

Configure Secure Access with Secure Firewall with High Availability

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Configure](#)

[Configure the VPN on Secure Access](#)

[Data for Tunnel Setup](#)

[Configure the tunnel on Secure Firewall](#)

[Configure the Tunnel Interface](#)

[Configure Static Route for the Secondary Interface](#)

[Configure the VPN to Secure Access in VTI Mode](#)

[Endpoints Configuration](#)

[IKE Configuration](#)

[IPSEC Configuration](#)

[Advanced Configuration](#)

[Access Policy Configuration Scenarios](#)

[Internet Access Scenario](#)

[RA-VPN Escenario](#)

[CLAP-BAP ZTNA Escenario](#)

[Configure Policy Base Routing](#)

[Configure Internet Access Policy on Secure Access](#)

[Configure Private Resource Access for ZTNA and RA-VPN](#)

[Troubleshoot](#)

[Verify Phase1 \(IKEv2\)](#)

[Verify Phase2 \(IPSEC\)](#)

[High Availability Function](#)

[Verify Traffic Routing to Secure Access](#)

[Related Information](#)

Introduction

This document describes how to configure Secure Access with Secure Firewall with High Availability.

Prerequisites

- [Configure User Provisioning](#)
- [ZTNA SSO Authentication Configuration](#)

- [Configure Remote Access VPN Secure Access](#)

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Management Center 7.2
- Firepower Threat Defence 7.2
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless ZTNA

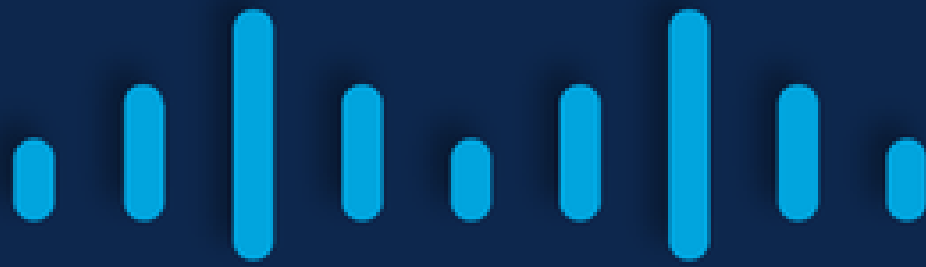
Components Used

The information in this document is based on:

- Firepower Management Center 7.2
- Firepower Threat Defence 7.2
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

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

Secure Firewall

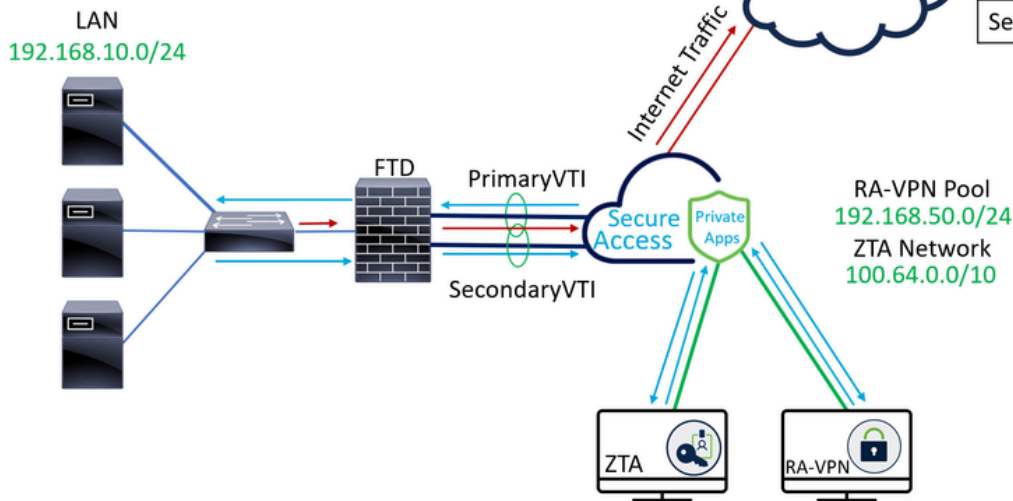
FTD

Cisco has designed Secure Access to protect and provide access to private applications, both on-premise and cloud-based. It also safeguards the connection from the network to the internet. This is achieved through the implementation of multiple security methods and layers, all aimed at preserving the information as they access it via the cloud.

Network Diagram

Internet Access Traffic — (red line)
 Private Apps Traffic — (blue line)

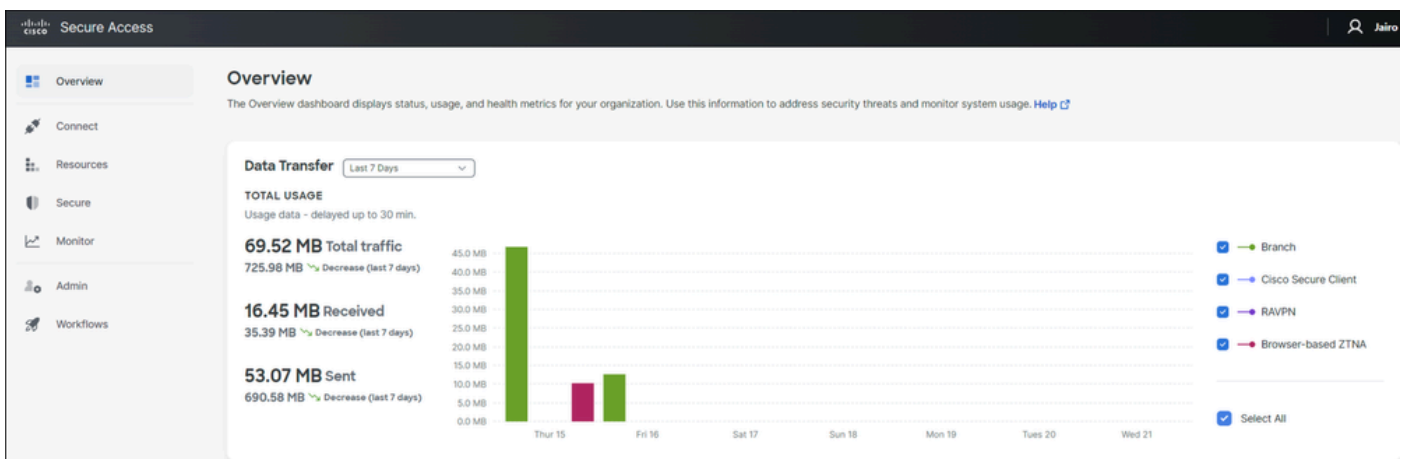
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



