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

### Contents

ntroduction
Prerequisites
Requirements
Components Used
Background Information
Limitations and Restrictions
Configuration Steps on FMC
/erify
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 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. 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 <u>Configure DVTI with Multi-SA on Secure Firewall</u>.

#### **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**.

Overview Analysis	Policies	Devic	es Obj	ects	AMP Int	elligence		
<b>Device Management</b>	NAT	VPN 🔻	QoS	Pla	form Settings	FlexConfig	Certificates	
		Site To S	Site					
View By : Group	į	Remote Troubles	Access	D)	Warning (0)	Offline (0)   N	ormal (1)   Dep	loymer

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

Topology Name:*	VTI-ASA				
	O Policy Based (Crypto Map)   Route Based (VTI)				
Network Topology:	← Point to Point				
IKE Version:*	🗌 IKEv1 🗹 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.

Endpoints	IKE	IPsec	Advanced			
	Node A		.	Node B		
Device:*			D	evice:*		
FTD		~		Empty	*	]
Virtual Tu	unnel Interface:*			irtual Tunnel Interface:*		
Tunnel	Source IP is Private	Edit VI		Empty Tunnel Source IP is Private	Edit VT	
Connecti	on Type:*			connection Type:*		
Bidirectio	nal	~	E	Bidirectional	*	
Tunnel IF Tunnel S Tunnel S	Address ource Interface ource Interface IP	:	T T	unnel IP Address unnel Source Interface unnel Source Interface IP	:	

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)

k.T	Add Virtual Tunnel Inte	Point   *** Hub and Snake   *** Full Mach   erface	? ×
rs	General		
	Name *:	VTI-ASA	C Enabled
	Description:	VTI Tunnel with Extranet ASA	
F	Security Zone:	VTI-Zone 🗸	
Vi	Tunnel ID *:	1	Range: 0 - 10413
E	IP Address *:	192.168.100.1/30	0
~	Tunnel Source *:	GigabitEthernet0/0 (Outside)	
в			
Γι			
			OK Cancel

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

16	Create New VPN Topo	ology		? ×
	Topology Name:*	VTI-ASA	pto Map) 💿 Route E	Based (VTI)
	Network Topology: IKE Version:*	⊷ Point to Point     IKEv1    IKEv2	Hub and Spoke	e 💠 Full Mesh
	Endpoints IKE No Device:* FTD Virtual Tunnel Inte VTI-ASA U Tunnel Source IP Connection Type:* Bidirectional Tunnel IP Address Tunnel Source Inte Tunnel Source Inte Additional Configur Route traffic to the Permit VPN traffic	IPsec ode A erface :* Is Private erface IP ration () e VTI : Routin : AC Poin	Advance	ed   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-NULL-S	SHA-LATEST		~	0
Authentication Type:	Pre-shared Auton	natic Key		Y	
Pre-shared Key Length:*	24 Char	acters	(Range 1-12	7)	

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

New IKEv2 Policy			? ×
Name:*	ASA-IKEv2-Policy		
Description: Priority: Lifetime:	1 86400	(1-65535) seconds (120-2147483647)	
Integrity Algorithms	Available Algorithms	Selected Algorithms	
Encryption Algorithms PRF Algorithms Diffie-Hellman Group	Image: Shape of the shape	Add	
		Save	ancel

Step 10. Choose the newly created or the **Policy** that exists.. Select the **Authentication Type**. If a Preshared 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

Endpoints IKE		IPsec	Advanced	
KEv1 Settings				
Policy:*	preshare	d_sha_aes256_dh14	_3 💙	0
Authentication Type:	Pre-share	ed Automatic Key	v	
Pre-shared Key Length:*	24	Characters	(Range 1-127)	
, ,			1	
IKEv2 Settings				
KEv2 Settings Policy:*	ASA-IKE	v2-Policy	~	] 💿
IKEv2 Settings Policy:* Authentication Type:	ASA-IKE	v2-Policy ed Manual Key	~	0
IKEv2 Settings Policy:* Authentication Type: Key:*	ASA-IKE	v2-Policy ed Manual Key	*	] 💿
IKEv2 Settings Policy:* Authentication Type: Key:*	ASA-IKE	v2-Policy ed Manual Key	~	] 💿
IKEv2 Settings Policy:* Authentication Type: Key:* Confirm Key:*	ASA-IKE	v2-Policy ed Manual Key	*	] <b>②</b> ] ]

