Configure Route Based Site to Site VPN Tunnel on FTD Managed by FMC

Contents

Introduction

This document describes how to configure a static route-based Site to Site VPN tunnel on a Firepower Threat Defense managed by a FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of how a VPN tunnel works.
- Understand how to navigate through the Firepower Management Center (FMC).

Components Used

The information in this document is based on these software versions:

- Cisco Firepower Management Center version 6.7.0
- Cisco Firepower Threat Defense (FTD) version 6.7.0

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.

Background Information

Route-based VPN allows determination of interesting traffic to be encrypted, or sent over VPN tunnel, and use traffic routing instead of policy/access-list as in Policy-based or Crypto-map based VPN. The encryption domain is set to allow any traffic which enters the IPsec tunnel. IPsec Local and remote traffic selectors are

set to 0.0.0.0/0.0.0..0. This means that any traffic routed into the IPsec tunnel is encrypted regardless of the source/destination subnet.

This document focuses on Static Virtual Tunnel Interface (SVTI) configuration. For Dynamic Virtual Tunnel Interface (DVTI) configuration on Secure Firewall, please refere to this [Configure DVTI with Multi-SA on Secure Firewall](#).

Limitations and Restrictions

These are known limitations and restrictions for Route Based tunnels on FTD:

- Supports IPsec only. GRE is not supported.

- Supports only IPv4 interfaces, as well as IPv4, protected networks, or VPN payload (No Support for IPv6).

- Static routing and only BGP Dynamic Routing protocol is supported for VTI interfaces that classify traffic for VPN (No Support for other protocols like OSPF, RIP, and so on).

- Only 100 VTIs are supported per interface.

- VTI is not supported on an FTD Cluster.

- VTI is not supported in these policies:

  - QoS
  - NAT
  - Platform settings

These algorithms are no longer supported on FMC/FTD version 6.7.0 for new VPN tunnels (FMC supports all the removed ciphers to manage FTD < 6.7):

- 3DES, DES, and NULL Encryption are unsupported in IKE Policy.

- DH groups 1, 2, and 24 are unsupported in IKE Policy and IPsec Proposal.

- MD5 Integrity is unsupported in IKE Policy.

- PRF MD5 is unsupported in IKE policy.

- DES, 3DES, AES-GMAC, AES-GMAC-192, and AES-GMAC-256 encryption algorithms are unsupported in IPsec Proposal.

Note: This holds true for both site to site route based as well as policy-based VPN tunnels. In order to upgrade an older FTD to 6.7 from FMC, it triggers a pre-validation check warning the user about changes that pertain to the removed ciphers that block the upgrade.


FTD 6.7 managed via FMC 6.7	Configuration Available	Site to Site VPN Tunnel
Fresh Install	Weak ciphers available, but cannot	Weak ciphers available, but cannot

	be used to configure the FTD 6.7 device.	be used to configure the FTD 6.7 device.
Upgrade: FTD only configured with weak ciphers.	Upgrade from FMC 6.7 UI, a pre-validation check displays an error. The upgrade is blocked until reconfiguration.	Post FTD upgrade, and assume the peer has not changed its settings, then tunnel is terminated.
Upgrade: FTD only configured with some weak ciphers and some strong ciphers.	Upgrade from FMC 6.7 UI, a pre-validation check displays an error. The upgrade is blocked until reconfiguration.	Post FTD upgrade, and assume the peer has strong ciphers, then the tunnel re-establishes.
Upgrade: Class C country (Does not have a strong crypto license.)	DES is allowed.	DES is allowed.

.

✎ **Note:** No additional licensing is needed, Route Based VPN can be configured in Licensed as well as Evaluation Modes. Without crypto compliance (Export Controlled Features Enabled), only DES can be used as an encryption algorithm.