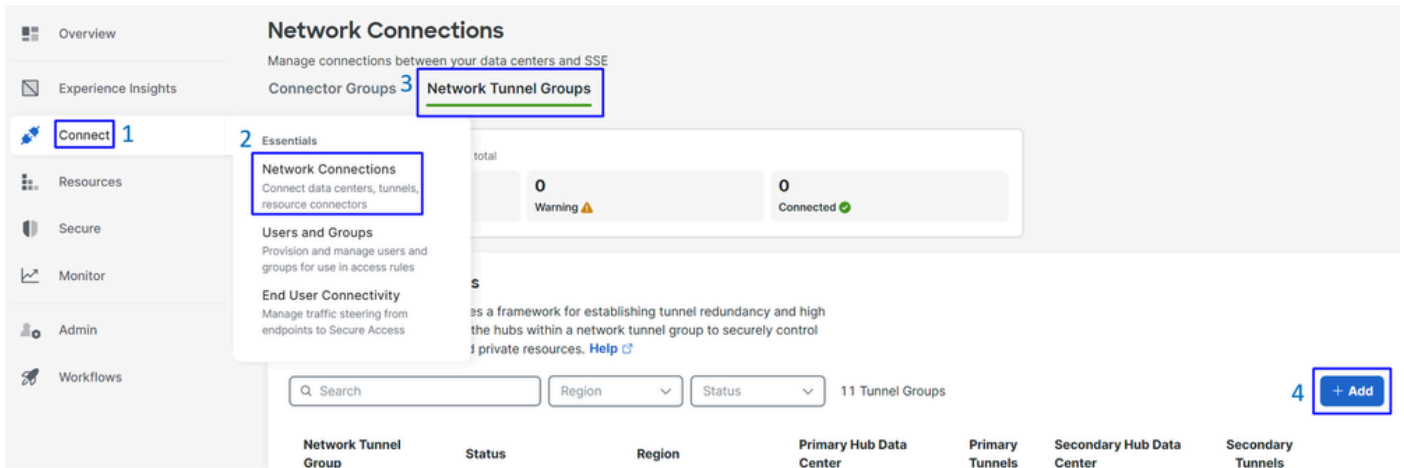
Configure

Configure the VPN on Secure Access

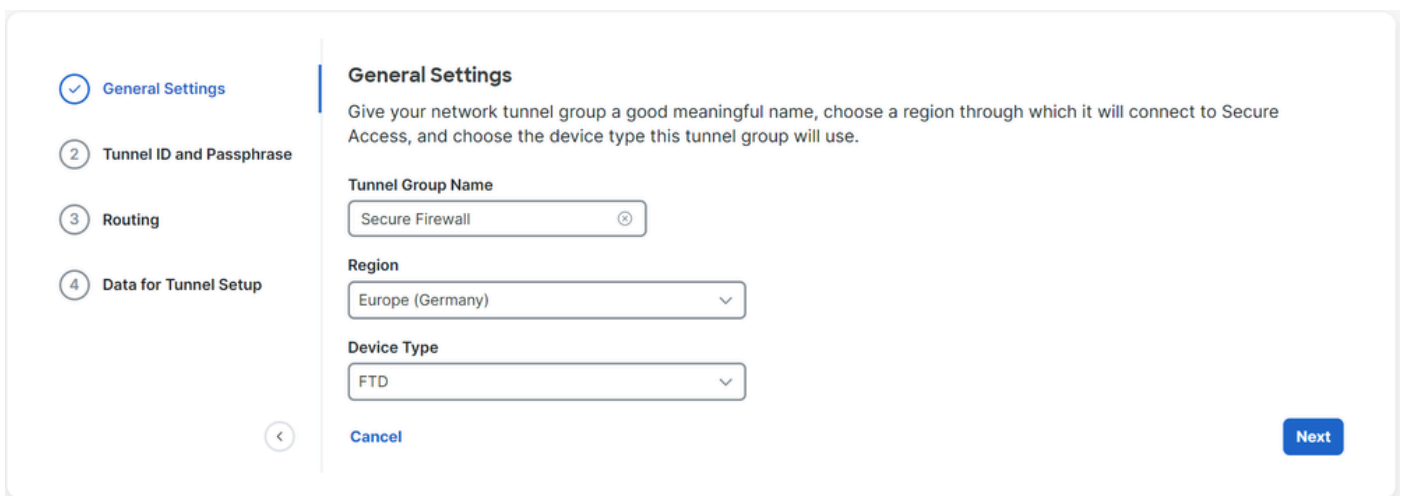
Navigate to the admin panel of [Secure Access](#).



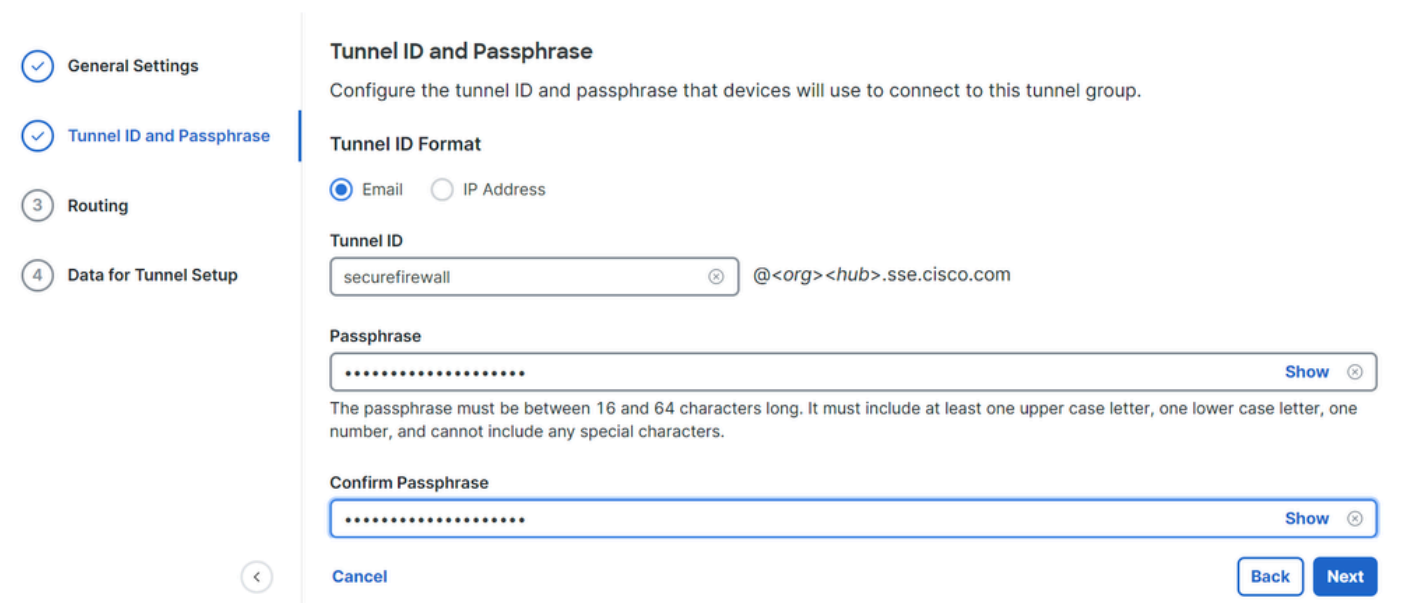
- Click on Connect > Network Connections
- Under Network Tunnel Groups click on + Add



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



- Configure the Tunnel ID Format and Passphrase
- Click Next



- Configure the IP address ranges or hosts that you have configured on your network and want to pass

the traffic through Secure Access

- ClickSave

Routing option

Static routing

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

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

Add

192.168.0.0/24 ✕

192.168.10.0/24 ✕

Dynamic routing

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

[Cancel](#)

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

After you click on **Save** the information about the tunnel gets displayed, please save that information for the next step, **Configure the tunnel on Secure Firewall**.

Data for Tunnel Setup

- General Settings
- Tunnel ID and Passphrase
- Routing
- 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:	securefirewall@[redacted]-sse.cisco.com ✕
Primary Data Center IP Address:	18.156.145.74 ✕
Secondary Tunnel ID:	securefirewall@[redacted]-sse.cisco.com ✕
Secondary Data Center IP Address:	3.120.45.23 ✕
Passphrase:	[redacted] ✕

[Download CSV](#)
[Done](#)

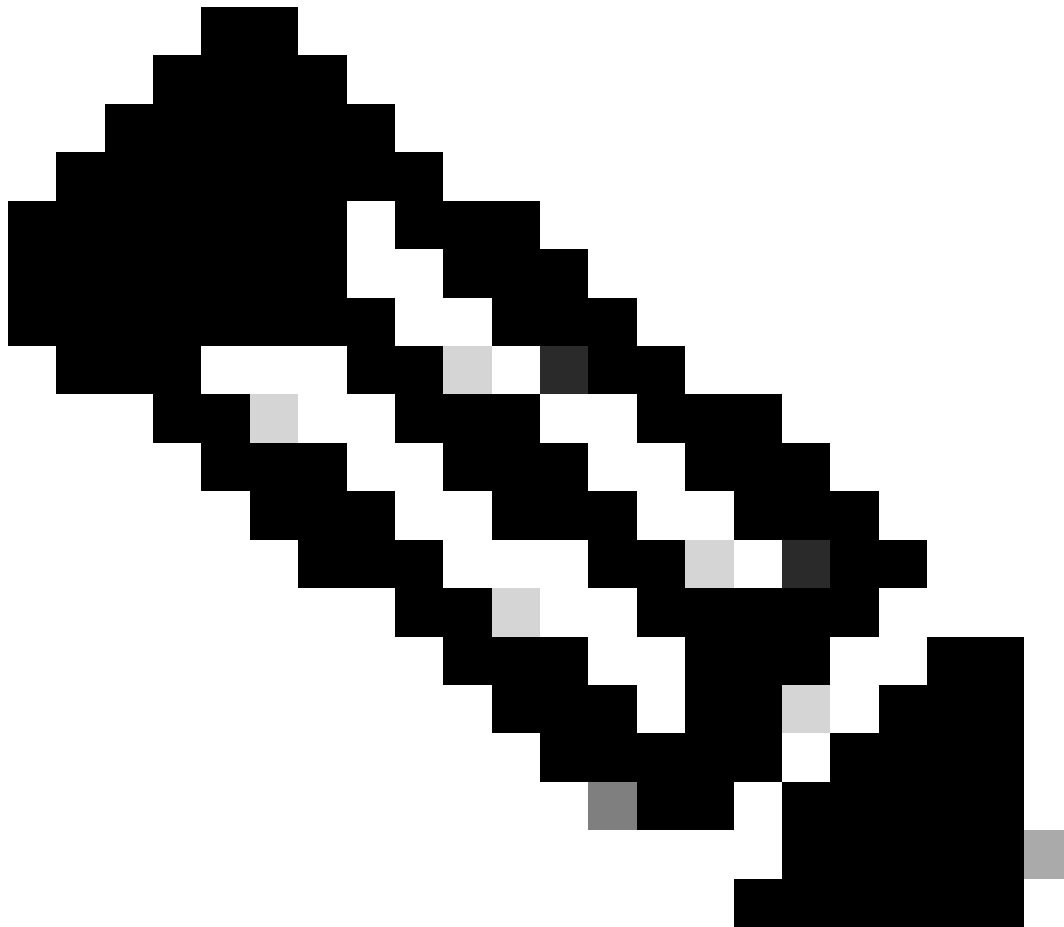
Configure the tunnel on Secure Firewall

Configure the Tunnel Interface

For this scenario, you use Virtual Tunnel Interface (VTI) configuration on Secure Firewall to achieve this goal; remember, in this case, you have double ISP, and we want to have HA if one of your ISPs fails.

INTERFACES	ROLE
------------	------

PrimaryWAN	Principal Internet WAN
SecondaryWAN	Secondary Internet WAN
PrimaryVTI	Linked to send the traffic through the Principal Internet WAN to Secure Access
SecondaryVTI	Linked to send the traffic through the Secondary Internet WAN to Secure Access



Note: 1. You need to add or assign a static route to the **Primary or Secondary Datacenter IP** to be able to have both tunnels up.



Note: 2. If you have ECMP configured between the interfaces, you do not need to create any static route to the **Primary or Secondary Datacenter IP** to be able to have both tunnels up.

