTD - BGP Routing

- Navigate to **BGP > IPv4**

2. Add BGP **Neighbor** - Secure Access BGP peers are 169.254.0.5 and. 169.254.0.9

Add Neighbor



IP Address*

169.254.0.5

Remote AS*

64512

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

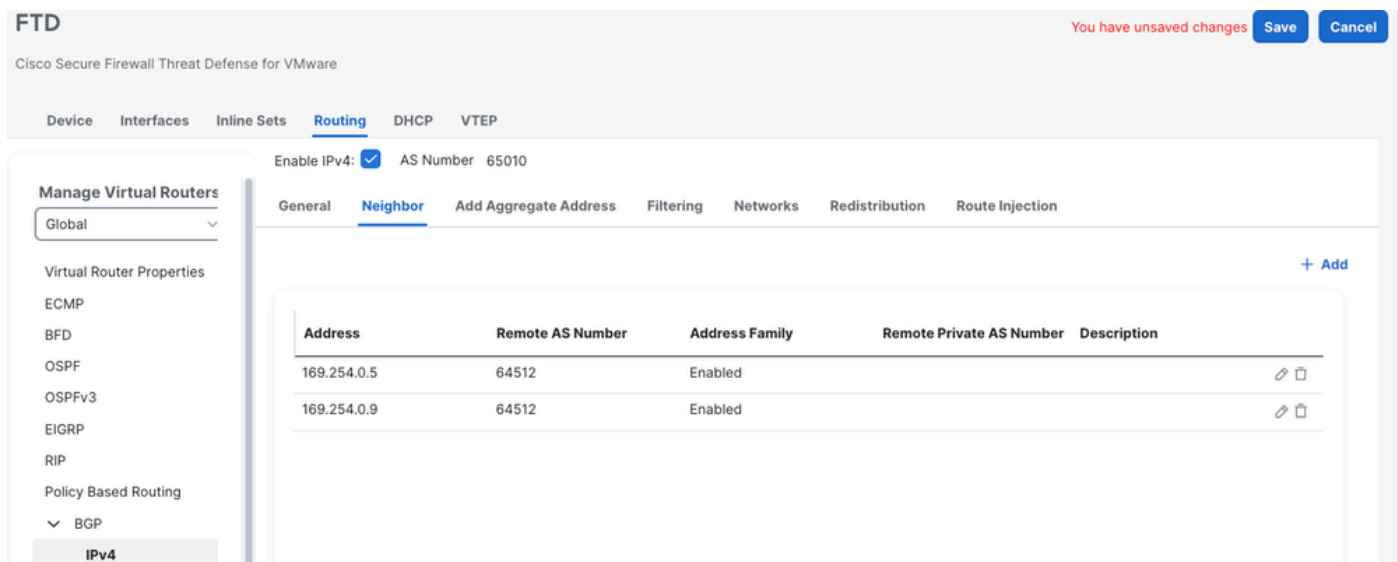
(1-254)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