Configuration Steps on FMC

Step 1. Navigate to **Devices >VPN >Site To Site**.
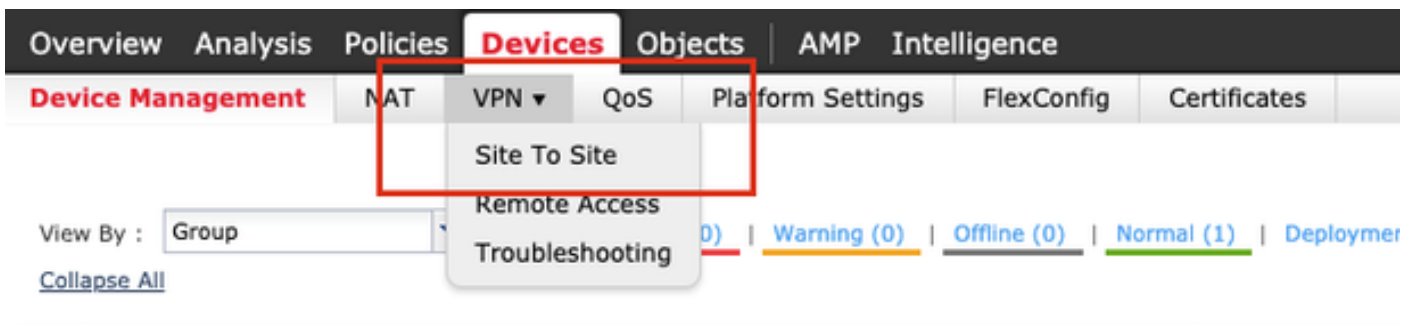
Step 2. Click **Add VPN**, and choose **Firepower Threat Defense Device**, as shown in the image.
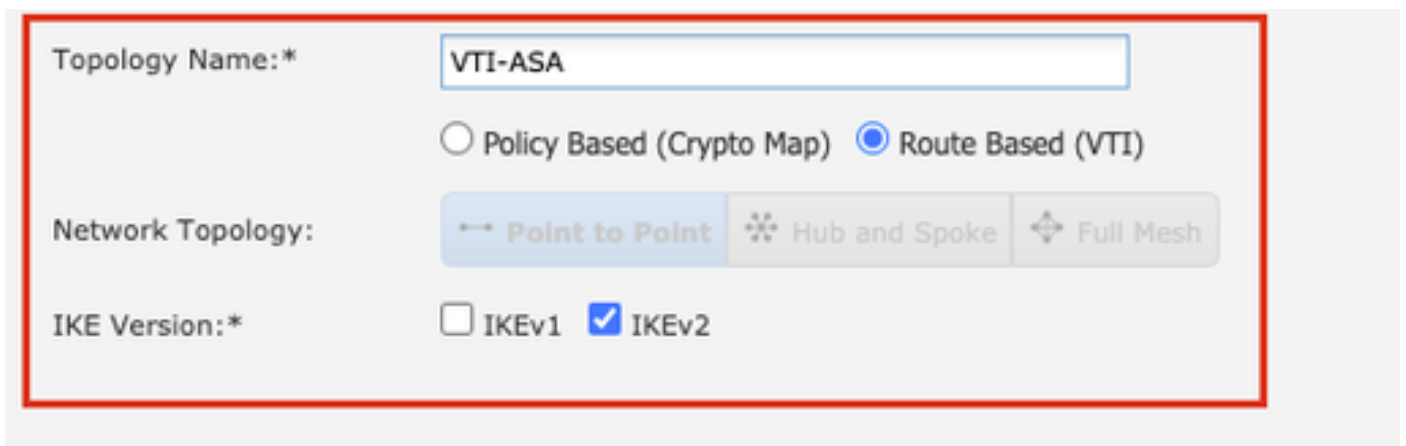
Step 3. Provide a **Topology Name** and select the Type of VPN as **Route Based (VTI)**. Choose the **IKE Version**.
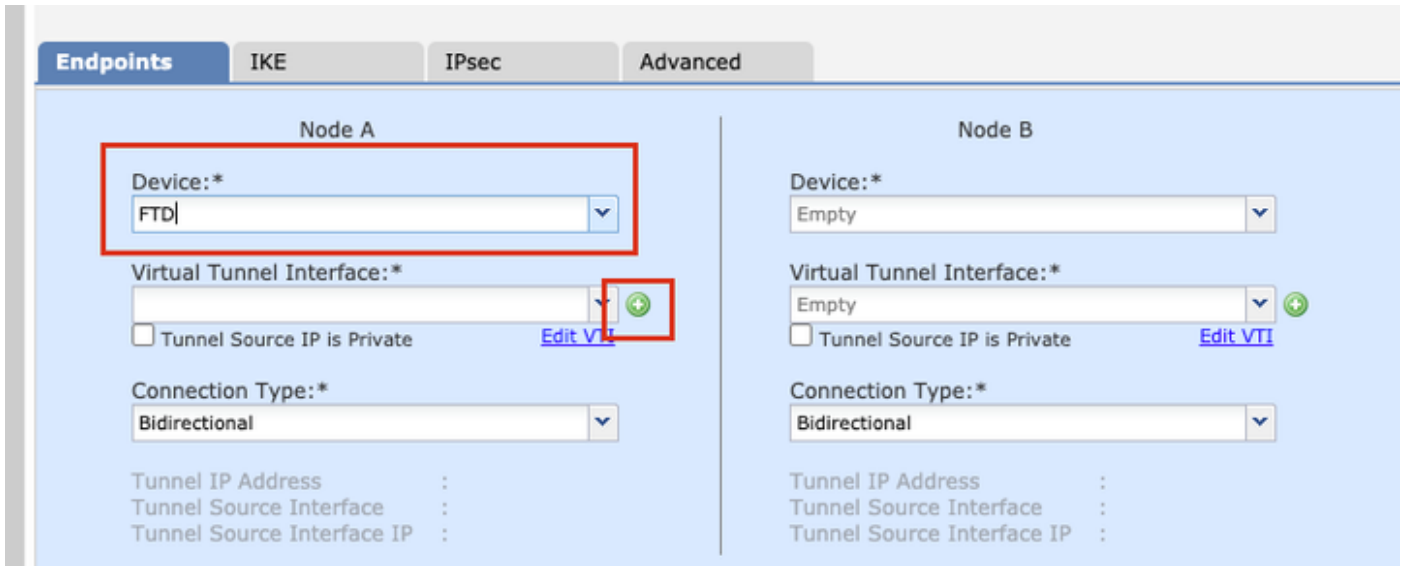
For the purpose of this demonstration:

Topology Name: VTI-ASA

IKE Version: IKEv2

Step 4. Choose the **Device** on which the tunnel needs to be configured, You can choose to add a new **Virtual Tunnel Interface** (click on the + icon), or select one from the list that exists.

Step 5. Define the parameters of the **New Virtual Tunnel Interface**. Click **Ok**.

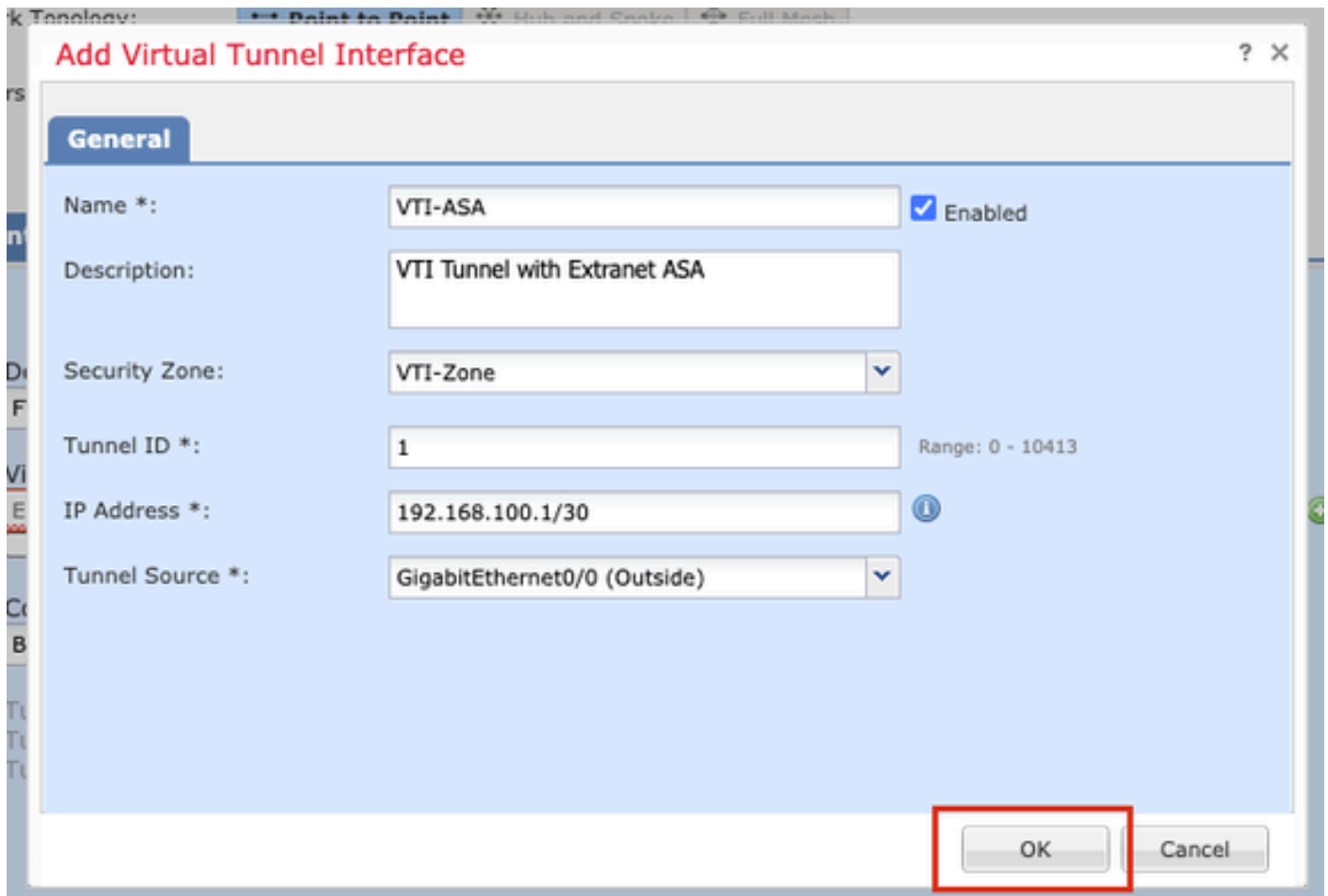For the purpose of this demonstration:

Name: VTI-ASA

Description (Optional): VTI Tunnel with Extranet ASA
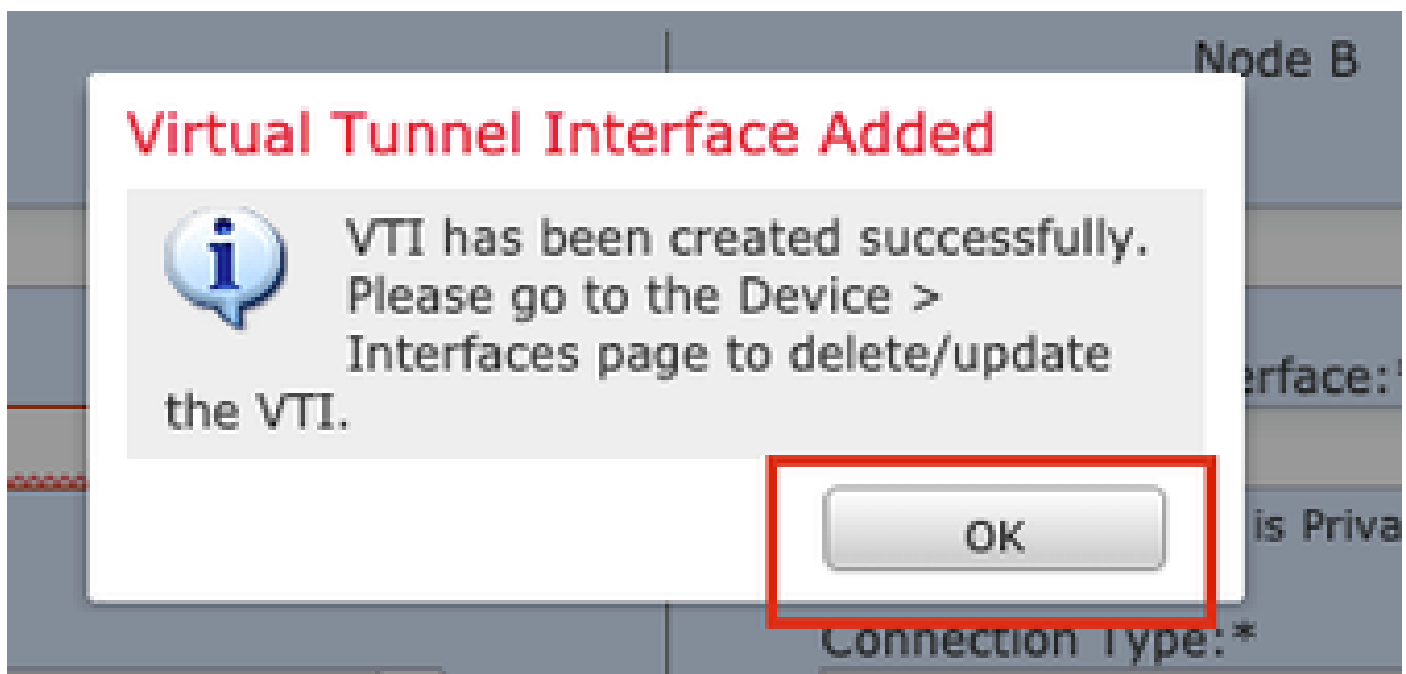
Security Zone: VTI-Zone

Tunnel ID: 1

IP Address: 192.168.100.1/30

Tunnel Source: GigabitEthernet0/0 (Outside)

Add Virtual Tunnel Interface ? ✕

General

Name *:	VTI-ASA	☑ Enabled
Description:	VTI Tunnel with Extranet ASA	
Security Zone:	VTI-Zone	
Tunnel ID *:	1	Range: 0 - 10413
IP Address *:	192.168.100.1/30	
Tunnel Source *:	GigabitEthernet0/0 (Outside)	

OK   Cancel

Step 6. Click **OK** on the popup mentioning that the new VTI has been created.

Virtual Tunnel Interface Added

ⓘ VTI has been created successfully. Please go to the Device > Interfaces page to delete/update the VTI.

OK

Step 7. Choose the newly created VTI or a VTI that exists under **Virtual Tunnel Interface**. Provide the information for Node B (which is the peer device).

For the purpose of this demonstration:

Device: Extranet

Device Name: ASA-Peer

Endpoint IP Address: 10.106.67.252

Step 8. Navigate to the **IKE** tab. You can choose to use a pre-defined **Policy** or click the + button next to the **Policy** tab and create a new one.

Step 9. (Optional, if you create new IKEv2 Policy.) Provide a **Name** for the Policy and select the **Algorithms** to be used in the policy. Click **Save**.