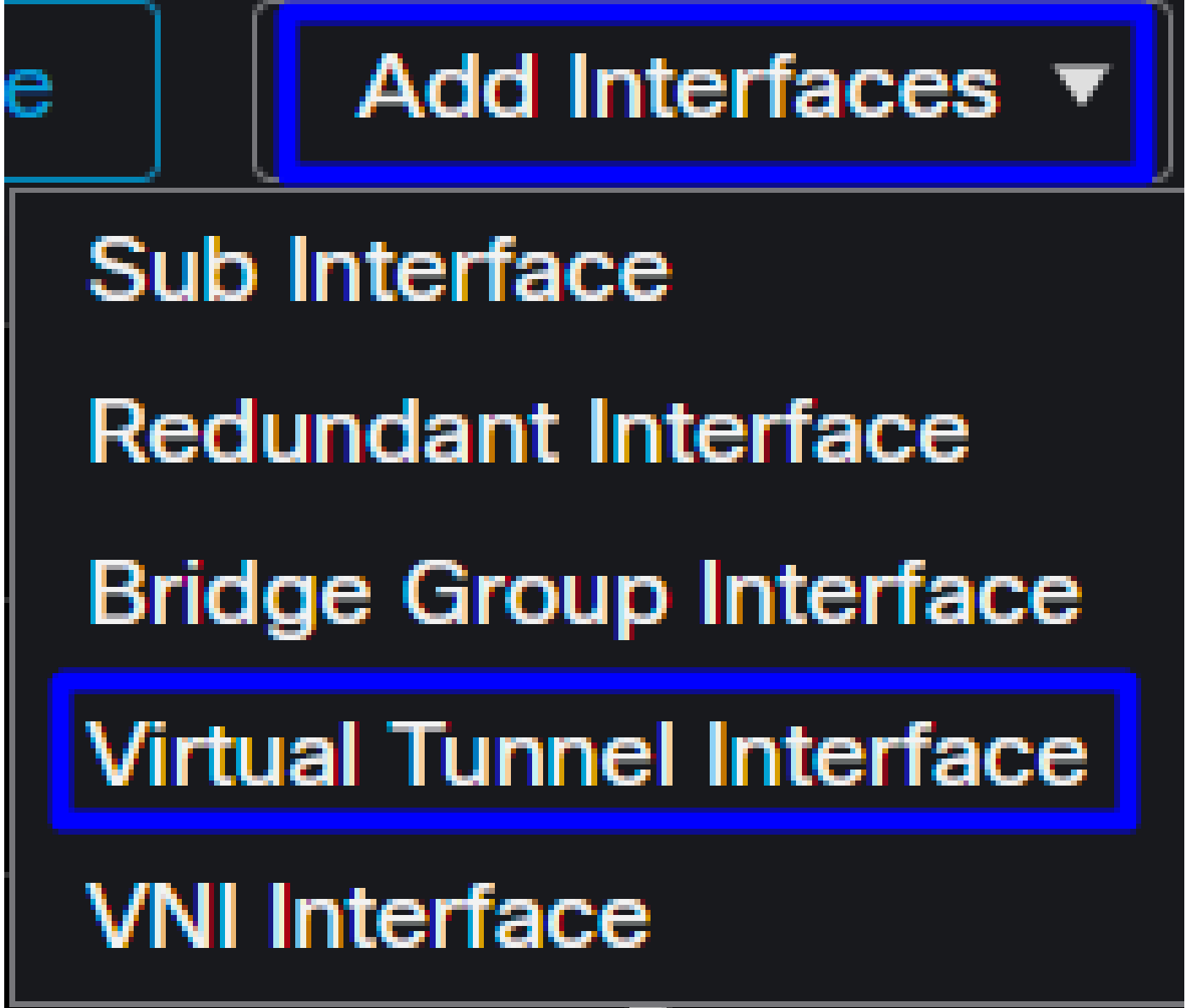
Based on the scenario, we have **PrimaryWAN** and **SecondaryWAN**, which we must use to create the VTI interfaces.

Navigate to your Firepower Management Center > Devices.

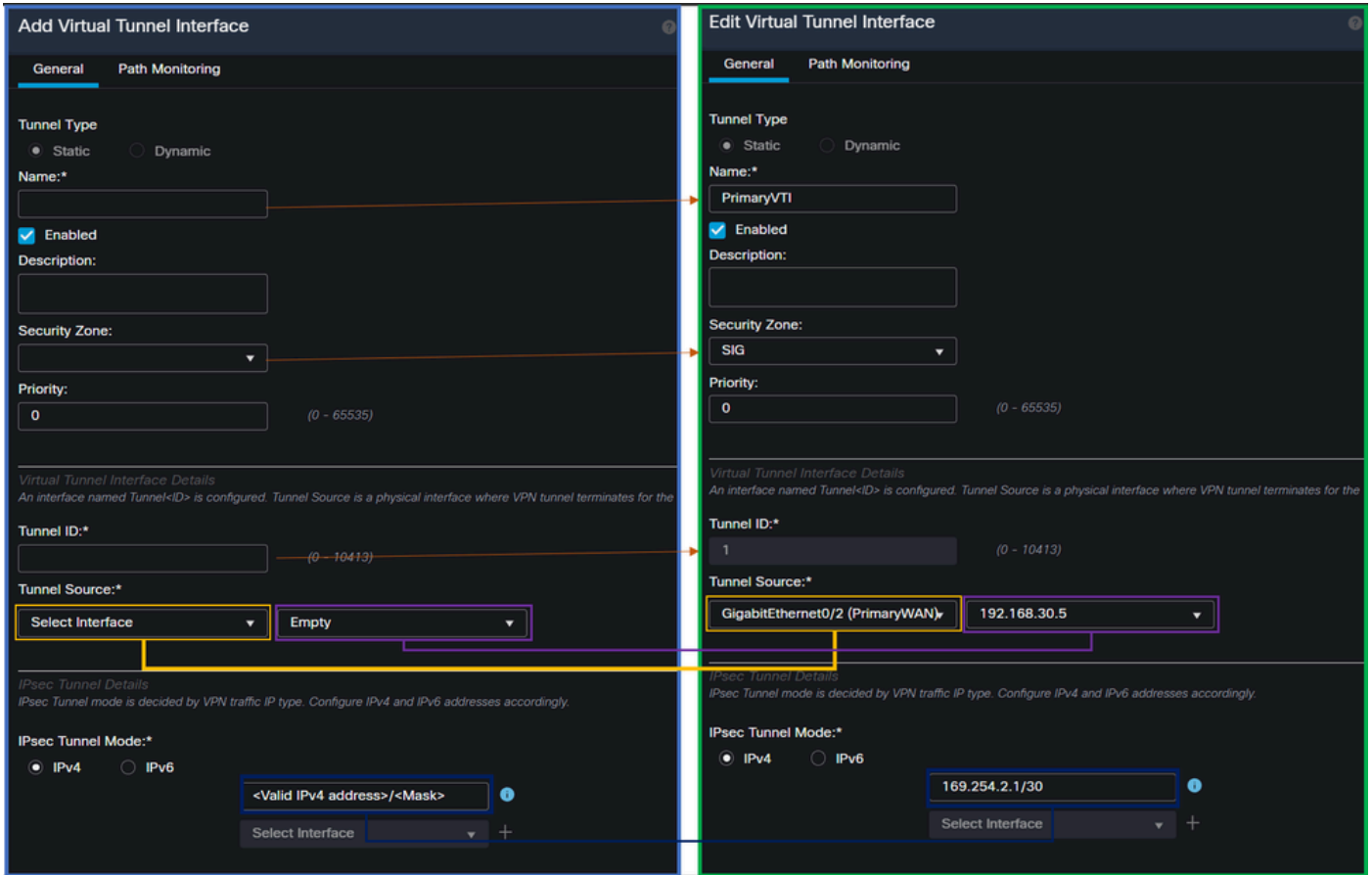
- Choose your FTD
- Choose **Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- Click on **Add Interfaces > Virtual Tunnel Interface**



- Configure the interface based on the next information



- **Name** : Configure a name that refers to the **PrimaryWAN** interface
- **Security Zone** : You can reuse another **Security Zone**, but creating a new one for Secure Access traffic is better
- **Tunnel ID** : Add a number for the Tunnel ID
- **Tunnel Source** : Choose your **PrimaryWAN** interface and choose the private or public IP of your interface
- **IPsec Tunnel Mode** : Choose **IPv4** and configure a non-routable IP in your network with mask 30

Note: For the VTI interface, you must use a non-routable IP; for example, if you have two VTI interfaces, you can use 169.254.2.1/30 for the **PrimaryVTI** and 169.254.3.1/30 for the **SecondaryVTI**.