**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 Editbutton next to the IKEv2 IPsec Proposal tab.

Crypto Map Type:	Static Opynamic	2	
IKEv2 Mode:	Tunnel	~	
Transform Sets:	IKEv1 IPsec Proposals	0	IKEv2 IPsec Proposals* 🥜
	tunnel_aes256_sha		AES-GCM
Enable Security A	ssociation (SA) Strength	Enforcem	ent

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

Name:*				
	ASA-IPSec-Policy			
Description.				
ESP Hash	Available Algorithms		Selected Algorithm	ns
ESP Encryption	AES-GCM-256		@ AES-256	8
	AES-256		-U-	0
	AES-GCM-192			
	@ AES-192			
	AES-GCM	Add		
	i AES			
	3DES			
	ige DES			
	AES-GMAC-256			
			Save	Cancel

Step 13. Choose the newly created **Proposal** or **Proposal** that exists from the list of proposals available. Click **OK**.

on:*	IKEv2 IPsec Proposal			? ×
o Tr e: Set	Available Transform Sets C Search AES-GCM AES-SHA ASA-IPSec-Policy DES_SHA-1	Add	Selected Transform Sets	
Sec Peri s G				
ze:			ок	Cancel

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)

Ļ	Enable Security Ass	ociation (SA) Stree	ath Enforce	ement
L	Enable Perfect Forw	ard Secrecy		
L	Modulus Group:	21	~	
L	Lifetime Duration*:	28800		Seconds (Range 120-2147483647)
L	Lifetime Size:	4608000		Kbytes (Range 10-2147483647)
ľ	—			

Step 15. Check the configured settings. Click Save, as shown in this image.

Topology Name:*	VTI-ASA							
		Based (Crypto M	lap) 💿 Route B	ased (VTI)				
Network Topology:	++ Poin	t to Point 🛠		💠 Full Mesh				
IKE Version:*	IKEv1	✓ IKEv2						
Endpoints	IKE	IPsec	Advance	d				
Crypto Map Type:	Static Opyr	namic						
IKEv2 Mode:	Tunnel	~						
Transform Sets:	IKEv1 IPsec Prop	osals 🥜	IKEv2 IPsec P	oposals* 🥜				
	tunnel_aes256_s	iha	ASA-IPSec-Po	licy				
Enable Security A	ssociation (SA) Stre	ngth Enforcem	ent					
Enable Perfect Fo	rward Secrecy							
Modulus Group:	21	*						
Lifetime Duration*:	28800	5	Seconds (Range	120-214748364	17)			
Lifetime Size:	4608000	ł	Kbytes (Range 10	)-2147483647)				
- ESPv3 Setting	gs							
						_		
						6	Save	Cancel

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

au Ruie						
Name	VTI-Traffic		Enabled	Insert into Mand	iatory	~
Action	Allow	V 00.8	ti 5			
Time Range	None 🗸 🕥					
Zones	Networks VLAN Tags A Use	rs Applications	Ports URLs SGT/IS	E Attributes	Inspection Logo	aina Comments
vailable Zor	nes Ĉ		Source Zones (2)		Destination Zones (2)	
Search by	name		In-Zone	8	In-Zone	
- In-Zone		-	- Out-Zone	6	- Out-Zone	
2. Out-Zone				_		
VTI-Zone		Add to				
		Source				
		Add to				
		Destination				
d Rule			1 -			1
d Rule	VTI-Traffic		Z Enabled	Insert into Man	fatory	?
d Rule	VTI-Traffic		Enabled	Insert into Mane	latory	1
d Rule ame ction ime Range	VTI-Traffic    VTI-Traffic     None		Enabled	Insert into Mane	fatory	1 
d Rule ame ction ime Range Zones	VTI-Traffic Allow None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None None Non	rs Applications	Enabled  Final Content of the second secon	Insert into Mana	Jatory Inspection Log	ging Comment:
d Rule ame ction ime Range Zones	VTI-Traffic Allow None VLAN Tags A Use works C	rs Applications	Ports URLs SGT/I Source Networks (2)	Insert into Mand	Inspection Log Destination Networks (2)	ging Comments
Id Rule	VTI-Traffic Allow None Cetworks VLAN Tags Works C ()	rs Applications	Ports URLs SGT/I Source Networks (2)	Insert into Mana	Inspection Log Destination Networks (2)	ging Comments
d Rule ame ction ime Range Zones N vailable Net	VTI-Traffic  Allow None Cetworks VLAN Tags Use works Geolocation	rs Applications	Enabled  Ports URLs SGT/I  Source Networks (2)  Source In-Netwrk	Insert into Mana	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comment
d Rule ame ction ime Range Zones N vailable Net Netwo g IPv4-Privat	VTI-Traffic Allow None None None None Networks VLAN Tags Use works C Other Geolocation te-172.16.0.0-12	Applications	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network Remote-Network	Insert into Mana SE Attributes Original Client	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comment:
Id Rule Iame Ction Time Range Zones Nailable Net Netwo IPv4-Priva IPv4-Priva	VTI-Traffic Allow None VLAN Tags & Use works C works	Add To Source	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network	Insert into Mana SE Attributes Original Client	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
Id Rule Iame Ction Ime Range Zones Netwo IPv4-Priva IPv4-Priva IPv4-Priva	VTI-Traffic   Allow  None  Contraction  None  Contraction  Networks  Contraction  VLAN Tags  Contraction  VLAN Tags  Contraction  Contr	Add To Source Networks	Enabled     Ports URLs SGT/I     Source Networks (2)     Source     In-Netwrk     Remote-Network	Insert into Mand SE Attributes Original Client	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
d Rule lame ction ime Range Zones N vailable Net IPv4-Priva IPv4-Priva IPv4-Priva IPv4-Priva	VTI-Traffic  Allow None Contraction None Contraction None Contraction None Contraction Con	Add To Source Networks	Enabled  Ports URLs SGT/I  Source Networks (2)  Source  In-Netwrk  Remote-Network	Insert into Mand	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
d Rule lame ction ime Range Zones IPv4-Priva IPv4-Priva IPv4-Priva IPv4-Priva IPv6-IPv4- IPv6-Link- IPv6-Link-	VTI-Traffic Allow None VLAN Tags Works VLAN Tags Use Works C VLAN Tags Use Works C C VLAN Tags C VLAN Tags C C C C C C C C C C C C C	Add To Source Networks Add to Destination	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network	Insert into Mana	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
d Rule lame ction ime Range Zones IPv4-Priva IPv4-Priva IPv4-Priva IPv6-IPv4- IPv6-Link- IPv6-Priva IPv6-Priva	VTI-Traffic Allow None VLAN Tags Use works VLAN Tags Use works C works C work	Add To Source Networks Add to Destination	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network	Insert into Mana	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
Id Rule Iame ction Ime Range Zones Invailable Net IPv4-Priva IPv4-Priva IPv4-Priva IPv6-IPv4- IPv6-Inv- IPv6-Cink- IPv6-c	VTI-Traffic Allow None VLAN Tags Use works C Use works C () works C ()	Add To Add To Source Networks Add to Destination	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network	Insert into Mana SE Attributes Original Client	Jatory Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comments
Id Rule Iame Ction Ime Range Zones Ime Range Invailable Net Inv4-Prival IPv4-Prival IPv4-Prival IPv6-IPv4- IPv6-IPv4- IPv6-IPv4- IPv6-Cone Remote-Net VTI-ASA-T	VTI-Traffic Allow None VLAN Tags Use works VLAN Tags Use works C works C work	Add To Source Networks Add to Destination	Enabled  Ports URLs SGT/I  Source Networks (2)  Source Remote-Network  Enter an IP address	Insert into Mand	Jatory Inspection Log Destination Networks (2) Remote-Network Enter an IP addrese	ging Comments

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

Add Static Ro	ute Configuration	? ×
Type: Interface* Available Net Search	IPv4 O IPv6 VTI-ASA (Interface starting with this icon is signifies it is available for route twork C O End to the starting with this icon is signified it is available for route	leak)
In-Netwrk	Add       -Local       Add       icast       ate-10.0.0.0-8       ate-172.16.0.0-12       ate-192.168.0.0-1       ate-All-RFC1918	
Gateway* Metric: Tunneled:	VTI-ASA-Tunnel	
Route Tracking:	С ОК	Cancel

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-121
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>

extranet : ASA-Peer	FTD/VTI-ASA
show crypto ipsec sa peer	> show crypto ipsec sa peer 10.106.67.252
Not applicable for extranet peer	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 decrypt: 100, #pkts verify: 100 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 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 local crypto endpt.: 10.197.224.90/500, remote crypto endpt.:
show vpn-sessiondb detail l2l filter ipaddress	> 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           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         Rem Auth Mode:       preSharedKeys         Loc Auth Mode:       preSharedKeys         Encryption       : AES256         Rekey Int (T):       86400 Seconds         PRF       : SHA512         D/H Group       : 21

#### 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