Konfigurieren eines routenbasierten Site-to-Site-VPN-Tunnels auf dem vom FMC verwalteten FTD

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Einschränkungen und Einschränkungen Konfigurationsschritte auf FMC Überprüfung Von der FMC-GUI Von FTD CLI

Einleitung

In diesem Dokument wird die Konfiguration eines routenbasierten Site-to-Site-VPN-Tunnels auf einem von einem FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis der Funktionsweise eines VPN-Tunnels
- Sie wissen, wie Sie durch das FMC navigieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Routenbasiertes VPN ermöglicht die Bestimmung von interessantem Datenverkehr, der verschlüsselt oder über einen VPN-Tunnel gesendet werden soll, und die Verwendung von Traffic Routing anstelle von Richtlinien/Zugriffslisten, wie in richtlinienbasiertem oder Crypto-Mapbasiertem VPN. Die Verschlüsselungsdomäne ist so festgelegt, dass jeder Datenverkehr, der in den IPsec-Tunnel eintritt, zugelassen wird. Die Auswahl für lokalen und Remote-IPsec-Datenverkehr ist auf 0.0.0/0.0.0.0 festgelegt. Dies bedeutet, dass jeder Datenverkehr, der in den IPsec-Tunnel geleitet wird, unabhängig vom Quell-/Ziel-Subnetz verschlüsselt wird.

Einschränkungen und Einschränkungen

Dies sind bekannte Einschränkungen und Einschränkungen für routenbasierte Tunnel auf FTD:

- Unterstützt nur IPsec. GRE wird nicht unterstützt.
- Dynamisches VTI wird nicht unterstützt.
- Unterstützt nur IPv4-Schnittstellen sowie IPv4, geschützte Netzwerke oder VPN-Nutzlasten (keine Unterstützung für IPv6).
- Für VTI-Schnittstellen, die den VPN-Datenverkehr klassifizieren, wird statisches Routing und nur das dynamische BGP-Routing-Protokoll unterstützt (keine Unterstützung für andere Protokolle wie OSPF, RIP usw.).
- Pro Schnittstelle werden nur 100 VTIs unterstützt.
- VTI wird auf einem FTD-Cluster nicht unterstützt.
- VTI wird in diesen Richtlinien nicht unterstützt:
 - · QoS

NAT

· Plattformeinstellungen

Diese Algorithmen werden auf FMC/FTD Version 6.7.0 für neue VPN-Tunnel nicht mehr unterstützt (FMC unterstützt alle entfernten Chiffren zur Verwaltung von FTD < 6.7):

- 3DES-, DES- und NULL-Verschlüsselung werden von der IKE-Richtlinie nicht unterstützt.
- Die DH-Gruppen 1, 2 und 24 werden von der IKE-Richtlinie und dem IPsec-Vorschlag nicht unterstützt.
- Die MD5-Integrität wird in der IKE-Richtlinie nicht unterstützt.
- PRF MD5 wird in der IKE-Richtlinie nicht unterstützt.

• Die Verschlüsselungsalgorithmen DES, 3DES, AES-GMAC, AES-GMAC-192 und AES-GMAC-256 werden von IPsec Proposal nicht unterstützt.

Hinweis: Dies gilt sowohl für standortübergreifende als auch für richtlinienbasierte VPN-Tunnel. Um eine ältere FTD von FMC auf 6.7 zu aktualisieren, löst sie eine Überprüfung vor der Validierung aus, die den Benutzer vor Änderungen warnt, die sich auf die entfernten Chiffren beziehen, die die Aktualisierung blockieren.

FTD 6.7 verwaltet über FMC 6.7	Verfügbare Konfiguration	Site-to-Site-VPN-Tunnel
Neuinstallation	Es sind schwache Chiffren verfügbar, die jedoch nicht für die Konfiguration des FTD 6.7 verwendet werden können. Upgrade von der FMC 6.7-	Es sind schwache Chiffren verfügbar, die jedoch nicht für Konfiguration des FTD 6.7 verwendet werden können.
Upgrade: FTD nur mit schwachen Chiffren konfiguriert	Benutzeroberfläche. Eine Überprüfung vor der Validierung zeigt einen Fehler an. Das Upgrade wird bis zur Neukonfiguration blockiert.	Nach dem FTD-Upgrade und u der Annahme, dass der Peer s Einstellungen nicht geändert h wird der Tunnel beendet.
Upgrade: FTD wurde nur mit einigen schwachen und einigen starken Chiffren konfiguriert.	Upgrade von der FMC 6.7- Benutzeroberfläche. Eine Überprüfung vor der Validierung zeigt einen Fehler an. Das Upgrade wird bis zur Neukonfiguration blockiert.	Nach dem FTD-Upgrade und u der Annahme, dass der Peer s Chiffren hat, wird der Tunnel wiederhergestellt.
Upgrade: Land der Klasse C (keine starke Crypto-Lizenz)	DES zulassen ist zulässig	DES zulassen ist zulässig