After that, you need to do the same for the **SecondaryWAN** interface, and you have everything set up for the VTI High Availability, and as a result, you have the next result:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

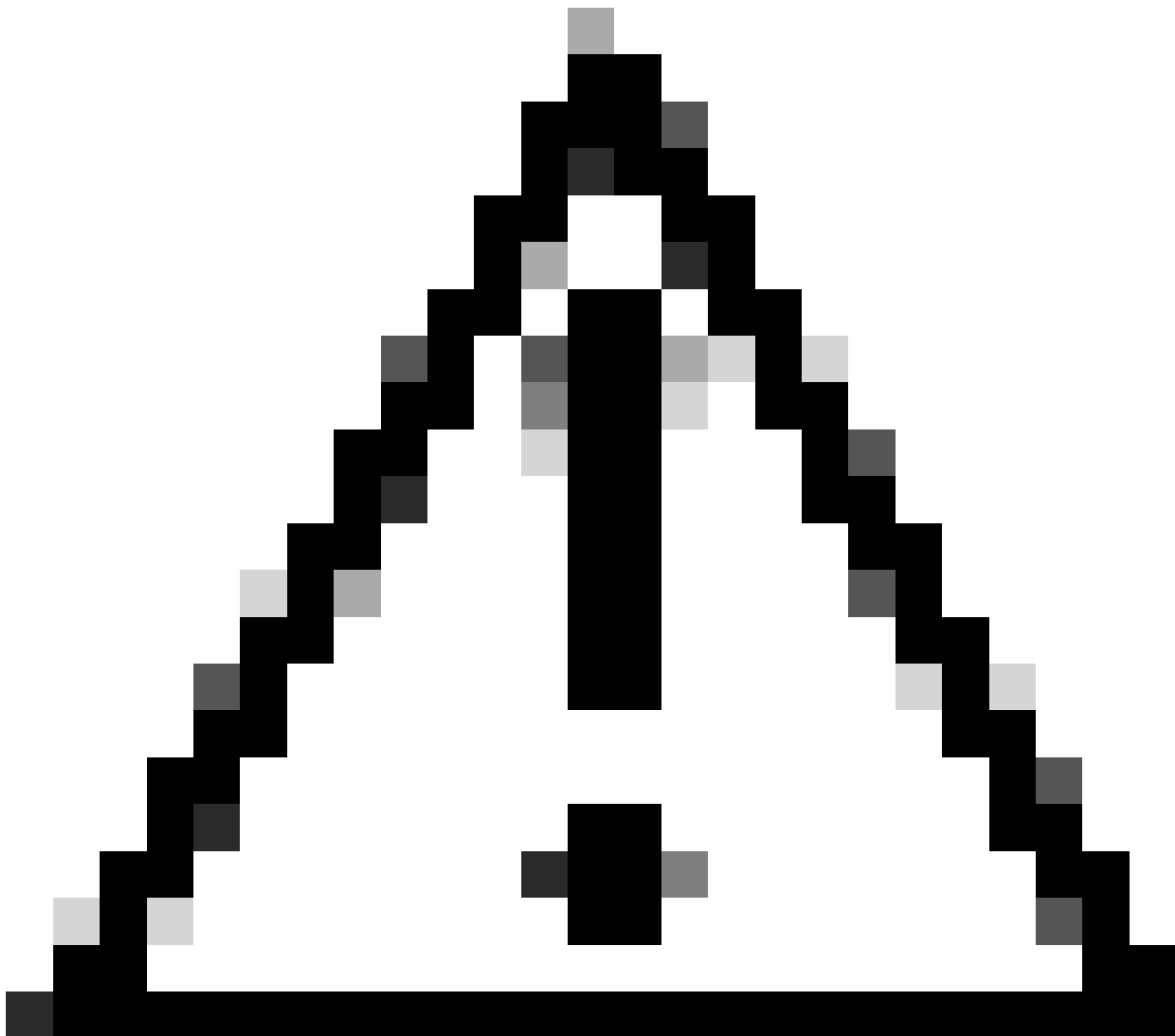
For this scenario, the IPs used are:

VTI IP Configuration

Logical Name	IP	Range
PrimaryVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
SecondaryVTI	169.254.3.1/30	169.254.3.1-169.254.3.2

Configure Static Route for the Secondary Interface

To permit the traffic of the **SecondaryWAN interface** to reach the **Secondary Datacenter IP Address** you need to configure a static route to the datacenter IP. You can configure it with a metric of one (1) to make it on top of the routing table; also, specify the IP as a host.



Caution: This is only needed if you do not have an ECMP setup between the WAN channels; if you have ECMP configured, you can jump to the next step.

- Click on your FTD device
- Click on **Routing**
- Choose **Static Route** > + **Add Route**

Edit Static Route Configuration ?

Type: IPv4 IPv6

Interface* SecondaryWAN → Choose the SecondaryWAN interface

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

Available Network ↻ +

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Add

Selected Network SecureAccessTunnel 🗑️

↓ Choose the Secondary Datacenter IP

Ensure that egress virtualrouter has route to that destination

Gateway Outside_GW → Choose the SecondaryWAN Gateway

Metric:

(1 - 254)

Tunneled: (Used only for default Route)





Route Tracking:

+

Cancel
OK

- **Interface:** Choose the SecondaryWAN Interface
- **Gateway:** Choose the SecondaryWAN Gateway

- Selected Network: Add the Secondary Datacenter IP as a host; you can find the information on the information given when you configure the tunnel on Secure Access step, [Data for Tunnel Setup](#)
- Metric: Use one (1)
- Click **OK** and **Save** to save the information, then deploy.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	 
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	 
▼ IPv6 Routes						

Configure the VPN to Secure Access in VTI Mode

To configure the VPN, navigate to your firewall:

- Click on **Devices > Site to Site**
- Click on **+ Site to Site VPN**

Endpoints Configuration

To configure the Endpoints step, you need to use the information provided under the step, [Data for Tunnel Setup](#).

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

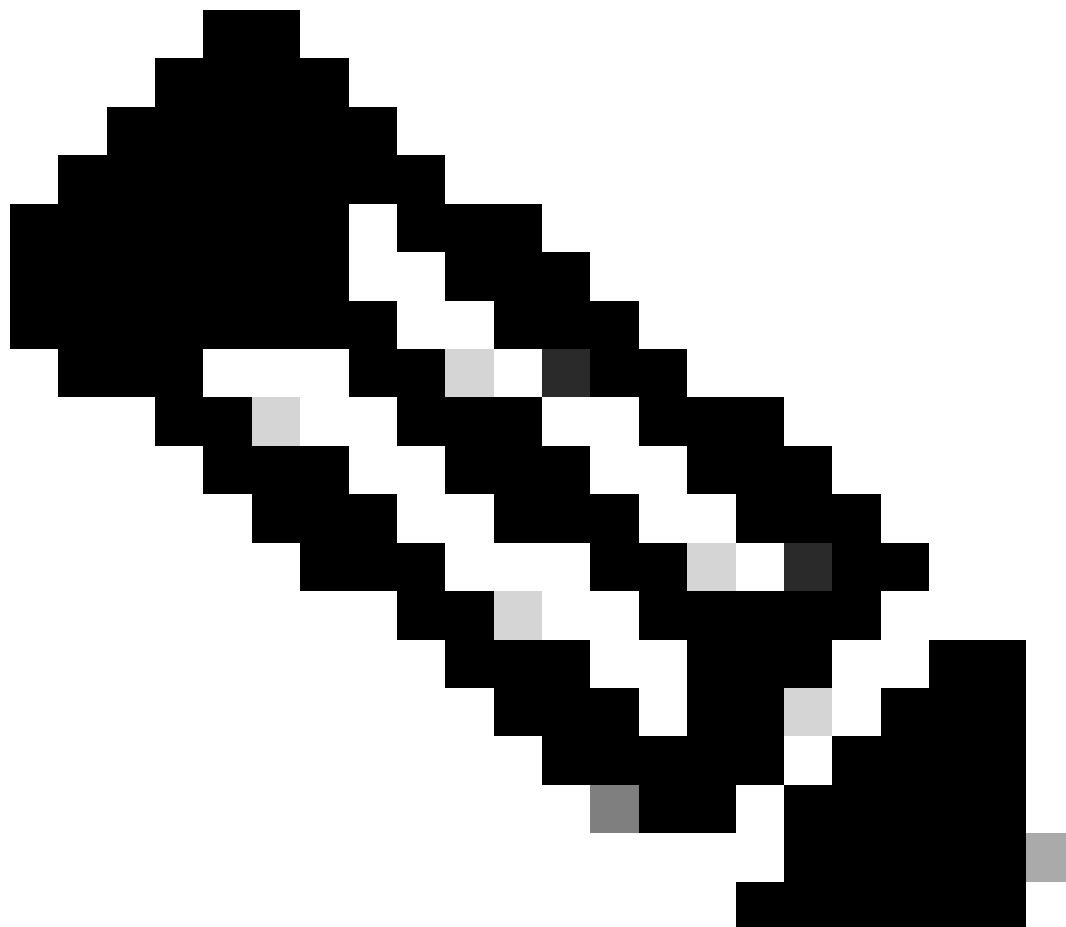
IKE Version:* IKEv1 IKEv2

Endpoints

Node A	Node B
Device:* <input type="text" value="FTD_HOME"/>	Device:* <input type="text" value="Extranet"/>
Virtual Tunnel Interface:* <input type="text" value="PrimaryVTI (IP: 169.254.2.1)"/> +	Device Name*: <input type="text" value="SecureAccess"/>
Tunnel Source: PrimaryWAN (IP: 192.168.30.5) Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers	Endpoint IP Address*: <input type="text" value="18.156.145.74,3.120.45.23"/>
Local Identity Configuration:* <input type="text" value="Email ID"/> <input type="text" value="jairohome@8195126-615626006-"/>	
Backup VTI: Remove	

- Topology Name: Create a name related to the Secure Access integration

- Choose **Routed Based (VTI)**
 - Choose **Point to Point**
 - IKE Version: Choose **IKEv2**
-



Note: IKEv1 is not supported for integration with Secure Access.

