Configure VPN Migration Between FTDs Managed by a Single FMC

Contents

Introduction

This document describes migrating a Site-to-Site VPN from one FTD to another, managed by the same FMC, while keeping the VPN connection to router.

Prerequisites

Requirements

To effectively carry out the migration process, Cisco recommends familiarity with the given topics:

- **FTD Registration with FMC:** Understanding how to register Firepower Threat Defense (FTD) devices with the Firepower Management Center (FMC).
- **Site-to-Site VPN Configuration:** Experience in configuring site-to-site VPNs on FTD devices managed by FMC.

Components Used

This document is based on the given software and hardware versions:

- **Firepower Threat Defense Virtual (FTDv):** Two instances running version 7.3.1.
- **Firepower Management Center (FMC):** Version 7.4.0.

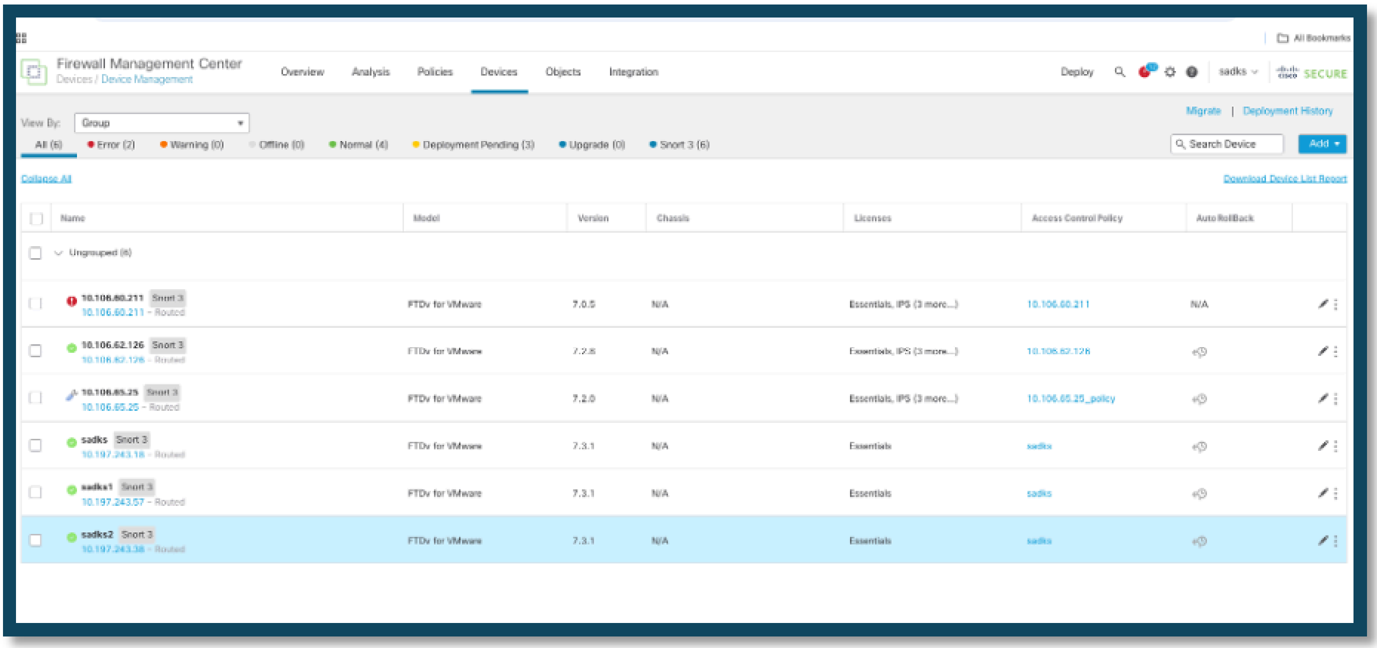
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Procedure