Hinweis: Es sind keine zusätzlichen Lizenzen erforderlich. Routen-basiertes VPN kann sowohl im Lizenzierungs- als auch im Evaluierungsmodus konfiguriert werden. Ohne Verschlüsselungskompatibilität (Export Controlled Features Enabled) kann nur DES als Verschlüsselungsalgorithmus verwendet werden.

Konfigurationsschritte auf FMC

Schritt 1: Navigieren Sie zu Geräte > 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	į	Remote Trouble	Access shooting	D)	Warning (0)	Offline (0) No	ormal (1) Depl	oymer

Schritt 2. Klicken Sie auf VPN hinzufügen und wählen Sie Firepower Threat Defense Device, wie

im Bild dargestellt.



Schritt 3: Geben Sie einen **Topologienamen an**, und wählen Sie den VPN-Typ als **routenbasiert** (VTI). Wählen Sie die IKE-Version aus.

Für diese Demonstration gilt Folgendes:

Topologiename: VTI-ASA

IKE-Version: IKEv2

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

Schritt 4. Wählen Sie das **Gerät**, auf dem der Tunnel konfiguriert werden muss. Sie können eine neue **virtuelle Vorlagenschnittstelle** hinzufügen (klicken Sie auf das +-Symbol) oder eine vorhandene Schnittstelle aus der Liste auswählen.

lpoints	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	<u> </u>	Empty Tunnel Source IP is Private	Edit VT	
Connecti	ion Type:*			Connection Type:*		
Bidirectio	onal	~		Bidirectional	*	
Tunnel I	P Address	:		Tunnel IP Address	:	
Tunnel S	ource Interface IP	1		Tunnel Source Interface IP	-	

Schritt 5: Definieren Sie die Parameter der **neuen virtuellen Tunnelschnittstelle**. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

Name: VTI-ASA

Beschreibung (optional): VTI-Tunnel mit Extranet-ASA

Sicherheitszone: VTI-Zone

Tunnel-ID: 1

IP-Adresse: 192.168.100.1/30

Tunnelquelle: GigabitEthernet0/0 (Außenbereiche)

k?	Tonology: Point	n Doint 🗰 Hok and Casks 🕀 Foll Mask				
	Add Virtual Tunnel In	terface			? >	<
rs	General					
	Name *:	VTI-ASA		Enabled		
n,	Description:	VTI Tunnel with Extranet ASA				
Di F	Security Zone:	VTI-Zone	~			
Vi	Tunnel ID *:	1		Range: 0 - 10413		
E	IP Address *:	192.168.100.1/30		0		1
~	Tunnel Source *:	GigabitEthernet0/0 (Outside)	*			
В						
Τι Τι Τι						
				OK Cance	el 🚽	

Schritt 6: Klicken Sie im Popup-Fenster auf **OK**, um anzugeben, dass der neue VTI erstellt wurde.

			Node B
	Virtual Tunnel Interf	face Added	
	VTI has been of Please go to the Interfaces page the VTI.	reated successfu e Device > e to delete/updat	illy. te erface:
00000		ок	is Priva
		Connection	Type:*

Schritt 7: Wählen Sie den neu erstellten VTI oder einen VTI, der unter "Virtual Tunnel Interface" vorhanden ist. Geben Sie die Informationen für Knoten B (das Peer-Gerät) an.

Für diese Demonstration gilt Folgendes:

"Slot0:": Extranet

Gerätename: ASA-Peer

Endpunkt-IP-Adresse: 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	

Schritt 8: Navigieren Sie zur Registerkarte IKE. Sie können eine vordefinierte Richtlinie verwenden oder auf die Schaltfläche + neben der Registerkarte Richtlinie klicken und eine neue erstellen.

