Configureer de routegebaseerde site-to-site VPN-tunnel op FTD die door FMC wordt beheerd

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Beperkingen en beperkingen Configuratiestappen op FMC Verifiëren Van FMC GUI Van FTD CLI

Inleiding

Dit document beschrijft hoe u een routegebaseerde site-to-site VPN-tunnel kunt configureren op basis van een Firepower Threat Defence (FTD) die wordt beheerd door een Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis begrip van hoe een VPN-tunnel werkt.
- Begrijp hoe je door het VCC moet navigeren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Firepower Management Center (FMC) versie 6.7.0
- Cisco Firepower Threat Defence (FTD) versie 6.7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Op route gebaseerde VPN maakt het mogelijk om interessant verkeer te versleutelen of te verzenden via een VPN-tunnel en verkeer te routeren in plaats van beleid/toegangslijst zoals in op beleid gebaseerde of op Crypto-kaart gebaseerde VPN. Het coderingsdomein is ingesteld om verkeer dat de IPsec-tunnel binnenkomt, toe te staan. IPsec Local en Remote Traffic Selectors zijn ingesteld op 0.0.0/0.0.0.0. Dit betekent dat elk verkeer dat in de IPsec-tunnel wordt gerouteerd, wordt versleuteld ongeacht het bron-/doelsubsysteem.

Beperkingen en beperkingen

Dit zijn bekende beperkingen en beperkingen voor routegebaseerde tunnels op FTD:

- Ondersteunt alleen IPsec. GRE wordt niet ondersteund.
- Geen ondersteuning voor Dynamic VTI.
- Ondersteunt alleen IPv4 interfaces, evenals IPv4, beschermde netwerken of VPN-payload (geen ondersteuning voor IPv6).
- Statische routing en alleen BGP Dynamic Routing Protocol worden ondersteund voor VTIinterfaces die verkeer voor VPN classificeren (geen ondersteuning voor andere protocollen zoals OSPF, RIP, enzovoort).
- Slechts 100 VTIs worden ondersteund per interface.
- VTI wordt niet ondersteund op een FTD-cluster.
- VTI wordt niet ondersteund in dit beleid:

·QoS

NAT

·Platforminstellingen

Deze algoritmen worden niet langer ondersteund door FMC/FTD versie 6.7.0 voor nieuwe VPNtunnels (FMC ondersteunt alle verwijderde algoritmen voor het beheer van FTD < 6.7):

- 3DES, DES en NULL-encryptie worden niet ondersteund in IKE-beleid.
- DH-groepen 1, 2 en 24 worden niet ondersteund in IKE-beleid en IPsec-voorstel.
- MD5-integriteit wordt niet ondersteund in IKE-beleid.
- PRF MD5 wordt niet ondersteund in IKE-beleid.
- DES, 3DES, AES-GMAC, AES-GMAC-192 en AES-GMAC-256 versleutelingsalgoritmen worden niet ondersteund in IPsec-voorstel.

Opmerking: dit geldt voor zowel de site-to-site route als voor op beleid gebaseerde VPNtunnels. Om een oudere FTD van het FMC te upgraden naar 6.7, wordt een prevalidatiecontrole gestart waarin de gebruiker wordt gewaarschuwd voor veranderingen die betrekking hebben op de verwijderde algoritmen die de upgrade blokkeren.

FTD 6.7 beheerd via FMC 6.7	Beschikbare configuratie	Site-to-site VPN-tunnel
Fresh Install	Er zijn zwakke algoritmen beschikbaar, maar deze kunnen niet worden gebruikt om het FTD 6.7- apparaat te configureren.	Er zijn zwakke algoritmen beschikbaar, maar deze kunne worden gebruikt om het FTD 6 apparaat te configureren.
Upgraden: FTD alleen geconfigureerd met zwakke algoritmen	Upgrade van FMC 6.7 UI, een pre- validatiecontrole toont een fout. De upgrade wordt geblokkeerd tot de aanpassing.	Na FTD upgrade, en veronders de peer zijn instellingen niet he gewijzigd, dan wordt de tunnel beëindigd.
Upgraden: FTD alleen geconfigureerd met enkele zwakke algoritmen en enkele sterke algoritmen	Upgrade van FMC 6.7 UI, een pre- validatiecontrole toont een fout. De upgrade wordt geblokkeerd tot de aanpassing.	Na FTD-upgrade, en veronders dat de peer sterke algoritmen h dan wordt de tunnel opnieuw ingesteld.
Upgraden: Klasse C-land (geen sterke cryptolicentie)	Toestaan dat DES wordt toegestaan	Toestaan dat DES wordt toege

