Secure Firewall - Configure Umbrella Secure Internet Gateway

Contents

Introduction

This document describes the step-by-step configuration of a Site-to-Site Secure Internet Gateway (SIG) VPN tunnel on Secure Firewall Threat Defense.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Site-to-Site VPNs

- Umbrella Admin Portal
- Secure Firewall Management Center (FMC)

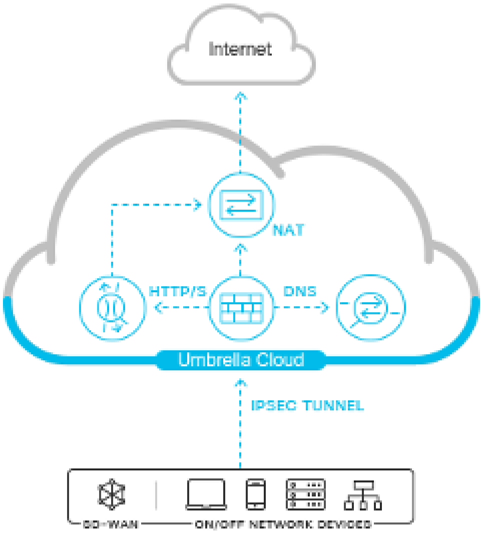
Components Used

The information in this document is based on these software and hardware versions.

- Umbrella Admin Portal
- Secure Firewall Version 7.2

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.

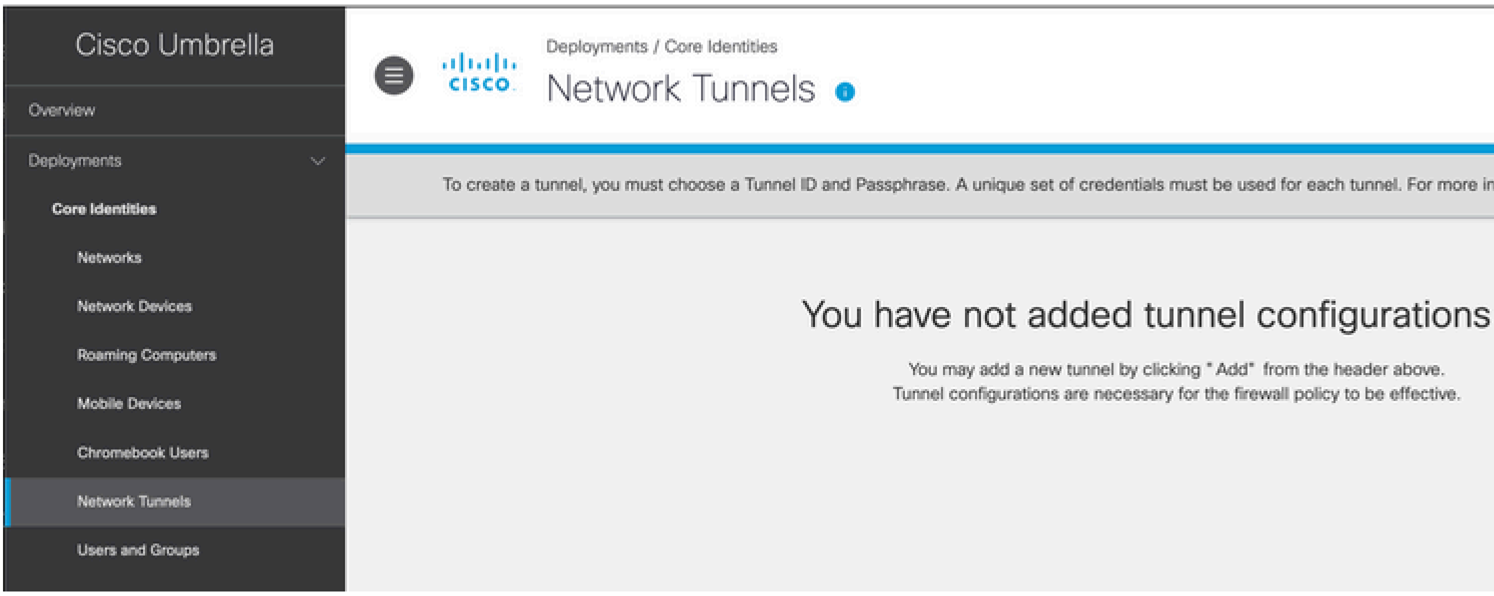
Network Diagram



Umbrella Network Tunnel Configuration

Network Tunnel

Login to Umbrella Dashboard:



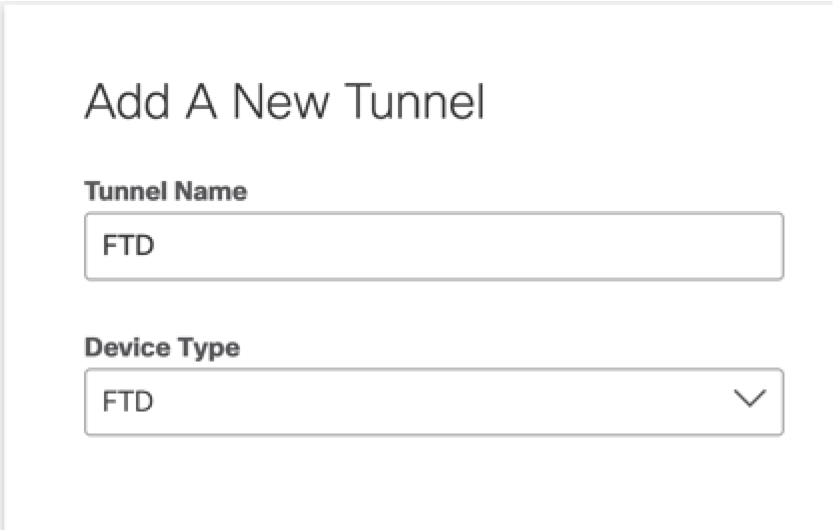
To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more in

You have not added tunnel configurations

You may add a new tunnel by clicking "Add" from the header above.
Tunnel configurations are necessary for the firewall policy to be effective.

Navigate to Deployments > Network Tunnels > Add.

Add a New Tunnel, choose the device type as FTD, and name it appropriately.



Add A New Tunnel

Tunnel Name

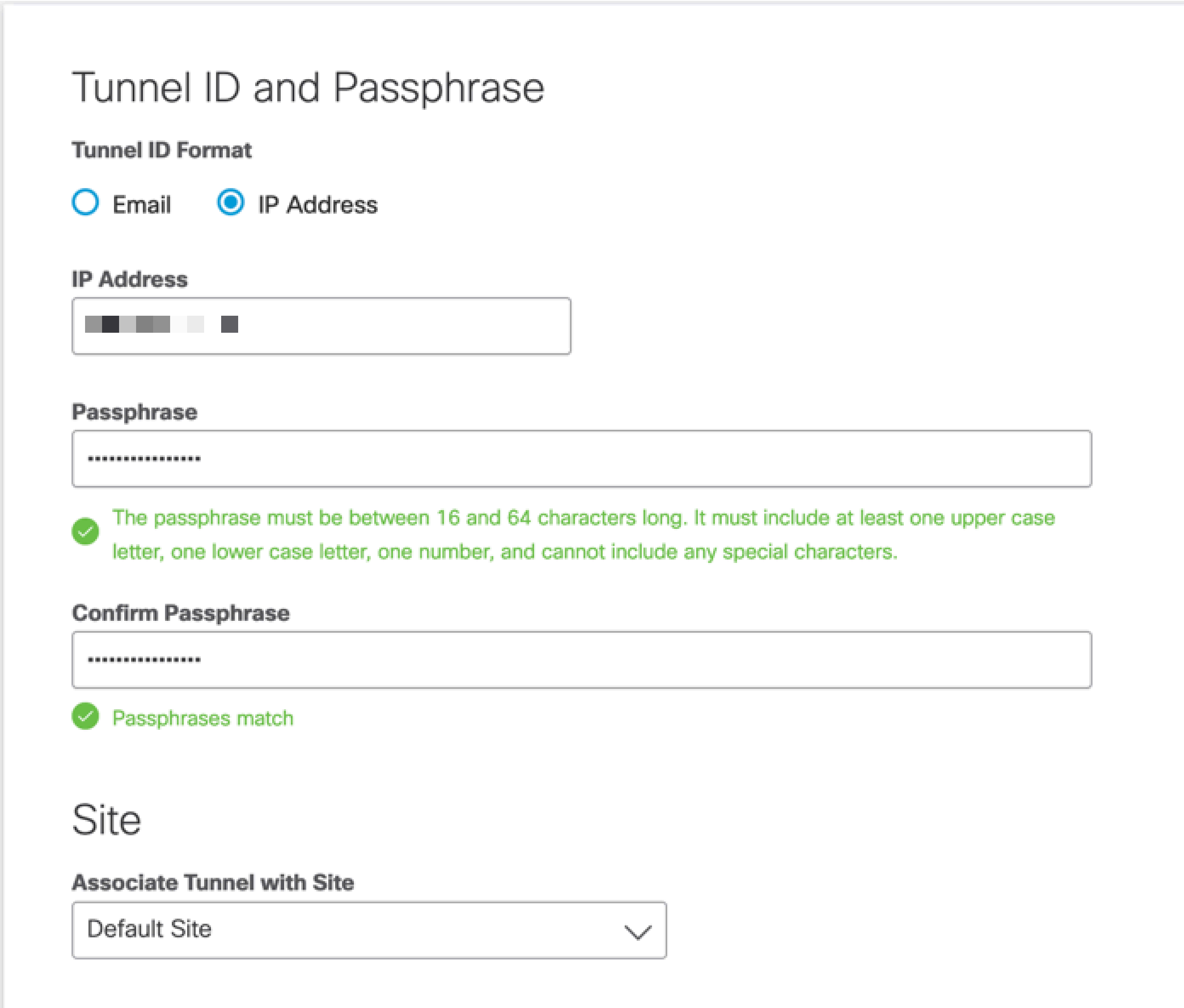
FTD

Device Type

FTD

Enter the Public IP address of the FTD along with a secure pre-shared key.

Attach the tunnel to the appropriate site for firewalling and traffic inspection policies.



Tunnel ID and Passphrase

Tunnel ID Format

○ Email ● IP Address

IP Address

[redacted]

Passphrase

••••••••••••••••

✓ 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

••••••••••••••••

✓ Passphrases match

Site

Associate Tunnel with Site

Default Site

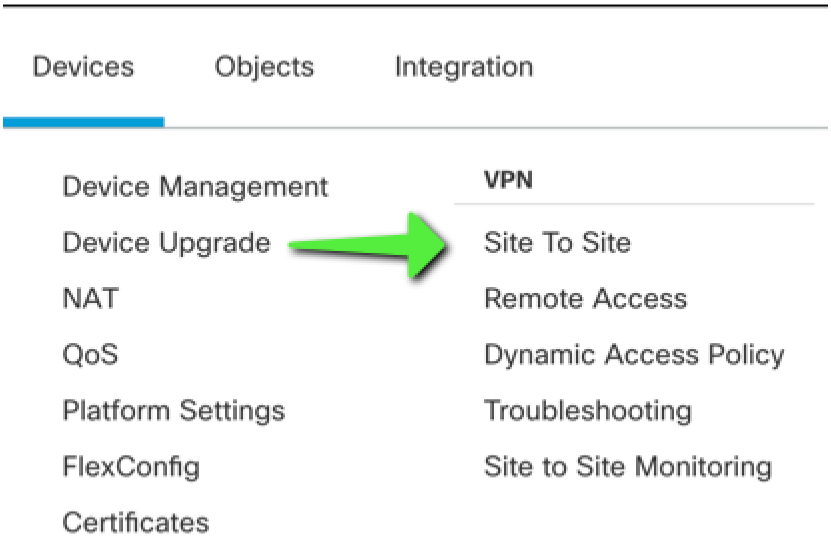
Configuration from Umbrella Portal is now complete.