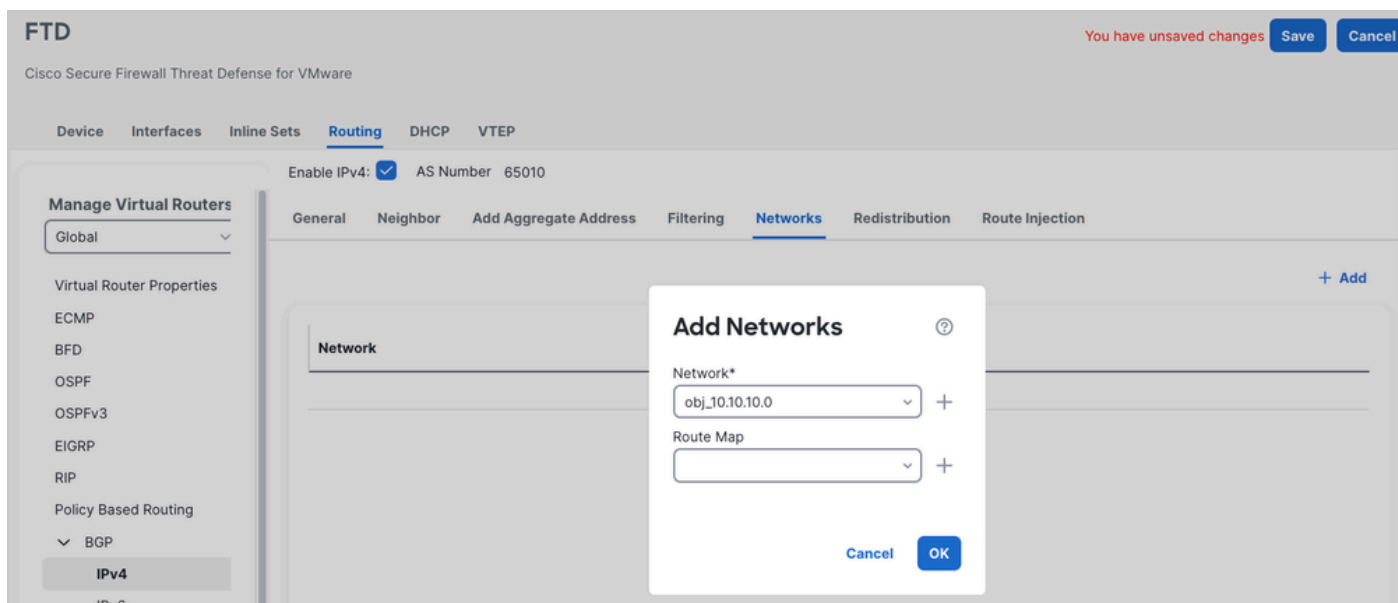
OK



Secure FTD - BGP Routing

3. Add the Networks - Networks that needs to be advertised to Secure Access

- Click OK

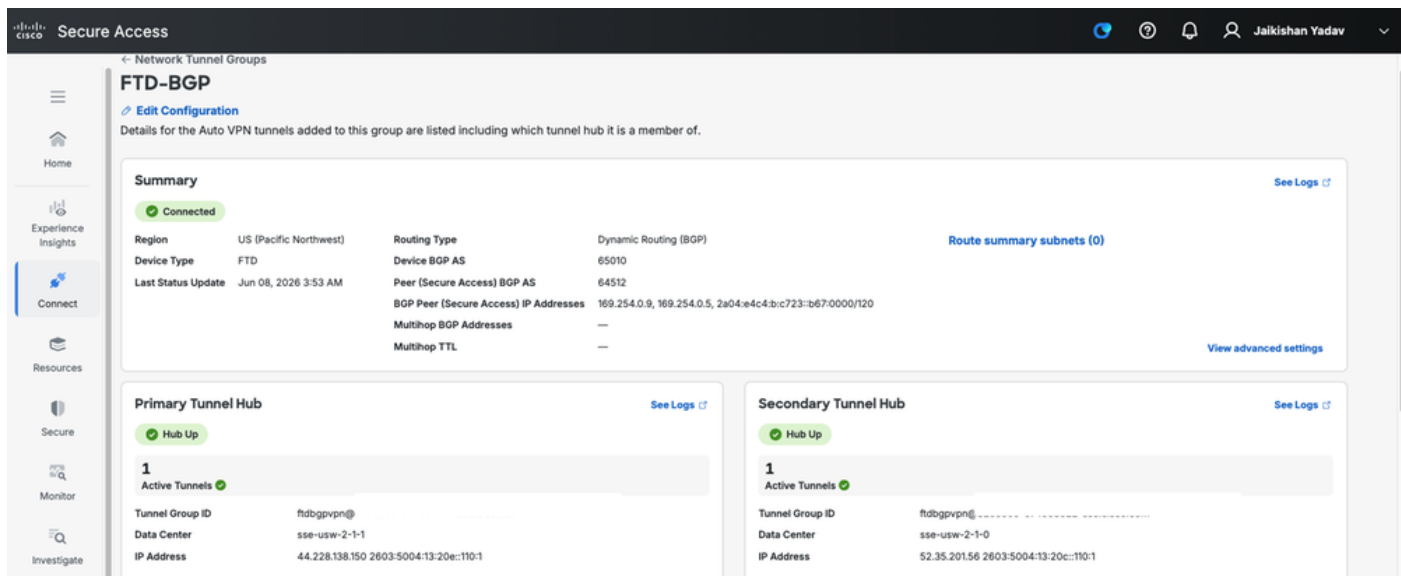


Secure FTD - BGP Routing

- Save and Deploy the changes