Opmerking: er is geen extra licentie nodig, routegebaseerde VPN kan worden geconfigureerd in zowel gelicentieerde als evaluatiemodes. Zonder crypto-compatibiliteit (Export Controlled Properties Enabled) kan alleen DES worden gebruikt als een encryptie-algoritme.

Configuratiestappen op FMC

Stap 1. Ga naar Apparaten >VPN >Site to Site.

Overview Analysis	Policies	Devic	es Obj	jects	AMP Inte	lligence		
Device Management	NAT	VPN 🔻	QoS	Pla	form Settings	FlexConfig	Certificates	
		Site To	Site					
View By : Group	7	Remote Trouble	Access shooting	D)	Warning (0)	Offline (0) No	ormal (1) Depl	oymer

Stap 2. Klik op Add VPN en kies Firepower Threat Defence Device, zoals in de afbeelding.



Stap 3. Geef een **topologienaam op** en selecteer het type VPN als **routegebaseerd (VTI)**. Kies de **IKE-versie**.

Ten behoeve van deze demonstratie:

Naam topologie: VTI-ASA

IKE versie: IKEv2

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

Stap 4. Kies het **apparaat** waarop de tunnel moet worden geconfigureerd, U kunt kiezen om een nieuwe **virtuele sjabloon interface** toe te voegen (klik op het + pictogram) of selecteer een van de lijst die bestaat.

ndpoints	IKE	IPsec	Advanced			
	Node A		_	Node B		
Device:*	:		D	evice:*		
FTD		~	E	Empty	*	
Virtual T	unnel Interface:*			irtual Tunnel Interface:*		
Tunne	I Source IP is Private	Edit VI		Tunnel Source IP is Private	Edit VTI	
Connect	ion Type:*		c	onnection Type:*		
Bidirectio	onal	*	E	Bidirectional	*	
Tunnel I Tunnel S Tunnel S	P Address Source Interface Source Interface IP		Т	unnel IP Address unnel Source Interface unnel Source Interface IP	:	

Stap 5. Definieer de parameters van de Nieuwe virtuele tunnelinterface. Klik op OK.

Ten behoeve van deze demonstratie:

Name: VTI-ASA

Beschrijving (optioneel): VTI-tunnel met extranet ASA

Security zone: VTI-zone

Tunnel-ID: 1

IP-adres: 192.168.100.1/30

Tunnelbron: Gigabit Ethernet0/0 (buiten)

kΞ	onology:	🕶 Doint to Doint 🛛 💥 Huh and Snake 🛛 🕀	Full Moch		
	Add Virtual Tu	unnel Interface			? ×
rs	General				
	Name *:	VTI-ASA		Enabled	
	Description:	VTI Tunnel with Extranet ASA			
Di	Security Zone:	VTI-Zone	¥		
Vi	Tunnel ID *:	1	Ra	nge: 0 - 10413	
E	IP Address *:	192.168.100.1/30	0)	
~	Tunnel Source *:	GigabitEthernet0/0 (Outside)	*		
в					
Γι Γι Γι					
				ок	Cancel

Stap 6. Klik op **OK** in de pop-up waarin wordt aangegeven dat het nieuwe VTI is gemaakt.



Stap 7. Kies het nieuwe VTI of een VTI die onder **Virtual Tunnel Interface** bestaat. Verstrek de informatie voor **Knooppunt B** (dat het peer apparaat is).