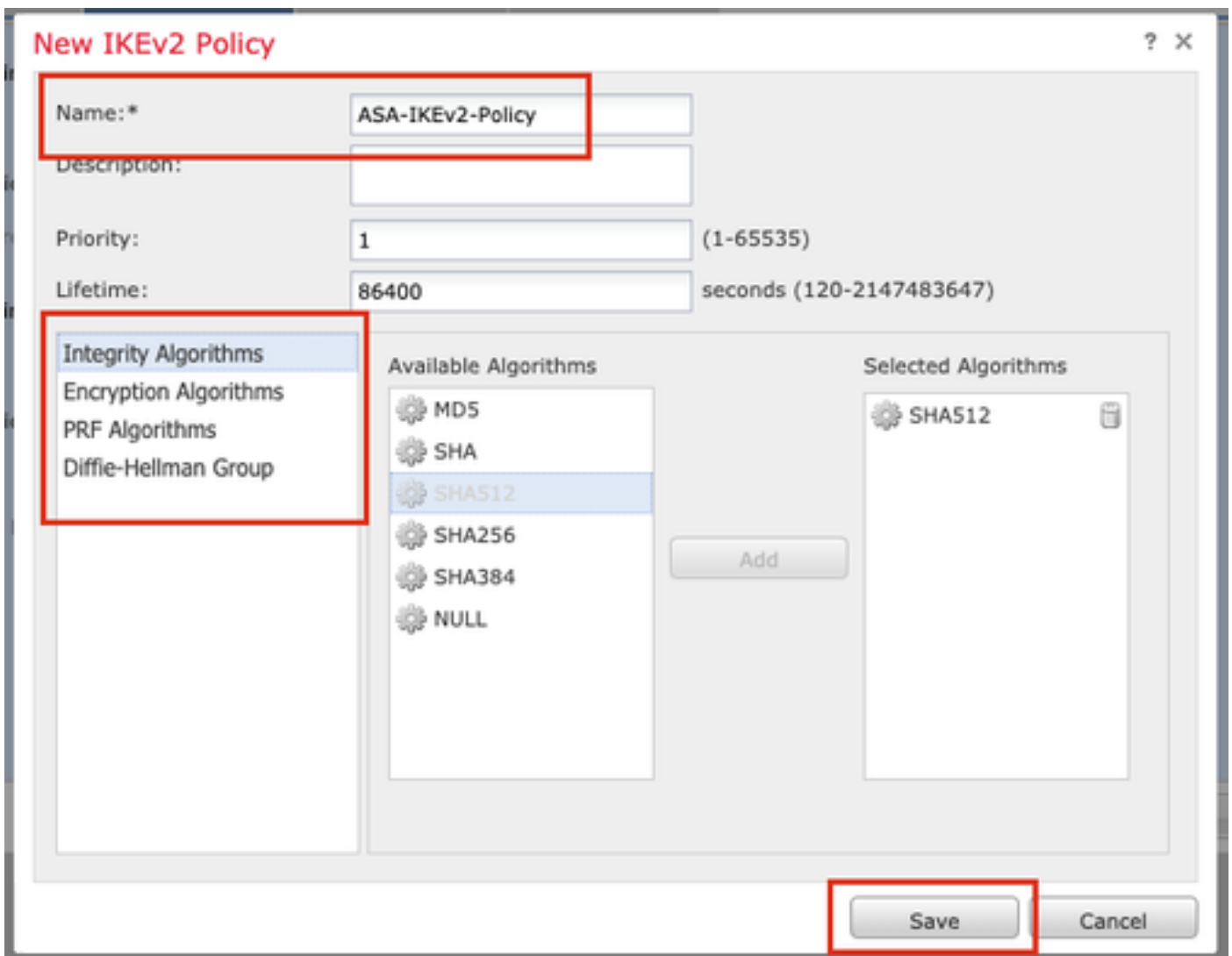For the purpose of this demonstration:

Name: ASA-IKEv2-Policy

Integrity Algorithms: SHA-512

Encryption Algorithms: AES-256

PRF Algorithms: SHA-512

Diffie-Hellman Group: 21

Step 10. Choose the newly created or the **Policy** that exists.. Select the **Authentication Type**. If a Pre-shared Manual Key is used, provide the key in the **Key** and **Confirm Key** boxes.

For the purpose of this demonstration:

Policy: ASA-IKEv2-Policy

Authentication Type: Pre-shared Manual Key

Key: cisco123

Confirm Key: cisco123

Note: If both the endpoints are registered on the same FMC, the option of Pre-shared Automatic Key can also be used.

Step 11. Navigate to the **IPsec** tab. You can choose to use a pre-defined IKEv2 IPsec Proposal or create a new one. Click the **Edit** button next to the **IKEv2 IPsec Proposal** tab.

Step 12. (Optional, if you create new IKEv2 IPsec Proposal.) Provide a **Name** for the Proposal and select

the **Algorithms** to be used in the Proposal. Click **Save**.

For the purpose of this demonstration:

Name: ASA-IPSec-Policy

ESP Hash: SHA-512

ESP Encryption: AES-256
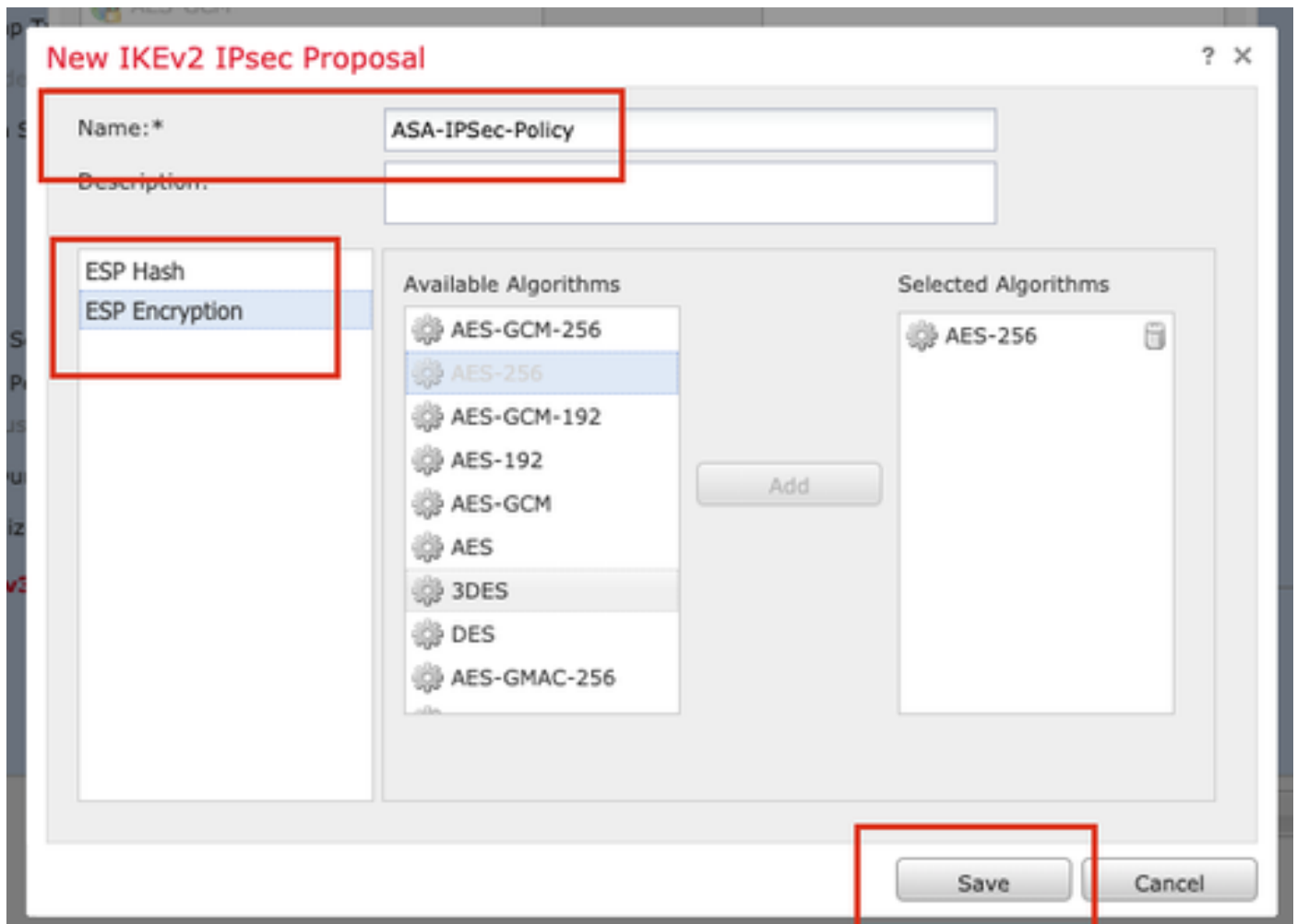
Step 13. Choose the newly created **Proposal** or **Proposal** that exists from the list of proposals available. Click **OK**.
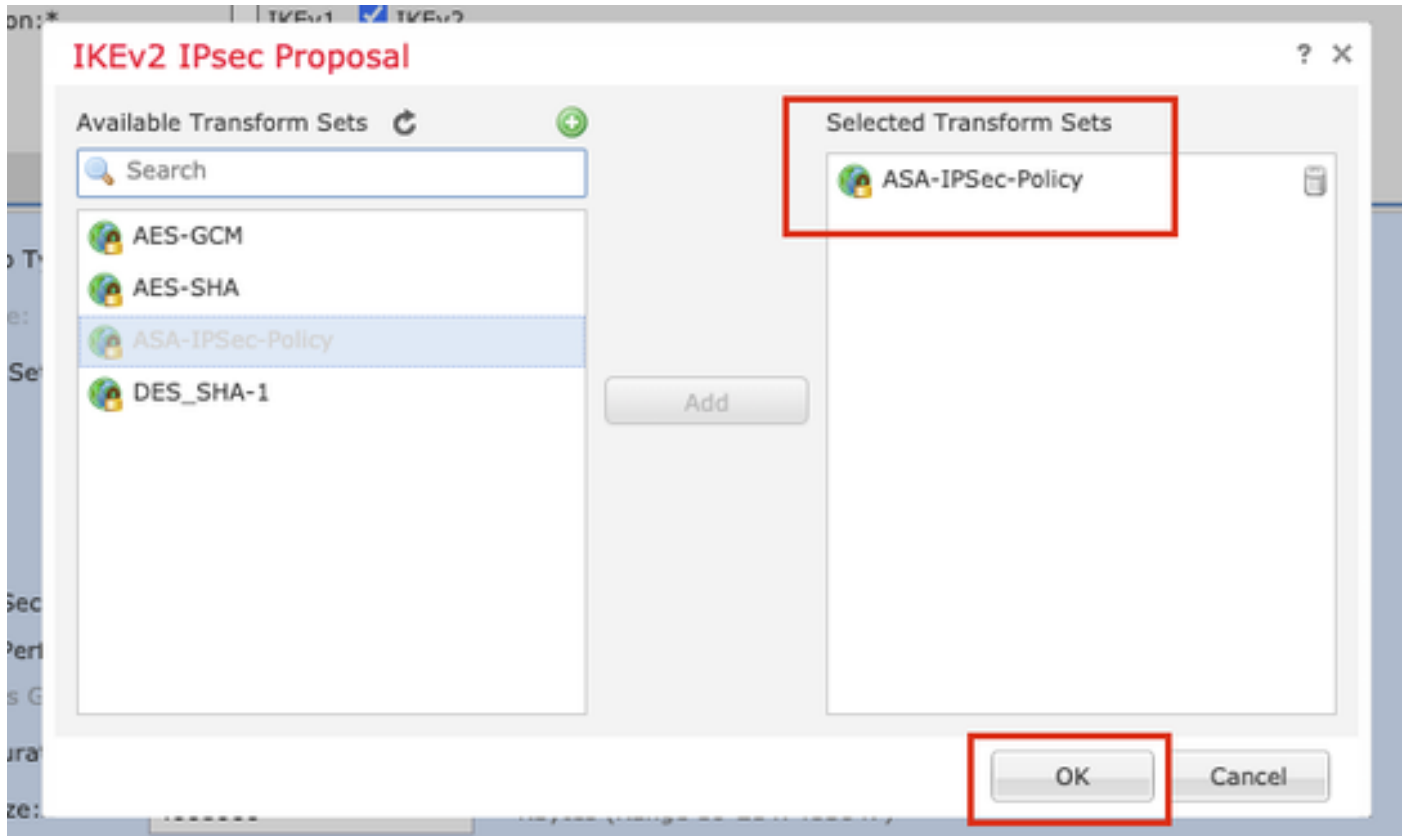
Step 14. (Optional) Choose the **Perfect Forward Secrecy** settings. Configure the IPsec **Lifetime Duration and Lifetime Size**.