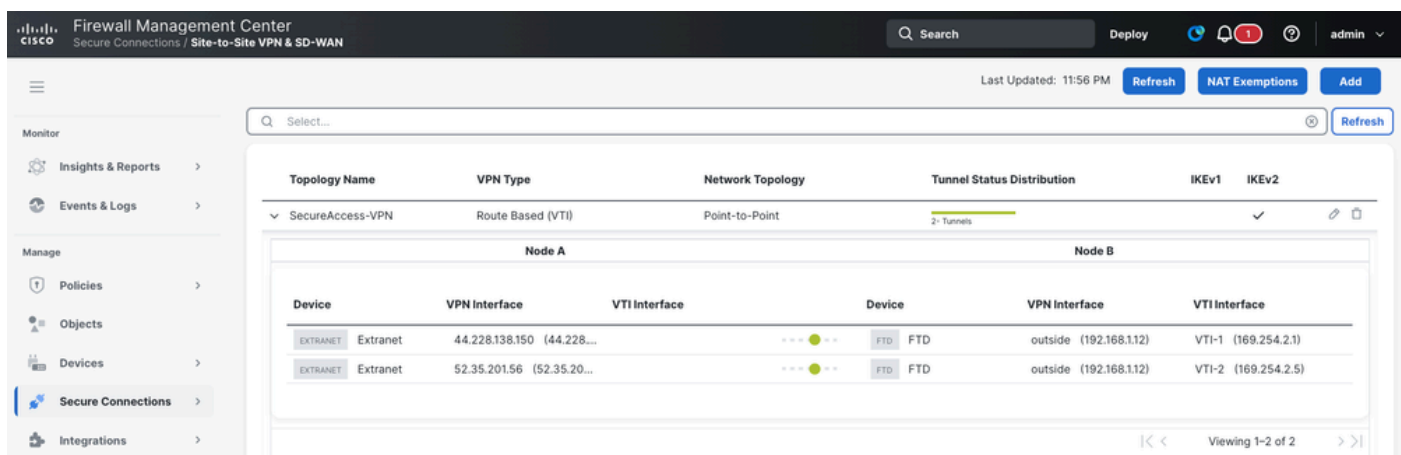
Verify Tunnel Status

On Secure Access



Secure FTD - IPsec Tunnel Status

On FMC

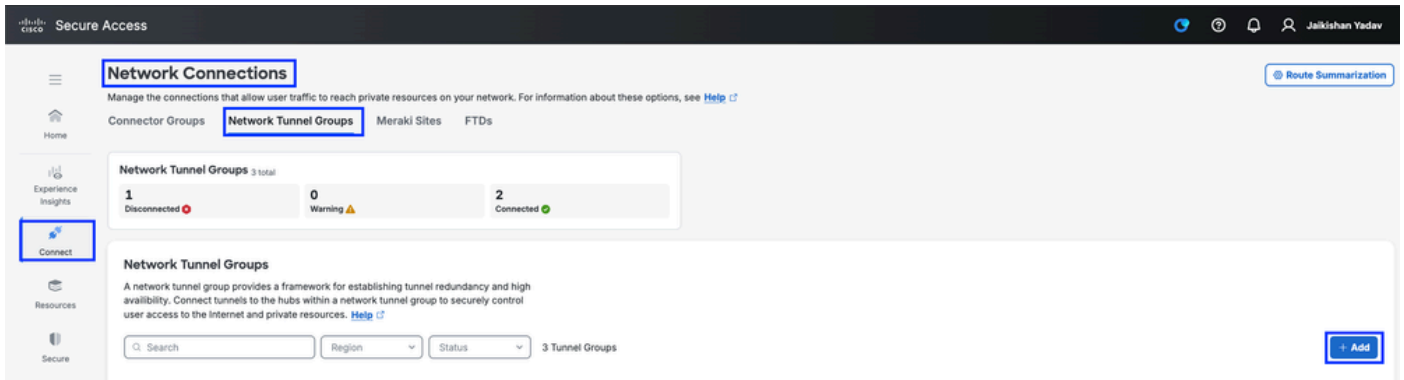


Secure FMC - IPsec Tunnel Status

Configure Static Route-based IPsec VPN on Adaptive Security Appliance (ASA) with PBR