Navigate to Umbrella Portal when the tunnel is connected in order to confirm the VPN status.

Secure Firewall Management Center Configuration

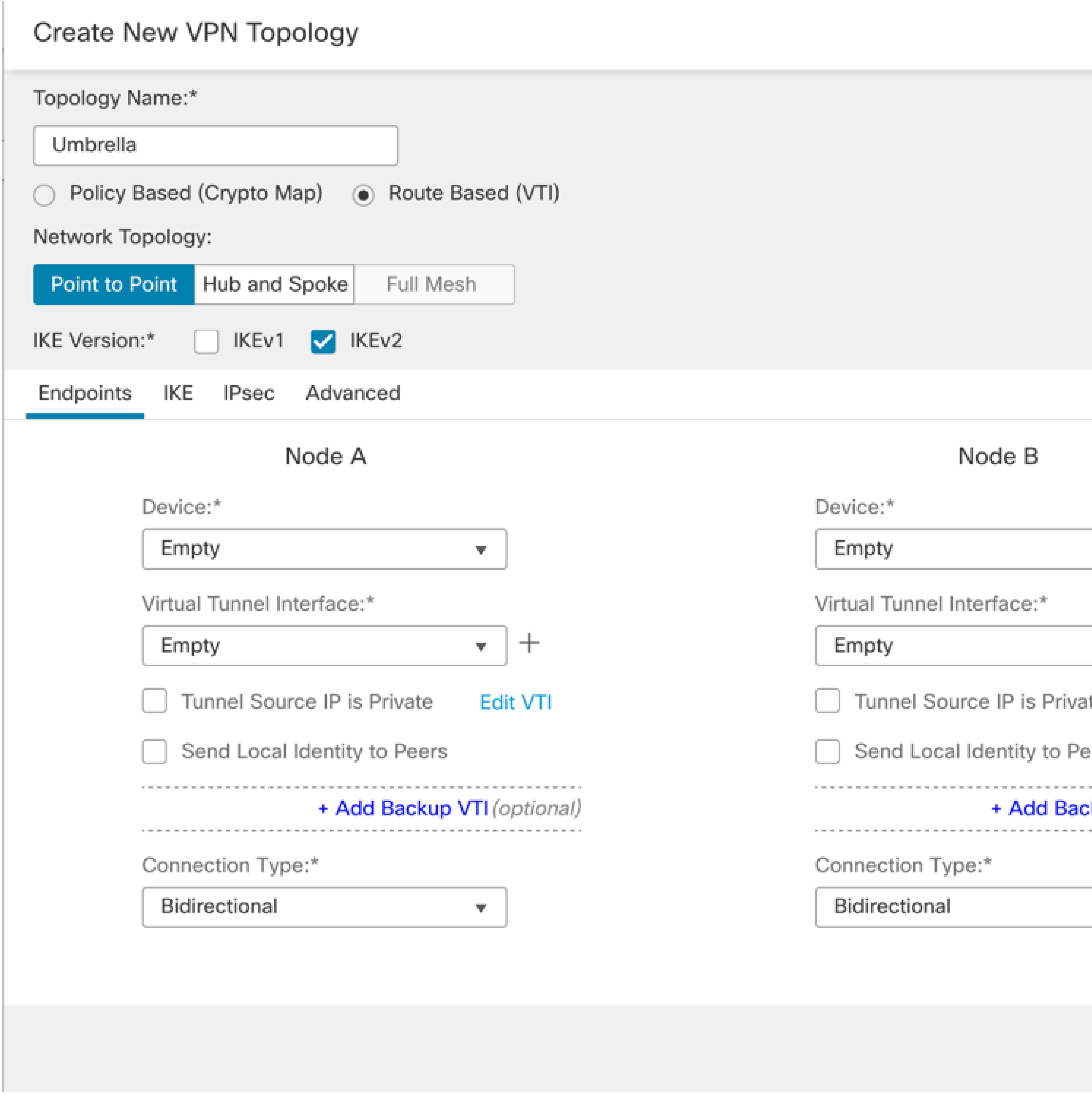
Configure Site-to-Site

Navigate to Devices > Site-to-Site :



Add New Site-to-Site Tunnel

Name the Topology and choose Route-based VTI:



Create New VPN Topology

Topology Name:* Umbrella

○ 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:* Empty

Virtual Tunnel Interface:* Empty +

□ Tunnel Source IP is Private Edit VTI

□ Send Local Identity to Peers

+ Add Backup VTI *(optional)*

Connection Type:* Bidirectional

Node B

Device:* Empty

Virtual Tunnel Interface:* Empty

□ Tunnel Source IP is Privat

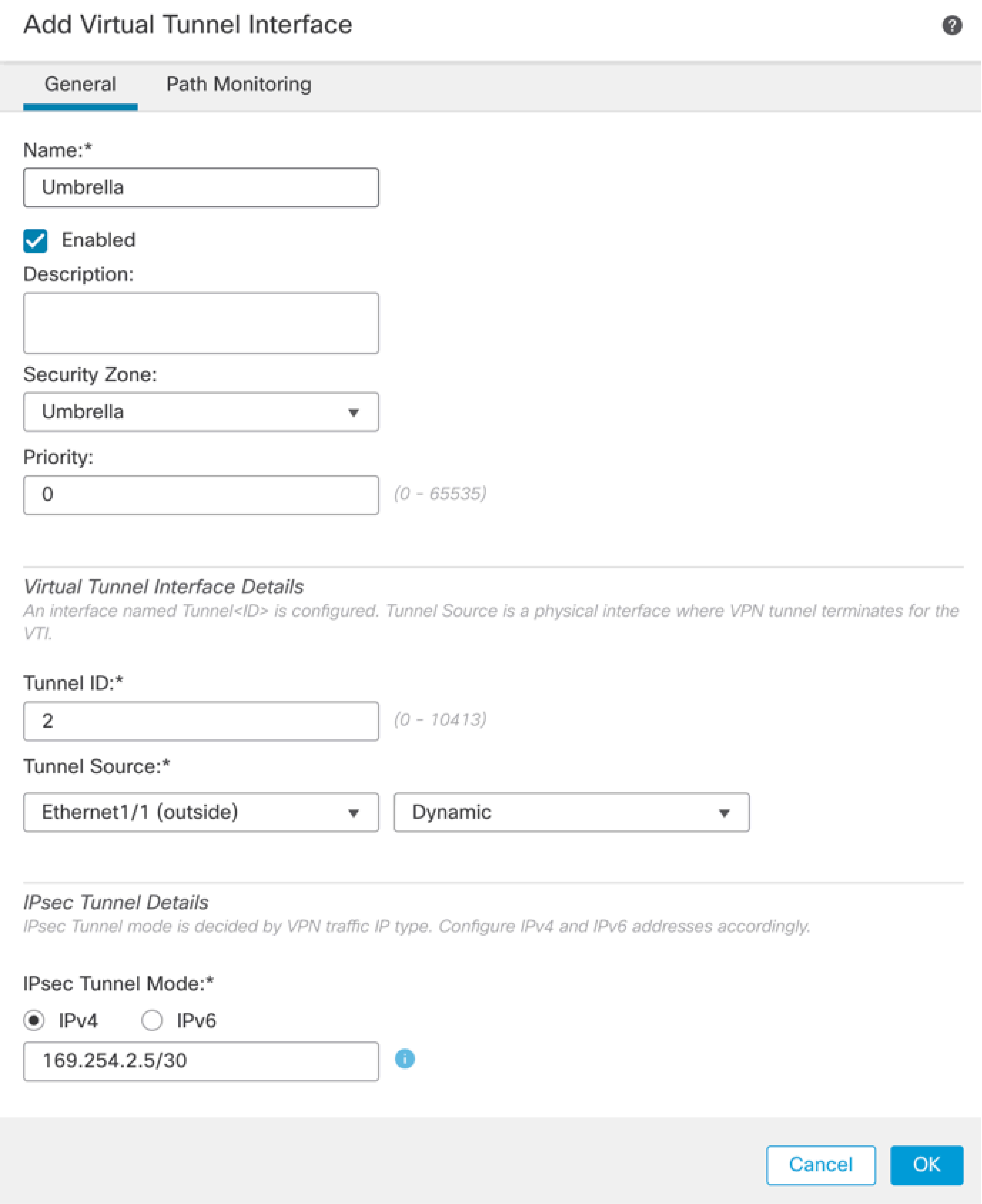
□ Send Local Identity to Pe

+ Add Bac

Connection Type:* Bidirectional

Add a New Virtual Tunnel Interface

- Name the Tunnel Interface
- Apply a New Security Zone to the Interface
- Assign a Tunnel ID number between 0-10413
- Choose Tunnel source (Interface with Public IP defined in Umbrella Portal)
- Create a non-routable/30 subnet for use with the VPN. For example, 169.254.72.0/30



Add Virtual Tunnel Interface

Name:* Umbrella

☑ Enabled

Description:

Security Zone: Umbrella ▾

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:* Ethernet1/1 (outside) ▾ Dynamic ▾

IPsec Tunnel Details

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

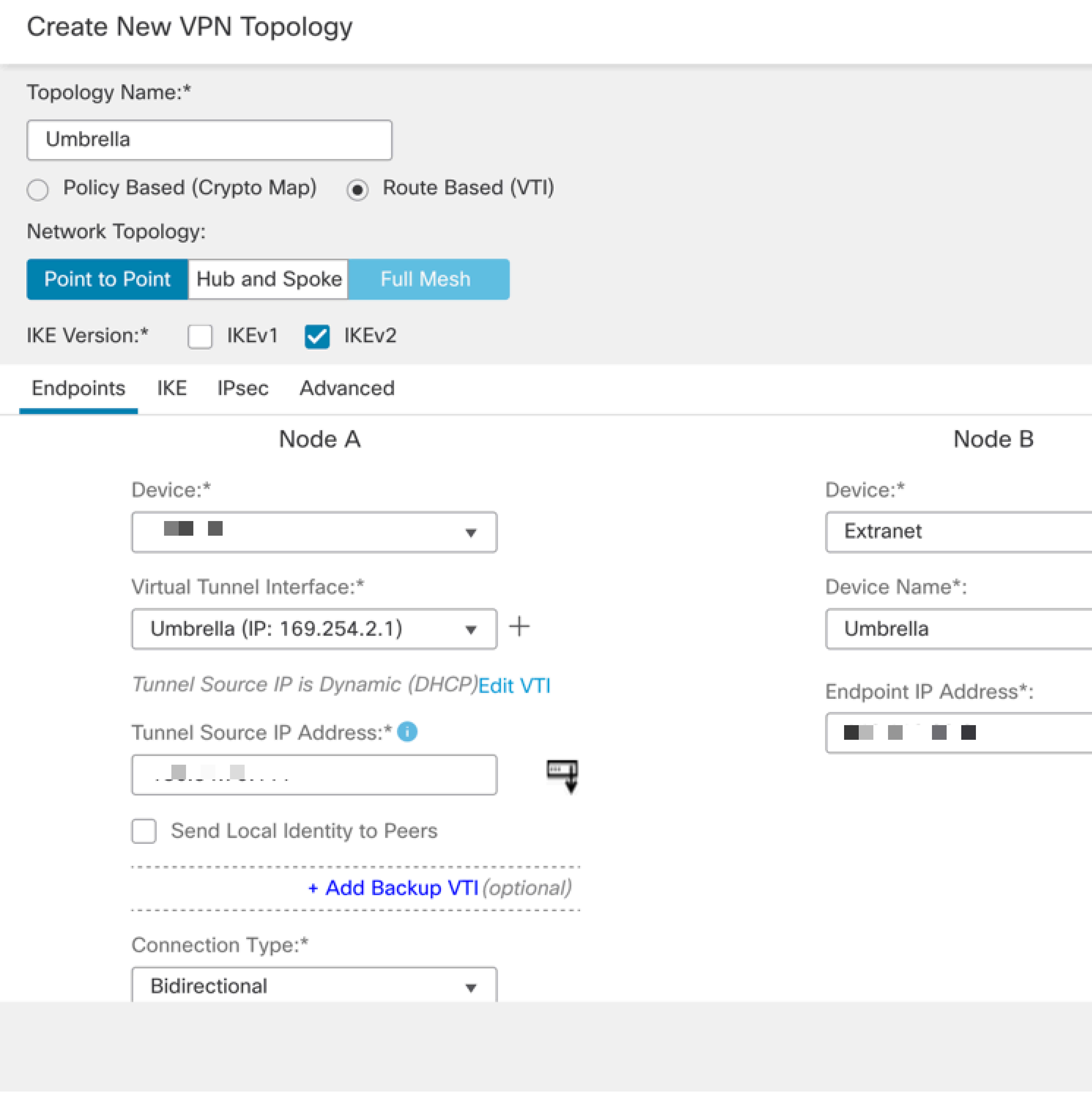
IPsec Tunnel Mode:*

● IPv4 ○ IPv6

169.254.2.5/30

Configure Topology Nodes

Assign FTD to Node A and Umbrella to Extranet Node B:



Create New VPN Topology

Topology Name:*

Umbrella

○ Policy Based (Crypto Map) ● Route Based (VTI)

Network Topology:

IKE Version:* □ IKEv1 ☑ IKEv2

Node A

Device:*

[redacted]

Virtual Tunnel Interface:*

Umbrella (IP: 169.254.2.1)

*Tunnel Source IP is Dynamic (DHCP)*Edit VTI

Tunnel Source IP Address:*

[redacted]

□ Send Local Identity to Peers

+ Add Backup VTI *(optional)*

Connection Type:*

Bidirectional

Node B

Device:*

Extranet

Device Name*:

Umbrella

Endpoint IP Address*:

[redacted]

Endpoint IP addresses for use with Umbrella Data Centers can be found here.

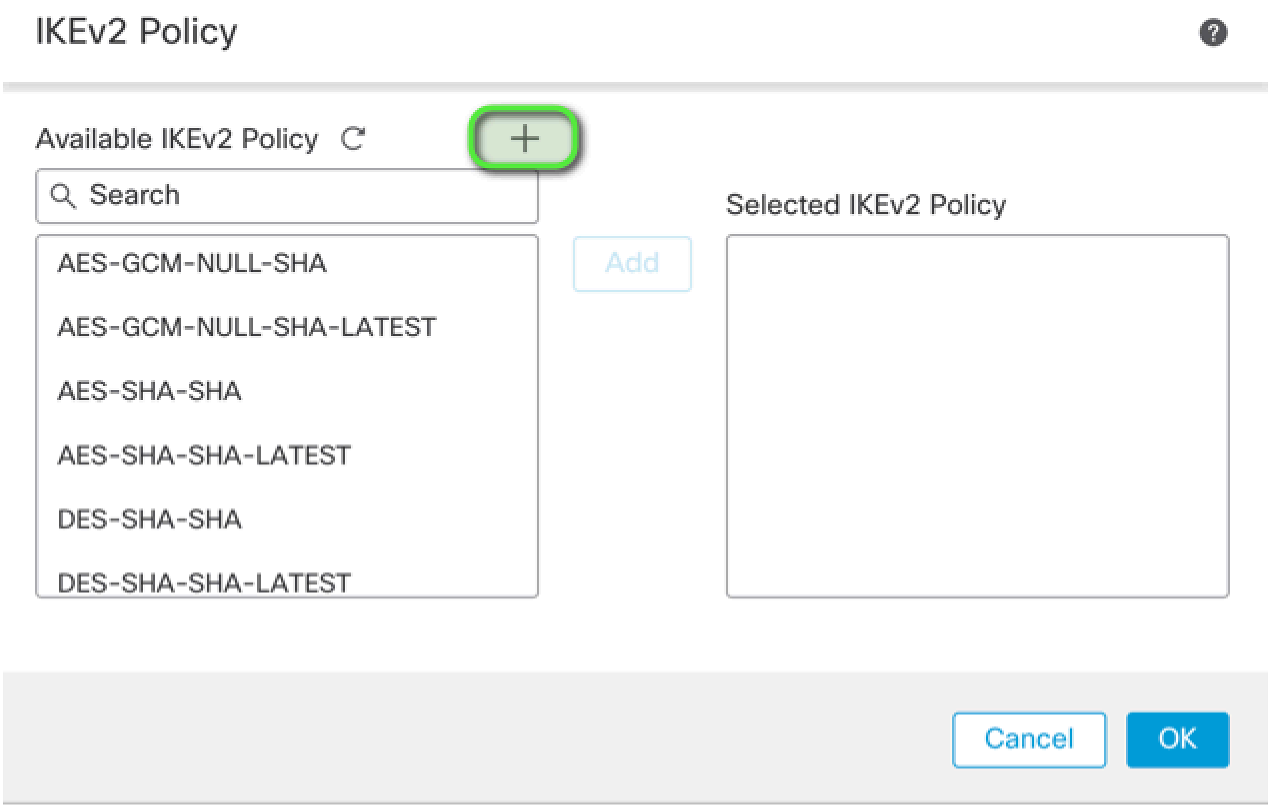
Choose the Data Center that is closest to the physical location of the device.

Define IKEv2 Phase 1 Parameters:

Acceptable parameters for tunnel negotiation can be found here.

Navigate to the IKE tab and create a new IKEv2 Policy:

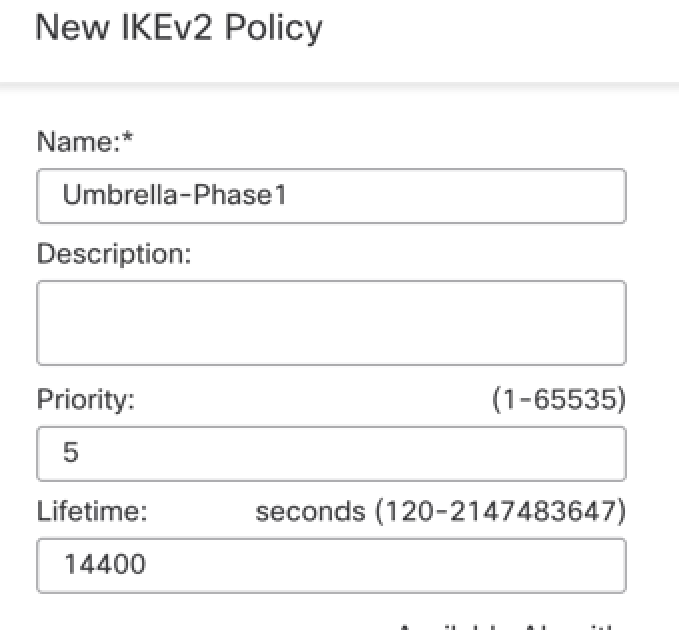
- Assign appropriate priority to avoid it from conflicting with the existing policies.
- Phase 1 lifetime is 14400 seconds.


IKEv2 Policy

Available IKEv2 Policy

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LATEST
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- DES-SHA-SHA
- DES-SHA-SHA-LATEST

Selected IKEv2 Policy


New IKEv2 Policy

Name:* Umbrella-Phase1

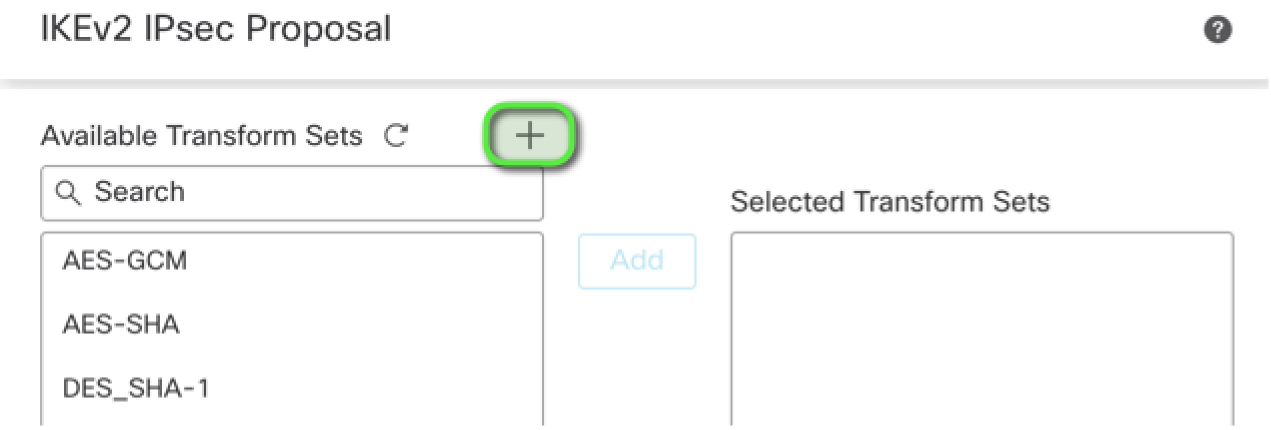
Description:

Priority: (1-65535) 5

Lifetime: seconds (120-2147483647) 14400

Define IPsec Phase 2 Parameters:

- Acceptable parameters for tunnel negotiation can be found here.
- Navigate to the IPsec tab and create a new IPsec Proposal.



IKEv2 IPsec Proposal

Available Transform Sets

Search

AES-GCM

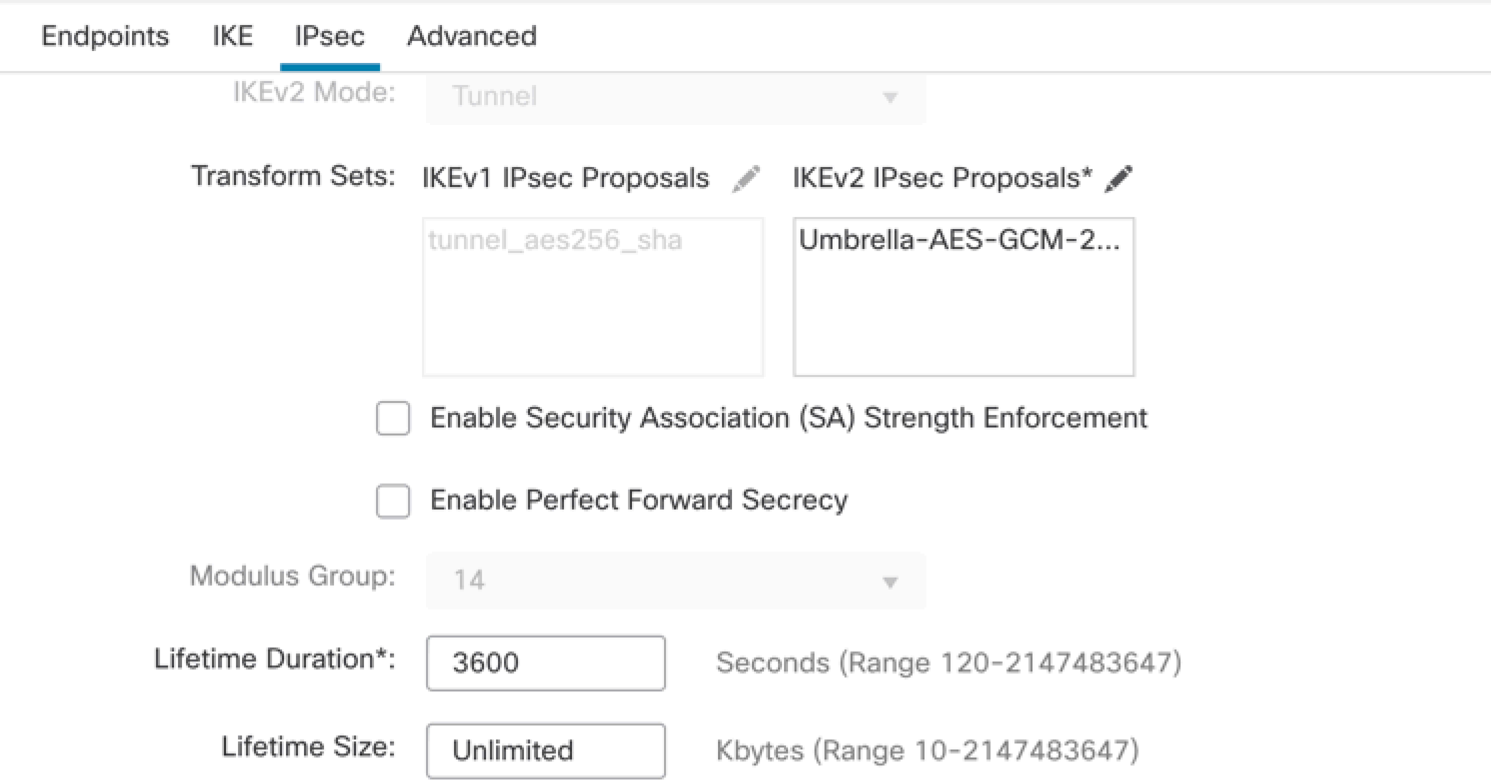
AES-SHA

DES_SHA-1

Add

Selected Transform Sets

Ensure that Phase 2 parameters match this:



Endpoints IKE IPsec Advanced

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals: tunnel_aes256_sha

IKEv2 IPsec Proposals*: Umbrella-AES-GCM-2...

