# Configuración del Túnel VPN Sitio a Sitio Basado en Ruta en FTD Administrado por FMC

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Límites y Restricciones
Pasos de configuración en FMC
Verificación
Desde la GUI de FMC
Desde CLI de FTD

## Introducción

Este documento describe cómo configurar un túnel VPN de sitio a sitio basado en una ruta estática en Firepower Threat Defense administrado por Firepower Management Center.

# Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de cómo funciona un túnel VPN.
- Comprender cómo navegar por el FMC.

### **Componentes Utilizados**

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Cisco Firepower Threat Defense (FTD) versión 6.7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Antecedentes

La VPN basada en rutas permite la determinación del tráfico interesante que se debe cifrar o enviar a través del túnel VPN, y utiliza el ruteo del tráfico en lugar de la política/lista de acceso como en la VPN basada en políticas o en mapas criptográficos. El dominio de cifrado está configurado para permitir el tráfico que entra en el túnel IPsec. Los selectores de tráfico local y remoto IPSec están configurados en 0.0.0.0/0.0.0.0. Esto significa que todo el tráfico enrutado en el túnel IPsec se cifra independientemente de la subred de origen/destino.

Este documento se centra en la configuración de la Interfaz de Túnel Virtual Estática (SVTI). Para obtener información sobre la configuración de la interfaz de túnel virtual dinámico (DVTI) en Secure Firewall, consulte este <u>documento</u>.

#### Límites y Restricciones

Estas son las limitaciones y restricciones conocidas para túneles basados en ruta en FTD:

- Sólo admite IPsec. GRE no es compatible.
- Solo admite interfaces IPv4, así como IPv4, redes protegidas o carga útil de VPN (sin compatibilidad con IPv6).
- El ruteo estático y solamente el protocolo de ruteo dinámico BGP se soporta para las interfaces VTI que clasifican el tráfico para VPN (No soporta otros protocolos como OSPF, RIP, y así sucesivamente).
- Sólo se admiten 100 VTI por interfaz.
- VTI no es compatible con un clúster de FTD.
- VTI no es compatible con estas políticas:
  - •QoS •NAT · Configuración de la plataforma

Estos algoritmos ya no son compatibles con la versión 6.7.0 del FMC/FTD para los nuevos túneles VPN (FMC admite todos los cifrados eliminados para gestionar el FTD < 6.7):

- 3DES, DES y el cifrado NULL no son compatibles con la directiva IKE.
- Los grupos DH 1, 2 y 24 no son compatibles con la directiva IKE y la propuesta IPsec.

- La política IKE no admite la integridad MD5.
- PRF MD5 no es compatible con la política IKE.
- Los algoritmos de cifrado DES, 3DES, AES-GMAC, AES-GMAC-192 y AES-GMAC-256 no son compatibles con la propuesta IPSec.

Nota: Esto se aplica tanto a los túneles VPN basados en políticas como a las rutas entre sitios. Para actualizar un FTD antiguo a 6.7 desde FMC, se activa una comprobación de validación previa que advierte al usuario de los cambios que pertenecen a los cifrados eliminados que bloquean la actualización.

FTD 6.7 gestionado mediante FMC 6.7	Configuración disponible	Túnel VPN de sitio a sitio
Instalación nueva	Cifras débiles disponibles pero que no se pueden utilizar para configurar el dispositivo FTD 6.7.	Cifras débiles disponibles pero que no se pueden utilizar para configurar el dispositivo FTD 6.7.
Actualización: FTD solo configurado con cifrados débiles	Actualización desde FMC 6.7 UI, una comprobación previa a la validación muestra un error. La actualización se bloquea hasta que se vuelva a configurar.	Después de la actualización de FTD, y suponga que el peer no ha cambiado su configuración, entonces el túnel se termina.
Actualización: FTD solo se configura con algunas cifras débiles y algunas cifradas fuertes	Actualización desde FMC 6.7 UI, una comprobación previa a la validación muestra un error. La actualización se bloquea hasta que se vuelva a configurar.	Después de la actualización de FTD, y asuma que el peer tiene cifrados fuertes, luego el túnel se restablece.
Actualización: país de clase C (no dispone de una licencia criptográfica segura)	Permitir DES está permitido	Permitir DES está permitido

Nota: No se necesitan licencias adicionales, la VPN basada en ruta se puede configurar en los modos con licencia y de evaluación. Sin cumplimiento de cifrado (funciones de exportación controladas habilitadas), sólo DES se puede utilizar como algoritmo de cifrado.