VPN Configuration on Secure Access

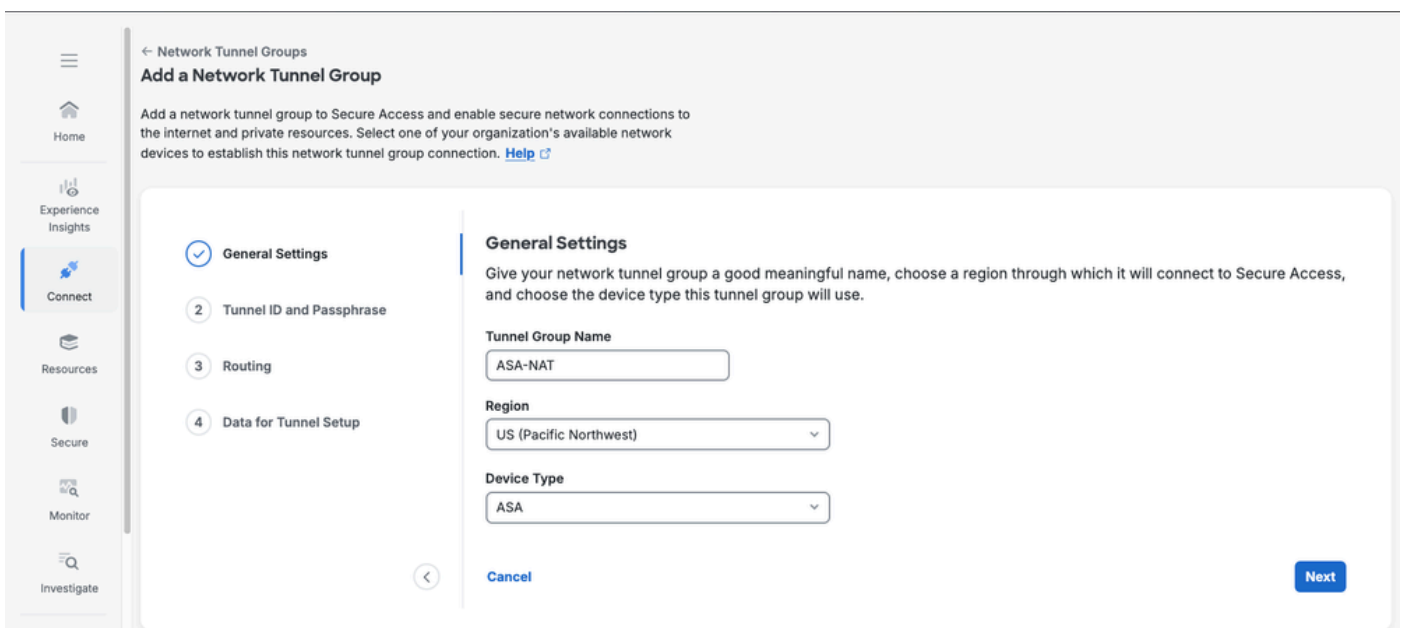
1. Login to Secure Access dashboard [Secure Access](#)
2. Navigate to **Connect** > **Network Connections** > **Network Tunnel Groups** and click on **+Add** to configure the Network Tunnel Group



Secure Access - Network Tunnel Groups

3. Configure Network Tunnel Group - General Settings

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



Secure Access - Network Tunnel Groups General Settings

4. Configure Tunnel ID and Passphrase.

- Configure the Tunnel ID and Passphrase.
- Click on Next

Flow 2 - Router 2 to Router 1 (Secure Access to Site)

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the Internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

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

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**
Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access
Source NAT

All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Secure Access → Site
Source NAT
Add a destination mapping to enable this rule

Destination NAT Mappings

Name	Direction	Original CIDR	Translated CIDR	
ASA-To-FTD	Site → Secure Access	10.10.10.102/32	192.168.10.102/32	☒

