# Configuration du tunnel VPN site à site basé sur la route sur FTD géré par FMC

### Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Limitations et restrictions Étapes de configuration sur FMC Vérifier À partir de FMC GUI À partir de FTD CLI

### Introduction

Ce document décrit comment configurer un tunnel VPN de site à site basé sur la route sur une défense contre les menaces Firepower gérée par un centre de gestion Firepower.

## Conditions préalables

#### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du fonctionnement d'un tunnel VPN.
- Comprendre comment naviguer dans le FMC.

#### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Management Center (FMC) 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### Informations générales

Le VPN basé sur la route permet de déterminer le trafic intéressant à chiffrer, ou à envoyer sur le tunnel VPN, et d'utiliser le routage du trafic au lieu de la politique/liste d'accès comme dans le VPN basé sur la politique ou basé sur la crypto-carte. Le domaine de chiffrement est configuré pour autoriser tout trafic entrant dans le tunnel IPsec. Les sélecteurs de trafic local et distant IPsec sont définis sur 0.0.0.0/0.0.0.0. Cela signifie que tout trafic acheminé dans le tunnel IPsec est chiffré quel que soit le sous-réseau source/de destination.

#### Limitations et restrictions

Voici les limitations et restrictions connues pour les tunnels basés sur la route sur FTD :

- Prend en charge IPsec uniquement. GRE n'est pas pris en charge.
- Aucune prise en charge de Dynamic VTI.
- Prend en charge uniquement les interfaces IPv4, ainsi que IPv4, les réseaux protégés ou les données utiles VPN (pas de prise en charge d'IPv6).
- Le routage statique et uniquement le protocole de routage dynamique BGP est pris en charge pour les interfaces VTI qui classifient le trafic pour VPN (pas de prise en charge d'autres protocoles tels qu'OSPF, RIP, etc.).
- Seules 100 interfaces VTI sont prises en charge par interface.
- VTI n'est pas pris en charge sur un cluster FTD.
- VTI n'est pas pris en charge dans ces politiques :
  - · QoS
  - •NAT
  - · Paramètres de plate-forme

Ces algorithmes ne sont plus pris en charge sur FMC/FTD version 6.7.0 pour les nouveaux tunnels VPN (FMC prend en charge tous les chiffrements supprimés pour gérer FTD < 6.7) :

- Le chiffrement 3DES, DES et NULL n'est pas pris en charge dans la stratégie IKE.
- Les groupes DH 1, 2 et 24 ne sont pas pris en charge dans la stratégie IKE et la proposition IPsec.
- L'intégrité MD5 n'est pas prise en charge dans la stratégie IKE.
- PRF MD5 n'est pas pris en charge dans la stratégie IKE.

- Les algorithmes de chiffrement DES, 3DES, AES-GMAC, AES-GMAC-192 et AES-GMAC-256 ne sont pas pris en charge dans la proposition IPsec.
- Remarque : cela est vrai pour les tunnels VPN basés sur la route de site à site ainsi que sur les politiques. Afin de mettre à niveau un FTD plus ancien vers 6.7 à partir de FMC, il déclenche un contrôle de pré-validation avertissant l'utilisateur des modifications qui concernent les chiffres supprimés qui bloquent la mise à niveau.

