

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Limitations and Restrictions](#)

[Configuration Steps on FMC](#)

[Verify](#)

[From FMC GUI](#)

[From FTD CLI](#)

Introduction

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

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 FMC.

Components Used

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

- Cisco Firepower Management Center (FMC) 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 refer to this [document](#).


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.

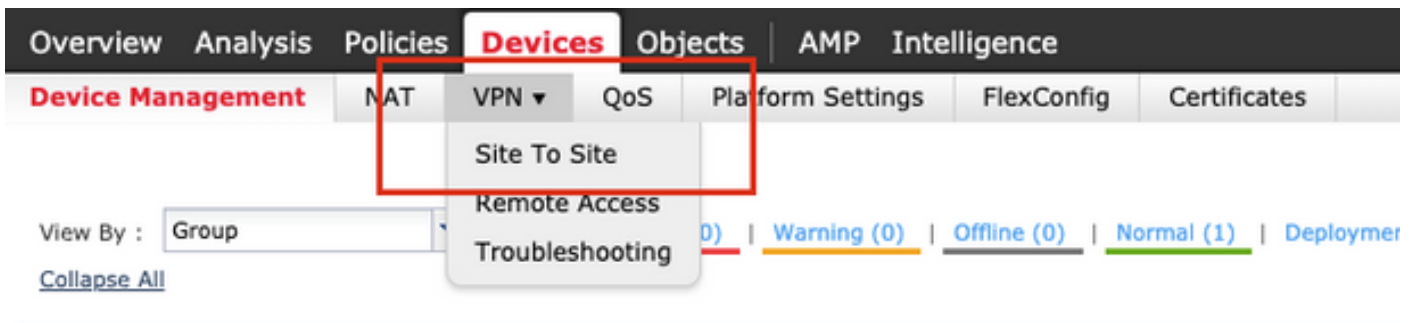
| FTD 6.7 managed via FMC 6.7 | Configuration Available | Site to Site VPN Tunnel |
|-----------------------------|--|--|
| Fresh Install | Weak ciphers available but cannot be used to configure the FTD 6.7 | Weak ciphers available but cannot be used to configure the FTD 6.7 |

| | | |
|---|--|--|
| | device. | 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 (Do not have a strong crypto license) | Allow DES is allowed | Allow 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.

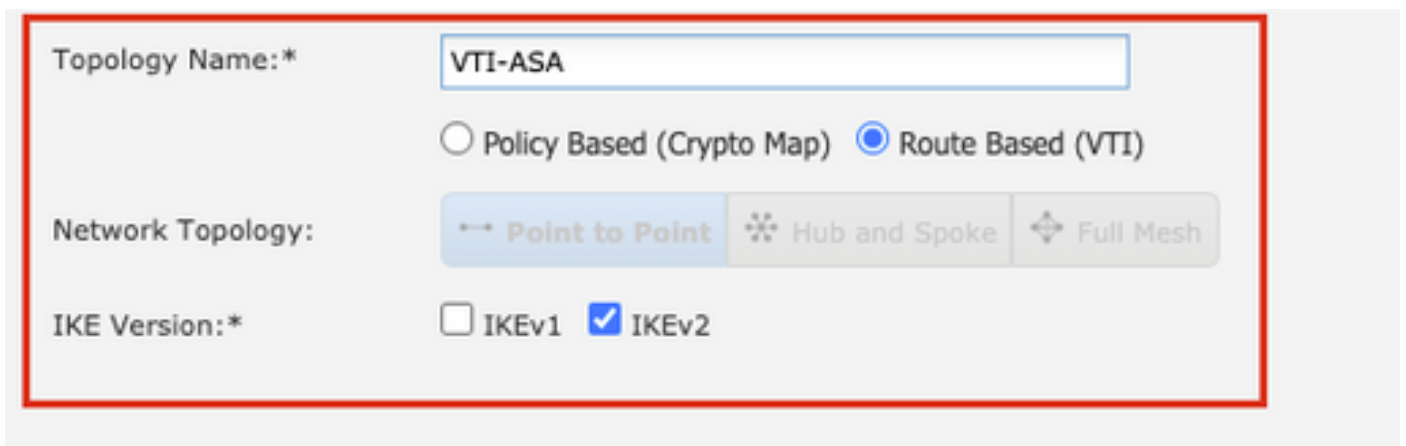


Step 3. Provide a **Topology Name** and select the Type of VPN as **Route Based (VTI)**. Choose the **IKE Version**.

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 Template Interface** (click on the + icon), or select one from the list that exists.

The screenshot shows the configuration page for IPsec endpoints. At the top, there are tabs for 'Endpoints', 'IKE', 'IPsec', and 'Advanced'. The 'Endpoints' tab is selected. The page is divided into two columns: 'Node A' and 'Node B'.
Node A configuration:
- Device: * (dropdown menu) - Value: FTD
- Virtual Tunnel Interface: * (dropdown menu) - Value: Empty
- Tunnel Source IP is Private:
- Connection Type: * (dropdown menu) - Value: Bidirectional
- Tunnel IP Address :
- Tunnel Source Interface :
- Tunnel Source Interface IP :
Node B configuration:
- Device: * (dropdown menu) - Value: Empty
- Virtual Tunnel Interface: * (dropdown menu) - Value: Empty
- Tunnel Source IP is Private:
- Connection Type: * (dropdown menu) - Value: Bidirectional
- Tunnel IP Address :
- Tunnel Source Interface :
- Tunnel Source Interface IP :
A red box highlights the 'Device' dropdown for Node A and the '+' icon next to the 'Virtual Tunnel Interface' dropdown for Node A.

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

For the purpose of this demonstration:

Name: VTI-ASA

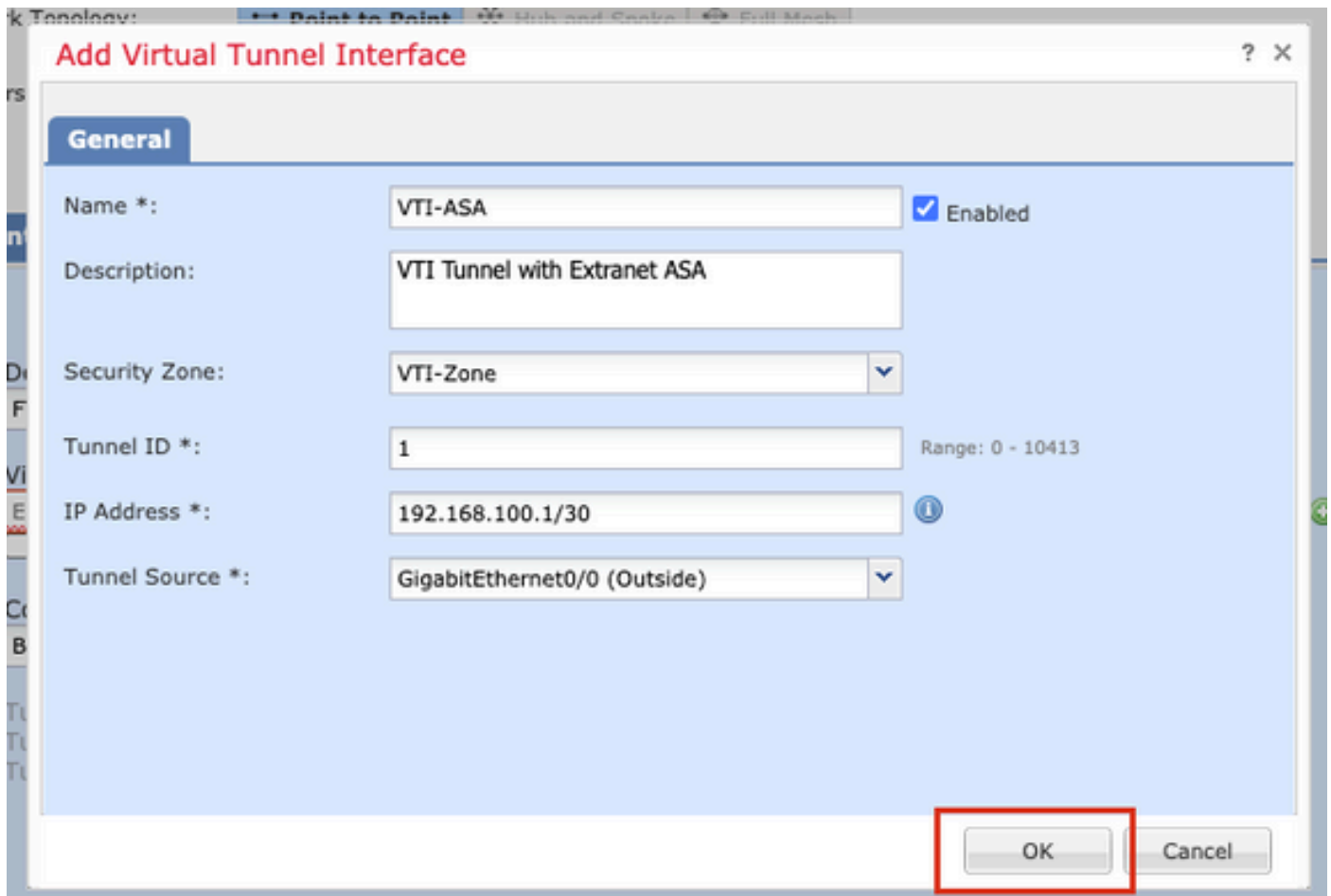
Description (Optional): VTI Tunnel with Extranet ASA

Security Zone: VTI-Zone

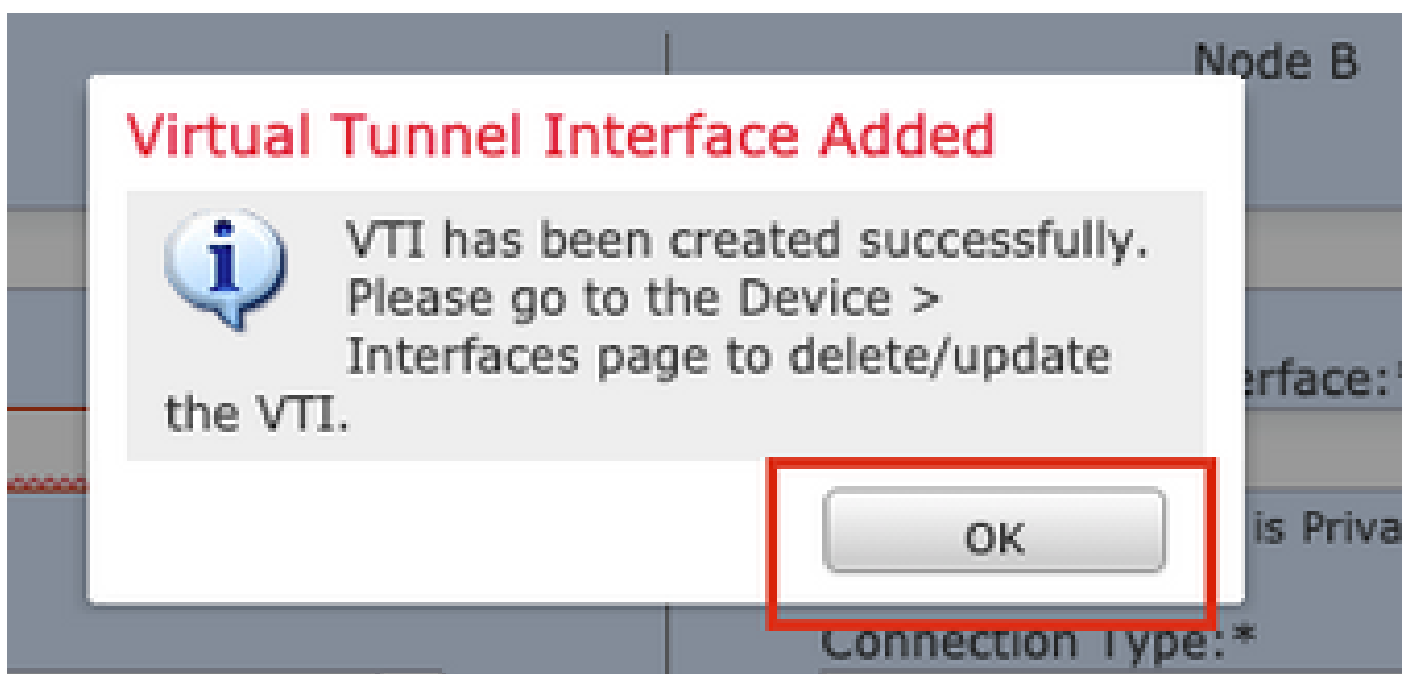
Tunnel ID: 1

IP Address: 192.168.100.1/30

Tunnel Source: GigabitEthernet0/0 (Outside)



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



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

Create New VPN Topology

Topology Name:* VTI-ASA

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:* FTD

Virtual Tunnel Interface:* VTI-ASA Tunnel Source IP is Private [Edit VTI](#)

Connection Type:* Bidirectional

Tunnel IP Address : 192.168.100.1
Tunnel Source Interface : Outside
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B

Device:* Extranet

Device Name*: ASA-Peer

Endpoint IP Address*: 10.106.67.252

Save Cancel

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.

IKEv2 Settings

Policy:* AES-GCM-NUL-NULL-SHA-LATEST

Authentication Type: Pre-shared Automatic Key

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

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:

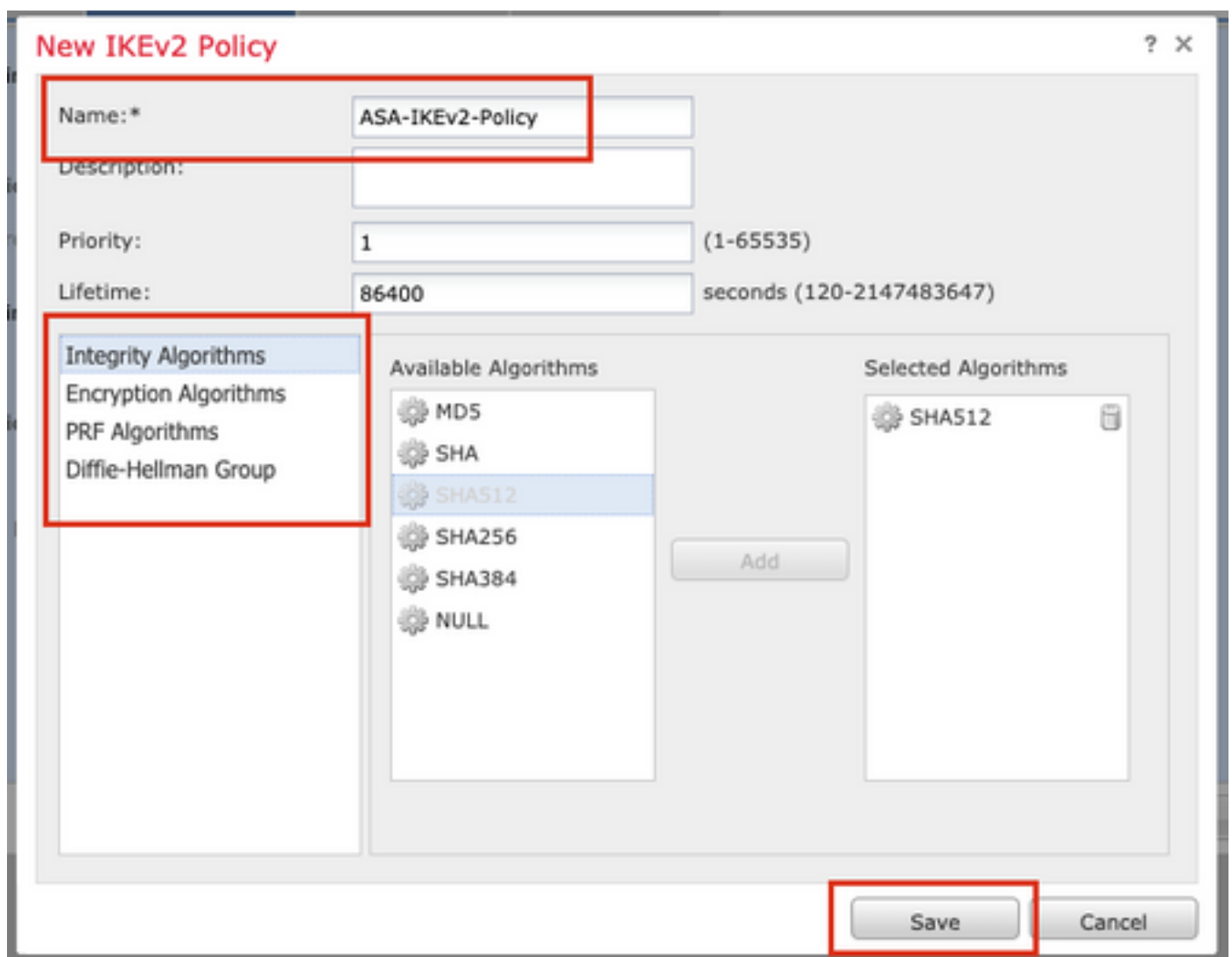
Name: ASA-IKEv2-Policy

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

The screenshot shows the configuration page for IKE. It has four tabs: Endpoints, IKE (selected), IPsec, and Advanced. Under the IKE tab, there are two sections: IKEv1 Settings and IKEv2 Settings. The IKEv1 Settings section includes: Policy:* (dropdown menu with 'preshared_sha_aes256_dh14_3' selected), Authentication Type: (dropdown menu with 'Pre-shared Automatic Key' selected), and Pre-shared Key Length:* (input field with '24' and a note '(Range 1-127)'). The IKEv2 Settings section is highlighted with a red border and includes: Policy:* (dropdown menu with 'ASA-IKEv2-Policy' selected), Authentication Type: (dropdown menu with 'Pre-shared Manual Key' selected), Key:* (password field with 8 dots), Confirm Key:* (password field with 8 dots), and an unchecked checkbox labeled 'Enforce hex-based pre-shared key only'.

 **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.

The screenshot shows the IPsec configuration page. It has two main sections: IKEv1 IPsec Proposals and IKEv2 IPsec Proposals*. The IKEv1 section has a dropdown menu for 'IKEv1 IPsec Proposals' with 'tunnel_aes256_sha' selected. The IKEv2 section has a dropdown menu for 'IKEv2 IPsec Proposals*' with 'AES-GCM' selected. The 'Edit' button (pencil icon) next to 'AES-GCM' is highlighted with a red box. At the bottom, there is an unchecked checkbox labeled 'Enable Security Association (SA) Strength Enforcement'.

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

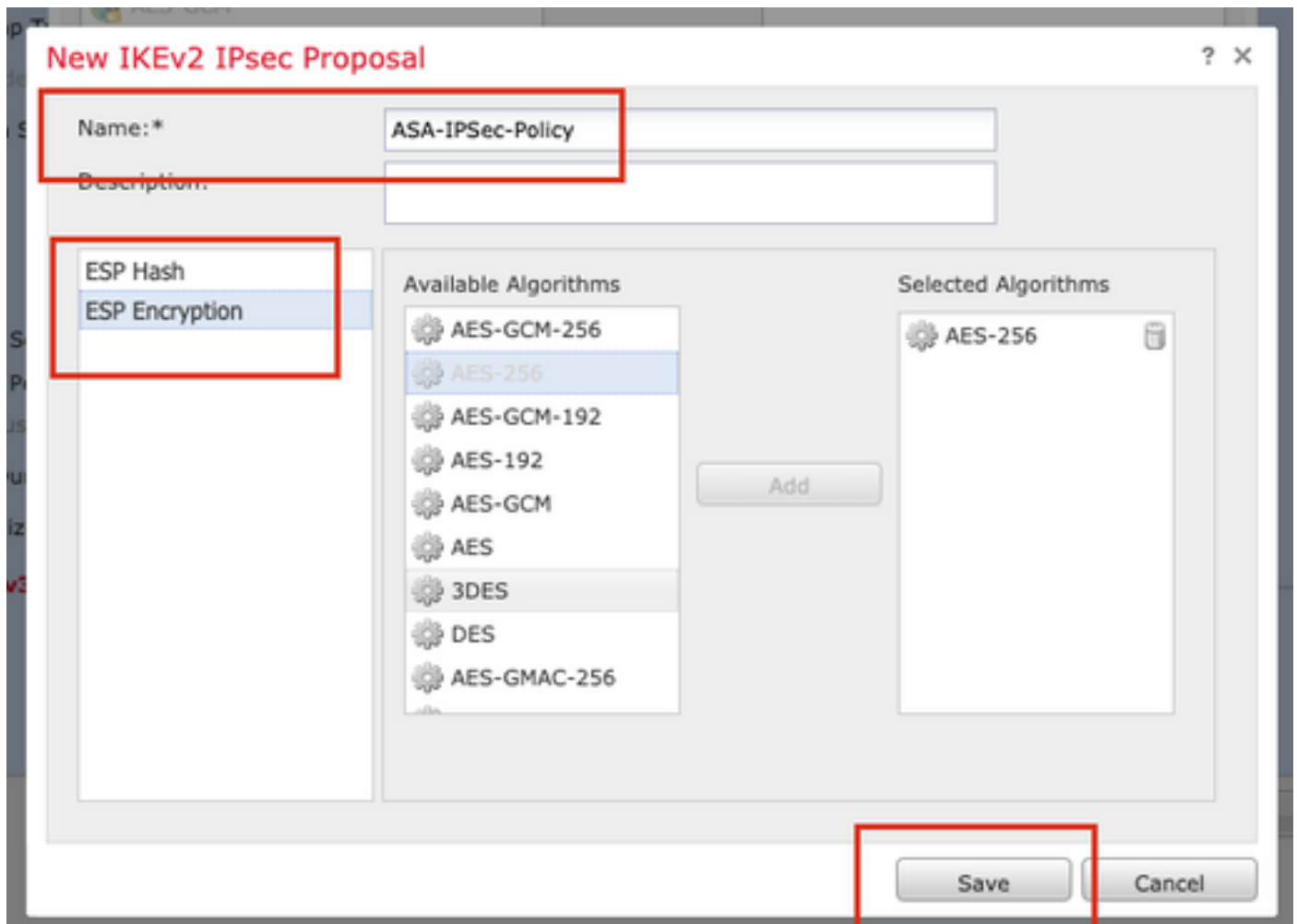
the **Algorithms** to be used in the Proposal. Click **Save**.

For the purpose of this demonstration:

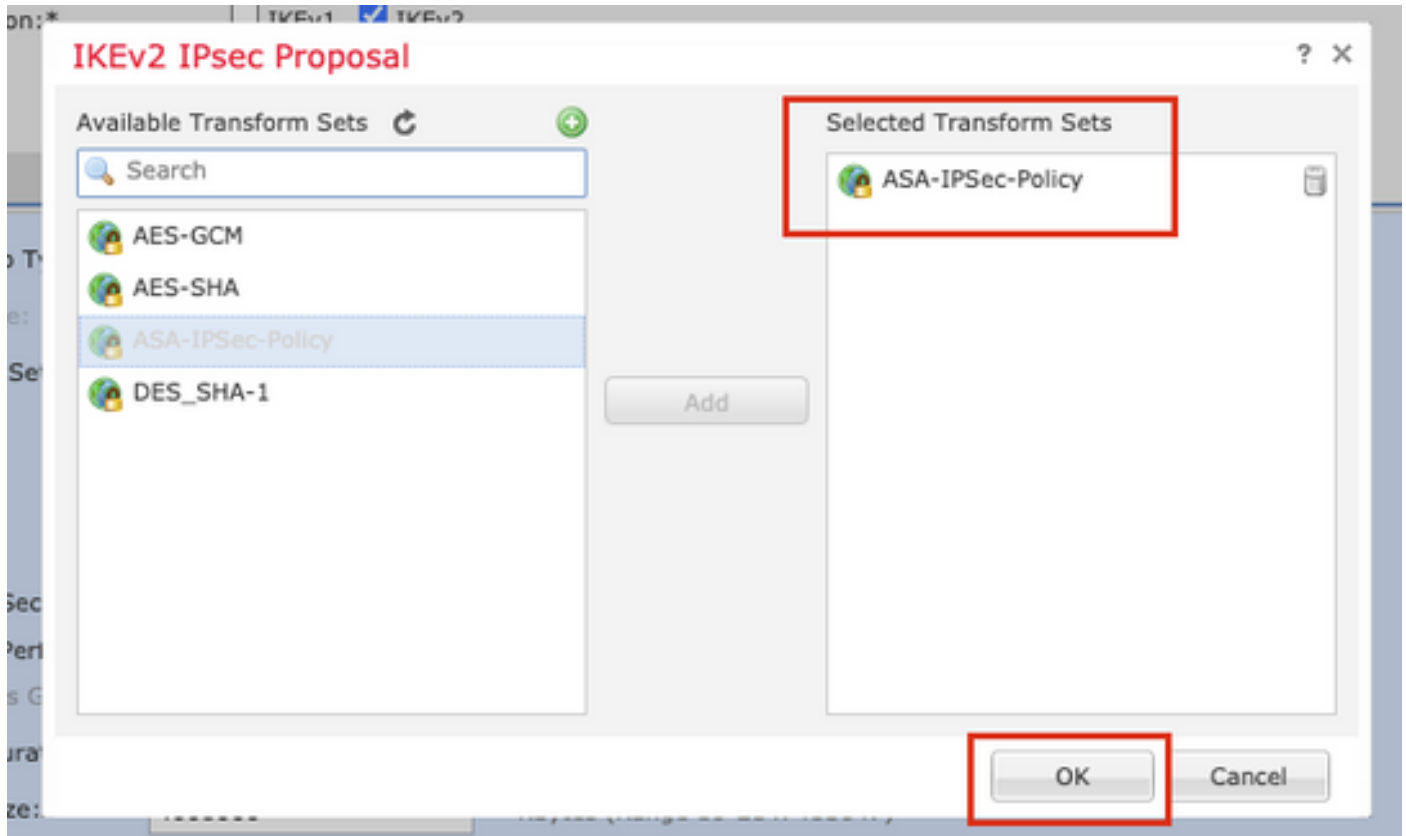
Name: ASA-IPSec-Policy

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**.



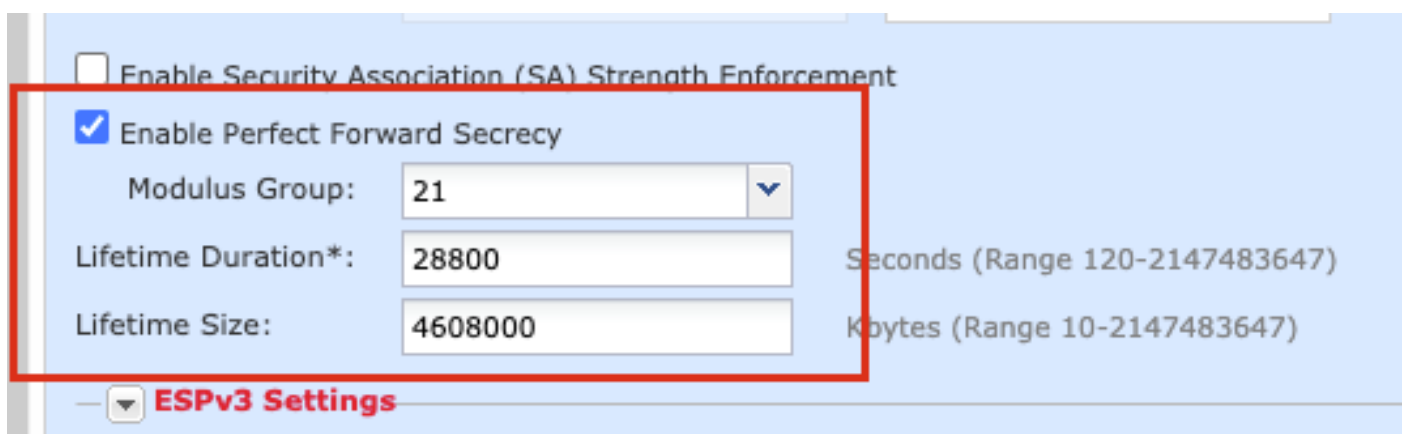
Step 14. (Optional) Choose the **Perfect Forward Secrecy** settings. Configure the IPsec **Lifetime Duration and Lifetime Size**.

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.

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets: **IKEv1 IPsec Proposals** **IKEv2 IPsec Proposals***

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

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**.

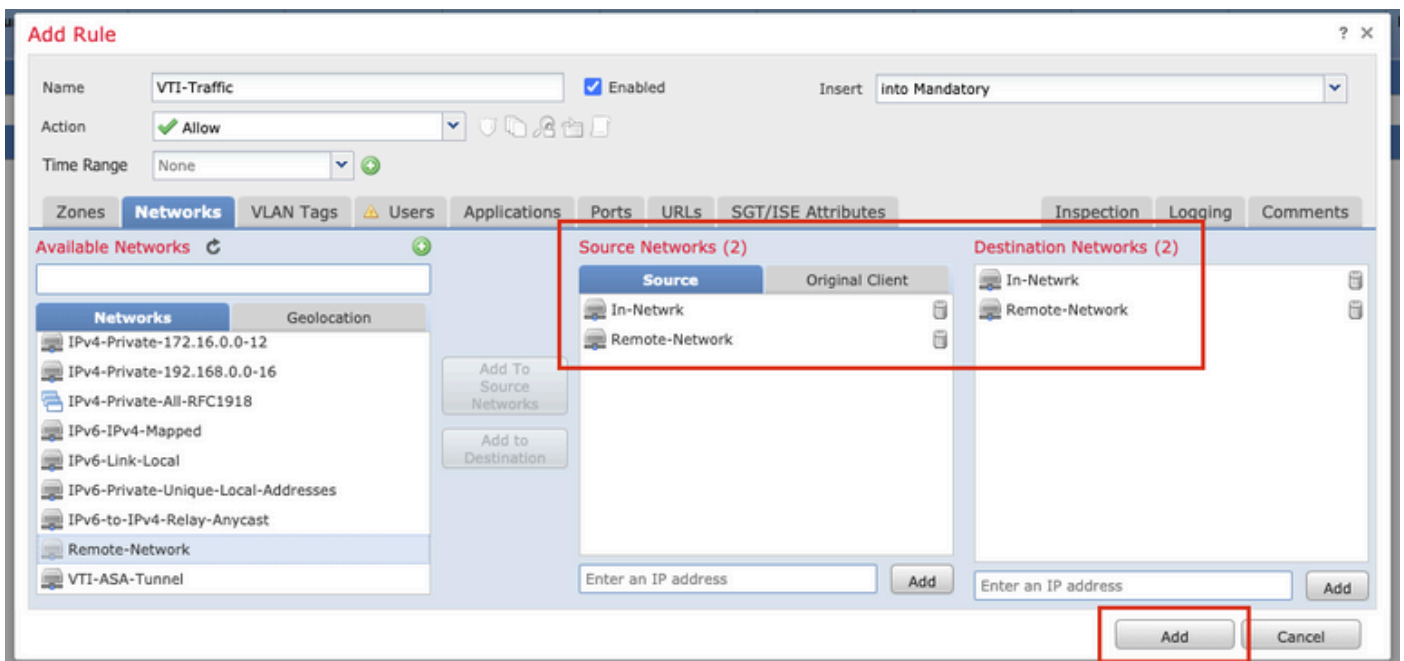
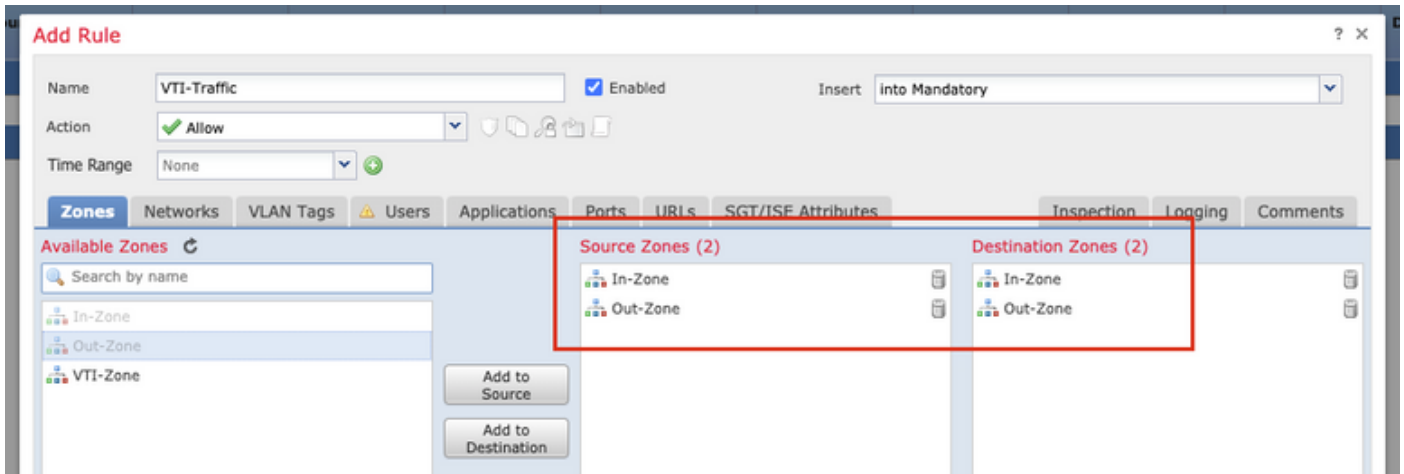
For the purpose of this demonstration:

Source Zones: In-Zone and Out-Zone

Destination Zones: Out-Zone and In-Zone

Source Networks: In-Netwrk and Remote-Network

Destination Networks: Remote-Network and In-Netwrk



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**.

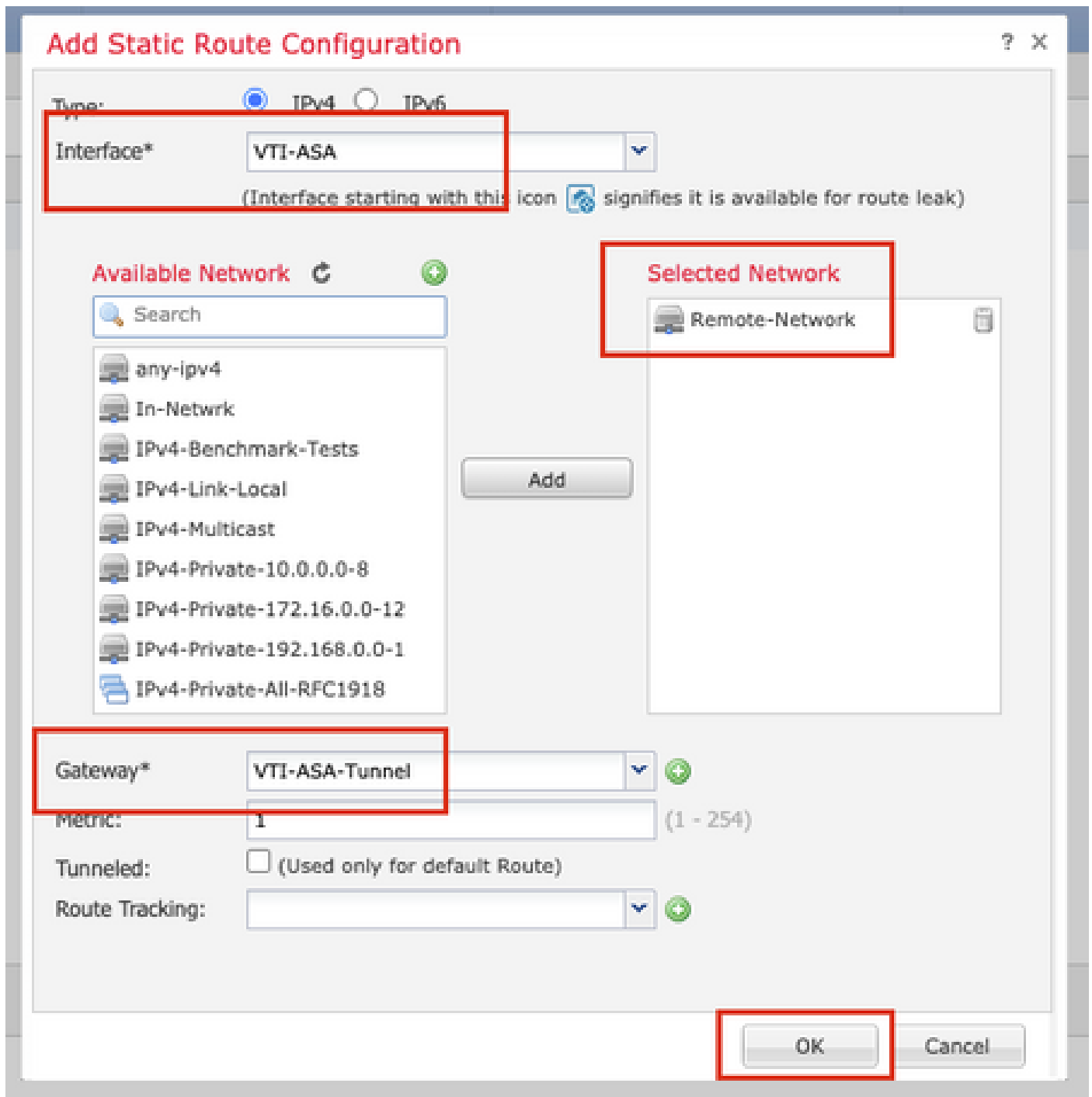
Provide the **Interface**, choose the **Network**, provide the **Gateway**. Click **OK**.

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

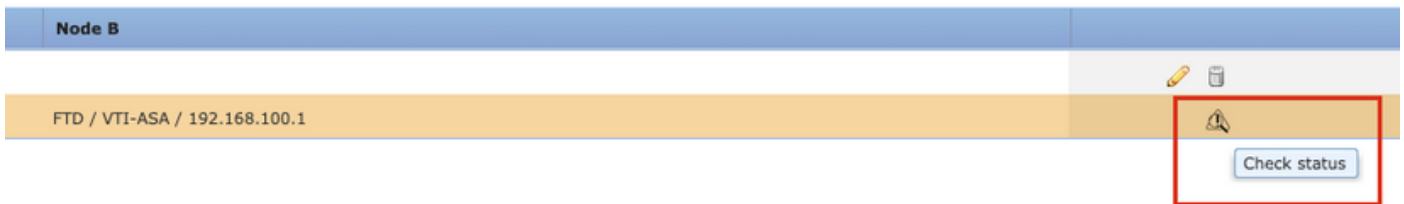
    tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

```

Verify

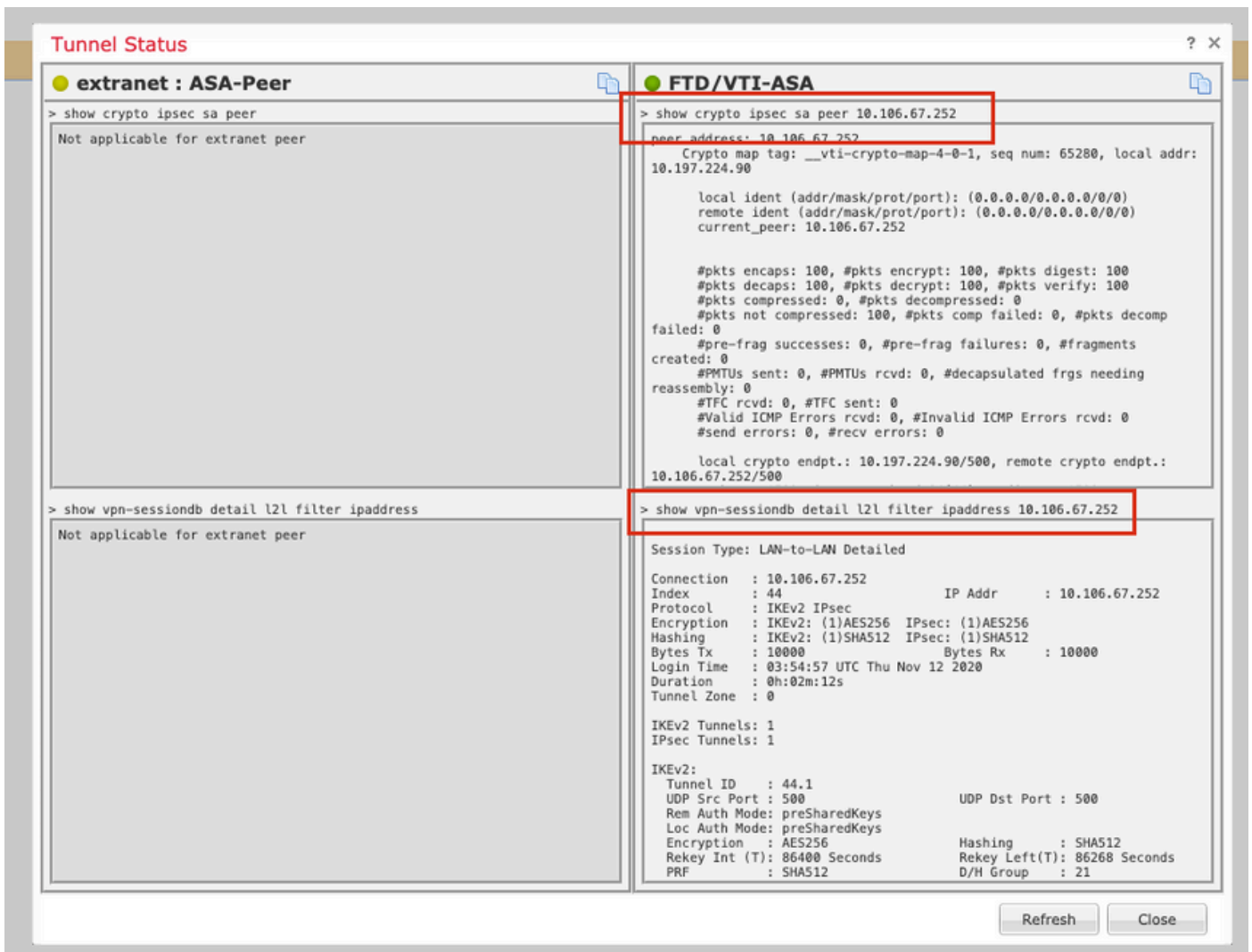
From FMC GUI

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



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>**



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 121
```