Policy:* AES-GCM-NULL-SHA-LATEST Authentication Type: Pre-shared Automatic Key Pre-shared Key Length:* 24 Characters (Range 1-127)	IKEv2 Settings					
Authentication Type: Pre-shared Automatic Key Pre-shared Key Length:* 24 Characters (Range 1-127)	Policy:*	AES-GCM-	NULL-SHA-LATES	T	Y	0
Pre-shared Key Length:* 24 Characters (Range 1-127)	Authentication Type:	Pre-shared	d Automatic Key		*	
	Pre-shared Key Length:*	24	Characters	(Range 1-12	27)	

Schritt 9: (Optional, wenn Sie eine neue IKEv2-Richtlinie erstellen) Geben Sie einen **Namen** für die Richtlinie ein, und wählen Sie die in der Richtlinie zu verwendenden **Algorithmen aus**. Klicken Sie auf **Speichern**.

Für diese Demonstration gilt Folgendes:

Name: ASA-IKEv2-Richtlinie

Integritätsalgorithmen: SHA-512

Verschlüsselungsalgorithmen: AES-256

PRF-Algorithmen: SHA-512

Diffie-Hellman-Gruppe: 21

lew 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: MD5 Image: SHA Image: SHA512 Image: SHA256 Image: SHA384 Image: SHA384 Image: SHA384 Image: SHA384 Image: SHA384 Image: SHA384 Image: SHA384	Add	
		Save	Cancel

Schritt 10: Wählen Sie die neu erstellte oder die vorhandene **Richtlinie**. Wählen Sie den **Authentifizierungstyp aus**. Wenn ein **vorinstallierter manueller Schlüssel** verwendet wird, geben Sie den Schlüssel in den Feldern **Schlüssel** und **Schlüssel bestätigen ein**.

Für diese Demonstration gilt Folgendes:

Richtlinie: ASA-IKEv2-Richtlinie

Authentifizierungstyp: Vorinstallierter manueller Schlüssel

Wichtigste: cisco123

Schlüssel bestätigen: cisco123

Endpoints	IKE	IPsec	Advar	nced	
KEv1 Settings					
Policy:*	pres	hared_sha_aes256_	dh14_3	~	\bigcirc
Authentication Ty	/pe: Pre-	shared Automatic Ke	Ŷ	*	
Pre-shared Key L	ength:* 24	Characters	(Range	1-127)	
KEv2 Settings					
KEv2 Settings Policy:*	ASA	-IKEv2-Policy		~	0
KEv2 Settings Policy:* Authentication Ty	ASA /pe: Pre-	-IKEv2-Policy shared Manual Key		× ×	0
KEv2 Settings Policy:* Authentication Ty Key:*	ASA /pe: Pre-	-IKEv2-Policy shared Manual Key		* *	0
KEv2 Settings Policy:* Authentication Ty Key:* Confirm Key:*	/pe: Pre-	-IKEv2-Policy shared Manual Key		¥ ¥	0

Hinweis: Wenn beide Endpunkte auf demselben FMC registriert sind, kann auch die Option "**Pre-shared Automatic Key**" verwendet werden.

Schritt 11. Navigieren Sie zur Registerkarte **IPsec.** Sie können einen vordefinierten **IKEv2-IPsec-Vorschlag** verwenden oder einen neuen erstellen. Klicken Sie auf die Schaltfläche Bearbeiten neben der Registerkarte **IKEv2 IPsec-Angebot**.

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 Enforcer	nent

Schritt 12: (Optional, wenn Sie einen neuen IKEv2 IPsec-Vorschlag erstellen) Geben Sie einen **Namen** für den Vorschlag an, und wählen Sie die **Algorithmen** aus, die im Vorschlag verwendet werden sollen. Klicken Sie auf **Speichern**.

Für diese Demonstration gilt Folgendes:

Name: ASA-IPSec-Richtlinie

ESP-Hash: SHA-512

scription.	ASA-IPSec-Policy	
P Hash	Available Algorithms	Selected Algorithms
PEncryption	AES-GCM-256 AES-GCM-192 AES-GCM-192 AES-GCM AES AES-GCM AES AES AES AES AES-GCM AES AES AES-GCM	Add

Schritt 13: Wählen Sie aus der Liste der verfügbaren Angebote den neu erstellten Vorschlag oder Vorschlag aus. Klicken Sie auf OK.

on:*	TKEV1 V TKEV2			
	IKEv2 IPsec Proposal			? ×
	Available Transform Sets	0	Selected Transform Sets	
	🔍 Search		ASA-IPSec-Policy	8
T	AES-GCM			
	AES-SHA			
e:	ASA-IPSec-Policy			
Se	@ DES_SHA-1	Add		
Sec				
Perl				
s G				
ira)			ок	Cancel
ze:			· · · · · · · · · · · · · · · · · · ·	

Schritt 14. (Optional) Wählen Sie die Einstellungen **Perfect Forward Secrecy** (**Perfektes Weiterleitungsgeheimnis**) aus. Konfigurieren der IPsec-Lebenszeitdauer und -Größe.