Ten behoeve van deze demonstratie:

Apparaat: Extranet

Apparaatnaam: ASA-peer

IP-adres eindpunt: 10.106.67.252

11	Create New VPN Topo	logy			? ×
1	Topology Name:*	VTI-ASA			
		O Policy Based (Crypto Map)) 💿 Route B	ased (VTI)	
	Network Topology:	Hu	b and Spoke	💠 Full Mesh	
	IKE Version:*	🗌 IKEv1 🗹 IKEv2			
l	Endpoints IKE	IPsec	Advance	d	
	No Device:* FTD Virtual Tunnel Inte VTI-ASA Tunnel Source IP Connection Type:* Bidirectional	inde A	· •	Node B Device:* Extranet Device Name*: ASA-Peer Endpoint IP Address*: 10.106.67.252	
	Tunnel IP Address Tunnel Source Inte Tunnel Source Inte Additional Configur Route traffic to the Permit VPN traffic	: 192.168.100.1 erface : Outside erface IP : 10.197.224.90 ration () e VTI : <u>Routing Policy</u> : <u>AC Policy</u>			
				Save Cancel	

Stap 8. Navigeer naar het tabblad **IKE**. U kunt ervoor kiezen een vooraf gedefinieerd **beleid** te gebruiken of op de **+**-knop naast het **tabblad Beleid** te klikken en een nieuw tabblad te maken.

Policy:*	AES-GCM-	NULL-SHA-LATES	г	4	0
Authentication Type:	Pre-shared	l Automatic Key		~	
Pre-shared Key Length:*	24	Characters	(Range 1-12	27)	

Stap 9. (Optioneel Als u een nieuw IKEv2-beleid maakt) Geef een **naam** voor het beleid en selecteer de **algoritmen** die in het beleid moeten worden gebruikt. Klik op Save (Opslaan).

Ten behoeve van deze demonstratie:

Name: ASA 5500-IKEv2-beleid

Integriteitsalgoritmen: SHA-512-software

Encryptiealgoritmen: AES-256 router

PRF-algoritmen: SHA-512-software

Diffie-Hellman groep: 21

New IKEv2 Policy			? ×
Name:*	ASA-IKEv2-Policy		
Priority: Lifetime:	1 86400	(1-65535) seconds (120-2147483647)	
Integrity Algorithms	Available Algorithms	Selected Algorithms	
Encryption Algorithms PRF Algorithms Diffie-Hellman Group	Image: MD5 Image: SHA Image: SHA12 Image: SHA256 Image: SHA384 Image:	Add	
		Save Ca	incel

Stap 10. Kies het nieuwe ontwerp of het **beleid** dat bestaat. Selecteer het **verificatietype**. Als een **Vooraf gedeelde handmatige sleutel** wordt gebruikt, geef dan de sleutel op in de **sleutelvakjes** en **bevestig de** sleutelvakjes.

Ten behoeve van deze demonstratie:

Beleid: ASA-IKEv2-Policy

Verificatietype: Vooraf gedeelde handmatige sleutel

Sleutel: Cisco IP123

Bevestig sleutel: Cisco IP123

ndpoints I	KE	IPsec	Advar	nced	
(Ev1 Settings					
Policy:*	prest	hared_sha_aes256_o	dh14_3	*	0
Authentication Typ	e: Pre-s	shared Automatic Ke	у	*	
Pre-shared Key Le	nath * 24	Characters	(Pance	1-127)	
the sharea ney cer	24	Gildraddera	(Range	1-12/)	
KEv2 Settings	24	Characters	(Range	1-127)	
KEv2 Settings Policy:*	ASA-	IKEv2-Policy	(Kalige	· · · · · · · · · · · · · · · · · · ·	0
KEv2 Settings Policy:* Authentication Typ	ASA- e: Pre-s	IKEv2-Policy	(Kange	×	0
KEv2 Settings Policy:* Authentication Typ Key:*	ASA- e: Pre-s	IKEv2-Policy shared Manual Key	(Kange	× ×	0
KEv2 Settings Policy:* Authentication Typ Key:* Confirm Key:*	ASA- e: Pre-s	IKEv2-Policy shared Manual Key	(Kange	×	0

Opmerking: als beide eindpunten op hetzelfde VCC zijn geregistreerd, kan ook de optie **Pre-Shared Automatic Key (Vooraf gedeelde automatische sleutel)** worden gebruikt.