1. **Register the New FTD with FMC:**

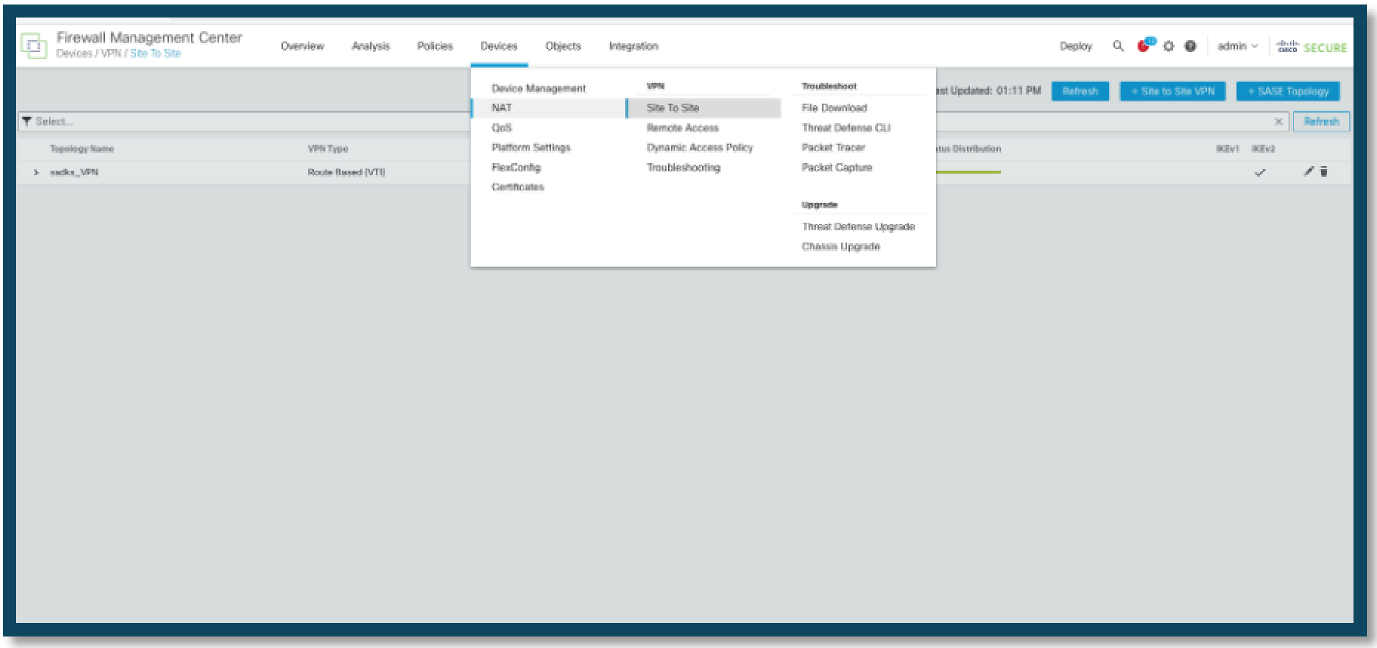
- Begin by registering the new Firepower Threat Defense (FTD) device within the Firepower Management Center (FMC) under Devices > Device Management.
- In this example, The new device registered is named "sadks2."



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (6)						
10.106.60.211 Snort 3 10.106.60.211 - Routed	FTDv for VMware	7.0.5	N/A	Essentials, IPS (3 more...)	10.106.60.211	N/A
10.106.62.126 Snort 3 10.106.62.126 - Routed	FTDv for VMware	7.2.8	N/A	Essentials, IPS (3 more...)	10.106.62.126	
10.106.65.25 Snort 3 10.106.65.25 - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (3 more...)	10.106.65.25_policy	
sadks Snort 3 10.197.243.18 - Routed	FTDv for VMware	7.3.1	N/A	Essentials	sadks	
sadks1 Snort 3 10.197.243.57 - Routed	FTDv for VMware	7.3.1	N/A	Essentials	sadks	
sadks2 Snort 3 10.197.243.38 - Routed	FTDv for VMware	7.3.1	N/A	Essentials	sadks	

New FTD Registered

2. **Access the Site-to-Site Tunnel Configuration:**
   - Navigate to the site-to-site tunnel settings by going to **Devices > Site to Site** in the FMC interface.



