

Configure Dual ISP VTI on FTD Managed by FMC

Contents

[Introduction](#)

[Prerequisites](#)

[Basic Requirements](#)

[Components Used](#)

[Configurations on FMC](#)

[Topology Configuration](#)

[Endpoint Configuration](#)

[IKE configuration](#)

[IPsec configuration](#)

[Routing Configuration](#)

Introduction

This document describes deploying dual ISP setup using Virtual Tunnel Interfaces on a FTD device managed by FMC.

Prerequisites

Basic Requirements

- A foundational understanding of Site-to-Site VPNs would be beneficial. This background assists in grasping the VTI setup process, including the key concepts and configurations involved.
- Understanding the fundamentals of configuring and managing VTIs on the Cisco Firepower platform is essential. This includes knowledge of how VTIs function within the FTD and how they are controlled via the FMC interface.

Components Used

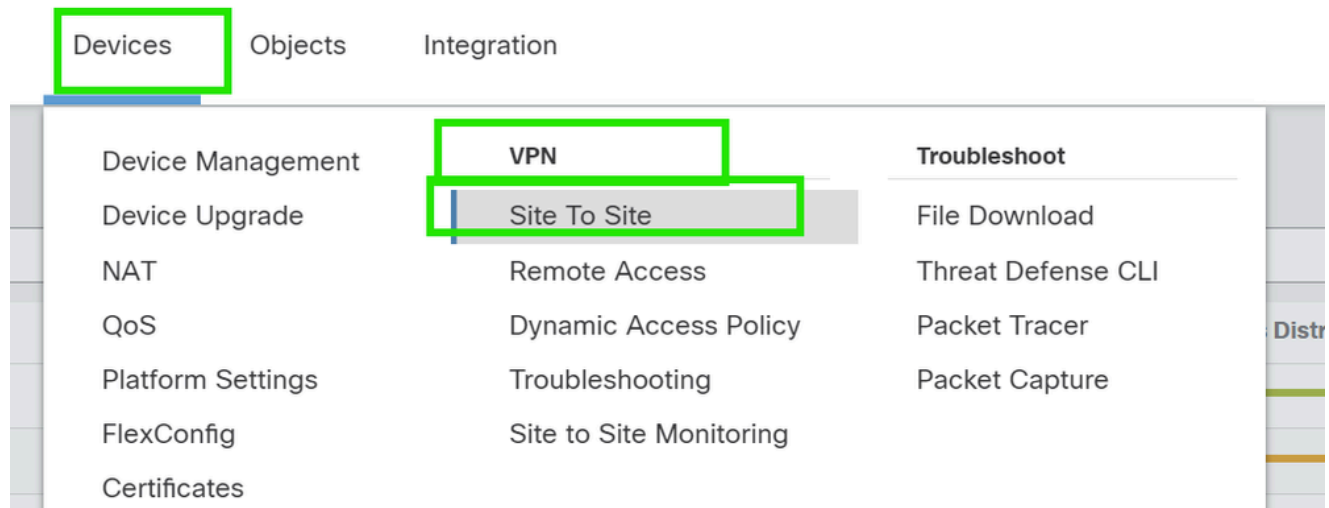
- Cisco Firepower Threat Defense (FTD) for VMware: Version 7.0.0
- Firepower Management Center (FMC): Version 7.2.4 (build 169)

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.

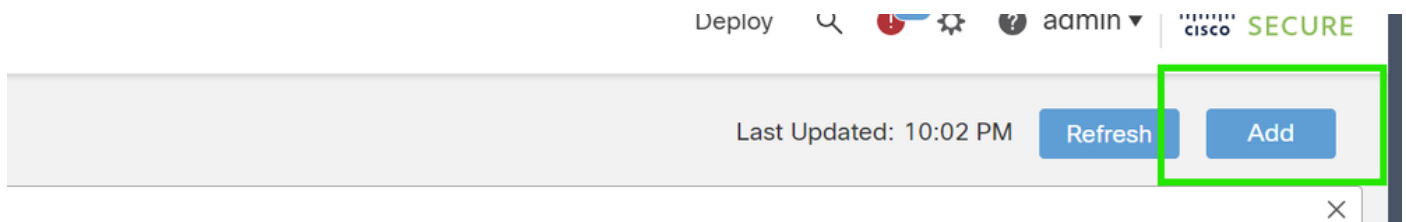
Configurations on FMC

Topology Configuration

1. Navigate to **Devices >VPN > Site To Site**.



2. Click **Add** to add VPN topology.



3. Give a name for the topology, choose VTI and Point-to-Point, and select an IKE version (IKEv2 in this case).



Endpoint Configuration

1. Choose the device on which the tunnel needs to be configured.

Add the remote peer details.

You can either add a new Virtual Template Interface by clicking on the "+" icon or select one from the existing list.

Node A

Device:*
New_FTD

Virtual Tunnel Interface:*
[] +

Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

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

Connection Type:*
Bidirectional

Node B

Device:*
Extranet

Device Name*:
VTI-Peer

Endpoint IP Address*:
10.10.10.2

Cancel Save

If you are creating a new VTI interface, then add the correct parameters, enable it, and click "OK".

