

Configure VRF Aware Route-Based Site-to-Site VPN on FTD Managed by FDM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configure the FTD](#)

[Configure the ASA](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure VRF-aware route-based site-to-site VPN on FTD managed by FDM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Virtual Private Networks (VPN)
- Basic understanding of Virtual Routing and Forwarding (VRF)
- Experience with Firepower Device Manager (FDM)

Components Used

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

- Cisco FTdV version 7.4.2
- Cisco FDM version 7.4.2
- Cisco ASA v9.20.3

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.

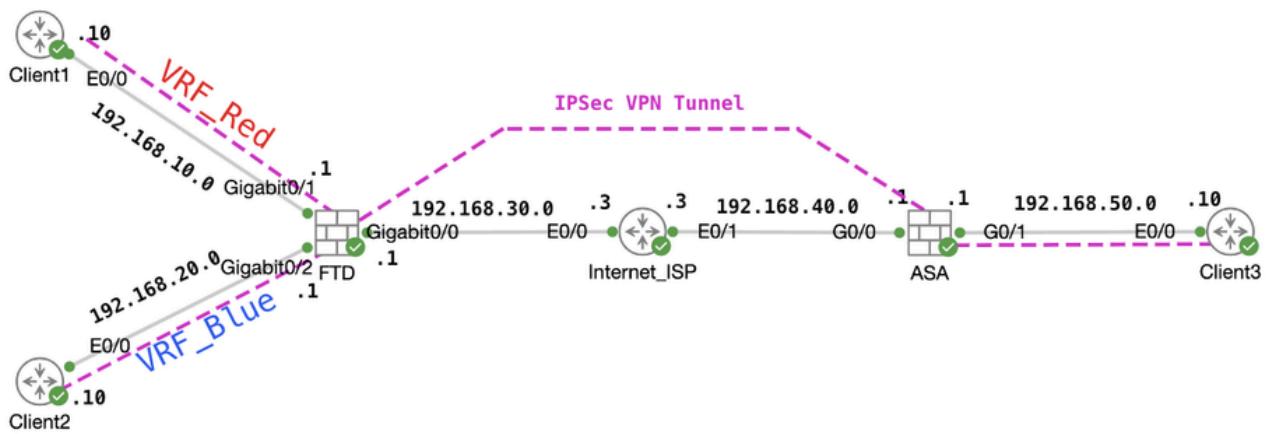
Background Information

VRF on FDM allows you to create multiple isolated routing instances on a single Firepower Threat Defense (FTD) device. Each VRF instance operates as a separate virtual router with its routing table, enabling logical separation of network traffic and providing enhanced security and traffic management capabilities.

This document explains how to configure VRF-aware IPSec VPN with VTI. VRF Red network and VRF Blue network are behind FTD. Client1 in VRF Red network and Client2 in VRF Blue would communicate with Client3 behind ASA through the IPSec VPN tunnel.

Configure

Network Diagram



Topology

Configure the FTD

Step 1. It is essential to ensure that the preliminary configuration of IP interconnectivity between nodes has been completed. Client1 and Client2 have FTD inside IP addresses as gateways. Client3 is with ASA inside the IP address as a gateway.

Step 2. Create a virtual tunnel interface. Login the FDM GUI of FTD. Navigate to **Device > Interfaces**. Click **View All Interfaces**.

FTD_View_Interfaces

Step 2.1. Navigate to the **Virtual Tunnel Interfaces** tab and click the **+** button.

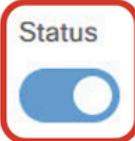
FTD_Create_VTI

Step 2.2. Provide the necessary information and click the **OK** button.

- Name: demovti
- Tunnel ID: 1
- Tunnel Source: outside (GigabitEthernet0/0)
- IP Address And Subnet Mask: 169.254.10.1/24
- Status: click the slider to the Enabled position

Name

Status



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

Description

Tunnel ID 

Tunnel Source 

outside (GigabitEthernet0/0)