Stap 1. Navigeer naar het tabblad **IPsec**. U kunt een vooraf gedefinieerd **IKEv2 IPsec-voorstel** gebruiken of een nieuw voorstel maken. Klik op de knop Bewerken naast het tabblad **Voorstel voor 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 Ass	ociation (SA) Strength Enforcem	ent

Stap 12. (optioneel Als u een nieuw IKEv2 IPsec-voorstel maakt) Geef een **naam** voor het voorstel en selecteer de **algoritmen** die in het voorstel moeten worden gebruikt. Klik op Save (Opslaan).

Ten behoeve van deze demonstratie:

Name: ASA 5500-IPS beleid

ESP-hash: SHA-512-software

ame:*	ASA-IPSec-Policy			
SP Hash	Available Algorithms		Selected Algorithm	ns
esp encryption	AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES AES AES DES AES-GMAC-256	Add	256 AES-256	
		ſ		1

Stap 13. Kies het nieuwe **voorstel** of **voorstel** uit de lijst met voorstellen die beschikbaar zijn. Klik op OK.

on:*	IKEv2 IPsec Proposal				? ×
	Available Transform Sets	٢	S	elected Transform Sets	
	Search			ASA-IPSec-Policy	8
	AES-GCM				
2.15	(AES-SHA)				
e:	ASA-IPSec-Policy				
Se	@ DES_SHA-1		Add		
Sec					
Perl					
s G					
ıra				OK	Cancel
ze:				,	Cancer

Stap 14. (Optioneel) Kies de **perfecte voorwaartse** instellingen voor **geheimhouding**. Configureer de **duur en** de **grootte van de levensduur van** IPsec.

Ten behoeve van deze demonstratie:

Perfect voorwaartse geheimhouding: Modulus-groep 21

Levensduur: 28800 (standaard)

Levensduur: 4608000 (standaard)

Enable Security Ass	ociation (SA) Strength Enf	forcement	
Enable Perfect Forw	ard Secrecy		
Modulus Group:	21	▼	
Lifetime Duration*:	28800	Seconds (Range 120-2147483647)	
Lifetime Size:	4608000	Kpytes (Range 10-2147483647)	
- ESPv3 Settings			

Stap 15. Controleer de ingestelde instellingen. Klik op **Opslaan**, zoals in deze afbeelding.

Topology Name:*	VTI-ASA				
	O Policy Based (Cry	pto Map) 💿 Route Based (VTI)			
Network Topology	Point to Point	🛠 Hub and Spoke 💠 Full Mesh			
IKE Version:*	🗌 IKEV1 🗹 IKEV2				
Endpoints	IKE IPsec	Advanced			
Crypto Map Type:	Static O Dynamic				
IKEv2 Mode:	Tunnel 💌				
Transform Sets:	IKEv1 IPsec Proposals 🥜	IKEv2 IPsec Proposals* 🥜			
	tunnel_aes256_sha	ASA-IPSec-Policy			
Enable Security	Association (SA) Strength Enfor	rcement			
C Enable Perfect Fo	orward Secrecy				
Modulus Group:	21 👻				
Lifetime Duration*:	28800	Seconds (Range 120-214748364	7)		
Lifetime Size:	4608000	Kbytes (Range 10-2147483647)			
— 🖵 ESPv3 Settin	gs				
				Save	Cancel

Stap 16. (Optioneel) Configureer het **NAT-**beleid. Ga naar **Apparaten > NAT**. **Kies** het NAT-beleid dat aan dit FTD is toegewezen.

Geef de broninterfaceobjecten en de doelinterfaceobjecten op het tabblad Interfaceobjecten op.

Vermeld de oorspronkelijke bron, de **oorspronkelijke bestemming**, de **vertaalde bron**, de **vertaalde bron**, de **vertaalde bestemming** in het **tabblad** Vertaling. Klik op OK.