Under the **Node A**, you need to configure the next parameters:

Node A

Device:*

FTD_HOME ▼

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1) ▼



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@ [redacted]

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

- **Device:** Choose your FTD device
- **Virtual Tunnel Interface:** Choose the VTI related to the **PrimaryWAN Interface**.
- Mark the checkbox for **Send Local Identity to Peers**
- **Local Identity Configuration:** Choose Email ID, and fill in the information based on the **Primary Tunnel ID** provided in your configuration on the step, [Data for Tunnel Setup](#)

After you configure the information on the **PrimaryVTI** click on **+ Add Backup VTI:**

Backup VTI:

Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼



Tunnel Source: SecondaryWAN (IP: 192.168.0.202) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@

- **Virtual Tunnel Interface:** Choose the VTI related to the **PrimaryWAN Interface**.
- Mark the checkbox for **Send Local Identity to Peers**
- **Local Identity Configuration:** Choose **Email ID**, and fill in the information based on the **Secondary Tunnel ID** provided in your configuration on the step, [Data for Tunnel Setup](#)

Under the **Node B**, you need to configure the next parameters:

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- **Device:** Extranet
- **Device Name:** Choose a Name to recognize Secure Access as the destination.
- **Endpoint IP Address:** The configuration for primary and secondary must be Primary **Datacenter IP**, Secondary **Datacenter IP**, you can find that information in the step, [Data for Tunnel Setup](#)

After that, your configuration for **Endpoints** is completed, and you can now go to the step, IKE Configuration.

IKE Configuration

To configure the IKE parameters, click on **IKE**.

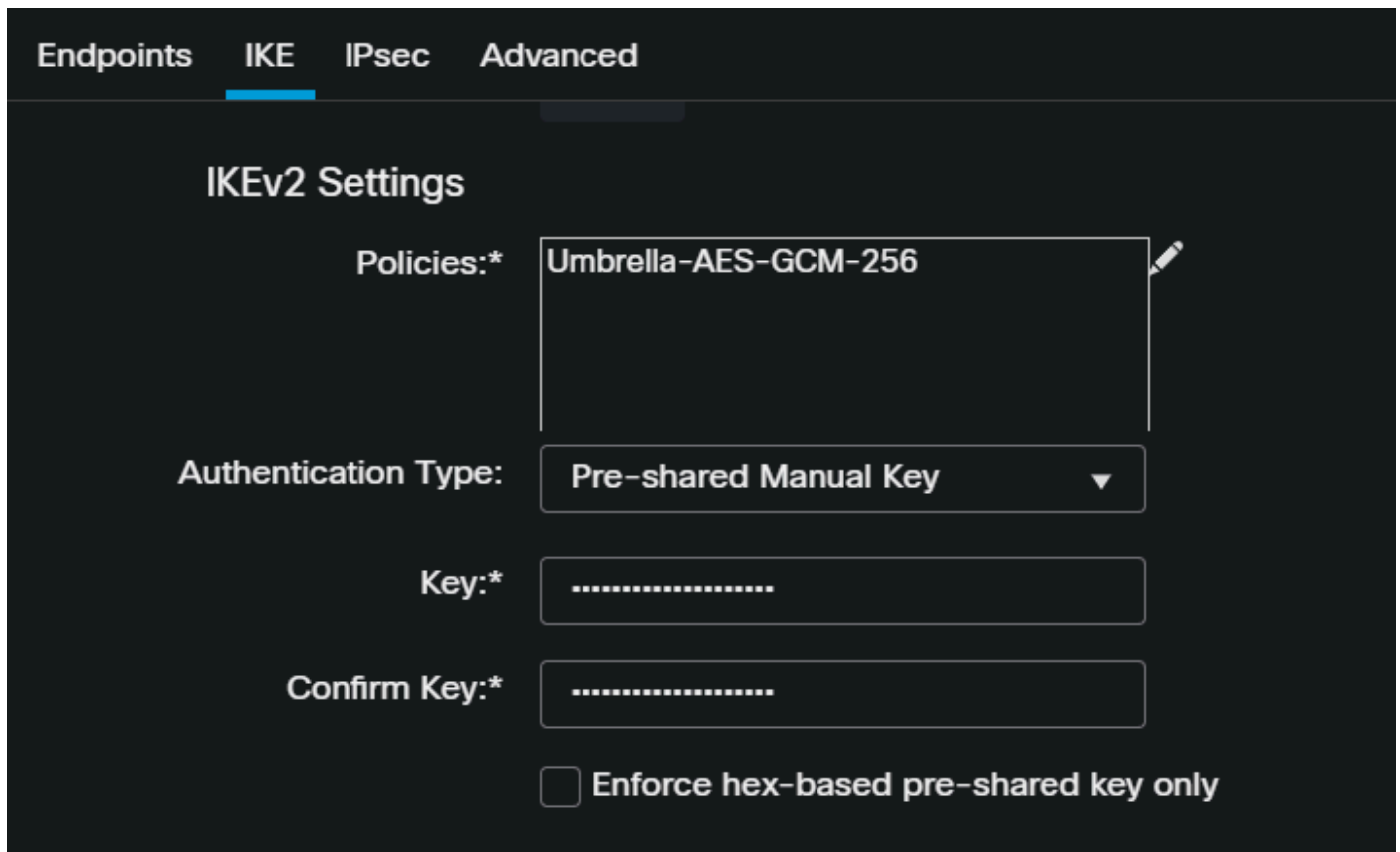
Endpoints

IKE

IPsec

Advanced

Under **IKE**, you need to configure the next parameters:



- **Policies:** You can use the default Umbrella configuration **Umbrella-AES-GCM-256** or you can configure a different parameters based on the [Supported IKEv2 and IPSEC Parameters](#)
- **Authentication Type:** Pre-shared Manual Key
- **Key and Confirm Key:** You can find the **Passphrase** information in the step, [Data for Tunnel Setup](#)

After that, your configuration for **IKE** is completed, and you can now go to the step, **IPSEC Configuration**.

IPSEC Configuration



To configure the IPSEC parameters, click on IPSEC.



Under **IPSEC**, you need to configure the next parameters:

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: You can use the default Umbrella configuration **Umbrella-AES-GCM-256** or you can configure a different parameters based on the [Supported IKEv2 and IPSEC Parameters](#)

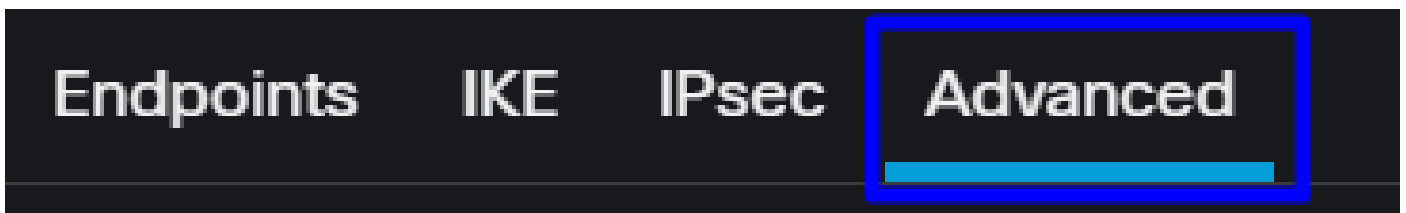


Note: Nothing else is required on IPSEC.

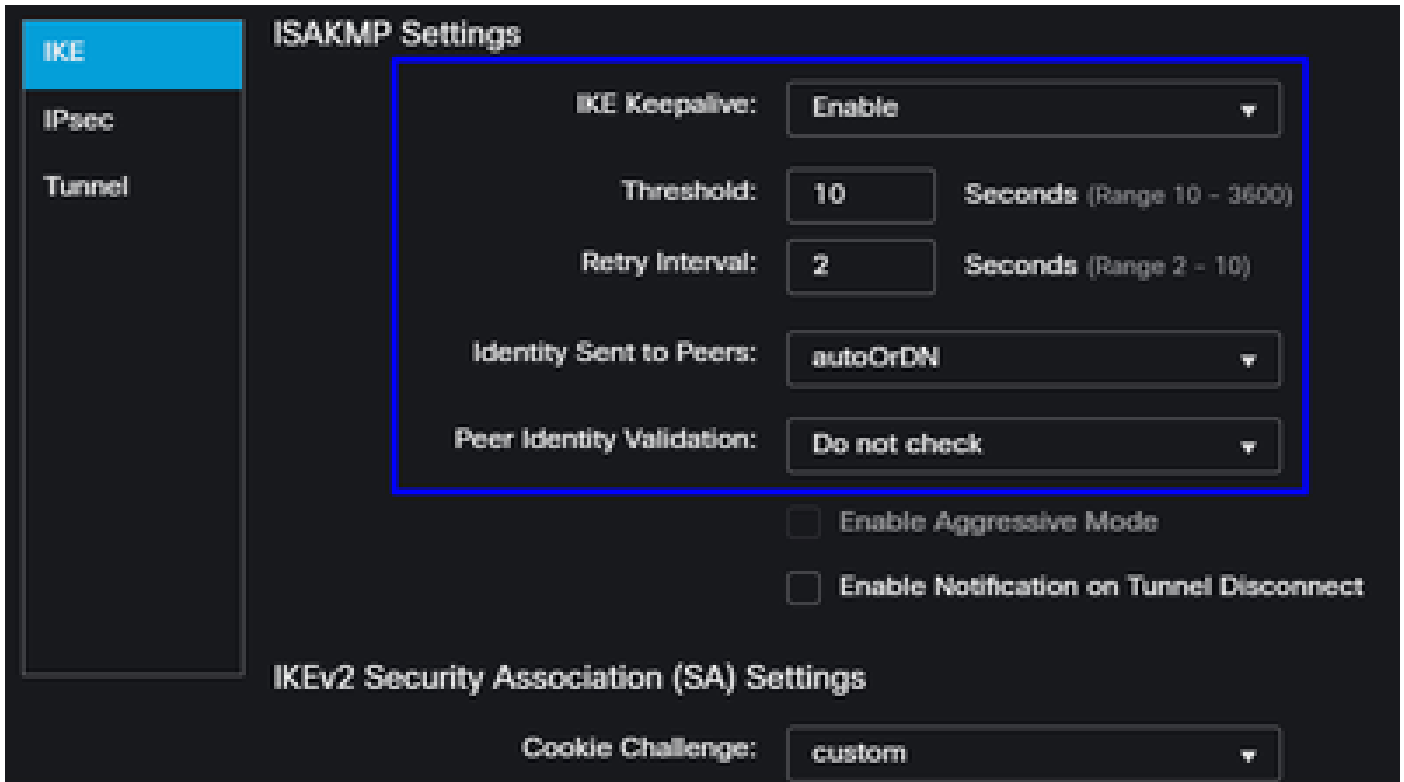
After that, your configuration for **IPSEC** is completed, and you can now go to the step, Advanced Configuration.