▼

IP Address and Subnet Mask

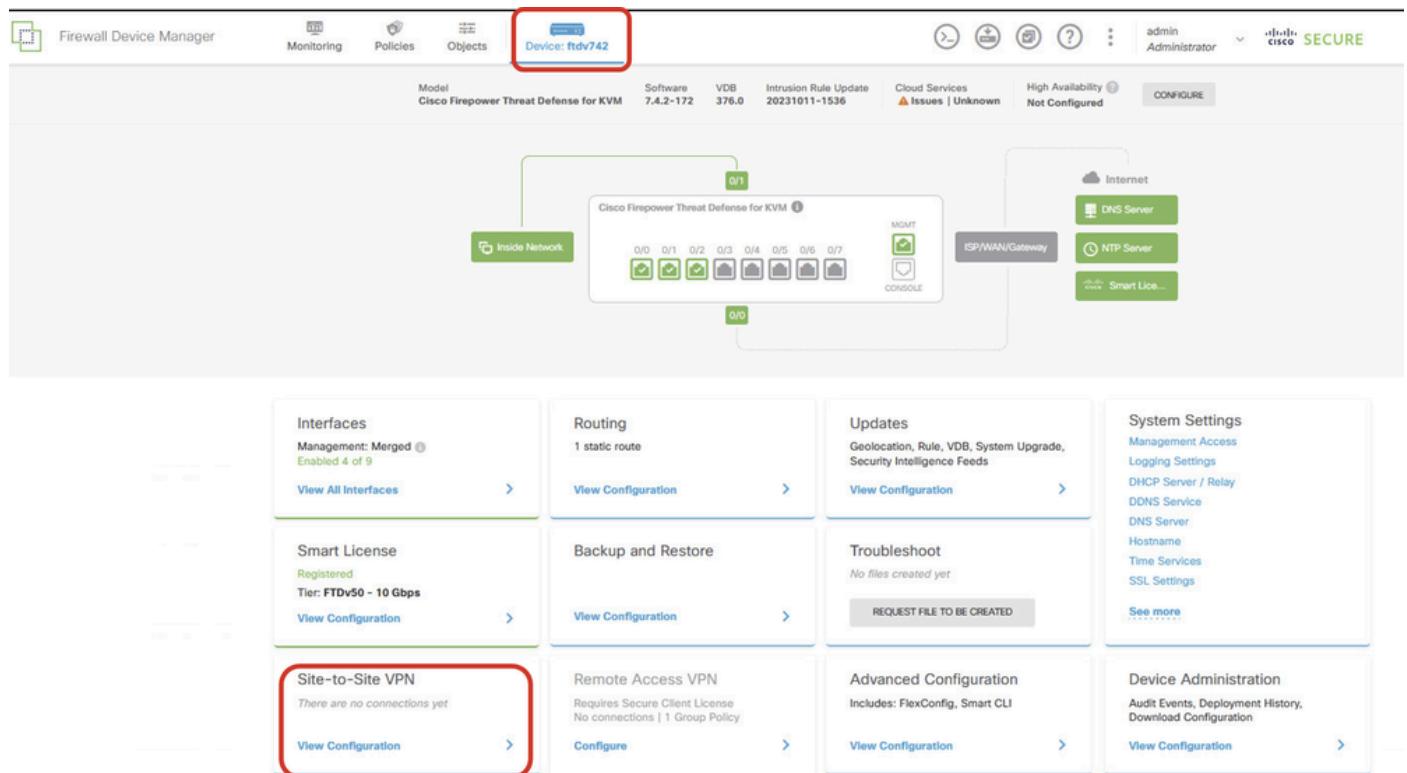
/

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL
OK

FTD_Create_VTI_Details

Step 3. Navigate to **Device > Site-to-Site VPN**. Click the **View Configuration** button.



The screenshot shows the Cisco Firepower Device Manager interface. At the top, the device name "ftd742" is highlighted with a red box. Below the header, there's a network diagram showing the device connected to an "Inside Network" and an "Internet" connection through an "ISP/WAN/Gateway".

The main content area contains several configuration sections:

- Interfaces**: Management: Merged 4 of 9. [View All Interfaces](#)
- Smart License**: Registered, Tier: FTDv50 - 10 Gbps. [View Configuration](#)
- Site-to-Site VPN**: There are no connections yet. [View Configuration](#) (highlighted with a red box)
- Routing**: 1 static route. [View Configuration](#)
- Backup and Restore**: [View Configuration](#)
- Remote Access VPN**: Requires Secure Client License. No connections | 1 Group Policy. [Configure](#)
- Updates**: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. [View Configuration](#)
- Troubleshoot**: No files created yet. [REQUEST FILE TO BE CREATED](#)
- Advanced Configuration**: Includes: FlexConfig, Smart CLI. [View Configuration](#)
- System Settings**: Management Access, Logging Settings, DHCP Server / Relay, DDNS Service, DNS Server, Hostname, Time Services, SSL Settings. [See more](#)
- Device Administration**: Audit Events, Deployment History, Download Configuration. [View Configuration](#)

FTD_Site-to-Site_VPN_View_Configurations

Step 3.1. Start to create a new site-to-site VPN. Click the **CREATE SITE-TO-SITE CONNECTION** or the + button.

The screenshot shows the 'Device Summary' section for 'Site-to-Site VPN'. At the top, there are tabs for Monitoring, Policies, Objects, and Device (ftdv742). On the right, it shows the user 'admin' with 'Administrator' privileges and a 'Cisco SECURE' status. Below the tabs, there's a search bar with 'Filter' and 'Preset filters: Route Based (VTI), Policy Based'. A table header includes columns for #, NAME, TYPE, LOCAL INTERFACES, LOCAL NETWORKS, REMOTE NETWORKS, NAT EXEMPT, IKE V1, IKE V2, and ACTIONS. A message states 'There are no Site-to-Site connections yet.' followed by 'Start by creating the first Site-to-Site connection.' A blue 'CREATE SITE-TO-SITE CONNECTION' button is highlighted with a red box.

FTD_Create_Site2Site_Connection

Step 3.2. Provide the necessary information and click **NEXT**.

- Connection Profile Name: Demo_S2S
- Type: Route Based (VTI)
- Local VPN Access Interface: demovti (created in Step 2)
- Remote IP Address: 192.168.40.1 (this is peer ASA outside IP address)

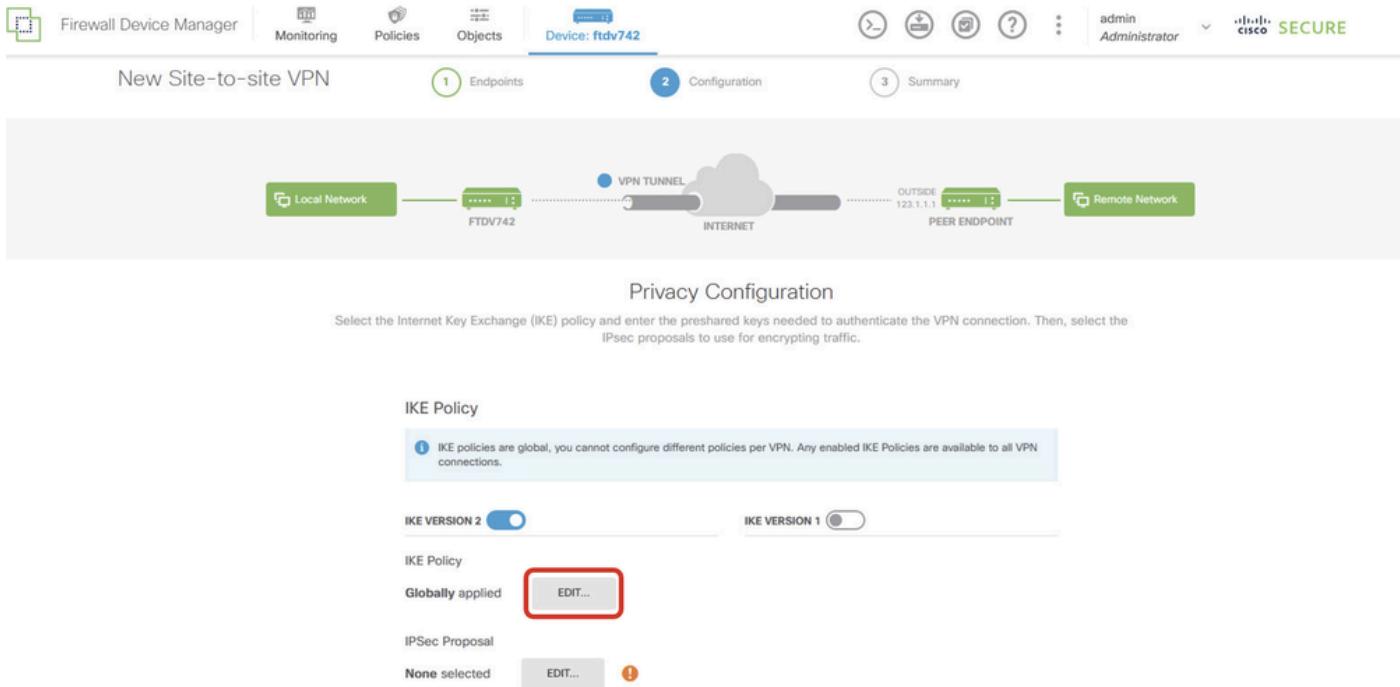
The screenshot shows the 'New Site-to-site VPN' configuration wizard at Step 1: Endpoints. It displays a network diagram with nodes: Local Network, FTDV742, INTERNET, OUTSIDE INTERFACE, and Remote Network. A 'VPN TUNNEL' connects FTDV742 to the INTERNET, and another connects the INTERNET to the OUTSIDE INTERFACE. Below the diagram, the 'Define Endpoints' section asks to identify local and remote interfaces and networks. Configuration fields include:

- Connection Profile Name: Demo_S2S
- Type: Route Based (VTI) (highlighted with a red box)
- LOCAL SITE: Local VPN Access Interface: demovti (Tunnel1) (highlighted with a red box)
- REMOTE SITE: Remote IP Address: 192.168.40.1 (highlighted with a red box)

At the bottom, there are 'CANCEL' and 'NEXT' buttons, with 'NEXT' highlighted with a red box.

FTD_Site-to-Site_VPN_Endpoints

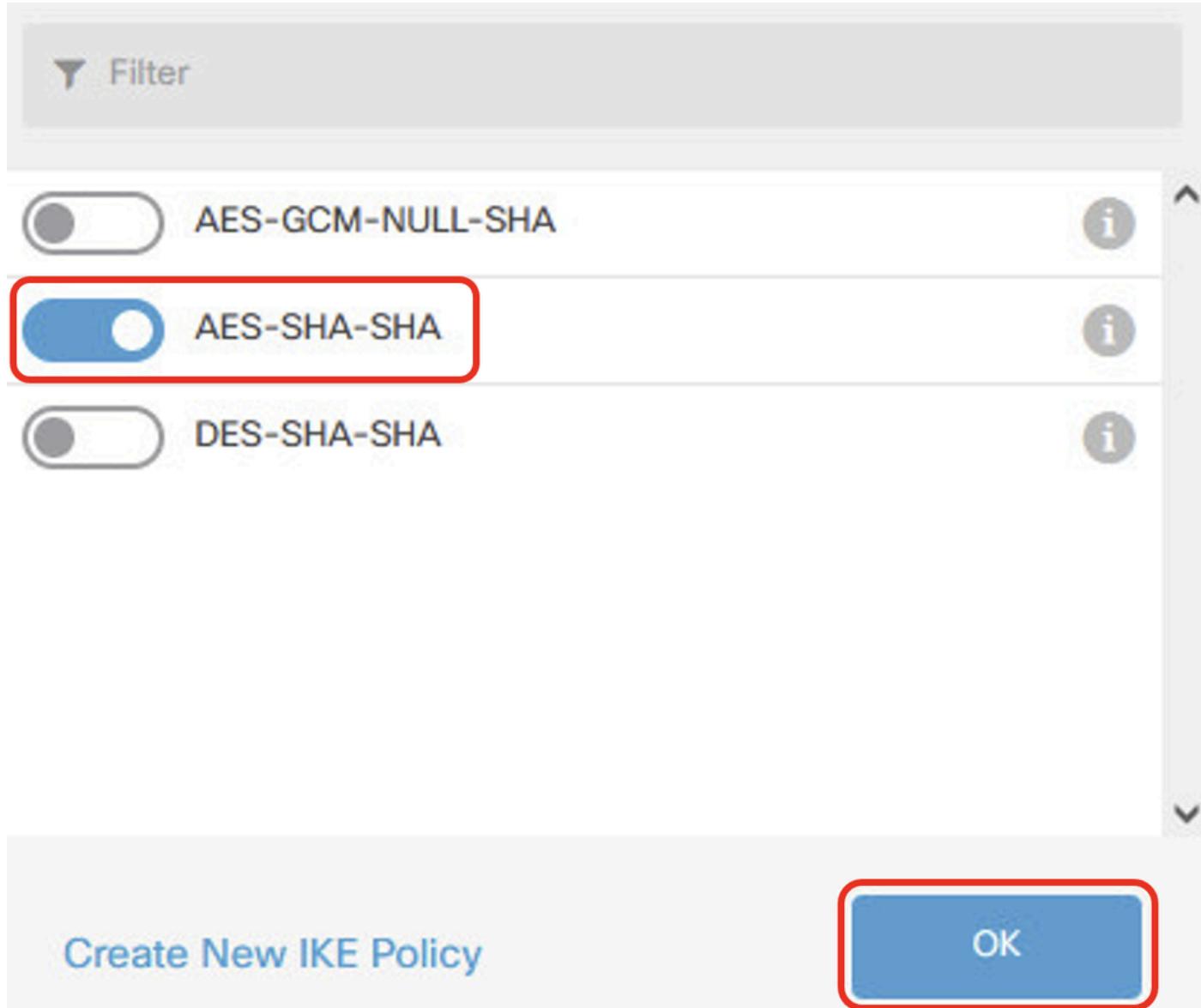
Step 3.3. Navigate to IKE Policy. Click the **EDIT** button.