Für diese Demonstration gilt Folgendes:

Perfect Forward Secrecy: Modulgruppe 21

Lebensdauer: 28800 (Standard)

Lebenszeitgröße: 4608000 (Standard)

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

Schritt 15: Überprüfen Sie die konfigurierten Einstellungen. Klicken Sie auf **Speichern**, wie in diesem Bild dargestellt.

Topology Name:*	VTI-ASA				
	O Policy Based (Cry	oto 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 A	ssociation (SA) Strength Enfor	cement			
Enable Perfect Fo	rward Secrecy				
Modulus Group:	21 💙				
Lifetime Duration*:	28800	Seconds (Range 120-2147483647)		
Lifetime Size:	4608000	Kbytes (Range 10-2147483647)			
- ESPv3 Setting	gs				
				Save	Cancel

Schritt 16: Konfigurieren Sie optional die **NAT-**Richtlinie. Navigieren Sie zu **Geräte > NAT**. **Wählen Sie** die diesem FTD zugewiesene NAT-Richtlinie aus.

Geben Sie auf der Registerkarte Interface Objects (Schnittstellenobjekte) die Quellschnittstellenobjekte und die Zielschnittstellenobjekte an.

Geben Sie die Originalquelle, das **ursprüngliche Ziel**, die **übersetzte Quelle** und das **übersetzte Ziel** auf der Registerkarte "**Übersetzung" ein**. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

Quellschnittstellenobjekte: In-Zone

Zielschnittstellenobjekte: Out-Zone

Ursprüngliche Quelle: Im Netzwerk

Ursprüngliches Ziel: Remote-Netzwerk

Übersetzte Quelle: Im Netzwerk

Übersetztes Ziel: Remote-Netzwerk

Add NAT Rule							? >
NAT Rule:	Manual NAT Rule	•		Insert: Above R	ule	▼ 1	
Type:	Static	~	🗹 Enat	ble			
Description:							
Interface Objects	Translation	PAT Pool	Advar	nced			
Available Interface O	bjects C			Source Interface Objects (1)		Destination Interface Objects (1)	
Search by name				🚠 In-Zone	6	🚠 Out-Zone	i
👬 In-Zone					-		
Out-Zone		Ad	d to				
🚠 VTI-Zone		Ad	d to ination				

ſ	Add NAT Rule											?	×
	NAT Rule:	Manual NAT Ru	le 💙	Inse	art:			Above Rule	▼ 1				
ł	Type:	Static	*	Enable									
	Description:			-									
	Interface Objects	Translation	PAT Pool	Advanced									
l	Original Packet					7	Translat	ed Packet					Н
l	Original Source:*	In-Netwr	(× 0		Translated	Source:	Address		~		Ш
	Original Destination:	Address			*				In-Netwrk		*	0	Н
		Remote-N	letwork		× 0		Translated	Destination:	Remote-Netw	vork	*	\bigcirc	Ш
l	Original Source Port:				-	,	translated	Source Port:			•	0	1
	Original Destination Por	rt:			~ O	,	Translated	Destination Port:			*	0	
										ок	Cano	el	

Hinweis: Stellen Sie sicher, dass die Freistellung für statische NAT für den standortübergreifenden Tunnel zusätzlich zu den dynamischen NAT/PAT-Regeln hinzugefügt wird.

Schritt 17: Konfigurieren der **Zugriffskontrollrichtlinie**. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**. **Bearbeiten Sie** die auf das FTD angewendete Richtlinie.

Hinweis: sysopt connection permit-vpn funktioniert nicht mit Routen-basierten VPN-Tunneln. Die Zugriffskontrollregeln müssen sowohl für IN-> OUT-Zonen als auch für OUT -> IN-Zonen konfiguriert werden.

Geben Sie die Quellzonen und die Zielzonen auf der Registerkarte Zonen an.

Geben Sie auf der Registerkarte **"Netzwerke"** die **Namen Quellnetzwerke** und **Zielnetzwerke** ein. Klicken Sie auf Hinzufügen.