Ten behoeve van deze demonstratie:

Broninterfaceobjecten: In zone

Doelinterfaceobjecten: out-zone

Oorspronkelijke bron: In het netwerk

Oorspronkelijke bestemming: Remote-Network

Vertaalde bron: In het netwerk

Vertaalde bestemming: Remote-Network

Add NAT Rule							? :
NAT Rule:	Manual NAT Rul	e 👻		Insert: Above R	ule	▼ 1	
Type:	Static	~	🗹 Enal	ble			
Description:							
Interface Objects	Translation	PAT Pool	Advar	oced			
Available Interface O	bjects C			Source Interface Objects (1)		Destination Interface Objects (1)	
🔍 Search by name				in-Zone	8	🚠 Out-Zone	8
🚠 In-Zone					-		
📩 Out-Zone		Ad	ld to				
VTI-Zone		Ad	ld to ination				

ſ	Add NAT Rule										? ×
	NAT Rule: Type: Description:	Manual NAT Ru Static	le 💙	Inse Enable	ert:		Above Rule	v 1			
l	Interface Objects	Translation	PAT Pool	Advanced							
l	Original Packet					-	Translated Packet				
l	Original Source:*	In-Netwr	(~ O		Translated Source:	Address		-	
	Original Destination:	Address			~			In-Netwrk	`	• 0	
		Remote-N	letwork		~ O		Translated Destination:	Remote-Network		• 0	
ľ	Original Source Port:				• 0	t	translated Source Port:			- 0	-
	Original Destination Por	rt:			~ O		Translated Destination Port:		,	• 0	
	1						1	ок	Ca	ncel	

Opmerking: Zorg ervoor dat de statische NAT-vrijstelling voor de site-to-site tunnel wordt toegevoegd bovenop de dynamische NAT/PAT-regels.

Stap 17. Configureer het **toegangscontrolebeleid**. Ga naar **Beleid > Toegangsbeheer > Toegangsbeheer**. **Bewerk** het op het FTD toegepaste beleid.

Opmerking: sysopt connection license-vpn werkt niet met routegebaseerde VPN-tunnels. De toegangscontroleregels moeten worden geconfigureerd voor zowel IN-> OUT-zones als OUT-> IN-zones.

Geef de **bronzones** en de **doelzones op** in het tabblad **Zones**.

Verstrek de **Bronnetwerken**, **Bestemmingsnetwerken** in het tabblad **Netwerken**. Klik op Add (Toevoegen).

Ten behoeve van deze demonstratie:

Source Zones: In-Zone en Out-Zone

Bestemmingszones: out-zone en in-zone

Bronnetwerken: In-Network en Remote-Network

Bestemmingsnetwerken: Remote-Network en In-Network

								? >
Name	VTI-Traffic			Enabled	Insert into Manda	itory	~	
Action	Allow		V 00.81	ta 🗊				
Time Range	None	 O 						
Zonas	Notworks MAN T	ane A Lleare	Applications	Dorte LIDLe SCT/IS	E Attributor	Inspection Log	aina Commente	
vailable Zon	Networks VLAN I	aga <u>a</u> 0acia	Applications	Source Zones (2)	L AITHUITES	Destination Zones (2)	ging comments	3
Search by	name			in-Zone		the In-Zone		8
- Io 7000				Out-Zone	8	Out-Zone		6
A Out-Zone			L		5			
VTI-Zone			Add to	1				
			Source	J				
			Add to					
			Destination					
lame	VII-Traffic			- Enabled	Incast Into Manda	atanı	~	?
Name Action Time Range	VTI-Traffic	v 0	• 00,81	Z Enabled	Insert into Manda	atory	×	?
Name Action Fime Range Zones	VTI-Traffic Allow None VLAN T	▼ ③ [°] ags ▲ Users	Applications	Enabled Ports URLs SGT/I:	Insert into Manda	atory Inspection Log	ging Comment	?
Name Action Time Range Zones N vailable Netv	VTI-Traffic Allow None VLAN T works C	rags ▲ Users	Applications	Enabled Ports URLs SGT/II Source Networks (2)	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Fime Range Zones N vallable Netv	VTI-Traffic Allow None VLAN T works C	rags ▲ Users	Applications	Enabled Ports URLs SGT/I: Source Networks (2) Source	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Inction Time Range Zones N vailable Netv	VTI-Traffic Allow None VLAN T works C rks Ge	rags 🛆 Users	Applications	Enabled Ports URLs SGT/I: Source Networks (2) Source In-Netwrk	Insert into Manda	Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comment	?
Name Action Time Range Zones N vailable Netv Networ 2 IPv4-Privat	VTI-Traffic Allow None None VLAN T works C rks Get te-172.16.0.0-12	ags 🛆 Users	Applications	Enabled Ports URLs SGT/I Source Networks (2) Source Remote-Network	Insert into Manda	Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comment	?
Name Action Fime Range Zones N vailable Netvo Networ IPv4-Privat IPv4-Privat	VTI-Traffic Allow None VLAN T works C rks Ge rks Ge rks. Ge	iags 🛆 Users	Applications	Enabled Ports URLs SGT/II Source Networks (2) Source In-Netwrk Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Time Range Zones N vailable Netvo Networ IPv4-Privat IPv4-Privat IPv4-Privat	VTI-Traffic Allow None VLAN T works C rks Ge te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918	iags 🛆 Users	Applications	Enabled Ports URLs SGT/I: Source Networks (2) Source Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Time Range Zones N vailable Netv Netwo IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4-1 IPv6-IPv4-1	VTI-Traffic Allow None VLAN T works C rks Get te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped local	iags 🛆 Users	Applications	Enabled Ports URLs SGT/I: Source Networks (2) Source In-Netwrk Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Time Range Zones N vailable Netv Netwo IPv4-Privat IPv4-Privat IPv6-Inv4- IPv6-Inv4- IPv6-Ink-L IPv6-Privat	VTI-Traffic Allow None VLAN T works C rks Ge te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unigue-Local-Addres	ags 🛆 Users	Applications Add To Source Networks Add to Destination	Enabled Ports URLs SGT/IS Source Networks (2) Source Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Fime Range Zones N vailable Netvo IPv4-Privat IPv4-Privat IPv6-IPv4-I IPv6-IPv4-I IPv6-Link-L IPv6-c-IPv IPv6-to-IPv	VTI-Traffic Allow None VLAN T works VLAN T works C rks Ge te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addres v4-Relay-Anycast	✓ ② Tags ▲ Users ③ olocation	Add To Source Networks Add to Destination	Enabled Ports URLs SGT/II Source Networks (2) Source In-Netwrk Remote-Network	Insert into Manda	Inspection Log Destination Networks (2) In-Netwrk Remote-Network	ging Comment	?
Vame Action Time Range Zones N Vailable Netvo IPv4-Privat IPv4-Privat IPv6-IPv4-1 IPv6-IPv4-1 IPv6-Clnk-L IPv6-clnk-L IPv6-clnk-L Remote-Ne	VTI-Traffic Allow None VLAN T works C rks Ge te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addres v4-Relay-Anycast stwork	iags 🛆 Users	Applications Add To Source Networks Add to Destination	Enabled Ports URLs SGT/I: Source Networks (2) Source Remote-Network	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Name Action Fime Range Zones N vailable Netv IPv4-Privat IPv4-Privat IPv6-Inv4-I IPv6-Privat IPv6-c-Inv Remote-Ne VTI-ASA-Tu	VTI-Traffic Allow None VLAN T works C rks Gen te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addres v4-Relay-Anycast stwork unnel	iags 🛆 Users	Add To Source Networks Add to Destination	Enabled Ports URLs SGT/I: Source Networks (2) Source Remote-Network Enter an IP address	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?
Aame Aame Aame Zones N vailable Netv Netwo IPv4-Privat IPv4-Privat IPv6-IPv4-I IPv6-Link-L IPv6-c-IPv Remote-Ne VTI-ASA-Tu	VTI-Traffic Allow None VLAN T works C rks Gen te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addres v4-Relay-Anycast etwork unnel	iags 🛆 Users	Add To Source Networks Add to Destination	Enabled Ports URLs SGT/I: Source In-Networks (2) Remote-Network Enter an IP address	Insert into Manda	Inspection Log Destination Networks (2)	ging Comment	?