### Pasos de configuración en FMC

Paso 1. Vaya a Dispositivos >VPN >Sitio a sitio.

Overview Analysis	Policies	Devic	es Obj	jects	AMP Inte	lligence		
Device Management	NAT	VPN v	QoS	Pla	form Settings	FlexConfig	Certificates	
		Site To S	Site					
View By : Group	į	Remote Troubles	Access	D)	Warning (0)	Offline (0)   No	ormal (1)   Dep	loymer

Paso 2. Haga clic en Add VPN, y elija Firepower Threat Defence Device, como se muestra en la imagen.

<b>e</b>	Deploy	System	Help 🔻	admin 🔻
			O A	dd VPN 👻
	Fire	epower Devi	ice	
6	Fire	epower Thre	eat Defense	e Device

Paso 3. Proporcione un nombre de topología y seleccione el tipo de VPN como basado en ruta (VTI). Elija la versión IKE.

A efectos de esta demostración, se entenderá por:

Nombre de topología: VTI-ASA

Versión IKE: IKEv2

Topology Name:*	VTI-ASA		
	O Policy Based (Crypto Map) O Route Based (VTI)		
Network Topology:	Point to Point     Hub and Spoke     Full Mesh		
IKE Version:*	🗌 IKEv1 🗹 IKEv2		

Paso 4. Elija el Dispositivo en el que debe configurarse el túnel, Puede elegir agregar una nueva Interfaz de plantilla virtual (haga clic en el icono +), o seleccione una de la lista que existe.

ndpoints	IKE	IPsec	Advanced			
	Node A		.	Node B		
Device:*	:			Device:*		
FTD		*		Empty	*	
Virtual T	unnel Interface:*			Virtual Tunnel Interface:*	×	
Tunne	I Source IP is Private	Edit VI		Tunnel Source IP is Private	Edit VTI	
Connect	ion Type:*			Connection Type:*		
Bidirectio	onal	*		Bidirectional	*	
Tunnel I Tunnel S Tunnel S	P Address Source Interface Source Interface IP	:		Tunnel IP Address Tunnel Source Interface Tunnel Source Interface IP	:	

Paso 5. Defina los parámetros de la nueva interfaz de túnel virtual. Click OK.

A efectos de esta demostración, se entenderá por:

Nombre: VTI-ASA

Descripción (opcional): Túnel VTI con Extranet ASA

Zona de seguridad: VTI-Zone

ID de túnel: 1

Dirección IP: 192.168.100.1/30

Fuente del túnel: GigabitEthernet0/0 (exterior)

k.I	Add Virtual Tunnel	t to Point   🔆 Hub and Sonke   🕀 Full Mesh Interface			?	×
'S	General					
	Name *:	VTI-ASA		C Enabled		
Ì	Description:	VTI Tunnel with Extranet ASA				
Di	Security Zone:	VTI-Zone	~			
/i	Tunnel ID *:	1		Range: 0 - 10413		
E	IP Address *:	192.168.100.1/30		0		
2	Tunnel Source *:	GigabitEthernet0/0 (Outside)	*			
в						
Fil Fil						
				OK Can	cel	

Paso 6. Haga clic en OK en la ventana emergente que indica que se ha creado el nuevo VTI.



Paso 7. Elija el VTI recién creado o un VTI que exista en Virtual Tunnel Interface. Proporcione la información para el Nodo B (que es el dispositivo par).