Advanced Configuration

To configure the advanced parameters, click on Advanced.



Under **Advanced**, you need to configure the next parameters:



- **IKE Keepalive:** Enable
- **Threshold:** 10
- **Retry Interval:** 2
- **Identity Sent to Peers:** autoOrDN
- **Peer Identity Validation:** Do not Check

After that, you can click on **Save** and **Deploy**.



Note: After a few minutes, you see the VPN established for both nodes.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet	3.120.4... (3.120.45.23)●.....	FTD FTD_HOME	Secon... (192.168.0.202)	Seconda... (169.254.3.1)
EXTRANET Extranet	18.15... (18.156.145.74)●.....	FTD FTD_HOME	Primary... (192.168.30.5)	PrimaryVTI (169.254.2.1)

After that, your configuration for the VPN to Secure Access in VTI Mode is completed, and you can now go to the step, **Configure Policy Base Routing**.



Warning: Traffic to Secure Access is forwarded only to the primary Tunnel when both tunnels are established; if the primary gets down, Secure Access allow the traffic to be forwarded through the secondary Tunnel.

Note: The failover on the Secure Access site is based on the DPD values documented on the [user guide](#) for Supported IPsec values.

Access Policy Configuration Scenarios

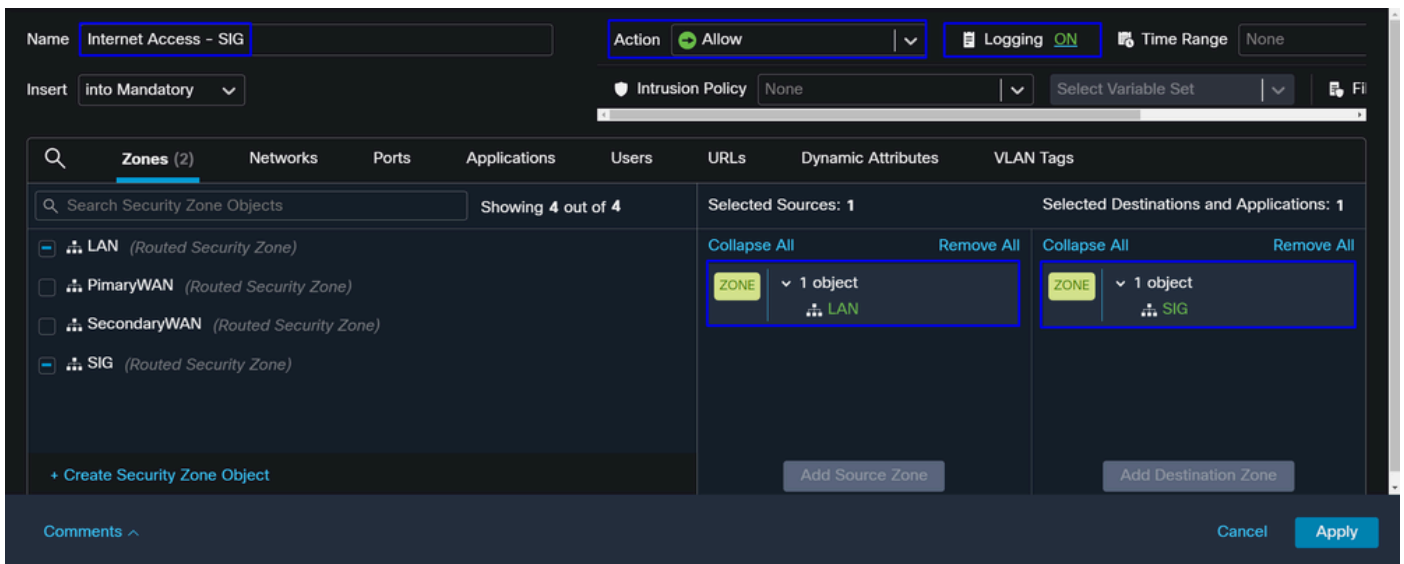
The access policy rules defined are based on:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

Interface	Zone
PrimaryVTI	SIG
SecondaryVTI	SIG
LAN	LAN

Internet Access Scenario

To provide access to the internet to all the resources that you configure on the Policy Base Routing, you need to configure some access rules and also some policies in secure access, so let me explain how to achieve that in this scenario:



This rule provide access to the LAN to the Internet, and in this case, the Internet is SIG.

RA-VPN Escenario

To provide access from the RA-VPN users, you need to configure it based on the range you assigned on the RA-VPN Pool.



Note: To configure your RA-VPNaaS policy, you can go through [Manage Virtual Private Networks](#)

How do you verify the IP pool of your VPNaaS?

Navigate to your [Secure Access Dashboard](#)

- Click on **Connect > End User Connectivity**
- Click on **Virtual Private Network**
- Under **Manage IP Pools**, click on **Manage**

End User Connectivity ↓ Cisco Secure Client Manage DNS Servers (2)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** Internet Security

Global FQDN
fb57.vpn.sse.cisco.com [Copy](#)

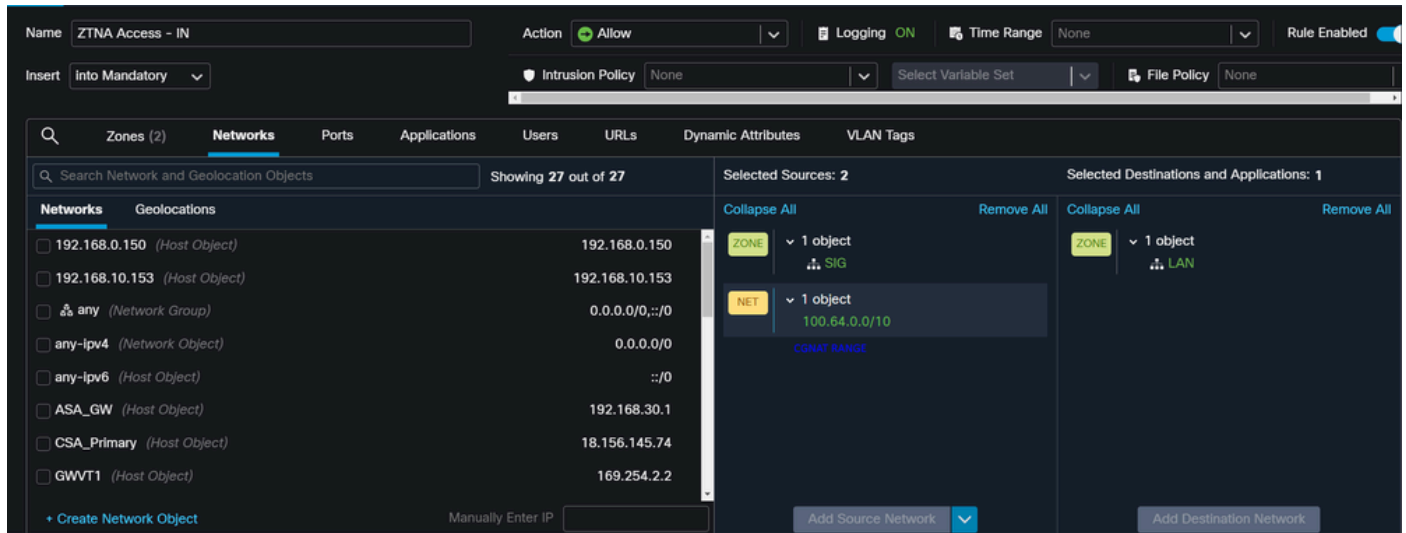
Manage IP Pools Manage
2 Regions mapped

CLAP-BAP ZTNA Escenario

You must configure your network based on the CGNAT range 100.64.0.0/10 to provide access to your network from the Client Base ZTA or Browser Base ZTA users.