□ Enable Security Association (SA) Strength Enforcement

□ Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 3600 Seconds (Range 120-2147483647)

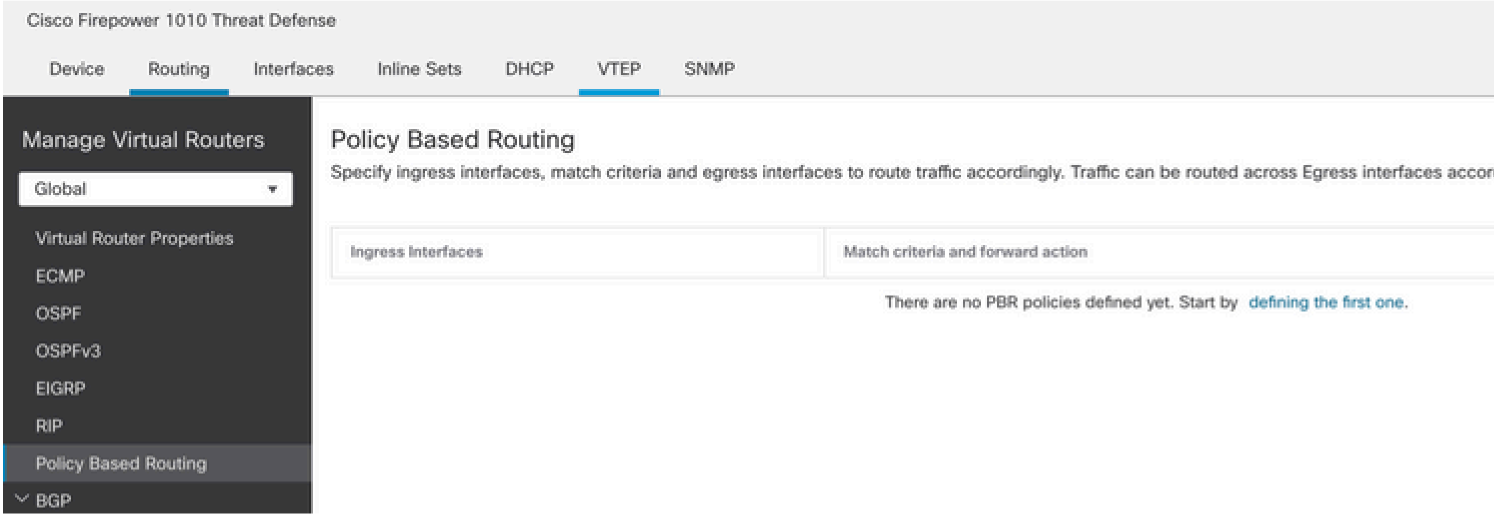
Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

Save Topology and Deploy to the Firewall.

Configure Policy Based Routing (PBR)

Navigate to **Devices** > **Device Management** > **Select the FTD/HA Pair** > **Routing** > **Policy Based Routing**.

Add New Policy.



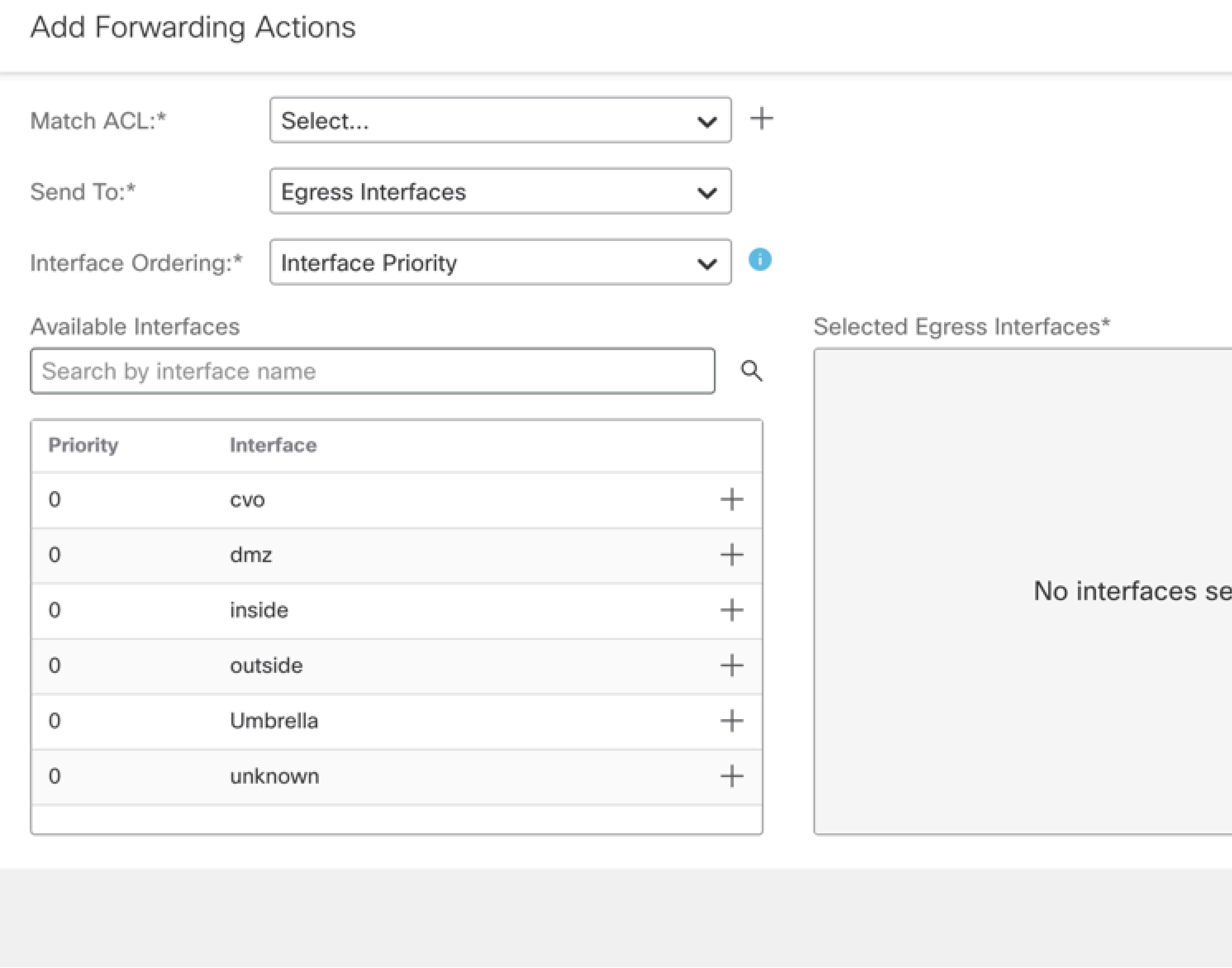
Policy Based Routing

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

Ingress Interfaces	Match criteria and forward action

There are no PBR policies defined yet. Start by defining the first one.

Configure the Forwarding Actions:



Add Forwarding Actions

Match ACL:* Select...

Send To:* Egress Interfaces

Interface Ordering:* Interface Priority

Available Interfaces

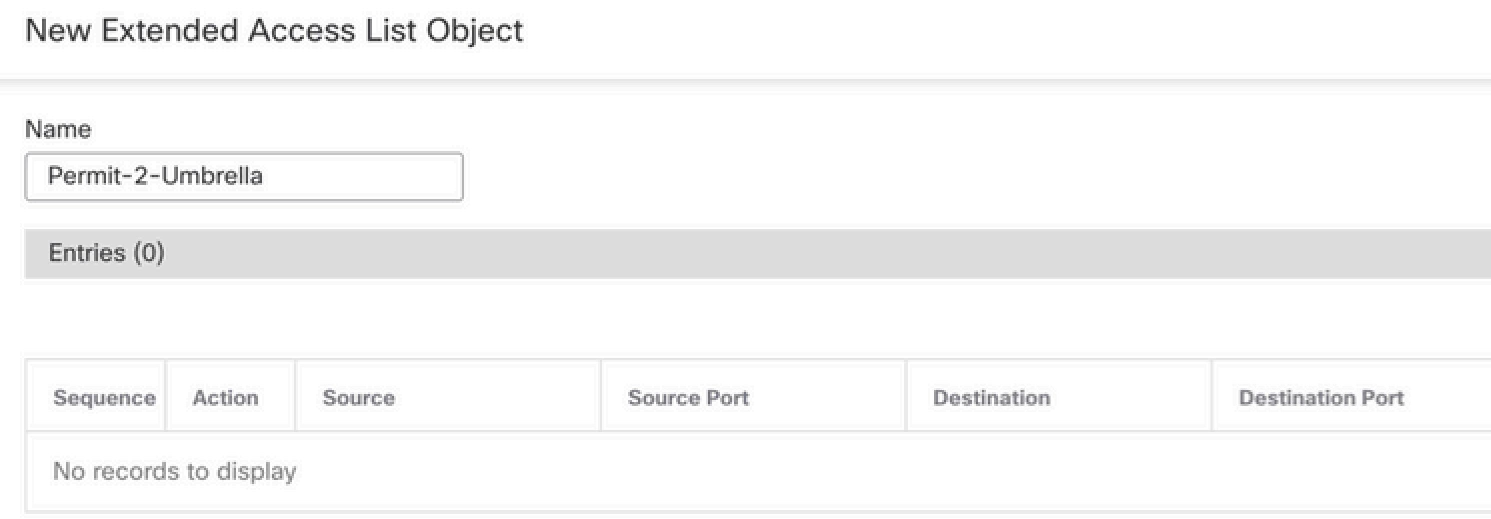
Search by interface name

Priority	Interface
0	cvo
0	dmz
0	inside
0	outside
0	Umbrella
0	unknown

Selected Egress Interfaces*

No interfaces se

Create the Match ACL for the traffic that must navigate through the SIG tunnel:



New Extended Access List Object

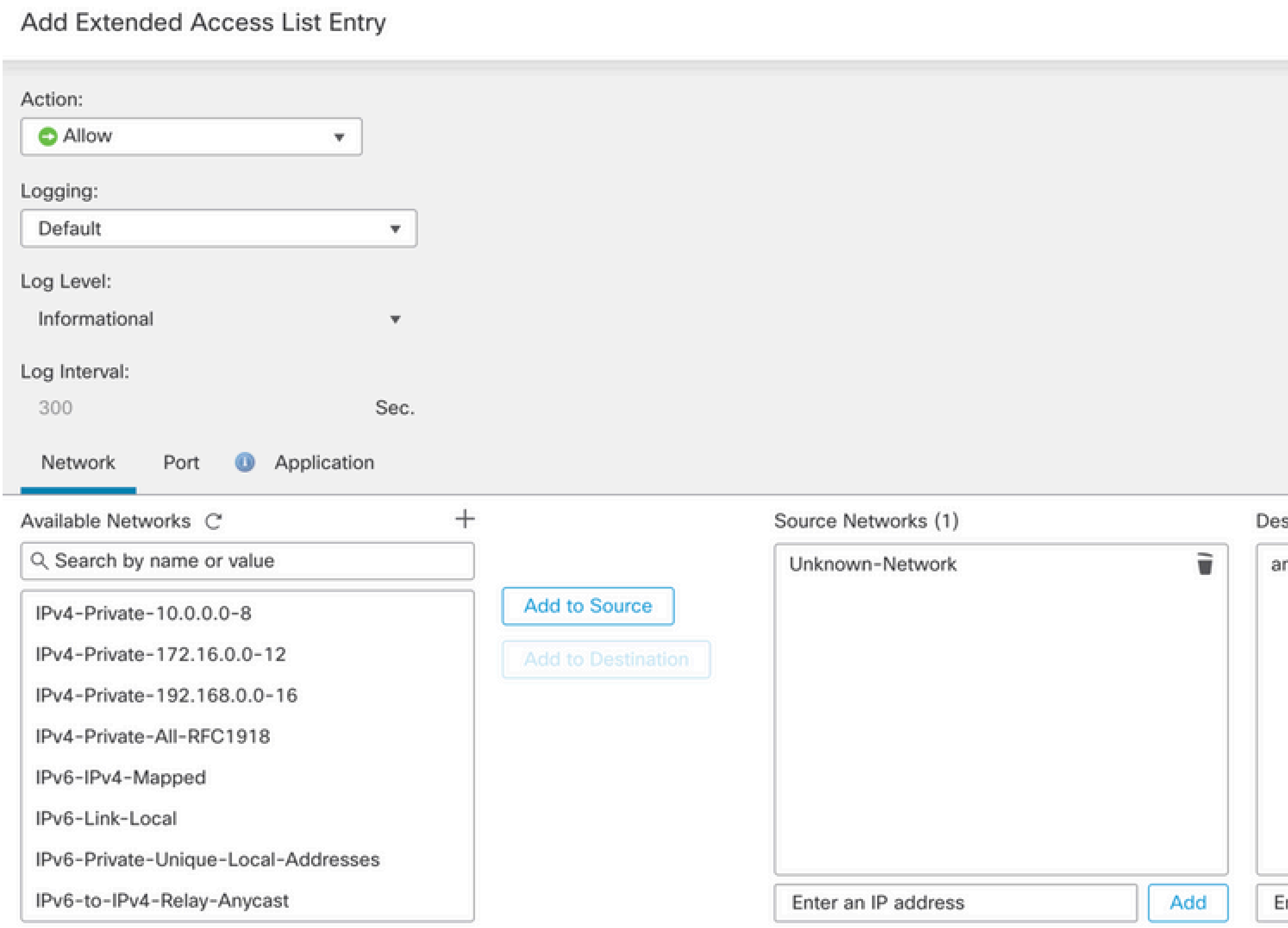
Name

Permit-2-Umbrella

Entries (0)

Sequence	Action	Source	Source Port	Destination	Destination Port
No records to display					

Add Access Control Entries defining the Umbrella SIG traffic:



Add Extended Access List Entry

Action: Allow

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

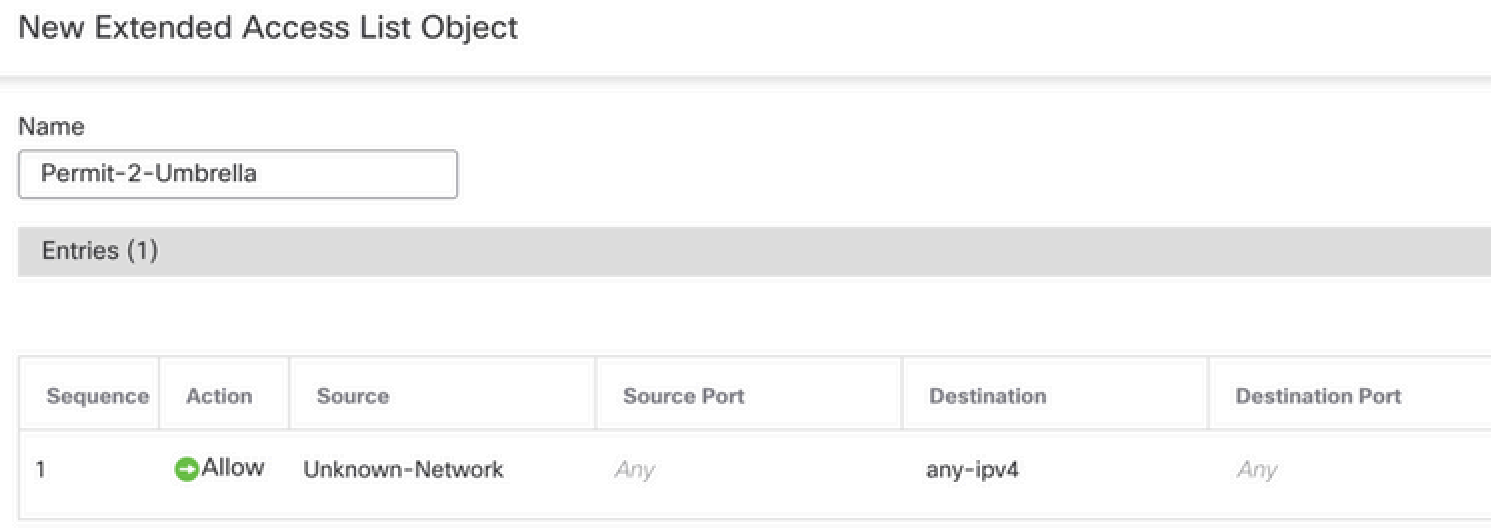
Source Networks (1)

Unknown-Network

- Source Networks define internal traffic.

  - Destination Networks are the remote networks that must be inspected by Umbrella.

Completed Extended ACL:



New Extended Access List Object

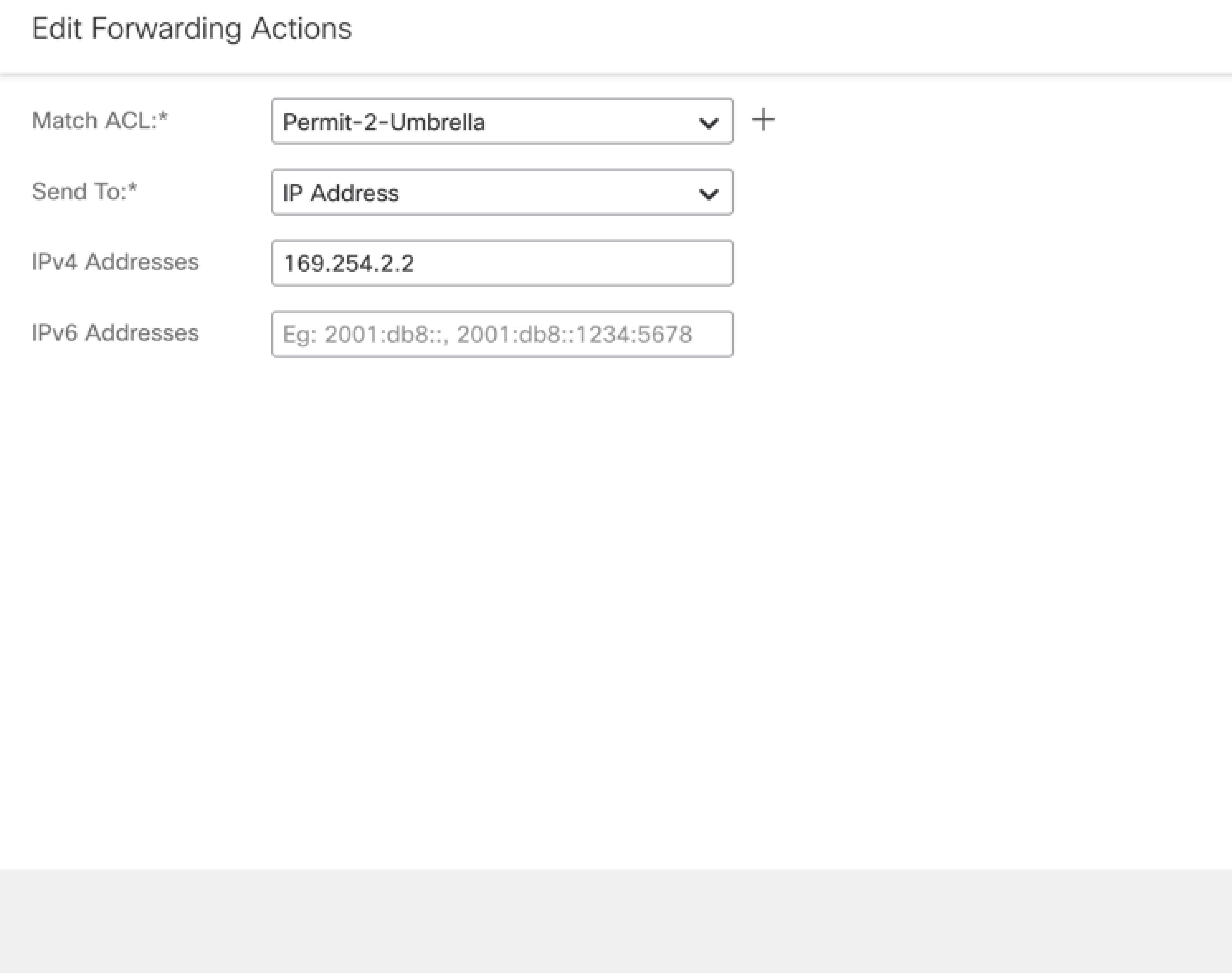
Name

Permit-2-Umbrella

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Allow	Unknown-Network	*Any*	any-ipv4	*Any*

Configure Send To:



Edit Forwarding Actions

Match ACL:* Permit-2-Umbrella

Send To:* IP Address

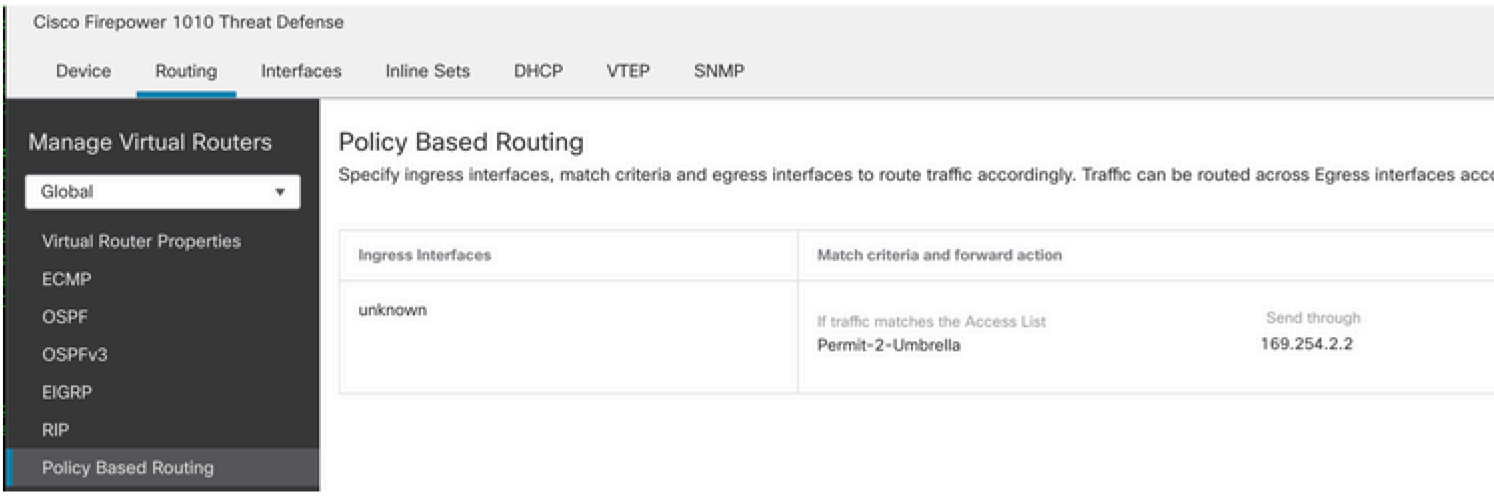
IPv4 Addresses 169.254.2.2

IPv6 Addresses Eg: 2001:db8::, 2001:db8::1234:5678

Define the Send To IPv4 address as the second available IP in the /30 subnet.