A efectos de esta demostración, se entenderá por:

### Dispositivo: Extranet

### Nombre del dispositivo: ASA-Peer

#### Dirección IP del terminal: 10.106.67.252

11	Create New VPN Topo	logy					? ×
1	Topology Name:*	VTI-ASA					
l		O Policy Based (	Crypto Map) 💿 R	Route Base	ed (VTI)		
l	Network Topology:	++ Point to Po	int 🛠 Hub and	Spoke	🕈 Full Mesh		
l	IKE Version:*	🗆 IKEV1 🗹 IKE	v2				
l							
	Endpoints IKE	IPsec	Ad	vanced			
	Nor Device:* FTD Virtual Tunnel Inter VTI-ASA Tunnel Source IP I Connection Type:* Bidirectional Tunnel IP Address Tunnel Source Inter Tunnel Source Inter Additional Configur Route traffic to the Permit VPN traffic	de A  rface:*  Is Private  rface : 192 rface : Outs rface IP : 10.1 ration  ration  ration  : VTI : Rour : AC H	✓ Edit VII ✓ 168.100.1 side .97.224.90 ting Policy Policy	]	Node B Device:* Extranet Device Name*: ASA-Peer Endpoint IP Address*: 10.106.67.252		
						Save Can	cel

Paso 8. Vaya a la pestaña IKE. Puede optar por utilizar una directiva predefinida o hacer clic en el botón + situado junto a la pestaña Directiva y crear una nueva.

	-		NULL-SHA-LATEST		$\mathbf{v}$	
Au	uthentication Type:	Pre-shared	Pre-shared Automatic Key			~
Pr	e-shared Key Length:*	24	Characters	(Range 1-12	27)	

Paso 9. (Opcional, si crea una nueva política IKEv2.) Proporcione un nombre para la política y seleccione los algoritmos que se utilizarán en la política. Click Save.

A efectos de esta demostración, se entenderá por:

Nombre: ASA-IKEv2-Policy

- Algoritmos de integridad: SHA-512
- Algoritmos de cifrado: AES-256

Algoritmos PRF: SHA-512

Grupo Diffie-Hellman: 21

iscription:			
ority: 1			
	(1-65	5535)	
etime: 86400	0 secon	nds (120-2147483647)	
tegrity Algorithms	ailable Algorithms	Selected Algorithm	s
ncryption Algorithms RF Algorithms iffie-Hellman Group	MD5 SHA SHA512 SHA256 SHA384 NULL	dd	

Paso 10. Elija el recién creado o la Política que existe. Seleccione el Tipo de autenticación. Si se utiliza una clave manual precompartida, especifíquela en los cuadros Key y Confirm Key.

A efectos de esta demostración, se entenderá por:

Política: ASA-IKEv2-Policy

Tipo de autenticación: clave manual previamente compartida

Clave: cisco123

Confirmar clave: cisco123

KEv1 Settings   Policy:*   preshared_sha_aes256_dh14_3   Authentication Type:   Pre-shared Automatic Key   Pre-shared Key Length:*   24   Characters   (Range 1-127)   Kev2 Settings   Policy:*   ASA-IKEv2-Policy   Authentication Type:   Pre-shared Manual Key   Key:*   Confirm Key:*   Enforce hex-based pre-shared key only	Endpoints IKE	IPsec	Adv	anced	
Policy:* preshared_sha_aes256_dh14_3   Authentication Type: Pre-shared Automatic Key   Pre-shared Key Length:* 24   Characters (Range 1-127)   KEv2 Settings   Policy:* ASA-IKEv2-Policy   Authentication Type: Pre-shared Manual Key   Key:* •••••••   Confirm Key:* •••••••   Enforce hex-based pre-shared key only	VEv1 Settings				
Policy:* preshared_sha_aes256_dh14_3   Authentication Type: Pre-shared Automatic Key   Pre-shared Key Length:* 24   Characters (Range 1-127)   Kev2 Settings   Policy:* ASA-IKEv2-Policy   Authentication Type: Pre-shared Manual Key   Key:* •••••••   Confirm Key:* •••••••   Enforce hex-based pre-shared key only	KEVI Settings				
Authentication Type: Pre-shared Automatic Key   Pre-shared Key Length: 24   Characters (Range 1-127)   Kev2 Settings   Policy:* ASA-IKEv2-Policy   Authentication Type: Pre-shared Manual Key   Key:* •••••••   Confirm Key:* •••••••   Enforce hex-based pre-shared key only	Policy:*	preshared_sha_aes2	256_dh14_3	× (	0
Pre-shared Key Length:* 24 Characters (Range 1-127)   Key:*   Authentication Type: Pre-shared Manual Key     Key:* ••••••••   Confirm Key:* ••••••••   Enforce hex-based pre-shared key only	Authentication Type:	Pre-shared Automat	ic Key	Y	
KEv2 Settings   Policy:*   ASA-IKEv2-Policy   Authentication Type:   Pre-shared Manual Key   Key:*   Confirm Key:*   Enforce hex-based pre-shared key only	Pre-shared Key Length:*	24 Charact	ers (Rang	e 1-127)	
Policy:* ASA-IKEv2-Policy   Authentication Type: Pre-shared Manual Key   Key:* •••••••   Confirm Key:* •••••••   Enforce hex-based pre-shared key only	KEv2 Settings				
Policy:*       ASA-IKEv2-Policy       Image: Confirm Key:*         Confirm Key:*       •••••••         Enforce hex-based pre-shared key only					
Authentication Type:       Pre-shared Manual Key         Key:*       •••••••         Confirm Key:*       •••••••         Enforce hex-based pre-shared key only					_
Key:*     ••••••       Confirm Key:*     ••••••       □ Enforce hex-based pre-shared key only	Policy:*	ASA-IKEv2-Policy		<b>~</b> (	0
Confirm Key:*  Enforce hex-based pre-shared key only	Policy:* Authentication Type:	ASA-IKEv2-Policy Pre-shared Manual H	(ey	<ul> <li></li> <li><th>0</th></li></ul>	0
Enforce hex-based pre-shared key only	Policy:* Authentication Type: Key:*	ASA-IKEv2-Policy Pre-shared Manual H	(ey	<ul> <li></li> <li></li></ul>	0
	Policy:* Authentication Type: Key:* Confirm Key:*	ASA-IKEv2-Policy Pre-shared Manual H	(ey	<ul> <li>▼</li> <li></li> </ul>	0
	Policy:* Authentication Type: Key:* Confirm Key:*	ASA-IKEv2-Policy Pre-shared Manual H	(ey d pre-shared key	v only	0

Nota: Si ambos terminales están registrados en el mismo FMC, también se puede utilizar la opción de clave automática precompartida.

Paso 11. Vaya a la pestaña IPsec. Puede optar por utilizar una propuesta IPsec IKEv2 predefinida o crear una nueva. Haga clic en el botón Editar situado junto a la ficha Propuesta IKEv2 IPsec.

Crypto Map Type:	Static Opynamic	
IKEv2 Mode:	Tunnel 💙	
Transform Sets:	IKEv1 IPsec Proposals 🥜	IKEv2 IPsec Proposals* 🥜
	tunnel_aes256_sha	AES-GCM
Enable Security A	ssociation (SA) Strength Enforcen	nent

Paso 12. (Opcional, si crea una nueva propuesta IKEv2 IPsec.) Proporcione un nombre para la propuesta y seleccione los algoritmos que se utilizarán en la propuesta. Click Save.

A efectos de esta demostración, se entenderá por:

Nombre: ASA-IPSec-Policy

Hash ESP: SHA-512

Cifrado ESP: AES-256

ame:*	ASA-IPSec-Policy	
SP Hash	Available Algorithms	Selected Algorithms
SP Encryption	AES-GCM-256	🔅 AES-256
	AES-GCM-192 AES-192 AES-GCM AES AES AES DES	Add
	AES-GMAC-256	

Paso 13. Elija la Propuesta o la Propuesta recién creada que exista en la lista de propuestas disponibles. Click OK.

on:*	IKEv2 IPsec Proposal			? ×
	Available Transform Sets C	Se	lected Transform Sets	
o Tr	Search     AES-GCM     AES-SHA		ASA-IPSec-Policy	
Se'	DES_SHA-1	Add		
Sec				- 1
s G				
ura ze:			ок	Cancel

Paso 14. (Opcional) Elija la configuración Perfect Forward Secrecy. Configuración de la duración y el tamaño de la vida útil de IPsec.