Stap 18. Voeg de routing toe via de VTI-tunnel. Ga naar **Apparaten > Apparaatbeheer**. **Bewerk** het apparaat waarop de VTI-tunnel is ingesteld.

Navigeer naar statische route onder het tabblad Routing. Klik op Route toevoegen.

Verstrek de interface, kies het netwerk, verstrek de gateway. Klik op OK.

Ten behoeve van deze demonstratie:

Interface: VTI-ASA

Netwerk: Remote-Network

Gateway: VTI-ASA-Tunnel

Add Static Ro	oute Configuration	? ×
Type: Interface*	IPv4 O IPv6 VTI-ASA (Interface starting with this icon signifies it is available for response)	oute leak)
Available Net Search Real any-ipv4 Real In-Netwr Real IPv4-Ben Real IPv4-Ben Real IPv4-Priv Real IPv4-Priv Real IPv4-Priv Real IPv4-Priv	k chmark-Tests c-Local ticast ate-102.168.0.0-12 ate-All-RFC1918	
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel	
	ок	Cancel

Stap 19. Navigeer om > Plaatsing te implementeren. Kies de FTD waarop de configuratie moet worden ingezet en klik op Implementeren.

Configuratie naar de FTD CLI geduwd na succesvolle implementatie:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400
crypto ikev2 enable Outside
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
```

```
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2
```

tunnel-group 10.106.67.252 type ipsec-l2l tunnel-group 10.106.67.252 general-attributes default-group-policy .DefaultS2SGroupPolicy tunnel-group 10.106.67.252 ipsec-attributes ikev2 remote-authentication pre-shared-key ***** ikev2 local-authentication pre-shared-key *****

```
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
ip address 192.168.100.1 255.255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4
tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

Verifiëren

Van FMC GUI

Klik op de optie **Status controleren** om de live status van de VPN-tunnel vanuit de GUI zelf te bewaken



Dit omvat de volgende opdrachten die zijn overgenomen van de FTD CLI:

- crypto ipsec tonen als peer <peer IP-adres>
- toon vpn-sessiondb detail I2I filter ipaddress <Peer IP Address>

Tunnel Status		? ×
😑 extranet : ASA-Peer	• FTD/VTI-ASA	P
> show crypto ipsec sa peer	> show crypto ipsec sa peer 10.106.67.252	
Not applicable for extranet peer	<pre>peer address: 10 106 67 252 Crypto map tag:vti-crypto-map-4-0-1, seq num: 652 10.197.224.90 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0. remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0. current_peer: 10.106.67.252 #pkts encaps: 100, #pkts encrypt: 100, #pkts diges #pkts decaps: 100, #pkts decrypt: 100, #pkts diges #pkts ompressed: 0, #pkts decompressed: 0 #pkts not compressed: 100, #pkts comp failed: 0, # failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #ff created: 0</pre>	280, local addr: .0/0/0) 3.0/0/0) st: 100 fy: 100 Wpkts decomp ragments
> show vpn-sessiondb detail l2l filter ipaddress	<pre>#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frg: reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors r #send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.224.90/500, remote cry 10.106.67.252/500</pre>	s needing rcvd: 0 ypto endpt.: 7.252
Not applicable for extranet peer		
	Session Type: LAN-to-LAN Detailed Connection : 10.106.67.252 Index : 44 Protocol : IKEV2 IPsec Encryption : IKEV2: (1)AES256 Bytes : INEV2: (1)SHA512 Bytes : Tx: 10000 Bytes : Stess Rx : 100 Login Time : 03:54:57 Tunnel Zone : 0 IKEv2 Tunnels: 1 IPsec Tunnels: 1	.106.67.252 900
	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 : 2	500 5HA512 36268 Seconds 21
	Refresh	Close

Van FTD CLI

Deze opdrachten kunnen vanuit de FTD CLI worden gebruikt om de configuratie en de status van de VPN-tunnels te bekijken.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.