> **Note**: This IP address is not defined in Umbrella. It is only needed for traffic forwarding.

Completed PBR:



Cisco Firepower 1010 Threat Defense

Policy Based Routing

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

Ingress Interfaces	Match criteria and forward action	
unknown	If traffic matches the Access List Permit-2-Umbrella	Send through 169.254.2.2

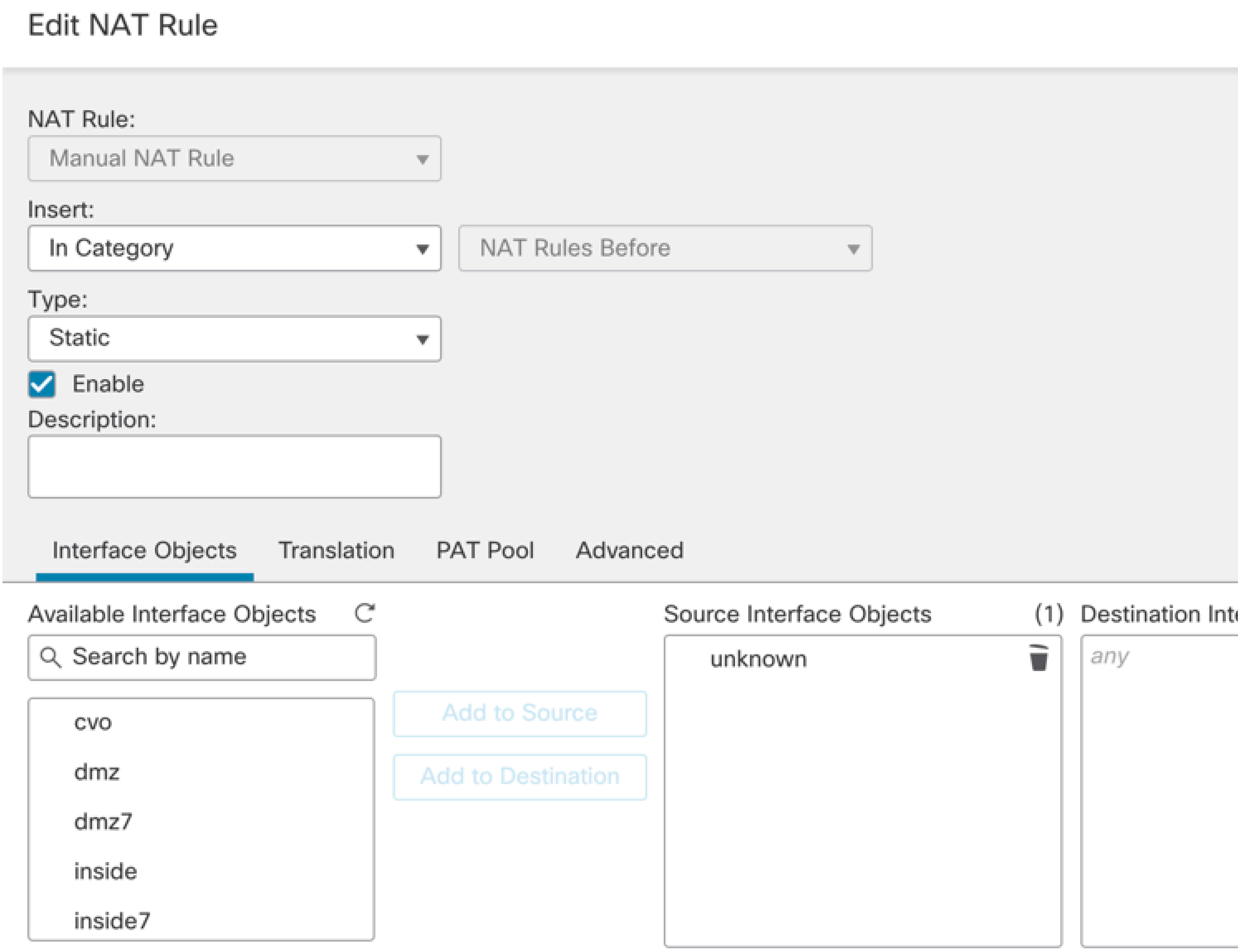
Make note of the ingress interface, this is needed later for Access Control Policy (ACP) and Network Address Translation (NAT) configuration.

Save Configuration and Deploy to the Firewall.

Configure NAT and ACP

Navigate to Devices > NAT.

Create a new manual NAT rule like this:



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static

☑ Enable

Description:

Available Interface Objects

- cvo
- dmz
- dmz7
- inside
- inside7

Source Interface Objects (1)

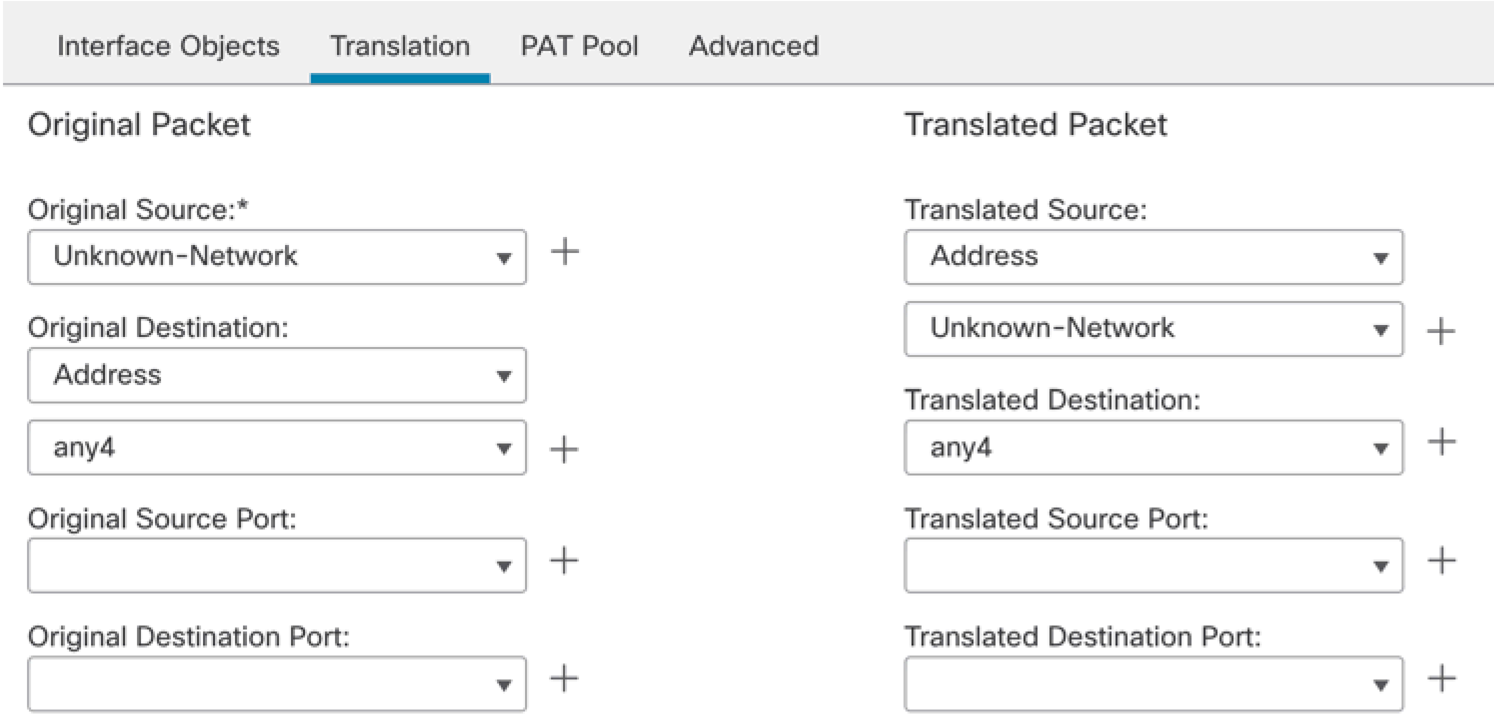
- unknown

Destination Int

- any

- Source Interface â€“ Internal protected source.
- Destination Interface â€“ Any â€“ This allows the traffic to be diverted to the VTI.

Translation:



Original Packet

Original Source:* Unknown-Network

Original Destination: Address

any4

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Unknown-Network

Translated Destination: any4

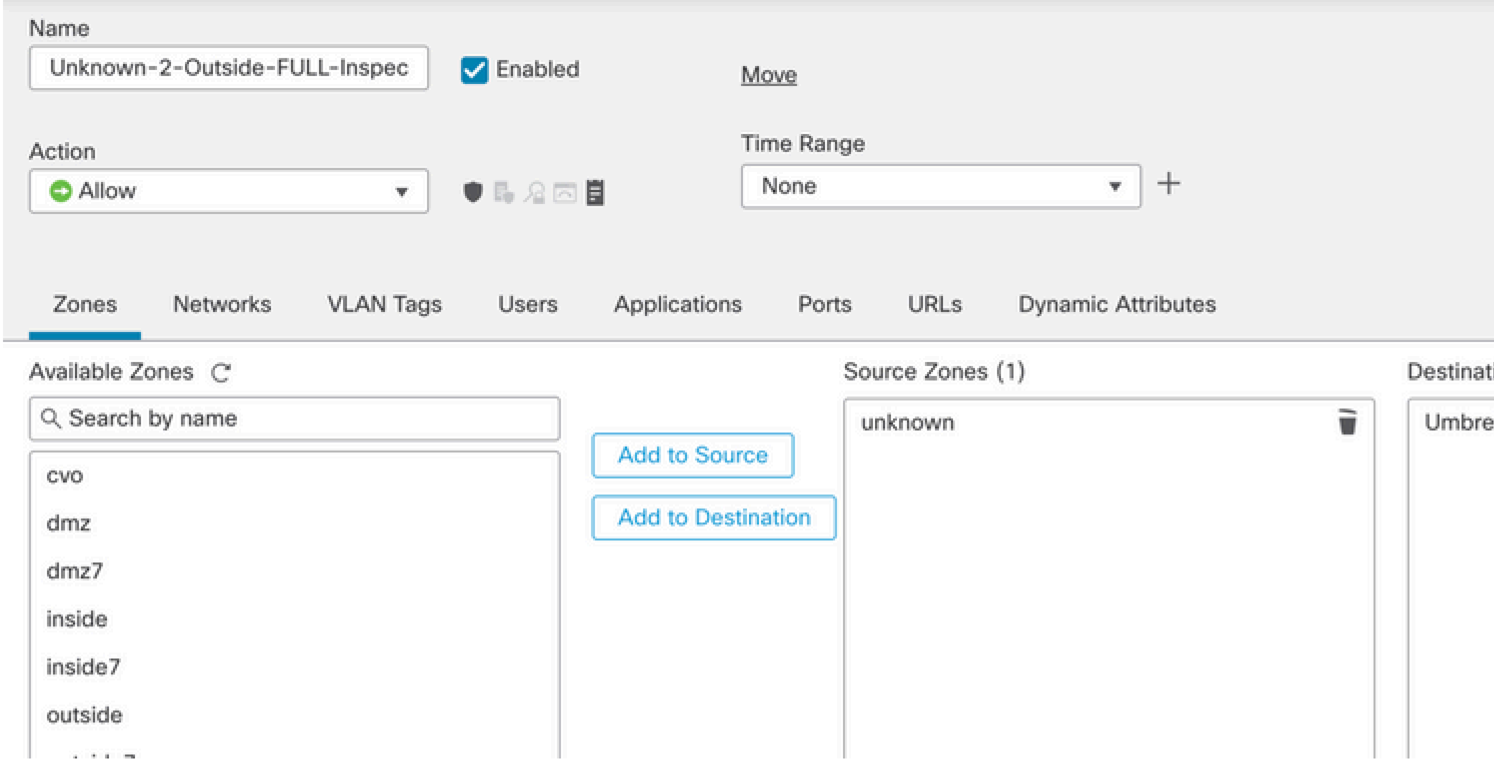
Translated Source Port:

Translated Destination Port:

- Original and Translated Source - Internal protected network object
- Original and Translated Destination â€“ any4 â€“ 0.0.0.0/0

Navigate to Policy > Access Control.