FTD 6.7 géré via FMC 6.7	Configuration disponible	Tunnel VPN de site à site
Nouvelle installation	Chiffres faibles disponibles, mais ne peuvent pas être utilisés pour configurer le périphérique FTD 6.7. Mise à niveau à partir de	Chiffres faibles disponibles, mais ne peuvent pas être utilisés pour configurer le périphérique FTD 6.7.
Mise à niveau : FTD configuré uniquement avec des chiffrements faibles	l'interface utilisateur de FMC 6.7, un contrôle de prévalidation affiche une erreur. La mise à niveau est bloquée jusqu'à la reconfiguration.	Après la mise à niveau FTD, et supposez que l'homologue n'a pas modifié ses paramètres, le tunnel est terminé.
Mise à niveau : FTD configuré uniquement avec des chiffrements faibles et certains chiffrements forts	Mise à niveau à partir de l'interface utilisateur de FMC 6.7, un contrôle de prévalidation affiche une erreur. La mise à niveau est bloquée jusqu'à la reconfiguration.	Après la mise à niveau FTD, et supposez que l'homologue a des chiffres forts, le tunnel se rétablit.
Mise à niveau : pays de classe C (ne dispose pas d'une licence de chiffrement puissante)	Autoriser DES est autorisé	Autoriser DES est autorisé



Nemarque : aucune licence supplémentaire n'est nécessaire, le VPN basé sur la route peut être configuré en mode sous licence et en mode d'évaluation. Sans la conformité au chiffrement (Exportation des fonctionnalités contrôlées activée), seul DES peut être utilisé comme algorithme de chiffrement.

# Étapes de configuration sur FMC

Étape 1. Accédez à Périphériques > VPN > Site à 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	-1	Remote Trouble	Access shooting	D)	Warning (0)	Offline (0)   No	ormal (1)   Depl	loymer

Étape 2. Cliquez sur Add VPN, et choisissez Firepower Threat Defense Device, comme illustré dans l'image.

⊘ (	Deploy	System	Help 🔻	admin 🔻
			💿 A	dd VPN 👻
	Fire	epower Devi	ice	
<i>₽</i> 6	Fire	epower Thre	at Defense	e Device

Étape 3. Indiquez un nom de topologie et sélectionnez le type de VPN comme VTI (Route Based). Sélectionnez la version IKE.

Pour les besoins de cette démonstration :

Nom de la topologie : VTI-ASA

Version IKE : IKEv2

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

Étape 4. Choisissez le Périphérique sur lequel le tunnel doit être configuré, Vous pouvez choisir d'ajouter une nouvelle interface de modèle virtuel (cliquez sur l'icône +), ou sélectionnez-en une dans la liste qui existe.

Endpoints	IKE	IPsec	Advanced			
	Node A		_	Node B		
Device:*	:			Device:*		
FTD		¥		Empty	*	
Virtual T	unnel Interface:*			Virtual Tunnel Interface:*		
-			0	Empty	×	
L Tunne	I Source IP is Private	Edit V H	_	Tunnel Source IP is Private	Edit VII	
Connect	ion Type:*			Connection Type:*		
Bidirectio	onal	*		Bidirectional	*	
Tunnel I	P Address	:		Tunnel IP Address	:	
Tunnel S	Source Interface	1		Tunnel Source Interface	:	
Tunnel S	Source Interface IP	:		Tunnel Source Interface IP	:	

Étape 5. Définissez les paramètres de la nouvelle interface de tunnel virtuel. Click OK.

Pour les besoins de cette démonstration :

Nom : VTI-ASA

Description (en option) : tunnel VTI avec Extranet ASA

Zone de sécurité : VTI-Zone

ID de tunnel : 1

Adresse IP : 192.168.100.1/30

Source du tunnel : GigabitEthernet0/0 (externe)

Ton	dd Virtual Tunnel Inte	Point   🏵 Hub and Sanke   🕀 Full Mech-  erface	? ×
ſ	General		
P	Name *:	VTI-ASA	C Enabled
C	Description:	VTI Tunnel with Extranet ASA	
S	Security Zone:	VTI-Zone	
т	Funnel ID *:	1	Range: 0 - 10413
I	P Address *:	192.168.100.1/30	0
т	Funnel Source *:	GigabitEthernet0/0 (Outside)	
			OK Cancel

Étape 6. Cliquez sur OK dans la fenêtre contextuelle mentionnant que la nouvelle interface VTI a été créée.