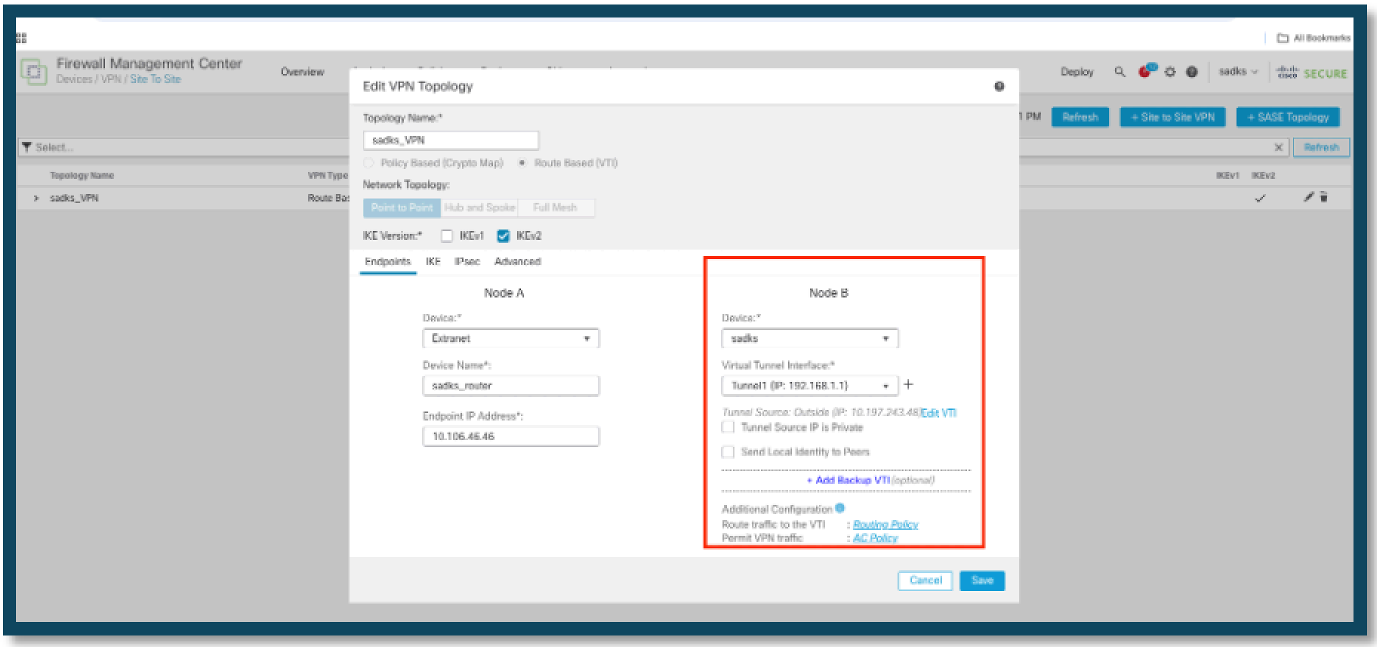
Topology Name	VPN Type	tus Distribution	IKEv1	IKEv2
sadks_VPN	Route Based (VTI)			✓

Navigate to VPN Config

3. **Modify the VPN Configuration:**

- Select the VPN configuration that you intend to update.

- Example: In this scenario, the VPN configuration involves an FTD device and a router. Here, **Node B** represents the **FTD device**, and the configuration has been updated to change the device association from "**sadks**" to "**sadks2**."