Create a new ACP rule like this:



Name: Unknown-2-Outside-FULL-Inspec

☑ Enabled

Action: Allow

Time Range: None

Available Zones

cvo
dmz
dmz7
inside
inside7
outside

Source Zones (1)

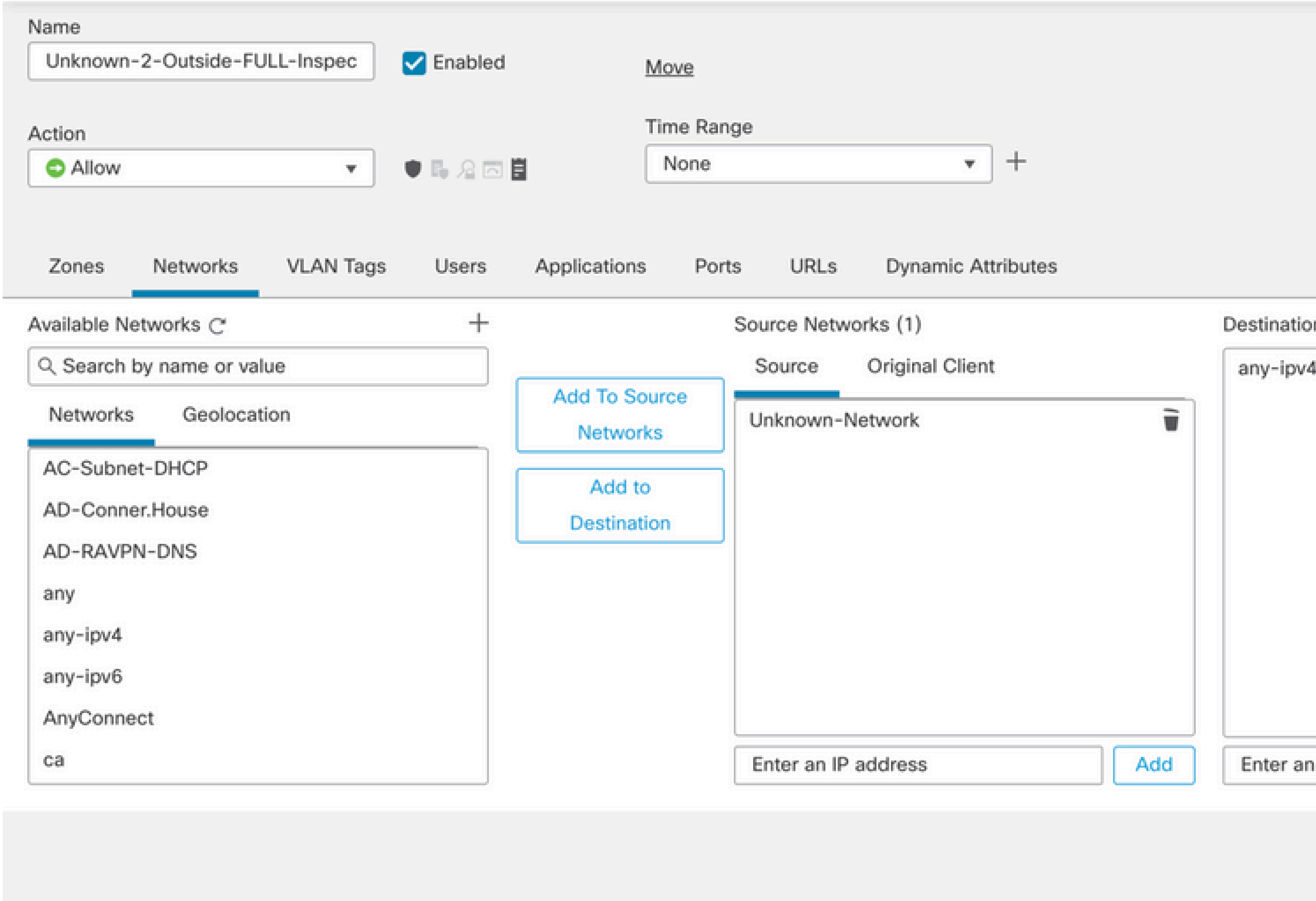
unknown

Destinat

Umbre

- Source Zone â€“ Internal Protected Source.
- Destination Zone â€“ VTI Zone â€“ This allows the traffic to be diverted to the VTI.

Networks:



Name: Unknown-2-Outside-FULL-Inspec

☑ Enabled

Action: Allow

Time Range: None

Source Networks (1): Unknown-Network

Destinatio: any-ipv4

- Source Networks - Internal protected network object(s)
- Destination Networks â€“ any4 â€“ 0.0.0.0/0

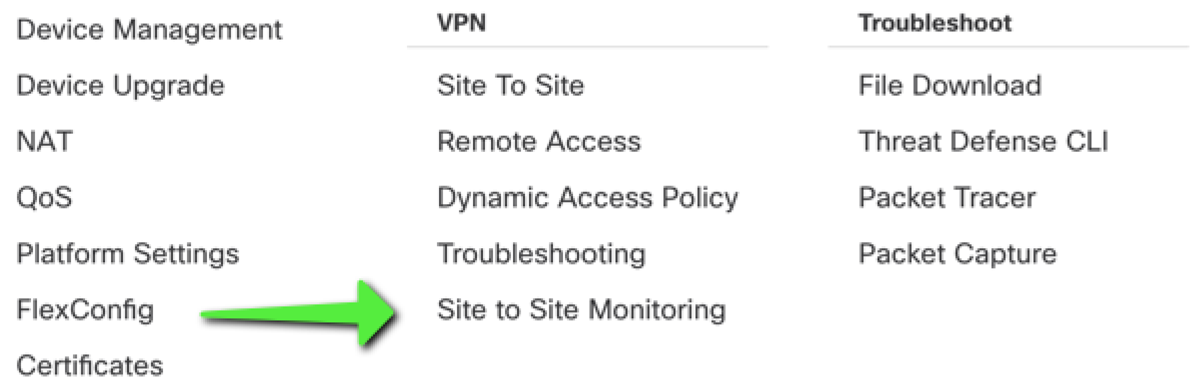
Save the configuration and deploy it to the Firewall.

Verify

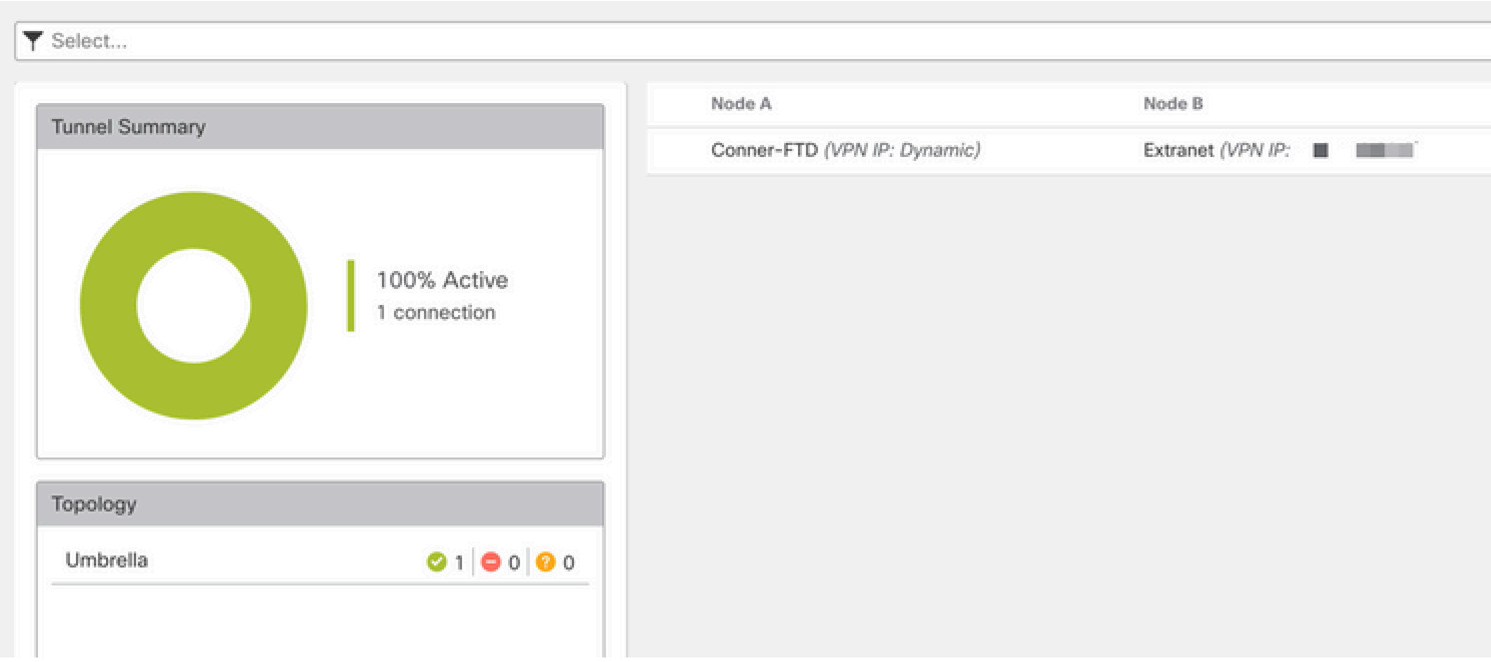
Site-to-Site Monitoring

Verify tunnel status with the Secure Firewall Management Center (FMC) Site-to-Site Monitoring tool.

Navigate to Devices > Site to Site Monitoring.