FTD_Edit_IKE_Policy

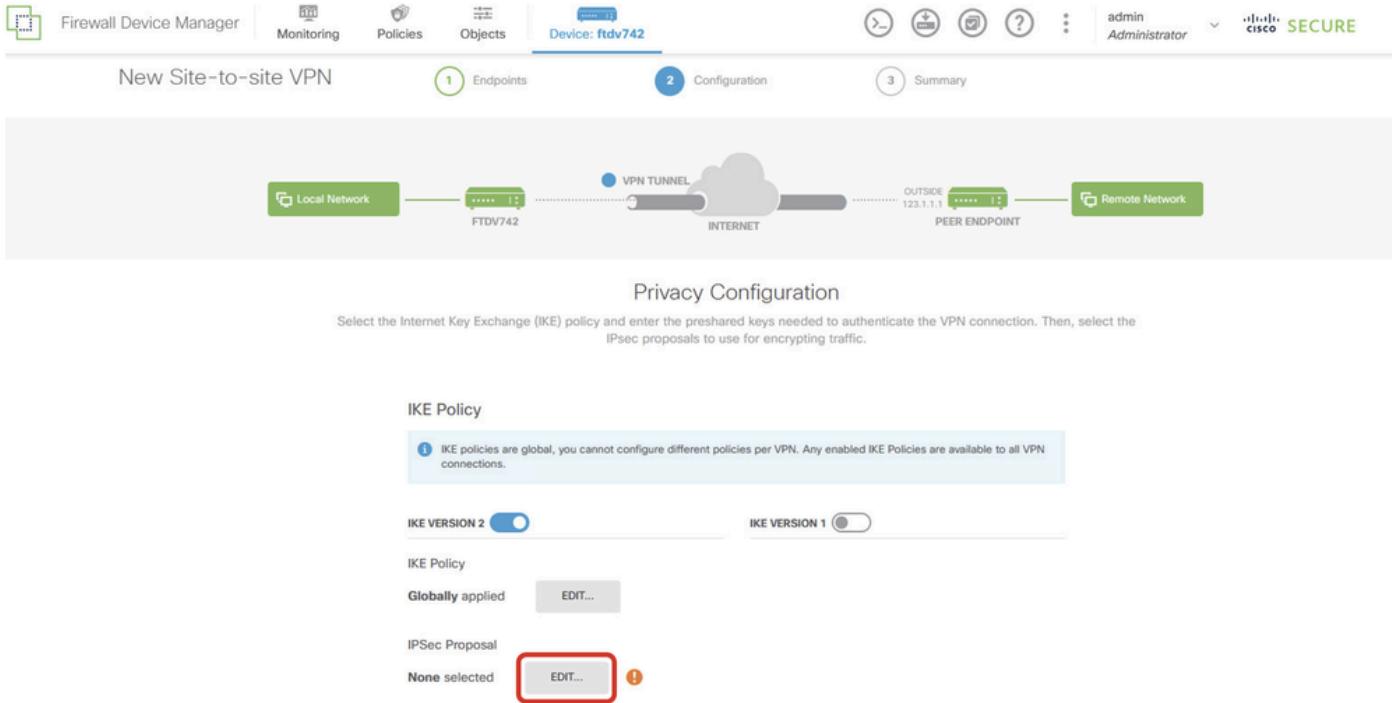
Step 3.4. For the IKE policy, you can use a pre-defined or you can create a new one by clicking **Create New IKE Policy**.

In this example, toggle an existing IKE policy name **AES-SHA-SHA**. Click the **OK** button in order to save.



FTD_Enable_IKE_Policy

Step 3.5. Navigate to IPSec Proposal. Click the **EDIT** button.



FTD_Edit_IPSec_Proposal

Step 3.6. For the IPsec proposal, you can use a pre-defined or you can create a new one by clicking **Create new IPsec Proposal**.

In this example, toggle an existing IPsec Proposal name **AES-SHA**. Click the **OK** button to save.

Select IPSec Proposals



The screenshot shows a list of IPSec proposals. The 'AES-SHA' proposal is selected, indicated by a checked checkbox and a blue background. Other proposals listed are 'AES-GCM in Default Set' and 'DES-SHA-1'. At the bottom left is a 'Create new IPSec Proposal' link. On the right are 'CANCEL' and 'OK' buttons, with 'OK' being highlighted with a red box.

Proposal	Status
AES-GCM in Default Set	In Default Set
AES-SHA	Selected
DES-SHA-1	Available

FTD_Enable_IPSec_Proposal

Step 3.7. Scroll down the page and configure the pre-shared key. Click **NEXT** button.

Note down this pre-shared key and configure it on ASA later.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | FTDV742 | INTERNET | PEER ENDPOINT | admin Administrator | Cisco SECUR|

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

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 EDIT...

IPSec Proposal
Custom set selected EDIT...

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

BACK NEXT

FTD_Configure_Pre_Shared_Key

Step 3.8. Review the VPN configuration. If anything needs to be modified, click the **BACK** button. If everything is good, click the **FINISH** button.

Demo_S2S Connection Profile

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

VPN Access Interface	demovti (169.254.10.1)	Peer IP Address	192.168.40.1
IKE V2			
IKE Policy	aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14		
IPSec Proposal	aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1		
Authentication Type	Pre-shared Manual Key		
IKE V1: DISABLED			
IPSEC SETTINGS			
Lifetime Duration	28800 seconds		
Lifetime Size	4608000 kilobytes		
ADDITIONAL OPTIONS			
<p>i 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.</p> <p>Diffie-Hellman Group: Null (not selected)</p>			
BACK	FINISH		

FTD_Review_VPN_Configuration

Step 3.9. Create an Access Control rule in order to allow traffic to pass through the FTD. In this example, allow all for demo purposes. Modify your policy based on your actual needs.

#	NAME	ACTION	SOURCE ZONES	NETWORKS	PORTS	DESTINATION ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
> 1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Edit Delete

FTD_ACP_Example

Step 3.10. (Optional) Configure NAT exempt rule for the client traffic on FTD if there is dynamic NAT configured for the client to access the internet. In this example, there is no need to configure a NAT-exempt rule because there is no dynamic NAT configured on FTD.

Step 3.11. Deploy the configuration changes.



FTD_Deployment_Changes

Step 4. Configure virtual routers.

Step 4.1. Create network objects for static routes. Navigate to **Objects > Networks** and click the + button.



FTD_Create_NetObjects

Step 4.2. Provide necessary information on each network object. Click the **OK** button.

- Name: local_blue_192.168.20.0
- Type: Network
- Network: 192.168.20.0/24

Add Network Object



Name

local_blue_192.168.20.0

Description

Type

Network

Host

Network

192.168.20.0/24

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

CANCEL

OK

FTD_VRF_Blue_Network

- Name: local_red_192.168.10.0
- Type: Network
- Network: 192.168.10.0/24

Add Network Object



Name

local_red_192.168.10.0

Description

Type

Network

Host

Network

192.168.10.0/24

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

CANCEL

OK

FTD_VRF_Red_Network

- Name: remote_192.168.50.0
- Type: Network
- Network: 192.168.50.0/24

Add Network Object



Name

remote_192.168.50.0

Description

Type

Network

Host

FQDN

Range

Network

192.168.50.0/24

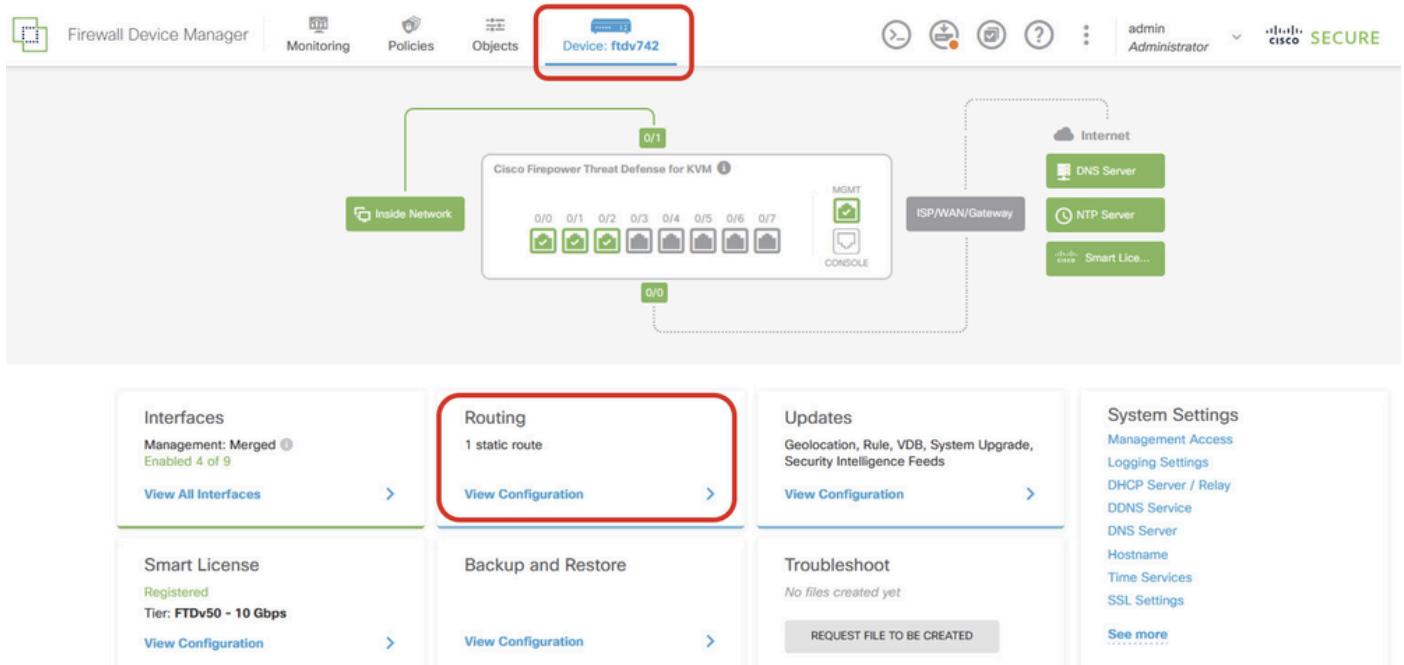
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

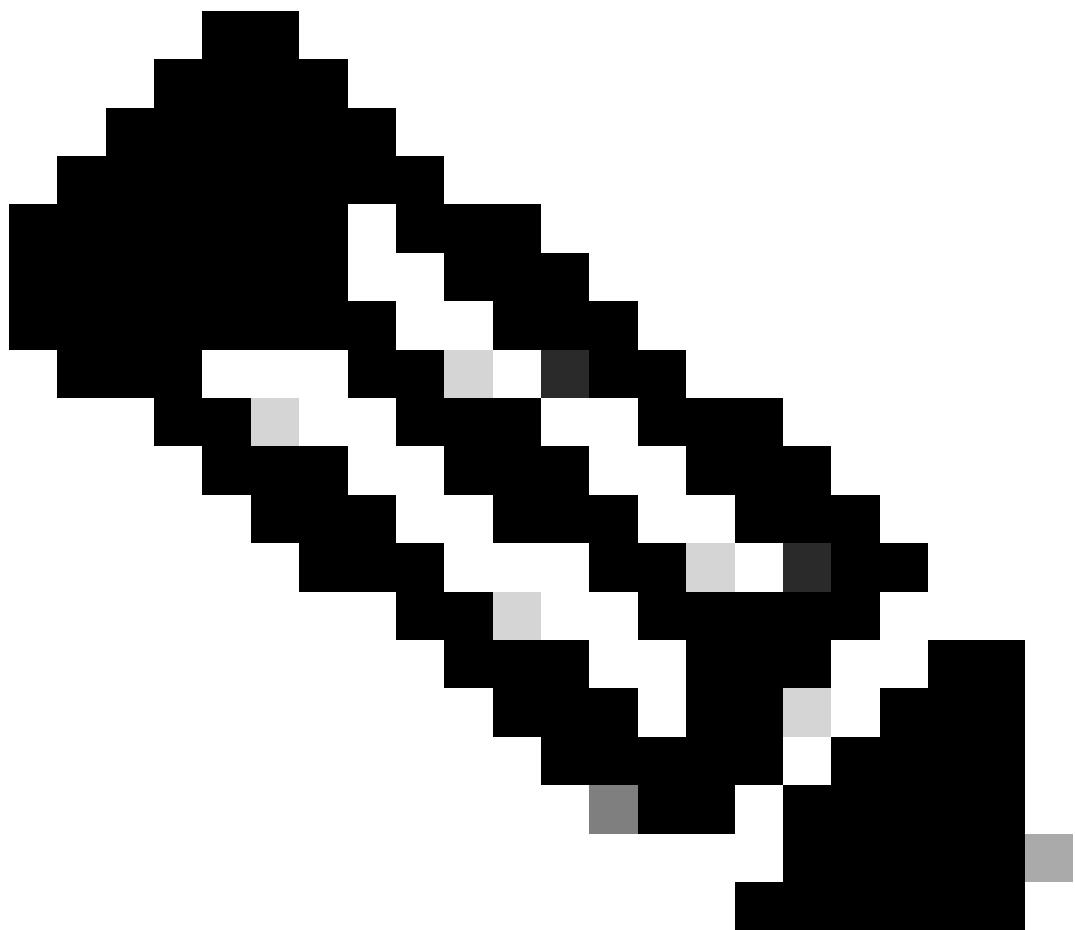
FTD_Remote_Network

Step 4.3. Create the first virtual router. Navigate to **Device > Routing** and click **View Configuration**.



FTD_View_Routing_Configuration

Step 4.4. Click **Add Multiple Virtual Routers**.



Note: A static route through an outside interface has already been configured during FDM initialization. If you do not have it, configure it manually.

Screenshot of the Firewall Device Manager (FDM) interface showing the configuration of a static route.

The top navigation bar includes links for Firewall Device Manager, Monitoring, Policies, Objects, and the currently selected "Device: ftdv742". It also shows the user is logged in as "admin Administrator".

The main area displays the "Device Summary" and "Routing" section. A red box highlights the "Add Multiple Virtual Routers" button.

The "Static Routing" tab is selected, showing one route entry:

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3	

A red box highlights the first row of the table, corresponding to the "StaticRoute_IPv4" entry.

FTD_Add_First_Virtual_Router

Step 4.5. Click **CREATE FIRST CUSTOM VIRTUAL ROUTER**.

The screenshot shows the Firewall Device Manager interface. At the top, there are tabs for Monitoring, Policies, Objects, and a selected 'Device: ftdv742'. On the left, under 'Routing', there's a 'Virtual Route Forwarding (Virtual Routing) Description' section. To the right, a diagram titled 'How Multiple Virtual Routers Work' illustrates a 'THREAT DEFENSE' system with multiple virtual routers (A, B, N) handling traffic from various customer networks (A, B, N). A red box highlights the 'CREATE FIRST CUSTOM VIRTUAL ROUTER' button at the bottom of the diagram area.

FTD_Add_First_Virtual_Router2

Step 4.6. Provide necessary information on the first virtual router. Click the **OK** button. After the first virtual router creation, a VRF name **Global** is shown automatically.

- Name: vrf_red
- Interfaces: inside_red (GigabitEthernet0/1)

The screenshot shows the 'Add Virtual Router' dialog box over a blurred background of the Firewall Device Manager interface. The dialog has fields for 'Name' (set to 'vrf_red') and 'Interfaces' (set to 'inside_red (GigabitEthernet0/1)'). Both the 'Name' and 'Interfaces' fields are highlighted with red boxes. The 'OK' button at the bottom right is also highlighted with a red box.

FTD_Add_First_Virtual_Router3

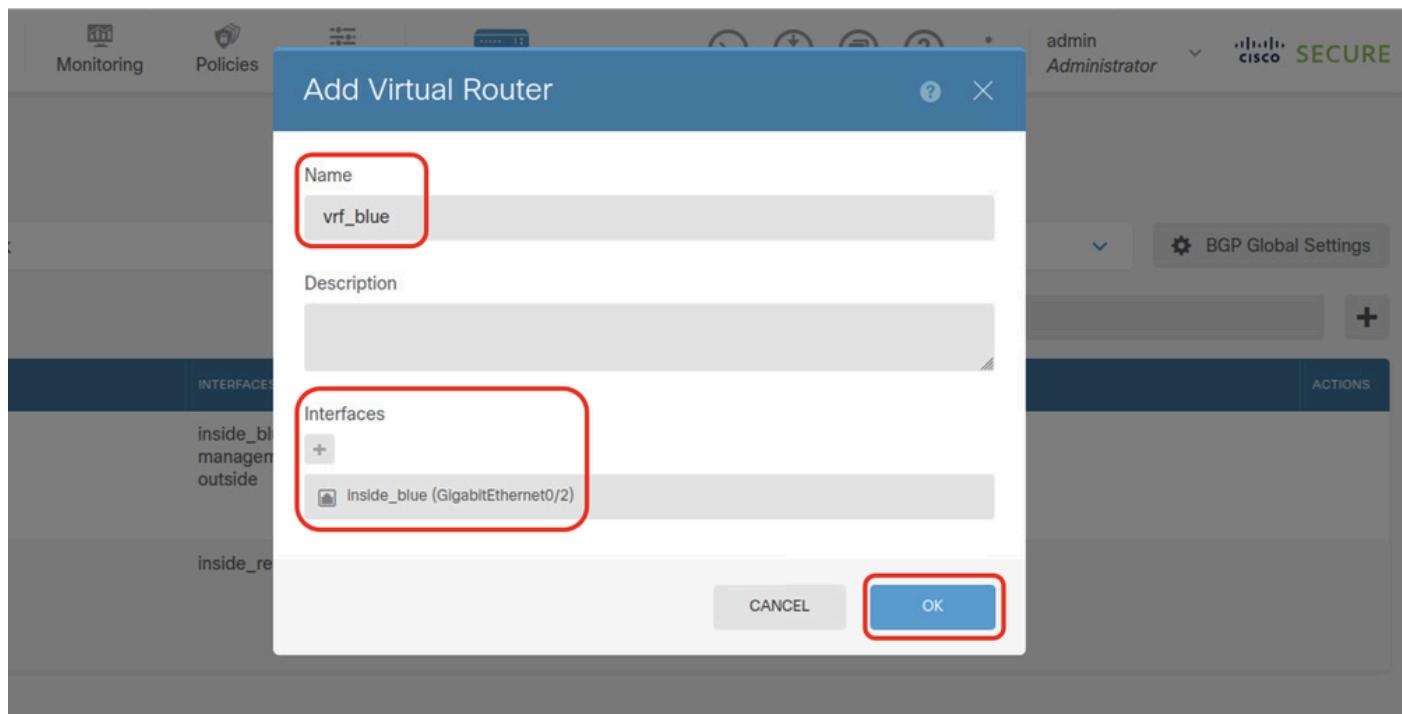
Step 4.7. Create a second virtual router. Navigate to **Device > Routing**. Click **View Configuration** and then the **+** button.



FTD_Add_Second_Virtual_Router

Step 4.8. Provide necessary information on the second virtual router. Click the **OK** button.

- Name: vrf_blue
- Interfaces: inside_blue (GigabitEthernet0/2)



FTD_Add_Second_Virtual_Router2

Step 5. Create route leak from vrf_blue to Global. This route allows endpoints on the 192.168.20.0/24 network to initiate connections that traverse the site-to-site VPN tunnel. For this example, the remote endpoint is protecting the 192.168.50.0/24 network.

Navigate to **Device > Routing**. Click **View Configuration** and then the **View** icon in the Action cell for the virtual router vrf_blue.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work

BGP Global Settings

3 virtual routers

NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1 Global	management outside	> Routes > Ipv6 routes > BGP > OSPF	
2 vrf_blue	inside_blue	> Routes > Ipv6 routes > BGP > OSPF	Edit View
3 vrf_red	inside_red	> Routes > Ipv6 routes > BGP > OSPF	

FTD_View_VRF_Blue

Step 5.1. Click the **Static Routing** tab and then the + button.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work

Virtual Router Properties **Static Routing** BGP OSPF ECMP Traffic Zones

Commands

+ Filter

FTD_Create_Static_Route_VRF_Blue

Step 5.2. Provide necessary information. Click the **OK** button.

- Name: Blue_toASA
- Interface: demovti (Tunnel1)
- Networks: remote_192.168.50.0
- Gateway: Leave this item blank.

Name
Blue_to ASA|

Description

Interface
demovti (Tunnel1)

Belongs to current Router
N/A

Protocol
 IPv4 IPv6

Networks
+
remote_192.168.50.0

Gateway
Please select a gateway

Metric
1

SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor

CANCEL OK

FTD_Create_Static_Route_VRF_Blue_Details

Step 6. Create route leak from vrf_red to Global. This route allows endpoints on the 192.168.10.0/24 network to initiate connections that traverse the site-to-site VPN tunnel. For this example, the remote endpoint is protecting the 192.168.50.0/24 network.

Navigate to **Device > Routing**, click **View Configuration**, and then the **View** icon in the Action cell for the virtual router vrf_red.

The screenshot shows the 'Virtual Routers' table in the Firewall Device Manager. There are three entries:

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management, outside	> Routes > IPv6 routes > BGP > OSPF	
2	vrf_blue	inside_blue	> Routes > IPv6 routes > BGP > OSPF	
3	vrf_red	inside_red	> Routes > IPv6 routes > BGP > OSPF	

FTD_View_VRF_Red

Step 6.1. Click the **Static Routing** tab and then the **+** button.

The screenshot shows the 'Virtual Router Properties' screen for 'vrf_red'. The 'Static Routing' tab is selected, and the '+' button in the top right corner is highlighted with a red box.

FTD_Create_Static_Route_VRF_Red

Step 6.2. Provide the necessary information and click the **OK** button.

- Name: Red_toASA
- Interface: demovti (Tunnel1)
- Networks: remote_192.168.50.0
- Gateway: Leave this item blank.

vrf_red

Add Static Route



Name

Red_to ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol

IPv4

IPv6

Networks



remote_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

FTD_Create_Static_Route_VRF_Red_Details

Step 7. Create route leak from Global to virtual routers. The routes allow endpoints protected by the remote end of the site-to-site VPN to access the 192.168.10.0/24 network in the vrf_red virtual router and

192.168.20.0/24 network in the vrf_blue virtual router.

Navigate to **Device > Routing**, click **View Configuration**, and then click the **View** icon in the Action cell for the Global virtual router.

The screenshot shows the Firewall Device Manager interface with the 'Virtual Routers' tab selected. There are three virtual routers listed: 'Global', 'vrf_blue', and 'vrf_red'. The 'Global' router is highlighted. In the 'Actions' column for the Global router, there is a 'View' button and a 'Edit' button, both of which are highlighted with red boxes. The 'Edit' button is located at the bottom right of the row.

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	>- Routes >- IPv6 routes >- BGP >- OSPF	
2	vrf_blue	inside_blue	>- Routes >- IPv6 routes >- BGP >- OSPF	
3	vrf_red	inside_red	>- Routes >- IPv6 routes >- BGP >- OSPF	

FTD_View_VRF_Global

Step 7.1. Click the **Static Routing** tab and then the **+** button.

The screenshot shows the 'Virtual Router Properties' screen for the 'Global' router. The 'Static Routing' tab is selected. At the bottom right of the table, there is a large red-bordered '+' button, which is the 'Add New' button for creating a static route. The table header includes columns for NAME, INTERFACE, IP TYPE, NETWORKS, GATEWAY IP, SLA MONITOR, METRIC, and ACTIONS.

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

FTD_Create_Static_Route_VRF_Global

Step 7.2. Provide the necessary information and click **OK**.

- Name: S2S_leak_blue
- Interface: inside_blue (GigabitEthernet0/2)
- Networks: local_blue_192.168.20.0
- Gateway: Leave this item blank.

Global

Add Static Route



Name

S2S_leak_blue

Description

⚠ The selected Interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside_blue (GigabitEthernet0/2)

Belongs to different Router



vrf_blue

Protocol

IPv4

IPv6

Networks



local_blue_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

```
encryption aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
group 21 20 16 15 14
prf sha512 sha384 sha256 sha
lifetime seconds 86400
```

Step 10. Create an IKEv2 ipsec-proposal that defines the same parameters configured on the FTD.

```
<#root>

crypto ipsec ikev2 ipsec-proposal

AES-SHA

protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

Step 11. Create an ipsec profile, referencing ipsec-proposal created in Step 10.

```
<#root>

crypto ipsec profile

demo_ipsec_profile

set ikev2 ipsec-proposal

AES-SHA

set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800
```

Step 12. Create a group policy allowing the IKEv2 protocol.

```
<#root>

group-policy

demo_gp_192.168.30.1

internal
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

Step 13. Create a tunnel group for the peer FTD outside the IP address, referencing the group policy created in Step 12. and configuring the same pre-shared-key with FTD (created in Step 3.7).

```
<#root>
```

```
tunnel-group 192.168.30.1 type ipsec-l2l  
tunnel-group 192.168.30.1 general-attributes  
  default-group-policy  
  
demo_gp_192.168.30.1
```

```
tunnel-group 192.168.30.1 ipsec-attributes  
  ikev2 remote-authentication pre-shared-key *****  
  ikev2 local-authentication pre-shared-key *****
```

Step 14. Enable IKEv2 on the outside interface.

```
crypto ikev2 enable outside
```

Step 15. Create a virtual tunnel.

```
<#root>  
  
interface Tunnel1  
  nameif demovti_asa  
  ip address 169.254.10.2 255.255.255.0  
  tunnel source interface outside  
  tunnel destination 192.168.30.1  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile  
  
demo_ipsec_profile
```

Step 16. Create a static route.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1  
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1  
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Navigate to the CLI of FTD and ASA via console or SSH in order to verify the VPN status of phase 1 and phase 2 through the commands **show crypto ikev2 sa** and **show crypto ipsec sa**.

FTD:

```
> system support diagnostic-cli
```

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

```
ftdv742#  
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id Local	Remote
32157565 192.168.30.1/500	192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83	

```
ftdv742# show crypto ipsec sa
```

interface: demovti

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1
```

```
Protected vrf (ivrf): Global  
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: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30  
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 30, #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.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500  
path mtu 1500, ipsec overhead 94(44), media mtu 1500  
PMTU time remaining (sec): 0, DF policy: copy-df  
ICMP error validation: disabled, TFC packets: disabled  
current outbound spi: A493CC83  
current inbound spi : 4CF55637
```

inbound esp sas:

```
spi: 0x4CF55637 (1291146807)  
SA State: active  
transform: esp-aes-256 esp-sha-512-hmac no compression  
in use settings ={L2L, Tunnel, IKEv2, VTI, }  
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1  
sa timing: remaining key lifetime (kB/sec): (4055040/16867)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
    0x00000000 0x00000001
```

outbound esp sas:

```
spi: 0xA493CC83 (2761149571)  
SA State: active  
transform: esp-aes-256 esp-sha-512-hmac no compression  
in use settings ={L2L, Tunnel, IKEv2, VTI, }  
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
```

```
sa timing: remaining key lifetime (kB/sec): (4285440/16867)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id Local	Remote
26025779 192.168.40.1/500	192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637	

```
ASA9203#
```

```
ASA9203# show cry
```

```
ASA9203# show crypto ipsec sa
```

```
interface: demovti_asa
```

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
```

```
Protected vrf (ivrf): Global
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: 192.168.30.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #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.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 4CF55637
current inbound spi : A493CC83
```

```
inbound esp sas:
```

```
spi: 0xA493CC83 (2761149571)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4101120/16804)
IV size: 16 bytes
```

```

replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
outbound esp sas:
 spi: 0x4CF55637 (1291146807)
 SA State: active
 transform: esp-aes-256 esp-sha-512-hmac no compression
 in use settings ={L2L, Tunnel, IKEv2, VTI, }
 slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
 sa timing: remaining key lifetime (kB/sec): (4055040/16804)
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001

```

Step 2. Verify the route of VRF and Global on FTD.

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 192.168.30.3 to network 0.0.0.0

```

S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti
L       169.254.10.1 255.255.255.255 is directly connected, demovti
SI      192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI      192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C       192.168.30.0 255.255.255.0 is directly connected, outside
L       192.168.30.1 255.255.255.255 is directly connected, outside

```

ftdv742# show route vrf vrf_blue

Routing Table: vrf_blue

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

```

C       192.168.20.0 255.255.255.0 is directly connected, inside_blue
L       192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI      192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti

```

ftdv742# show route vrf vrf_red

```
Routing Table: vrf_red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, + - replicated route
      SI - Static InterVRF, BI - BGP InterVRF
```

Gateway of last resort is not set

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

Step 3. Verify ping test.

Before ping, check the counters of **show crypto ipsec sa | inc interface:|encap|decap** on FTD.

In this example, Tunnel1 shows 30 packets for both encapsulation and decapsulation.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
  #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
  #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 ping Client3 successfully.

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

Client2 ping Client3 successfully.

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

Check the counters of **show crypto ipsec sa | inc interface:|encap|decap** on FTD after ping successfully.

In this example, Tunnel1 shows 40 packets for both encapsulation and decapsulation after a successful ping. Additionally, both counters increased by 10 packets, matching the 10 ping echo requests, indicating that the ping traffic successfully passed through the IPSec tunnel.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
#pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
#pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

You can use those debug commands to troubleshoot the VPN section.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

You can use those debug commands in order to troubleshoot the route section.

```
debug ip routing
```

Related Information

- [Cisco Secure Firewall Device Manager Configuration Guide, Version 7.4](#)
- [Cisco Secure Firewall ASA VPN CLI Configuration Guide, 9.20](#)
- [Cisco Technical Support & Downloads](#)