Access Rule Configuration

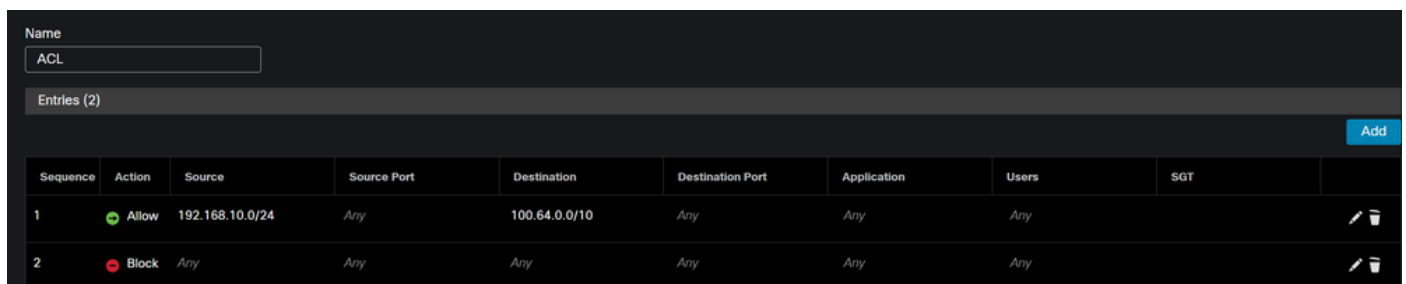
If you are only configuring Secure Access to use it with the capabilities to access the private applications resources, your access rule can look like this:



That rule permits traffic from the ZTNA CGNAT Range 100.64.0.0/10 to your LAN.

ACL Configuration

To permit the routing traffic from SIG using CGNAT to your LAN, you must add it under the ACL to make it work under the PBR.



Configure Policy Base Routing

To provide access to internal resources and the Internet through Secure Access, you must create routes via Policy Base Routing (PBR) that facilitate routing the traffic from the source to the destination.

- Navigate to **Devices > Device Management**
- Choose the FTD device where you create the route

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungruped (1)		
<input checked="" type="checkbox"/>	FTD_HOME Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- Click on **Routing**
- Choose Policy Base Routing
- Click Add

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

In this scenario, you select all the interfaces you use as a source to route traffic to Secure Access or to provide user authentication to Secure Access using RA-VPN or client-based or browser-based ZTA access to the Network internal resources:

- Under Ingress Interface, select all the interfaces that send traffic through Secure Access:

Edit Policy Based Route

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

Ingress Interface*

LAN

- Under Match Criteria and Egress Interface, you define the next parameters after you click on Add:

Match Criteria and Egress Interface
 Specify forward action for chosen match criteria.

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

↑ Internal Sources

Match ACL:* ACL

Send To:* IP Address

IPv4 Addresses: 169.254.2.2, 169.254.3.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

- **Match ACL:** For this ACL, you configure everything that you route to Secure Access:

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✗ REJECT

Name: SSPT_FTD_ACL

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.222.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✓ ACCEPT

- **Send To:** Choose IP Address
- **IPv4 Addresses:** You must use the next IP under the mask 30 configured on both VTI; you can check that under the step, [VTI Interface Config](#)

Interface	IP	GW
PrimaryVTI	169.254.2.1/30	169.254.2.2
SecondaryVTI	169.254.3.1/30	169.254.3.2



After you configure it like that, you have the next result, and you can proceed to click Save:

Match ACL:* **ACL** +

Send To:* **IP Address**

IPv4 Addresses: **169.254.2.2,169.254.3.2**

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: **None**

Default Interface

IPv4 settings IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel Save

After that, you need to Save it again, and you have it configured in the next way:

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

Ingress Interface* **LAN**

Match Criteria and Egress Interface Add

Specify forward action for chosen match criteria.

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 169.254.3.2 → Send the traffic to the PrimaryVTI

If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save



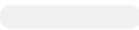


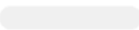


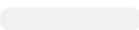


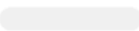


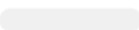


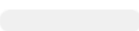


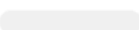

After that, you can Deploy, and you see the traffic of the machines configured on the ACL routing the traffic to Secure Access:

From the **Conexion Events** in the FMC:

<input type="checkbox"/>	Action ×	Initiator IP ×	Responder IP ×	↓ Application Risk ×	Access Control Policy ×	Ingress Interface ×	Egress Interface ×
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

From the Activity Search in Secure Access:

40,678 Total  Viewing activity from Mar 13, 2024 12:30 AM to Mar 14, 2024 12:30 AM Page: 1  Results per page

Request	Source	Rule Identity 	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	



Note: By default, the default Secure Access Policy allows traffic to the internet. To provide access to private applications, you need to create private resources and add them to the access policy for private resource access.

Configure Internet Access Policy on Secure Access

To configure the access for internet access, you need to create the policy on your [Secure Access Dashboard](#):

- Click on **Secure > Access Policy**

The screenshot shows a navigation sidebar on the left with four items: 'Secure' (highlighted with a blue border), 'Monitor', 'Admin', and 'Workflows'. The main content area is titled 'Policy' and contains two items: 'Access Policy' (highlighted with a blue border) and 'Data Loss Prevention Policy'. The 'Access Policy' description reads: 'Create rules to control and secure access to private and internet destinations'. The 'Data Loss Prevention Policy' description reads: 'Prevent data loss/leakage with policy rules'.

- Click on Add Rule > Internet Access

The screenshot shows a dialog box with a blue 'Add Rule ^' button in the top right corner. The dialog contains two options, each with a title and a description:

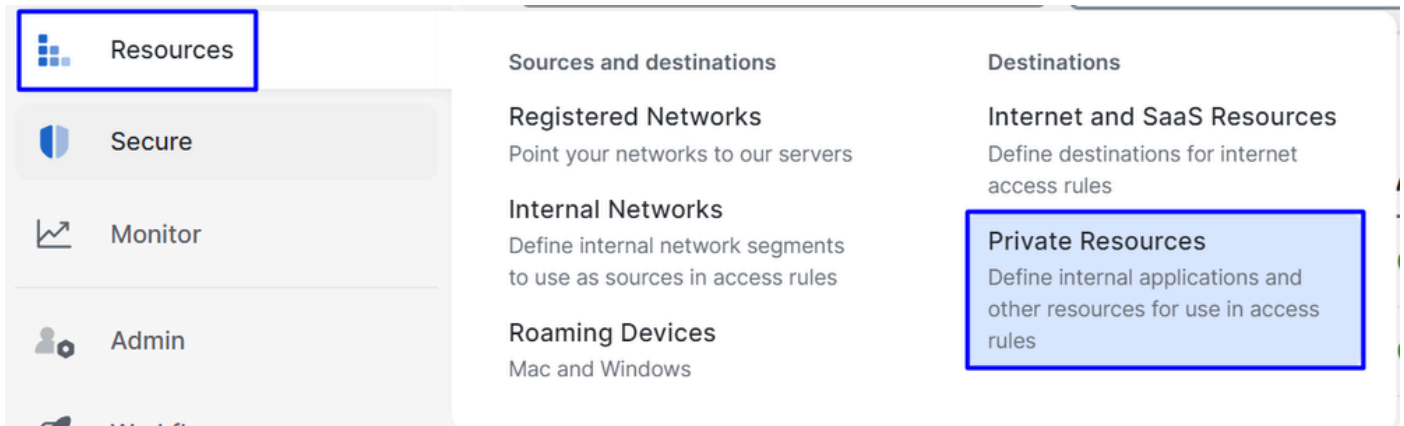
- Private Access**
Control and secure access to resources and applications that cannot be accessed by the general public.
- Internet Access**
Control and secure access to public destinations from within your network and from managed devices

There, you can specify the source as the tunnel, and to the destination, you can choose any, depending on what you want to configure on the policy. Please check the [Secure Access User Guide](#).

Configure Private Resource Access for ZTNA and RA-VPN

To configure the access for private resources, you need to create the resources first under the [Secure Access Dashboard](#):

Click on **Resources > Private Resources**



- Then click **ADD**

Under the configuration, you find the next sections to configure: **General**, **Communication with Secure Access Cloud** and **Endpoint Connection Methods**.

General

General

Private Resource Name

Description (optional)

- Private Resource Name : Create a name for the resource you provide access through Secure Access to your network

Endpoint Connection Methods

Zero-trust connections
 Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
 Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
 Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ
 https:// ⓘ

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:** Mark the checkbox.
- **Client-based connection:** If you enable it, you can use the Secure Client - Zero Trust Module to enable access through client-base mode.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Configure the resources IP or FQDN; if you configure FQDN, you need to add the DNS to resolve the name.
- **Browser-based connection:** If you enable it, you can access your resources via browser (Please only add resources with HTTP or HTTPS communication)
- **Public URL for this resource:** Configure the public URL you use through the browser; Secure Access protects this resource.
- **Protocol:** Select the protocol (HTTP or HTTPS)

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

VPN Connection: Mark the checkbox to enable access via RA-VPNaaS.

After that, click **Save** and you are able to add that resource to the **Access Policy**.

Configure the Access Policy

When you create the resource, you need to assign it to one of the secure access policies:

- Click on **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Click Add > Private Resource

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

For this Private Access rule, you configure the default values to provide access to the resource. To know more about policy configurations, check the [User Guide](#).

1 Specify Access

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

Action

<input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met.	<input type="radio"/> Block Block specified traffic.
--	--

From

Specify one or more sources.

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

Information about destinations, including selecting multiple destinations. [Help](#)

- **Action** : Choose Allow to provide access to the resource.
- **From** : Specify the user that can be used to log in to the resource.
- **To** : Choose the resource that you want to access through Secure Access.