		Node B
Virtual Tunnel Interfac	e Added	
VTI has been creat Please go to the D Interfaces page to the VTI.	ited successfully. Device > Device delete/update	erface:
	ок	is Priva
	Connection Typ	e:*

Étape 7. Sélectionnez le VTI nouvellement créé ou un VTI qui existe sous Virtual Tunnel Interface. Fournissez les informations pour le noeud B (qui est le périphérique homologue).

Pour les besoins de cette démonstration :

#### Périphérique : Extranet

#### Nom du périphérique : homologue ASA

#### Adresse IP du point d'extrémité : 10.106.67.252

11	Create New VPN Topo	logy			? ×
	Topology Name:*	VTI-ASA	to Map) 💿 Route B	ased (VTI)	
	Network Topology: IKE Version:*	Point to Point     IKEv1 IKEv2	* Hub and Spoke	Full Mesh	
	Nor Device:* FTD Virtual Tunnel Inter VTI-ASA Tunnel Source IP i Connection Type:* Bidirectional Tunnel IP Address Tunnel Source Inter	de A  rface:*  is Private  : 192.168  erface : 0utside		Node B Device:* Extranet Device Name*: ASA-Peer Endpoint IP Address*: 10.106.67.252	·
	Additional Configur Route traffic to the Permit VPN traffic	ration (1) VTI : <u>Routing</u> : <u>AC Polic</u>	<u>Policy</u> K		Save Cancel

Étape 8. Accédez à l'onglet IKE. Vous pouvez choisir d'utiliser une politique prédéfinie ou cliquer sur le bouton + en regard de l'onglet Politique et en créer une nouvelle.

IKEv2 Settings		
Policy:*	AES-GCM-NULL-SHA-LATEST	٢
Authentication Type:	Pre-shared Automatic Key	
Pre-shared Key Length:*	24 Characters (Range 1-127)	

Étape 9. (Facultatif, si vous créez une nouvelle stratégie IKEv2.) Fournissez un nom pour la stratégie et sélectionnez les algorithmes à utiliser dans la stratégie. Cliquez sur Save.

Pour les besoins de cette démonstration :

Nom : ASA-IKEv2-Policy

Algorithmes d'intégrité : SHA-512

Algorithmes de chiffrement : AES-256

Algorithmes PRF : SHA-512

Diffie-Hellman Groupe : 21

ew IKEv2 Policy			?
Name:*	ASA-IKEv2-Policy		
Description:			
Priority:	1	(1-65535)	
Lifetime:	86400	seconds (120-2147483647)	
Integrity Algorithms	Available Algorithms	Selected Algorithm	s
PRF Algorithms Diffie-Hellman Group	Image: MD5         Image: SHA         Image: SHA256         Image: SHA384         Image: SHA384         Image: NULL	Add SHA512	
		Save	Cancel

Étape 10. Choisissez la politique nouvellement créée ou la politique qui existe. Sélectionnez le type d'authentification. Si une clé manuelle pré-partagée est utilisée, fournissez la clé dans les zones Key et Confirm Key.

Pour les besoins de cette démonstration :

Stratégie : ASA-IKEv2-Policy

Type d'authentification : clé manuelle pré-partagée

Clé : cisco123

Confirmer la clé : cisco123

ndpoints IKE		IPsec	Advanced		
(KEv1 Settings					
Policy:*	preshare	d_sha_aes256_dh1	4_3	• 0	
Authentication Type:	Pre-share	ed Automatic Key		~	
Pre-shared Key Length:	* 24	Characters	(Range 1-127	7)	
KEv2 Settings Policy:*	ASA-IKE	v2-Policy		<b>~</b> ()	
Authentication Type:	Pre-share	ed Manual Key		~	
Key:*	•••••				
Confirm Kourt					
Commit Key.					

Remarque : si les deux terminaux sont enregistrés sur le même FMC, l'option Pre-shared Automatic Key (Clé automatique pré-partagée) peut également être utilisée.