A efectos de esta demostración, se entenderá por:

Confidencialidad directa perfecta: grupo de módulos 21

Duración de la vida útil: 28800 (Predeterminado)

Tamaño de vida útil: 4608000 (predeterminado)

Ļ	Enable Security Ass	sociation (SA) St	rength Enforce	ment
L	Enable Perfect Forv	ard Secrecy		
L	Modulus Group:	21	*	
L	Lifetime Duration*:	28800		Seconds (Range 120-2147483647)
L	Lifetime Size:	4608000		Kbytes (Range 10-2147483647)
ľ	-			

Paso 15. Compruebe los parámetros configurados. Haga clic en Save, como se muestra en esta imagen.

Topology Name:*	VTI-ASA					
		Based (Crypto M	ap) 💿 Route Based (VTI)			
Network Topology	r: 🗠 Poin	t to Point 😽	Hub and Spoke 💠 Full Mes			
IKE Version:*	IKEv1	IKEv2				
Endpoints	IKE	IPsec	Advanced			
Crypto Map Type:	Static O Dy	namic				
IKEv2 Mode:	Tunnel	×				
Transform Sets:	IKEv1 IPsec Prop	oosals 🥜	IKEv2 IPsec Proposals* 🥜			
	tunnel_aes256_	sha	ASA-IPSec-Policy			
Enable Security	Association (SA) Str	ength Enforceme	nt			
Enable Perfect Ferres Ferre	orward Secrecy					
Modulus Group:	21	*				
Lifetime Duration*:	28800	S	econds (Range 120-2147483	547)		
Lifetime Size:	4608000	K	bytes (Range 10-214748364)	7)		
	igs					
					Save	Cancel

Paso 16. Configure la política de control de acceso. Vaya a Políticas > Control de acceso > Control de acceso. Edite la política aplicada al FTD.

Nota: sysopt connection permit-vpn no funciona con túneles VPN basados en ruta. Las reglas de control de acceso deben configurarse para las zonas IN-> OUT y OUT -> IN.

Proporcione las Zonas de Origen y las Zonas de Destino en la pestaña Zonas .

Proporcione Redes de origen, Redes de destino en la pestaña Redes. Haga clic en Add (Agregar).

A efectos de esta demostración, se entenderá por:

Zonas de origen: zona interna y zona externa

Zonas de destino: zona externa e interna

Redes de origen: en red y red remota

#### Redes de destino: redes remotas e internas

Name VII-Traffic Finabled Inset in Mandatory VIAN Tags Users Applications Ports URLs SCIT/SE Attributes Insection Longing Comments Action Vian Tage User Applications Ports URLs SCIT/SE Attributes Insection Consection Co	Add Rule						? ×
Action VLAN Tags & Users Applications Parts URLS SCT/ISE Attributes Inspection Looping Comments Available Zones C Source Cones (2) Source Cones (2) Source Cones (2) Source (2) Source Cones (2) Source (2) Source (2) Source (2) Source (2) Source (2) Source (2) Source (2) Source (2) Source (2) Source (2)	Name	VTI-Traffic		Enabled	Insert into Manda	atory	~
None       None         Zones       Networks       VLAN Tags       Users       Applications       Ports       LRLs       SCTU/SE Attributes       Insaection Longins       Comments         Available Zones       Source Zones (2)       Destination Zones (2)       In-Zone       In-Zone <t< th=""><th>Action</th><th>Allow</th><th>V U D .8</th><th>ආ<i>日</i></th><th></th><th></th><th></th></t<>	Action	Allow	V U D .8	ආ <i>日</i>			
Zones       Networks       VLAN Tags       Users       Application       Ports       UILIS       Start/ISE Attributes       Inspection       Lagoing       Comments         Available Zones       C       Surce Zones       C       Destination Zones       C <th>Time Range</th> <th>None</th> <th></th> <th></th> <th></th> <th></th> <th></th>	Time Range	None					
Zones       Networks       VLAN Tags       & Users       Application       Ports       IRLs       SCITISE Attributes       Inspection       Lagging       Comments         Available Zones       C       Destination Zones (2)       Destination Zones (2)       Destination Zones (2)       Destination Zones (2)         Search by name       Im-Zone       Im-Implication       Im-Zone       Im-Z	Time runge						
Available Zones C   Search by name In-Zone   In-Zone In-Zone   In-Zone In-Zone   In-Zone In-Zone   In-Zone In-Zone   In-Zone In-Zone   In-Zone In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     In-Zone     Add to   Destination     Add to     Destination     Add to     Destination     Add to     In-Vetwrk     In-Vetwrks     In-Vetwrk	Zones	Networks VLAN Tags 🛆 Use	rs Applications	Ports URLs SGT/	ISE Attributes	Inspection Loggi	ng Comments
Search hy name	Available Zon	nes Ċ	_	Source Zones (2)		Destination Zones (2)	
Add to Source Add to Destination Add to Destination Add to Destination Add to Destination Add to Destination Add to Destination Time Range None Zones Networks VIAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection In	Search by	name		in-Zone	8	in-Zone	
Add to Add to Add to Add to Destination Add Rule Add Rule	in-Zone			Dut-Zone	6	📸 Out-Zone	6
Add to Destination Add to Destination Add Rule Add Rule	Out-Zone		L	_			
Add to Destination  Add to Destination  Add to Destination  Add Rule   Add to Name	👬 VTI-Zone		Add to				
Add To Source Original Client IPv4-Private-172.16.0.0-12 IPv4-Private-1172.16.0.0-13 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-1172.16.0.0-16 IPv4-Private-118-RC1918 IPv5-Link-Local IPv5-Link-Local IPv5-Link-Local IPv5-Link-Aslay-Anycast IPv5-Link-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Aslay-Asla			Source				
Add Rule Name VTI-Traffic Finabled Insert Into Mandatory Action Allow Time Range None Zones Networks VLAN Tags & Users Applications Ports URLS SGT/ISE Attributes Inspection Logoing Comments Available Networks C Networks C Networks Geolocation IPv4-Private-192.168.0.0-16 Source Network Remote-Network IPv4-Private-NI-RFC1918 IPv4-Private-NI-RFC1918 IPv6-IDv4-Relay-Anycast Remote-Network Enter an IP address Add To Variable Network Enter an IP address Add Cancel			Add to Destination				
Add Rule 27 × Name VTI-Traffic File Finabled Insert into Mandatory Action Allow Set Applications Ports URLs SGT/ISE Attributes Inspection Looging Comments Available Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Looging Comments Available Networks C Destination Networks (2) Networks Geolocation I Pv4-Private-172.16.0.0-12 I Pv4-Private-172.16.0.0-12 I Pv4-Private-All-RFC1918 I Pv4-Private-All-RFC1918 I Pv6-to-1Pv4-Relay-Anycast Remote-Network Prof-to-1Pv4-Relay-Anycast Remote-Network VTI-ASA-Tunnel Enter an IP address Add Cancel							
Add Rule							
Name       VTI-Traffic       Insert       into Mandatory         Action       Allow       Insert       into Mandatory         Time Range       None       Image: No	Add Rule						? ×
Action Allow Time Range None Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Networks C Original Client In-Networks (2) Networks Geolocation IPv4-Private-172.16.0.0-12 IPv4-Private-192.168.0.0-16 IPv4-Private-192.168.0.0-16 IPv6-Link-Local IPv6-IPv4-Relay-Anycast Remote-Network IPv6-to-IPv4-Relay-Anycast Remote-Network IPv6-to-IPv4-Relay-Anycast Remote-Network IPv6-To-IPv4-Relay-Anycast Remote-Network Add to Destination In-Network Enter an IP address Add Enter an IP address Add Add Cancel	Name	VTI Traffic		Eastlad	tores line stores		