For the purpose of this demonstration:

Perfect Forward Secrecy: Modulus Group 21

Lifetime Duration: 28800 (Default)

Lifetime Size: 4608000 (Default)
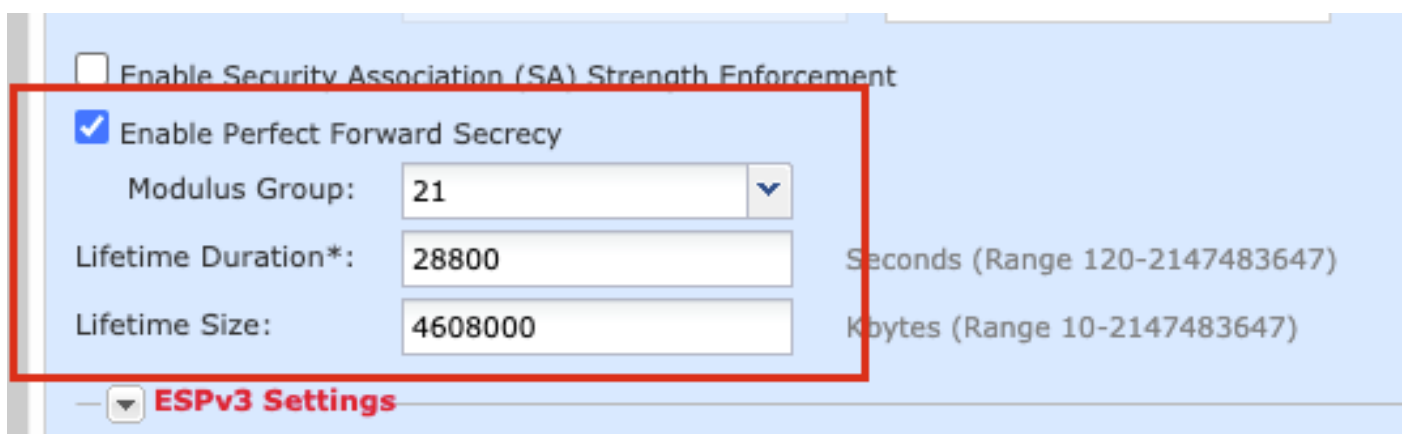
Step 15. Check the configured settings. Click **Save**, as shown in this image.

Step 16. Configure the Access Control Policy. Navigate to **Policies > Access Control > Access Control**. **Edit** the Policy applied to the FTD.

> **Note:** sysopt connection permit-vpn does not work with Route Based VPN tunnels. The Access Control Rules need to be configured for both IN > OUT zones and OUT > IN zones.

Provide the **Source Zones** and the **Destination Zones** in the **Zones** tab.

Provide the **Source Networks**, **Destination Networks** in the **Networks** tab. Click **Add**.

For the purpose of this demonstration:

Source Zones: In-Zone and Out-Zone

Destination Zones: Out-Zone and In-Zone

Source Networks: In-Network and Remote-Network

Destination Networks: Remote-Network and In-Network
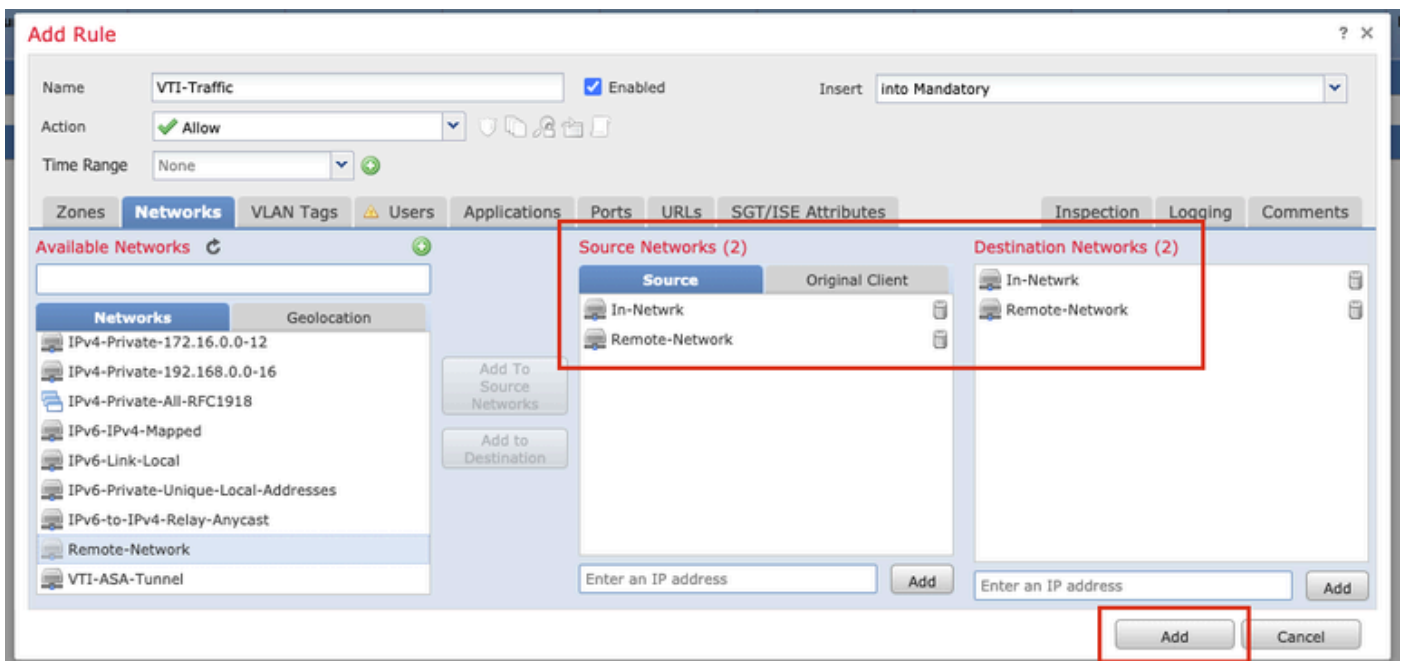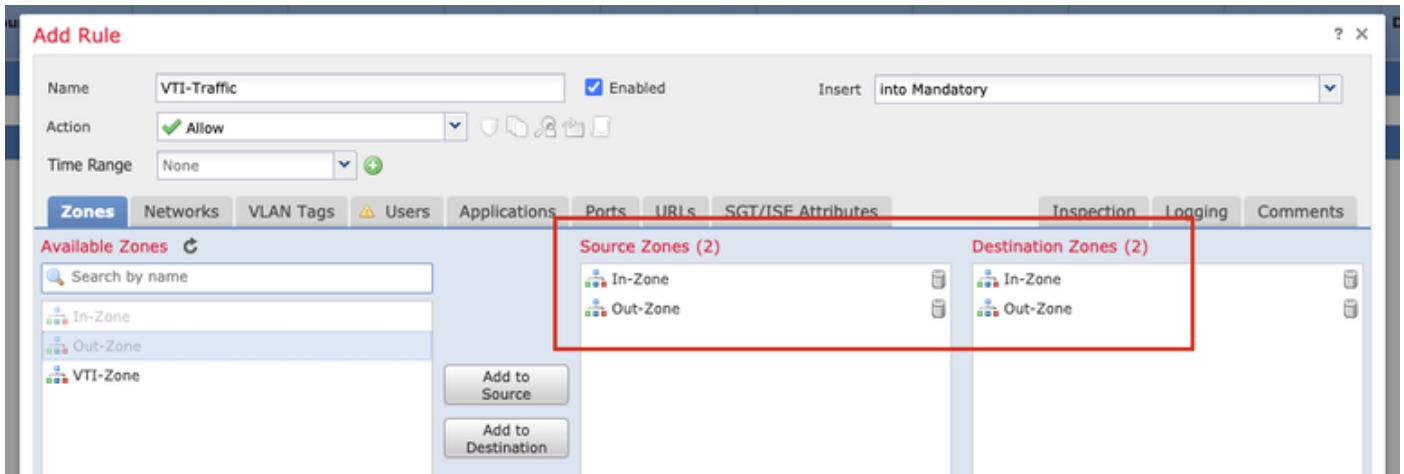
Step 17. Add the routing over the VTI tunnel. Navigate to **Devices > Device Management**. **Edit** the device where the VTI tunnel is configured on.