Étape 11. Accédez à l'onglet IPsec. Vous pouvez choisir d'utiliser une proposition IKEv2 IPsec prédéfinie ou d'en créer une nouvelle. Cliquez sur le bouton Modifier en regard de l'onglet IKEv2 IPsec Proposal.

Crypto Map Type:	Static Opynamic					
IKEv2 Mode:	Tunnel	~				
Transform Sets:	IKEv1 IPsec Proposals 🧷		IKEv2 IPsec Proposals* 🥜			
	tunnel_aes256_sha		AES-GCM			
Enable Security Association (SA) Strength Enforcement						

Étape 12. (Facultatif, si vous créez une nouvelle proposition IKEv2 IPsec.) Saisissez un nom pour la proposition et sélectionnez les algorithmes à utiliser dans la proposition. Cliquez sur Save.

Pour les besoins de cette démonstration :

Nom : ASA-IPSec-Policy

Hachage ESP : SHA-512

Cryptage ESP : AES-256

Name:* ASA-IPSec-Policy Description.  ESP Hash ESP Encryption AcS-256 AcS-256 AcS-256 AcS-256 AcS-30CM	ew IKEv2 IPsec P	roposal			?
ESP Hash ESP Encryption Available Algorithms AES-GCM-256 AES-256 AES-256 AES-256 AES-256 AES-256 Add Add Add Add Add Add Add Add Add Ad	Name:*	ASA-IPSec-Policy			
ESP Hash Available Algorithms   ESP Encryption     AES-GCM-256   AES-GCM-192   AES-192   AES-GCM   AES-GCM   AES   DES   AES-GMAC-256	Description.				
ESP Encryption  AES-GCM-256  AES-256  AES-256  AES-256  AES-192  Add  Add  AES  Add  AES  Add  AES  Add  AES  Add  Add	ESP Hash	Available Algorithms		Selected Algorithm	s
AES-256 AES-GCM-192 AES-192 AES-GCM AES AES AES AES AES AES AES AES	ESP Encryption	AES-GCM-256		@ AES-256	8
AES-GCM-192 AES-192 Add Add Add Add Add Add Add Ad		🤹 AES-256			-
AES-192 AES-GCM AES AES DES AES-GMAC-256		AES-GCM-192			
AES-GCM AES DES AES-GMAC-256		@ AES-192	Add		
AES B 3DES B AES-GMAC-256		AES-GCM			
DES AES-GMAC-256		i AES			
AES-GMAC-256		ige 3DES			
Star AES-GMAC-250		AFS CMAC 256			
		wige AES-GMAC-256			
				Save	Cancel

Étape 13. Choisissez la nouvelle proposition ou la nouvelle proposition qui existe dans la liste des propositions disponibles. Click OK.

on:*	IKEv2 IPsec Proposal			? ×
	Available Transform Sets C		Selected Transform Sets	
o Tr	<ul> <li>AES-GCM</li> <li>AES-SHA</li> </ul>	] [		
Se	ASA-IPSec-Policy       OBS_SHA-1	Add		
Sec				
Perl				
s G				
ura'			ок	Cancel
ce:				

Étape 14. (Facultatif) Sélectionnez les paramètres Perfect Forward Secrecy. Configurez la durée de vie et la taille de vie d'IPsec.

Pour les besoins de cette démonstration :

Secret direct parfait : Groupe de modules 21

Durée de vie : 28800 (par défaut)

Durée de vie : 4608000 (par défaut)

Ļ	Enable Security Ass	ociation (SA) Strengt	h 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	-	1		

Étape 15. Vérifiez les paramètres configurés. Cliquez sur Save, comme illustré dans cette image.