Verify that the tunnel status is now connected:

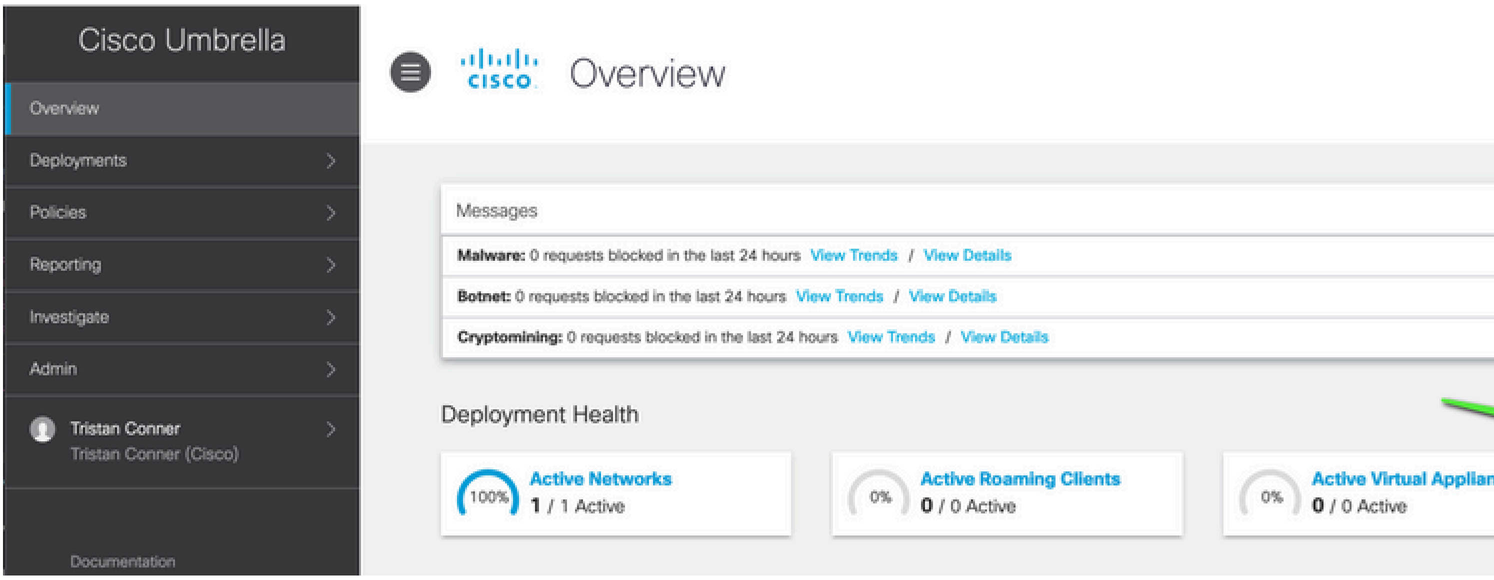


Node A	Node B
Conner-FTD *(VPN IP: Dynamic)*	Extranet *(VPN IP:* [redacted]

Hovering the cursor over the topology displays more detailed options. This can be used to inspect packets moving in and out of the tunnel along with tunnel up time and various other tunnel stats.

Umbrella Dashboard

From the Dashboard, navigate to Active Network Tunnels. There must be a blue ring indicating that the tunnel is connected.



Messages

Malware: 0 requests blocked in the last 24 hours View Trends / View Details

Botnet: 0 requests blocked in the last 24 hours View Trends / View Details

Cryptomining: 0 requests blocked in the last 24 hours View Trends / View Details

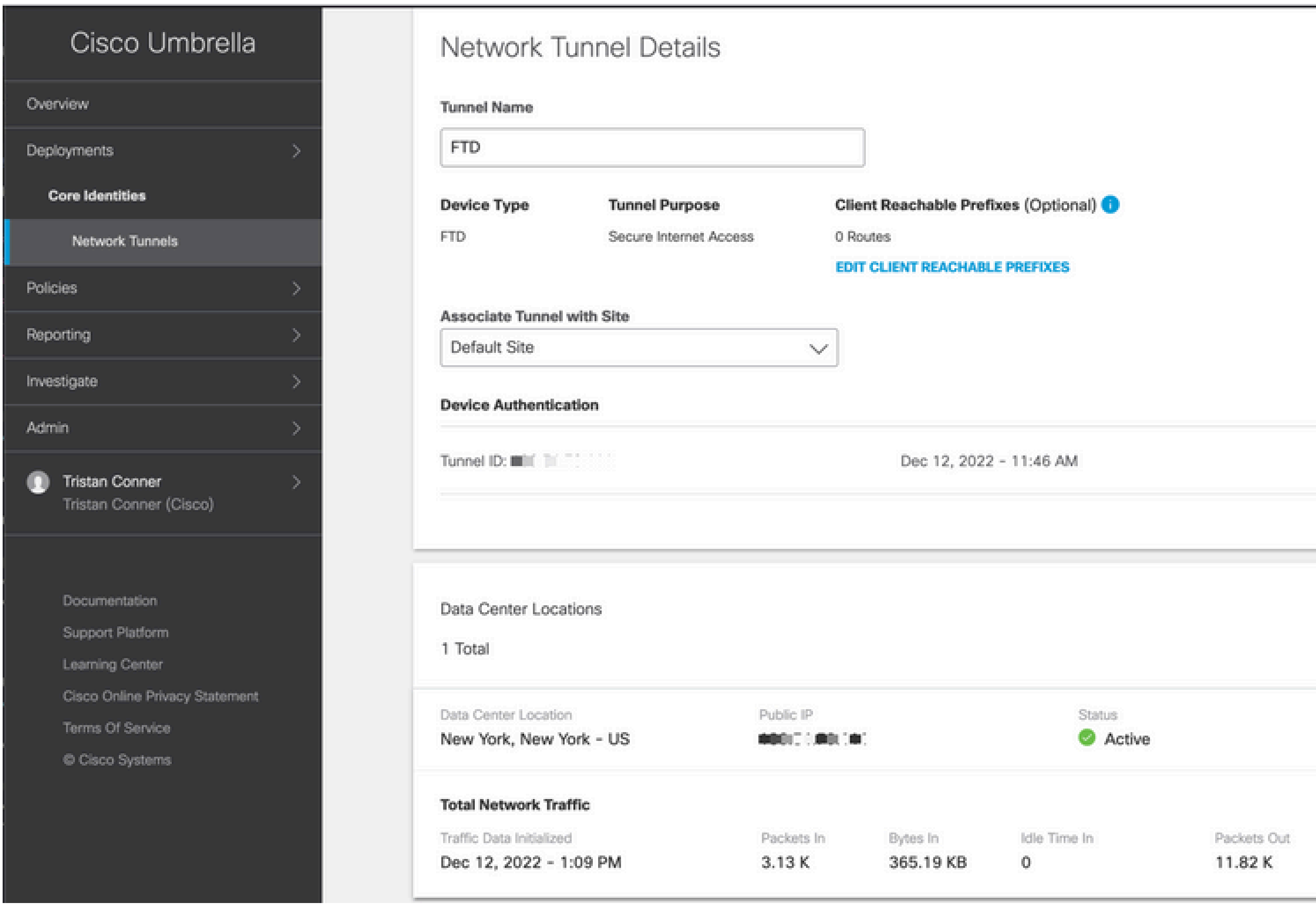
Deployment Health

Active Networks 100% 1 / 1 Active

Active Roaming Clients 0% 0 / 0 Active

Active Virtual Applian 0% 0 / 0 Active

Expand the appropriate tunnel in order to see more details about traffic flowing through the tunnel:



Network Tunnel Details

Tunnel Name: FTD

Device Type: FTD

Tunnel Purpose: Secure Internet Access

Client Reachable Prefixes (Optional): 0 Routes

Associate Tunnel with Site: Default Site

Device Authentication

Tunnel ID: [redacted] Dec 12, 2022 - 11:46 AM

Data Center Locations

1 Total

Data Center Location	Public IP	Status
New York, New York - US	[redacted]	Active

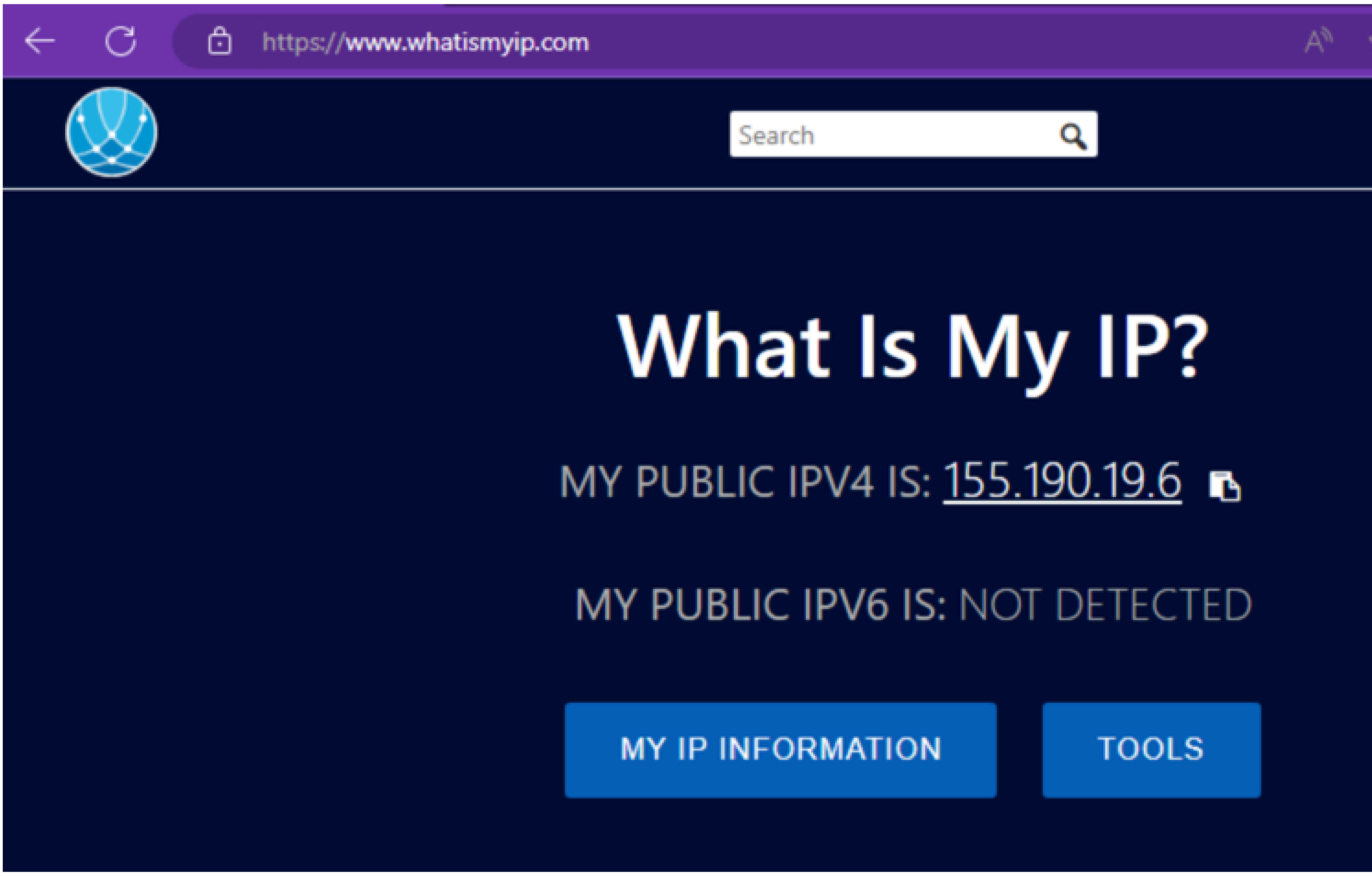
Total Network Traffic

Traffic Data Initialized	Packets In	Bytes In	Idle Time In	Packets Out
Dec 12, 2022 - 1:09 PM	3.13 K	365.19 KB	0	11.82 K

Tunnel showing as Active with data traversing the tunnel.

Internal Host

From an internal host that has its traffic traverse the tunnel, perform a public IP lookup from a web browser. If the public IP shown falls inside these two ranges, the device is now protected by SIG.


https://www.whatismyip.com
Search
What Is My IP?
MY PUBLIC IPV4 IS: 155.190.19.6
MY PUBLIC IPV6 IS: NOT DETECTED
MY IP INFORMATION
TOOLS

Firewall Threat Defense CLI

Show commands:

- show crypto ikev2 sa
- show crypto ipsec sa
- show vpn-sessiondb l2l filter ipaddress Umbrella-DC-IP

Troubleshoot

Firewall Threat Defense CLI

IKEv2 Debugs:

- Debug crypto ikev2 protocol 255
- Debug crypto ikev2 platform 255
- Debug crypto ipsec 255

ISAKMP Captures:

ISAKMP capture can be used in order to determine what is causing tunnel connectivity issues without the need for debugs. The suggested capture syntax is: capture name type isakmp interface FTD-Tunnel-Source match ip host FTD-Public-IP host Umbrella-DC-IP.