Edit VPN Topology

Topology Name:* sadks_VPN

○ 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:* Extranet

Device Name*: sadks_router

Endpoint IP Address*: 10.106.46.46

Node B

Device:* sadks

Virtual Tunnel Interface:* Tunnel1 (IP: 192.168.1.1)

Tunnel Source: Outside (IP: 10.197.243.48) Edit VTI

□ Tunnel Source IP is Private

□ Send Local Identity to Peers

+ Add Backup VTI (optional)

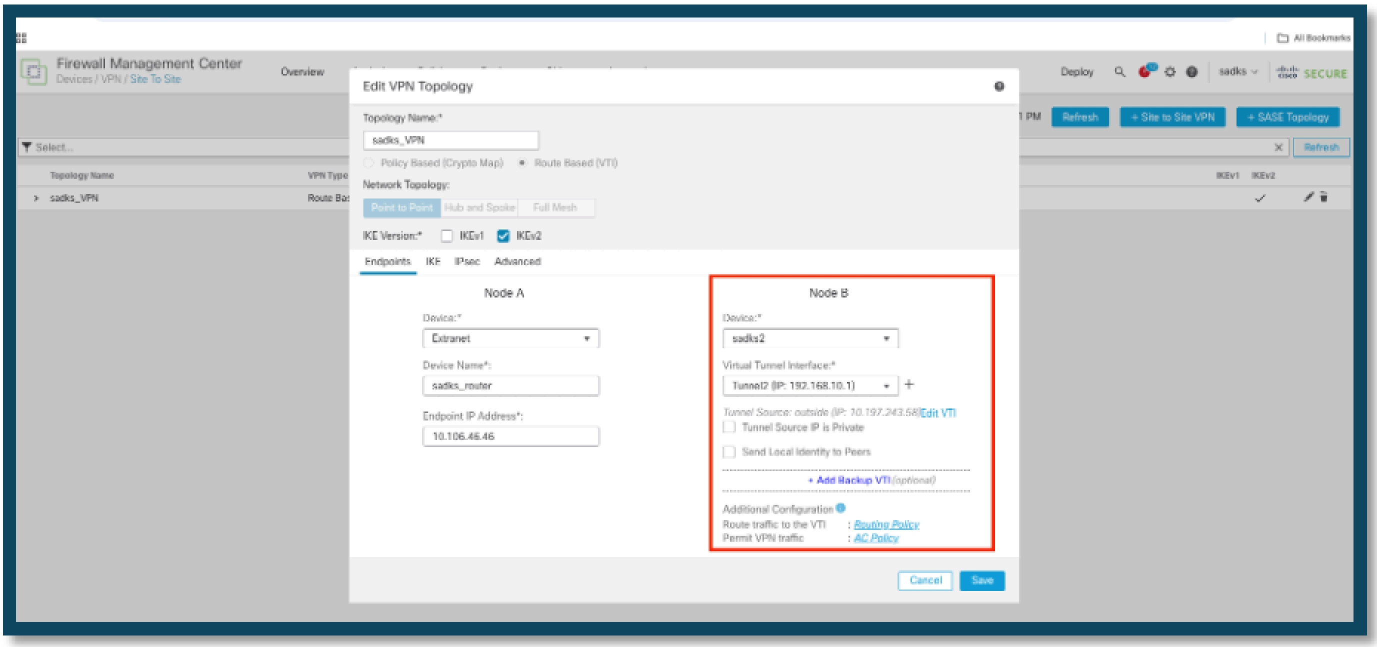
Additional Configuration

Route traffic to the VTI : Routing Policy

Permit VPN traffic : AC Policy

Old FTD Device

TO



Edit VPN Topology

Topology Name:* sadks_VPN

○ 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:* Extranet

Device Name*: sadks_router

Endpoint IP Address*: 10.106.46.46

Node B

Device:* sadks2

Virtual Tunnel Interface:* Tunnel2 (IP: 192.168.10.1)

Tunnel Source: outside (IP: 10.197.243.58) Edit VTI

□ Tunnel Source IP is Private

□ Send Local Identity to Peers

+ Add Backup VTI (optional)