Topology Name:*	VTI-ASA					
	O Policy Ba	sed (Crypto Map)	Route Based (VTI)			
Network Topology	++ Point t	o Point 💥 Hut	and Spoke 👇 Full Mesh			
IKE Version:*	IKEv1	IKEv2				
Endpoints	IKE	Psec	Advanced			
Crypto Map Type:	Static O Dyna	mic				
IKEv2 Mode:	Tunnel	v				
Transform Sets:	IKEv1 IPsec Propos	als 🥜 🛛 IK	Ev2 IPsec Proposals* 🥜			
	tunnel_aes256_sha	A	SA-IPSec-Policy			
Enable Security A	ssociation (SA) Streng	gth Enforcement				
C Enable Perfect Fo	rward Secrecy					
Modulus Group:	21	*				
Lifetime Duration*:	28800	Seco	nds (Range 120-2147483647	')		
Lifetime Size:	4608000	Kbyt	es (Range 10-2147483647)			
– 👻 ESPv3 Settin	gs					
					Save	Cancel

Étape 16. (Facultatif) Configurez la stratégie NAT. Accédez à Devices > NAT. Sélectionnez la stratégie NAT affectée à ce FTD.

Fournissez les Objets d'interface source et les Objets d'interface de destination dans l'onglet Objets d'interface.

Fournissez la source d'origine, la destination d'origine, la source traduite, la destination traduite dans l'onglet Traduction. Click OK.

Pour les besoins de cette démonstration :

Objets d'interface source : dans la zone

Objets d'interface de destination : zone de sortie

Source d'origine : In-Network

Destination d'origine : Remote-Network

Source traduite : In-Network

#### Destination traduite : Réseau distant

Add NAT Rule						? >
NAT Rule:	Manual NAT Rul	e 💙	Insert:	Above Rule	▼ 1	
Type:	Static	¥ 🗹 i	Enable			
Description:						
Interface Objects	Translation	PAT Pool Ad	vanced			1
Available Interface O	bjects C		Source Interfac	e Objects (1)	Destination Interface Objects (1)	
🔍 Search by name			in-Zone	6	🖧 Out-Zone	8
🚠 In-Zone						
📩 Out-Zone		Add to				
🚠 VTI-Zone		Add to Destination	on			

[	Add NAT Rule											?	×
	NAT Rule:	Manual NAT Ru	le 💌	Ins	ert:			Above Rule	▼ 1				
	Type:	Static	~	Enable									
	Description:			-									
I	Interface Objects	Translation	PAT Pool	Advanced									1
l	Original Packet					-	Translate	d Packet					
l	Original Source:*	In-Netwri	¢		¥ 0		Translated	Source:	Address		*		Ш
I	Original Destination:	Address			~				In-Netwrk		~	0	Ш
l		Remote-M	letwork		<b>~</b> C		Translated	Destination:	Remote-Netw	ork	~	0	Ш
ľ	Original Source Port:				• 0	1	translated	Source Port:			•	0	1
	Original Destination Port	t:			<b>~</b> 0		Translated	Destination Port:			~	0	
										ок	Cano	el	)

Remarque : assurez-vous que l'exemption NAT statique pour le tunnel site à site est ajoutée en plus des règles NAT/PAT dynamiques.

Étape 17. Configurez la stratégie de contrôle d'accès. Accédez à Politiques > Contrôle d'accès > Contrôle d'accès. Modifiez la stratégie appliquée au FTD.

Remarque : sysopt connection permit-vpn ne fonctionne pas avec les tunnels VPN basés sur la route. Les règles de contrôle d'accès doivent être configurées pour les zones IN-> OUT et OUT -> IN.

Indiquez les zones source et de destination dans l'onglet Zones.

Fournissez les réseaux source, réseaux de destination dans l'onglet Réseaux. Cliquez sur Add.