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

Secure Access - Network Tunnel Groups NAT Settings



Caution: When NAT is enabled, BGP is not possible . Also, configure static VPN on Customer Edge devices as well



Tip: Always remember to ping a translated IP .
Translated IP goes in Translated CIDR and Real IP goes in Original CIDR

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access ⓘ
Source NAT
All source IP addresses translate to range:

☐ Translate to Secure Access NAT subnet

Secure Access → Site ⓘ
Source NAT
All source IP addresses translate to range:

☒ Translate to Secure Access NAT subnet

Destination NAT Mappings

Name	Direction ⓘ	Original CIDR	Translated CIDR	...
> ASA-To-FTD	Site → Secure Access	10.10.10.102/32	→ 192.168.10.102/32	ⓘ ⌵
> FTD-To-ASA	Secure Access → Site	10.10.10.101/32	→ 172.16.10.101/32	ⓘ ⌵

Rows per page < **1** >

[+ Add Mappings](#)

Internet Protocol Version Setting for Routing

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

Secure Access - Network Tunnel Groups NAT Settings

Click on **Save**



Tip: For traffic going from 'Site A' to 'Site B', from CNHE-1 point of view direction is 'Site-> SecureAccess'

For traffic going from 'site B' to 'site A', from CNHE-1 point of view direction is 'SecureAccess -> Site'

VPN Configuration on ASA

1. Log into ASA CLI, enter enable mode and verify basic IP connectivity towards the internet

```
ASA# sh ip
```

System IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 manual

GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

Current IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 manual

GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

```
ASA# ping 8.8.8.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/30 ms

ASA#

2. Configure IKEv2 policy and enable IKEv2 on the outside interface

```
crypto ikev2 policy 10
encryption aes-gcm-256
integrity null
group 19
lifetime seconds 86400
crypto ikev2 enable outside
```

3. Configure IPSec proposal

```
crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary
protocol esp encryption aes-gcm-256
```

4. Configure IPsec profile

```
crypto ipsec profile csa-profile-primary
set ikev2 ipsec-proposal Ipsec-Proposal-primary
set ikev2 local-identity email-id <primary tunnel-id>
```

5. Configure Group Policy, and enable IKEv2 protocol under attribute.

```
group-policy csa-policy-primary internal
group-policy csa-policy-primary attributes
vpn-tunnel-protocol ikev2
```

6. Configure Tunnel Group.

```
tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary
tunnel-group 44.228.138.150 ipsec-attributes
ikev2 remote-authentication pre-shared-key <pre-shared-key>
ikev2 local-authentication pre-shared-key <pre-shared-key>
```

7. Configure Virtual Tunnel Interface (VTI)

- Nameif can be if your choice
- IP address assigned to VTI **must not overlap** with any other interface on the ASA

- Tunnel source **must** be the outside interface of the firewall
- Tunnel destination **must** be the Data Center IP address

```
interface Tunnel1
nameif VTI-1
ip address 169.254.2.1 255.255.255.252
tunnel source interface outside
tunnel destination 44.228.138.150
tunnel mode ipsec ipv4
tunnel protection ipsec profile csa-profile-primary
```

8. Configure routing in way that, traffic to the mapped IP address or subnet is routed inside the VTI interface. Next hop needs to be IP within range of VTI.

```
route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5. ( for internet based, RAVPN pool or CGNAT traffic
```

or

```
route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5
```

Policy Based Routing

1. Access List