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

Private Resources: **SplunkFTD**

Zero Trust Browser-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

Private Resources: **SplunkFTD**

- **Zero-Trust Client-based Posture Profile**: Choose the default profile for client base access
- **Zero-Trust Browser-based Posture Profile**: Choose the default profile browser base access



Note: To learn more about the posture policy, please check the [user guide](#) for Secure Access.

After that, click **Next** and **Save** and your configuration, and you can try to access your resources through RA-VPN and Client Base ZTNA or Browser Base ZTNA.

Troubleshoot

To troubleshoot based on the communication between Secure Firewall and Secure Access, you can be able to verify if Phase1 (IKEv2) and phase2 (IPSEC) are established between the devices without a problem.

Verify Phase1 (IKEv2)

To verify Phase1 you need to run the next command on the CLI of your FTD:

```
show crypto isakmp sa
```


In this case, the desired output is two **IKEv2 SAs** established to the Datacenter IPs of Secure Access and the desired status as **READY**:

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
    Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
    Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x4af761fd/0xfbca3343
```

Verify Phase2 (IPSEC)

To verify Phase2, you need to run the next command on the CLI of your FTD:

```
interface: PrimaryVTI
  Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

  Protected vrf (ivrf): Global
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer: 18.156.145.74

  #pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965
  #pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500
  path mtu 1500, ipsec overhead 63(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
```

ICMP error validation: disabled, TFC packets: disabled
current outbound spi: FBCA3343
current inbound spi : 4AF761FD

inbound esp sas:

spi: 0x4AF761FD (1257726461)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (3916242/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0xFBCA3343 (4224332611)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4239174/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

interface: SecondaryVTI

Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 3.120.45.23

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C27FD2BA
current inbound spi : FB34754C

inbound esp sas:

spi: 0xFB34754C (4214519116)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes
replay detection support: Y

```
Anti replay bitmap:
 0x00000000 0x00000001
outbound esp sas:
 spi: 0xC27FD2BA (3263156922)
 SA State: active
 transform: esp-aes-gcm-256 esp-null-hmac no compression
 in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
 slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel12-0-2
 sa timing: remaining key lifetime (kB/sec): (4239360/27412)
 IV size: 8 bytes
 replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

In the last output, you can see both tunnels established; what is not desired is the next output under the packet encaps and decaps.

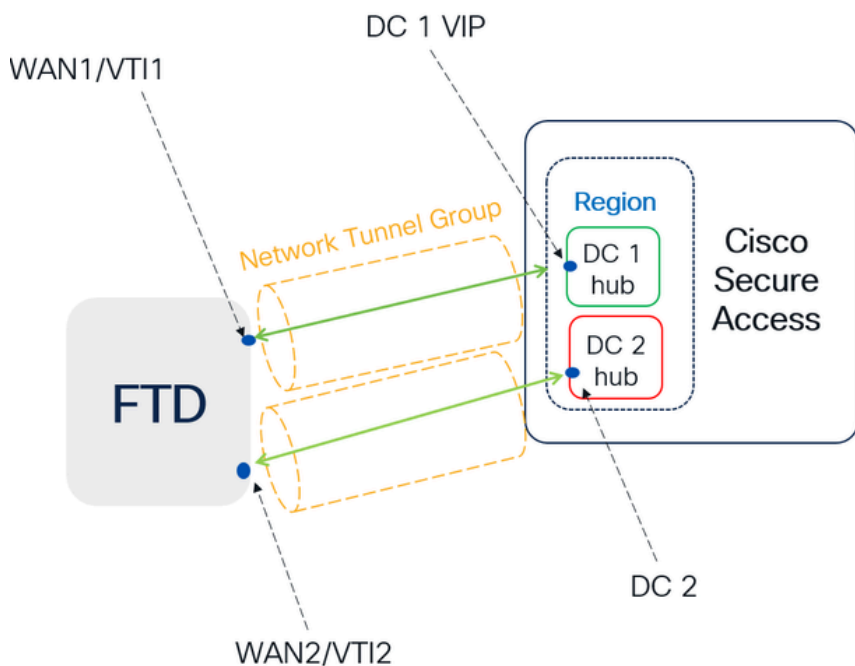
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
Access to your firewall
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

If you have this scenario, open a case with TAC.

High Availability Function

The function of the tunnels with Secure Access communicating with the datacenter in the cloud is active/passive, which means only the door for DC 1 will be open to receive traffic; the DC 2 door is closed until tunnel number 1 gets down.

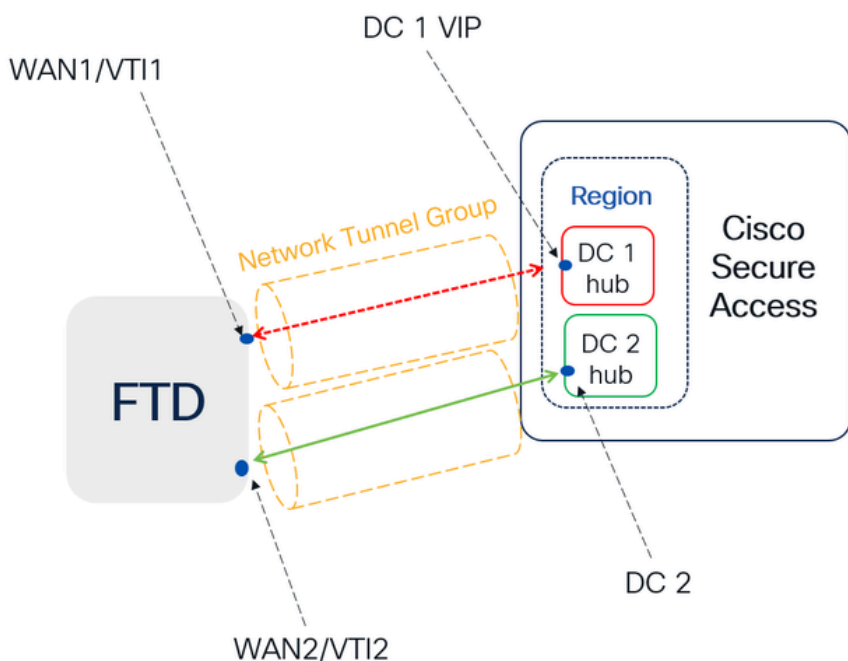
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

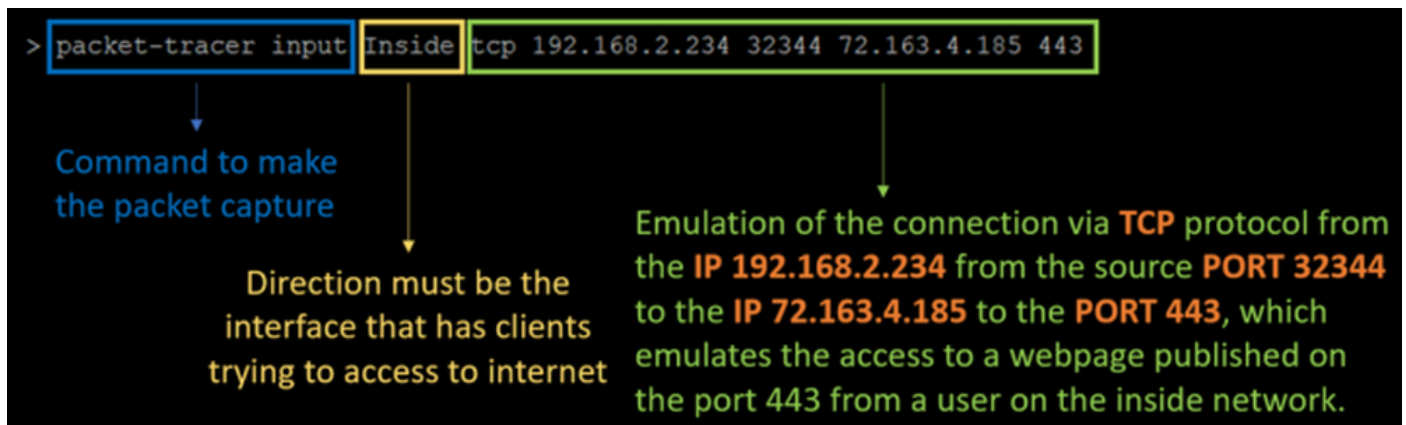
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Verify Traffic Routing to Secure Access

In this example, we use the source as the machine on the firewall network:

- Source: 192.168.10.40
- Destination: 146.112.255.40 (Secure Access Monitoring IP)

Example:



Command:

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

Output:

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 14010 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

```
Phase: 3
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
  Source Object Group Match Count:      0
  Destination Object Group Match Count: 0
  Object Group Search:                  0
```

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 233 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435
access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
class-map class_map_Any
match access-list Any
policy-map policy_map_LAN
class class_map_Any
set connection decrement-ttl
service-policy policy_map_LAN interface LAN
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Elapsed time: 18680 ns
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Elapsed time: 25218 ns
Config:
Additional Information:

Phase: 10
Type: NAT
Subtype: per-session

Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow

Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns

Here, many things can give us context about the communication and know if everything is correctly under the PBR configuration to route the traffic correctly to Secure Access:

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
Matched route-map FMC GENERATED PBR 1707686032813, sequence 5, permit
Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

Phase 2 indicates that the traffic is being forwarded to the **PrimaryVTI** interface, which is correct because, based on the configurations in this scenario, the internet traffic must be forwarded to Secure Access through the VTI.

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information: