

# Configure Route Based VPN with Static Route on FTD Managed by FDM

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configuration Steps on FDM](#)

[Verify](#)

[Related Information](#)

---

## Introduction

This document describes how to configure a static route-based site to site VPN tunnel on a FTD managed by FDM.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of how a VPN tunnel works.
- Prior knowledge of navigating through the Firepower Device Manager(FDM).

### Components Used

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

- Cisco Firepower Threat Defense (FTD) version 7.0 managed by Firepower Device Manager(FDM).

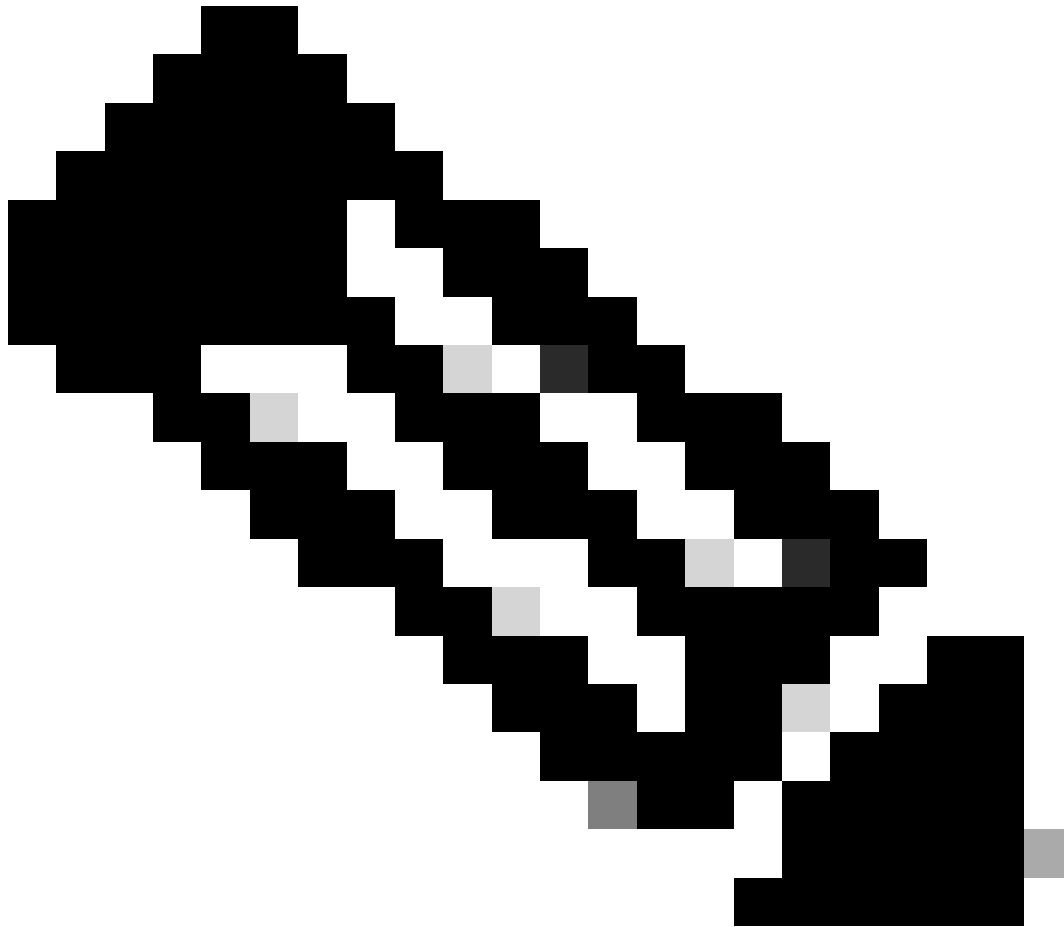
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## 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.

---

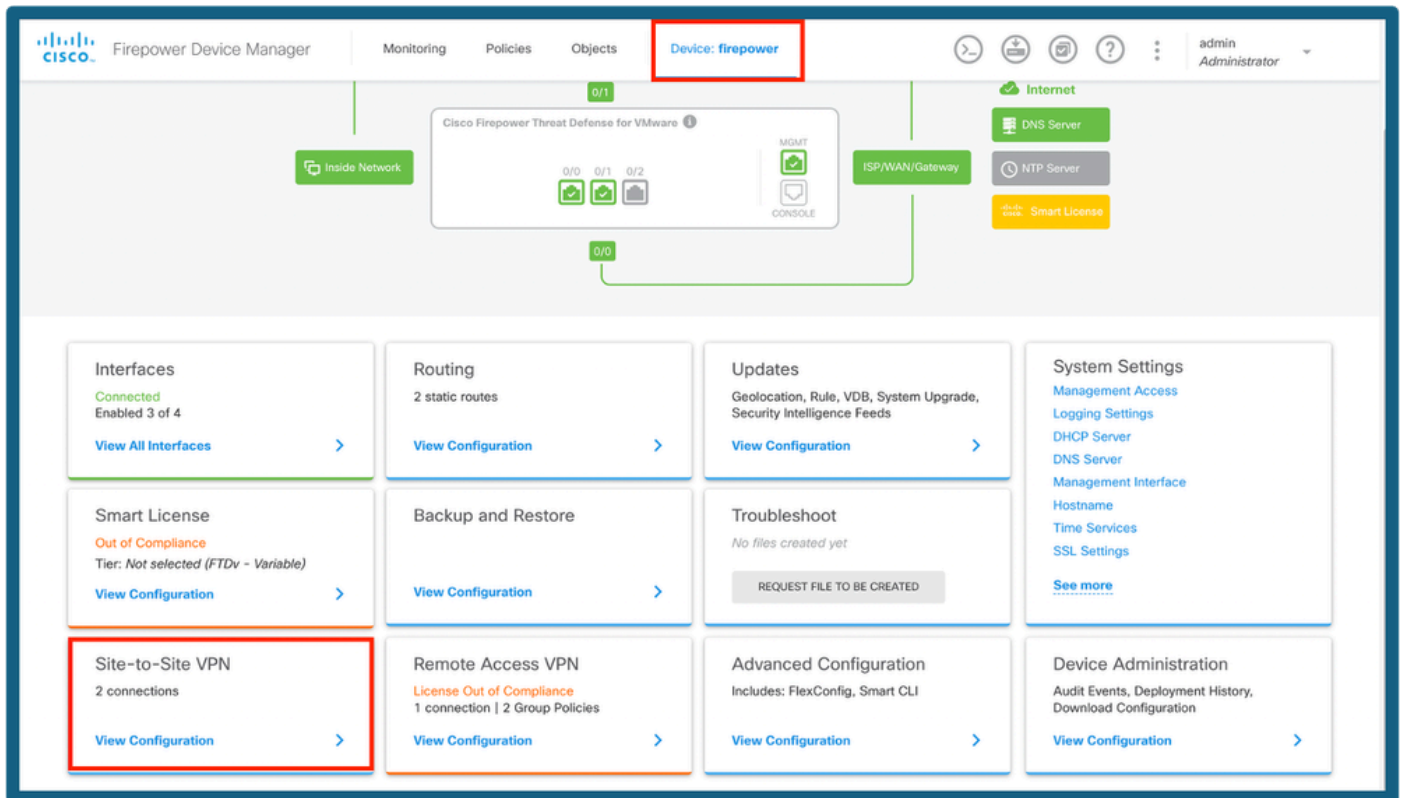


**Note:** No additional licensing is needed, Route Based VPN can be configured in Licensed as well as Evaluation Modes. Without crypto compliance (Export Controlled Features Enabled), only DES can be used as an encryption algorithm.

---

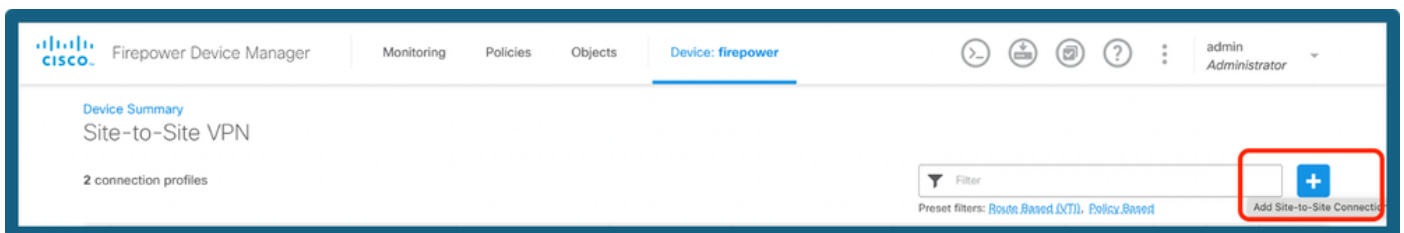
## Configuration Steps on FDM

Step 1. Navigate to **Device > Site To Site**.



FDM Dashboard

Step 2. Click on the + icon to add a new site to site connection.



Add S2S Connection

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

Click on **Local VPN Access Interface**, and then click **Create new Virtual Tunnel Interface** or select one from the list that exists.

Firepower Device Manager | Monitoring | Policies | Objects | **Device: firepower**

Local Network — FIREPOWER — VPN TUNNEL — INTERNET — OUTSIDE INTERFACE — PEER ENDPOINT — Remote Network

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

**Connection Profile Name**  
vdi-ipsec

**Type**  
**Route Based (VTI)** Policy Based

**Sites Configuration**

**LOCAL SITE**  
Local VPN Access Interface  
Please select

**REMOTE SITE**  
Remote IP Address

Filter

Nothing found

[Create new Virtual Tunnel Interface](#)

NEXT

*Add Tunnel Interface*

Step 4. Define the parameters of the New Virtual Tunnel Interface. Click **Ok**.

# Create Virtual Tunnel Interface

Name

tunnel10

Status

☒

*Most features work with named interfaces only, although some require unnamed interfaces.*

Description

Tunnel ID i

10

0 - 10413

Tunnel Source i

outside (GigabitEthernet0/0)

IP Address and Subnet Mask

192.168.1.1 / 255.255.255.252

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

CANCEL

OK

VTI Config

Step 5. Choose the newly created VTI or a VTI that exists under Virtual Tunnel Interface. Provide the **Remote IP address**.

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Local Network FIREPOWER VPN TUNNEL INTERNET OUTSIDE INTERFACE PEER ENDPOINT Remote Network

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type: ☒ Route Based (VTI) ☐ Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface:

REMOTE SITE

Remote IP Address:

Add Peer IP

Step 6. Choose the **IKE Version** and choose the **Edit** button to set the IKE and IPsec parameters as shown in the image.

### IKE Policy

**i** IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

**IKE VERSION 2** ☒ **IKE VERSION 1** ☐

IKE Policy

Globally applied

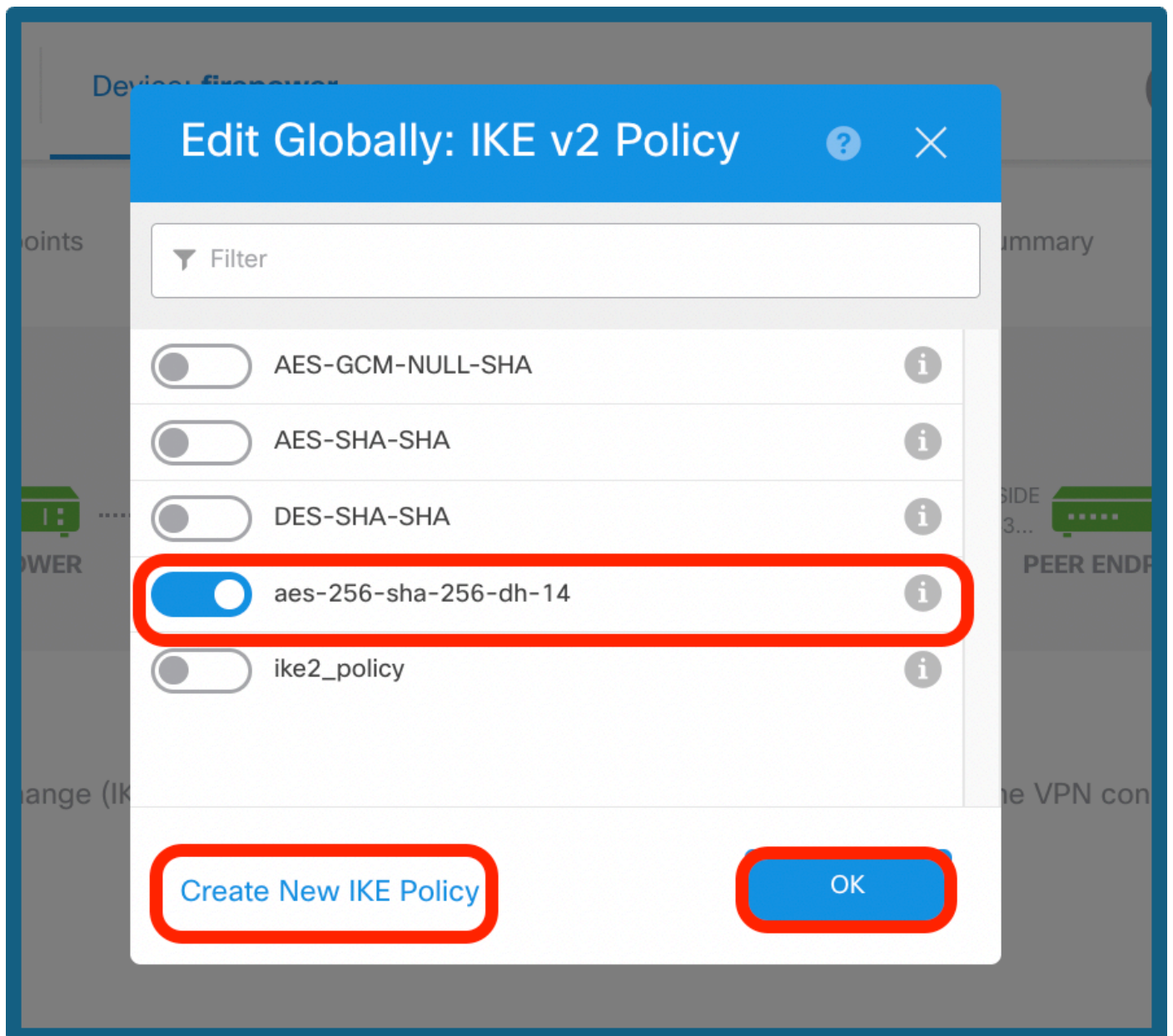
IPSec Proposal

Custom set selected

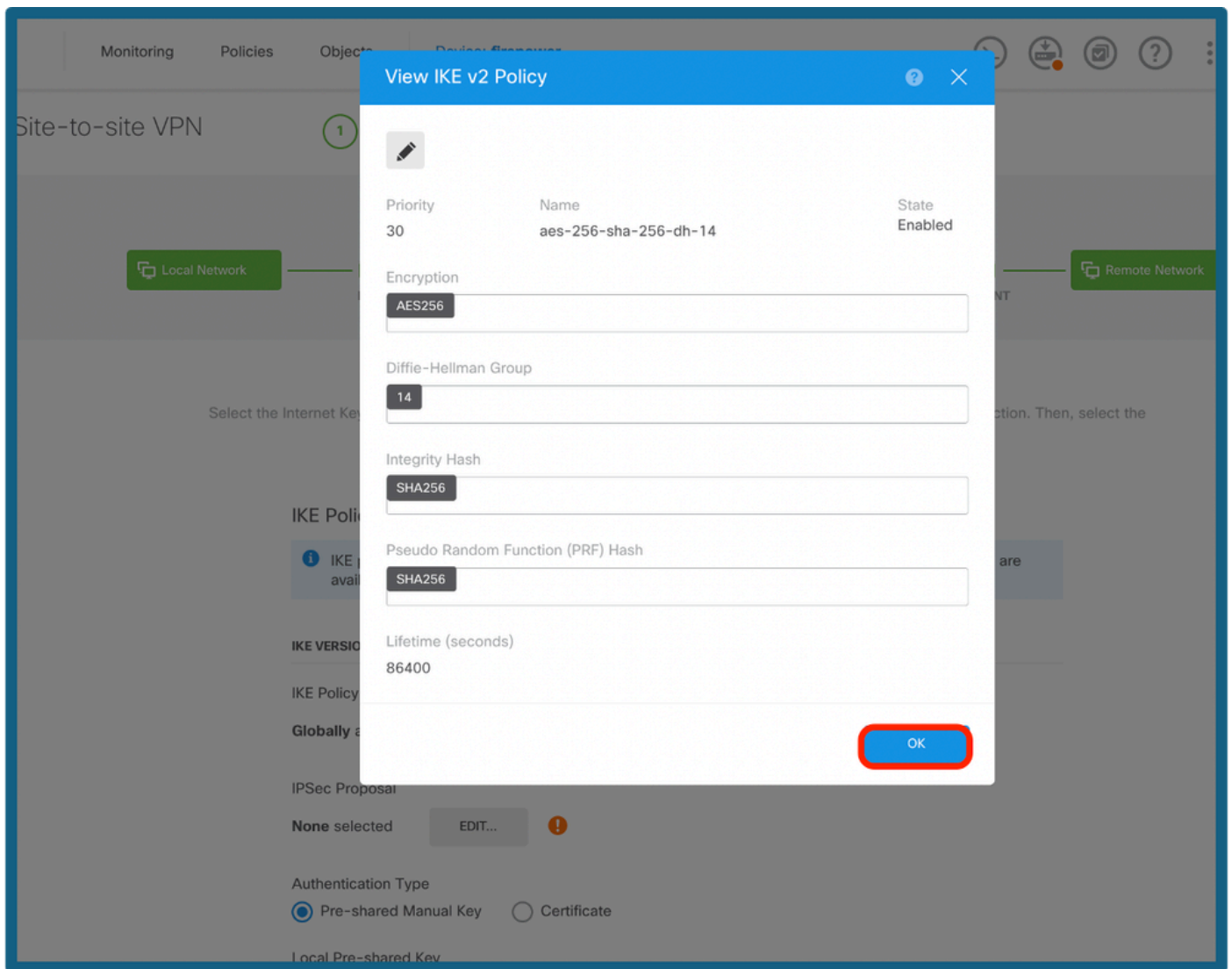
Configure IKE Version

Step 7a. Choose the **IKE Policy** button as shown in the image and click on **ok** button or **Create New IKE Policy**, if you like to create a new policy.





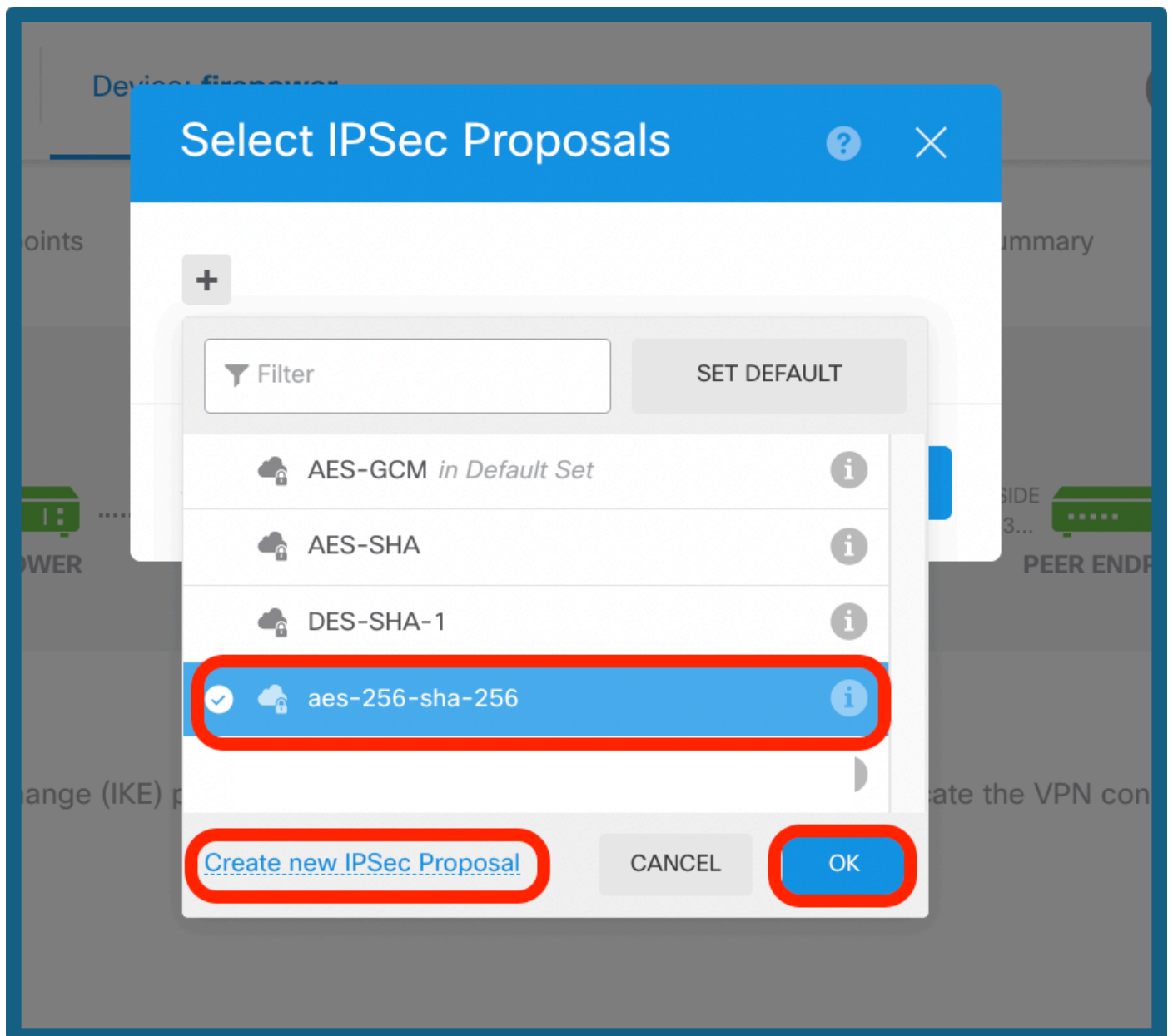
Choose IKE Policy



*Config of IKE Policy*

Step 7b. Choose the **IPSec Policy** button as shown in the image and click on **ok** button or **Create New IPSec Proposal**, if you like to create a new proposal.





Select IPsec Proposal

**IKE v2 IPsec Proposal**

Name  
aes-256-sha-256

Encryption  
AES256

Integrity Hash  
SHA256

OK

*Config of IPsec Proposal*

Step 8a. Select the **Authentication Type**. If Pre-shared Manual Key is used, provide the **Local** and **Remote** Pre-shared Key.

Step 8b. (Optional) Choose the **Perfect Forward Secrecy** settings. Configure the IPsec **Lifetime Duration** and **Lifetime Size**, and then click on next.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied 

EDIT...

IPSec Proposal

Custom set selected 

EDIT...

Authentication Type

☒ Pre-shared Manual Key ☐ Certificate

Local Pre-shared Key

••••••••

Remote Peer Pre-shared Key

••••••••|

IPSEC SETTINGS

Lifetime Duration

28800

seconds

120 - 2147483647; (Default: 28800)

Lifetime Size

4608000

kilobytes

10 - 2147483647; (Default: 4608000).  
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off) ▼

i

BACK

NEXT


PSK and Lifetime Config

Step 9. Review the configuration and click on **Finish**.

## Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

### Vti-Ipsec Connection Profile

 Peer endpoint needs to be configured according to specified below configuration.

**VPN Access  
Interface IP**  tunnel10 (1.1.1.1)



**Peer IP Address** 10.106.63.23

#### IKE V2

**IKE Policy** aes-256-sha256-sha256-14

**IPSec Proposal** aes-256-sha-256

**Authentication  
Type** Pre-shared Manual Key

#### IKE V1: DISABLED

#### IPSEC SETTINGS

**Lifetime  
Duration** 28800 seconds

**Lifetime Size** 4608000 kilobytes

#### ADDITIONAL OPTIONS

**Diffie-Hellman  
Group** Null (not selected)

 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

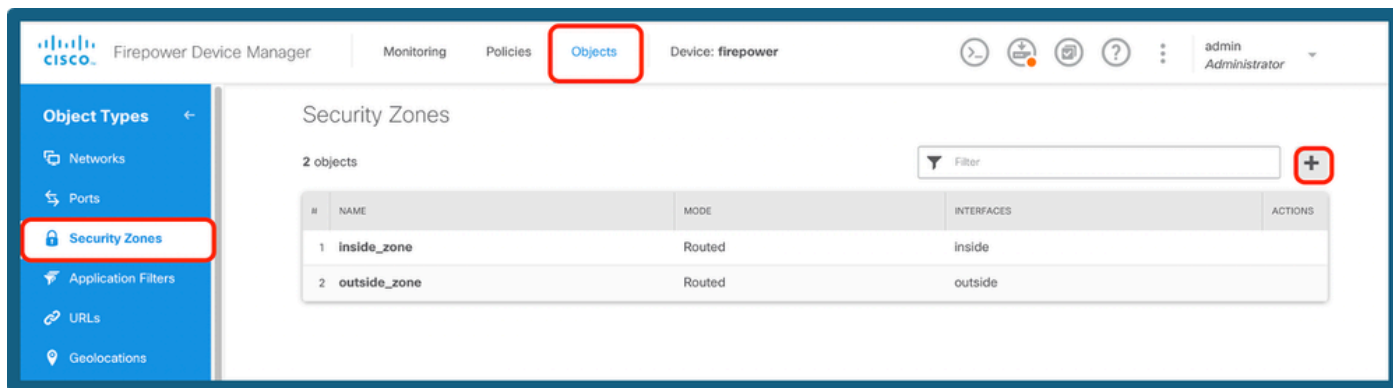
BACK

FINISH

*Configuration Summary*

Step 10a. Navigate to **Objects > Security Zones** and then click on + icon.





*Add a Security Zone*

Step 10b. Create a zone, and select the VTI interface as shown below.

### Add Security Zone

Name

vti-zone

Description

Mode

☒ Routed ☐ Passive

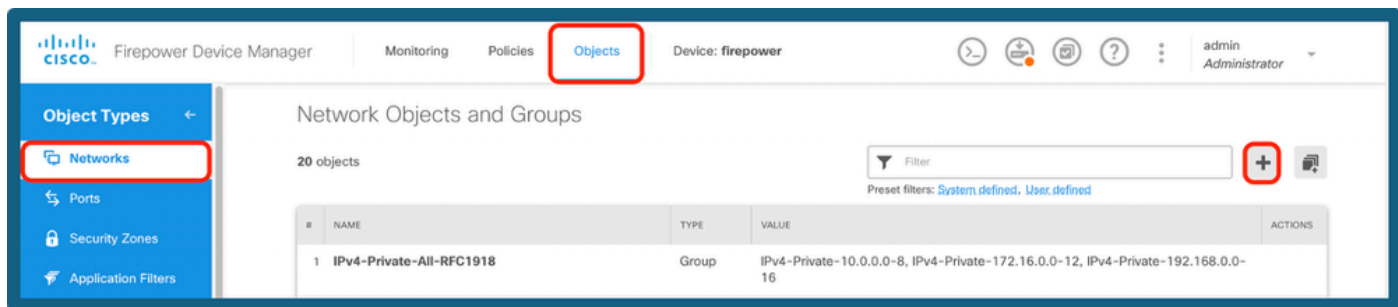
Interfaces

+ tunnel10 (Tunnel10)

CANCEL OK

*Config of Security Zone*

Step 11a. Navigate to **Objects > Networks**, click on + icon.



Add Network Objects

Step 11b. Add a **host** object, and create a gateway with tunnel ip of peer end.

### Edit Network Object

**Name**

vpn-gateway

**Description**

**Type**

☐ Network ☒ **Host** ☐ FQDN ☐ Range

**Host**

192.168.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL OK

Configure VPN Gateway

Step 11c. Add the remote subnet and the local subnet.



Edit Network Object

?

×

Name

remote-vpn-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Remote IP Config

Edit Network Object

?

×

Name

inside-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

10.10.10.0/24

*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

Local IP Config

Step 12. Navigate to **Device > Policies**, and configure the **Access Control Policy**.

**Add Access Rule**

Order: 1 | Title: vti-acl | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

**SOURCE**

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

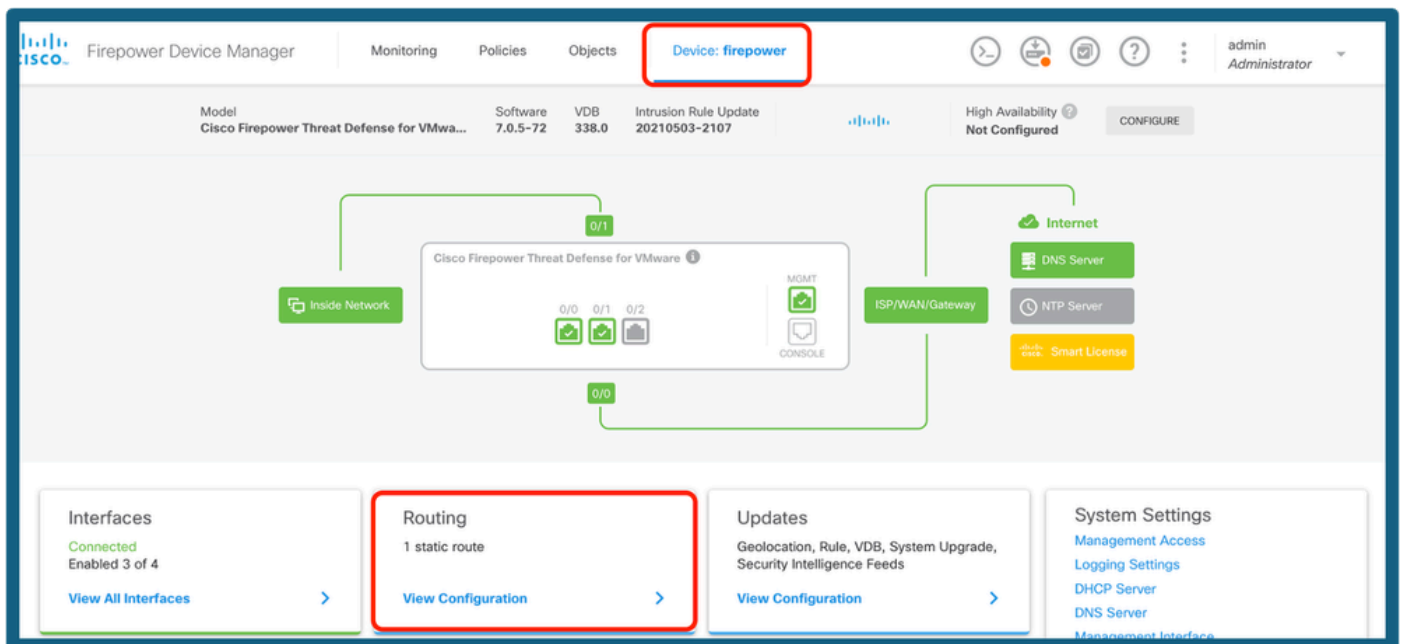
**DESTINATION**

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

Show Diagram: ☐ | CANCEL | OK

Add Access Control Policy

Step 13a. Add the routing over the VTI tunnel. Navigate to **Device > Routing**.



Select Routing

Step 13b. Navigate to **Static Route** under the **Routing** tab. Click + icon.

Device Summary

Routing

Add Multiple Virtual Routers

Commands

BGP Global Settings

Static Routing

BGP

OSPF

EIGRP

ECMP Traffic Zones

1 route

Filter

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

Add Route

Step 13c. Provide the **Interface**, choose the **Network**, provide the **Gateway**. Click **OK**.

## Add Static Route

Name

vti-route

Description

Interface

tunnel10 (Tunnel10)

Protocol

☒ IPv4 ☐ IPv6

Networks

+

remote-vpn-network

Gateway

vpn-gateway

Metric

1

SLA Monitor

Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

Configure Static Route

Step 14. Navigate to **Deploy**. Review the changes then click on **Deploy Now**.



Pending Changes
? ×

✓ **Last Deployment Completed Successfully**  
26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)	Pending Version <span>LEGEND</span>																												
<div> + Static Route Added: <i>vti-route</i> </div> <table> <tr><td>-</td><td>metricValue: 1</td></tr> <tr><td>-</td><td>ipType: IPv4</td></tr> <tr><td>-</td><td>name: vti-route</td></tr> <tr><td>iface:</td><td></td></tr> <tr><td>-</td><td>tunnel10</td></tr> <tr><td>gateway:</td><td></td></tr> <tr><td>-</td><td>vpn-gateway</td></tr> <tr><td>networks:</td><td></td></tr> <tr><td>-</td><td>remote-vpn-network</td></tr> </table>		-	metricValue: 1	-	ipType: IPv4	-	name: vti-route	iface:		-	tunnel10	gateway:		-	vpn-gateway	networks:		-	remote-vpn-network										
-	metricValue: 1																												
-	ipType: IPv4																												
-	name: vti-route																												
iface:																													
-	tunnel10																												
gateway:																													
-	vpn-gateway																												
networks:																													
-	remote-vpn-network																												
<div> + Access Rule Added: <i>vti-acl</i> </div> <table> <tr><td>-</td><td>logFiles: false</td></tr> <tr><td>-</td><td>eventLogAction: LOG_NONE</td></tr> <tr><td>-</td><td>ruleId: 268435458</td></tr> <tr><td>-</td><td>name: vti-acl</td></tr> <tr><td>sourceZones:</td><td></td></tr> <tr><td>-</td><td>vti-zone</td></tr> <tr><td>-</td><td>inside_zone</td></tr> <tr><td>destinationZones:</td><td></td></tr> <tr><td>-</td><td>vti-zone</td></tr> <tr><td>-</td><td>inside_zone</td></tr> <tr><td>sourceNetworks:</td><td></td></tr> <tr><td>-</td><td>remote-vpn-network</td></tr> <tr><td>-</td><td>inside-network</td></tr> <tr><td>destinationNetworks:</td><td></td></tr> </table>		-	logFiles: false	-	eventLogAction: LOG_NONE	-	ruleId: 268435458	-	name: vti-acl	sourceZones:		-	vti-zone	-	inside_zone	destinationZones:		-	vti-zone	-	inside_zone	sourceNetworks:		-	remote-vpn-network	-	inside-network	destinationNetworks:	
-	logFiles: false																												
-	eventLogAction: LOG_NONE																												
-	ruleId: 268435458																												
-	name: vti-acl																												
sourceZones:																													
-	vti-zone																												
-	inside_zone																												
destinationZones:																													
-	vti-zone																												
-	inside_zone																												
sourceNetworks:																													
-	remote-vpn-network																												
-	inside-network																												
destinationNetworks:																													

MORE ACTIONS ▼

CANCEL

DEPLOY NOW ▼

Deploy the Config

## Verify

Once the deployment is complete, you can verify the tunnel status on CLI by using commands:

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>



```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	Status	Role
3294213359	10.106.52.222/500	10.106.63.23/500	READY	INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/141 sec				
Child sa:	local selector 0.0.0.0/0 - 255.255.255.255/65535			
	remote selector 0.0.0.0/0 - 255.255.255.255/65535			
	ESP spi in/out: 0x26a14554/0xd5db88bc			

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
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: 10.106.63.23
```

*Show Commands*

## Related Information

For further information regarding Site-to-Site VPNs on the FTD managed by FDM, you can find the full configuration guide here:

[FTD Managed by FDM Configuration Guide](#)