Pour les besoins de cette démonstration :

Zones source : In-Zone et Out-Zone

Zones de destination : zone de sortie et zone d'entrée

Réseaux sources : réseau interne et réseau distant

Réseaux de destination : réseau distant et réseau interne

Add Rule								? ×
Name	VTI-Traffic	1			Enabled	Insert into Manda	atory	~
Action	Allow				21 E			
Time Range	None	~	0					
Zones	Networks	VLAN Tags	🛆 Users	Applications	Ports URLS SGT/	ISE Attributes	Inspection Loggi	ng Comments
Available Zor	nes C				Source Zones (2)		Destination Zones (2)	
Search by	name				In-Zone	9	in-Zone	
In-Zone					Gi Out-Zone		Gut-Zone	
Out-Zone				<b>L</b>				
VTI-Zone				Add to Source				
				Add to				
				Destination	J			
Add Rule								? X
Name	VTI-Traffic	1			Enabled	Insert into Mand	atory	~
Action	Allow			V UD.Q	ta ∏î			
Time Panne	Nene	~						
nine kange	None							
Zones N	letworks	VLAN Tags	🛆 Users	Applications	Ports URLs SGT	/ISE Attributes	Inspection Logo	ng Comments
Available Net	works C		0		Source Networks (2)		Destination Networks (2)	
					Source	Original Client	📄 In-Netwrk	8
Netwo	rks	Geolocat	ion		🚍 In-Netwrk	6	Remote-Network	6
IPv4-Privat	te-172.16.0.	0-12			Remote-Network	6		
IPv4-Privat	te-192.168.0	.0-16		Add To Source				
Pv4-Privat	te-All-RFC19	18		Networks				
IPv6-IPv4-	Mapped			Add to				
IPv6-Link-I	Local	ent Addresses						
IPv6-to-ID	vd-Relav-Art	car-Addresses						
Remote-Ne	etwork	reat						
VTI-ASA-T	unnel				Enter an IP address	Add	Enter on 10 address	
						Add	Enter an IP address	Add
							Add	Cancel

Étape 18. Ajoutez le routage sur le tunnel VTI. Accédez à Périphériques > Gestion des périphériques. Modifiez le périphérique sur lequel le tunnel VTI est configuré.

Accédez à Static Route sous l'onglet Routing. Cliquez sur Add Route.

Fournissez l'interface, choisissez le réseau, fournissez la passerelle. Click OK.

Pour les besoins de cette démonstration :

Interface : VTI-ASA

Réseau : réseau distant

Passerelle : tunnel VTI-ASA

Add Static Ro	ute Configuratio	n			? X
Type: Interface*	IPv4 O IPv6     VTI-ASA     (Interface starting without)	ith this icon 👩	signifies it is availa	able for route	: leak)
Available Ne Search Search Search Available Ne Search Se	twork C ③	Add	Selected Net	twork Network	
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel	fault Route)	<ul> <li>(1 - 254)</li> <li>(254)</li> </ul>		
				ок	Cancel

Étape 19. Accédez à Déployer > Déploiement. Choisissez le FTD vers lequel la configuration doit être déployée et cliquez sur Deploy.

Configuration envoyée à l'interface de ligne de commande FTD après un déploiement réussi :

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

### Vérifier

#### À partir de FMC GUI

Cliquez sur l'option Check Status pour surveiller l'état en direct du tunnel VPN à partir de

Node B			
	6	/	
FTD / VTI-ASA / 192.168.100.1		<u>A</u>	
		Check status	

Cela inclut les commandes suivantes, extraites de l'interface de ligne de commande FTD :

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

😑 extranet : ASA-Peer	- Ph	• 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 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 #TFC rcvd: 0, #TFC sent: 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::
show was sessiondh datail 101 filter inaddraes		> show you consistent detail 121 filter incidence 10 106 67 252
Net applicable for extract per		> show vph-sessionab detail (2) filter ipadaress 10.100.07.232
		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)AE5256 IPsec: (1)AE5256 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 Refresh Close

### À partir de FTD CLI

Ces commandes peuvent être utilisées à partir de l'interface de ligne de commande FTD pour afficher la configuration et l'état des tunnels 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

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.