Navigate to **Static Route** under the **Routing** tab. Click **Add Route**.

Provide the **Interface**, choose the **Network**, provide the **Gateway**. Click **OK**.

For the purpose of this demonstration:

Interface: VTI-ASA

Network: Remote-Network

Gateway: VTI-ASA-Tunnel
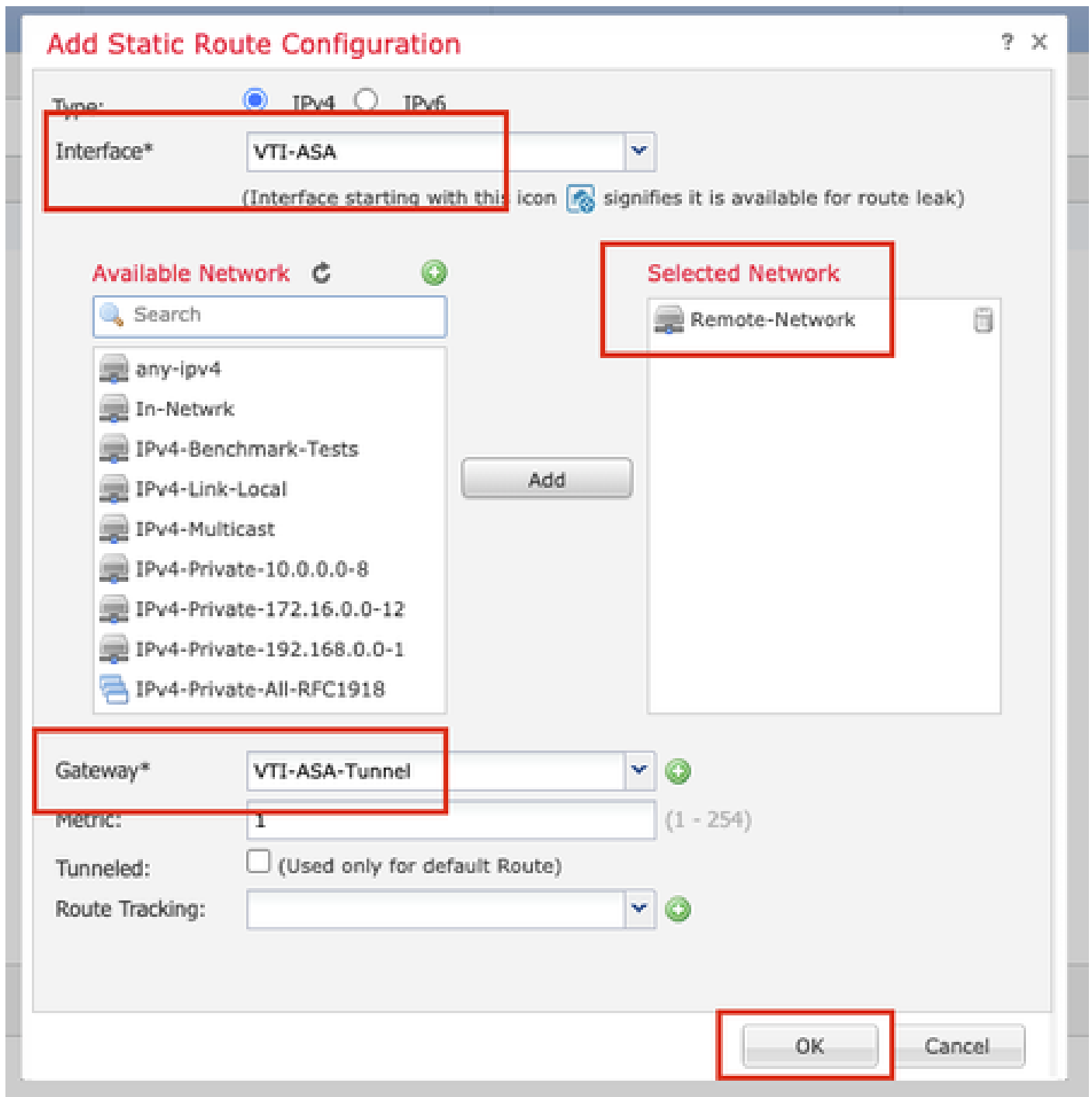
Step 18. Navigate to **Deploy > Deployment**. Choose the **FTD** to which the configuration needs to be deployed, and click **Deploy**.