Für diese Demonstration gilt Folgendes:

Quellzonen: In- und Out-Zone

Zielzonen: Out-Zone und In-Zone

Quellnetzwerke: In- und Remote-Netzwerk

Zielnetzwerke: Remote-Netzwerk und In-Network

								? ×
Name	VTI-Traffic			Enabled	Insert into Mand	latory	~	•
Action	Allow		V 00.81	1 J				
Time Range	None	0						
Zones N	Networks VLAN Tags	🛆 Users	Applications	Ports URLs SGT/ISE	E Attributes	Inspection Log	ging Comment	ts
Available Zon	ies Ċ			Source Zones (2)		Destination Zones (2)		_
🔍 Search by r	name			🚠 In-Zone	ii ii	🚠 In-Zone		8
In-Zone				🚠 Out-Zone	6	🚠 Out-Zone		8
Out-Zone			L					
🚠 VTI-Zone			Add to					
			Source					
			Add to Destination					
dd Rule								2.5
Name	VTI-Traffic			C Enabled	Insert into Mand	latory		~
Name	VTI-Traffic		V n D. Q	Enabled	Insert into Mano	latory		•
Name Action	VTI-Traffic		• • • • • • • • • • • • • • • • • • •	Enabled	Insert into Mand	latory		~
Name Action Time Range	VTI-Traffic Allow None	0	 ▼ ▼ 0.21 	Enabled	Insert into Mand	latory	v	•
Name Action Time Range Zones	VTI-Traffic Allow None Current VLAN Tags	 O ▲ Users 	Applications	Enabled Ports URLs SGT/IS	Insert into Mand	latory Inspection Log	aging Commen	▼ Its
Name Action Time Range Zones No Available Netw	VTI-Traffic Allow None VLAN Tags works C	⊘ ▲ Users	✓ ◯ D dB 1 Applications	Enabled Ports URLs SGT/IS Source Networks (2)	Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	√
Name Action Time Range Zones No Available Netw	VTI-Traffic Allow None VLAN Tags works C	C A Users C	Applications		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	▼ Its
Name Action Time Range Zones No Available Networ Networ	VTI-Traffic Allow None Kone Kone Kone	On	Applications		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	r Its
Name Action Time Range Zones No Available Networ Networ	VTI-Traffic Allow None Curvers VLAN Tags works C rks Geolocati te-172.16.0.0-12	On	Applications		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	r Its
Name Action Time Range Zones N Available Networ Private Private	VTI-Traffic Allow None VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16	On Users	Applications		Insert into Mand E Attributes Original Client	Inspection Log Destination Networks (2)	aging Commen	r Its
Name Action Time Range Zones No Available Networ IPv4-Private IPv4-Private	VTI-Traffic Allow None VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Manada	⊘ ▲ Users ⊙	Applications	Enabled Ports URLs SGT/IS Source Networks (2) Source In-Netwrk Remote-Network	Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	r its
Name Action Time Range Zones Networ Networ IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-M IPv6-IPv4-M	VTI-Traffic Allow None VLAN Tags works VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local	On On	Applications Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	r Its
Name Action Time Range Zones N Available Networ IPv4-Privato IPv4-Privato IPv4-Privato IPv6-IPv4-N IPv6-Inv4-N IPv6-Link-Lu IPv6-Link-Lu	VTI-Traffic Allow None VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unigue-Local-Addresses	On Users	Applications Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	r its
Name Action Time Range Zones N Available Networ IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-IPv4-N IPv6-Link-Li IPv6-rivate IPv6-rivate	VTI-Traffic Allow None VLAN Tags works VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast	ON Users	Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2) In-Netwrk Remote-Network	2ging Commen	r Its
Name Action Time Range Zones N Available Networ IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-IPv4-N IPv6-Link-Li IPv6-rivate IPv6-rivate IPv6-rivate IPv6-rivate	VTI-Traffic Allow None VLAN Tags works VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast ttwork	ON ON	Applications Applications Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2)	ing Commen	r Its
Name Action Time Range Zones N Available Netw IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-Link-Li IPv6-Vivate IPv6-Vivate IPv6-Vivate IPv6-Vivate IPv6-Vivate IPv6-Vivate IPv6-Vivate	VTI-Traffic Allow None VLAN Tags works VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast ttwork unnel	On	Applications Applications Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2) In-Netwrk Remote-Network Enter an IP address	aging Commen	ts
Name Action Time Range Zones N Available Networ IPv4-Private IPv4-Private IPv4-Private IPv6-IPv4-N IPv6-Inv-L IPv6-Inv-L IPv6-c-IPv Remote-Net VTI-ASA-Tu	VTI-Traffic Allow None VLAN Tags works VLAN Tags works C rks Geolocati te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses vd-Relay-Anycast etwork unnel	On	Applications Applications Add To Source Networks Add to Destination		Insert into Mand	Inspection Log Destination Networks (2)	aging Commen	v lts