Action Time Range None Conserver VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Networks C Source Original Client In-Netwrk Remote-Network Remote-Network Remote-Network Remote-Network Remote-Network Prv4-Private-JInique-Local-Addresses Prv6-Inv4-eligu-Local-Addresses Prv6-tink-Local Prv6-tink-Local Prv6-tink-Local Prv6-tink-Local Prv6-tink-Local Prv6-tink-Local Prv6-tink-Addresses Prv6-tink-Ad	Name	v11-frame		M Enabled	Insert Into Mand	atory	*
Time Range       None       Image	Action	Allow		ta U			
Zones       Networks       VLAN Tags       Users       Applications       Ports       URLs       SGT/ISE Attributes       Inspection       Logging       Comments         Available Networks       C       Source       Networks (2)       Destination       Networks (2)         Networks       Geolocation       In-Network       In-Network       In-Network       In-Network       In-Network         IPv4-Private-192.168.0.0-16       Add To       Source       Networks       In-Network       In-Network       In-Network       In-Network         IPv6-IPv4-Mapped       Add to       Source       Destination       Destination         IPv6-Private-Unique-Local-Addresses       Add to       Destination       Enter an IP address       Add       Enter an IP address       Add         VTI-ASA-Tunnel       Enter an IP address       Add       Enter an IP address       Add	Time Range	None 💌 📀					
Available Networks C       Source Networks (2)       Destination Networks (2)         Networks       Geolocation       In-Netwrk       In-Netwrk         IPV4-Private-172.16.0.0-12       Add To       Remote-Network       In         IPV4-Private-192.168.0.0-16       Add To       Networks       In         IPV4-Private-All-RFC1918       Add to       Networks       In         IPV6-IPv4-Mapped       Add to       Destination       Networks         IPV6-Private-Unique-Local-Addresses       Add to       Destination       Enter an IP address         IPv6-Private-Network       Enter an IP address       Add       Cancel	Zones	letworks VLAN Tags 🔺 Us	ers Applications	Ports URLs SGT	/ISE Attributes	Inspection Logg	ing Comments
Source       Original Client       In-Netwrk         IPv4-Private-172.16.0.0-12       In-Netwrk       Remote-Network         IPv4-Private-192.168.0.0-16       Add To       Source         IPv4-Private-All-RFC1918       Add to       Source         IPv6-IPv4-Mapped       Add to       Destination         IPv6-Private-Unique-Local-Addresses       Add to       Destination         IPv6-to-IPv4-Relay-Anycast       Enter an IP address       Add         VTI-ASA-Tunnel       Enter an IP address       Add	Available Netv	works C	0	Source Networks (2)		Destination Networks (2)	
Networks       Geolocation         IPv4-Private-172.16.0.0-12       In-Netwrk         IPv4-Private-192.168.0.0-16       Remote-Network         IPv4-Private-All-RFC1918       Add To Source         IPv6-IPv4-Mapped       Add to         IPv6-Private-Unique-Local-Addresses       Add to         IPv6-Private-Unique-Local-Addresses       Enter an IP address         VTI-ASA-Tunnel       Enter an IP address				Source	Original Client	💂 In-Netwrk	8
IPv4-Private-172.16.0.0-12   IPv4-Private-192.168.0.0-16   IPv4-Private-192.168.0.0-16   IPv4-Private-All-RFC1918   IPv6-IPv4-Mapped   Add to   Destination     IPv6-Private-Unique-Local-Addresses   IPv6-to-IPv4-Relay-Anycast   Remote-Network   Remote-Network     Enter an IP address   Add   Cancel	Netwo	rks Geolocation		📻 In-Netwrk	6	Remote-Network	8
IPv4-Private-192.168.0.0-16   IPv4-Private-All-RFC1918   IPv6-IPv4-Mapped   IPv6-Inv-Local   IPv6-Link-Local   IPv6-Private-Unique-Local-Addresses   IPv6-Private-Unique-Local-Addresses   IPv6-to-IPv4-Relay-Anycast   Remote-Network   VTI-ASA-Tunnel    Enter an IP address  Add Cancel	IPv4-Privat	te-172.16.0.0-12		Remote-Network	6		
IPv4-Private-All-RFC1918   IPv6-IPv4-Mapped   IPv6-IPv4-Mapped   IPv6-Link-Local   IPv6-Private-Unique-Local-Addresses   IPv6-Private-Unique-Local-Addresses   IPv6-to-IPv4-Relay-Anycast   Remote-Network   VTI-ASA-Tunnel    Enter an IP address  Add Cancel	IPv4-Privat	te-192.168.0.0-16	Add To Source				
IPv6-IPv4-Mapped       Add to         IPv6-Link-Local       Destination         IPv6-Private-Unique-Local-Addresses       IPv6-to-IPv4-Relay-Anycast         Remote-Network       Enter an IP address         VTI-ASA-Tunnel       Enter an IP address	Pv4-Privat	te-All-RFC1918	Networks				
IPv6-Link-Local       Destination         IPv6-Private-Unique-Local-Addresses       IPv6-Private-Unique-Local-Addresses         IPv6-to-IPv4-Relay-Anycast       Inter an IP address         Remote-Network       Inter an IP address         VTI-ASA-Tunnel       Enter an IP address	IPv6-IPv4-	Mapped	Add to				
IPv6-Private-Unique-Local-Addresses     IPv6-to-IPv4-Relay-Anycast     Remote-Network     VTI-ASA-Tunnel     Inter an IP address     Add     Cancel	IPv6-Link-L	Local					
	IPv6-Privat	te-Unique-Local-Addresses					
VTI-ASA-Tunnel Enter an IP address Add Enter an IP address Add	Protecto-IP	ve-keiay-Anycast					
Add Cancel	VTLASA-T	unnel		Enter an IP address			
Add Cancel	age v 11-9434-10	with the second s		Lines all IF address	Add	Enter an IP address	Add
						Add	Cancel

Paso 17. Agregue el ruteo sobre el túnel VTI. Vaya a Devices > Device Management. Edite el dispositivo en el que está configurado el túnel VTI.

Vaya a Static Route en la pestaña Routing. Haga clic en Agregar ruta.

Proporcione la interfaz, elija la red, proporcione la puerta de enlace. Click OK.

A efectos de esta demostración, se entenderá por:

Interfaz: VTI-ASA

Red: Red remota

Puerta de enlace: Túnel VTI-ASA

Add Static Ro	ute Configuration				? ×
Type: Interface* Available Net Search	IPv4 O IPv6 VTI-ASA (Interface starting with twork C O thmark-Tests -Local icast ite-10.0.0.0-8 ite-172.16.0.0-12 ite-192.168.0.0-1	Add	Selecte	available for rou	te leak)
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel    Used only for defa	ult Route)	<ul> <li>♥ ②</li> <li>(1 - 2)</li> <li>♥ ③</li> </ul>	54)	
				ок	Cancel

Paso 18. Vaya a Deploy > Deployment. Elija el FTD en el que debe implementarse la configuración y haga clic en Deploy.

Configuración enviada a la CLI de FTD después de una implementación correcta:

<#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 protection ipsec profile FMC\_IPSEC\_PROFILE\_1

### Verificación

#### Desde la GUI de FMC

tunnel mode ipsec ipv4

Haga clic en la opción Check Status para monitorear el estado en vivo del túnel VPN desde la propia GUI



Esto incluye estos comandos tomados de la CLI de FTD:

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail I2I filter ipaddress <Peer IP Address>

extranet : ASA-Peer	TTD/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 add           10.197.224.90
	<pre>#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</pre>
show vpn-sessiondb detail l2l filter ipaddress	<pre>&gt; show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252</pre>
Not applicable for extranet peer	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         Rem Auth Mode:       preSharedKeys         Loc Auth Mode:       preSharedKeys         Encryption:       : AES256         Rekey Int (T):       : 86400 Seconds         PRF       : SHA512         D/H Group       : 21

#### Desde CLI de FTD

Estos comandos se pueden utilizar desde la CLI de FTD para ver la configuración y el estado de los túneles VPN.

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

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).