Additional Configuration

Route traffic to the VTI : Routing Policy

Permit VPN traffic : AC Policy

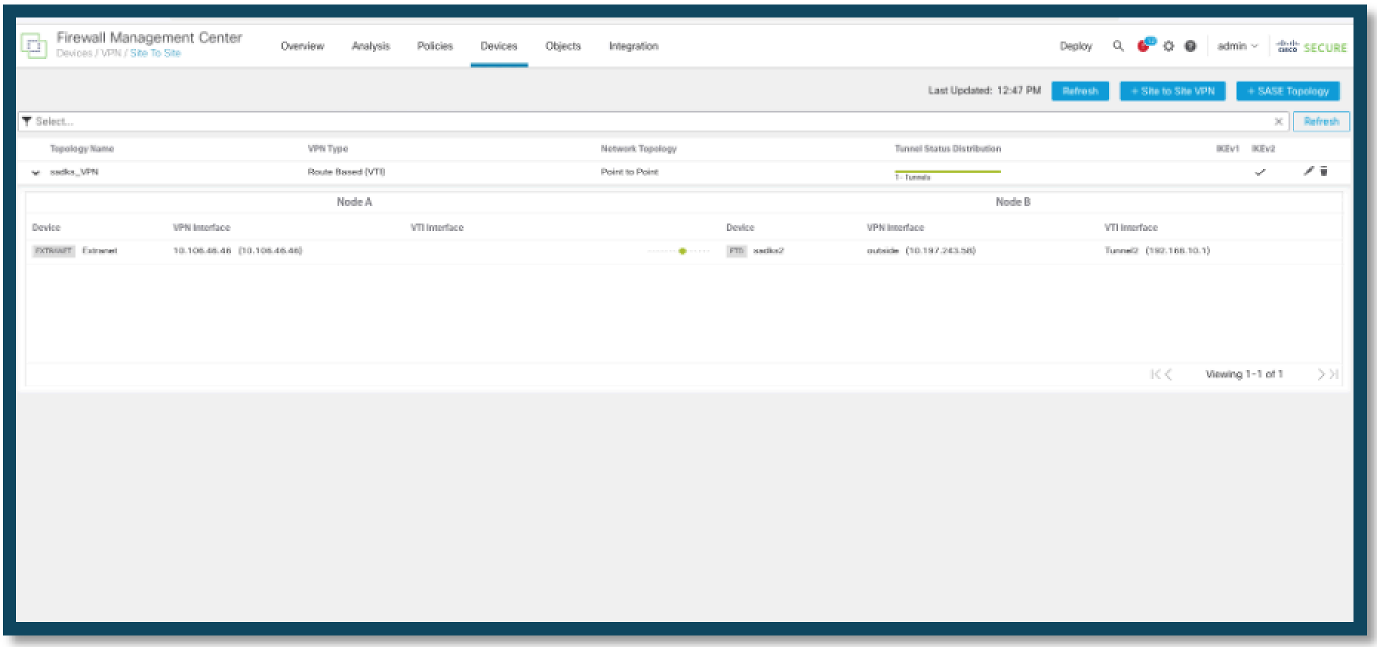
New FTD Device

4. **Save and Deploy the Configuration:**

- After making the necessary changes, save the configuration and deploy it to activate the updates.

Verify

The tunnel comes up once deployed.



Last Updated: 12:47 PM

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
sadks_VPN	Route Based (VTI)	Point to Point	1 - Tunnels		✓

Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet	10.106.46.46 (10.106.46.46)		FTD sadks2	outside (10.197.243.58)	Tunnel2 (192.168.10.1)

Tunnel Status

Troubleshoot

Initial Connectivity Issues

When building a VPN there are two sides negotiating the tunnel. Therefore, it is best to get both sides of the conversation when you troubleshoot any type of tunnel failure. A detailed guide on how to debug IKEv2 tunnels can be found here: How to debug IKEv2 VPNs

The most common cause of tunnel failures is a connectivity issue. The best way to determine this is to take packet captures on the device. Use this command to take packet captures on the device:

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

Once the capture is in place, try to send traffic over the VPN and check for bi-directional traffic in the packet capture.

Review the packet capture with this command:

<#root>

```
show cap capout
```

Traffic-Specific Issues

Common traffic issues that you experience are:

- Routing issues behind the FTD -- internal network unable to route packets back to the assigned IP addresses and VPN clients.
- Access control lists blocking traffic.
- Network Address Translation not being bypassed for VPN traffic.

For further information regarding VPNs on the FTD managed by FMC, you can find the full configuration guide here: FTD managed by FMC configuration guide