NOTE: This becomes the primary VTI.

Add Virtual Tunnel Interface



General

Name:*

VTI-1

Enabled

Description:

This is the primary VTI tunnel.
This VTI goes through ISP 1.

Security Zone:

OUT

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

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

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside1)

10.106.52.104

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.10.1/30



Cancel

OK

3. Click on "+ ". Add Backup VIT" to add a secondary VIT.

Device:*

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: *outside1 (IP: 10.106.52.104)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

+ Add Backup VTI (optional)

Connection Type:*

Bidirectional ▼

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

4. Click on "+" to add parameter for secondary VTI (if not already configured).

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: outside1 (IP: 10.106.52.104) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

▼ +

Tunnel Source IP is Private

[Edit VTI](#)

Send Local Identity to Peers

Connection Type:*

5. If you are creating a new VTI interface, then add the correct parameters, enable it, and click "OK".

NOTE: This becomes the secondary VTI.

Add Virtual Tunnel Interface



General

Name:

VTI-2

Enabled

Description:

This is the secondary VTI tunnel..
VTI goes through ISP 2.

Security Zone:

OUT

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

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

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (outside2)

10.106.53.10

IPsec Tunnel Details

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

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.20.1/30



Cancel

OK

IKE configuration

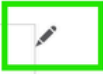
1. Navigate to the IKE tab. You can choose to use a predefined policy else click the pencil button next to the Policy tab to create a new one or select another available policy based on your requirement.

Endpoints **IKE** IPsec Advanced

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings



Policies:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

Cancel Save


IKEv2 Policy ?

Available IKEv2 Policy  

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LAT...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- Arko_Test_IKEv2
- DES-SHA-SHA