Configuration pushed to the FTD CLI after successful deployment:

<#root>

```
crypto ikev2 policy 1


 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 86400
```

```
crypto ikev2 enable Outside


crypto ipsec ikev2 ipsec-proposal CSM_IP_1


 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1


 set ikev2 ipsec-proposal CSM_IP_1
 set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****


interface Tunnel1


 description VTI Tunnel with Extranet ASA

 nameif VTI-ASA


 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4

 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

Verify

From FMC GUI

Click the **Check Status** option to monitor the live status of the VPN tunnel from the GUI itself

Node B	
	✏️ 🗑️
FTD / VTI-ASA / 192.168.100.1	⚠️
	Check status

This includes these commands taken from the FTD CLI:

- **show crypto ipsec sa peer <Peer IP Address>**
- **show vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>**

Tunnel Status   ? ✕

🟢 **extranet : ASA-Peer**   📋   🟢 **FTD/VTI-ASA**   📋

```
> show crypto ipsec sa peer

Not applicable for extranet peer
```

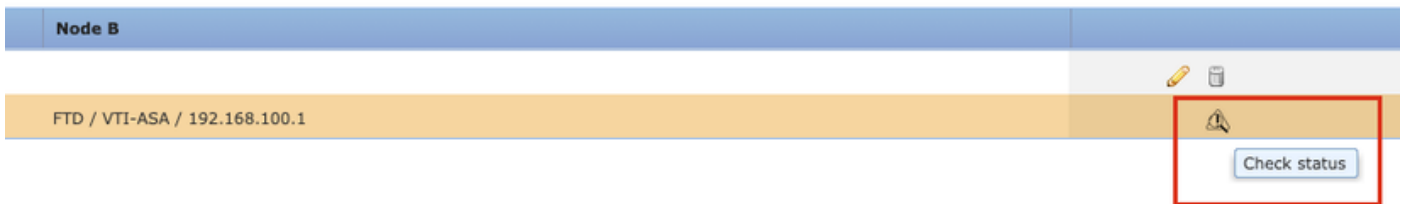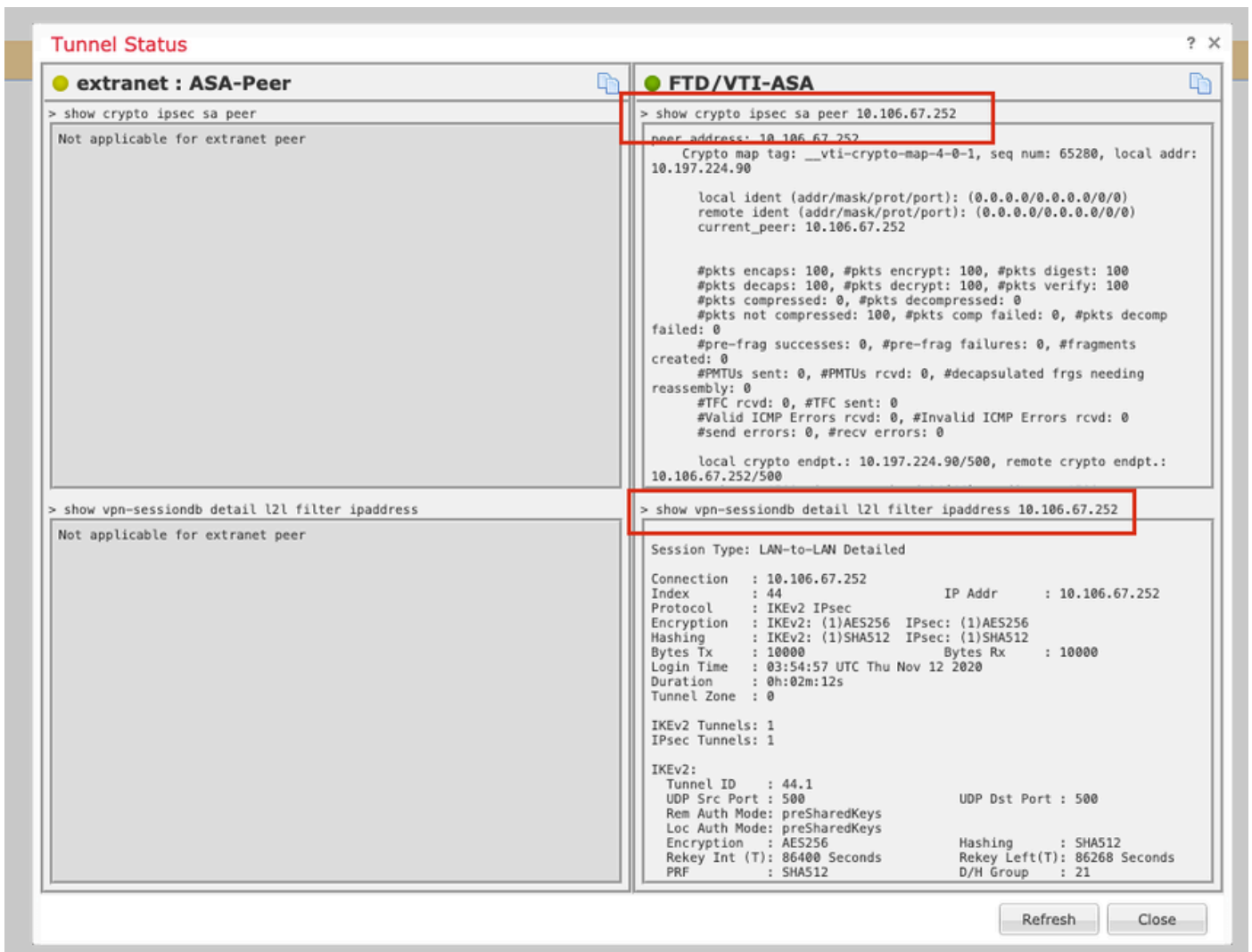```
> show crypto ipsec sa peer 10.106.67.252

peer address: 10.106.67.252
      Crypto map tag: __vti-crypto-map-4-0-1, seq num: 65280, local addr:
10.197.224.90

      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: 10.106.67.252

      #pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
      #pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 100, #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.: 10.197.224.90/500, remote crypto endpt.:
10.106.67.252/500
```

```
> show vpn-sessiondb detail l2l filter ipaddress

Not applicable for extranet peer
```

```
> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252

Session Type: LAN-to-LAN Detailed

Connection   : 10.106.67.252
Index        : 44                      IP Addr      : 10.106.67.252
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA512  IPsec: (1)SHA512
Bytes Tx     : 10000                   Bytes Rx     : 10000
Login Time   : 03:54:57 UTC Thu Nov 12 2020
Duration     : 0h:02m:12s
Tunnel Zone  : 0

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 44.1
  UDP Src Port : 500                   UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                Hashing      : SHA512
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86268 Seconds
  PRF          : SHA512                D/H Group    : 21
```

Refresh   Close

From FTD CLI

These commands can be used from the FTD CLI to view the configuration and the status of the VPN tunnels.

```
show running-config crypto
show running-config nat
show running-config route
```

```
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail l2l
```