```
access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any
```

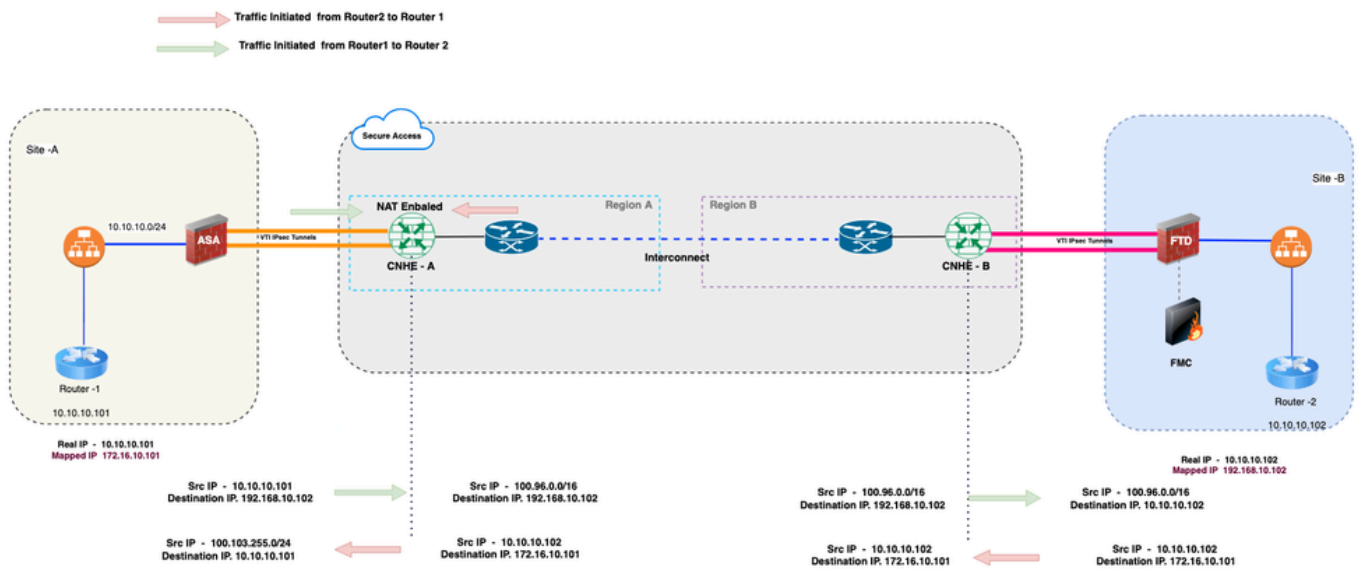
2. Route-map

```
route-map RM-CSA permit 10
match ip address PBR
set ip next-hop 169.254.2.2 169.254.2.6
```

3. Apply Route-map on ingress interface

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA
```

Verify



Router interface and GW reachability status

```
Router1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet1         192.168.1.101   YES NVRAM    down        down
GigabitEthernet2         10.10.10.101    YES NVRAM    up          up
GigabitEthernet3         unassigned      YES NVRAM    administratively down down
GigabitEthernet9         unassigned      YES unset   administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Test 1- Router2 --> Router1. - Ping Test

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

Packet capture on ASA (Local FW)

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown

```

Packet Capture on FTD (Remote FW)

```

ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

```

10 packets captured

```

 1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```

 1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
 2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
 3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
 4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
 5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
 6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
 7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
 8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
 9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486      10.10.10.102 > 100.96.2.0 icmp: echo reply

```

10 packets shown

Test 2. - Router 2 ---> Router 1 ping test

```

Router2#sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet1   unassigned      YES NVRAM    administratively down down
GigabitEthernet2   10.10.10.102    YES NVRAM    up              up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```

FTD Packet Capture (Local FW)

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

ASA packet capture (Remote FW)


```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

  1: 11:08:30.288391      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289123      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504566      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.504963      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710992      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711404      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917112      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917402      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128243      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128640      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 11:08:30.287964      100.103.255.195 > 10.10.10.101 icmp: echo request
  2: 11:08:30.289322      10.10.10.101 > 100.103.255.195 icmp: echo reply
  3: 11:08:30.504505      100.103.255.195 > 10.10.10.101 icmp: echo request
  4: 11:08:30.505009      10.10.10.101 > 100.103.255.195 icmp: echo reply
  5: 11:08:30.710961      100.103.255.195 > 10.10.10.101 icmp: echo request
  6: 11:08:30.711434      10.10.10.101 > 100.103.255.195 icmp: echo reply
  7: 11:08:30.917066      100.103.255.195 > 10.10.10.101 icmp: echo request
  8: 11:08:30.917417      10.10.10.101 > 100.103.255.195 icmp: echo reply
  9: 11:08:31.128197      100.103.255.195 > 10.10.10.101 icmp: echo request
 10: 11:08:31.128685      10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```