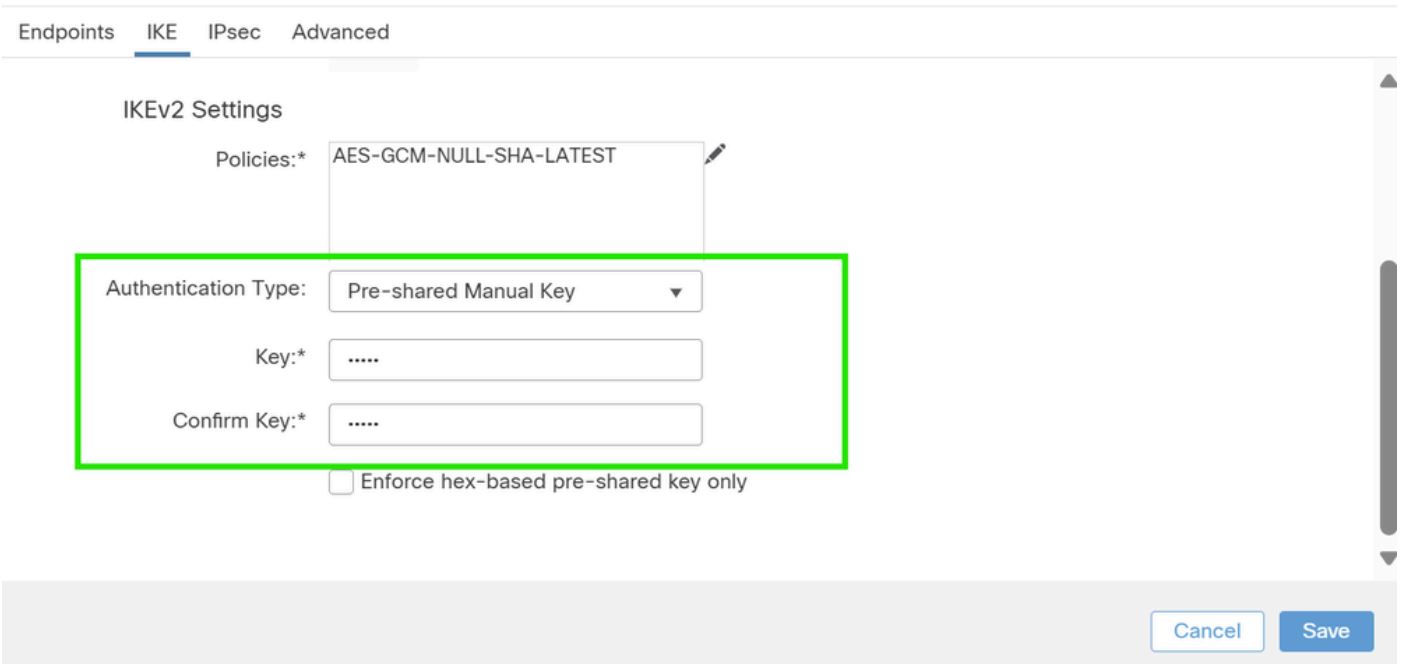
Add

Selected IKEv2 Policy

AES-GCM-NULL-SHA-LATEST 

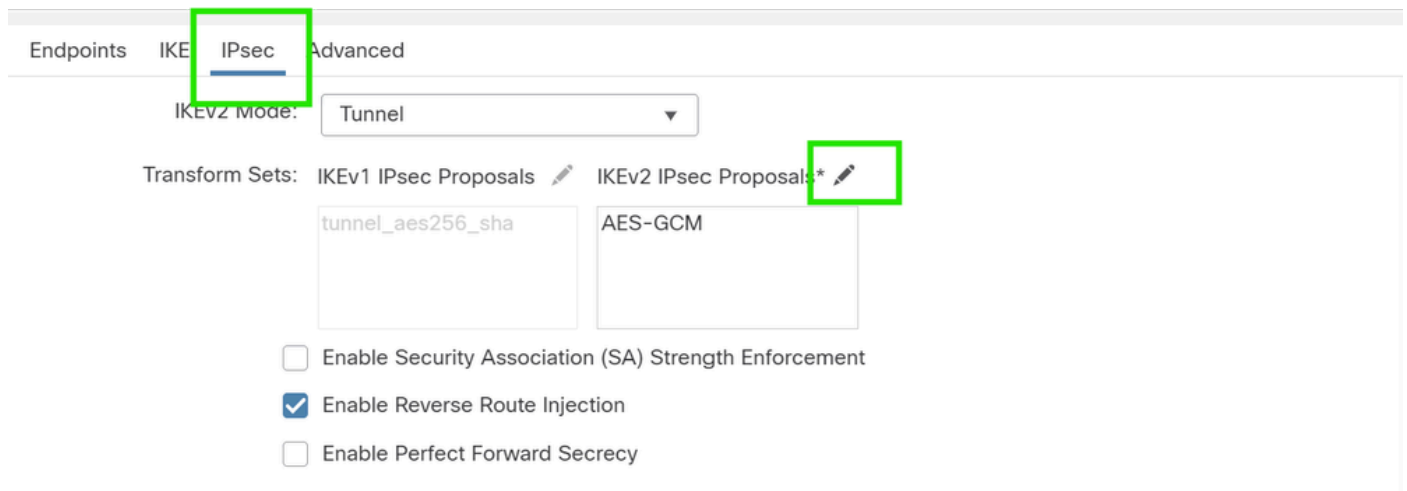
Cancel OK

2. Select the Authentication Type. If a pre-shared manual key is used, provide the key in the Key and Confirm Key boxes.



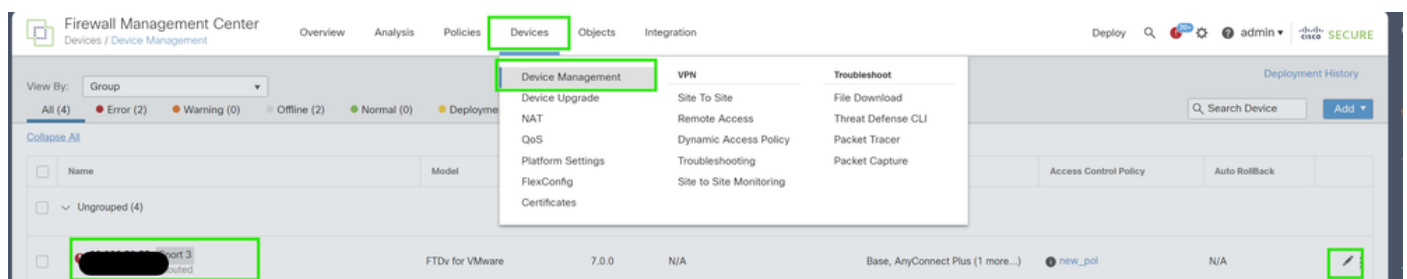
IPsec configuration

Navigate to the IPsec tab. You can choose to use a predefined proposal by clicking the pencil button next to the proposal tab to create a new one or select another available proposal based on your requirement.



Routing Configuration

1. Go to **Device > Device Management** and click on the pencil icon to edit the device (FTD).



2. Go to **Routing > Static Route** and click on the "+" button to add a route to the primary and secondary VTI.

NOTE: You can configure the appropriate routing method for your traffic to pass through the tunnel interface. In this case, static routes have been used.

The screenshot shows the Cisco configuration interface with the 'Routing' tab selected. A sidebar menu titled 'Manage Virtual Routers' is open, with 'Static Route' highlighted. In the main interface, the '+ Add Route' button is highlighted. The interface also shows a table for routes with columns: Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. The table is currently empty, with expandable sections for IPv4 and IPv6 routes.

3. Add two routes for your protected network and set a higher AD value (in this case 2) for the secondary route.

The first route uses the VTI-1 interface, and the second uses the VTI-2 interface.

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

Verify

1. Go to Devices > VPN > Site to Site Monitoring .

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Site to Site Monitoring

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

2. Click on the eye to check more details about the status of the tunnel.



View full information

Dual-ISP-VTI

Active

2024-06-11 06:55:26

Dual-ISP-VTI

Active

2024-06-12 14:27:22