Schritt 18: Fügen Sie das Routing über den VTI-Tunnel hinzu. Navigieren Sie zu **Geräte > Geräteverwaltung**. **Bearbeiten Sie** das Gerät, auf dem der VTI-Tunnel konfiguriert ist.

Navigieren Sie auf der Registerkarte Routing zu Static Route. Klicken Sie auf Route hinzufügen.

Stellen Sie die **Schnittstelle bereit**, wählen Sie das **Netzwerk**, und stellen Sie das **Gateway bereit**. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

Schnittstelle: VTI-ASA

Netzwerk: Remote-Netzwerk

Gateway: VTI-ASA-Tunnel

	ute Configuratio	n		? ×
Type: Interface*	IPv4 O IPv6 VTI-ASA (Interface starting w)	ith this icon 👩	signifies it is available f	or route leak)
Available Net	twork C ③	Add	Selected Network	k ork
Gateway* Metric: Tunneled:	VTI-ASA-Tunnel	fault Route)	 ✓ ② (1 - 254) 	

Schritt 19: Navigieren Sie zu **Bereitstellen > Bereitstellung**. Wählen Sie den FTD aus, für den die Konfiguration bereitgestellt werden soll, und klicken Sie auf **Deploy (Bereitstellen)**.

Konfiguration wird nach erfolgreicher Bereitstellung auf die FTD-CLI übertragen:

```
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
```

Überprüfung

Von der FMC-GUI

Klicken Sie auf die Option **Check Status (Status prüfen**), um den Live-Status des VPN-Tunnels über die Benutzeroberfläche selbst zu überwachen.



Dazu gehören die folgenden Befehle aus der FTD-CLI:

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

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, s 10.197.224.90 local ident (addr/mask/prot/port): (0.0 remote ident (addr/mask/prot/port): (0.0 current_peer: 10.106.67.252 #pkts encaps: 100, #pkts encrypt: 100, #pkts decaps: 100, #pkts decompressed #pkts not compressed: 0, #pkts decompressed #pkts not compressed: 100, #pkts comp f failed: 0 #pre-frag successes: 0, #pre-frag failu created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decaps</pre>	eq num: 65280, local addr:).0.0/0.0.0.0/0/0) 0.0.0/0.0.0.0/0/0) #pkts digest: 100 #pkts verify: 100 f: 0 failed: 0, #pkts decomp ures: 0, #fragments sulated frgs needing
> show vpn-sessiondb detail l2l filter ipaddress	<pre>reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid IC #Send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.224.90/500, 10.106.67.252/500 > show vpn-sessiondb detail l2l filter ipaddree </pre>	MP Errors rcvd: 0 , remote crypto endpt.: ss 10.106.67.252
Not applicable for extranet peer	Session Type: LAN-to-LAN Detailed Connection : 10.106.67.252 Index : 44 IP Addi Protocol : IKEv2 IPsec Encryption : IKEv2: (1)AE5256 IPsec: (1)AE Hashing : IKEv2: (1)SHA512 IPsec: (1)5H Bytes Tx : 10000 Bytes F Login Time : 03:54:57 UTC Thu Nov 12 2020 Duration : 0h:02m:12s Tunnel Zone : 0 IKEv2: Tunnels: 1 IPsec Tunnels: 1 IPsec Tunnel ID : 44.1 UUP Src Port : 500 UUP ID Bem Auth Mode precharedKeys	r : 10.106.67.252 :5256 :4512 tx : 10000 Pst Port : 500
	Loc Auth Mode: presharedKeys Encryption : AES256 Hashi Rekey Int (T): 86400 Seconds Rekey PRF : SHA512 D/H (Ing : SHA512 Y Left(T): 86268 Seconds iroup : 21 Refresh Close

Von FTD CLI

Diese Befehle können über die FTD-CLI verwendet werden, um die Konfiguration und den Status der VPN-Tunnel anzuzeigen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.